Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 417-421, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

POLYNOMIALS OF GALOIS REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

(elliptic curves/galois groups)

AMADEU REVERTER* and NÚRIA VILA**

* Departament de Matemàtiques. I.E.S. Bellvitge. Avda Amèrica, 99. E-08907 L'Hospitalet de Llobregat. Spain. E-mail: 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. e-mail: vila@mat.ub.es

ABSTRACT

We construct polynomials with Galois groups the images of mod p Galois representations attached to elliptic curves. Explicit polynomials are computed for each subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{GL}_2(\mathbb{F}_5)$ that appears as an image for elliptic curves without complex multiplication and with conductor ≤ 200.

RESUMEN

Construimos polinomios cuyos grupos de Galois son las imágenes de la representaciones galoisianas módulo p asociadas a curvas elípticas. Para cada uno de los subgrupos de $\mathrm{GL}_2(\mathbb{F}_3)$ y de $\mathrm{GL}_2(\mathbb{F}_5)$ que aparecen como imagen para las curvas elípticas sin multiplicación compleja y con conductor ≤ 200, calculamos explícitamente polinomios con estos grupos como grupos de Galois sobre el cuerpo de los racionales.

INTRODUCTION

Let E be an elliptic curve defined over a field K of characteristic 0. Let $\overline{K}$ be an algebraic closure of K and $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K. Let p be a prime number and $E[p]$ denote the group of the p-torsion points of E. The Galois group G_K acts naturally on the group $E(\overline{K})$ of all $\overline{K}$-rational points of E. The Galois action of G_K on $E[p]$ defines a mod p Galois representation

$$\rho_{E,p} : G_K \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p).$$

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

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

[1] This research has been partially supported by DGES grant PB96-0970-C02-01.

The purpose of this paper is, given an elliptic curve E defined over K and a prime number p, to find a polynomial with coefficients in K whose Galois group over K will be the group $\rho_{E,p}(G_K) = \mathrm{Gal}\big(K(E[p])/K\big)$.

As is well known, Serre [4] has shown that whenever E is an elliptic curve defined over a number field and without complex multiplication this representation is surjective for all but finitely many prime numbers p. In [2] it is studied the images of the mod p Galois representation associated to elliptic curves having an isogeny defined over K of degree p, the non surjective case. The Galois group $\mathrm{Gal}\big(\mathbb{Q}(E[p])/\mathbb{Q}\big)$ for all elliptic curves E defined over $\mathbb{Q}$ without complex multiplication and with conductor $N \leq 200$, for all primes p, is determined.

In this paper we prove that the Galois group of the polynomial Ψ_p^E, whose roots are the first coordinates of the non-trivial p-torsion points of E, is $\rho_{E,p}(G_K) \simeq \simeq \mathrm{Gal}\big(K(E[p])/K\big)$, for the non-$p$-exceptional elliptic curves over K which admits a K-isogeny of degree p. In the surjective case, that is $\rho_{E,p}(G_K) \simeq \mathrm{Gal}\big(K(E[p])/K\big) \simeq \simeq \mathrm{GL}_2(\mathbb{F}_p)$, we determine an irreducible polynomial with Galois group over K such a group. Finally, we will give examples of polynomials whose Galois group over $\mathbb{Q}$ are $\rho_{E,p}(G_\mathbb{Q})$. More precisely, we will give polynomials for each subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{GL}_2(\mathbb{F}_5)$ that appears as an image of the representation attached to the elliptic curves without complex multiplication with conductor $N \leq 200$.

1. POLYNOMIALS IN NON-p-EXCEPTIONAL CASE

Let E/K be an elliptic curve defined over K, consider a Weierstrass model of E over K. 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 E. By the Weil pairing, $\det \rho_{E,p}(\sigma) = \chi_p(\sigma)$, for all $\sigma \in G_K$.

Definition. Let E/K be an elliptic curve and let $p \neq 2$ 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 exist an elliptic curve E'/K and a K-isogeny $\phi : E \to E'$ 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.

We note that of the 722 elliptic curves over $\mathbb{Q}$ without complex multiplication with conductor ≤200 listed in the Antwerp tables [1], only 31 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 $\mathbb{Q}$.

Theorem 1.1. *Let E be a non-p-exceptional elliptic curve over K that admits a K-isogeny of degree p. Let Ψ_p^E be the polynomial whose roots are the first coordinates of the non-trivial p-torsion points of E. Then the Galois group over K of the polynomial Ψ_p^E is $\rho_{E,p}(G_K) = \mathrm{Gal}(K(E[p])/K)$.*

Proof. By [2, Theorem 1.5], there exists a basis of $E[p]$ such that

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

Then $-\mathrm{id} \notin \rho_{E,p}(G_K)$. Let $K(x(E[p]))$ denote the field generate by the first coordinates of the p-torsion points. It is clear that, if $\sigma \in G_K$ fixes all the x-coordinates, then $\sigma(P) = \pm P$. Moreover, the sign does not depend on the point, if $\sigma(P) = P$ and $\sigma(Q) = -Q$, then $\sigma(P + Q) \neq \pm(P + Q)$. So,

$$\rho_{E,p}(\mathrm{Gal}(K(E[p])/K(x(E[p])))) \subseteq \{\pm \mathrm{id}\}.$$

Therefore, the Galois group over K of the polynomial Ψ_p^E is

$$\rho_{E,p}(G_K) = \mathrm{Gal}(K(E[p])/K).$$

Remark 1.2. *We note that the point, in the above result, is that* $-\mathrm{id}$ *is not in the image $\rho_{E,p}(G_K)$. Therefore, whenever E/K is an elliptic curve with this property, e.g. if the elliptic curve E has non-trivial p-torsion points defined over K, the Galois group of the polynomial Ψ_p^E over K is $\rho_{E,p}(G_K) = \mathrm{Gal}(K(E[p])/K)$.*

2. POLYNOMIALS IN THE SURJECTIVE CASE

The following theorem allows us to find polynomials with coefficients in K whose Galois group over K is $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$ or $\mathrm{GL}_2(\mathbb{F}_p)$.

Theorem 2.1. *Let E be an elliptic curve defined over K. Let $p \neq 2$ be a prime number, assume that the representation $\rho_{E,p} : G_K \to \mathrm{GL}_2(E[p])$ is surjective, then*

(i) The polynomial Ψ_p^E whose roots are the first coordinates of the non-trivial p-torsion points of E is irreducible and its Galois group over K is $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$.

(ii) Let $P = (x, y) \in E[p]\setminus\{0\}$. The characteristic polynomial of the multiplication by $x + y$ in $K(x, y)$ is irreducible and its Galois group over K is $\mathrm{GL}_2(\mathbb{F}_p)$.

Proof. First, we will see that the set of conjugates of x is

$$\{x^\sigma : \sigma \in G_K\} = \{x_i : (x_i, \pm y_i) \in E[p] \setminus \{0\}\},$$

and the set of conjugates of $x + y$ is

$$\{(x + y)^\sigma : \sigma \in G_K\} = \{x_i \pm y_i : (x_i, \pm y_i) \in E[p] \setminus \{0\}\}.$$

Since $(x, y)^\sigma \in E[p]$, for $\sigma \in G_K$, there exists i such that $(x, y)^\sigma = (x_i, \pm y_i)$. So, $x^\sigma = x_i$, $y^\sigma = \pm y_i$, and $(x + y)^\sigma = x_i \pm y_i$. Reciprocally, if $(x_i, \pm y_i) \in E[p]$ is non-trivial, let $R = (x_i, y_i)$. Let $\{P, Q\}$ be a $\mathbb{F}_p$-basis of $E[p]$, with $P = (x, y)$. Let $a, b \in \mathbb{F}_p$ be such that $R = aP + bQ$. Since $a \neq 0$ or $b \neq 0$, there exists $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$. Since $\rho_{E,p}$ is surjective, there exist $\sigma_0, \sigma_1 \in G_K$ with $\rho_{E,p}(\sigma_0) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $\rho_{E,p}(\sigma_1) = \begin{pmatrix} -a & c \\ -b & d \end{pmatrix}$. Then, $x^{\sigma_0} = x_i$, $(x + y)^{\sigma_0} = x_i + y_i$ and $(x + y)^{\sigma_1} = x_i - y_i$.

(i) Clearly $\#\{x^\sigma : \sigma \in G_K\} = \frac{p^2-1}{2} = \deg \Psi_p^E$, then Ψ_p^E is the irreducible polynomial of x over K and its Galois group over K is $\mathrm{Gal}(K(x(E[p]))/K) = \mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$.

(ii) Since

$$K(E[p]) = K(\{x_i \pm y_i\}_{i=1,\ldots,\frac{p^2-1}{2}}) = K(\{(x + y)^\sigma\}_{\sigma \in G_K}),$$

the decomposition field over K of the irreducible polynomial $\mathrm{Irr}(x + y, K)$ of $x + y$ over K is $K(E[p])$ and its Galois group over K is $\rho_{E,p}(G_K) = \mathrm{GL}_2(\mathbb{F}_p)$. On the other hand, since $p \neq 2$ and $-\mathrm{id} \in \mathrm{Gal}(K(E[p])/K(x(E[p])))$, it is easy to see that $x_i \pm y_i \neq x_j \pm y_j$ for all $i \neq j$, and $x_i + y_i \neq x_i - y_i$ for all i. Then, the degree of $\mathrm{Irr}(x + y, K)$ is $p^2 - 1$. Let $m_{x+y} : K(x, y) \to K(x, y)$ be the morphism multiplication by $x + y$ in $K(x, y)$. The dimension of $K(x, y)$ over K is $p^2 - 1$. Therefore, the characteristic polynomial of the morphism m_{x+y} is $\mathrm{Irr}(x + y, K)$ and its Galois group is $\mathrm{GL}_2(\mathbb{F}_p)$.

Example. Let $E : Y^2 = 4X^3 - g_2X - g_3$ be an elliptic curve and $p = 3$. The polynomial Ψ_3^E whose roots are the first coordinates of the non-trivial 3-torsion points of E is

$$\Psi_3^E = 3X^4 - \frac{3}{2} g_2X^2 - 3g_3X - \frac{g_2^2}{16}.$$

Let $P = (x, y)$ be a non-trivial 3-torsion point, we have the relations

$$x^4 = \frac{g_2}{2} x^2 + g_3x + \frac{g_2^2}{48}, \qquad y^2 = 4x^3 - g_2x - g_3.$$

Let us consider $\{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$ as a K-basis of the vectorial space $K(x, y)$. Then, the characteristic polynomial of

$$m_{x+y} : K(x, y) \to K(x, y)$$
$$a \mapsto a \cdot (x + y).$$

is the characteristic polynomial of the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ \frac{g_2^2}{48} & g_3 & \frac{g_2}{2} & 0 & 0 & 0 & 0 & 1 \\ -g_3 & -g_2 & 0 & 4 & 0 & 1 & 0 & 0 \\ \frac{g_2^2}{12} & 3g_3 & g_2 & 0 & 0 & 0 & 1 & 0 \\ 0 & \frac{g_2^2}{12} & 3g_3 & g_2 & 0 & 0 & 0 & 1 \\ \frac{g_2^3}{48} & g_2g_3 & \frac{7g_2^2}{12} & 3g_3 & \frac{g_2^2}{48} & g_3 & \frac{g_2}{2} & 0 \end{pmatrix}.$$

If $\rho_{E,3}$ is surjective, this characteristic polynomial has Galois group $\rho_{E,3}(G_K) = \mathrm{GL}_2(\mathbb{F}_3)$. In particular, if we take the generic elliptic curve

$$E_T : y^2 = 4x^3 - Tx - T,$$

which defines a surjective mod p Galois representation of $G_{\mathbb{Q}(T)}$, for all p (cf. [5], § 63), we obtain the polynomial with coefficients in $\mathbb{Q}(T)$ computed in the table 23b of [3].

3. POLYNOMIALS FOR $\rho_{E,p}(G_{\mathbb{Q}})$, $p = 3, 5$

In this section we will give examples of polynomials whose Galois groups over $\mathbb{Q}$ are the images $\rho_{E,p}(G_{\mathbb{Q}})$. In [2, Theorem 3.2] it is determined the Galois group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ for all the elliptic curves E defined over $\mathbb{Q}$ without complex multiplication with conductor $N \leq 200$ and for all primes p. Now, we will give a polynomial for each subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{GL}_2(\mathbb{F}_5)$ that appears as Galois group.

(a) $p = 3$.

(i) $\rho_{11B,3}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_3)$. We remark that $11B$ is the modular curve $X_0(11)$. The polynomial obtained by using Theorem 2.1, is given in table 23b [3].

(ii) $\rho_{14C,3}(G_{\mathbb{Q}}) = \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.

$$\Psi_3^{14C} = \frac{1}{2304} (4X + 1)(12X - 25)(144X^2 + $$
$$+ 264X + 1849).$$

By Theorem 1.1, the polynomial is the quadratic factor.

(iii) $\rho_{14A,3}(G_{\mathbb{Q}}) = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

$$\Psi_3^{14A} = \frac{1}{2304} (12X - 1)(576X^3 + 48X^2 -$$
$$- 596X + 625).$$

By Theorem 1.1, the polynomial is the factor of degree 3.

(iv) $\rho_{14E,3}(G_{\mathbb{Q}}) = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

$$\Psi_3^{14E} = \frac{1}{2304} (4X + 25)$$
$$(1728X^3 - 10800X^2 - 521820X - 2679769).$$

By Theorem 1.1, the polynomial is the factor of degree 3.

(v) $\rho_{50A,3}(G_{\mathbb{Q}}) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Since $\Psi_3^{50A} = \left(X - \frac{5}{12}\right) \cdot \tilde{\Psi}_3$, with $\tilde{\Psi}_3$ an irreducible polynomial over $\mathbb{Q}$ of degree 3, we can take the basis $\{P, Q\}$ of $E^{50A}[3]$ with $P = \left(\frac{5}{12}, \sqrt{5}\right)$ and $Q = (x, y)$, where x is a root of $\tilde{\Psi}_3$. The matricial expression of the image of the representation tells us that any 3-torsion point different from $\pm P$ is conjugated with Q. Hence,

$$\{(x+y)^\sigma : \sigma \in G_{\mathbb{Q}}\} = \left\{x_i \pm y_i : (x_i, \pm y_i) \in E^{50A}[3],\ x_i \neq \frac{5}{12}\right\}.$$

So, the decomposition field over $\mathbb{Q}$ of $\mathrm{Irr}(x + y, \mathbb{Q})$ is

$$\mathbb{Q}(\{x_i \pm y_i\}_{i=1,2,3}) \subseteq \mathbb{Q}(E^{50A}[3]).$$

But we can check that the polynomial $\mathrm{Irr}(x + y, \mathbb{Q})$ is

$$X^6 + \frac{5}{6}X^5 + \frac{30845}{432}X^4 - \frac{397015}{1296}X^3 + \frac{37960175}{20736}X^2 - \frac{735364625}{373248}X + \frac{47376998675}{8957952},$$

which has the dihedral group $D_6 \simeq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ as Galois group over $\mathbb{Q}$. So, $\mathbb{Q}(\{x_i \pm y_i\}_{i=1,2,3}) = \mathbb{Q}(E^{50A}[3])$, and the above polynomial is the one we are looking for.

(vi) $\rho_{98C,3}(G_{\mathbb{Q}}) = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$, in the $\mathbb{F}_3$-basis of $E^{98C}[3]$

$$P = \left(-\frac{847}{12}, 343\sqrt{-7}\right),\quad Q = \left(\frac{175}{4}, \frac{686}{9}\sqrt{21}\right).$$

We have

$$\mathbb{Q}(E^{98C}[3]) = \mathbb{Q}\left(343\sqrt{-7}, \sqrt{\frac{847}{12}}\right) = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}) = \mathbb{Q}(\sqrt{-3} + \sqrt{-7})$$

So, the polynomial is

$$\mathrm{Irr}(\sqrt{-3} + \sqrt{-7}, \mathbb{Q}) = X^4 + 20X^2 + 16.$$

(b) $p = 5$.

(i) $\rho_{20B,5}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_5)$. We remark that $20B$ is the modular curve $X_0(20)$, and the polynomial is given in table 23b of [3].

(ii) $\rho_{11B,5}(G_{\mathbb{Q}}) = \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.

$$\Psi_5^{11B} = \frac{1}{531441}(3X-14)(3X-47)(45X^2+75X-241)(81X^4 + 189X^3 + 1026X^2 + 3954X + 9391)(81X^4 + 1323X^3 + 10989X^2 + 23097X + 19081).$$

By Theorem 1.1, we can take either of the factors of degree 4.

(iii) $\rho_{11A,5}(G_{\mathbb{Q}}) = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

$$\Psi_5^{11A} = \frac{1}{531441}(3X - 2)(3X + 1)(295245X^{10} + 98415X^9 - 1121931X^8 + 3595428X^7 + 260253X^6 + 54675X^5 + 293544X^4 - 693360X^3 + 912627X^2 - 333516X + 55049).$$

By Theorem 1.1, we can take the factor of degree 10.

(iv) $\rho_{11C,5}(G_{\mathbb{Q}}) = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

$$\Psi_5^{11C} = \frac{1}{531441}(45X^2 + 4575X + 116279)(243X^5 + 21060X^4 - 2063205X^3 - 322004880X^2 - 13790509365X - 198101488289)(243X^5 - 45765X^4 - 15650955X^3 - 1358064135X^2 - 48900953415X - 644288081042).$$

By Theorem 1.1, since the Galois group of either of the irreducible factors of degree 5 is the Frobenius group $F_{20} \subset \mathfrak{S}_5$, of order 20, we can take either of these polynomials.

(v) $\rho_{99D,5}(G_{\mathbb{Q}}) = \begin{pmatrix} \pm 1 & 0 \\ 0 & * \end{pmatrix}$.

$$\Psi_5^{99D} = (X + 14)(X + 47)(5X^2 - 25X - 241)(X^4 - 7X^3 + 114X^2 - 1318X + 9391)(X^4 - 49X^3 + 1221X^2 - 7699X + 19081)$$

Let $\{P, Q\}$ be a $\mathbb{F}_5$-basis of $E^{99D}[5]$ such that the image of the representation has the previous matricial form. We take $P = (-14, 33\sqrt{-3})$ and $Q = (x, y)$, where Q is a 5-torsion point with x a root of one of the factors of Ψ_5^{99D} of degree 4. So, we can choose

$$Q = \left(\frac{5}{2} + \frac{33\sqrt{5}}{10}, \sqrt{3267 - \frac{6534\sqrt{5}}{25}}\right).$$

Then,

$$\mathbb{Q}\left(\sqrt{-3}, \sqrt{3267 - \frac{6534\sqrt{5}}{25}}\right) \subseteq \mathbb{Q}(E[5]).$$

Since $[\mathbb{Q}(E^{99D}[5]) : \mathbb{Q}] = 8$, the irreducible polynomial over $\mathbb{Q}$ with decomposition field $\mathbb{Q}(E^{99D}[5]$ is the polynomial of degree 8

$$X^8 - 13056X^6 + \frac{7914686688}{125}X^4 - \frac{16891361683776}{125}X^2 + \frac{1674227268777390336}{15625}.$$

(vi) $\rho_{99C,5}(G_{\mathbb{Q}}) = \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix}.$

$$\Psi_5^{99C} = (X-1)(X+2)$$
$$(5X^{10} - 5X^9 - 171X^8 - 1644X^7 + 357X^6 - 225X^5 + 3624X^4 + 25680X^3 + 101403X^2 + 111172X + 55049).$$

Let $\{P, Q\}$ be a $\mathbb{F}_5$-basis of $E[5]$ such that the image of the representation has the previous matricial form. We can take $P = (1, 3\sqrt{-3})$, $Q = (x, y)$, where x is any root of the factor of degree 10. The matricial expression of the image of the representation indicates us that any 5-torsion point different from $\pm P$ is conjugated with Q, and so,

$$\{(x+y)^\sigma : \sigma \in G_{\mathbb{Q}}\} = \{x_i \pm y_i : (x_i, \pm y_i) \in E[5] \setminus \langle P \rangle\}.$$

Then,

$$\mathbb{Q}(E^{99C}[5]) = \mathbb{Q}(\{x_i \pm y_i\}_{i=1,\dots,10}, \sqrt{-3}) = \mathbb{Q}(\{x_i, y_i\}_{i=1,\dots,10}, \sqrt{-3}),$$

and consequently, the polynomial of degree 22 we are looking for is $\mathrm{Irr}(x+y, \mathbb{Q})(X^2+3)$.

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

$$\Psi_5^{50G} = \frac{5}{8916100448256}(12X-85)(12X+35)$$
$$(61917364224X^{10} + 257989017600X^9 - 55628881920000X^8 + 1206636134400000X^7 - 3537551232000000X^6 - 58165801920000000X^5 + 1009074753000000000X^4 - 11967618375000000000X^3 + 87165442132031250000X^2 - 313745335166015625000X + 442487707579345703125).$$

By Remark 1.2, the polynomial we are looking for is the factor of degree 10.

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

$$\Psi_5^{50E} = \frac{5}{8916100448256}(144X^2 + 120X - 155)$$
$$(248832X^5 - 1347840X^4 + 432000X^3 - 2541600X^2 - 826500X - 6632125)$$
$$(248832X^5 + 1140480X^4 + 4579200X^3 - 6170400X^2 - 5290500X - 3749125).$$

By Remark 1.2, since the Galois group of either of the irreducible factors of degree 5 is the Frobenius group $F_{20} \subset \mathfrak{G}_5$, of order 20, we can take either of the two above factor polynomials.

REFERENCES

1. Birch, B. & Kuyk, W. (eds.) (1972), *Modular Functions of One Variable IV,* Lecture Notes in Math., Vol. 476, Springer-Verlag.
2. Reverter, A. & Vila, N. (2001), Images of mop p Galois representations associated to elliptic curves, *Canadian Mathematical Bulletin,* **44**.
3. Reverter, A. & Vila, N. (1992), Grups de Galois, In: *Corbes modulars: taules,* Bayer, P.; Travessa, A. (eds.), Notes del Seminari, n. 1, ISBN 84-604-3577-6.
4. Serre, J.-P. (1972), Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones mathematicae,* **15**, 259-331.
5. Weber, H. (1908), *Lehrbuch der Algebra III,* Vieweg, Braunschweig.