Canad. Math. Bull. Vol. **44** (3), 2001 pp. 313–322

Images of mod p Galois Representations Associated to Elliptic Curves

Amadeu Reverter and Núria Vila

Abstract. We give an explicit recipe for the determination of the images associated to the Galois action on p-torsion points of elliptic curves. We present a table listing the image for all the elliptic curves defined over $\mathbb{Q}$ without complex multiplication with conductor less than 200 and for each prime number p.

Introduction

Let E be an elliptic curve defined over a number field K. Let $\overline{K}$ be an algebraic closure of K. Let p be a prime number and let $E[p]$ denote the group of p-torsion points of E. The action of the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ of K on the group $E[p]$ defines a mod p Galois representation

$$\rho_{E,p} \colon G_K \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

As is well known, Serre [4] has shown that whenever E is an elliptic curve without complex multiplication this representation is surjective for all but finitely many prime numbers p.

Let $K(E[p])$ denote the number field generated by the coordinates of the p-torsion points of E. The Galois extension $K(E[p])/K$ has Galois group

$$\mathrm{Gal}\big(K(E[p])/K\big) \cong \rho_{E,p}(G_K) \subseteq \mathrm{GL}_2(\mathbb{F}_p).$$

In this paper we study the Galois groups of $K(E[p])/K$, *i.e.*, the images of the mod p Galois representation associated to E. We analyze the relationship between the image $\rho_{E,p}(G_K)$, the existence of isogenies for E of degree p defined over K and of non-trivial p-torsion points of E defined over K. We determine the image $\rho_{E,p}(G_K)$ for a large family of elliptic curves having an isogeny defined over K of degree p. For $p = 3$ we describe the images of $\rho_{E,3}(G_{\mathbb{Q}})$ in terms of explicit conditions on the polynomial Ψ_3^E whose roots are the x-coordinates of the 3-torsion points of an elliptic curve $E/\mathbb{Q}$. Our main concern is to compute the Galois group $\mathrm{Gal}\big(\mathbb{Q}(E[p])/\mathbb{Q}\big)$ for each prime p and for each elliptic curve E defined over $\mathbb{Q}$ without complex multiplication and with conductor $N \leq 200$, Theorem 3.2 of Section 3 summarizes the results obtained.

Received by the editors August 5, 1999; revised April 20, 2000.
This research has been partially supported by DGES grant PB96-0970-C02-01.
AMS subject classification: 11R32, 11G05, 12F10, 14K02.
Keywords: Galois groups, elliptic curves, Galois representation, isogeny.

https://doi.org/10.4153/CMB-2001-031-1 Published online by Cambridge University Press

1 Images and Isogenies

Let E/K be an elliptic curve defined over a field K of characteristic 0. Let p be a prime number and let χ_p be the mod p cyclotomic character. Let $\rho_{E,p}$ be the mod p Galois representation associated to the p-torsion points $E[p]$ of the elliptic curve E. By the Weil pairing we have that $\det \rho_{E,p}(\sigma) = \chi_p(\sigma)$, for all $\sigma \in G_K$. Observe that the elliptic curve E/K admits an isogeny of degree p defined over K if and only if the image $\rho_{E,p}(G_K)$ is contained in a Borel subgroup. If E_1/K and E_2/K are related by an isogeny defined over K of degree prime to p, then this isogeny induces a G_K-module isomorphism from $E_1[p]$ to $E_2[p]$ and the subgroups $\rho_{E_1,p}(G_K)$ and $\rho_{E_2,p}(G_K)$ of $\mathrm{GL}_2(\mathbb{F}_p)$ are conjugate for all primes p not dividing the degree of the isogeny.

Moreover, we have:

Lemma 1.1 *Let E_1/K, E_2/K be two elliptic curves and $\phi\colon E_1 \to E_2$ be a K-isogeny of degree p. Then the following conditions are equivalent:*

(i) There exists a one-dimensional G_K-stable subspace of $E_1[p]$ not annihilated by ϕ.
(ii) $\rho_{E_1,p}(G_K)$ is contained in a split Cartan subgroup of $\mathrm{GL}_2(E_1[p])$.
(iii) There exists an elliptic curve E_3/K non-K-isomorphic to E_2 and a K-isogeny ϕ': $E_1 \to E_3$ of degree p.

Proposition 1.2 *Let E/K be an elliptic curve with non-trivial p-torsion points defined over K. Then there exists a basis of $E[p]$ such that*

$$\rho_{E,p}(G_K) = \begin{cases} \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix}, & \textit{if } E \textit{ has only one } K\textit{-isogeny of degree } p \\ \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix}, & \textit{otherwise.} \end{cases}$$

Proof We can take a basis such that the image satisfies

$$\begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix} \subseteq \rho_{E,p}(G_K) \subseteq \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

Proposition 1.3 *Let E_1/K, E_2/K be two elliptic curves and $\phi\colon E_1 \to E_2$ be a K-isogeny of degree p. Assume that*

(i) $\chi_p(G_K) \neq \{1\}$.
(ii) E_1 and E_2 have non-trivial K-rational p-torsion points.
(iii) The image $\rho_{E_1,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{smallmatrix}\right)$.

Then the image $\rho_{E_2,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{smallmatrix}\right)$.

Proof $\phi(E_1[p])$ is a G_K-stable line in $E_2[p]$ on which G_K acts via χ_p, and $E_2[p]$ also contains a G_K-stable line on which G_K acts trivially, by assumption (ii). The result follows from (i).

Proposition 1.4 *Let E_1/K, E_2/K be two elliptic curves and $\phi\colon E_1 \to E_2$ be a K-isogeny of degree p. Assume that $E_2(K)[p] = \{0\}$. Then, the curve E_1 has non-trivial K-rational p-torsion points if and only if $\rho_{E_2,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{smallmatrix}\right)$.*

Proof Assume that $E_1(K)[p] \neq \{0\}$. By Proposition 1.2 there exists a $\mathbb{F}_p$-basis $\{P, Q\}$ of $E_1[p]$, such that

$$\rho_{E_1,p}(G_K) = \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

Since $E_2(K)[p] = \{0\}$, we have $\ker \phi = \langle P \rangle$ and $\phi(Q) \neq 0$. Let $P' \in E_2[p]$ be such that $\{\phi(Q), P'\}$ is a $\mathbb{F}_p$-basis of $E_2[p]$.

Then it is easy to see that $\rho_{E_2,p}(G_K) = \left(\begin{smallmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{smallmatrix}\right)$. Conversely, let $\{P, Q\}$ be a $\mathbb{F}_p$-basis of $E_2[p]$ such that $\rho_{E_2,p}(G_K) = \left(\begin{smallmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{smallmatrix}\right)$. Consider $\widehat{\phi}\colon E_2 \to E_1$ the dual isogeny to ϕ. By Lemma 1.1, $\widehat{\phi}(P) = 0$, hence $\widehat{\phi}(Q) \neq 0$ is a K-rational p-torsion point of E_1.

Definition Let E/K be an elliptic curve and let $p \geq 3$ be a prime number. We will say that E is a p-exceptional elliptic curve over K if it satisfies the following conditions:

(i) The elliptic curve E has no non-trivial K-rational p-torsion points.
(ii) There exists an elliptic curve E'/K and a K-isogeny $\phi\colon E \to E'$ of degree p.
(iii) Every elliptic curve E' K-isogenous to E with isogeny of degree p has no non-trivial K-rational p-torsion points.

Remark From the 722 elliptic curves without complex multiplication with conductor ≤ 200, listed in the Antwerp tables [1], only 39 are 3-exceptional over $\mathbb{Q}$, 27 are 5-exceptional over $\mathbb{Q}$, 8 are 7-exceptional over $\mathbb{Q}$, 4 are 11-exceptional over $\mathbb{Q}$ and 4 are 13-exceptional over $\mathbb{Q}$; if $p > 13$ all elliptic curves are non-p-exceptional over $\mathbb{Q}$.

The image of the mod p Galois representation attached to p-exceptional elliptic curves must be studied individually. Using Propositions 1.2 and 1.4 we can give the images of the mod p Galois representation attached to non-p-exceptional elliptic curves which admit a K-isogeny of degree p.

Theorem 1.5 *Let E/K be a non-p-exceptional elliptic curve over K. Assume that E admits a K-isogeny of degree p.*

(i) If $E(K)[p] \neq \{0\}$ and E admits only one K-isogeny of degree p, then there exists a basis of $E[p]$ such that

$$\rho_{E,p}(G_K) = \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

(ii) If $E(K)[p] \neq \{0\}$ and E admits more than one K-isogeny of degree p, then there exists a basis of $E[p]$ such that

$$\rho_{E,p}(G_K) = \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

(iii) If $E(K)[p] = \{0\}$, then there exists a basis of $E[p]$ such that

$$\rho_{E,p}(G_K) = \begin{pmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{pmatrix}.$$

Remark Professor Gerhard Frey has pointed out to us that if E is a non-p-exceptional elliptic curve over K having a K-isogeny of degree p, the twisted curves E_D by the quadratic character χ_D are, in fact, p-exceptional over K, but we can determine the image of the attached mod p Galois representation in this case, since $\rho_{E_D,p} = \rho_{E,p} \otimes \chi_D$ (*cf.* Theorem 3.2).

2 $\rho_{E,p}(G_{\mathbb{Q}})$, for $p \leq 3$

For $p = 2$ it is known that the image of the mod 2 Galois representation associated to an elliptic curve can be determined in terms of the discriminant and the K-rational two-torsion points of E (*cf.* [4, 5.3]). We note that the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ is $\left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$, the cyclic subgroup of order 3, and the cyclic subgroups of order 2 are the conjugated Borel subgroups $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{F}_2)$.

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

$$\rho_{E,2}(G_K) = \begin{cases} \mathrm{GL}_2(\mathbb{F}_2), & \text{if } E(K)[2] = \{0\} \text{ and } \Delta_E \notin K^2 \\ C_3, & \text{if } E(K)[2] = \{0\} \text{ and } \Delta_E \in K^2 \\ C_2, & \text{if } E(K)[2] \neq \{0\} \text{ and } \Delta_E \notin K^2 \\ \{\mathrm{id}\}, & \text{if } E(K)[2] \neq \{0\} \text{ and } \Delta_E \in K^2. \end{cases}$$

In the case $p = 3$, we will describe the image $\rho_{E,3}(G_{\mathbb{Q}})$ through the polynomial Ψ_3^E whose roots are the x-coordinates of the 3-torsion points of an elliptic curve $E/\mathbb{Q}$.

Proposition 2.2 *Let $E/\mathbb{Q}$ be an elliptic curve given by the equation $Y^2 = 4X^3 - g_2X - g_3$. Let $x_0, x_1 \in \overline{\mathbb{Q}}$ be two different roots of the polynomial $\Psi_3^E = 3X^4 - \frac{3}{2}g_2X^2 - 3g_3X - \frac{1}{16}g_2^2$. Then*

$$\mathbb{Q}(E[3]) = \begin{cases} \mathbb{Q}(x_0, x_1, \sqrt{-x_0}, \sqrt{-x_1}), & \text{if } g_2 \neq 0 \\ \mathbb{Q}(\sqrt[3]{g_3}, \sqrt{-g_3}, \sqrt{3g_3}), & \text{if } g_2 = 0. \end{cases}$$

Proof Assume $g_2 \neq 0$. Let $P, Q \in E[3]$ be such that $x_0 = x(P)$, $x_1 = x(Q)$. We can consider $\{P, Q\}$ as a $\mathbb{F}_3$-basis of $E[3]$. Let $\Psi_3^E = 3(X - x_0)q(X)$. Since $q(x_1) = 0$, we have that

$$y_1 = y(Q) = \pm 2\left(x_1 + \frac{4x_0^2 - g_2}{8x_0}\right)\sqrt{-x_0},$$

and

https://doi.org/10.4153/CMB-2001-031-1 Published online by Cambridge University Press

$$y_0 = y(P) = \pm 2\left(x_0 + \frac{4x_1^2 - g_2}{8x_1}\right)\sqrt{-x_1}.$$

Using addition formulae we can explicitely compute $x_2 = x(P+Q)$, $x_3 = x(P-Q)$, $y_2 = y(P+Q)$ and $y_3 = y(P-Q)$. We verify that $x_2, x_3, y_2, y_3 \in \mathbb{Q}(x_0, x_1, y_0, \sqrt{-x_0})$. In the case $g_2 = 0$, we have $\Psi_3^E = 3X(X^3 - g_3)$, $Y^2 = 4X^3 - g_3$ and $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt[3]{g_3}, \sqrt{-g_3}, \sqrt{3g_3})$.

Theorem 2.3 *Let $E/\mathbb{Q}$ be an elliptic curve given by the equation $Y^2 = 4X^3 - g_2X - g_3$ and let $\Psi_3^E = 3X^4 - \frac{3}{2}g_2X^2 - 3g_3X - \frac{1}{16}g_2^2$.*

(a) Assume that $g_2 \neq 0$.

(i) If Ψ_3^E has two rational roots x_0, x_1, then there exists a basis of $E[3]$ such that

$$\rho_{E,3}(G_{\mathbb{Q}}) = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}, & \text{if } -x_0 \in \mathbb{Q}^{*^2} \text{ or } -x_1 \in \mathbb{Q}^{*^2} \\ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, & \text{otherwise.} \end{cases}$$

(ii) If Ψ_3^E has only one rational root x_0, let $x_1 \neq x_0$ be a root of Ψ_3^E, then there exists a basis of $E[3]$ such that

$$\rho_{E,3}(G_{\mathbb{Q}}) = \begin{cases} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, & \text{if } E(\mathbb{Q})[3] = \{0\} \text{ and } \sqrt{-x_0} \notin \mathbb{Q}(x_1, y_0) \\ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}, & \text{if } E(\mathbb{Q})[3] \neq \{0\} \\ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}, & \text{otherwise.} \end{cases}$$

(iii) If Ψ_3^E has no rational roots then

(1) If $\Delta_E \notin \mathbb{Q}^{*^3}$ then $\rho_{E,3}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_3)$.

(2) If $\Delta_E \in \mathbb{Q}^{*^3}$ and Ψ_3^E splits as a product of two irreducible polynomials of degree 2 over $\mathbb{Q}$, then there exists a basis of $E[3]$ such that $\rho_{E,3}(G_{\mathbb{Q}}) = \left\{ \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{smallmatrix}\right) \right\}$.

(3) If $\Delta_E \in \mathbb{Q}^3$ and Ψ_3^E is irreducible, then $\rho_{E,3}(G_{\mathbb{Q}})$ is contained in the normalizer of a non-split Cartan subgroup.

https://doi.org/10.4153/CMB-2001-031-1 Published online by Cambridge University Press

(b) *Assume that* $g_2 = 0$. *Then there exists a basis of* $E[3]$ *such that*

$$\rho_{E,3}(G_{\mathbb{Q}}) = \begin{cases} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}, & \textit{if } g_3 \notin \mathbb{Q}^{*^3},\ -g_3 \in \mathbb{Q}^{*^2} \\ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}, & \textit{if } g_3 \notin \mathbb{Q}^{*^3},\ 3g_3 \in \mathbb{Q}^{*^2} \\ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, & \textit{if } g_3 \in \mathbb{Q}^{*^3},\ -g_3 \notin \mathbb{Q}^{*^2},\ 3g_3 \notin \mathbb{Q}^{*^2} \\ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, & \textit{if } g_3 \notin \mathbb{Q}^{*^3},\ -g_3 \notin \mathbb{Q}^{*^2},\ 3g_3 \notin \mathbb{Q}^{*^2} \\ \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}, & \textit{if } g_3 \in \mathbb{Q}^{*^3},\ -g_3 \textit{ or } 3g_3 \in \mathbb{Q}^{*^2}. \end{cases}$$

Proof First we note that if $\rho_{E,3}(G_{\mathbb{Q}})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of order 2 it is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$, if $\rho_{E,3}(G_{\mathbb{Q}})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of order 4 it is conjugate to $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ and if $\rho_{E,3}(G_{\mathbb{Q}})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of order 6 it is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ or to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.

(a) Assume $g_2 \neq 0$.

(i) If $-x_0 \in \mathbb{Q}^{*^2}$, then by Proposition 2.2 $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-x_1})$, hence $-x_1 \notin \mathbb{Q}^{*^2}$, since the determinant is surjective. If $-x_0$ and $-x_1 \notin \mathbb{Q}^{*^2}$, then $E(\mathbb{Q})[3] = \{0\}$ and $[\mathbb{Q}(\sqrt{-x_0}, \sqrt{-x_1}) : \mathbb{Q}] = 4$.

(ii) Assume that Ψ_3^E has only one rational root x_0. If $E(\mathbb{Q})[3] = \{0\}$ and $-x_0 \in \mathbb{Q}^{*^2}$ then $\mathbb{Q}(E[3]) = \mathbb{Q}(x_1, \sqrt{-x_1})$ has degree 6 over $\mathbb{Q}$ and $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. If $-x_0 \notin \mathbb{Q}^{*^2}$ and $\sqrt{-x_0} \in \mathbb{Q}(x_1, y_0) = \mathbb{Q}(x_1, \sqrt{-x_1})$, we obtain the same, $\mathbb{Q}(E[3]) = \mathbb{Q}(x_1, \sqrt{-x_1})$ and $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. If $E(\mathbb{Q})[3] = \{0\}$, $-x_0 \notin \mathbb{Q}^{*^2}$ and $\sqrt{-x_0} \notin \mathbb{Q}(x_1, y_0)$, then $\mathbb{Q}(E[3])$ has degree 12 over $\mathbb{Q}$ and $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. If $E(\mathbb{Q})[3] \neq \{0\}$ then $y_0 \in \mathbb{Q}$ and $\mathbb{Q}(E[3]) = \mathbb{Q}(x_1, \sqrt{-x_0})$. Since $\big(\mathbb{Q}(E[3]) : \mathbb{Q}\big) \neq 3$, $-x_0 \notin \mathbb{Q}^{*^2}$ and $\big(\mathbb{Q}(E[3]) : \mathbb{Q}\big) = 6$. Then $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.

(iii) Assume that Ψ_3^E has no rational roots. Then Ψ_3^E is irreducible or factors as a product of two irreducible polynomials of degree two.

Using the identification between $\mathrm{Aut}(E[3])/\{\pm 1\} \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ and the symmetric group S_4, we have that $\Delta_E \in \mathbb{Q}^{*^3}$ if and only if $3 \nmid \#\rho_{E,3}(G_{\mathbb{Q}})$. As a consequence, if $\Delta_E \notin \mathbb{Q}^{*^3}$ we have that $\rho_{E,3}(G_{\mathbb{Q}})$ must be $\mathrm{GL}_2(\mathbb{F}_3)$, since it is not contained in a Borel subgroup. If $\Delta_E \in \mathbb{Q}^3$ then $3 \nmid \#\rho_{E,3}(G_{\mathbb{Q}})$ and we have that $\rho_{E,3}(G_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup, taking into account the complex conjugation and cardinality arguments. The polynomial Ψ_3^E factors as a product of two irreducible polynomials of degree two if and only if the Cartan subgroup is split.

https://doi.org/10.4153/CMB-2001-031-1 Published online by Cambridge University Press

(b) Assume $g_2 = 0$. By Proposition 2.2, $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt[3]{g_3}, \sqrt{-g_3}, \sqrt{3g_3})$, in each case we compute the degree of $\mathbb{Q}(E[3])$ over $\mathbb{Q}$ and we obtain the result.

3 Determination of $\rho_{E,p}(G_{\mathbb{Q}})$, $N_E \leq 200$

We recall some conditions for obtaining surjectivity for the mod p Galois representation attached to elliptic curves, which we will use to determine the image $\rho_{E,p}(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$, for $p \geq 5$ prime.

Let $E/\mathbb{Q}$ be an elliptic curve. It is well known, that if the order of $\rho_{E,p}(G_{\mathbb{Q}})$ is divisible by p then $\rho_{E,p}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_p)$ or $\rho_{E,p}(G_{\mathbb{Q}})$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Then, if E does not have any $\mathbb{Q}$-isogeny of degree p, $\rho_{E,p}$ is surjective. On the other hand, by Mazur's results [2], $\rho_{E,p}$ is surjective or $\rho_{E,p}(G_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ or $p \leq 19$ or $p = 37, 43, 67$, or 163.

If the invariant j_E is not an integer and $p \nmid v_\ell(j_E) < 0$, for some prime ℓ, the action of the inertia group on the Tate curve gives an element in $\rho_{E,p}(G_{\mathbb{Q}})$ of order p (*cf.* [3, IV, A.1.5]). Then we have:

Proposition 3.1 *Let $E/\mathbb{Q}$ be an elliptic curve without $\mathbb{Q}$-isogenies of degree $p > 2$ and $p \nmid v_\ell(j_E) < 0$, for some prime ℓ. Then $\rho_{E,p}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_p)$.*

If $E/\mathbb{Q}$ has semistable reduction at $p \neq 5$, then $\rho_{E,p}$ is surjective or the image of $\rho_{E,p}$ is contained in the normalizer of a Cartan subgroup or in a Borel subgroup. For $p = 5$ we obtain the same result if there exists an element $s \in \rho_{E,p}(G_{\mathbb{Q}})$ such that $\mathrm{tr}(s)^2/\det(s) = 3$ (*cf.* [4, 2.7, 2.8]). Moreover, if $E/\mathbb{Q}$ is semistable $\rho_{E,p}$ is surjective for $p \geq 11$ (*cf.* [2, Th. 4]).

If the invariant j_E is an integer we will use Serre-Tate's results (*cf.* [5]) concerning the subgroups Φ_ℓ, for some prime $\ell \neq p$. The action of the inertia group I_ℓ on $E[p]$ factors through the finite quotient Φ_ℓ and it is injective. Moreover, they prove that the group Φ_ℓ is isomorphic to a subgroup of the automorphism group of the reduced curve $\widetilde{E}_\ell/\overline{\mathbb{F}}_\ell$. Then we have the following three cases:

(a) If $\ell \neq 2, 3$ then the group Φ_ℓ is the cyclic group of order 2, 3, 4, or 6, depending on the reduction of the special fiber of the Neron model at ℓ:

  (i) $\#\Phi_\ell = 2$ if and only if $v_\ell(\Delta_E) \equiv 6 \pmod{12}$.

  (ii) $\#\Phi_\ell = 3$ if and only if $v_\ell(\Delta_E) \equiv 4$ or $8 \pmod{12}$.

  (iii) $\#\Phi_\ell = 4$ if and only if $v_\ell(\Delta_E) \equiv 3$ or $9 \pmod{12}$.

  (iv) $\#\Phi_\ell = 6$ if and only if $v_\ell(\Delta_E) \equiv 2$ or $10 \pmod{12}$.

(b) If $\ell = 2$ then Φ_2 is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, of order 2, 3, 4, 6, 8 or 24 and $\#\Phi_2 \cdot v_2(\Delta_E) \equiv 0 \pmod{12}$.

(c) If $\ell = 3$ then Φ_3 is cyclic of order 2, 3, 4 or 6 or a semidirect product of a cyclic group of order 4 and a normal subgroup of order 3.

Now, we can add a new column to the Antwerp tables [1] with the following information: For each elliptic curve E without complex multiplication and for each prime

p, the image $\rho_{E,p}(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$, of the attached Galois representation, *i.e.*, the Galois groups of $\mathbb{Q}(E[p])/\mathbb{Q}$, for all primes p, and all elliptic curves without complex multiplication with conductor $N \leq 200$. We summarize:

Theorem 3.2 *If $E/\mathbb{Q}$ is an elliptic curve without complex multiplication with conductor $N \leq 200$, then:*

(i) *The image $\rho_{E,p}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_p)$, for all prime numbers $p > 13$.*

(ii) *The image $\rho_{E,13}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_{13})$, except for the curves 147A, 147B, 147I and 147J, whose image is contained in a Borel subgroup.*

(iii) *The image $\rho_{E,11}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_{11})$, except for the curves 121F, 121G, 121H and 121I, whose image is contained in a Borel subgroup.*

(iv) *The image $\rho_{E,7}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_7)$, except for the curves 26D, 26E, 162A, 162B, 162C, 162D, 162G, 162H, 162I, 162J, 174G and 174H.*
The image $\rho_{E,7}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_7)$, for the curves 162A, 162B, 162C, 162D, 162G, 162H, 162I and 162J.
The image $\rho_{E,7}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_7)$, for 26D and 174G.
The image $\rho_{E,7}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_7)$, for 26E and 174H.

(v) *The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 11A, 38A, 38C, 50A, 50B, 57F, 58B, 75C, 110C, 123A, 155D and 175A.*
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 11C, 38B, 38E, 50C, 50D, 57G, 58C, 66K, 66L, 75D, 110D, 118C, 123B, 155E and 175B.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 11B and 38D.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 99D, 121B and 176E.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} \pm 1 & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 99C, 121A, 171I and 176D.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & \pm 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_5)$, for the curves 99E, 121C, 171J and 176F.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left\{\left(\begin{smallmatrix} \pm 1 & * \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \pm 2 & * \\ 0 & -1 \end{smallmatrix}\right)\right\}$, for the curves 50E, 50F, 75A, 150G, 150H and 175F.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is conjugate to $\left\{\left(\begin{smallmatrix} 1 & * \\ 0 & \pm 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & * \\ 0 & \pm 2 \end{smallmatrix}\right)\right\}$, for the curves 50G, 50H, 75B, 150E, 150F and 175G.
The image $\rho_{E,5}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_5)$ otherwise.

(vi) *The image $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$, for the curves 14C, 14D, 19B, 26B, 35B, 37C, 54A, 54E, 77D, 91C, 126C, 126D, 158B, 171B, 182B, 189D and 189F.*
The image $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$, for the curves 14A, 14B, 19A, 20A, 20B, 26A, 30A, 30B, 30D, 30E, 34A, 34B, 35A, 37B, 44A, 50E, 50G, 51A, 54B, 54D, 66A, 66B, 77C, 84C, 84D, 90A, 90B, 90G, 90J, 90K, 90L, 90M, 90N, 91B, 92A, 102A, 102B, 106B, 106E, 110A, 110E, 114A, 114B, 116A, 124B, 126E, 126F, 130E, 130F, 138G, 138H, 140A, 142C, 153B, 156A, 156B, 158A, 158H, 162A, 162D, 162E, 162G, 162I, 162J, 162K, 170D, 170F, 170H, 170I, 171C, 172A, 174I, 178A, 180C, 180D, 182A, 186B, 187A, 189A, 189H, 190A, 196C, 198A, 198B, 198G, 198H, 198M and 198N.

https://doi.org/10.4153/CMB-2001-031-1 Published online by Cambridge University Press

The image $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$, *for the curves* 14*E*, 14*F*, 19*C*, 20*C*, 20*D*, 26*C*, 30*C*, 30*F*, 30*G*, 30*H*, 34*C*, 34*D*, 35*C*, 37*D*, 44*B*, 50*F*, 50*H*, 51*B*, 54*C*, 54*F*, 66*C*, 66*D*, 77*E*, 84*E*, 84*F*, 90*C*, 90*D*, 90*E*, 90*F*, 90*H*, 90*I*, 90*O*, 90*P*, 91*D*, 92*B*, 102*C*, 102*D*, 106*C*, 106*F*, 110*B*, 110*F*, 114*C*, 114*D*, 116*B*, 124*C*, 126*A*, 126*B*, 130*G*, 130*H*, 138*I*, 138*J*, 140*B*, 142*D*, 153*A*, 156*C*, 156*D*, 158*C*, 158*I*, 162*B*, 162*C*, 162*F*, 162*H*, 162*L*, 170*E*, 170*G*, 170*J*, 170*K*, 171*A*, 172*B*, 174*J*, 178*B*, 180*A*, 180*B*, 182*C*, 186*C*, 187*B*, 189*E*, 189*G*, 190*B*, 196*D*, 198*C*, 198*D*, 198*E*, 198*F*, 198*O and* 198*P*.

The image $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$, *for the curves* 98*C*, 98*D*, 112*G*, 112*H and* 175*D*.

The image $\rho_{E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$, *for the curves* 50*A*, 50*B*, 50*C*, 50*D*, 80*A*, 80*B*, 80*C*, 80*D*, 98*A*, 98*B*, 98*E*, 98*F*, 100*A*, 100*B*, 100*C*, 100*D*, 112*E*, 112*F*, 112*I*, 112*J*, 150*I*, 150*J*, 150*K*, 150*L*, 150*M*, 150*N*, 150*O*, 150*P*, 175*C*, 175*E*, 176*A*, 176*B*, 196*A and* 196*B*.

The image $\rho_{E,3}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_3)$ *otherwise.*

(vii) The image $\rho_{E,2}(G_{\mathbb{Q}})$ is $\{\mathrm{id}\}$ *for the curves* 15*B*, 15*C*, 15*E*, 17*B*, 17*C*, 21*B*, 21*D*, 24*B*, 24*C*, 30*B*, 30*F*, 33*B*, 39*B*, 40*B*, 42*B*, 42*C*, 45*B*, 45*C*, 45*E*, 48*B*, 48*C*, 55*B*, 56*D*, 57*B*, 62*B*, 63*B*, 63*D*, 66*F*, 70*B*, 72*B*, 75*F*, 75*G*, 75*I*, 78*B*, 80*F*, 90*F*, 90*J*, 96*A*, 96*E*, 98*F*, 99*I*, 102*H*, 102*J*, 105*B*, 112*B*, 114*H*, 117*B*, 120*B*, 120*F*, 120*H*, 126*H*, 126*I*, 129*B*, 130*B*, 130*F*, 138*B*, 141*B*, 144*F*, 144*G*, 147*D*, 147*F*, 150*J*, 150*N*, 153*F*, 154*F*, 161*B*, 168*A*, 168*F*, 171*E*, 174*B*, 182*F*, 192*B*, 192*F*, 192*G*, 192*L*, 192*M*, 192*R*, 195*B*, 195*D*, 195*E*, 198*J and* 200*H*.

The image $\rho_{E,2}(G_{\mathbb{Q}})$ is C_3 for the elliptic curves of conductor 196.

The image $\rho_{E,2}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_2)$ *for the elliptic curves of conductor 11, 19, 26, 35, 37, 38, 43, 44, 50, 51, 54, 58, 61, 67, 76, 79, 83, 88, 89, 91, 92, 100, 101, 104, 106, 109, 110, 115, 118, 121, 122, 123, 124, 131, 135, 139, 140, 143, 149, 152, 162, 163, 166, 172, 175, 176, 179, 186, 187, 189, 190, 197 and for the elliptic curves* 57*E*, 57*F*, 57*G*, 75*A*, 75*B*, 75*C*, 75*D*, 77*C*, 77*D*, 77*E*, 77*F*, 99*C*, 99*D*, 99*E*, 116*A*, 116*B*, 116*E*, 129*E*, 141*E*, 141*H*, 141*I*, 142*C*, 142*D*, 142*E*, 142*F*, 142*G*, 147*A*, 147*B*, 147*I*, 147*J*, 153*A*, 153*B*, 153*C*, 153*D*, 155*C*, 155*D*, 155*E*, 158*A*, 158*B*, 158*C*, 158*D*, 158*E*, 158*H*, 158*I*, 170*C*, 170*D*, 170*E*, 170*F*, 170*G*, 171*A*, 171*B*, 171*C*, 171*H*, 171*I*, 171*J*, 174*E*, 174*F*, 174*G*, 174*H*, 174*I*, 174*J*, 178*A*, 178*B*, 182*A*, 182*B*, 182*C*, 182*D*, 182*I*, 182*J*, 184*A*, 184*B*, 184*C*, 185*A*, 185*D*, 195*I*, 195*J*, 195*K*, 200*A and* 200*B*.

The image $\rho_{E,2}(G_{\mathbb{Q}})$ is C_2 otherwise.

For $p = 2$ or 3, we use the results of Section 2. For $p \geq 5$, we use the results of Section 1 if E has a $\mathbb{Q}$-isogeny of degree p and is non-p-exceptional, otherwise we use the results of the beginning of this section. In the case of 5-exceptional and 7-exceptional elliptic curves it is necessary to study each curve individually. As an example we will examine the images of the mod p Galois representation attached to the 5-exceptional curve 50*E*, for all prime p.

50*E*: $Y^2 + XY + Y = X^3 - X - 2$. $\Delta_E = -2 \cdot 5^4$. Since $\ell = 2$ is a multiplicative reduction prime and $v_2(j_E) = -1 < 0$, then $\rho_{50E,p}$ is surjective, or the image is contained in a Borel subgroup, for all primes p. On the other hand, 50*E* only has $\mathbb{Q}$-isogenies of degree 3 and 5. Then $\rho_{50E,p}$ is surjective, for all primes $p \neq 3, 5$. For

$p = 3$, since $50E(\mathbb{Q})[3] = \{0, (2, 1), (2, -4)\}$ and $50E$ admits only one $\mathbb{Q}$-isogeny of degree 3, we have, by Theorem 1.5, that $\rho_{50E,3}(G_{\mathbb{Q}})$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.

For $p = 5$, the elliptic curve $50E$ is 5-exceptional. Let $K = \mathbb{Q}(\sqrt{5})$, we have $K \subseteq \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(E[5])$, for all elliptic curves E. So, the index $\big(\rho_{E,5}(G_{\mathbb{Q}}) : \rho_{E,5}(G_K)\big) = 2$ and $\chi_5(G_K) = \det \rho_{E,5}(G_K) = \mathbb{F}_5^{*2} = \{\pm 1\}$. By Theorem 1.5 there exists a basis $\{P, Q\}$ of $50A[5]$ such that $\rho_{50A,5}(G_{\mathbb{Q}}) = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ and $\rho_{50A,5}(G_K) = \left(\begin{smallmatrix} 1 & * \\ 0 & \pm 1 \end{smallmatrix}\right)$. Let ϕ the $\mathbb{Q}$-isogeny of degree 5 between $50A$ and $50C$, there exists a basis $\{\phi(Q), P'\}$, such that $\rho_{50C,5}(G_{\mathbb{Q}}) = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Computations on the polynomial Ψ_5^{50C} of 5-torsion points give that $50C[5](K) = \{0\}$. Then in the basis $\{\phi(Q), P'\}$,

$$\begin{pmatrix} \pm 1 & * \\ 0 & 1 \end{pmatrix} = \rho_{50C,5}(G_K) \subseteq \rho_{50C,5}(G_{\mathbb{Q}}) = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Since $50C$ and $50E$ are twisted curves over K, we can consider the K-isomorphism $h\colon 50C \to 50E$. Then, $\big\{ h\big(\phi(Q)\big), h(P') \big\}$ is a $\mathbb{F}_5$-basis of $50E[5]$. Let $\sigma \in G_{\mathbb{Q}}$, since $h^{\sigma} \circ h^{-1} \in \operatorname{Aut}(50E) = \{\pm \mathrm{id}\}$, we have that $\rho_{50E,5}(G_{\mathbb{Q}})$ is a group of order 20 and

$$\begin{pmatrix} \pm 1 & * \\ 0 & 1 \end{pmatrix} = \rho_{50E,5}(G_K) \subseteq \rho_{50E,5}(G_{\mathbb{Q}}) \subseteq \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix}.$$

By Proposition 1.4, $\rho_{50E,5}(G_{\mathbb{Q}}) \not\subseteq \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} \pm 1 & * \\ 0 & 1 \end{smallmatrix}\right) \subseteq \rho_{50E,5}(G_{\mathbb{Q}})$, we have that there exists $a \in \mathbb{F}_5^*$ such that $\left(\begin{smallmatrix} \pm a & * \\ 0 & -1 \end{smallmatrix}\right) \subseteq \rho_{50E,5}(G_{\mathbb{Q}})$. But $\det \rho_{50E,5}(G_{\mathbb{Q}}) = \mathbb{F}_5^*$, so $a = \pm 2$. Consequently,

$$\rho_{50E,5}(G_{\mathbb{Q}}) = \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pm 2 & * \\ 0 & -1 \end{pmatrix} \right\}.$$

References

[1] B. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV.* Lecture Notes in Math. **476**, Springer-Verlag, 1972.

[2] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44**(1978), 129–162.

[3] J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves.* W. A. Benjamin, Inc., 1968.

[4] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), 259–331.

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

Departament de Matemàtiques
I.E.S. Bellvitge
Avda Amèrica, 99
E-08907 L'Hospitalet de Llobregat
Spain
email: areverte@pie.xtec.es

Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
E-08007 Barcelona
Spain
email: vila@cerber.mat.ub.es