Tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ over $\mathbb{Q}$

Sara Arias-de-Reyna and Núria Vila

Abstract

In this paper we obtain realizations of the 4-dimensional general symplectic group over a prime field of characteristic $\ell > 3$ as the Galois group of a tamely ramified Galois extension of $\mathbb{Q}$. The strategy is to consider the Galois representation ρ_ℓ attached to the Tate module at ℓ of a suitable abelian surface. We need to choose the abelian varieties carefully in order to ensure that the image of ρ_ℓ is large and simultaneously maintain a control on the ramification of the corresponding Galois extension. We obtain an explicit family of curves of genus 2 such that the Galois representation attached to the ℓ-torsion points of their Jacobian varieties provide tame Galois realizations of the desired symplectic groups.

1 Introduction

A central problem in number theory is the study of the structure of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Inverse Galois Problem over $\mathbb{Q}$, first considered by D. Hilbert, can be reformulated as a question about the finite quotients of this absolute Galois group. In spite of the many efforts made to solve the Inverse Galois Problem, it still remains open. Of course, these attempts have not been fruitless, and there are many finite groups that are known to be Galois groups over $\mathbb{Q}$. For an idea of the progress made, the reader can leaf through [32] or [23].

Assume that a finite group G can be realized as a Galois group over $\mathbb{Q}$, say $G \simeq \mathrm{Gal}(K_1/\mathbb{Q})$, where $K_1/\mathbb{Q}$ is a finite Galois extension. But perhaps

2010 Mathematics Subject Classification: 12F12, 11F80, 11G30, 11R32

Research supported by a FPU predoctoral grant AP-20040601 of the MEC and partially supported by MEC grant MTM2006-04895.

we are interested in field extensions with some ramification property, and $K_1/\mathbb{Q}$ does not satisfy it. We can ask whether there exists some other finite Galois extension, $K_2/\mathbb{Q}$, with Galois group G and enjoying this additional property. In this connection, several variants of the Inverse Galois Problem have been studied.

This paper is concerned with the following problem, posed by Brian Birch (cf. [5], Section 2).

Problem 1.1 (Tame Inverse Galois Problem)**.** Given a finite group G, is there a tamely ramified Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$?

This problem has already been dealt with for certain families of groups. It is known that solvable groups, all symmetric groups S_n, all alternating groups A_n, the Mathieu groups M_{11} and M_{12}, and their finite central extensions are realizable as the Galois group of a tamely ramified extension (cf. [17], [28], [27]).

One way to deal with the Inverse Galois Problem, and eventually with Problem 1.1, is to consider continuous Galois representations of the absolute Galois group of the rational field. Let V be a finite dimensional vector space over a finite field $\mathbb{F}$, and consider a continuous representation of $G_{\mathbb{Q}}$ (endowed with the Krull topology) in the group of automorphisms of V (with the discrete topology), say

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

Then

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

where $K/\mathbb{Q}$ is a finite Galois extension.

In other words, a continuous Galois representation of $G_{\mathbb{Q}}$ provides 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], [8], [9], [36], [10], [16]).

In this paper we will study the Galois representations that arise through the action of the absolute Galois group $G_{\mathbb{Q}}$ on the ℓ-torsion points of abelian surfaces.

For each prime number p, let us fix an immersion $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. This induces an inclusion of Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G_{\mathbb{Q}}$. Inside $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ we can consider the inertia subgroup $I_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{unr}})$ and the wild inertia subgroup $I_{p,\mathrm{w}} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{t}})$, where $\mathbb{Q}_{p,\mathrm{unr}}$ and $\mathbb{Q}_{p,\mathrm{t}}$ denote the maximal unramified extension and the maximal tamely ramified extension of $\mathbb{Q}_p$, respectively. A prime p is unramified (respectively tamely ramified) in the Galois extension $K/\mathbb{Q}$ if and only if $\rho(I_p) = \{\mathrm{Id}\}$ (respectively $\rho(I_{p,\mathrm{w}}) = \{\mathrm{Id}\}$). Therefore, if we want a Galois representation ρ to yield a tamely ramified Galois extension $K/\mathbb{Q}$, we will have to ensure that $\rho(I_{p,\mathrm{w}}) = \{\mathrm{Id}\}$ for all prime numbers p.

In [2], the authors apply this strategy to solve Problem 1.1 for the family of 2-dimensional linear groups $\mathrm{GL}_2(\mathbb{F}_\ell)$. More precisely, they consider the Galois representations attached to the ℓ-torsion points of elliptic curves, and construct explicitly elliptic curves such that this representation is surjective and moreover the image of the wild inertia group $I_{p,\mathrm{w}}$ is trivial for all primes p. In this paper we will extend these results to the case of curves of genus 2. Namely, we will prove that, for all prime number $\ell \geq 5$ there exist (infinitely many) genus 2 curves C such that the Galois representation attached to the ℓ-torsion points of the Jacobian of C provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (cf. Theorem 5.5).

We want to thank Luis Dieulefait for many enlightening conversations.

2 The Action of the Inertia Group

Let $A/\mathbb{Q}$ be an abelian variety of dimension n, and let us fix a prime ℓ. Consider the Galois representation

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

attached to the ℓ-torsion points of A. This representation gives rise to a realization of $\mathrm{Im}\rho_\ell$ as Galois group over $\mathbb{Q}$, say $\mathrm{Im}\rho_\ell \simeq \mathrm{Gal}(K/\mathbb{Q})$, where K is the number field fixed by $\ker \rho_\ell$. In this section we are interested in finding conditions over the variety A that ensure that $K/\mathbb{Q}$ is tamely ramified.

Note that it suffices to control the image by ρ_ℓ of $I_{p,\mathrm{w}}$ just for a finite quantity of primes p. Indeed, $I_{p,\mathrm{w}}$ is a pro-p-group, so that if p does not divide the cardinal of $\mathrm{GL}_{2n}(\mathbb{F}_\ell)$, the cardinal of $\mathrm{Im}(I_{p,\mathrm{w}})$ must be $p^0 = 1$.

We will first address the problem of obtaining tame ramification at a prime $p \neq \ell$. Let us place ourselves in a more general setting. Let F be a number field, and let us consider an abelian variety A/F. Let $\mathfrak{p}$ be a prime ideal of the ring of integers $\mathcal{O}_F$ of F. We begin by recalling what it means for A to have semistable reduction at $\mathfrak{p}$ (see [13], § A.9.4.).

Definition 2.1. We will say that A/F has *semistable reduction* at a prime $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_F$ if the connected component of the special fibre of the Néron model of A at $\mathfrak{p}$, $\mathcal{A}^0_{\mathfrak{p}}$, is the extension of an abelian variety by a torus.

The kind of reduction of an abelian variety at a prime $\mathfrak{p}$ is reflected in the action of the inertia group at $\mathfrak{p}$ on the Tate module of the variety. For instance, if the variety has good reduction, the Néron-Ogg-Shafarevich criterion ensures that the inertia group acts trivially on the Tate module. Moreover, a result of Grothendieck characterizes the case when the reduction is semistable in terms of the action of the inertia group. As a consequence, we have the following result.

Theorem 2.2. *Let $A/\mathbb{Q}$ be an abelian variety, and let ℓ, p be two different prime numbers. Assume that A has semistable reduction at p. Then the image of the wild inertia group $I_{p,\mathrm{w}}$ by the Galois representation ρ_ℓ is trivial.*

Proof. Let us see that $I_{p,\mathrm{w}}$ acts trivially on $T_\ell(A)$. By Proposition 3.5 of [12], we know that there exists a submodule $T' \subset T_\ell(A)$, fixed by the action of I_p, and such that I_p acts trivially on both T' and $T_\ell(A)/T'$. Taking a suitable basis of $T_\ell(A)$, I_p acts through a matrix of the shape $\begin{pmatrix} \mathrm{Id}_r & * \\ 0 & \mathrm{Id}_s \end{pmatrix}$.

But the order of such a matrix is a divisor of ℓ. Since $I_{p,\mathrm{w}}$ is a pro-p-group, its elements all act as the identity. $\square$

To control the image of the wild inertia group at the prime ℓ is a much more subtle matter. The first author addresses this problem in [3], and obtains a condition that guarantees that the action is trivial (Theorem 3.3). Let us recall the statement here.

Theorem 2.3. *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.

This result will allow us to hold in check the action of the wild inertia group at ℓ.

3 Image of the Representation

In the previous section we considered the tameness condition. Our aim in this section is to obtain some control on the image of the representation.

Let us fix a prime ℓ, let $A/\mathbb{Q}$ be an abelian variety of dimension n, and let us denote by $\rho_\ell : G_\mathbb{Q} \to \mathrm{GL}_{2n}(\mathbb{F}_\ell)$ the Galois representation attached to the ℓ-torsion points of A. Assume A is principally polarized. Then the Weil pairing gives rise to a non-degenerated symplectic form on the group of ℓ-torsion points of A, $\langle \cdot, \cdot \rangle : A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*$. Furthermore, the elements of the Galois group $G_\mathbb{Q}$ behave well with respect to this pairing. This compels the image of the representation to be contained in the general symplectic group $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$.

Now a well-known result of Serre states that, if the principally polarized abelian variety has the endomorphism ring equal to $\mathbb{Z}$, and furthermore its dimension is either odd or equal to 2 or 6, then the image of the representation ρ_ℓ is the whole general symplectic group for all but finitely many primes ℓ (see Theorem 3 of 137 in [34]).

We are particularly interested in the case of abelian surfaces over $\mathbb{Q}$. In this case, the result of Serre boils down to:

Theorem 3.1. *Let $A/\mathbb{Q}$ be an abelian surface, principally polarized, such that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then, for all but finitely many primes ℓ, it holds that*

$$\mathrm{Im}\rho_\ell = \mathrm{GSp}_4(\mathbb{F}_\ell).$$

We will take the explicit results of P. Le Duff [18] as our starting point. We will sketch some of his reasoning in order to make use of it later on, and then we will dwell upon some specific points where we need to modify it.

The method of Le Duff rests upon finding a certain set of elements in the image of the representation which generate the whole $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Therefore, at the core of the method lies a theorem about generators of this group. More specifically, the main result upon which Le Duff builds his method is the following (see Theorem 2.7 of [18]):

Proposition 3.2. *The symplectic group $\mathrm{Sp}_4(\mathbb{F}_\ell)$ is generated by a transvection and an element whose characteristic polynomial is irreducible.*

It is easy to see that, if the image of the Galois representation contains the subgroup $\mathrm{Sp}_4(\mathbb{F}_\ell)$, then it necessarily contains the whole group $\mathrm{GSp}_4(\mathbb{F}_\ell)$, since the composition of the representation with the projection

$\mathrm{GSp}_4(\mathbb{F}_\ell) \to \mathrm{GSp}_4(\mathbb{F}_\ell)/\mathrm{Sp}_4(\mathbb{F}_\ell)$ equals the cyclotomic character, which is surjective. Therefore, the problem boils down to finding two elements in $\mathrm{Im}\rho_\ell$, satisfying that one is a transvection and that the other has an irreducible characteristic polynomial.

This is the way we approached the matter at first, but in order to produce an element with irreducible characteristic polynomial in $\mathrm{Im}\rho_\ell$ we needed to make use of a conjecture of Hardy and Littlewood (namely Conjecture (F) of [14]). Following a suggestion by L. Dieulefait we have managed to devise a way to ensure a large image without resorting to this conjecture.

Let us consider the following result (Theorem 2.2 of [18]).

Theorem 3.3. *Let G be a proper subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and assume that G contains a transvection. Then one of the following three assertions holds.*

(1) G stabilizes a hyperplane and a line belonging to it.

(2) G stabilizes a totally isotropic plane.

(3) The elements of G stabilize or exchange two orthogonal supplementary non-totally isotropic planes.

Remark 3.4. If G is a subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ which contains an element with irreducible characteristic polynomial, it cannot satisfy any of the three assertions of the theorem (see Theorem 2.7 of [18]). Therefore Proposition 3.2 is an easy consequence of this result.

Our strategy will be the following: for each of the three assertions, we shall ensure the existence of an element of $G = \mathrm{Im}\rho_\ell$, contained in $\mathrm{Sp}_4(\mathbb{F}_\ell)$, which does not satisfy it. In this way, we will prove that G cannot be a proper subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Instead of asking directly that there exists an element with irreducible characteristic polynomial, which rules out the three possibilities at once, we will require that there are elements such that the corresponding characteristic polynomial decomposes in different ways.

Remark 3.5. The second assertion in the above theorem occurs when G is contained in a maximal parabolic subgroup. In this case, it is easy to check that, choosing a suitable symplectic basis, this maximal subgroup consists of matrices of the form $\begin{pmatrix} A & * \\ 0 & (A^{-1})^t \end{pmatrix}$, where $(A^{-1})^t$ denotes the transpose of the inverse matrix of A (cf. the remark following the proof of Theorem 2.2

in [18]). On the other hand, if the third assertion holds, then the elements of G leave two supplementary orthogonal non-totally isotropic planes stable, or else interchange them (this is case (3) of Proposition 2 of [15]). If an element of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ interchanges two such planes, then it can be seen that its trace is zero. Therefore an element which belongs to this kind of maximal subgroup either has trace 0 or stabilizes two planes. Moreover, if it stabilizes two planes, it can be expressed as $\begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$ with respect to some suitable basis, where A and B belong to $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Let us consider an element in $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and call its characteristic polynomial $P(X)$. It is easy to see that this polynomial can be written as $P(X) = X^4 + aX^3 + bX^2 + aX + 1$ for some $a, b \in \mathbb{F}_\ell$. In turn, this implies that there exist $\alpha, \beta \in \overline{\mathbb{F}}_\ell$ such that $P(X)$ decomposes as $(X-\alpha)(X-\beta)(X-1/\alpha)(X-1/\beta)$ over $\overline{\mathbb{F}}_\ell$ (for $P(\alpha) = 0$ implies that $P(1/\alpha) = 0$).

Now there are essentially two ways in which such a polynomial can break up in quadratic factors, namely

$$P(X) = \begin{cases} \Big((X-\alpha)(X-1/\alpha)\Big) \cdot \Big((X-\beta)(X-1/\beta)\Big) \\ \Big((X-\alpha)(X-\beta)\Big) \cdot \Big((X-1/\alpha)(X-1/\beta)\Big). \end{cases}$$

The first case is labelled *"unrelated" 2-dimensional constituents* and the second one *"related" 2-dimensional constituents* in [9].

There is a nice way to discern whether the first decomposition takes place. Namely, consider the polynomial $P_0(X) = X^2 + aX + (b-2)$. The roots of this polynomial are precisely $\alpha + 1/\alpha, \beta + 1/\beta$. Therefore, if the first factorization occurs, this polynomial is reducible and its discriminant $\Delta_0 = a^2 - 4b + 8$ is a square in $\mathbb{F}_\ell$. To determine whether the other factorization takes place is more difficult. Given an element of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ with characteristic polynomial $P(X) = X^4 + aX^3 + bX^2 + aX + 1$, we will denote $\Delta_0(P) = a^2 - 4b + 8$.

Theorem 3.6. *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, $P_1(X)$ and $P_2(X)$, satisfy the following: denoting by $\alpha_i, 1/\alpha_i, \beta_i, 1/\beta_i$ the four roots of $P_i(X)$, $i = 1, 2$,*

- $\alpha_1 + 1/\alpha_1, \beta_1 + 1/\beta_1 \notin \mathbb{F}_\ell$ *and* $\alpha_1 + 1/\alpha_1 + \beta_1 + 1/\beta_1 \neq 0$.
- $\alpha_2 + 1/\alpha_2, \beta_2 + 1/\beta_2 \in \mathbb{F}_\ell$, $\Delta_0(P_2) \neq 0$ *and* $\alpha_2 \notin \mathbb{F}_\ell$.

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

Proof. Since G contains a transvection, Theorem 3.3 implies that either G is the whole symplectic group or else one of the assertions (1), (2) or (3) of the theorem holds. We will see that, in fact, none of them is satisfied.

If assertion (1) holds, then all the elements of G must leave a line invariant. But this implies that each element has one eigenvalue which belongs to $\mathbb{F}_\ell$. But $\alpha_1 + 1/\alpha_1$ and $\beta_1 + 1/\beta_1$ do not belong to $\mathbb{F}_\ell$. Therefore assertion (1) does not hold.

Assume now that assertion (2) holds. Then G is contained in a group which stabilizes a totally isotropic plane. Therefore, with respect to a suitable symplectic basis, it is contained in a subgroup of the shape $\begin{pmatrix} A & * \\ 0 & (A^{-1})^t \end{pmatrix}$ (see Remark 3.5). In particular, this implies that if $P(X)$ is the characteristic polynomial of an element of G, it must factor over $\mathbb{F}_\ell$ into two polynomials of degree two. Call the roots of one of the factors α and β. Then the roots of the other factor are $1/\alpha$ and $1/\beta$.

Let us consider the polynomial $P_2(X) = (x-\alpha_2)(x-\beta_2)(x-1/\alpha_2)(x-1/\beta_2)$. Labelling the roots anew if necessary, we can assume that α_2 and β_2 are the roots of one of the quadratic factors, as above. We can consider two cases:

- $\beta_2 = 1/\alpha_2$ or $\beta_2 = \alpha_2$. In this case $P(X)$ can be factored as $P(X) = (X^2 - AX + 1)^2$ for a certain $A \in \mathbb{F}_\ell$. If we work out this expression, we obtain $P(X) = X^4 + 2AX^3 + (A^2+2)X^2 + 2AX + 1$. Writing out $P(X) = X^4 + a_2X^3 + b_2X^2 + a_2X + 1$ and comparing these two expressions we obtain that $\Delta_0(P_2) = 0$, which contradicts our hypotheses on $P_2(X)$.

- $\beta_2 \neq \alpha_2, 1/\alpha_2$. In this case, the polynomials $(X-\alpha_2)(X-1/\alpha_2)$ and $(X-\alpha_2)(X-\beta_2)$ are different, and both are defined over $\mathbb{F}_\ell$. Therefore, one can use the Euclid algorithm to compute their greatest common divisor $(X-\alpha_2)$. This implies that $\alpha_2 \in \mathbb{F}_\ell$, which contradicts our hypotheses on $P_2(X)$.

Finally, assume that Assertion (3) holds. Then any element in G satisfies that either its trace is zero or it stabilizes two planes, which are supplementary, orthogonal and are not totally isotropic (see Remark 3.5). Consider again the element with characteristic polynomial $P_1(X)$. Since it has non-zero trace, it must stabilize two such planes. But then $P_1(X)$ should break into two quadratic factors defined over $\mathbb{F}_\ell$. Moreover, since the determinant of the corresponding matrix is 1 for each of the factors (cf. Remark 3.5), their independent terms must be 1. But this means that the factors have to be $(X-\alpha_1)(X-1/\alpha_1)$ and $(X-\beta_1)(X-1/\beta_1)$, and we know these polynomials are not defined over $\mathbb{F}_\ell$. Therefore Assertion (3) cannot hold. $\square$

4 Explicit Construction

In this section we will face the problem of constructing explicitly, for a given prime number ℓ, a genus 2 curve such that the Jacobian variety attached to it gives rise to a Galois representation yielding a finite Galois extension $K/\mathbb{Q}$, tamely ramified, with Galois group $\mathrm{GSp}_4(\mathbb{F}_\ell)$, thus providing an affirmative answer to the Tame Inverse Galois Problem for this group. In the preceding sections we have worked out some statements that give very accurate and explicit conditions for the Galois representation attached to the ℓ-torsion points of an abelian surface to satisfy the desired properties. Our aim in this section is to replace all these conditions by others, which are more restrictive, but are simply congruences modulo powers of different primes. We shall tackle each of the conditions separately; thus the section will be split in several different subsections. In the last section we shall state a theorem possessing a very explicit flavour.

4.1 Explicit control of the ramification

Assume we have a hyperelliptic curve C of genus g defined over a certain field k by an equation of the shape $y^2 + Q(x) \cdot y = P(x)$, where $P(X)$ has degree $2g+2$. The *discriminant* of this equation is defined as

$$\Delta = 2^{-4(g+1)} \cdot \mathrm{disc}(4P(x) + Q(x)^2).$$

It holds that if $\Delta \neq 0$, the curve C is smooth (see [20], § 2).

In fact, if we fix a prime p, the p-adic valuation of the discriminant is a bound of the conductor exponent of C, which in turn coincides with the conductor exponent of the Jacobian variety attached to C.

Consider the genus 2 curve defined over $\mathbb{Q}$ by the hyperelliptic equation

$$y^2 = x^6 + 1.$$

The discriminant of this equation is $\Delta = -2^6 \cdot 3^6$. Therefore, $\Delta \not\equiv 0 \pmod p$, for $p \neq 2, 3$. Now, if we have a genus 2 curve C defined by a hyperelliptic equation

$$y^2 = f(x), \tag{1}$$

where $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree 6 such that $f(x) \equiv x^6 + 1$ modulo a prime $p > 3$, then the prime p cannot divide the discriminant of Equation (1), thus C has good reduction at p. In this way, we obtain a condition that we can ask a curve to satisfy if we want it to have good reduction at a given prime $p \neq 2, 3$. For the primes 2 and 3 one has to require other conditions. The following propositions provide these conditions.

Proposition 4.1. *Let C be a genus 2 curve given by the hyperelliptic equation*

$$y^2 = f(x),$$

where $f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ satisfies:

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod 3 \\ f_1 \equiv f_5 \equiv 0 \pmod 3 \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 1 \pmod 3 \\ f_3 \equiv 0 \pmod 3. \end{cases}$$

Then C has good reduction at $p = 3$.

Proof. The hyperelliptic equation $y^2 = x^6 + x^4 + x^2 + 1$ has discriminant $\Delta = -4194304 \equiv 2 \pmod 3$. Because of the congruence conditions on the coefficients $f_0, \ldots, f_6$, it is clear that the discriminant of the hyperelliptic equation defining C is congruent with Δ modulo 3, thus it is not divisible by 3. $\square$

Proposition 4.2. *Let C be a genus 2 curve given by the hyperelliptic equation*

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

where $f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ satisfies that:

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{16} \\ f_1 \equiv f_5 \equiv 0 \pmod{16} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 4 \pmod{16} \\ f_3 \equiv 2 \pmod{16}. \end{cases}$$

Then the Jacobian surface attached to C has either good reduction or semistable reduction at $p = 2$.

Proof. Let us consider the following change of variables

$$\begin{cases} x := x \\ y := x^3 + 2y + 1. \end{cases}$$

Applying it to Equation (2), we obtain an equation with integer coefficients, which are congruent to those of $y + x^3y + y^2 = x^4 + x^2$ modulo 4. But the discriminant of this equation (modulo 4) is $\Delta = 2$, therefore it is divisible by 2, and once only. Since the 2-adic valuation of the discriminant bounds the conductor exponent at 2, this ensures that the Jacobian surface attached to C has either good reduction or bad semistable reduction at 2. $\square$

In this way we can construct an abelian surface $J(C)$ with semistable reduction at any finite set of primes $p \neq \ell$. Concerning the prime ℓ, in [3] the author gives a very explicit condition to ensure that the wild inertia group at ℓ acts trivially on the ℓ-torsion points of the Jacobian of a genus 2 curve. We recall this result here.

Theorem 4.3. *Let ℓ be a prime number, let $\overline{a} \in \mathbb{F}_\ell$ such that $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$, and lift it to $a \in \mathbb{Z}$. The equation*

$$y^2 = x^6 + \frac{1-a}{a}x^4 + \frac{1-a}{a}x^2 + 1$$

defines a genus 2 curve such that its Jacobian variety satisfies the hypothesis of Theorem 2.3.

Moreover, in Theorem 6.4 of [3] this result is expanded to cover a larger family of curves.

Theorem 4.4. *Let ℓ be a prime number, let $\overline{a} \in \mathbb{F}_\ell$ such that $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$, and lift it to $a \in \mathbb{Z}$. Let $f_0, f_1, \ldots, f_6 \in \mathbb{Z}$ satisfy*

$$\begin{cases} f_6 \equiv f_0 \pmod{\ell^4} \\ f_5 \equiv f_1 \pmod{\ell^4} \\ f_4 \equiv f_2 \pmod{\ell^4}. \end{cases}$$

Furthermore, assume that

$$\begin{cases} f_6 \equiv 1 \pmod{\ell} \\ f_5 \equiv 0 \pmod{\ell} \end{cases} \quad \begin{cases} f_4 \equiv \frac{1-a}{a} \pmod{\ell} \\ f_3 \equiv 0 \pmod{\ell}. \end{cases}$$

The equation $y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + 1$ defines a genus 2 curve such that its Jacobian variety satisfies the hypothesis of Theorem 2.3.

Remark 4.5. Note that the genus 2 curves from theorem 4.3 have a non-hyperelliptic involution. In fact, their Jacobians are reducible. Therefore, the image of the representations attached to the ℓ-torsion points of these Jacobians cannot be $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The enlargement of the family of curves carried out in Theorem 4.4 is thus essential to our construction.

4.2 Control of the image: the transvection

Our aim in this section is to ensure the existence of a transvection in the image of $G_{\mathbb{Q}}$ by the Galois representation ρ_ℓ attached to the Jacobian of a genus 2 curve. Combining Proposition 1.3 and Lemma 4.1 of [18] we can state the following result:

Proposition 4.6. *Let p be a prime number, let $C/\mathbb{Q}$ be a genus 2 curve and J its Jacobian. Assume that C has stable reduction of type (II) or (VI) at p.*

If $\ell \neq p$ is a prime number such that it does not divide $(\widetilde{J}_v : \widetilde{J}_v^0)$ (which denotes the order of the group of connected components of the special fibre of the Néron model of J at p), then there exists an element in the inertia group I_p such that its image by ρ_ℓ is a transvection.

Recall that if C is a smooth, projective, geometrically connected curve of genus $g \geq 2$ over a number field K, then C has stable reduction at a prime $\mathfrak{p}$ if and only if the Jacobian variety attached to C has semistable reduction at $\mathfrak{p}$ (see [21], Remark 4.26 of chapter 10).

Proposition 4.6 leaves us a great amount of freedom to choose p, and as a matter of fact we will always choose $p = 5$. Of course, this construction will not work for $\ell = 5$, but this is a minor hindrance. We just need a special construction for $\ell = 5$.

We want to build a genus 2 curve, defined over $\mathbb{Q}$, with stable reduction of type (II) at 5. Moreover, we will require that the order of the group of connected components of the special fibre of the Néron model at 5 is 1 (thus ensuring that ℓ does not divide it).

A theorem of Deligne and Mumford tells us that every smooth, geometrically connected, projective curve defined over a local field, say K, acquires stable reduction over a finite extension of K (see [21], Theorem 4.3 of Chapter

10). This stable reduction can belong to one of the following types (I), (II), (III), (IV), (V), (VI), (VII). When the curve has genus 2, Q. Liu has worked out a characterization of the type of (potential) stable reduction in terms of the Igusa invariants (see [19]). We will denote them by $J_2, J_4, J_6, J_8, J_{10}$, and also $I_4 := J_2^2 - 2^3 3 J_4$, $I_{12} := -2^3 J_4^3 + 3^2 J_2 J_4 J_6 - 3^3 J_6^2 - J_2^2 J_8$.

A technical remark should be made at this point. The results of Liu are stated over a local field K with separably closed residual field k. We shall assume, from now on, that our curve C is defined over $\mathbb{Q}_{p,\mathrm{unr}}$ (the maximal unramified extension of $\mathbb{Q}_p$, which satisfies this condition). In this way, what we shall obtain after some reasoning is the existence of a transvection inside the Galois group of the extension $\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{unr}}$, which in fact is the inertia group at p. In the computation of the order of the group of connected components of the special fibre of the Néron model at p, the p-adic valuation in $\mathbb{Q}_{p,\mathrm{unr}}$ shall come into play; but since $\mathbb{Q}_{p,\mathrm{unr}}$ is an unramified extension of $\mathbb{Q}_p$, this valuation shall coincide with the usual valuation in $\mathbb{Q}_p$, without any need to normalize. Therefore, considering $\mathbb{Q}_{p,\mathrm{unr}}$ as the base field will not give rise to any significant modification, and we shall be able to apply the results of Liu without paying any further attention to this point. We will just state the results concerning potential good reduction (that is to say, type (I)) and type (II).

Theorem 4.7. *Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and quotient field K. Let C/K be a smooth geometrically connected projective curve of genus 2, defined by the equation $y^2 = f(x)$, where $f(x)$ is a degree 6 polynomial. Denote by $J_2, \ldots, J_{10}$ the Igusa invariants of $f(x)$, and denote by $\mathcal{C}_{\overline{s}}$ the geometric special fibre of a stable model of C over some finite extension of K. Then it holds:*

- *$\mathcal{C}_{\overline{s}}$ is smooth if and only if $J_{2i}^5 J_{10}^{-i} \in R$ for all $i \leq 5$.*
- *$\mathcal{C}_{\overline{s}}$ is irreducible with a unique double point if and only if $J_{2i}^6 I_{12}^{-i} \in R$ for all $i \leq 5$ and $J_{10}^6 I_{12}^{-5} \in \mathfrak{m}$. If this is the case, the group Φ of connected components of the Néron model at v is isomorphic to $\mathbb{Z}/e\mathbb{Z}$, where $e = \frac{1}{6} v(J_{10}^6 J_{12}^{-5})$.*

Remark 4.8. In the first case in the theorem above, the curve C is said to have *potential good reduction*, and in the second case *potential stable good reduction of type (II)*.

Let us now turn our attention to a simple example:

Example 4.9. Let us consider the curve C defined by the following equation:

$$y^2 = x^6 + x^5 + x^3 + x + 1.$$

By using the Magma Computational Algebra System, we can compute the Igusa invariants of C. We obtain the following results:

$$J_2 = -97/4, J_4 = 1323/128, J_6 = -14515/1024,$$
$$J_8 = 3881491/65536, J_{10} = 6845/256.$$

Recall that the last of the invariants was the discriminant of the equation. Since $J_{10} = 6845/256 = 2^{-8} \cdot 5 \cdot 37^2$, the only two odd primes of bad reduction are 5 and 37. Thus we know that, outside these two primes and possibly 2, the curve has good reduction.

Let us study the type of reduction at 5. Computing $J_{2i}^5 J_{10}^{-i}$, for $i = 1, 2, 3, 4, 5$, we see that, if $p = 5$ (and also if $p = 37$), these numbers do not all belong to $\mathbb{Z}_p$. Therefore, for $p = 5$ (and $p = 37$), the reduction of C at p is not good.

Now we wish to determine if the reduction is of type (II). We have to compute $J_{2i}^6 I_{12}^{-i}$ for $i = 1, 2, 3, 4, 5$. We begin with I_{12};

$$I_{12} = -\frac{1095163}{64} = -2^{-6} \cdot 37 \cdot 29599.$$

Note that $p = 5$ divides the discriminant of the equation, but it does not divide I_{12}. And this is enough to ensure that the reduction at $p = 5$ is (potentially) stable of type (II). Moreover, since $p = 5$ divides the discriminant of the equation just once, the reduction is indeed stable. And it turns out that $v_5(J_{10}^6 I_{12}^{-5}) = 6$, which means that the order of the group of connected components of the special fibre of the Néron model at $p = 5$ is 1.

Now we will take advantage of this example to state a general result:

Theorem 4.10. *Let C be a genus 2 curve defined over $\mathbb{Q}$ by the equation $y^2 = f(x)$, where $f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ is a polynomial of degree 6 without multiple roots, satisfying that*

$$\begin{cases} f_6 \equiv f_5 \equiv f_3 \equiv f_1 \equiv f_0 \equiv 1 \mod 25 \\ f_4 \equiv f_2 \equiv 0 \mod 25. \end{cases}$$

Then C has stable reduction at 5, and this reduction is of type (II). The order of the group of connected components of the special fibre of the Néron model at $p = 5$ is 1.

Proof. Due to the congruence condition above, the discriminant of the equation $y^2 = f(x)$ is congruent to the discriminant of the equation $y^2 = x^6+x^5+x^3+x+1$ modulo 25, that is to say, it is congruent to $28037120 \equiv 20 \mod 25$. Therefore $p = 5$ divides the discriminant of our equation once and only once, thus ensuring that the curve C has stable reduction. Let us see what type of reduction it has. Since the invariant I_{12} of the polynomial $x^6+x^5+x^3+x+1$ is not divisible by 5, the same holds for the invariant I_{12} of $f(x)$ (for both are congruent to each other modulo 25). Consequently, since the invariants J_{2i} belong to $\mathbb{Z}_5$ (the only denominators which can appear are the powers of 2), $J_{12}^{2i} I_{12}^{-i} \in \mathbb{Z}_5$. And finally, since 5 does divide the discriminant of $f(x)$, that is to say, J_{12}, it is clear that $J_{12}^{10} I_{12}^{-5}$ belongs to the maximal ideal of $\mathbb{Z}_5$. Theorem 4.7 implies that the reduction is of type (II).

□

4.3 Control of the image: characteristic polynomials

Let us now deal with the existence of elements in $\mathrm{Im}\rho_\ell$ with particular characteristic polynomials. The candidate elements we are going to look at are the images of the Frobenius elements at primes different from ℓ, where C has good reduction, since we have a great deal of information about their shape.

Namely, let $q \neq \ell$ be a prime number, and assume that $J(C)$ has good reduction at q. Inside $G_\mathbb{Q}$ we can consider the decomposition group at q, which is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Different immersions of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ into $G_\mathbb{Q}$ give rise to conjugate subgroups. Consider the Frobenius morphism $x \mapsto x^q$ in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. There are many liftings of this element to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Since C has good reduction at q, the image by ρ_ℓ of any two lifts of the Frobenius must coincide, and thus an element in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is determined save conjugacy. In any case, the characteristic polynomial of an element in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is not altered by conjugation, so this polynomial is well defined, independently of any choices we may make along the way. What does this polynomial look like?

Let us consider the Frobenius endomorphism ϕ_q acting on the reduction $\widetilde{C}$ of C at q. It is well known (see for instance [7], § 14.1.6, Theorem 14.16) that the characteristic polynomial of ϕ_q has the following shape:

$$P(X) = X^4 + aX^3 + bX^2 + aqX + q^2,$$

for certain $a, b \in \mathbb{Z}$. More precisely, if we denote by N_1 (resp. N_2) the number of points of C over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$), we can compute a and b by using the formulae

$$\begin{cases} a := N_1 - q - 1 \\ b := (N_2 - q^2 - 1 + a^2)/2. \end{cases} \tag{3}$$

Furthermore, it can be proven (cf. Proposition 10.20 in [24]) that the polynomial obtained from $P(X)$ by reducing its coefficients modulo ℓ coincides with the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_q)$.

In the previous section our problem was to construct a curve such that, at a certain well chosen prime p, it satisfied some condition. Our strategy there was to choose the prime p once and for all at the beginning; namely, we took $p = 5$, and we established a congruence condition modulo 5^2 such that, whenever it is satisfied by a genus 2 curve C, we achieve our objective. The first point in which this section differs from the previous one is that now we will not choose the primes q_1 and q_2 beforehand; the primes q_1 and q_2 will actually depend on ℓ.

When we face this problem, a natural question arises: Given a prime q, what conditions must a pair (a, b) satisfy in order to ensure that the polynomial $P(X) = X^4 + aX^3 + bX^2 + qaX + q^2$ is the characteristic polynomial of the Frobenius endomorphism at q of a genus 2 curve?

In [22], the authors address the problem of determining whether, given finite field $\mathbb{F}_q$ and a pair of positive natural numbers (N_1, N_2), there exists a genus 2 curve C with N_1 points over $\mathbb{F}_q$ and N_2 points over $\mathbb{F}_{q^2}$. We shall make use of their results.

Firstly, let us recall the definition of a Weil polynomial (see Definition 2.2 of [22]).

Definition 4.11. Let q be a power of a prime number. We will say that the polynomial $P(X) = X^4 + aX^3 + bX^2 + qaX + q^2 \in \mathbb{Z}[X]$ is a *Weil polynomial* if $|a| \leq 4\sqrt{q}$ and $2|a|\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q$.

Remark 4.12. To simplify the problem, we will always choose $a = 1$, so we will only have to take care to choose b satisfying $2\sqrt{q} - 2q \leq b \leq \frac{1}{4} + 2q$.

Let us fix an odd prime number q. Collecting Theorem 2.15 and Theorem 4.3 of [22], we can state the following result:

Theorem 4.13. *Let $P(X) = X^4 + aX^3 + bX^2 + qaX + q^2 \in \mathbb{Z}[X]$ be a Weil polynomial, and let $\Delta_0 = a^2 - 4b + 8q$. Assume that Δ_0 is not a square in $\mathbb{Z}$, $q \nmid b$ and $a^2 \notin \{0, q + b, 2b, 3(b - q)\}$. Then there exists a smooth projective curve of genus 2, defined over $\mathbb{F}_q$, with $N_1 = q + 1 + a$ points over $\mathbb{F}_q$ and $N_2 = 2b - a^2 + q^2 + 1$ points over $\mathbb{F}_{q^2}$.*

Remark 4.14. The previous result claims the existence of a genus 2 curve, say C, defined over $\mathbb{F}_q$ with N_1 points over $\mathbb{F}_q$ and N_2 points over $\mathbb{F}_{q^2}$. If q is odd, we know that there exists a hyperelliptic equation $y^2 = f(x)$ defining C, with $f(x) \in \mathbb{F}_q[x]$ a polynomial of degree 6 and without multiple roots. Since there is only a finite number of such polynomials $f(x) \in \mathbb{F}_q[x]$, one can compute the curve C simply by an exhaustive search, so one can say that this construction is effective. Nevertheless, there are algorithms to compute genus 2 curves with a given number of points over $\mathbb{F}_q$ and over $\mathbb{F}_{q^2}$. For instance, see [11].

Keeping this result in mind, the following two propositions show us how to construct suitable q_1 and q_2.

Proposition 4.15. *Let ℓ be an odd prime number. Choose q_1 such that $q_1 \equiv 1 \pmod{\ell}$. Then there exists a projective curve of genus 2, $C_1/\mathbb{Q}$, such that it has good reduction at q_1, and the characteristic polynomial of the Frobenius endomorphism at q_1, $P_1(X) = X^4 + a_1X^3 + b_1X^2 + q_1a_1X + q_1^2$ satisfies that $\Delta_0(P_1)$ is not a square in $\mathbb{F}_\ell$ and $a_1 \not\equiv 0 \pmod{\ell}$.*

Proof. Fix $a_1 = 1$. Since $q_1 \equiv 1 \pmod{\ell}$, it follows that $q_1 > \ell$. Therefore, if we choose any element $\overline{b}_1 \in \mathbb{F}_\ell$, there exists $b_1 \in \mathbb{Z}$, $0 < b_1 < q_1$ mapping into $\overline{b}_1$. Therefore $P_1(X) = X^4 + a_1X^3 + b_1X^2 + q_1a_1X + q_1^2$ is a Weil polynomial. We will choose $\overline{b}_1$ such that $1 - 4\overline{b}_1 + 8q_1$ is not a square in $\mathbb{F}_\ell$ (since 4 is prime to ℓ, the expression $1 - 4\overline{b}_1 + 8q_1$ runs through all the elements of $\mathbb{F}_\ell$ as $\overline{b}_1$ varies, so this is clearly feasible).

Now it is easy to check that the pair (a_1, b_1) satisfies all the conditions in Theorem 4.13, so that there exists a smooth projective curve of genus 2 defined over $\mathbb{F}_{q_1}$ with a suitable number of points over $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_1^2}$. Lifting this curve to $\mathbb{Q}$, we obtain the curve we were seeking. □

Proposition 4.16. *Let ℓ be an odd prime number. Choose q_2 such that $q_2 \equiv 1 \pmod{\ell}$ and $q_2 > 3\ell$. Then there exists a projective curve of genus 2, $C_2/\mathbb{Q}$, such that it has good reduction at q_2, and the characteristic polynomial of the Frobenius endomorphism at q_2, $P_2(X) = X^4 + a_2X^3 + b_2X^2 + q_2a_2X + q_2^2$*

satisfies that $\Delta_0(P_2)$ is a non-zero square in $\mathbb{F}_\ell$ but is not a square in $\mathbb{Z}$, and $P_2(X)$ does not break up in linear factors over $\mathbb{F}_\ell$.

Proof. As in the proof of Proposition 4.15, we will fix $a_2 = 1$. Note that, since $q_2 > 3\ell$, for each element $\overline{b}_2 \in \mathbb{F}_\ell$ there exist three values of $b_2 \in \mathbb{Z}, 0 < b_2 < q_2$ such that b_2 maps into $\overline{b}_2$, which can be taken as b_2, $\ell + b_2$, $2\ell + b_2$.

Let us choose an element $z \in \mathbb{F}_\ell$ such that $z^2 - 16q_2$ is not a square in $\mathbb{F}_\ell$. Such an element exists: if we take any square $x^2 \in \mathbb{F}_\ell$, and add $-16q_2$ as many times as we wish, we can obtain any element in $\mathbb{F}_\ell$ that we like. In particular, if we consider the sequence $x^2, x^2 - 16q_2, x^2 - 2\cdot 16q_2, x^2 - 3\cdot 16q_2, \ldots$, a point will come when we obtain a non-square element. The previous element shall be our z^2. If $z^2 = 1$, we will take $z = 1$. Now let us choose $b_2 < q_2$ such that $1 - 4b_2 + 8q_2$ is congruent to $(z+1)^2$ modulo ℓ. This is possible for the same reason as in the proof of Proposition 4.15. Moreover, at the beginning of the proof we noted that there are, in fact, three possible choices for b_2 which are strictly smaller than q_2. It is not difficult to check that for the three of them $1 - 4b_2 + 8q_2$ cannot be a square in $\mathbb{Z}$. We have set this claim aside in Lemma 4.17. Therefore, we can choose b_2 such that $1 - 4b_2 + 8q_2$ is not a square in $\mathbb{Z}$, and furthermore b_2 is not divisible by q_2.

If we choose b_2 in this way, it is easy to check that the conditions of Theorem 4.13 hold. Therefore, there exists a smooth projective genus 2 curve over $\mathbb{F}_{q_2}$ such that the characteristic polynomial of the Frobenius endomorphism of q_2 is $P_2(X) = X^4 + a_2X^3 + b_2X^2 + q_2a_2X + q_2^2$. Now we ascertain that the thesis of our Proposition holds. It is clear that $\Delta_0(P_2) \equiv (z+1)^2 \pmod{\ell}$ is a non-zero square in $\mathbb{F}_\ell$. It remains to show that $P_2(X)$ does not split into linear factors. Call $\alpha_2, q_2/\alpha_2, \beta_2, q_2/\beta_2$ the roots of $P_2(X)$. The fact that $\Delta_0(P_2)$ is a square tells us that the polynomials $(X - \alpha_2)(X - q_2/\alpha_2)$ and $(X - \beta_2)(X - q_2/\beta_2)$ are defined over $\mathbb{F}_\ell$. We will achieve our objective if we see that one of these polynomials is irreducible over $\mathbb{F}_\ell$. Since both $\alpha_2 + q_2/\alpha_2$ and $\beta_2 + q_2/\beta_2$ are roots of $P_0(X) = X^2 + a_2X + b_2 - (b_2 - 2q_2)$, they are given by the expressions $\frac{-a_2 \pm \sqrt{a_2^2 - 4(b_2 - 2q_2)}}{2}$. Interchanging α_2 and β_2 if necessary, we can assume that $\alpha_2 + q_2/\alpha_2 = \frac{-a_2 + \sqrt{a_2^2 - 4(b_2 - 2q_2)}}{2}$. Therefore the polynomial $(X - \alpha_2)(X - q_2/\alpha_2)$ can be written as $X^2 - \frac{-a_2 + \sqrt{a_2^2 - 4(b_2 - 2q_2)}}{2}X + q_2$, and its discriminant is

$$\Delta = \left(\frac{-a_2 + \sqrt{a_2^2 - 4(b_2 - 2q_2)}}{2} \right)^2 - 4q_2.$$

Let us compute this quantity modulo ℓ. Since $a_2 = 1$, $\Delta_0 = 1-4b_2+8q_2 \equiv (z+1)^2$, we obtain that $\Delta \equiv \frac{z-16q_2}{4} \pmod{\ell}$, which is not a square in $\mathbb{F}_\ell$ because of the choice of z. This proves that $P_2(X)$ does not decompose in linear factors over $\mathbb{F}_\ell$.

□

Lemma 4.17. *Let A be a natural number, and let ℓ be a prime. Then the three numbers A, $A-4\ell$, $A-8\ell$ cannot be squares in $\mathbb{Z}$.*

Proof. Assume that there exist x, y, z positive integers such that $A = x^2$, $A - 4\ell = y^2$ and $A - 8\ell = z^2$. From the first two equations we obtain that $4\ell = x^2 - y^2 = (x+y)(x-y)$. Therefore $\ell = \frac{x+y}{2} \cdot \frac{x-y}{2}$. Since ℓ is a prime number, it follows that $x - y = 2$, and moreover $\ell = \frac{(y+2)+y}{2} \cdot \frac{(y+2)-y}{2} = y+1$. The same reasoning applied to the last two equations yields that $y - z = 2$, and we can write $\ell = \frac{y+z}{2} \cdot \frac{y-z}{2} = \frac{(z+2)+z}{2} \cdot \frac{(z+2)-z}{2} = z+1$. This is clearly a contradiction. □

5 Main Result

In this section we will state the main result concerning tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Our starting point is the following straightforward statement:

> Let C be a smooth projective curve of genus 2, defined over $\mathbb{Q}$ and such that, if we denote by J the Jacobian variety attached to C and by ρ_ℓ the Galois representation attached to the ℓ-torsion points of J, the following conditions are satisfied:
>
> - The Galois extension obtained by adjoining to $\mathbb{Q}$ the coordinates of the ℓ-torsion points of J is tamely ramified.
> - The image of ρ_ℓ coincides with the general symplectic group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.
>
> Then ρ_ℓ provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Throughout this paper, we have sought to remodel these conditions in order to make them look like congruences. We have succeeded to a great extent. Replacing these conditions with those (more restrictive but simpler) obtained in the previous sections, we obtain the following result:

Theorem 5.1. *Let C be a genus 2 curve defined by a hyperelliptic equation*

$$y^2 = f(x),$$

where $f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ is a polynomial of degree 6 without multiple factors. Let $\ell \geq 7$ be a prime number, and let $\mathcal{P}$ be the set of prime numbers that divide the order of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Let $a \in \mathbb{F}_\ell$ be such that the elliptic curve defined by $y^2 = x^3 + (1-a)/ax^2 + (1-a)/ax + 1$ is supersingular. Furthermore, let $q_1, q_2 \equiv 1 \pmod{\ell}$ be different prime numbers with $q_2 > 3\ell$. Let $C_1/\mathbb{Q}$ be a genus 2 curve such that it has good reduction at q_1, and the characteristic polynomial of the Frobenius endomorphism at q_1, $P_1(X) = X^4 + a_1X^3 + b_1X^2 + q_1a_1X + q_1^2$ satisfies that $\Delta_0(P_1)$ is not a square in $\mathbb{F}_\ell$ and $a_1 \not\equiv 0 \pmod{\ell}$. Let $C_2/\mathbb{Q}$ be a genus 2 curve such that it has good reduction at q_2, and the characteristic polynomial of the Frobenius endomorphism at q_2, $P_2(X) = X^4 + a_2X^3 + b_2X^2 + q_2a_2X + q_2^2$ satisfies that $\Delta_0(P_2)$ is a non-zero square in $\mathbb{F}_\ell$ but is not a square in $\mathbb{Z}$, and $P_2(X)$ does not break up in linear factors over $\mathbb{F}_\ell$. Consider hyperelliptic equations $y^2 = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$ and $y^2 = d_6x^6 + d_5x^5 + d_4x^4 + d_3x^3 + d_2x^2 + d_1x + d_0$ defining C_1 and C_2.

Assume that the following conditions hold:

- *The following congruences mod 2^4 hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{16} \\ f_1 \equiv f_5 \equiv 0 \pmod{16} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 4 \pmod{16} \\ f_3 \equiv 2 \pmod{16}. \end{cases}$$

- *The following congruences mod 3 hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{3} \\ f_1 \equiv f_5 \equiv 0 \pmod{3} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 1 \pmod{3} \\ f_3 \equiv 0 \pmod{3}. \end{cases}$$

- *The following congruences mod 5^2 hold:*

$$\begin{cases} f_6 \equiv f_5 \equiv f_3 \equiv f_1 \equiv f_0 \equiv 1 \mod 25 \\ f_4 \equiv f_2 \equiv 0 \mod 25. \end{cases}$$

- *The following congruences mod ℓ^4 hold:*

$$\begin{cases} f_6 \equiv f_0 \pmod{\ell^4} \\ f_5 \equiv f_1 \pmod{\ell^4} \\ f_4 \equiv f_2 \pmod{\ell^4}. \end{cases}$$

Furthermore,

$$\begin{cases} f_6 \equiv 1 \pmod{\ell} \\ f_5 \equiv 0 \pmod{\ell} \end{cases} \quad \begin{cases} f_4 \equiv (1-a)/a \pmod{\ell} \\ f_3 \equiv 0 \pmod{\ell}. \end{cases}$$

- *The following congruences mod q_1 hold:*

$$f_i \equiv c_i \pmod{q_1}, i = 0, 1, \ldots, 6.$$

- *The following congruences mod q_2 hold:*

$$f_i \equiv d_i \pmod{q_2}, i = 0, 1, \ldots, 6.$$

- *For all $p \in \mathcal{P}$ different from 2, 3, 5, q_1, q_2 and ℓ, the following congruences hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{p} \\ f_1 \equiv f_5 \equiv 0 \pmod{p} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 0 \pmod{p} \\ f_3 \equiv 0 \pmod{p}. \end{cases}$$

Then the Galois representation attached to the ℓ-torsion points of the Jacobian of C provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Proof. The existence of $a \in \mathbb{F}_\ell$ follows from Theorem 1-(b) of [6] (cf. Corollary 3.6 of [2]), and the existence of the genus two curves C_1 and C_2 is proved in Propositions 4.15 and 4.16. The result is a direct consequence of the considerations made in the previous sections. □

A quick look at this theorem shows that, for each prime number $\ell \geq 7$, there exists a genus 2 curve C satisfying all the hypotheses, simply because of the Chinese Remainder Theorem. Therefore, we may write the following corollary:

Corollary 5.2. *For each prime number $\ell \geq 7$, there exists a Galois extension over $\mathbb{Q}$ which is tamely ramified and has Galois group* $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Remark 5.3. As we remarked at the beginning of Section 4.2, we excluded the prime $\ell = 5$ just in order to write a neat statement for all $\ell \neq 5$. Let us now tackle the case $\ell = 5$. Consider the hyperelliptic curve C defined over $\mathbb{Q}$ by the equation

$$y^2 = x^6 + 391300x^4 + 1170x^3 + 1300x^2 + 1. \tag{4}$$

To simplify the notation, call $f_6 = 1$, $f_5 = 0$, $f_4 = 391300$, $f_3 = 1170$, $f_2 = 1300$, $f_1 = 0$, $f_0 = 1$.

We can compute the reduction data of this particular curve by means of the algorithm of Liu (which is implemented in SAGE). We obtain that this curve has good reduction outside (possibly) the primes 2, 27792683 and 195476205803858674906021. In any case, at the last two primes the conductor exponent is 1. Therefore the curve has stable reduction at all odd primes. The algorithm of Liu does not compute the conductor at the prime 2. Nevertheless, in this case it is easy to check that the coefficients f_i of the equation defining the curve satisfy that

$$\begin{cases} f_6 \equiv f_0 \equiv 1 \pmod{16} \\ f_5 \equiv f_1 \equiv 0 \pmod{16} \end{cases} \quad \begin{cases} f_4 \equiv f_2 \equiv 4 \pmod{16} \\ f_3 \equiv 2 \pmod{16}. \end{cases}$$

Therefore, Proposition 4.2 ensures that the reduction of C at 2 is also stable. As a conclusion, we can say that the Galois representation attached to the 5-torsion points of the Jacobian surface of C is tamely ramified outside the prime $\ell = 5$.

On the other hand, note that the equation defining C is congruent modulo 5^4 with the supersingular symmetric equation $y^2 = x^6 + 1300x^4 + 1170x^3 + 1300x^2 + 1$. This guarantees that the wild inertia group at 5 acts trivially on the group of 5-torsion points.

Let us denote by $\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{F}_5)$ the Galois representation which arises from the action of the Galois group on the points of 5-torsion of the Jacobian variety attached to C.

The computation of the reduction data of C at the prime $p = 27792683$ shows that the stable reduction at p is of type (II). Therefore, this prime satisfies the hypothesis of Proposition 4.6. Furthermore the order of the group of connected components of the special fibre of the Néron model at p is 1, so it is not divisible by 5. This ensures the existence of a transvection in the group $\mathrm{Im}\rho_\ell \subset \mathrm{GSp}_4(\mathbb{F}_\ell)$. In order to prove that the image of the Galois representation is $\mathrm{GSp}_4(\mathbb{F}_\ell)$, we will make use of Proposition 3.2.

For instance, let us consider the prime $q = 19$. The number of points of C over $\mathbb{F}_{19}$ is 22, and the number of points of C over $\mathbb{F}_{19^2}$ is 410. Therefore, Equations (3) allow us to compute the characteristic polynomial of the Frobenius endomorphism at q, namely $P(X) = X^4 + 2X^3 + 26X^2 + 38X + 361$. It is not difficult to ascertain that this polynomial is irreducible over $\mathbb{F}_5$. Therefore, we conclude that the image of ρ_5 is $\mathrm{GSp}_4(\mathbb{F}_5)$. Thus this group can also be realized as the Galois group over $\mathbb{Q}$ of a tamely ramified extension.

The previous remark allows us to state Corollary 5.2 without excluding the prime $\ell = 5$:

Corollary 5.4. *For each prime number $\ell \geq 5$, there exists a Galois extension over $\mathbb{Q}$ which is tamely ramified and has Galois group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.*

As a matter of fact, we have proven not just the existence of a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, but of infinitely many of them.

Theorem 5.5. *For each prime number $\ell \geq 5$, there exist infinitely many tamely ramified Galois extensions over $\mathbb{Q}$ with Galois group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.*

Proof. If $\ell \geq 7$, this is clear from the statement of Theorem 5.1. If $\ell = 5$, note that the cardinal of $\mathrm{GSp}_4(\mathbb{F}_5)$ equals $37440000 = 2^9 \cdot 3^2 \cdot 5^4 \cdot 13$. Therefore, each curve C given by a hyperelliptic equation congruent to (4) modulo a suitable power of the primes $2, 3, 5, 13, 27792683$ will provide a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_5)$. $\square$

Remark 5.6. The symplectic group $\mathrm{GSp}_4(\mathbb{F}_2)$ is isomorphic to the symmetric group S_6, thus it is already known to be realizable as the Galois group of a tamely ramified extension of $\mathbb{Q}$ (cf. Proposition 1 in [29]). If $\ell = 3$, we hope that a tame Galois realization of $\mathrm{GSp}_4(\mathbb{F}_3)$ can also be obtained by using different techniques. For instance, one could make use of the isomorphism $\mathrm{Sp}_4(\mathbb{F}_3) \simeq U(4, 2)$ to obtain a regular realization of this group (cf. [23]), and then apply the techniques in [27].

6 Example

In this section we will present an example to illustrate how Theorem 5.1 allows us to compute explicitly genus 2 curves providing tame Galois realizations of the group $\mathrm{GSp}_4(\mathbb{F}_\ell)$. In fact, Theorem 5.1 can easily be turned into an algorithm to compute these genus 2 curves. Even though we have not explicitly formulated it in this way, we hope this example will clarify how the algorithm works.

Firstly, note the simple well-known result:

Lemma 6.1. *Let q be a prime number. Then*

$$\operatorname{card}(\mathrm{GSp}_{2n}(\mathbb{F}_q)) = (q-1)q^{\frac{(2n)^2}{4}} \prod_{j=1}^{n}(q^{2j}-1).$$

Let us take $\ell = 7$. We will compute all the elements that appear in the statement of Theorem 5.1.

- First of all, let us compute the set $\mathcal{P}$ of prime numbers which divide the order of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Since $\ell = 7$ and $n = 2$, Lemma 6.1 yields that $\operatorname{card}(\mathrm{GSp}_4(\mathbb{F}_\ell)) = 1659571200 = 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^4$. Therefore, the set of primes that divide the order of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is $\mathcal{P} = \{2, 3, 5, 7\}$.

- Next, we need to compute the element $a \in \mathbb{F}_7$ such that the equation $y^2 = x^3 + (1-a)/ax^2 + (1-a)/ax + 1$ defines a supersingular elliptic curve. In order to do this, we compute the Deuring polynomial

$$H_7(x) = \sum_{j=0}^{3} \binom{3}{j}^2 \cdot x^j = x^3 + 2x^2 + 2x + 1 = (x+1)(x+3)(x+5).$$

  Therefore, $x^2 - x + 5 = (x+1)(x+5)$ divides the Deuring polynomial, so we can take $a = 5$ in $\mathbb{F}_7$.

- The following elements that emerge are the primes q_1 and q_2. We must choose two different prime numbers, q_1 and q_2, which are congruent to 1 modulo 7 and such that $q_2 > 3 \cdot 7 = 21$. We may take $q_1 = 29$, $q_2 = 43$. Now we must find the genus 2 curves C_1 and C_2.

  - Choosing the curve C_1: firstly, fix $a_1 = 1$. According to Proposition 4.15, we need to find b_1 such that $1 - 4 \cdot b_1 + 8 \cdot 29$ is not a square modulo ℓ. For instance, we can take $b_1 = 1$. Now that we have a pair (a_1, b_1), we seek a genus 2 curve over $\mathbb{F}_{29}$ with $N_1 = 29 + 1 + a_1 = 31$ points over $\mathbb{F}_{29}$ and $N_2 = 29^2 + 1 + 2b_1 - a_1^2 = 843$ points over $\mathbb{F}_{29^2}$. We know that such a curve exists, and if we scrutinize the set of all hyperelliptic curves defined over $\mathbb{F}_{29}$ (which is a finite set), we can obtain the curve given by the hyperelliptic equation $y^2 = x^6 + x^5 + 17x + 5$.

- Choosing the curve C_2: again, fix $a_1 = 1$. According to Proposition 4.16, the first step is to find an element $z \in \mathbb{F}_7$ such that $z^2 - 16 \cdot 43$ is not a square in $\mathbb{F}_7$. For instance, we can consider $z = 1$. Next, we must find b_2 such that $1-4\cdot b_2+8\cdot 43$ is congruent to $(z+1)^2 = 4$ modulo 7. For instance, take $b_2 = 3$. Note that $1-4\cdot 3+8\cdot 43 = 333$ is not a square in $\mathbb{Z}$. We have a pair (a_2, b_2). We must seek a genus 2 curve over $\mathbb{F}_{43}$ with $N_1 = 43+1+a_2 = 45$ points over $\mathbb{F}_{43}$ and $N_2 = 43^2 + 1 + 2b_2 - a_2^2 = 1855$ points over $\mathbb{F}_{43^2}$. Such a curve exists, and again an exhaustive search can provide it. For instance, we have taken the curve defined by the hyperelliptic equation $y^2 = x^6 + x^5 + 3x^2 + 13x + 21$.

Let us now go through Theorem 5.1 replacing the elements that appear there by the ones we have chosen above:

Proposition 6.2. *Let C be a genus 2 curve defined by a hyperelliptic equation*

$$y^2 = f(x),$$

where $f(x) = f_6x^6+f_5x^5+f_4x^4+f_3x^3+f_2x^2+f_1x+f_0 \in \mathbb{Z}[x]$ is a polynomial of degree 6 without multiple factors. Assume that the following conditions hold:

- *The following congruences mod 2^4 hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{16} \\ f_1 \equiv f_5 \equiv 0 \pmod{16} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 4 \pmod{16} \\ f_3 \equiv 2 \pmod{16}. \end{cases}$$

- *The following congruences mod 3 hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{3} \\ f_1 \equiv f_5 \equiv 0 \pmod{3} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 1 \pmod{3} \\ f_3 \equiv 0 \pmod{3}. \end{cases}$$

- *The following congruences mod 5^2 hold:*

$$\begin{cases} f_6 \equiv f_5 \equiv f_3 \equiv f_1 \equiv f_0 \equiv 1 \mod 25 \\ f_4 \equiv f_2 \equiv 0 \mod 25. \end{cases}$$

- *The following congruences mod 7^4 hold:*

$$\begin{cases} f_6 \equiv f_0 \pmod{7^4} \\ f_5 \equiv f_1 \pmod{7^4} \\ f_4 \equiv f_2 \pmod{7^4}. \end{cases}$$

  Furthermore,

$$\begin{cases} f_6 \equiv 1 \pmod{7} \\ f_5 \equiv 0 \pmod{7} \end{cases} \quad \begin{cases} f_4 \equiv 2 \pmod{7} \\ f_3 \equiv 0 \pmod{7}. \end{cases}$$

- *The following congruences mod 29 hold:*

$$\begin{cases} f_6 \equiv 1 \pmod{29} \\ f_5 \equiv 1 \pmod{29} \\ f_4 \equiv 0 \pmod{29} \\ f_3 \equiv 0 \pmod{29} \end{cases} \quad \begin{cases} f_2 \equiv 0 \pmod{29} \\ f_1 \equiv 17 \pmod{29} \\ f_0 \equiv 5 \pmod{29}. \end{cases}$$

- *The following congruences mod 43 hold:*

$$\begin{cases} f_6 \equiv 1 \pmod{43} \\ f_5 \equiv 1 \pmod{43} \\ f_4 \equiv 0 \pmod{43} \\ f_3 \equiv 0 \pmod{43} \end{cases} \quad \begin{cases} f_2 \equiv 3 \pmod{43} \\ f_1 \equiv 13 \pmod{43} \\ f_0 \equiv 21 \pmod{43}. \end{cases}$$

Then the Galois extension $\mathbb{Q}(J(C)[7])/\mathbb{Q}$ provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_7)$.

It is easy to construct infinitely many such curves. For instance, we may take the genus 2 curve defined by the hyperelliptic equation

$$\begin{aligned} y^2 = x^6 + 9757776 \cdot x^5 + 8853700 \cdot x^4 + 10422426 \cdot x^3 + \\ + 677292100 \cdot x^2 + 3179077776 \cdot x + 342862800. \end{aligned}$$

References

[1] Arias-de-Reyna, S. "Galois representations and tame Galois realizations," PhD diss., Universidad de Barcelona, 2009. Available at http://www.tesisenxarxa.net/TDX-0612109-101019/.

[2] Arias-de-Reyna, S. and N. Vila. "Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ over $\mathbb{Q}$." *J. Number Theory* 129, Issue 5 (2009): 1056-1065.

[3] Arias-de-Reyna, S. "Formal groups, supersingular abelian varieties and tame ramification." Preprint (2009).

[4] Artin, E. *Geometric algebra*. New York-London: Interscience Publishers, Inc., 1957.

[5] Birch, B. "Noncongruence subgroups, Covers and Drawings." In *The Grothendieck theory of dessins d'enfants*, edited by Leila Schneps, 25–46. Cambridge Univ. Press, 1994.

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

[7] Cohen, H. and G. Frey *Hanbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and its Applications. Chapman & Hall/CRC Taylor & Francis Group, 2006.

[8] Dieulefait, L. and N. Vila. "Projective linear groups as Galois groups over Q via modular representations." *J. Symbolic Comput* 30, no. 6 (2000): 799–810.

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

[10] Dieulefait, L. and G. Wiese. "On Modular Forms and the Inverse Galois Problem." Preprint (2009). arXiv:0905.1288v1 [math.NT] in the arXiv at http://front.math.ucdavis.edu/.

[11] Eisenträger K. and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields." Preprint (2004). arXiv:math/0405305v2 [math.NT] in the arXiv at http://front.math.ucdavis.edu/.

[12] Grothendieck, A. “Modeles de Néron et monodromie.” Exposé IX in *Groupes de monodromie en géométrie algébrique I.* Lecture Notes in Mathematics, Vol. 288. Berlin-New York: Springer-Verlag, 1972.

[13] Hindry, M. and J. H. Silverman. *Diophantine Geometry: An Introduction.* Graduate Texts in Mathematics 201. Springer, 2000.

[14] Hardy, G. H. and J. E. Littlewood. “Some problems of ‘partitio numerorum’ III: on the expression of a number as a sum of primes.” *Acta Mathematica* 44 (1923): 1–70.

[15] Kawamura, T. “The effective surjectivity of mod ℓ Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring.” *Comment. Math. Helv.* 78, no. 3 (2003): 486–493.

[16] Khare, C., M. Larsen and G. Savin. “Functoriality and the inverse Galois problem.” Preprint (2006). arXiv:math.NT/0610860 in the arXiv at http://front.math.ucdavis.edu/.

[17] Klüners, J. and G. Malle. “Counting nilpotent Galois extensions.” *J. Reine Angew. Math.* 572 (2004): 1–26.

[18] Le Duff, P. “Représentations galoisiennes associées aux points d’ordre ℓ des jacobiennes de certaines courbes de genre 2.” *Bull. Soc. Math. France* 126, no. 4 (1998): 507–524.

[19] Liu, Q. “Courbes stables de genre 2 et leur schema de modules.” *Math. Ann.* 295 (1993): 201-222.

[20] Liu, Q. “Modeles entiers des courbes hyperelliptiques sur un corps de valuation discrete.” *Trans. Amer. Math. Soc.* 348, no. 11 (1996): 4577–4610.

[21] Liu, Q. *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford: Oxford University Press, 2002.

[22] Maisner, D. and E. Nart. “Abelian Surfaces over Finite Fields as Jacobians.” *Experimental Mathematics* 11, 3 (2001): 321–337.

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

[24] Milne, J. S., *Abelian varieties*. Version 2.0, March 16, 2008. Available at www.jmilne.org/math/.

[25] Namikawa, Y. and K. Ueno. "The complete classification of fibres in pencils of curves of genus two." *Manuscripta Math.* 9 (1973): 143–186.

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

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

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

[29] Plans, B. and N. Vila. "Trinomial extensions of $\mathbb{Q}$ with ramification conditions." *J. Number Theory* 105, no. 2 (2004): 387–400.

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

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

[32] Serre, J-P. *Topics in Galois Theory*. Research Notes in Mathematics. Boston: Jones and Bartlett Publishers, 1992.

[33] Serre, J-P. and J. Tate. "Good reduction of abelian varieties." *Ann. of Math.* (2) 88 (1968): 492–517.

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

[35] Vila. "Arithmetical-geometrical Galois representations and the inverse Galois problem." In *Algebra, arithmetic and geometry with applications*, 775–782. Berlin: Springer, 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 B. Edixhoven, G. van der Geer and B. Moonen, 343–350. Cambridge University Press, 2008.