Galois Representations and the Tame Inverse Galois Problem[1]

Sara Arias-de-Reyna and Núria Vila [2]

1 Introduction

In this paper we will focus on a variant of the Inverse Galois Problem over the rationals, emphasizing the progress made through the analysis of the Galois representations arising from arithmetic-geometric objects. The study of the Inverse Galois Problem explores the finite quotients of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and sheds light on its structure.

The Inverse Galois Problem over $\mathbb{Q}$, first considered by D. Hilbert around 1890, asks whether, given a finite group G, there exists a finite Galois extension $K/\mathbb{Q}$ with Galois group G. This problem, which remains unsolved today, has given rise to significant mathematical advances, and several different techniques have been developed to address it. A strategy to deal with it is the constructive Galois theory (or rigidity method), which roughly consists in realizing the group G as the Galois group of a polynomial with coefficients in the complex numbers (which is possible thanks to the Riemann existence theorem for compact surfaces) and imposing some conditions that guarantee that, in fact, the polynomial is defined over $\mathbb{Q}(T)$, where T is a variable. This method has been very successful, and thanks to it many simple groups are now known to be realizable as Galois groups over $\mathbb{Q}$. For instance, all sporadic simple groups save the Mathieu group M_{23} have been realized through this method (cf. [20]).

Given a finite group G, when this method is applied one usually obtains a realization of G as the Galois group of a wildly ramified extension. Noting this fact, B. Birch posed the following question around 1994 (see Section 2 of [5], cf. [16]).

Problem 1.1. Given a finite group G, is there a tamely ramified Galois extension $K/\mathbb{Q}$ with Galois group G?

This problem is one of the possible variants of the Inverse Galois Problem, involving a ramification condition, which have been studied. For instance, let us fix a finite set of primes, say S, and let G be a finite group. Can we realize the group G as the Galois group of an extension $K/\mathbb{Q}$ which is unramified in S? Note that this is a stronger question than Problem 1.1, since if it can be solved for a

[1]Preprint version. A final version is published in *WIN—women in numbers*, 277–288, Fields Inst. Commun., 60, Amer. Math. Soc., Providence, RI, 2011.

[2]Dept. d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via de les Corts, Catalanes, 585, 08007 Barcelona, Spain
E-mail addresses: ariasdereyna@ub.edu (S. Arias-de-Reyna), nuriavila@ub.edu (N. Vila).

finite group G and any prefixed set S, we can, in particular, choose a set S containing all the primes dividing the order of G. The extension $K/\mathbb{Q}$ obtained will be tamely ramified. In this way it can be proved that Problem 1.1 has an affirmative answer for finite abelian groups, symmetric groups (and all groups such that the Noether Problem has an affirmative answer [31]), finite solvable groups (see [22], [18]) and alternating groups A_n [24].

On the other hand, the Mathieu groups M_{11} and M_{12}, the group of automorphisms of M_{22} (cf. [25]), and the finite central extensions of symmetric groups, alternating groups and the Mathieu groups M_{11} and M_{12} (cf. [23]) can be realized as the Galois group of a finite tamely ramified extension of $\mathbb{Q}$.

A different approach to the Inverse Galois Problem is the study of Galois representations of the absolute Galois group $G_{\mathbb{Q}}$, obtained through an action upon certain geometric objects with arithmetic properties. Let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$$

be a continuous Galois representation, where V denotes a finite-dimensional vector space over a finite field $\mathbb{F}$ of positive characteristic ℓ, endowed with the discrete topology, and where the topology on $G_{\mathbb{Q}}$ is the Krull topology. It holds that

$$\mathrm{Im}\rho \simeq G_{\mathbb{Q}}/\ker\rho \simeq \mathrm{Gal}(K/\mathbb{Q}),$$

where $K/\mathbb{Q}$ is a finite Galois extension. Thus we obtain a realization of $\mathrm{Im}(\rho)$ as a Galois group over $\mathbb{Q}$. This strategy has already been used to address the Inverse Galois Problem for families of linear groups (cf. [35], [10], [11], [36], [12], [17]). In order to make use of techniques of this kind, it is essential to have explicit criteria to determine precisely the image of such a representation.

This strategy can be adapted to address Problem 1.1. Although the realizations obtained are mostly wildly ramified, this ramification usually occurs only at the prime ℓ, or perhaps also at a finite set of primes which is related to the properties of the arithmetic-geometric object. The key point is to choose this object carefully in order to obtain stronger control over the ramification that may occur, and simultaneously ensuring that the image of the Galois representation is large. One needs explicit criteria that ensure that the ramification at every prime is at most tame. It will usually be far easier to tackle the primes p different from ℓ than to ensure tame ramification at the prime ℓ. The construction of Galois representations with prefixed local behaviour is a very active research field today.

To fix some notation, we will denote by I_p the inertia group at the prime p, and by $I_{p,\mathrm{w}}$ the wild inertia group at p (see section 3). Note that the Galois extension $K/\mathbb{Q}$ will be unramified (respectively tamely ramified) at p if $\rho(I_p) = \{\mathrm{Id}\}$ (respectively $\rho(I_{p,\mathrm{w}}) = \{\mathrm{Id}\}$).

First we will consider the Galois representations attached to the ℓ-torsion points of elliptic curves, and we will give a sketch of [1], attaining tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for each prime number ℓ. The next section is devoted to present some progress in the tame Galois realization of linear groups in the families $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ and $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ by means of the Galois representations attached to modular forms. Finally, the last section gives an overview of the results in [3] and [4] (see also [2]), where tame Galois realizations of the groups in the family $\mathrm{GSp}_4(\mathbb{F}_\ell)$ are obtained for every prime $\ell \geq 5$ through the study of the Galois representations attached to the ℓ-torsion points of Jacobians of genus

2 curves. We also present some general criteria concerning the Galois representations attached to the ℓ-torsion points of an abelian variety in any dimension.

Acknowledgements: Research partially supported by MEC grant MTM2009-07024. The first author is also supported by a FPU predoctoral grant AP-20040601 of the MEC.

2 Elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals. Let us consider the group $E[\ell]$ of ℓ-torsion points of E. There is a natural action of the absolute Galois group $G_{\mathbb{Q}}$ on $E[\ell]$, which gives rise to a continuous Galois representation

$$\varphi_\ell : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

This representation provides a realization of the image of φ_ℓ as a Galois group over $\mathbb{Q}$, since

$$\mathrm{Im}\ \varphi_\ell \simeq G_{\mathbb{Q}}/\ker \varphi_\ell \simeq \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}),$$

where $\mathbb{Q}(E[\ell])/\mathbb{Q}$ denotes the finite Galois extension obtained by adjoining to $\mathbb{Q}$ the coordinates of the ℓ-torsion points of E. Therefore, if φ_ℓ is surjective, we obtain a realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$. It is a well-known result of J-P. Serre that if E does not have complex multiplication, then φ_ℓ is surjective for all but finitely many primes ℓ (see [32], Theorem 2 of § 4.2). This result suggests that one can use these representations to realize groups of the family $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois groups over $\mathbb{Q}$. In fact, Serre establishes in Example 5.5.6 of [32] that the Galois representation attached to the elliptic curve E of conductor $N = 37$ provides a Galois realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for all primes ℓ (cf. [28] for an explicit determination of the images of Galois representations associated to elliptic curves). In order to obtain results of this kind, one needs an explicit control of the exceptional primes, i.e., the primes ℓ such that φ_ℓ is not surjective. For instance, if the elliptic curve $E/\mathbb{Q}$ is semistable, then the Galois representation attached to the ℓ-torsion points of E is surjective if $\ell \geq 11$ (see Theorem 4 of [21]).

In order to produce tame Galois realizations, we need explicit conditions upon the elliptic curve E that ensure that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified. If $p \neq \ell$ is a prime number and E has semistable reduction at p, then the image of the wild inertia group at p by φ_ℓ is trivial. On the other hand, things become more complicated at the prime ℓ. In [32], Serre proves that if the kind of reduction of E at ℓ is good and supersingular, then the image of the wild inertia group at ℓ by φ_ℓ is trivial. Therefore we have the following result.

Theorem 2.1. *Let $\ell \geq 11$ be a prime number, and consider a semistable elliptic curve $E/\mathbb{Q}$ such that ℓ has good supersingular reduction. Then the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Given a prime number $\ell \geq 11$, we want to construct an elliptic curve E satisfying the conditions in Theorem 2.1. The most interesting point in this construction is to produce a supersingular

elliptic curve $\widetilde{E}/\mathbb{F}_\ell$. We give a construction in [1], § 3, based on some results of [6] concerning the factorization of the Deuring polynomial. Another construction has appeared in [7].

In fact, it turns out that one can replace the conditions of Theorem 2.1 with others which are more restrictive but also very simple. Namely, it suffices to consider the elliptic curve defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ satisfy certain congruences modulo powers of different prime numbers. One can find a precise statement in Theorem 4.4 of [1]. The primes 2, 3, 5 and 7 can be handled similarly, applying specific criteria that ensure that the Galois representation φ_ℓ is surjective (namely, see Proposition 2.1 in [28], Theorem 2.3-(iii) in [28], § 5.3 and Proposition 19 in [32]). As a consequence we have the following result (see [1], Theorem 4.6).

Theorem 2.2. *For each prime number ℓ, there exist infinitely many elliptic curves $E/\mathbb{Q}$ such that the Galois extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Moreover, the construction is explicit: given ℓ, we can produce such elliptic curves.

3 Modular forms

Let f be a cuspidal form of weight 2 and level N, which is an eigenform for all Hecke operators. Assume that f is normalized, and call $\mathbb{Q}_f$ the field of coefficients of f, that is to say, the number field generated over $\mathbb{Q}$ by adjoining all the coefficients of the Fourier expansion of f. A classical construction of Shimura attaches to f a continuous Galois representation

$$\overline{\rho}_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell).$$

As we saw in the introduction, such a representation provides us with a realization of $\mathrm{Im}(\overline{\rho}_{f,\ell})$ as Galois group over $\mathbb{Q}$. In [29], K. Ribet studies the image of this representation. Under certain hypothesis, he concludes that the image of $\overline{\rho}_{f,\ell}$ coincides with $\{x \in \mathrm{GL}_2(\mathbb{F}_\lambda) : \det(x) \in \mathbb{F}_\ell^*\}$, where $\mathbb{F}_\lambda$ is a certain finite extension of $\mathbb{F}_\ell$. In order to get rid of the condition on the determinant above, we will consider the projection of $\mathrm{Im}(\overline{\rho}_{f,\ell})$ inside the projective space $\mathrm{PGL}_2(\mathbb{F}_\lambda)$. The precise statement is the following (cf. [26]).

Theorem 3.1. *Let $f \in S_2(N)$ be a newform with no complex multiplication and no non-trivial inner twists. For a rational prime ℓ, let $\mathbb{F}_\lambda$ be the corresponding residue field of the coefficient field $\mathbb{Q}_f$, and call $r = [\mathbb{F}_\lambda : \mathbb{F}_\ell]$. For all but finitely many primes ℓ, the projective image of $\overline{\rho}_{\ell,f}$ coincides with $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ if r is even and $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ if r is odd.*

Therefore, in this section we try to obtain tame Galois realizations of groups of the families $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ and $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$.

Given a continuous, odd, irreducible Galois representation

$$\overline{\rho}_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

there is a way to measure the ramification away from ℓ. In [33], J-P. Serre attaches to each Galois representation as above a *conductor* $N(\overline{\rho}_\ell)$, a *weight* $k(\overline{\rho}_\ell)$ and a *character* $\varepsilon(\overline{\rho}_\ell)$, and he conjectures that $\overline{\rho}_\ell$ is isomorphic to the Galois representation $\overline{\rho}_{g,\ell}$ attached to a modular form g of level $N(\overline{\rho}_\ell)$, weight $k(\overline{\rho}_\ell)$ and character $\varepsilon(\overline{\rho}_\ell)$. The conductor $N(\overline{\rho}_\ell)$ constitutes a precise measure of the ramification of $\overline{\rho}_\ell$ at the primes $p \neq \ell$.

Let us briefly sketch its definition. Fix a prime number p. Then one can define an integer number $n(p)$ in the following way (see [33], § 1). Let us fix an extension w to $\overline{\mathbb{Q}}$ of the p-adic valuation in $\mathbb{Q}$. This is equivalent to fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

On the other hand, since $\overline{\rho}_\ell$ is continuous, there exists a finite Galois extension $K/\mathbb{Q}$ such that $\ker \overline{\rho}_\ell \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The embedding above restricts to an embedding $K \hookrightarrow K_w$, where K_w denotes the completion of K with respect to the restriction to K of the valuation w. Let $\mathcal{O}_w$ be the ring of integers of K_w with respect to the valuation w, and normalize w so that $w(\mathcal{O}_w) = \mathbb{Z}$. For each $i \in \mathbb{N}$, we can define the *i-th higher ramification group* as

$$G_i = \{\sigma \in \mathrm{Gal}(K_w/\mathbb{Q}_p) \text{ such that } w(\sigma(x) - x) \geq i + 1 \text{ for all } x \in \mathcal{O}_w\}.$$

Since $\mathrm{Gal}(K_w/\mathbb{Q}_p)$ is isomorphic to the decomposition group of w in $\mathrm{Gal}(K/\mathbb{Q})$, we can view G_i inside $\mathrm{Gal}(K/\mathbb{Q})$.

In this way we obtain a decreasing sequence of subgroups of the inertia group at p:

$$I_p(K/\mathbb{Q}) = G_0 \supset I_{p,\mathrm{w}}(K/\mathbb{Q}) = G_1 \supset G_2 \supset \cdots \supset G_i \supset \cdots . \tag{1}$$

Let V be a 2-dimensional vector space over $\overline{\mathbb{F}}_\ell$, and consider the action of $G_\mathbb{Q}$ given by $\overline{\rho}_\ell$ upon V. For each $i \in \mathbb{N}$, define

$$V_i := \{v \in V : \overline{\rho}_\ell(\sigma)(v) = v \text{ for all } \sigma \in G_i\}$$

A way to measure the size of G_i is to consider the dimension of V_i as $\overline{\mathbb{F}}_\ell$-vector space. More precisely, one can consider the quantity

$$n(p) = \sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{(G_0 : G_i)}, \tag{2}$$

where $(G_0 : G_i)$ denotes the index of G_i in G_0. It can be seen that $n(p)$ is an integer number, which is greater than or equal to zero. Moreover, $n(p) = 0$ if and only if $\overline{\rho}_\ell$ is unramified at p. Since $\overline{\rho}_\ell$ can only ramify in the primes which are ramified in the extension $K/\mathbb{Q}$, $n(p) = 0$ for all but finitely many primes p.

Definition 3.2. The *Artin conductor* is defined as

$$N(\overline{\rho}_\ell) = \prod_{\substack{p \neq \ell \\ p \text{ prime}}} p^{n(p)},$$

where $n(p)$ is given by Equation (2).

If $n(p) = 1$, it must hold that $\dim(V/V_0) = 1$ and all the remaining terms are zero. In particular, $V_1 = V$, that is to say, the wild inertia group at p acts trivially upon V. Therefore, a sufficient condition for $\overline{\rho}_\ell$ to be tamely ramified at a prime $p \neq \ell$ is that the exponent $n(p)$ of p in the Artin conductor $N(\overline{\rho}_\ell)$ is either 0 or 1. In particular, if $N(\overline{\rho}_\ell)$ is squarefree, then $\overline{\rho}_\ell$ is tamely ramified at all primes $p \neq \ell$.

Let us consider the Galois representation $\overline{\rho}_{f,\ell}$ attached to a newform $f \in S_2(N)$. According to Serre's conjecture, $\overline{\rho}_{f,\ell}$ comes from a modular form g of level $N(\overline{\rho}_{f,\ell})$ (and weight $k(\overline{\rho}_{f,\ell})$, character $\varepsilon(\overline{\rho}_{f,\ell})$). But it may well be that $N \neq N(\overline{\rho}_{f,\ell})$. Luckily, there is a strong relationship between the two values: thanks to the work of Carayol and Livné (cf. [8], remark following Theorem 1 and [19], Proposition 0.1), we know that $N(\overline{\rho}_{f,\ell})$ divides N (when $\overline{\rho}_{f,\ell}$ is irreducible). Therefore, if N is squarefree, then $N(\overline{\rho}_{f,\ell})$ has no choice but to be squarefree too.

Proposition 3.3. *Let $f \in S_2(N)$ be a newform, and let $\overline{\rho}_{f,\ell}$ be the Galois representation attached to f. Assume that $\overline{\rho}_{f,\ell}$ is irreducible. If N is squarefree, then $\overline{\rho}_{f,\ell}$ is tamely ramified at all primes $p \neq \ell$.*

Now that we have dealt with all primes $p \neq \ell$, we address the problem of obtaining some control over the ramification at the prime ℓ. In the case of elliptic curves, this was achieved by requiring the elliptic curve to have good supersingular reduction at ℓ. Is there a similar condition in this general context?

As a matter of fact, the answer is affirmative. There exist the concepts of *ordinary* and *supersingular* (see [30], Chapter 2, § 2.1).

Definition 3.4. Let $f \in S_k(N, \varepsilon)$ be a newform, and call a_p the eigenvalue corresponding to the Hecke operator T_p. Let ℓ be a prime number. We will say that the newform f is *supersingular* at ℓ if there exists a homomorphism φ from the ring of integers of $\mathbb{Q}_f$ to $\overline{\mathbb{F}}_\ell$ such that $\varphi(a_\ell) = 0$

Fontaine has studied the image by $\overline{\rho}_{f,\ell}$ of the inertia group at ℓ when f is supersingular. The following theorem, which is Theorem 2.6 of [13], seems to have appeared in a letter from Fontaine to Serre.

Theorem 3.5 (Fontaine)**.** *Let f be a newform in $S_k(N, \varepsilon)$ with $2 \leq k \leq \ell + 1$. Assume that $\overline{\rho}_{f,\ell}$ is supersingular at ℓ. Then $\overline{\rho}_{f,\ell}$ is irreducible and*

$$\overline{\rho}_{f,\ell}|_{I_\ell} = \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix},$$

where ψ and ψ' are the two fundamental characters of level 2.

As a corollary, we obtain:

Corollary 3.6. *Let $f \in S_2(N)$ be a newform, and let $\overline{\rho}_{f,\ell}$ be the Galois representation attached to f. If $\overline{\rho}_{f,\ell}$ is supersingular, then it is tamely ramified at ℓ.*

Let us now consider the image of $\overline{\rho}_{f,\ell}$. We know that for all but finitely many primes ℓ the projective image of $\overline{\rho}_{f,\ell}$ is $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ for a certain exponent r, provided that some good conditions hold (no complex multiplication and no non-trivial inner twists). This result is similar to Serre's result about the image of the Galois representations attached to the ℓ-torsion points of elliptic curves. But recall that this was not enough for us, and we had to resort to a theorem of Mazur, which allowed us to replace the condition "for all but finitely many primes ℓ" by "for all primes $\ell \geq 11$", provided we also required the elliptic curve to be semistable.

A result of this kind is not available in this context. Therefore we will put to use such means as we have. A result of L. Dieulefait and N. Vila (see [10]) provides us with an algorithm which takes as input a modular form f and produces a finite set of primes S such that the representation has large image at all primes outside this set. In this way, they manage to realize the groups $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$, $\mathrm{PGL}_2(\mathbb{F}_{\ell^3})$, $\mathrm{PSL}_2(\mathbb{F}_{\ell^4})$ for many primes ℓ.

Their method relies on some results of Ribet (see [29]). More precisely, they make use of the following theorem (cf. § 3 of [29]).

Theorem 3.7. *Let $f \in S_2(N)$ be a newform with coefficient field $\mathbb{Q}_f$ and ring of integers $\mathcal{O}$, ℓ a prime number and λ a prime of $\mathcal{O}$ above ℓ. Call $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Let $\rho_{f,\lambda}$ the λ-adic Galois representation attached to f. Then the image of this representation equals $\{x \in \mathrm{GL}_2(\mathcal{O}_\ell) : \det(x) \in \mathbb{Z}_\ell^*\}$ if the following conditions are satisfied:*

(0) ℓ does not ramify in $\mathbb{Q}_f/\mathbb{Q}$.

(1) The determinant map $det \circ \rho_{f,\lambda}$ is surjective.

(2) $\ell \geq 5$.

(3) The image of $\rho_{f,\lambda}$ contains an element x_ℓ such that $(\mathrm{trace}\ x_\ell)^2$ generates $\mathcal{O}_\ell$ as a $\mathbb{Z}_\ell$-algebra.

(4) For each $\lambda|\ell$, the image of the composition of $\rho_{f,\lambda}$ with the reduction modulo λ is an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_\lambda)$ whose order is divisible by ℓ.

The algorithm of Dieulefait and Vila consists of several steps, which are designed to guarantee that some of the conditions above hold. As a general remark, we can say that each step consists of finding an auxiliary prime p, satisfying perhaps some conditions regarding the level N and the prime ℓ, and such that the coefficient a_p enjoys some suitable property involving λ. If the image of the representation $\rho_{f,\lambda}$ is large, such a prime p will exist. A complete description of the algorithm can be found in section 2.2 of [10].

Our wish is to combine this algorithm with the tameness results presented above in order to obtain tame Galois realizations of linear groups of the form $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$. Unfortunately, we have not been able to obtain a procedure that, given a prime number ℓ, constructs a suitable modular form yielding a tame Galois realization of the corresponding group. This problem remains a challenging issue for further investigation. Nevertheless, the results we have explained allow us to present a few concrete examples.

In [10], section 3.1, the authors apply their algorithm to some weight 2 newforms whose field of coefficients is a quadratic extension of $\mathbb{Q}$. More precisely, they consider newforms of level 23, 29, 410, 414, 496, 418, 546. For each newform, they provide a finite set of primes such that the Galois representation attached to it has large image (in the sense of Theorem 3.1) whenever ℓ does not belong to this set. We present their results in the following table:

Table 1: Computations of big image

Modular form	Level	Coefficient Field	Set of primes
f_1	23	x^2-5	5, 11
f_2	29	x^2-2	7
f_3	410	x^2-3	5, 41
f_4	410	x^2-17	5, 41
f_5	414	x^2-7	7, 23
f_6	496	x^2-33	11, 31
f_7	418	x^2-13	11, 13, 19
f_8	546	x^2-57	7, 13, 19

Our purpose is to take advantage of their computations and try to produce tamely ramified Galois realizations of groups of the form $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ from the modular forms $f_1,\dots,f_8$ presented above. First of all, note that the numbers 23, 29, 410, 418, 546 are squarefree. Therefore, we know that the Galois representations $\overline{\rho}_{f,\ell}$ corresponding to the modular forms $f=f_1,f_2,f_3,f_4,f_7,f_8$ can be wildly ramified only at the prime ℓ. In order to ensure that they are also tamely ramified at ℓ, we will make use of Corollary 3.6.

We have taken each of the modular forms f_1,f_2,f_3,f_4,f_7,f_8 and have looked at their coefficients a_ℓ, for all primes $\ell<5000$. Since we are looking for Galois realizations of groups of the form $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$, we are only interested in the primes which are inert in the extension $\mathbb{Q}_{f_i}/\mathbb{Q}$. For each modular form f_i we can find the coefficient field $\mathbb{Q}_{f_i}$ in the table above.

For each $i=1,2,3,4,7$ and 8, we list below the primes $\ell\leq 5000$ such that ℓ is inert in the extension $\mathbb{Q}_{f_i}/\mathbb{Q}$ and $a_\ell\in(\ell)$:

As a consequence of Proposition 3.3, Corollary 3.6 and Tables 1 and 2, we obtain the following result.

Proposition 3.8. *The following groups occur as Galois groups of a tamely ramified extension of* $\mathbb{Q}$*:*

$$\mathrm{PSL}_2(\mathbb{F}_{23^2}),\mathrm{PSL}_2(\mathbb{F}_{31^2}),\mathrm{PSL}_2(\mathbb{F}_{43^2}),\mathrm{PSL}_2(\mathbb{F}_{47^2}),\mathrm{PSL}_2(\mathbb{F}_{59^2}),\mathrm{PSL}_2(\mathbb{F}_{149^2}),$$
$$\mathrm{PSL}_2(\mathbb{F}_{173^2}),\mathrm{PSL}_2(\mathbb{F}_{1033^2}),\mathrm{PSL}_2(\mathbb{F}_{1709^2}),\mathrm{PSL}_2(\mathbb{F}_{4391^2}),\mathrm{PSL}_2(\mathbb{F}_{4799^2}).$$

Remark 3.9. We are developing these techniques in order to obtain tamely ramified extensions of an infinite set of groups in the family $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$.

Table 2: Inert supersingular primes

Modular Form	Primes ℓ
f_1	43, 1033
f_2	
f_3	173
f_4	23, 31, 4391
f_7	59, 149, 1709
f_8	47, 4799

4 Abelian varieties

Let $A/\mathbb{Q}$ be an abelian variety of dimension n, and let ℓ be a prime number. As in the case of elliptic curves, there is an action of the absolute Galois group $G_{\mathbb{Q}}$ upon the group $A[\ell]$ of ℓ-torsion points of A. This action gives rise to a continuous Galois representation

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{Aut}(A[\ell]) \simeq \mathrm{GL}_{2n}(\mathbb{F}_\ell).$$

Let us assume that A is principally polarized. One first variation with respect to the case of dimension 1 is that, if $n > 1$, then ρ_ℓ cannot be surjective. This is due to the existence of the Weil pairing, which is a non-degenerate, Galois compatible symplectic form. This compels the image of ρ_ℓ to be contained in the general symplectic group $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. As a matter of fact, if the endomorphism ring of the abelian variety is equal to $\mathbb{Z}$ and the dimension n is either odd or equal to 2 or 6, then $\mathrm{Im}\rho_\ell \simeq \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ for all but finitely many primes ℓ (see [34], Theorem 3 of 137). Therefore, one can try to obtain tame realizations of this general symplectic group as the Galois group of the extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$, obtained by adjoining to $\mathbb{Q}$ the coordinates of the points of $A[\ell]$. This problem has been addressed by the authors in [3] and [4] (cf. [2]).

Concerning the ramification, let us note that since the wild inertia group at a prime p is a pro-p-group, the only primes we need to take care of are the primes dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, that is to say, a finite quantity of primes. If $p \neq \ell$ is a prime number where A has semistable reduction, then it follows from a result of Grothendieck (see [15], Proposition 3.5 of Exposé IX, *Modeles de Néron et monodromie*) that the wild inertia group at p acts trivially on $A[\ell]$. On the other hand, the control of the action of the wild inertia group at the prime ℓ is more subtle. In [4], a condition upon the formal group law of A is found that, combined with supersingularity, allows one to control the wild ramification at ℓ (see Theorem 3.4 in [3], cf. Theorem 4.9 in [2]).

Theorem 4.1. *Let ℓ be a prime number, and let $A/\mathbb{Q}$ be an abelian variety of dimension n with good supersingular reduction at ℓ. Call $\mathbf{F}$ the formal group law attached to A at ℓ, v_ℓ the ℓ-adic valuation on $\overline{\mathbb{Q}}_\ell$ and V the group of ℓ-torsion points attached to $\mathbf{F}$. Assume that there exists a positive $\alpha \in \mathbb{Q}$ such that, for all non-zero $(x_1, \ldots, x_n) \in V$, it holds that $\min\{v_\ell(x_i) : 1 \leq i \leq n\} = \alpha$.*

Then the image of the wild inertia group by the Galois representation attached to the ℓ-torsion points of A is trivial.

If we restrict ourselves to the case of dimension $n = 2$, then we can provide very explicit conditions that ensure that the wild inertia group (at the prime ℓ as well as at all other primes $p \neq \ell$) acts trivially upon the ℓ-torsion points of the Jacobian of a genus 2 curve (see Theorem 2.7 in [4], cf. Theorem 9.2 in [2]).

Theorem 4.2. *Let C be a genus 2 curve defined by a hyperelliptic equation*

$$y^2 = f(x), \tag{3}$$

where $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ is a polynomial of degree 6 without multiple factors. Let $\ell > 2$ be a prime number, and let $\mathcal{P}$ be the set of prime numbers that divide the order of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Assume that the following conditions hold:

- *For all $p \in \mathcal{P}$ different from ℓ, C has stable reduction at p.*
- *The reduction of $f(x)$ modulo ℓ is of the form $x^6 + bx^4 + bx^2 + 1$, and the elliptic curve E defined over $\mathbb{F}_\ell$ by $y^2 = x^3 + bx^2 + bx + 1$ is supersingular.*

Then the Galois extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$ is tamely ramified.

Several tools are involved in the proof of this theorem. First of all, the multiplication by ℓ-map in the formal group law attached to the Jacobians of curves defined by an equation (3) satisfying the hypothesis of Theorem 4.2 has a very special shape, namely, it is essentially defined by one single equation. The proof of this fact is based upon the explicit computation of the formal group law attached to the Jacobian of a genus 2 curve carried out by V. Flynn in [14] (cf. [9]). This property of the multiplication by ℓ map allows one to compute the value of $\min\{v_\ell(x_i) : (x_1, x_2) \in V\}$, which in turn allows us to apply Theorem 4.1. Note that one needs a genus 2 curve with good supersingular reduction at ℓ of a particular shape, which is constructed as a very specific bielliptic curve.

It turns out that the curves in the family given in Theorem 4.2 have reducible Jacobians. We need to "deform" them a bit in order to sort out this difficulty. This requires a careful analysis of the proximity (with respect to the ℓ-adic valuation) of the solutions of two systems of equations in formal power series that are near coefficientwise.

In the case of Jacobians of genus 2 curves, one can give explicit results to control the image of the Galois representation ρ_ℓ. More specifically, we can make use of the following result (Theorem 3.7 of [4], cf. Theorem 11.9 of [2]):

Theorem 4.3. *Let G be a subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and assume that G contains a transvection. Furthermore, assume that it contains two elements whose characteristic polynomials, $P_i(X) = X^4 + a_iX^3 + b_iX^2 + a_iX + 1$ ($i = 1, 2$), satisfy the following: denoting by α_i, $1/\alpha_i$, β_i, $1/\beta_i$ the four roots of $P_i(X)$,*

- $\alpha_1 + 1/\alpha_1, \beta_1 + 1/\beta_1 \notin \mathbb{F}_\ell$ *and* $\alpha_1 + 1/\alpha_1 + \beta_1 + 1/\beta_1 \neq 0$.
- $\alpha_2 + 1/\alpha_2, \beta_2 + 1/\beta_2 \in \mathbb{F}_\ell$, $a_2^2 - 4b_2 + 8 \neq 0$ *and* $\alpha_2 \notin \mathbb{F}_\ell$.

Then G equals $\mathrm{Sp}_4(\mathbb{F}_\ell)$.

We can combine the conditions on the ramification of ρ_ℓ and the conditions on the image in order to obtain tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The task of constructing genus 2 curves satisfying all the conditions still remains. Actually, as in the case of elliptic curves, one can replace each of the conditions by a congruence modulo a certain power of a prime. That is to say, it is possible to write a statement asserting that, if $\ell \geq 5$ is a prime number and $f_0, f_1, \ldots, f_6 \in \mathbb{Z}$ satisfy certain congruences, then the Jacobian of the genus 2 curve defined by $y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ provides a tame Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. One such statement is Theorem 5.1 of [4] (cf. Theorem 12.25 of [2]), which we have not included here because of its cumbersome length. In order to obtain this theorem, one needs to exploit certain tools. For instance, one needs some results of Q. Liu relating the type of reduction of a genus 2 curve and its Igusa invariants in order to construct a transvection inside the image of ρ_ℓ. The reader can find the details in [4].

To sum up, the result we obtain is the following:

Theorem 4.4. *Let $\ell \geq 5$ be a prime number. There exist infinitely many genus 2 curves C such that the Galois representation attached to the ℓ-torsion points of $J(C)$ provides a tame Galois realization of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

References

[1] Arias-de-Reyna, S., Vila, N. *Tame Galois realizations of* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$. Journal of Number Theory, Volume **129**, Issue 5, May (2009), pages 1056-1065.

[2] Arias-de-Reyna, S. *Galois representations and tame Galois realizations*, Ph.D. Thesis, Barcelona, June 2009. Available at

`http://www.tesisenxarxa.net/TDX-0612109-101019/`

[3] Arias-de-Reyna, S. *Formal groups, supersingular abelian varieties and tame ramification*. Preprint, 2009. arXiv:0910.1212v1 [math.NT]

[4] Arias-de-Reyna, S., Vila, N. *Tame Galois realizations of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$. Preprint, 2009. arXiv:0910.1445v1 [math.NT]

[5] Birch, B. *Noncongruence subgroups, Covers and Drawings*, pages 25–46 in *The Grothendieck theory of dessins d'enfants*, Leila Schneps, editor. Cambridge Univ. Press (1994).

[6] Brillhart, J., Morton, P. *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106**, no. 1, pages 79–111 (2004).

[7] Bröker, R. *Constructing supersingular elliptic curves*, Journal of Combinatorics and Number Theory, Volume **1**, Issue 3 (2009), pages 269–273.

[8] Carayol, H. *Sur les représentations galoisiennes modulo l attachées aux formes modulaires*. Duke Math. J. **59** (1989), no. 3, pages 785–801.

[9] Cassels, J. W. S., Flynn, E. V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Matematical Society Lecture Note Series 230, Cambridge University Press (1996).

[10] Dieulefait, L., Vila, N. *Projective linear groups as Galois groups over Q via modular representations*. Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), no. 6, pages 799–810.

[11] Dieulefait, L. *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$. Experiment. Math. **11** (2002), no. 4, pages 503–512 (2003).

[12] Dieulefait, L.; Wiese, G. *On Modular Forms and the Inverse Galois Problem*. Preprint, 2009. arXiv:0905.1288v1 [math.NT]

[13] Edixhoven, B. *The weight in Serre's conjectures on modular forms*. Invent. Math. **109** (1992), no. 3, pages 563–594.

[14] Flynn, E. V., *The Jacobian and Formal Group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), no. 3, pages 425–441.

[15] Grothendieck, A. *Groupes de monodromie en géométrie algébrique I*. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, Vol. **288**. Springer-Verlag, Berlin-New York, (1972).

[16] Harbater, D. *Galois groups with prescribed ramification*. Arithmetic geometry (Tempe, AZ, 1993), pages 35–60, Contemp. Math., **174**, Amer. Math. Soc., Providence, RI, (1994).

[17] Khare, C.; Larsen, M.; Savin, G. *Functoriality and the inverse Galois problem*. Compos. Math. **144** (2008), no. 3, 541–564.

[18] Klüners, J., Malle, G. *Counting nilpotent Galois extensions*. J. Reine Angew. Math. **572**, pages 1–26 (2004).

[19] Livné, R. *On the conductors of mod l Galois representations coming from modular forms*. J. Number Theory **31** (1989), no. 2, pages 133–141.

[20] Malle, G., Matzat, B. H. *Inverse Galois theory*, Springer Monographs in Mathematics Springer-Verlag, (1999).

[21] Mazur, B. *Rational Isogenies of Prime Degree*, Inventiones math. **44**, pages 129–162 (1978).

[22] Neukirch, J., Schmidt, A., Wingberg, K. *Cohomology of number Fields*, Grundlehren der mathematischen Wissenschaften **323**, Springer, (2000).

[23] Plans, B., *Central embedding problems, the arithmetic lifting property, and tame extensions of* $\mathbb{Q}$., Int. Math. Res. Not. **23**, pages 1249–1267 (2003).

[24] Plans, B., Vila, N. *Tame* A_n*-extensions of* $\mathbb{Q}$, J. Algebra **266**, no. 1, pages 27–33 (2003).

[25] Plans, B., Vila, N. *Galois covers of* $\mathbb{P}^1$ *over* $\mathbb{Q}$ *with prescribed local or global behavior by specialization*. J. Théor. Nombres Bordeaux **17**, no. 1, pages 271–282. (2005).

[26] Reverter, A., Vila, N. *Some projective linear groups over finite fields as Galois groups over* $\mathbb{Q}$ in *Recent developments in the inverse Galois problem* (Seattle, WA, 1993), 51–63, Contemp. Math., **186**, Amer. Math. Soc., Providence, RI, (1995).

[27] Reverter, A., Vila, N. *Galois representations attached to the product of two elliptic curves*. Rocky Mountain J. Math. **30**, no. 3, pages 1121–1127 (2000).

[28] Reverter, A., Vila, N. *Images of mod* p *Galois representations associated to elliptic curves*. Canad. Math. Bull. **44**, no. 3, pages 313–322. (2001).

[29] Ribet, K. A. *On* l*-adic representations attached to modular forms. II*. Glasgow Math. J. **27** (1985), pages 185–194.

[30] Ribet, K. A., Stein, W. A. *Lectures on Serre's conjectures*. Arithmetic algebraic geometry (Park City, UT, 1999), pages 143–232, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, (2001).

[31] Saltman, D. J. *Generic Galois extensions and problems in field theory*. Adv. in Math. **43** (1982), no. 3, pages 250–283.

[32] Serre, J-P. *Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques*, Inventiones math. **15**, pages 259–331 (1972).

[33] Serre, J-P. *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{Q}/Q)$. Duke Math. J. **54** (1987), no. 1, pages 179–230.

[34] Serre, J-P. *Œuvres 4*, Springer-Verlag (2000), pages 1–55.

[35] Vila, N. *Arithmetical-geometrical Galois representations and the inverse Galois problem* in *Algebra, arithmetic and geometry with applications* (West Lafayette, IN, 2000), 775–782, Springer, Berlin, (2004).

[36] Wiese, G. *On projective linear groups over finite fields as Galois groups over the rational numbers*. In: *Modular Forms on Schiermonnikoog* edited by Bas Edixhoven, Gerard van der Geer and Ben Moonen. Cambridge University Press, 2008, 343-350.