Julio FERNÁNDEZ et Joan-C. LARIO

On elliptic Galois representations and genus-zero modular units

On elliptic Galois representations and genus-zero modular units

par Julio FERNÁNDEZ et Joan-C. LARIO

RÉSUMÉ. Etant donnés un nombre premier p impair et une représentation ϱ du groupe de Galois absolu d'un corps de nombres k sur $\mathrm{PGL}_2(\mathbb{F}_p)$ avec déterminant cyclotomique, l'espace des modules des courbes elliptiques définies sur k et dont la p-torsion donne lieu à ϱ est composé de deux tordues galoisiennes de la courbe modulaire $X(p)$. On explicite ici les seuls cas de genre zéro, $p = 3$ et $p = 5$, qui sont aussi les seuls cas *symétriques* : $\mathrm{PGL}_2(\mathbb{F}_p) \simeq \mathcal{S}_n$ pour $n = 4$ ou $n = 5$, respectivement. Dans ce but, on étudie les actions galoisiennes correspondantes aux deux tordues sur le corps de fonctions de la courbe, duquel on donne une description au moyen d'unités modulaires. Comme conséquence, on retrouve une équivalence entre l'*ellipticité* de ϱ et sa *pincipalité*, c'est-à-dire l'existence dans son corps fixe d'un élément α de degré n sur k tel que α and α^2 ont tous les deux trace zéro sur k.

ABSTRACT. Given an odd prime p and a representation ϱ of the absolute Galois group of a number field k onto $\mathrm{PGL}_2(\mathbb{F}_p)$ with cyclotomic determinant, the moduli space of elliptic curves defined over k with p-torsion giving rise to ϱ consists of two twists of the modular curve $X(p)$. We make here explicit the only genus-zero cases $p = 3$ and $p = 5$, which are also the only *symmetric* cases: $\mathrm{PGL}_2(\mathbb{F}_p) \simeq \mathcal{S}_n$ for $n = 4$ or $n = 5$, respectively. This is done by studying the corresponding twisted Galois actions on the function field of the curve, for which a description in terms of modular units is given. As a consequence of this twisting process, we recover an equivalence between the *ellipticity* of ϱ and its *principality*, that is, the existence in its fixed field of an element α of degree n over k such that α and α^2 have both trace zero over k.

1. Introduction

For an odd prime p, the projective group $\mathrm{PGL}_2(\mathbb{F}_p)$ can be realized as Galois group over $\mathbb{Q}$ or, more generally, over a number field k linearly disjoint from the p-th cyclotomic extension of $\mathbb{Q}$. Indeed, the action of the

---

absolute Galois group G_k on the p-torsion points of an elliptic curve E defined over k produces a representation

$$\overline{\rho}_{E,p} : \mathrm{G}_k \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

which is generically surjective and whose determinant is the quadratic character

$$\varepsilon_p : \mathrm{G}_k \longrightarrow \mathrm{Gal}\big(k(\sqrt{\pm p}\,)/k\big) \simeq \mathbb{F}_p^* / \mathbb{F}_p^{*2}$$

obtained as a power of the p-th cyclotomic character of G_k. Furthermore, the conjugacy class of $\overline{\rho}_{E,p}$ is an invariant of the isomorphism class of E unless j_E is 0 or 1728. Except for a finite number of complex multiplication cases depending on p, the fixed field of $\overline{\rho}_{E,p}$ is the Galois extension of k generated by the j-invariants of the elliptic curves defined over the algebraic closure $\overline{k}$ that have an isogeny of degree p to E.

The inverse problem can be stated as follows: given a surjective Galois representation

$$\varrho : \mathrm{G}_k \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

with *cyclotomic* determinant ε_p, find the elliptic curves E defined over k *realizing* ϱ, namely those satisfying $\overline{\rho}_{E,p} = \varrho$. Note that the cyclotomic condition on ϱ forces the number field k to be linearly disjoint from the p-th cyclotomic extension of $\mathbb{Q}$.

This problem was the subject of the PhD thesis of the first author [2]. The second author and A. Rio had already made contributions in [6] and [3] from the Galois theoretic point of view. The present paper pursues a reformulation of the results in [6] and [3] in terms of modular units and twisted modular function fields.

In [6], the problem is addressed for the *octahedral* case, namely for $p = 3$. As shown there, the existence of elliptic curves realizing a representation ϱ is equivalent to the existence of a lifting of ϱ into $\mathrm{GL}_2(\mathbb{F}_3)$. In this case, such curves are then parametrized by the rational points on two conics. As suggested by a remark of J.-P. Serre included in that paper, these conics would turn out to be twists of a modular curve – even though they were not obtained by modular arguments. Here lies one of the motivations for the present article.

In [2], it is proved that the solutions to the problem for a projective mod p Galois representation ϱ with cyclotomic determinant are given by the rational points on two concrete twists $X(p)_\varrho$ and $X(p)'_\varrho$ of a certain model for the modular curve $X(p)$. In order to make explicit the twists, a special care should be taken in fixing such a model. For our purposes, this information is gathered in Section 2, where we also include a discussion on the function fields of the curves $X(p)_\varrho$ and $X(p)'_\varrho$ as well as on the corresponding twisted Galois actions.

The only genus-zero cases occur for $p = 3$ and $p = 5$. In these cases, a characterization for the existence of solutions to the problem is given in [3]. It amounts to the *principality* of ϱ, namely to the existence of a polynomial in $k[X]$ of the form $X^4 + b\,X + c$ (for $p = 3$) or of the form $X^5 + a\,X^2 + b\,X + c$ (for $p = 5$) having the fixed field of ϱ as splitting field over k. This is achieved, following the ideas in [6], by completely algebraic manipulation based on the classical concept of Tschirnhaus transformation and the knowledge of certain 3-torsion and 5-torsion polynomials attached to an elliptic curve.

In the present paper we make explicit the above twisted curves in the genus-zero cases in terms of *modular units*, that is, modular functions whose zeros and poles are all taken at the set of cusps. Thus, Section 3 may be regarded as a modular reformulation of [6]. The characterization of principal octahedral Galois representations with cyclotomic determinant as those which are of the form $\overline{\rho}_{E,3}$ for an elliptic curve E over k is reobtained by applying the moduli recipe in Section 2, so that now the point of view and the methods render very different the proof and hence its exposition. The main ingredient required consists of a suitable description for the function field of the modular curve $X(3)$ that permits an easy way to express the twisted Galois actions. This technique is exploited again in Section 4, where we deal with the non-octahedral genus-zero case, namely with the twists of $X(5)$ attached to a Galois representation onto $\mathrm{PGL}_2(\mathbb{F}_5)$ with cyclotomic determinant. The modular units considered to handle the function field of the curve now come from Siegel functions instead of the Dedekind η-functions used in Section 3.

We finish this introduction by recalling some facts on the group $\mathrm{PGL}_2(\mathbb{F}_p)$ that are assumed through the paper. We collect them in the following list:

- Let us identify $\mathbb{F}_p^*$ with the centre of $\mathrm{GL}_2(\mathbb{F}_p)$. The group $\mathrm{PSL}_2(\mathbb{F}_p)$, defined as the quotient $\mathrm{SL}_2(\mathbb{F}_p)/\langle -1 \rangle$, can be viewed as a subgroup of index two inside the group $\mathrm{PGL}_2(\mathbb{F}_p)$, defined as $\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^*$. Indeed, the determinant map $\mathrm{GL}_2(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^*$ induces an exact sequence

$$1 \longrightarrow \mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^*/\mathbb{F}_p^{*2} \longrightarrow 1.$$

- The order of $\mathrm{PGL}_2(\mathbb{F}_p)$ is $p\,(p-1)(p+1)$.
- A system of generators for $\mathrm{PSL}_2(\mathbb{F}_p)$ is given by the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which have order p and satisfy the relation $T\,U^{p-2}\,T = U^2$.

· The above matrices T and U are commutators inside $\mathrm{PGL}_2(\mathbb{F}_p)$, so $\mathrm{PSL}_2(\mathbb{F}_p)$ is in fact the derived subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ and, in particular, its only subgroup of index two.

· The group $\mathrm{PSL}_2(\mathbb{F}_p)$ is not a direct factor of $\mathrm{PGL}_2(\mathbb{F}_p)$. The possible complementary subgroups for $\mathrm{PSL}_2(\mathbb{F}_p)$ inside $\mathrm{PGL}_2(\mathbb{F}_p)$ are exactly those generated by a conjugate of the matrix

$$V = \begin{pmatrix} 0 & -v \\ 1 & 0 \end{pmatrix},$$

where v is a non-square in $\mathbb{F}_p^*$. One has the relations $V\,T = U^{-v^{-1}}\,V$ and $V\,U = T^{-v}\,V$, so $\mathrm{PGL}_2(\mathbb{F}_p)$ is generated by V and either T or U. Note that the conjugacy class of V depends on the value of p mod 4. Indeed, it includes the p matrices

$$\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}, \quad \text{for} \ \ b \in \mathbb{F}_p,$$

if and only if $p \equiv 3 \pmod 4$.

· The usual action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on the projective line $\mathbb{P}^1(\mathbb{F}_p)$ yields an embedding of this group inside the symmetric group $\mathcal{S}_{p+1}$. In particular, $\mathrm{PGL}_2(\mathbb{F}_3)$ is isomorphic to $\mathcal{S}_4$, since both groups have the same order. For $p = 5$, one actually has $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathcal{S}_5$ (see the proof of Proposition 4.4).

· Both $\mathrm{PSL}_2(\mathbb{F}_p)$ and $\mathrm{PGL}_2(\mathbb{F}_p)$ have trivial centre, so they are isomorphic to their respective inner automorphism groups.

· The action by conjugation of $\mathrm{PGL}_2(\mathbb{F}_p)$ on itself makes this group isomorphic to its automorphism group and also to that of $\mathrm{PSL}_2(\mathbb{F}_p)$.

Most of the assertions in the above list can be obtained with no difficulty. The last one can be read from Theorem 12.5.1 in [1]. We thank the referee for pointing out this reference.

2. Twisting the modular curve $X(p)$

This section deals with the rationality over k for $X(p)$ and its automorphisms. Among the many ways to fix a rational model for this curve, our choice gives, by specialization over the j-line, the fixed field of the projective mod p Galois representation $\overline{\rho}_{E,\,p}$ attached to an elliptic curve E over k. In this section we review both the definition of this model and the construction of its *cyclotomic projective* twists $X(p)_\varrho$ and $X(p)'_\varrho$.

2.1. A rational model for $X(p)$. Consider the modular curve $X(p)$ attached to the congruence subgroup $\Gamma(p)$, which is defined as the kernel of the mod p reduction map $\mathrm{PSL}_2(\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{F}_p)$. This curve is the

Riemann surface obtained by compactifying the quotient of the complex upper-half plane $\mathbb{H}$ by the restriction to $\Gamma(p)$ of the usual action of $\mathrm{PSL}_2(\mathbb{R})$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad z \longmapsto \gamma(z) = \frac{a\,z + b}{c\,z + d} \,.$$

The elements of that quotient are in one-to-one correspondence with the isomorphism classes of elliptic curves over $\mathbb{C}$ together with a p-torsion basis that is sent under the Weil pairing to a fixed root of unity, say ζ_p. The rest of points of $X(p)$, namely the finite set of *cusps* adjuncted to compactify, are identified with the quotient of the projective line $\mathbb{P}^1(\mathbb{Q})$ by the action of $\Gamma(p)$ induced from the one above.

Remark 2.1. The reduction mod p of the numerator and the denominator, taken to be coprime, of every element in $\mathbb{P}^1(\mathbb{Q})$ induces a bijection between the set of cusps of $X(p)$ and the quotient of the set $\mathbb{F}_p \times \mathbb{F}_p \backslash \{(0,0)\}$ by the equivalence relation identifying a pair (m, n) with $(-m, -n)$.

Consider analogously the modular curve $X(1)$ attached to $\mathrm{PSL}_2(\mathbb{Z})$. The natural map $X(p) \longrightarrow X(1)$ carries the above correspondence to the canonical bijection between the non-cuspidal points of $X(1)$ and the isomorphism classes of complex elliptic curves. This bijection is induced by the elliptic modular function $j : \mathbb{H} \longrightarrow \mathbb{C}$.

As a complex curve, $X(p)$ is a Galois cover of $X(1)$ with group $\mathcal{G}(p)$ given by the quotient $\mathrm{PSL}_2(\mathbb{Z})/\Gamma(p)$, so that we have a canonical isomorphism

$$\mathcal{G}(p) \simeq \mathrm{PSL}_2(\mathbb{F}_p)\,.$$

We recall that $\mathcal{G}(p)$ consists of the automorphisms g on $X(p)$ making the following diagram commutative:

$$
\begin{array}{ccc}
X(p) & \xrightarrow{\quad g \quad} & X(p) \\
 & \searrow \quad \swarrow & \\
 & X(1) &
\end{array}
$$
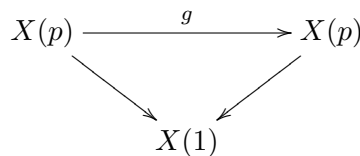
For $p \geq 7$, there are no other automorphisms on $X(p)$ than those in the group $\mathcal{G}(p)$. A proof for this is given in an appendix by Serre in [9].

Remark 2.2. The ramified points of the Galois cover $X(p) \longrightarrow X(1)$ are the cusps and the preimages of the points $j = 1728$ and $j = 0$ on $X(1)$, with ramification degrees p, 2 and 3, respectively. Thus, the Hurwitz formula yields $1 + (p+1)(p-1)(p-6)/24$ for the genus of $X(p)$. It follows that the genus is zero for $p = 3$ and $p = 5$, whereas it is greater than two for $p \geq 7$.

The cover $X(p) \longrightarrow X(1)$ can be defined over the field $k(\sqrt{\pm p}\,)$ inside the p-th cyclotomic extension $k(\zeta_p)$. This is proved in [11] and means that there exist models for both curves making the map $X(p) \longrightarrow X(1)$ and all

the automorphisms in the cover group $\mathcal{G}(p)$ be defined over that quadratic extension of k. We next follow the more general procedure of Section II.3 in [7], Section 2 in [8] or Section 1 in [10] to fix a suitable model for $X(p)$ over k that, in particular, makes the cover be defined over $k(\sqrt{\pm p}\,)$.

The modular function j provides a canonical model for $X(1)$ over k. As for $X(p)$, consider the canonical function field $k(\zeta_p)(X^{\mathrm{c}}(p))$ described in Sections 6.1 and 6.2 of [12]: it is the field of modular functions for $\Gamma(p)$ whose Fourier expansions have coefficients in $k(\zeta_p)$. The Galois action on this extension of $k(j)$ can be seen as an action on the right of the group $\mathrm{GL}_2(\mathbb{F}_p)/\langle -1\rangle$ whose restriction to the subgroup $\mathrm{PSL}_2(\mathbb{F}_p)$ coincides with the natural action induced by the cover group $\mathcal{G}(p)$: an automorphism given by a matrix γ in $\mathrm{PSL}_2(\mathbb{Z})$ sends a modular function f in $k(\zeta_p)(X^{\mathrm{c}}(p))$ to the function $f|\gamma$ defined by $f|\gamma\,(z) = f(\gamma(z))$. Moreover, the subfield fixed by the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)/\langle -1\rangle$ consisting of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \quad \text{for } d \in \mathbb{F}_p^*,$$

is the field of modular functions for $\Gamma(p)$ whose Fourier expansions have coefficients in k. This could be regarded as a *canonical* function field $k(X^{\mathrm{c}}(p))$ for the curve $X(p)$:
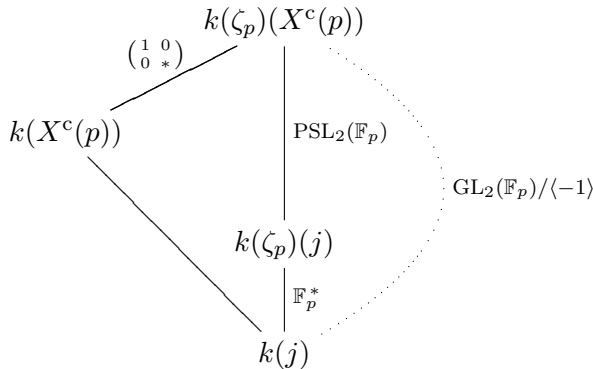
More generally, for every subgroup H of $\mathrm{GL}_2(\mathbb{F}_p)$ with surjective determinant, the subfield of $k(\zeta_p)(X^{\mathrm{c}}(p))$ fixed by $\pm H/\langle -1\rangle$ is a function field over k for the modular curve attached to the inverse image of $H \cap \mathrm{SL}_2(\mathbb{F}_p)$ under the mod p reduction map $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$.

Let us now take H to be a particular subgroup, say H_V, which gives rise by this correspondence to another model $X_V(p)$ over k for the curve $X(p)$:

$$k(\zeta_p)(X^c(p))$$

$H_V/\langle-1\rangle$ $\quad\quad\quad\quad\quad$ $\mathbb{F}_p^*/\langle-1\rangle$

$$k(\sqrt{\pm p}\,)(X_V(p))$$

$$k(X_V(p)) \quad\quad\quad \mathrm{PSL}_2(\mathbb{F}_p) \quad\quad\quad \mathrm{GL}_2(\mathbb{F}_p)/\langle-1\rangle$$

$$\mathrm{PGL}_2(\mathbb{F}_p)$$

$$k(\sqrt{\pm p}\,)(X(1))$$

$$k(X(1))$$
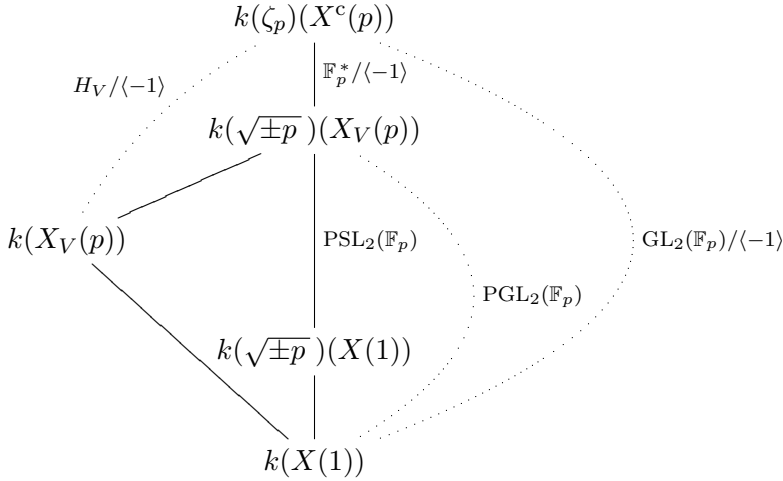
Specifically, we take a matrix V in $\mathrm{GL}_2(\mathbb{F}_p)$ with non-square determinant and with order two in $\mathrm{PGL}_2(\mathbb{F}_p)$. We then define H_V as the inverse image in $\mathrm{GL}_2(\mathbb{F}_p)$ of the subgroup generated by V in $\mathrm{PGL}_2(\mathbb{F}_p)$:

$$H_V = \mathbb{F}_p^* \cup \mathbb{F}_p^* V.$$

Up to conjugation in $\mathrm{GL}_2(\mathbb{F}_p)$, the subgroup H_V is the only one containing the centre $\mathbb{F}_p^*$ and mapping inside $\mathrm{PGL}_2(\mathbb{F}_p)$ onto a complementary subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$. Indeed, all such complementary subgroups are conjugated, as observed in Section 1. In particular, the k-isomorphism class of $X_V(p)$ does not depend on the choice of the matrix V.

Remark 2.3. We could have taken from the start the matrix

$$V = \begin{pmatrix} 0 & -v \\ 1 & 0 \end{pmatrix}$$

for a non-square v in $\mathbb{F}_p^*$, or rather the matrix

$$V = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

if $p \equiv 3 \pmod 4$. In the particular case $p = 3$, the model $X_V(p)$ associated with the latter matrix coincides with the above canonical model $X^c(p)$. This fact is used in Section 3 when giving an explicit description for the function field of $X(3)$.

Remark 2.4. As announced above, the cover $X_V(p) \longrightarrow X(1)$ is defined over $k(\sqrt{\pm p}\,)$, since $k(\sqrt{\pm p}\,)(X_V(p))$ is a Galois extension of $k(X(1))$. Moreover, the Galois group is $\mathrm{PGL}_2(\mathbb{F}_p)$. The extension is actually generated by the roots of the p-th modular polynomial, that is, by the modular

functions defined by

$$J_1(z) = j(pz), \qquad J_n(z) = j\left((z+n-2)/p\right), \quad n = 2, \ldots, p+1,$$

for z in $\mathbb{H}$. Each of these functions generates over $k(j)$ the function field of a modular curve. The first one corresponds to the canonical model over k for the modular curve $X_0(p)$.

The non-cuspidal algebraic points on $X_V(p)$ are in bijection with the isomorphism classes of pairs

$$(E, [P, Q]_V),$$

where E is an elliptic curve over $\overline{k}$, $[P, Q]$ is a basis for the p-torsion $E[p]$, and $[P, Q]_V$ is the corresponding orbit inside $E[p] \times E[p]$ by the action of H_V. Here H_V is viewed as a subgroup of automorphisms of $E[p]$ via the isomorphism $\mathrm{GL}_2(\mathbb{F}_p) \simeq \mathrm{Aut}(E[p])$ fixed by the basis $[P, Q]$. Two such pairs are isomorphic if there is an isomorphism between the corresponding elliptic curves sending one H_V-orbit to the other. The forgetful map $X_V(p) \longrightarrow X(1)$ sends the isomorphism class of $(E, [P, Q]_V)$ to the isomorphism class of E. Furthermore, the bijection is compatible with the Galois actions. Thus, a point on $X_V(p)$ given by a pair as above, with j-invariant different from 0 and 1728, is defined over an algebraic extension L of k if and only if the elliptic curve E is defined over L and the image of the linear representation

$$\rho_{E,p} : \mathrm{G}_L \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

attached to $E[p]$ lies inside a conjugate of the subgroup H_V.

2.2. The twisted curves $X(p)_\varrho$ and $X(p)_\varrho'$. Suppose that we are given a surjective Galois representation

$$\varrho : \mathrm{G}_k \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

with determinant equal to the cyclotomic character ε_p in Section 1. We now revise how to produce the twisted curves whose k-rational points give the elliptic curves over k realizing ϱ. We refer to [3] for a proof of Theorem 2.5.

From now on, we denote simply by $X(p)$ the k-rational model $X_V(p)$ in Subsection 2.1. The matrix V chosen in $\mathrm{PGL}_2(\mathbb{F}_p)$ to fix this model yields an isomorphism $\langle V \rangle \xrightarrow{\det} \mathbb{F}_p^* / \mathbb{F}_p^{*2}$ lifting ε_p to a quadratic character into $\mathrm{PGL}_2(\mathbb{F}_p)$ which we denote by the same letter:

$$\varepsilon_p : \mathrm{G}_k \longrightarrow \mathrm{Gal}\left(k(\sqrt{\pm p}\,)/k\right) \simeq \langle V \rangle.$$

Recall that the automorphism group $\mathcal{G}(p)$ of the cover $X(p) \longrightarrow X(1)$ is canonically isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$. Through the induced isomorphism $\mathrm{PGL}_2(\mathbb{F}_p) \simeq \mathrm{Aut}(\mathcal{G}(p))$, the character ε_p can be seen to give the Galois action on $\mathcal{G}(p)$.

The twisted curves for the moduli problem under consideration are obtained from certain elements in the cohomology set $H^1(\mathrm{G}_k, \mathcal{G}(p))$. Specifically, we take the cocycles $\xi = \varrho\,\varepsilon_p$ and $\xi' = V\,\xi\,V$, where we use the cyclotomic condition on ϱ as well as the identification $\mathrm{PSL}_2(\mathbb{F}_p) \simeq \mathcal{G}(p)$. For the two twists of $X(p)$ attached to ξ and ξ', respectively, we fix k-rational models $X(p)_\varrho$ and $X(p)'_\varrho$ along with isomorphisms

$$\psi : X(p)_\varrho \longrightarrow X(p)$$

$$\psi' : X(p)'_\varrho \longrightarrow X(p)$$

satisfying $\psi = \xi_\sigma\,{}^\sigma\psi$ and $\psi' = \xi'_\sigma\,{}^\sigma\psi'$ for every σ in G_k. Using the expression for the Galois action on $\mathcal{G}(p)$, one can check that these k-rational models are determined by the splitting field of ϱ up to order and k-isomorphism.

Theorem 2.5. *There exists an elliptic curve over k realizing ϱ if and only if the set of non-cuspidal k-rational points on the curves $X(p)_\varrho$ and $X(p)'_\varrho$ is not empty. In this case, the two compositions*

$$X(p)_\varrho \xrightarrow{\ \psi\ } X(p) \xleftarrow{\ \psi'\ } X(p)'_\varrho$$

$$X(1)$$

define a bijection from this set of points to the set of isomorphism classes of elliptic curves over k realizing ϱ.

Corollary 2.6. *For $p \geq 7$, the number of isomorphism classes of elliptic curves over k realizing ϱ is finite.*

Proof. It suffices to take into account Remark 2.2 and Faltings theorem. $\square$

The maps $X(p)_\varrho \longrightarrow X(1)$ and $X(p)'_\varrho \longrightarrow X(1)$ in Theorem 2.5 are easily checked to be defined over k, so we can regard $k(X(1))$ as a subfield of both $k(X(p)_\varrho)$ and $k(X(p)'_\varrho)$. We finish the section with a general description for these two function fields, which is closely related to the corresponding *twisted* Galois actions on the function field of $X(p)$. Both cases $X(p)_\varrho$ and $X(p)'_\varrho$ being analogous, we only treat the first one.

Attached to the cocycle ξ, one has the following twisted action on the set of algebraic points of $X(p)$:

$${}^\sigma_\xi P \;=\; \xi_\sigma({}^\sigma P)$$

for σ in G_k. Consider as well the action of G_k on $\overline{k}(X(p))$ given by

$${}^\sigma_\xi f \;=\; {}^\sigma f\,\xi_\sigma^{-1}.$$

Note that the relation ${}^\sigma_\xi f({}^\sigma_\xi P) = {}^\sigma(f(P))$ holds. We refer to these twisted actions as Galois ξ-*actions* related to ϱ.

Let us denote by K the fixed field of ϱ. The cyclotomic assumption on ϱ amounts to asking K to contain the *cyclotomic* quadratic extension $k(\sqrt{\pm p}\,)$. In particular, the cocycle ξ factors through $\mathrm{Gal}(K/k)$, and one gets the following:

Proposition 2.7. *For any normal extension L of k containing $k(\sqrt{\pm p}\,)$, the ξ-action of G_k can be restricted to $L(X(p))$. Moreover, if L is contained in K, then the ξ-action on $L(X(p))$ factors faithfully through $\mathrm{Gal}(K/k)$.*

Proof. The first part of the statement comes from the normality of L and the fact that the automorphisms in $\mathcal{G}(p)$ are defined over $k(\sqrt{\pm p}\,)$. If L is contained in K, then the ξ-action on $L(X(p))$ factors through $\mathrm{Gal}(K/k)$. Let then σ in $\mathrm{Gal}(K/k)$ act trivially, so that $^{\sigma}f = f\,\xi_{\sigma}$ for all f in $L(X(p))$. In particular, σ is trivial over L, hence $^{\sigma}f = f$ for all f in $L(X(p))$. Thus, the automorphism ξ_{σ} is trivial, and it follows that σ is trivial. $\qquad\square$

Corollary 2.8. *The ξ-action of G_k on the function field of $X(p)$ yields an isomorphism of Galois groups*

$$\iota:\ \mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}\big(\,k(\sqrt{\pm p}\,)(X(p))\,/\,k\,(X(1))\,\big)$$

such that $\iota(\sigma)(f) = {}^{\sigma}_{\xi}f$ for all f in $k(\sqrt{\pm p}\,)(X(p))$ and all σ in $\mathrm{Gal}(K/k)$.

Proof. As noticed in Remark 2.4, $k(\sqrt{\pm p}\,)(X(p))$ has Galois group $\mathrm{PGL}_2(\mathbb{F}_p)$ over $k(X(1))$. Thus, by Proposition 2.7 applied to $L = k(\sqrt{\pm p}\,)$, all one has to check is that the modular function j is fixed by the ξ-action of G_k, which follows straightaway from the definitions. $\qquad\square$

The function field of $X(p)_{\varrho}$ over k is identified through the isomorphism ψ in Theorem 2.5 with the subfield of functions in $\overline{k}\,(X(p))$ which are fixed by the ξ-action of G_k. Since any such a function must be defined over K, this field can actually be seen as the subfield $K(X(p))^{\xi}$ of $K(X(p))$ fixed by the ξ-action of $\mathrm{Gal}(K/k)$. It contains the modular function j.

From Corollary 2.8, it follows the existence of a Galois stable subset $\{\beta_1,\ldots,\beta_{p+1}\}$ of K that is compatible with the set of functions $\{J_1,\ldots,J_{p+1}\}$ in Remark 2.4 with respect to the ξ-action of $\mathrm{Gal}(K/k)$, in the sense that every Galois automorphism induces the same permutation in both sets. Note, in particular, that $\beta_1,\ldots,\beta_{p+1}$ are the roots of a polynomial in $k[X]$ with splitting field K. Then, the functions $H_1,\ldots,H_{p+1}$ in $K(X(p))$ defined by the linear system

$$\begin{pmatrix} J_1 \\ J_2 \\ \vdots \\ J_{p+1} \end{pmatrix} = \begin{pmatrix} \beta_1^p & \beta_1^{p-1} & \cdots & \beta_1 & 1 \\ \beta_2^p & \beta_2^{p-1} & \cdots & \beta_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{p+1}^p & \beta_{p+1}^{p-1} & \cdots & \beta_{p+1} & 1 \end{pmatrix} \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_{p+1} \end{pmatrix}$$

are invariant by the ξ-action of $\mathrm{Gal}(K/k)$. Thus, since

$$K(X(p)) = K(j, J_1, \ldots, J_{p+1}) = K(j, H_1, \ldots, H_{p+1}),$$

we obtain the following expression for the function field of $X(p)_\varrho$ over k:

$$K(X(p))^\xi = k(j, H_1, \ldots, H_{p+1}).$$

3. The octahedral genus-zero case

In this section we make explicit the twisted curves $X(3)_\varrho$, $X(3)'_\varrho$ parametrizing the elliptic curves that realize a given Galois representation ϱ of G_k onto $\mathrm{PGL}_2(\mathbb{F}_3)$ with cyclotomic determinant. In order to do that, we first need to describe the function field of the modular curve $X(3)$, which is carried out in Subsection 3.1. In Subsection 3.2 we then detail the twisted actions of G_k on this function field. As an application, we provide for both $X(3)_\varrho$ and $X(3)'_\varrho$ a k-rational model given by a certain conic $\mathfrak{X}(3)_f$ attached to an arbitrary quartic polynomial f in $k[X]$ with the fixed field of ϱ as splitting field over k.

3.1. The function field of the modular curve $X(3)$. As noticed in Remark 2.2, the genus of $X(3)$ is zero. Let us produce a *Hauptmodul F* for $X(3)$ over k, that is, an explicit isomorphism $X(3) \longrightarrow \mathbb{P}^1$ defined over k. Note that such a function is determined by the values that it takes at the cusps, namely at the points corresponding to $0, 1, 2, \infty$ in $\mathbb{P}^1(\mathbb{Q})$. As we show below, one can make these values to be essentially cubic roots of unity.

Our main tool to this end is the *Newman group* $\mathbb{G}_N$ of functions on $X_0(N)$. Here N stands for a positive integer, and $X_0(N)$ for the complex modular curve attached to the congruence subgroup $\Gamma_0(N)$. Consider the Dedekind function defined by

$$\eta(z) = e^{\pi i z/12} \prod_{l \in \mathbb{N}} (1 - e^{2\pi i l z})$$

for z in the complex upper-half plane $\mathbb{H}$. It is nowhere vanishing and holomorphic. The group $\mathbb{G}_N$ consists of the functions on $\mathbb{H}$ of the form

$$\prod_{0 < n \,|\, N} \eta(nz)^{r_n}$$

for any integers r_n satisfying certain compatibility conditions with the vanishing orders of the modular forms $\Delta(nz) = \eta(nz)^{24}$ at the cusps of $X_0(N)$. The functions in $\mathbb{G}_N$ are modular units for $X_0(N)$, that is, functions on this modular curve whose divisor, which is explicitly computable from the integers r_n, has support in the set of cusps. Moreover, these functions have Fourier expansions with integer coefficients. We refer to [4] for the details.

Proposition 3.1. *There exists a generator F for the function field of $X(3)$ over k with a simple pole at the cusp ∞ and taking the following values at the other cusps:*

$$F(0) = 3, \qquad F(1) = 3\,\zeta^2, \qquad F(2) = 3\,\zeta,$$

where $\zeta = e^{2\pi i/3}$. The expression for the modular function j in terms of F is

$$j = \frac{F^3(F^3 + 6^3)^3}{(F^3 - 3^3)^3}.$$

In particular, F takes the values $0, -6, -6\,\zeta, -6\,\zeta^2$ at the four points on $X(3)$ lying above the elliptic point $j = 0$ on $X(1)$.

Proof. The automorphism $z \mapsto z/3$ of $\mathbb{H}$ induces an isomorphism from $X(3)$ to $X_0(9)$ that sends, in particular, the cusps $0, \infty$ of $X(3)$ to the same cusps of $X_0(9)$. The modular function given by $G(z) = (\eta(z)/\eta(9z))^3$ belongs to the Newman group $\mathbb{G}_9$ and has divisor $(0) - (\infty)$. Hence,

$$F_0(z) = G(z/3) = \frac{\eta(z/3)^3}{\eta(3z)^3}$$

is a modular function for $\Gamma(3)$ with divisor $(0) - (\infty)$. Moreover, the Fourier expansion of F_0 has integer coefficients. For the *normalized* Hauptmodul defined by $F = F_0 + 3$, such a Fourier expansion begins as follows:

$$\frac{1}{q_3} + 5\,q_3^2 - 7\,q_3^5 + 3\,q_3^8 + 15\,q_3^{11} - 32\,q_3^{14} + 9\,q_3^{17} + 58\,q_3^{20} - 96\,q_3^{23} + \cdots$$

Here q_3 stands for the local parameter $e^{2\pi i z/3}$ at infinity. Note that $F(0) = 3$. To compute the values taken by F at the remaining cusps, consider the functions defined by

$$F_1(z) = F(z + 2), \qquad F_2(z) = F(z + 1),$$

whose divisors are $(1) - (\infty)$ and $(2) - (\infty)$, respectively. Using the development of the function η in terms of $e^{\pi i z/12}$, one obtains $F_1 = \zeta\,F - 3$ and $F_2 = \zeta^2 F - 3$, which implies $F(1) = 3\,\zeta^2$ and $F(2) = 3\,\zeta$, as required. The denominator of the expression given in the statement for the modular function j comes from the values taken by F at the cusps of $X(3)$, along with the fact that these points have ramification degree 3 over $X(1)$. The numerator can then be obtained using the Fourier expansions of F and j. $\qquad \square$

3.2. Rational points on the twisted curves $X(3)_\varrho$ and $X(3)'_\varrho$.

Consider a surjective representation

$$\varrho : \mathrm{G}_k \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3).$$

Its fixed field K determines ϱ up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_3)$. Let

$$f(X) = X^4 + a\,X^2 + b\,X + c$$

be a polynomial in $k[X]$ with splitting field K over k. Identify $\mathrm{Gal}(K/k)$ with the symmetric group $\mathcal{S}_4$ by ordering the roots $\beta_1, \beta_2, \beta_3, \beta_4$ of f. Consider then the generators σ, τ of $\mathrm{Gal}(K/k)$ corresponding respectively to the permutations $(1,\,2,\,3,\,4), (1,\,2)$. Also, take any two preimages of σ, τ in G_k and denote them in the same way. They satisfy the relation $\tau\sigma^3 = (\sigma\tau)^2$. On the other hand, the group $\mathrm{PGL}_2(\mathbb{F}_3)$ is generated by the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

which satisfy $TUT = VUV = U^2$ and $UTU = VTV = T^2$. So we can fix the isomorphism $\mathcal{S}_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ as follows, replacing if necessary ϱ by a conjugate representation:

$$\varrho(\sigma) = T^2\,U\,V, \qquad\qquad \varrho(\tau) = V.$$

Assume that the representation ϱ has cyclotomic determinant, namely that the quadratic extension of k inside K is generated by the cubic root of unity ζ, which amounts to saying that the discriminant of the polynomial f is -3 in k^*/k^{*2}. In this case, both automorphisms σ and τ send ζ to ζ^2.

Consider the cocycle $\xi\colon \mathrm{G}_k \longrightarrow \mathrm{Aut}\,(X(3))$ defined by ϱ as in Subsection 2.2. We want to describe explicitly the function field over k for the corresponding twisted curve $X(3)_\varrho$, that is, the subfield $K(X(3))^\xi$ of $K(X(3))$ consisting of those functions fixed by the ξ-action of G_k. The analogous case $X(3)'_\varrho$ attached to the cocycle ξ' is addressed later on.

The curve $X(3)_\varrho$ may not have k-rational points, so we cannot aim to find a Hauptmodul for it in the general case. Instead, one could look for two generators $\mathcal{X}, \mathcal{Y}$ of $K(X(3))^\xi$ of degree two as rational functions in the Hauptmodul F of Proposition 3.1. If they can be chosen with the same denominator, they will satisfy a quadratic polynomial equation over k.

Let us first study the twisted Galois action on the function field of $X(3)$. We refer to Subsection 2.2 for the general definition of this action.

Proposition 3.2. *With the above notations, the ξ-action of G_k on $K(F)$ is determined by the following identities:*

$$_\xi^\sigma F = 3\,\zeta\,\frac{F+6}{F-3}, \qquad\qquad _\xi^\tau F = F.$$

Proof. In view of the identifications $\varrho(\sigma) = T^2\,U\,V$, $\varrho(\tau) = V$ made above, the cocycle ξ is determined by the following rules: $\xi_\tau = 1$ and ξ_σ is the automorphism in the group of the cover $X(3) \longrightarrow X(1)$ corresponding to the matrix $T^2\,U$ in $\mathrm{PSL}_2(\mathbb{F}_3)$. Thus, since F is defined over k, we have $_\xi^\tau F = F$ and $_\xi^\sigma F = F\,|\gamma$ for any preimage γ in $\mathrm{PSL}_2(\mathbb{Z})$ of the matrix $U^2\,T$,

say $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 3 \end{smallmatrix}\right)$. We recall that $F\,|\gamma$ is the function on $X(3)$ defined by $F(\gamma(z))$ for z in $\mathbb{H}$. Consider the modular functions F_0, F_1, F_2 in the proof of Proposition 3.1. The function $F_0|\gamma$ has divisor $(\gamma^{-1}(0)) - (\gamma^{-1}(\infty))$, which can be checked to be $(2) - (0)$. This implies $F_0|\gamma = \omega\, F_2/F_0$ for some ω in $k(\zeta)$. By taking the values of $F_0|\gamma$, F_0 and F_2 at the cusp 1, we obtain $\omega = 3\,\zeta\,(\zeta - 1)$. Hence $F\,|\gamma = F_0|\gamma + 3 = 3\,\zeta\,(F + 6)/(F - 3)$, as claimed. $\qquad\square$

Corollary 3.3. *The ξ-action of σ on the four cusps of $X(3)$ is given by the permutation $(\infty,\,0,\,2,\,1)$. In other words, it is given through the isomorphism $F\colon X(3) \longrightarrow \mathbb{P}^1$ by the permutation $(\infty,\,3,\,3\,\zeta,\,3\,\zeta^2)$. Analogously, the ξ-action of σ on the four points of $X(3)$ lying above the elliptic point $j = 0$ is given through F by the permutation $(0,\,-6,\,-6\,\zeta,\,-6\,\zeta^2)$. In particular, the pullbacks by F of the divisors*

$$(\infty) + (0), \qquad (3) + (-6), \qquad (3\,\zeta) + (-6\,\zeta), \qquad (3\,\zeta^2) + (-6\,\zeta^2)$$

on $\mathbb{P}^1$ are cyclicly permuted by the ξ-action of σ.

Proof. For any point P on $X(3)$, the first identity in Proposition 3.2 applied to the relation $^\sigma_\xi F(^\sigma_\xi P) = {}^\sigma(F(P))$ yields the formula

$$F(^\sigma_\xi P) \,=\, 3\,\frac{^\sigma(F(P)) + 6\,\zeta}{^\sigma(F(P)) - 3\,\zeta}\,.$$

If we now take $F(P) = 3\,\zeta$, for instance, then we obtain $F(^\sigma_\xi P) = 3\,\zeta^2$, as desired. The other cases can be similarly checked. $\qquad\square$

The basic idea to compute $K(X(3))^\xi$ comes from the description of the function field of the twisted curve $X(p)_\varrho$ at the end of the previous section. Recall that $\beta_1, \beta_2, \beta_3, \beta_4$ stand for the roots of the above polynomial f, where the order of the roots has been fixed so that σ and τ induce permutations given by $(1, 2, 3, 4)$ and $(1, 2)$, respectively.

Consider the functions on $X(3)$ with zeros given by the divisors in Corollary 3.3 and with an only pole at the cusp ∞. Note that these functions, which are uniquely determined up to multiplication by non-zero constants, can be written as polynomials of degree at most two in F. Since $F(^\sigma_\xi \infty) = 3$, the ξ-action of σ followed by multiplication by $(F - 3)^2$ must permute these four functions. More precisely, if we take

$$\begin{aligned}
\mathcal{J}_3 &= -9\,F, \\
\mathcal{J}_4 &= (F - 3)(F + 6), \\
\mathcal{J}_1 &= \zeta^2\,(F - 3\,\zeta)(F + 6\,\zeta), \\
\mathcal{J}_2 &= \zeta\,(F - 3\,\zeta^2)(F + 6\,\zeta^2),
\end{aligned}$$

then we have the relations

$$\frac{^\sigma_\xi \mathcal{J}_1}{\mathcal{J}_2} \;=\; \frac{^\sigma_\xi \mathcal{J}_2}{\mathcal{J}_3} \;=\; \frac{^\sigma_\xi \mathcal{J}_3}{\mathcal{J}_4} \;=\; \frac{^\sigma_\xi \mathcal{J}_4}{\mathcal{J}_1} \;=\; \frac{-27\,\zeta}{(F - 3)^2}\,,$$

while the ξ-action of τ permutes $\mathcal{J}_1, \mathcal{J}_2$ and fixes $\mathcal{J}_3, \mathcal{J}_4$.

Consider now the functions $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4$ defined by the linear system

$$\begin{pmatrix} \mathcal{J}_1 \\ \mathcal{J}_2 \\ \mathcal{J}_3 \\ \mathcal{J}_4 \end{pmatrix} = \begin{pmatrix} \beta_1^3 & \beta_1^2 & \beta_1 & 1 \\ \beta_2^3 & \beta_2^2 & \beta_2 & 1 \\ \beta_3^3 & \beta_3^2 & \beta_3 & 1 \\ \beta_4^3 & \beta_4^2 & \beta_4 & 1 \end{pmatrix} \begin{pmatrix} \mathcal{H}_1 \\ \mathcal{H}_2 \\ \mathcal{H}_3 \\ \mathcal{H}_4 \end{pmatrix}.$$

These four functions are elements in $K[F]$ of degree at most two. Moreover, the quotient of any two of them is invariant by the ξ-action of G_k. Take

$$\mathcal{X} = \frac{\mathcal{H}_1}{\mathcal{H}_3}, \qquad \mathcal{Y} = \frac{\mathcal{H}_2}{\mathcal{H}_3}.$$

Then, the functions $\mathcal{X}, \mathcal{Y}$ satisfy the conic $\mathfrak{X}(3)_f$ given by the quadratic polynomial

$$(8\,a^3 - 3\,b^2 - 24\,a\,c)\,x^2 - 28\,a\,b\,x\,y - 4\,(a^2 - 4\,c)\,y^2 - 16\,(a^2 - 2\,c)\,x + 24\,b\,y + 8\,a$$

in $k[x, y]$. This can be proved eliminating, by means of a resultant, the Hauptmodul F in the expressions of $\mathcal{X}, \mathcal{Y}$ as elements of $K(F)$. Alternatively, it comes from the relations

$$(1) \qquad \begin{cases} \mathcal{J}_1 + \mathcal{J}_2 + \mathcal{J}_3 + \mathcal{J}_4 = 0, \\ \mathcal{J}_1^2 + \mathcal{J}_2^2 + \mathcal{J}_3^2 + \mathcal{J}_4^2 = 0, \end{cases}$$

the first of which actually amounts to the relation $4\,\mathcal{H}_4 = 3\,b\,\mathcal{H}_1 + 2\,a\,\mathcal{H}_2$. The non-degeneracy of $\mathfrak{X}(3)_f$ implies the equality $K(F) = K(\mathcal{X}, \mathcal{Y})$. Thus, the functions $\mathcal{X}, \mathcal{Y}$ satisfy

$$K(X(3))^\xi = k(\mathcal{X}, \mathcal{Y}),$$

hence yield the conic $\mathfrak{X}(3)_f$ as a k-rational model for the curve $X(3)_\varrho$.

To deal with the twist $X(3)'_\varrho$ let us consider in G_k the automorphism $\sigma' = \tau\,\sigma\,\tau$, whose restriction to $\mathrm{Gal}(K/k)$ corresponds to the root permutation $(1, 3, 4, 2)$ and generates along with τ this Galois group. If we replace ξ by ξ' and σ by σ' in Proposition 3.2, the proof remains valid. So one should now modify the above linear system as follows:

$$\begin{pmatrix} \mathcal{J}_2 \\ \mathcal{J}_1 \\ \mathcal{J}_3 \\ \mathcal{J}_4 \end{pmatrix} = \begin{pmatrix} \beta_1^3 & \beta_1^2 & \beta_1 & 1 \\ \beta_2^3 & \beta_2^2 & \beta_2 & 1 \\ \beta_3^3 & \beta_3^2 & \beta_3 & 1 \\ \beta_4^3 & \beta_4^2 & \beta_4 & 1 \end{pmatrix} \begin{pmatrix} \mathcal{H}_1' \\ \mathcal{H}_2' \\ \mathcal{H}_3' \\ \mathcal{H}_4' \end{pmatrix}.$$

Then, the functions $\mathcal{X}' = \mathcal{H}_1'/\mathcal{H}_3'$ and $\mathcal{Y}' = \mathcal{H}_2'/\mathcal{H}_3'$ are generators for $K(X(3))^{\xi'}$ over k and also satisfy the equation of the conic $\mathfrak{X}(3)_f$.

Remark 3.4. From the definitions, one can check that the cocycles ξ and ξ' yield different classes inside the first cohomology set of G_k with values in the group of the cover $X(3) \longrightarrow X(1)$. Since we have found k-rational models for the curves $X(3)_\varrho$ and $X(3)'_\varrho$ given by the same conic, ξ and ξ' are actually cohomologous when regarded as cocycles of G_k with values in $\mathrm{Aut}(X(3))$.

Recall that the function j belongs to both $K(X(3))^\xi$ and $K(X(3))^{\xi'}$. In order to get an expression for j as an element in each of these function fields, consider the polynomial $f_\mathcal{J}$ with coefficients in $k[F]$ given by

$$f_\mathcal{J}(X) = (X - \mathcal{J}_1)(X - \mathcal{J}_2)(X - \mathcal{J}_3)(X - \mathcal{J}_4)$$

and define $d_\mathcal{J}$ in $k[F]$ by the relation

$$\prod_{h<l}(\mathcal{J}_h - \mathcal{J}_l) = (1 + 2\zeta)\, d_\mathcal{J}\,.$$

Note that the discriminant of $f_\mathcal{J}$ is $-3\, d_\mathcal{J}^2$. The above relations (1) amount to saying that the polynomial $f_\mathcal{J}$ is of the form

$$f_\mathcal{J}(X) = X^4 + b_\mathcal{J}X + c_\mathcal{J}\,.$$

Moreover, the identities

$$\frac{3\, b_\mathcal{J}^2}{\pm d_\mathcal{J}} = \pm\frac{j - 1728}{j + 1728} = \pm\frac{1728/j - 1}{1728/j + 1}$$

hold in $k(F)$, where $b_\mathcal{J}$ and $d_\mathcal{J}$ can also be written from the above linear systems as homogeneous polynomials of degrees 3 and 6, respectively, in $k[\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3]$ as well as in $k[\mathcal{H}'_1, \mathcal{H}'_2, \mathcal{H}'_3]$. This gives explicitly the function j both inside $k(\mathcal{X}, \mathcal{Y})$ and inside $k(\mathcal{X}', \mathcal{Y}')$. Note that the expression of $-b_\mathcal{J}^2/d_\mathcal{J}$ in terms of $\mathcal{X}', \mathcal{Y}'$ is the same as that of $b_\mathcal{J}^2/d_\mathcal{J}$ in terms of $\mathcal{X}, \mathcal{Y}$.

The interpretation given in Theorem 2.5 for the k-rational points on $X(3)_\varrho$ and $X(3)'_\varrho$ can now be used to reobtain Theorem 3.1 in [3]. See also Theorem 3 in [6].

Theorem 3.5. *A representation of G_k onto $\mathrm{PGL}_2(\mathbb{F}_3)$ with cyclotomic determinant is principal if and only if it is realized by an elliptic curve defined over k, hence by infinitely many isomorphism classes of them.*

Proof. For $a = 0$, the above conic $\mathfrak{X}(3)_f$ has clearly k-rational points. The other implication follows from the above discussion. $\square$

Remark 3.6. The existence of k-rational points on the conic $\mathfrak{X}(3)_f$ does not depend on the quartic polynomial f chosen from the start. Whenever they exist, these points are in bijection with the polynomials

$$f_*(X) = X^4 + b_* X + c_*$$

in $k[X]$ having the same splitting field as f over k, up to transformations of the form $X^4 + \delta^3\, b_*\, X + \delta^4 c_*$ for δ in k^*. Specifically, to a point on $\mathfrak{X}(3)_f$ with projective coordinates $[x\colon y\colon z]$ corresponds the minimal polynomial over k of the element

$$x\,\beta_i^3 + y\,\beta_i^2 + z\,\beta_i + (3\,b\,x + 2\,a\,y)/4\,.$$

Thus, this set of polynomials parametrizes simultaneously the k-rational points on $X(3)_\varrho$ and those on $X(3)_\varrho'$. All these points are non-cuspidal. Indeed, given a polynomial f_* as above, write its discriminant as $-3\,d_*^2$ for some d_* in k, and let j_* be the element in k satistying

$$\frac{3\,b_*^2}{d_*} = \frac{j_* - 1728}{j_* + 1728}\,.$$

Both b_* and c_* must be non-zero, since the Galois group of an irreducible polynomial in $k[X]$ of the form $X^4 + c$ lies inside a dihedral group of order 8. This implies $d_* \neq \pm 3\,b_*^2$, hence $j_* \neq 0, 1728$. Then, j_* and $1728^2/j_*$ are the j-invariants of two elliptic curves over k realizing ϱ, one of them corresponding to a k-rational point on $X(3)_\varrho$ and the other one to a k-rational point on $X(3)_\varrho'$. Moreover, the j-invariant of any such elliptic curve is obtained in this way from some polynomial f_* as above.

4. The non-octahedral genus-zero case

We now deal with the genus-zero case left, namely the one corresponding to the modular curve $X(5)$. For a representation ϱ of G_k onto $\mathrm{PGL}_2(\mathbb{F}_5)$ with cyclotomic determinant, we make explicit the twists $X(5)_\varrho$, $X(5)_\varrho'$ parametrizing the elliptic curves over k that realize ϱ.

4.1. The function field of the modular curve $X(5)$. Following the notation in Remark 2.3, let us fix the k-rational model for $X(5)$ attached the matrix $V = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$ in $\mathrm{PGL}_2(\mathbb{F}_5)$. Unlike the octahedral case, this model is not k-isomorphic to the *canonical* model $X^{\mathrm{c}}(5)$ given by the field of modular functions for $\Gamma(5)$ whose Fourier expansions have coefficients in k. Nevertheless, both curves become isomorphic over the fifth cyclotomic extension of k, and one can try to determine the function field of the first one from an explicit knowledge of those modular functions.

According to Remark 2.1, the twelve cusps of $X(5)$ are given by the points

0 1 2 3 4 1/2 3/2 5/2 7/2 9/2 2/5 ∞

in $\mathbb{P}^1(\mathbb{Q})$ and are respectively represented by the following pairs in $\mathbb{F}_5 \times \mathbb{F}_5$:

(0,1) (1,1) (2,1) (2,4) (1,4) (1,2) (2,3) (0,2) (2,2) (1,3) (2,0) (1,0).

Denote by $\mathcal{P}$ the set consisting of these twelve pairs. This set appears in the proof of the next proposition, where we fix a Hauptmodul F for $X^{\mathrm{c}}(5)$

over k by means of the construction of modular units for $X(p)$ from Siegel functions. We refer to [5] for the details concerning this construction.

Proposition 4.1. *There exists a generator F for the function field of $X^c(5)$ over k with a simple zero at $2/5$ and a simple pole at ∞, and taking the following values at the other cusps*:

$$
\begin{aligned}
F(0) &= 1 + \zeta + \zeta^4, & F(1/2) &= 1 + \zeta^2 + \zeta^4, \\
F(1) &= 1 + \zeta^3 + \zeta^4, & F(3/2) &= \zeta + \zeta^3 + \zeta^4, \\
F(2) &= \zeta^2 + \zeta^3 + \zeta^4, & F(5/2) &= 1 + \zeta^2 + \zeta^3, \\
F(3) &= \zeta + \zeta^2 + \zeta^3, & F(7/2) &= \zeta + \zeta^2 + \zeta^4, \\
F(4) &= 1 + \zeta + \zeta^2, & F(9/2) &= 1 + \zeta + \zeta^3,
\end{aligned}
$$

where $\zeta = e^{2\pi i/5}$. The expression for the modular function j in terms of F is

$$
j = \frac{(F^{20} + 228\, F^{15} + 494\, F^{10} - 228\, F^5 + 1)^3}{F^5(F^{10} - 11\, F^5 - 1)^5}\,.
$$

Proof. For every pair (m, n) in the above set $\mathcal{P}$, consider the Siegel function $S_{(m,n)}$ defined by

$$
S_{(m,n)}(z) = q_5^{5/2\, B_2(m/5)}\, (1 - \zeta^n q_5^m) \prod_{l \geq 1} (1 - \zeta^n q_5^{5\,l+m})(1 - \zeta^{-n} q_5^{5\,l-m})
$$

for z in the complex upper-half plane. Here q_5 stands for the local parameter $e^{2\pi i z/5}$ at infinity, and $B_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial. The function $S_{(m,n)}$ is nowhere vanishing and holomorphic, and $S_{(m,n)}^{60}$ turns out to be a modular function for $\Gamma(5)$, so that it can be seen as a modular unit for $X(5)$. Furthermore, its divisor can be explicitly computed: the order of $S_{(m,n)}^{60}$ at a cusp represented by a pair (m', n') in $\mathcal{P}$ is $150\, B_2\left((m\, m' + n\, n')/5\right)$, where one regards the sum $m\, m' + n\, n'$ reduced mod 5. As a matter of fact, every modular unit for $X(5)$ can be explicitly written, up to the product by a non-zero constant function, as an element in the multiplicative group generated by the Siegel functions $S_{(m,n)}$. We use this result to produce, for every cusp P different from ∞, a function F_P on $X(5)$ with a simple zero at P and a simple pole at ∞ with residue one. For the cusp $2/5$, we obtain a *normalized* Hauptmodul

$$
F = F_{2/5} = (2 + \zeta + 2\,\zeta^2)/5\ S_{(0,1)}\, S_{(2,1)}^2\, S_{(2,4)}^2\, S_{(2,3)}^2\, S_{(0,2)}\, S_{(2,2)}^2\, S_{(2,0)}^2
$$

with k-rational Fourier expansion, which begins as follows:

$$
\frac{1}{q_5} + q_5^4 - q_5^{14} + q_5^{24} + q_5^{29} - q_5^{34} - 2\, q_5^{39} + 2\, q_5^{49} + 2\, q_5^{54} - q_5^{59} - 3\, q_5^{64} - q_5^{69} + \cdots
$$

In particular, F generates the function field of $X^c(5)$ over k. The values that F takes at the remaining cusps are computed using the Fourier expansions in terms of q_5 for the above functions F_P. One finds, for instance,

$F_0 = F + \zeta^2 + \zeta^3$ and $F_{5/2} = F + \zeta + \zeta^4$. As for the expression for the modular function j given in the statement, the denominator is obtained from the values that F takes at the cusps, all of which have ramification degree 5 over $X(1)$. The numerator can then be computed using the Fourier expansions of j and F. □

In view of this proposition, the function field of $X^c(5)$ over $k(\zeta)$ is $k(\zeta, F)$, which has Galois group $\mathrm{GL}_2(\mathbb{F}_5)/\langle -1 \rangle$ over $k(j)$. Recall that the natural action of this matrix group on $k(\zeta, F)$ is on the right. Now, the function field of $X(5)$ over k is the subfield fixed by $H_V/\langle -1 \rangle$, where V is the matrix in $\mathrm{PGL}_2(\mathbb{F}_5)$ at the beginning of the subsection and H_V is the preimage of $\langle V \rangle$ in $\mathrm{GL}_2(\mathbb{F}_5)$. The quotient $H_V/\langle -1 \rangle$ is generated by the matrix $2V$ regarded in $\mathrm{GL}_2(\mathbb{F}_5)$, where it can be written as follows:

$$2V = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}.$$

The first matrix in this product acts trivially on $k(F)$ and sends ζ to ζ^3, while the second matrix acts trivially on $k(\zeta, j)$ and sends F to the function $F \,|\, \gamma$ given by the matrix $\gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$. The divisor of $F \,|\, \gamma$ is $(5/2) - (0)$. From Proposition 4.1, one then obtains the equality

$$F \,|\, \gamma = \omega \, \frac{F + \zeta + \zeta^4}{F + \zeta^2 + \zeta^3}$$

for some ω in $k(\zeta)$. Taking the values of F and $F \,|\, \gamma$ at the cusp $2/5$, we get $\omega = 1 + \zeta + \zeta^4$. We have thus proved this statement:

Proposition 4.2. *The curve $X(5)$ is the twist of $X^c(5)$ over k attached to the cocycle $\eta : \mathrm{G}_k \longrightarrow \mathrm{Gal}(k(\zeta)/k) \longrightarrow \mathrm{Aut}(X^c(5))$ given by*

$$\underset{\eta}{^\nu}F = F \, \eta_\nu^{-1} = (1 + \zeta + \zeta^4) \, \frac{F + \zeta + \zeta^4}{F + \zeta^2 + \zeta^3} \,,$$

where F is the Hauptmodul for $X^c(5)$ in Proposition 4.1 and ν is the generator of $\mathrm{Gal}(k(\zeta)/k)$ sending ζ to ζ^3.

Corollary 4.3. *With the notation in Proposition 4.2, the η-action of the Galois automorphism ν on the cusps of $X^c(5)$ is given by the permutations*

$$(\infty, 0, 2/5, 5/2), \qquad (1, 3, 7/2, 1/2), \qquad (4, 2, 3/2, 9/2).$$

Let us now consider the factorization in $k[F]$ of the polynomials appearing in the expression given in Proposition 4.1 for the elliptic modular function j. Obviously, each of the three sets of points of $X^c(5)$ with $j = 0$

corresponding through the isomorphism $F \colon X^{\mathrm{c}}(5) \longrightarrow \mathbb{P}^1$ to the roots of

$$F^4 + 3\,F^3 - F^2 - 3\,F + 1,$$

$$F^8 + F^7 + 7\,F^6 - 7\,F^5 + 7\,F^3 + 7\,F^2 - F + 1,$$

$$F^8 - 4F^7 + 7F^6 - 2F^5 + 15F^4 + 2F^3 + 7F^2 + 4F + 1$$

is stable by the η-action of G_k. We can combine these polynomials with those attached to the sets of cusps in Corollary 4.3 to obtain functions on $X(5)$ defined over k. Thus, $F(F^2 - F - 1)/(F^4 + 3\,F^3 - F^2 - 3\,F + 1)$ would be the simplest one to choose, but it generates over $k(j)$ an extension of degree 15. We can take instead the modular function

$$\mathfrak{J} = \frac{-F(F^{10} - 11F^5 - 1)}{(F^4 + 3F^3 - F^2 - 3F + 1)(F^8 - 4F^7 + 7F^6 - 2F^5 + 15F^4 + 2F^3 + 7F^2 + 4F + 1)}$$

which satisfies over $k(j)$ the quintic irreducible polynomial

$$\Phi(X) = X^5 + \frac{40}{j}\,X^2 - \frac{5}{j}\,X + \frac{1}{j}\,.$$

Let us see that the splitting field of this polynomial over $k(j)$ is the function field $k(\sqrt{5}\,)(X(5))$, hence it has Galois group $\mathrm{PGL}_2(\mathbb{F}_5)$, as shown in the following diagram:
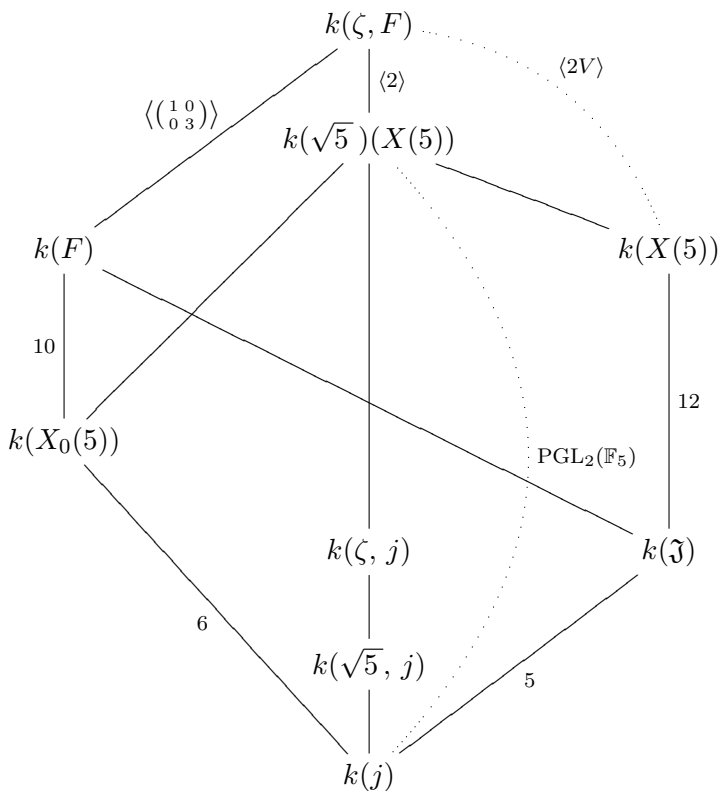
Proposition 4.4. *The function field* $k(\sqrt{5}\,)(X(5))$ *is generated over* k *by the roots over* $k(j)$ *of the above polynomial* $\Phi(X)$.

Proof. The function $\mathfrak{J}$ given before can be checked to be invariant by the automorphism in Proposition 4.2, so it generates over $k(j)$ a quintic extension inside $k(X(5))$. Since $j = (-40\,\mathfrak{J}^2 + 5\,\mathfrak{J} - 1)/\mathfrak{J}^5$, this quintic extension is actually generated by $\mathfrak{J}$ over k. Now, recall that the group $\mathrm{PGL}_2(\mathbb{F}_5)$ is generated by the above matrix V and the matrix U in Section 1. These matrices satisfy the relation $V\,U^4 = (U\,V)^3$. So the map from $\mathrm{PGL}_2(\mathbb{F}_5)$ to the symmetric group $\mathcal{S}_5$ that sends U and V to the permutations $(1, 2, 3, 4, 5)$ and $(1, 2)$, respectively, is an isomorphism. Thus, the Galois group of $k(\sqrt{5}\,)(X(5))$ over $k(j)$ is isomorphic to $\mathcal{S}_5$, so it must necessarily be the Galois group of $\Phi(X)$. $\square$

4.2. Rational points on the twisted curves $X(5)_\varrho$ and $X(5)'_\varrho$. Let us now take a surjective Galois representation

$$\varrho : \mathrm{G}_k \longrightarrow \mathrm{PGL}_2(\mathbb{F}_5)$$

with cyclotomic determinant. The fixed field K of ϱ determines ϱ up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_5)$. As noticed in the proof of Proposition 4.4, this group is isomorphic to $\mathcal{S}_5$. Consider a quintic polynomial f in $k[X]$ with splitting field K over k and identify $\mathrm{Gal}(K/k)$ with $\mathcal{S}_5$ by ordering the roots $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$ of f. The cyclotomic hypothesis on ϱ amounts to saying that the discriminant of f is 5 in k^*/k^{*2}, namely that the quadratic extension of k inside K is generated by $\sqrt{5}$.

Consider the cocycles ξ, ξ' of G_k with values in $\mathrm{Aut}(X(5))$ defined by ϱ as in Subsection 2.2, together with the curves $X(5)_\varrho$, $X(5)'_\varrho$ attached to them and the corresponding twisted Galois actions on the function field of $X(5)$. Both cases are completely analogous, so we just treat one of them in the next paragraph.

The function field of $X(5)_\varrho$ over k is identified with the subfield $K(X(5))^\xi$ of $K(X(5))$ fixed by the ξ-action of G_k. By Corollary 2.8, the (faithful) ξ-action of $\mathrm{Gal}(K/k)$ on $k(\sqrt{5}\,)(X(5))$ can be seen as the Galois action on this function field as an extension of $k(j)$. Thus, there exists an order $\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3, \mathfrak{J}_4, \mathfrak{J}_5$ for the roots of the polynomial $\Phi(X)$ in Proposition 4.4 that is compatible with the order of the above roots $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$ with respect to the ξ-action of $\mathrm{Gal}(K/k)$, in the sense that every Galois automorphism induces the same permutation in both sets of roots. Then, the functions

$\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4, \mathfrak{H}_5$ defined by the linear system

$$\begin{pmatrix} \mathfrak{J}_1 \\ \mathfrak{J}_2 \\ \mathfrak{J}_3 \\ \mathfrak{J}_4 \\ \mathfrak{J}_5 \end{pmatrix} = \begin{pmatrix} \beta_1^4 & \beta_1^3 & \beta_1^2 & \beta_1 & 1 \\ \beta_2^4 & \beta_2^3 & \beta_2^2 & \beta_2 & 1 \\ \beta_3^4 & \beta_3^3 & \beta_3^2 & \beta_3 & 1 \\ \beta_4^4 & \beta_4^3 & \beta_4^2 & \beta_4 & 1 \\ \beta_5^4 & \beta_5^3 & \beta_5^2 & \beta_5 & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{H}_1 \\ \mathfrak{H}_2 \\ \mathfrak{H}_3 \\ \mathfrak{H}_4 \\ \mathfrak{H}_5 \end{pmatrix}$$

are generators over k for the function field of $X_\varrho(5)$. Indeed, from Proposition 4.4 we obtain the equalities

$$K(X(5)) = K(\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3, \mathfrak{J}_4, \mathfrak{J}_5) = K(\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4, \mathfrak{H}_5).$$

Moreover, the functions $\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4, \mathfrak{H}_5$ are invariant by the ξ-action of $\mathrm{Gal}(K/k)$. Hence,

$$K(X(5))^\xi = k(\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4, \mathfrak{H}_5).$$

Since

$$\Phi(X) = (X - \mathfrak{J}_1)(X - \mathfrak{J}_2)(X - \mathfrak{J}_3)(X - \mathfrak{J}_4)(X - \mathfrak{J}_5),$$

explicit polynomial equations over k relating $\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4, \mathfrak{H}_5$ and j can be obtained. Note, in particular, that a k-rational point on $X(5)_\varrho$ yields a polynomial in $k[X]$ of the form

$$X^5 + \frac{40}{j_*} X^2 - \frac{5}{j_*} X + \frac{1}{j_*}$$

with splitting field K over k. The same holds for a k-rational point on $X(5)'_\varrho$.

Assume now that the given quintic polynomial f is of the form

$$f(X) = X^5 + a X^2 + b X + c$$

for some a, b, c in k. In this case, the relation $\mathfrak{J}_1 + \mathfrak{J}_2 + \mathfrak{J}_3 + \mathfrak{J}_4 + \mathfrak{J}_5 = 0$ translates into

$$5 \mathfrak{H}_5 = 4 b \mathfrak{H}_1 + 3 a \mathfrak{H}_2.$$

Let then $\mathfrak{S}_2, \mathfrak{S}_3, \mathfrak{S}_4, \mathfrak{S}_5$ be the last four elementary symmetric functions of $\mathfrak{J}_1, \mathfrak{J}_2, \mathfrak{J}_3, \mathfrak{J}_4, \mathfrak{J}_5$ regarded as homogeneous polynomials in $k[\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4]$. The coefficients of the polynomial $\Phi(X)$ yield the equalities

$$\mathfrak{S}_2 = 0, \qquad \mathfrak{S}_3 = 8 \mathfrak{S}_4 = 40 \mathfrak{S}_5 = -40/j,$$

so that one has the following expressions for j as homogeneous rational function on $\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3, \mathfrak{H}_4$:

$$j = -5^5 \frac{\mathfrak{S}_5{}^4}{\mathfrak{S}_4{}^5} = -8^4 5 \frac{\mathfrak{S}_4{}^3}{\mathfrak{S}_3{}^4}.$$

Thus, the curves $X(5)_\varrho$ and $X(5)'_\varrho$ are irreducible components of the one-dimensional projective variety $\mathfrak{X}(5)_f$ defined by the equations

$$\mathfrak{S}_2 = 0, \qquad 5\,\mathfrak{S}_3\,\mathfrak{S}_5 = 8\,\mathfrak{S}_4{}^2$$

in the polynomial ring $k[\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3, \mathfrak{h}_4]$. Furthermore, the correspondence $(\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3, \mathfrak{h}_4) \longmapsto (\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3)$ defines a birational map from $\mathfrak{X}(5)_f$ to a plane (singular) projective model with two irreducible components. Finally, the following computation, due to the second author and A. Rio, ensures the existence of k-rational points. Write the discriminant of the polynomial f as $5\,d^2$ for some d in k^*. Then, there is a choice for the sign of d such that

$$\mathfrak{h}_1 = 2\,(5\,a\,c - 8\,b^2)(18\,a^2 b^2 - 45\,a^3 c - 250\,b\,c^2 - 10\,b\,d),$$

$$\mathfrak{h}_2 = (5\,a\,c - 8\,b^2)(165\,a^2 b\,c + 625\,c^3 - 48\,a\,b^3 + 25\,c\,d),$$

$$\mathfrak{h}_3 = 2\,(5\,a\,c - 8\,b^2)^2\,(15\,a\,c - 4\,b^2),$$

$$\mathfrak{h}_4 = 702\,a^4 b^2 c + 9400\,a\,b^3 c^2 - 216\,a^3 b^4 - 640\,b^5 c - 810\,a^5 c^2$$
$$\qquad - 12375\,a^2 b\,c^3 - 15625\,c^5 + d\,(216\,a\,b^3 - 270\,a^2 b\,c - 625\,c^3)$$

are the coordinates of a point on $\mathfrak{X}(5)_f$. Both choices for the sign of d can actually be made whenever $\mathfrak{h}_3 \neq 0$.

The interpretation given in Theorem 2.5 for the k-rational points on $X(5)_\varrho$ and $X(5)'_\varrho$ translates now the above discussion into the next restatement of Theorem 3.2 in [3].

Theorem 4.5. *A representation of* G_k *onto* $\mathrm{PGL}_2(\mathbb{F}_5)$ *with cyclotomic determinant is principal if and only if it is realized by an elliptic curve defined over k, hence by infinitely many isomorphism classes of them.*

Remark 4.6. The k-rational points on $\mathfrak{X}(5)_f$ are in bijection with the principal polynomials

$$f_*(X) = X^5 + a_*\,X^2 + b_*\,X + c_*$$

in $k[X]$ that satisfy the relation $5\,a_* c_* = 8\,b_*^2$ and have splitting field K over k, up to transformations of the form $X^5 + \delta^2 a_*\,X^2 + \delta^3\,b_*\,X + \delta^4 c_*$ for δ in k^*. All three coefficients a_*, b_*, c_* must be non-zero, since a polynomial of the form $X^5 + c$ cannot have Galois group $\mathcal{S}_5$. Given such a polynomial f_*, the value

$$j_* = -5^5\,\frac{c_*^4}{b_*^5} = -8^4\,5\,\frac{b_*^3}{a_*^4}$$

is the j-invariant of an elliptic curve over k realizing ϱ, corresponding to a k-rational point on one of the twists $X(5)_\varrho$, $X(5)'_\varrho$. Moreover, the j-invariant of any such elliptic curve is obtained in this way from some polynomial f_* as above.

References

[1] R.W. Carter, *Simple groups of Lie type*. Pure and Applied Mathematics **28**. John Wiley & Sons, London-New York-Sydney, 1972.

[2] J. Fernández, *Elliptic realization of Galois representations*. PhD thesis, Universitat Politècnica de Catalunya, 2003.

[3] J. Fernández, J-C. Lario, A. Rio, *On twists of the modular curves $X(p)$*. Bull. London Math. Soc. **37** (2005), 342–350.

[4] J. González, *Equations of hyperelliptic modular curves*. Ann. Inst. Fourier (Grenoble) **41** (1991), 779–795.

[5] D. S. Kubert, S. Lang, *Modular units*. Grundlehren der Mathematischen Wissenschaften **244**. Springer-Verlag, New York, 1981.

[6] J-C. Lario, A. Rio, *An octahedral-elliptic type equality in* $\mathrm{Br}_2(k)$. C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 39–44.

[7] G. Ligozat, *Courbes modulaires de niveau* 11. Modular functions of one variable V, 149–237. Lecture Notes in Math. **601**, Springer, Berlin, 1977.

[8] B. Mazur, *Rational points on modular curves*. Modular functions of one variable V, 107–148. Lecture Notes in Math. **601**, Springer, Berlin, 1977.

[9] B. Mazur, *Open problems regarding rational points on curves and varieties*. Galois representations in arithmetic algebraic geometry (Durham, 1996), 239–265. London Math. Soc. Lecture Note Ser. **254**. Cambridge Univ. Press, 1998.

[10] D. E. Rohrlich, *Modular curves, Hecke correspondence, and L-functions*. Modular forms and Fermat's last theorem (Boston, 1995), 41–100. Springer, New York, 1997.

[11] K. Y. Shih, *On the construction of Galois extensions of function fields and number fields*. Math. Ann. **207** (1994), 99–120.

[12] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan **11**. Iwanami Shoten Publishers, Tokyo, 1971.

Julio Fernández
Departament de Matemàtica Aplicada 4
Universitat Politècnica de Catalunya
EPSEVG, av. Víctor Balaguer
E-08800 Vilanova i la Geltrú
E-mail: julio@ma4.upc.edu

Joan-C. Lario
Departament de Matemàtica Aplicada 2
Universitat Politècnica de Catalunya
Edifici Omega, Campus Nord
E-08034 Barcelona
E-mail: joan.carles.lario@upc.edu