# Galois representations and tame Galois realizations

**Sara Arias de Reyna**

**Departament d'Àlgebra i Geometria**
**Universitat de Barcelona**

# Galois representations and tame Galois realizations

Memòria presentada per a optar al grau de
Doctora en Matemàtiques
per
Sara Arias de Reyna Domínguez

UNIVERSITAT DE BARCELONA
Departament d'Àlgebra i Geometria
Barcelona 2009

Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Programa de doctorat en Matemàtiques,
Bienni 2004–2006

Títol de la tesi: `Galois representations and tame Galois realizations`
Doctoranda: `Sara Arias de Reyna Domínguez`
Directora de Tesi: `Núria Vila Oliva`

Núria Vila Oliva catedràtica
del Departament d'Àlgebra i Geometria
CERTIFICA
que aquesta memòria ha estat realitzada per Sara Arias de Reyna Domínguez sota la seva direcció i que constitueix la seva tesi per a optar al grau de Doctora en Matemàtiques.
Barcelona, Abril de 2009.

Signat: Núria Vila Oliva

Doctoral Dissertation Committee

Chair, Prof. Dr. Enric Nart Viñals

Members, Prof. Dr. Luis V. Dieulefait
Prof. Dr. Gerhard Frey

Date of dissertation public lecture presentation:

4 June 2009

Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona

# Galois representations and tame Galois realizations

Sara Arias de Reyna Domínguez

supported by a FPU predoctoral grant AP-20040601
of the Ministerio de Ciencia e Innovación.

*A mis padres y a Javi*

# Acknowledgements

In the first place I want to thank my advisor, Professor Núria Vila. I am deeply grateful for all the time she has devoted to guiding me, all the help and insight she has given me, and for her attentive support, generous patience and understanding.

I am also indebted to the Barcelona Number Theory Group (UB-UAB-UPC), who received me in a very friendly way and have provided me with a pleasing working environment. I am especially grateful to Luis Dieulefait and Victor Rotger for many stimulating conversations and helpful advice. The suggestions of Luis Dieulefait and Josep González have helped me to add some improvements to this thesis.

I am very grateful to Professors Gerhard Frey and Gabor Wiese for their kindness during my stay at the Institut für Experimentelle Mathematik in Essen, and for many enlightening conversations.

I want to express my gratitude to some of the professors in the Facultad de Matemáticas of the Universidad de Sevilla, who provided me with a solid background in mathematics when I was an undergraduate. I want to thank the professors in the Algebra Department, who have kindly followed my progress towards the completion of this thesis and have invariably supported me.

Finally I want to thank my family. My father and mother, my sisters Eva and María have given me love and encouragement throughout these years. I want to emphasize my gratefulness to my father, who showed me the beauty of mathematics even when I was a little girl. Through his teaching and more strongly through his example he stirred in me the love for mathematics, and especially number theory.

And I want to thank my betrothed, Javi, who has always been by my side in spite of the more than one thousand kilometers that sundered us. Without the strength of his love and his never-failing support, I doubt that I would have completed this project, or indeed have embarked on it.

# Contents

# Introduction

## Statement of the problem

A very natural question that an undergraduate who has begun the study of Galois theory can ask is the Inverse Galois Problem over $\mathbb{Q}$. Which finite groups can occur as Galois groups of an extension of the rational field? More precisely, given a finite group $G$, does there exist a Galois extension $K/\mathbb{Q}$ with Galois group $G$? This problem was first considered by D. Hilbert, who gave an affirmative answer in [35] when $G$ is a symmetric or an alternating group.

A central problem in number theory is the study of the structure of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Inverse Galois Problem 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, all 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 in this direction, the reader can leaf through [81] or [51]. The Inverse Galois Problem will constitute the groundwork of this dissertation.

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 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.

In this dissertation, we shall address the following problem, posed by Brian Birch. In [7], Section 2, he formulates the following question, which he describes as "somewhat malicious".

**Problem 0.1** (Tame Inverse Galois Problem)**.** Given a finite group G, is there a tamely ramified Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$?

In fact, it seems that at some point Birch has conjectured that all finite groups $G$ can be realized as the Galois group of a tamely ramified extension of $\mathbb{Q}$ (see [32], Section 2). We shall devote our attention to this problem, and seek an affirmative answer for some families of finite groups.

In [7], Birch notes that "extensions of $\mathbb{Q}$ with given Galois group constructed by the rigidity method are likely to be wildly ramified", hence his description of the problem as "malicious". In other words, the rigidity method is not well suited to produce such Galois realizations.

This remark has already caught the attention of some mathematicians. In [63], the authors show that the Mathieu groups $M_{11}$ and $M_{12}$, and the group of automorphisms of the Mathieu group $M_{22}$ can be realized as the Galois groups of tamely ramified Galois extensions of $\mathbb{Q}$ and, moreover, these realizations are obtained by specializing rigid extensions of $\mathbb{Q}(T)$.

Problem 0.1 is only one of the possible variants of the Inverse Galois Problem. There are many ways to strengthen the statement of the problem, by requiring that the Galois extension enjoys additional properties. Let us mention another such problem. Fix a finite set of prime numbers $S$. Can $G$ be realized as the Galois group of an extension $K/\mathbb{Q}$ which does not ramify in $S$? Note that if a group can be realized as the Galois group of an extension of $\mathbb{Q}$ which is unramified at any prescribed finite set of primes $S$, then it can also be realized as the Galois group of a tamely ramified extension. Namely, it suffices to pick $S$ as the set of primes which divide the order of $G$.

It is well known that if $G$ is a finite abelian group, then it can be realized as the Galois group of an extension which does not ramify in $S$, whatever finite set $S$ of primes has been chosen. Symmetric groups, and in general all groups such that the Noether problem has an affirmative answer, can also be realized as Galois groups of extensions which are not ramified in a prefixed finite set of primes $S$ ([73]). It is also known that the proof of Shafarevich that solvable groups can be realized as Galois groups over $\mathbb{Q}$ can be adapted to yield a Galois extension which is unramified in any prefixed finite set of primes $S$ (see [59], [41]). This problem has also been solved for alternating groups $A_n$ [62] and, if $n \neq 4, 6, 7$, for finite central extensions of $A_n$.

Consequently, all these groups can be realized as the Galois group of a tamely ramified extension of $\mathbb{Q}$. Problem 0.1 has also an affirmative answer for the finite central extensions of symmetric and alternating groups, and of the Mathieu groups $M_{11}$ and $M_{12}$ (see [61]).

## General strategy

One way to deal with the Inverse Galois Problem, and eventually with Problem 0.1, is to consider continuous Galois representations of the absolute Galois group of the rational field. Fix an algebraic closure of $\mathbb{Q}$. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can be endowed with a topology, namely the Krull topology (see [58], Chapter IV). The open subgroups of this topology correspond precisely with the finite subextensions $K/\mathbb{Q}$. Let $V$ be a finite dimensional vector space over a finite field $\mathbb{F}$, and consider a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in the group of automorphisms of $V$, say

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V).$$

Furthermore, assume that this representation is a continuous map, when we consider the discrete topology on $\mathrm{GL}(V)$ and the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular, the set containing only the identity element of $\mathrm{GL}(V)$ is an open set, and therefore $\rho^{-1}(\{\mathrm{Id}\}) = \ker\rho$ is an open (normal) subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. That is to say, there exists a finite (Galois) extension $K/\mathbb{Q}$ such that $\ker\rho = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Therefore

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

In other words, a continuous Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ provides a realization of $\mathrm{Im}\rho$ as a Galois group over $\mathbb{Q}$.

Throughout this dissertation, we shall adopt this strategy, and study Galois representations of the absolute Galois groups of the rational field. In particular, we shall study the Galois representations that arise through the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on some arithmetic-geometric objects, such as elliptic curves, or more generally abelian varieties, and modular forms.

How can one adapt this strategy to cope with Problem 0.1? We have to determine in which way the ramification of the Galois extension $K/\mathbb{Q}$ relates to the Galois representation $\rho$. When the Galois representation comes from geometric objects, a great deal of information is available. Namely, the representation is unramified outside a

finite set of primes, which depends on the geometry of the object. Also the characteristic polynomial of the image of the Frobenius elements at the unramified primes is known. We shall make use of these facts.

What conditions must $\rho$ satisfy in order to provide a Galois extension $K/\mathbb{Q}$ which is tamely ramified? In order to explain this, we need to introduce the inertia group and the wild inertia group. First of all, let us recall the definition of tame ramification.

**Definition 0.2.** Let $K/\mathbb{Q}$ be a finite Galois extension. Let $p$ be a prime number, and assume that the principal ideal generated by $p$ in the ring of integers $\mathcal{O}_K$ of $K$ decomposes as $(p) = (\prod_{i=1}^{n} \mathfrak{p}_i)^{e_p}$, where $\mathfrak{p}_i$ are different prime ideals of $\mathcal{O}_K$. Then $K/\mathbb{Q}$ is *tamely ramified at* $p$ if $p \nmid e_p$. We will say that $K/\mathbb{Q}$ is *tamely ramified* if it is tamely ramified at $p$ for all prime numbers $p$.

Let $p$ be a prime number, and let us consider the field of $p$-adic numbers $\mathbb{Q}_p$. Fix an algebraic closure of $\mathbb{Q}_p$ and an immersion $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. This induces an inclusion of Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Inside the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ 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 $\rho(I_{p,\mathrm{w}}) = \{\mathrm{Id}\}$). Note that this amounts to saying that the image of all the higher ramification groups is trivial.

Therefore, if we want a Galois representation $\rho$ 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 $p$. We will see that it will be far easier to ensure this property when the prime $p$ is different from the characteristic of the finite field $\mathbb{F}$. Throughout this dissertation we will refer by $\ell$ to the characteristic of $\mathbb{F}$, and we will denote by $p$ the prime numbers that occur in the course of our reasonings.

Note that this strategy of constructing Galois representations such that the image of the wild inertia group at all primes is trivial can be encompassed in the general trend of constructing Galois representations with prefixed local behaviour. This is a currently very active area of research; see for instance [90].

## Contents of the dissertation

This dissertation is split into two parts. In the first part, we tackle the realization of families of two dimensional linear groups over a finite field as the Galois group of a tamely ramified extension of $\mathbb{Q}$. We study the Galois representations attached to elliptic curves and to modular forms. In the second part we address the problem of realizing a family of four dimensional linear groups over a prime field as the Galois group of a tamely ramified extension of $\mathbb{Q}$. In this part we study the Galois representations attached to abelian surfaces.

The main results we have obtained are the following.

**Theorem 0.3.** *Let $\ell$ be a prime number. There exist infinitely many semistable elliptic curves $E$ with good supersingular reduction at $\ell$. The Galois representation attached to the $\ell$-torsion points of $E$ provides a tame Galois realization of* $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Furthermore, we give an explicit algorithm to construct these elliptic curves. See Theorem 1.19 and Theorem 1.20 for further details. The primes $\ell = 2, 3, 5, 7$ have been considered separately in Section 1.4.

**Theorem 0.4.** *Let $\ell \geq 5$ be a prime number. There exist infinitely many genus 2 curves $C$ such that the Galois representation attached to the $\ell$-torsion points of the Jacobian of $C$ provides a tame Galois realization of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

As in the previous result, we give an explicit algorithm that enables us to construct these curves. See Theorem 12.25 and Remark 12.27. Our reasonings do not apply for the primes $\ell = 2, 3$.

In addition, we have obtained tame Galois realizations of groups of the form $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ for several values of $\ell$ (see Proposition 2.10).

Let us go over the different chapters of this dissertation in more detail.

In the first chapter we study Galois representations attached to the $\ell$-torsion points of elliptic curves. It is a well-known result of J-P. Serre [77] that the image of these representations is the group $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all but finitely many primes $\ell$ whenever the elliptic curve has no complex multiplication. Combining it with a result of B. Mazur we manage to obtain Galois representations with large image. To obtain a tamely ramified extension, the most delicate point is the control of the

ramification of the representation at $\ell$. In fact, if we pick a semistable elliptic curve, we are assured that the ramification will be tame at all primes $p \neq \ell$. In order to obtain tame ramification at $\ell$, we ask the elliptic curve to have good supersingular reduction at this prime. We end the chapter by presenting an algorithm that computes, given a prime number $\ell$, a semistable elliptic curve with good supersingular reduction at $\ell$ and such that the Galois representation attached to the $\ell$-torsion points of $E$ is surjective. This elliptic curve provides a tame Galois realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Therefore we have an affirmative answer to Problem 0.1 for this family of groups. Note that we construct a supersingular elliptic curve over any prime field $\mathbb{F}_\ell$ with $\ell > 3$. We have recently found that some authors have given another construction that will soon appear in print (cf. [11]).

The contents of this first chapter are presented in [1].

In the second chapter we focus our attention on Galois representations attached to modular forms. K. Ribet [69] has studied the image of these representations when the modular form has no complex multiplication. As a conclusion, we can try to obtain tame Galois realizations of families of groups $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ and $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$. We recall some results of J-M. Fontaine concerning the ramification of the modular form at the prime $\ell$. Unfortunately, in this chapter we have not managed to obtain conclusive results. We point out the main difficulties that have arisen and, as a consequence of some computations of L. Dieulefait and N. Vila [23], we give some examples of tame Galois realizations of groups belonging to the family $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$.

The second part of this dissertation is a combination of many results, which fit together to produce tame Galois realizations of groups of the form $\mathrm{GSp}_4(\mathbb{F}_\ell)$. In this part we consider the Galois representations attached to the $\ell$-torsion points of an abelian surface $A$. The first chapters of this part address the problem of obtaining some control on the ramification of the Galois representation, and the last chapters deal with the issue of obtaining large image.

At the primes $p \neq \ell$, we will again take advantage of semistability. In Chapter 3 we recall a result of A. Grothendieck [31] about the Galois representation of semistable abelian varieties. As a consequence, the control of the ramification boils down to finding a way to deal with the ramification at $\ell$. This is the aim of chapters 4–10. In chapter 4, we review the case of elliptic curves, delving into the details of the reasoning that supersingularity implies tame ramification. We conclude that a key ingredient is the study of the formal group law

attached to the abelian variety. We introduce a condition (Hypothesis 4.7) such that, whenever it is satisfied by the formal group law attached to $A$, then the corresponding Galois representation is tamely ramified at $\ell$. Chapter 5 is devoted to recalling the notion of height of a formal group law of dimension greater than 1, and several points connected with it. In Chapter 6 we pause for a while to reflect on the results obtained up to this point. A new kind of formal group laws are introduced in Chapter 7, namely symmetric formal group laws (see Definition 7.3). This symmetry property, in contrast to Hypothesis 4.7, is easy to detect with a quick look at the formal power series that define the formal group law. The rest of Chapter 7 is devoted to proving that, under certain suitable conditions, symmetric formal group laws satisfy Hypothesis 4.7, and thus the Galois extension provided by the Galois representation attached to the $\ell$-torsion points of $A$ is tamely ramified.

Chapter 8 addresses the problem of finding in nature some abelian surfaces such that the corresponding formal group law is symmetric. Namely, it considers a certain kind of genus 2 curves, which we call symmetric (see Definition 8.3). It is proved that the Jacobian variety attached to such a curve is an abelian surface with symmetric formal group law. The last section of the chapter focuses on symmetric bielliptic curves.

One last issue must be addressed before leaving aside the matter of obtaining tame ramification. Namely, the main result obtained in the previous chapters ensures that certain abelian surfaces give rise to Galois representations that will be tamely ramified. However, these conditions are very restrictive: in particular they will also imply that the image of the Galois representation is not large. Therefore, the conditions must be relaxed in some way in order to overcome this last obstacle. This task is carried out in Chapter 10.

At last we come to the question of determining the image of the Galois representations attached to the $\ell$-torsion points of abelian surfaces. As in the case of dimension 1, a well-known result of J-P. Serre [82] asserts that, if the abelian variety does not have complex multiplication, then the image of the representation coincides with $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for all but finitely many primes $\ell$. Again, we have to devise a way of ensuring that the image of the representation is large. We take as starting point some explicit results of P. Le Duff, and following a suggestion of L. Dieulefait we present a nice statement in Chapter 11.

Finally, Chapter 12 is devoted to combining all the previous results

into an explicit algorithm, which, given a prime $\ell > 3$, produces a genus 2 curve whose Jacobian satisfies that the Galois representation attached to its $\ell$-torsion points provides a tame Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

We have added an Appendix which gathers a specific set of defining equations for the Jacobian of a genus 2 curve, which can be found at the web page of V. Flynn, but as far as I know have not appeared in print in this exact form (cf. [28]).

At the end there is a summary of the contents of the dissertation, written in Spanish.

# Part I

# Tame Galois realizations of 2-dimensional linear groups over $\mathbb{Q}$

# Chapter 1

# Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$

## 1.1 Introduction

Let $\ell$ be a prime number. In this chapter we will address the tame inverse Galois problem when $G = \mathrm{GL}_2(\mathbb{F}_\ell)$, that is to say, we will consider the question of constructing a tame Galois extension $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$ (see Problem 0.1). It is a classical result that the linear groups $\mathrm{GL}_2(\mathbb{F}_\ell)$ can be realized as Galois groups over the field of rational numbers (cf. [89]). Our aim is to show that one can obtain some Galois realization $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ with $K/\mathbb{Q}$ tamely ramified.

We will approach this problem by means of the Galois representations attached to the $\ell$-torsion points of elliptic curves. Under certain hypotheses, these representations will supply us with tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Let us consider an elliptic curve $E/\mathbb{Q}$ defined over the rational numbers. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the group of $\ell$-torsion points of the elliptic curve (which shall be denoted by $E[\ell]$), and thus gives rise to a group homomorphism

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

This homomorphism is continuous when we consider the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the discrete topology on $\mathrm{GL}_2(\mathbb{F}_\ell)$. In fact, to see this it is enough to show that the inverse image of the identity

(which is an open set in $\mathrm{GL}_2(\mathbb{F}_\ell)$) is open in the Krull topology. But this inverse image is the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where $K = \mathbb{Q}(E[\ell])$ is the finite Galois extension obtained by adjoining to $\mathbb{Q}$ the coordinates of the $\ell$-torsion points of $E$.

As a consequence, we obtain that the image of $\varphi_\ell$ can be realized as a Galois group over $\mathbb{Q}$;

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

Were $\varphi_\ell$ surjective, we would obtain a realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$.

Concerning the surjectivity of this representation, we have the following result of J-P. Serre (see [77], Theorem 2 of § 4.2).

**Theorem 1.1** (Serre)**.** *Let $K$ be an algebraic number field, and let $E/K$ be an elliptic curve without complex multiplication. Then, for all but finitely many primes $\ell$, the homomorphism $\varphi_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective.*

This result, of course, provides a great deal of information. For instance, combining it with other results in the paper, Serre proves that the image of the Galois representation $\varphi_\ell$ attached to the elliptic curve $E$ of conductor $\ell = 37$ coincides with $\mathrm{GL}_2(\mathbb{F}_\ell)$, for all primes $\ell$ (see Example 5.5.6 of [77]). In this way, the elliptic curve $E$ provides a Galois realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$, for all primes $\ell$.

But, unfortunately, given a prime $\ell$, Theorem 1.1 does not tell us how to check whether the result holds for our prime or, on the contrary, it is one of those exceptional primes for which the result does not apply. In [52] some explicit bounds for $\ell$ are computed, but they are far too high to suit our purposes. We will make use of the following result of B. Mazur (Theorem 4 of [53]).

**Theorem 1.2.** *Let $E/\mathbb{Q}$ be a semistable elliptic curve, and $\ell \geq 11$ a prime number. The Galois representation attached to the $\ell$-torsion points of $E$ is surjective.*

Therefore, for each prime $\ell \geq 11$, the Galois representation attached to the $\ell$-torsion points of a semistable elliptic curve defined over $\mathbb{Q}$ gives rise to a realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$. In the rest of the chapter, we shall only consider semistable elliptic curves. We need to find suitable conditions that guarantee that the

field extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified, so that we can combine them with the previous result. Following the notation used at the introduction of the dissertation, we shall denote by $I_p$ (respectively $I_{p,\mathrm{w}}$) the inertia group (respectively the wild inertia group) at a prime $p$.

**Theorem 1.3.** *Let $\ell \geq 11$ be a prime number, and consider a semistable elliptic curve $E/\mathbb{Q}$ such that $\ell$ has good supersingular reduction. Let us consider the Galois representation*

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

*attached to the $\ell$-torsion points of $E$. Then*

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell),$$

*and moreover the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified.*

*Proof.* Taking into account Theorem 1.2, it suffices to show that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified.

Let $p$ be a prime number. Let us check that $\varphi_\ell(I_{p,\mathrm{w}})$ is trivial.

Assume first that $p \neq \ell$. Since $E$ is semistable, there are only two possibilities: either $E$ has good reduction at $p$, or $E$ has bad multiplicative reduction at $p$. In the first case, the Néron-Ogg-Shafarevich criterion claims that $\varphi_\ell(I_p) = 1$, and therefore $\varphi_\ell(I_{p,\mathrm{w}})$ is also trivial. In the second case, the result can be proven using Tate curves. Following the notation of [84], Appendix C, § 14, we know that there exists $q \in \mathbb{Q}_p^*$ with $p$-adic absolute value $|q| < 1$, such that $E$ is isomorphic to the Tate curve $E_q$, either over $\mathbb{Q}_p$ or an unramified quadratic extension of $\mathbb{Q}_p$. In both cases, the action of the inertia group $I_p$ on the $\ell$-torsion points of $E$ coincides with the action on the $\ell$-torsion points of $E_q$. But the $\ell$-torsion points of $E_q$ satisfy the following short exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules:

$$0 \to \mu_\ell \to E_q[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0,$$

where $\mu_\ell$ denotes the group of the $\ell$-th roots of unity in $\mathbb{Q}_p^*$ and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\mathbb{Z}/\ell\mathbb{Z}$ is trivial (see Appendix A.1.2, p. IV-31 of [80]). Therefore, choosing a suitable basis of $E_q[\ell]$, the image of $I_p$ by the representation $\varphi_\ell$ satisfies

$$\varphi_\ell(I_p) \subseteq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

That is to say, it is contained in a cyclic group of order $\ell$. But since $I_{p,\mathrm{w}}$ is a pro-$p$-group, the elements of $\varphi_\ell(I_{p,\mathrm{w}})$ have order equal to a power of $p$. Therefore the image of $I_{p,\mathrm{w}}$ must be trivial.

Suppose now that $p = \ell$. In [77] J-P. Serre studies the image of the inertia and wild inertia groups by the Galois representations attached to the $p$-torsion points of an elliptic curve defined over a local field of characteristic zero and residual characteristic $p$. In particular, Serre proves that, if $E$ is an elliptic curve defined over the field of $p$-adic numbers which has good supersingular reduction, then the image of the wild inertia group $I_{p,\mathrm{w}}$ by the representation $\varphi_p$ is trivial (cf. [77], Proposition 12). This concludes the proof.

□

From now on, our aim shall be to find, for each prime $\ell \geq 11$, an elliptic curve satisfying the hypotheses of Theorem 1.3. In the next section we will focus on the construction of elliptic curves with good supersingular reduction at a given prime $\ell$. Afterwards, we will blend it into a construction which gives us an elliptic curve satisfying all the required conditions.

**Remark 1.4.** The most delicate point when we try to ensure that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified is the control of the ramification at the prime $p = \ell$. In Theorem 1.3, this control is achieved by asking that the reduction at the prime $\ell$ be good and supersingular.

Let us fix an elliptic curve $E/\mathbb{Q}$ without complex multiplication. J-P. Serre has proven that the set of primes having good supersingular reduction has density zero (see [74], § 3.4, Corollary 1). However, according to N. D. Elkies [27], this set is infinite. In any case, it seems that, given an elliptic curve, in this way we can prove only for few primes $\ell$ (that is to say, for primes $\ell$ belonging to a density zero set) that the realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ obtained will be tamely ramified. So a study of the ramification in the case of ordinary reduction might seem advisable. However, in a note to [77] (Note 1 to n° 94., p. 706 of [78]), Serre states that it might seem reasonable to think that the density of the set of primes of good ordinary reduction such that the wild inertia group acts trivially is also zero. Thus, this approach does not seem to be much more fruitful than the one we have taken.

## 1.2 Supersingular elliptic curves

In this section we are going to construct, for each prime number $\ell > 3$, an elliptic curve $E/\mathbb{Q}$ with good supersingular reduction at $\ell$. We will first recall some results on supersingular elliptic curves over finite fields, and then proceed to describe an explicit construction. Throughout the section, $\ell > 3$ will be a fixed prime number. Let us denote by $\overline{\mathbb{F}}_\ell$ an algebraic closure of $\mathbb{F}_\ell$.

We start with the definition of supersingular elliptic curve.

**Definition 1.5.** Let $E$ be an elliptic curve defined over a finite field of characteristic $\ell$. $E$ is *supersingular* if $E[\ell^r] = 0$, for all $r \geq 1$.

If $E$ is a supersingular elliptic curve over a finite field of characteristic $\ell$, it can be proven that its $j$-invariant lies in $\mathbb{F}_{\ell^2}$ (see [84], Theorem 3.1 of chap. V). Therefore, there are only a finite number of such curves. Next we recall a characterization of these curves in terms of the Deuring polynomial.

**Definition 1.6.** The *Deuring polynomial* is defined by the following expression:

$$H_\ell(x) = \sum_{k=0}^{\frac{\ell-1}{2}} \binom{\frac{\ell-1}{2}}{k}^2 x^k.$$

The roots of this polynomial give us all supersingular elliptic curves in Legendre normal form.

**Proposition 1.7.** *Let $\lambda \in \overline{\mathbb{F}}_\ell$, $\lambda \neq 0, 1$, and let us consider the elliptic curve $E$ defined over $\overline{\mathbb{F}}_\ell$ by the equation in Legendre form $y^2 = x(x-1)(x-\lambda)$. Then $E$ is supersingular if and only if $H_\ell(\lambda) = 0$.*

*Proof.* See [84], chapter V, Theorem 4.1. □

Let us bear in mind that we are looking for an elliptic curve $E$, defined over $\mathbb{Q}$, such that its reduction modulo $\ell$ is a supersingular elliptic curve. Therefore, the $j$-invariant of $E$ must belong to $\mathbb{Q}$, and consequently the $j$-invariant of the reduction must lie in $\mathbb{F}_\ell$. That is to say, only supersingular elliptic curves with $j$-invariant in $\mathbb{F}_\ell$ can be lifted to $\mathbb{Q}$. Our problem is therefore to find a root of $H_\ell(x)$ such that the elliptic curve given by the equation $y^2 = x(x-1)(x-\lambda)$ has $j$-invariant in $\mathbb{F}_\ell$. Certainly, if we find a value of $\lambda \in \mathbb{F}_\ell$ such that the elliptic curve defined over $\mathbb{F}_\ell$ by the equation $y^2 = x(x-1)(x-\lambda)$ is supersingular, it would be a simple task to lift this equation to $\mathbb{Z}$.

**Remark 1.8.** Assume $\ell$ is a prime congruent to 3 modulo 4, so that $\frac{\ell-1}{2}$ is odd. Then $H_\ell(x)$ contains an even number of terms, namely $\frac{\ell-1}{2}+1$. Besides, they can be paired in the following way:

$$\binom{\frac{p-1}{2}}{k}^2 x^k \quad \text{and} \quad \binom{\frac{p-1}{2}}{\frac{p-1}{2}-k}^2 x^{\frac{p-1}{2}-k}$$

Since $\frac{\ell-1}{2}$ is odd, $(-1)^k$ and $(-1)^{\frac{p-1}{2}-k}$ have opposite signs. Therefore, when $x=-1$, the paired terms cancel out, and so we obtain that $H_\ell(-1)=0$. That is to say, we have found a root of $H_\ell(x)$ in $\mathbb{F}_\ell$, provided $l \equiv 3 \pmod 4$.

Therefore we can conclude that the elliptic curve defined over $\mathbb{F}_\ell$ by the equation $y^2=x(x-1)(x+1)$ is a supersingular elliptic curve whenever $\ell$ is congruent to 3 modulo 4.

In the general case, however, things are not that simple. To begin with, if $\ell \equiv 1 \pmod 4$, $H_\ell(x)$ has no linear factors over $\mathbb{F}_\ell$ (see [10], Theorem 1-(a)). We shall need some knowledge of the roots of the Deuring polynomial. Let us recall the following well-known facts (see for instance Theorem 4.1-(c) of chapter V of [84] and Proposition 2.2 of [4]).

**Proposition 1.9.** *Let $\ell$ be an odd prime number.*

- *The roots of $H_\ell(x)$ are simple.*
- *The roots of $H_\ell(x)$ lie in $\mathbb{F}_{\ell^2}$.*

Since the roots of $H_\ell(x)$ are in $\mathbb{F}_{\ell^2}$, $H_\ell(x)$ splits in linear and quadratic factors over $\mathbb{F}_\ell$. Proposition 6 of [10] gives us a characterization of the factors that will yield an elliptic curve with $j$-invariant in $\mathbb{F}_\ell$.

**Proposition 1.10.** *The $j$-invariant of the supersingular elliptic curve defined by the Legendre equation $y^2=x(x-1)(x-\lambda)$ lies in $\mathbb{F}_\ell$ if and only if $\lambda$ is an element of $\mathbb{F}_\ell$, or else it is quadratic over $\mathbb{F}_\ell$ satisfying that either its norm is equal to 1, or its trace is equal to 1, or its norm and trace are equal to each other.*

We are going to focus on factors of the form $x^2-x+a$, that is to say, factors with trace equal to 1 (as a matter of fact, if we find an irreducible quadratic factor of this form, we can easily produce

quadratic factors of the other two types: see the proof of Theorem 1-(a, b) of [10]). In [14], L. Carlitz studies the divisibility of $H_\ell(x)$ by certain factors of this form (for instance, he proves that the factor $x^2 - x + 1$ divides $H_\ell(x)$ if $(-3/l) = -1$, see Theorem 16 of [14]). But we are not going to fix the value of $a$ in the expression $x^2 - x + a$; for us it will suffice to know that there exists a factor of this form, which can be computed effectively. J. Brillhart and P. Morton have counted the number of factors of this form that divide $H_\ell(x)$ (see Theorem 1-(b) of [10]).

**Theorem 1.11.** *Let $\ell$ be any prime greater than 3. The number of monic irreducible quadratic factors of $H_\ell(x)$ having middle coefficient $-1$ is*

$$N_2 = \begin{cases} h(-\ell)/2 & \text{if } \ell \equiv 1 \pmod 4, \\ (3h(-\ell) - 1)/2 & \text{if } \ell \equiv 3 \pmod 8, \\ (h(-\ell) - 1)/2 & \text{if } \ell \equiv 7 \pmod 8, \end{cases}$$

*where $h(-\ell)$ denotes the class number of $\mathbb{Q}(\sqrt{-\ell})$.*

**Corollary 1.12.** *Let $\ell > 3$ be a prime number. There exists $a \in \mathbb{F}_\ell$ such that $x^2 - x + a$ divides $H_\ell(x)$.*

*Proof.* Since $h(-\ell) \geq 1$, it is obvious from the above theorem that whenever $\ell \equiv 1 \pmod 4$ or $\ell \equiv 3 \pmod 8$ the number of monic irreducible quadratic factors of $H_\ell(x)$ having middle coefficient $-1$ is strictly greater than 0. Trouble may arise when $\ell \equiv 7 \pmod 8$ and $h(-\ell) = 1$. But the only prime which satisfies these two conditions is $\ell = 7$ (see [85]). If we factor $H_7(x)$, we obtain

$$H_7(x) = (x + 1)(x + 3)(x + 5)$$

Note that the product of the two factors $(x+1)(x+5)$ yields $x^2-x+5$, which has the desired form. □

Provided we have a factor of $H_\ell(x)$ of the form $x^2 - x + a$, what we are trying to do is to give a Weierstrass equation such that, after a change of coordinates, we can write it in Legendre form $y^2 = x(x - 1)(x - \lambda)$, where $\lambda$ is a root of this factor of $H_\ell(x)$, that is,

$$\lambda = \frac{1}{2} \pm \frac{\sqrt{1 - 4a}}{2}.$$

Let us consider a Weierstrass equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

and let us try to determine $e_1, e_2, e_3$ so that this equation satisfies the condition above.

A change of coordinates yields a Weierstrass equation in Legendre form, with

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1}. \tag{1.1}$$

Since we know that, in general, $\lambda$ does not lie in $\mathbb{F}_\ell$, we cannot expect to find $e_1, e_2, e_3$ all in $\mathbb{F}_\ell$. Instead, we shall assume one of them lies in $\mathbb{F}_{\ell^2}$. Automatically, this implies that one of the others is its conjugate, and that the remaining one lies in $\mathbb{F}_\ell$.

Taking all this into account, we will look for $b, c, d \in \mathbb{F}_\ell$, such that the equation

$$y^2 = (x - b)(x - (c + \theta))(x - (c - \theta)) \tag{1.2}$$

where $\theta \in \mathbb{F}_{\ell^2}$ satisfies $\theta^2 + d = 0$, defines an elliptic curve with $\lambda = \frac{1}{2} \pm \frac{\sqrt{1-4a}}{2}$.

Note that performing the product on the right hand side we get $(x-b)(x-(c+\theta))(x-(c-\theta)) = x^3-(b+2c)x^2+(2bc+c^2+d)x-(bc^2+bd)$ and so Equation (1.2) defines a curve over $\mathbb{F}_\ell$. We shall have to ensure that the discriminant is not zero.

According to Equation (1.1), we can express the curve defined by Equation (1.2) in Legendre form with $\lambda = \frac{1}{2} + \frac{b-c}{2\theta}$. So we simply shall look for $b, c, d \in \mathbb{F}_\ell$ such that

$$\frac{b - c}{\theta} = \pm\sqrt{1 - 4a}.$$

In particular, it suffices to ask that

$$\begin{aligned} d &= 4a - 1 \\ b &= c + (4a - 1). \end{aligned}$$

Let us gather together these considerations into a statement:

**Proposition 1.13.** *Let $\ell > 3$ be a prime number, and let $a \in \mathbb{F}_\ell$ be such that the polynomial $x^2 - x + a$ divides the Deuring polynomial $H_\ell(x)$. If $b, c, d \in \mathbb{F}_\ell$ satisfy*

$$\begin{aligned} d &= 4a - 1 \\ b &= c + (4a - 1) \end{aligned}$$

*then the equation*

$$y^2 = x^3 - (b+2c)x^2 + (2bc + c^2 + d)x - (bc^2 + bd) \tag{1.3}$$

*defines a supersingular elliptic curve over* $\mathbb{F}_\ell$.

*Proof.* To see that Equation (1.3) defines an elliptic curve, we have to check that its discriminant $\Delta = -64d((b-c)^2 + d)^2$ is different from zero. But the conditions above imply that $d \neq 0$ and $(b-c)^2 + d \neq 0$. Indeed, in the first case, we would have that $4a - 1 = 0$, and therefore $x^2 - x + a = x^2 - x + 1/4 = (x - 1/2)^2$, which has a double root, in contradiction with Proposition 1.9. In the second case, $4a(4a-1) = 0$, and hence either $a = 1/4$ (which cannot happen, as we have just seen) or $a = 0$. But then $x^2 - x$ would divide $H_\ell(x)$, and Definition 1.6 makes it clear that zero is never a root of the Deuring polynomial.

Finally, by construction this equation defines a supersingular elliptic curve. □

**Remark 1.14.** Given a prime $\ell > 3$, let $b, c, d \in \mathbb{F}_\ell$ be as above. Then lifting these coefficients to $\mathbb{Z}$, we obtain a Weierstrass equation, defined over $\mathbb{Q}$, such that reducing modulo $\ell$ we obtain the supersingular elliptic curve given in Proposition 1.13.

## 1.3 Explicit construction for $\ell \geq 11$

In this section we are going to construct, for each prime number $\ell \geq 11$, an elliptic curve $E$ such that the Galois representation attached to the group of $\ell$-torsion points of $E$ provides us with a tame realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$. The primes 2, 3, 5, and 7 will be handled in the next section.

Let us fix a prime $\ell \geq 11$. We shall start by stating the problem we wish to solve, once we take into account the contents of Theorem 1.3.

**Problem 1.15.** Find $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ such that:

- The Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.4}$$

  has non-zero discriminant, and therefore defines an elliptic curve.

- The elliptic curve defined by Equation (1.4) is semistable.

- The elliptic curve defined by Equation (1.4) has good supersingular reduction at the prime $\ell$.

In what follows, we are going to replace the conditions that appear in Problem 1.15 with others which are more restrictive but also more convenient for us. First of all, we shall look for $a_1, a_3, a_2, a_4, a_6 \in \mathbb{Z}$. This will allow us to control the behaviour of the different primes $p$ by requiring the coefficients of the equation to satisfy certain congruences modulo $p$.

Section 1.2 dealt with the last condition. Now, in order to tackle the semistability condition, let us briefly recall some elementary facts about reduction of elliptic curves.

Assume we have a Weierstrass equation (1.4) such that the $a_i$, $i = 1, 2, 3, 4, 6$, belong to the ring of integers $\mathbb{Z}$. Attached to it there are certain quantities; in particular one might consider $c_4$ and the discriminant $\Delta$ (their expressions in terms of the $a_i$, $i = 1, 2, 3, 4, 6$, can be found in [84], chap. III, § 1). If a prime $p$ does not divide either $\Delta$ or $c_4$, then Equation (1.4) is minimal with respect to the $p$-adic valuation (cf. [84], chap. VII, Remark 1.1).

The kind of reduction modulo $p$ of a curve defined by a Weierstrass equation over $\mathbb{Z}$, minimal with respect to the $p$-adic valuation, can easily be classified in terms of $c_4$ and $\Delta$:

**Lemma 1.16.** *Let $E/\mathbb{Q}_p$ be an elliptic curve defined by a Weierstrass equation* (1.4)*, minimal with respect to the $p$-adic valuation, and let $c_4$ and $\Delta$ be the corresponding quantities attached to it.*

*Then*

- *$E$ has good reduction if and only if $p \nmid \Delta$.*
- *$E$ has bad multiplicative reduction if and only if $p|\Delta$ but $p \nmid c_4$.*

According to Section 1.2, it is clear that when $\ell \equiv 3 \pmod 4$ one can give a simpler construction, so we will treat it first and then turn to the general case.

Assume therefore that $\ell \equiv 3 \pmod 4$. We are going to determine a value $\lambda \in \mathbb{Z}$ such that the equation

$$y^2 = x(x-1)(x-\lambda) \tag{1.5}$$

satisfies the conditions in Problem 1.15. From Remark 1.8 it follows that the last condition will be satisfied provided we require $\lambda \equiv -1$

(mod $\ell$). Now if we compute the quantities $c_4$ and $\Delta$ attached to Equation (1.5) we obtain

$$\begin{cases} \Delta = 16\lambda^2(\lambda-1)^2 \\ c_4 = 16(\lambda^2-\lambda+1). \end{cases}$$

It follows that, if $p \neq 2$, Equation 1.5 is a minimal Weierstrass equation, and further that the reduction of $E$ at $p$ is either good or bad of multiplicative kind, since $p$ cannot divide both $\Delta$ and $c_4$. Thus, in order to ensure semistability, we just have to control the prime $p = 2$.

In order to study the behaviour of the prime 2 we must change coordinates so that we obtain a minimal Weierstrass equation with respect to the 2-adic valuation. Let us consider the following change:

$$\begin{cases} x = 2^2x' + r \\ y = 2^3y' + 2^2sx' + t \end{cases} \tag{1.6}$$

where $r, s, t \in \mathbb{Q}$. If we write $c_4'$ for the quantity attached to the new equation, we have the relation

$$c_4' = c_4/2^4 = \lambda^2 - \lambda + 1,$$

which is always an odd number. Therefore, if we choose $r, s, t$ so that the new equation has again coefficients in $\mathbb{Z}$, it will be a minimal Weierstrass equation, and moreover at $p = 2$ there will be either good reduction or bad multiplicative reduction, according to whether $\Delta'$ is odd or not.

Now if we apply the change of variables (1.6) to Equation (1.5), we get

$$\begin{aligned} &y'^2 + sx'y' + \frac{1}{4}ty' = x'^3 + \frac{1}{4}(-1-\lambda+3r-s^2)x'^2 + \\ &+ \frac{1}{16}(\lambda - 2r - 2\lambda r + 3r^2 - 2st)x' + \frac{1}{64}(\lambda r - r^2 - \lambda r^2 + r^3 - t^2). \end{aligned}$$

Hence, to ensure that the coefficients of the new equation will be integers, we just have to solve the following congruence system:

$$\begin{cases} t & \equiv 0 \pmod 4 \\ 1+\lambda-3r+s^2 & \equiv 0 \pmod 4 \\ -\lambda+2r+2\lambda r-3r^2+2st & \equiv 0 \pmod{16} \\ -\lambda r + r^2 + \lambda r^2 - r^3 + t^2 & \equiv 0 \pmod{64}. \end{cases}$$

Let us choose $r = s = 1$, $t = 0$. Then the system reduces to the single equation

$$\lambda \equiv 1 \pmod{16},$$

and the new equation we obtain is $y'^2 + x'y' = x'^3 + \frac{1}{4}(1-\lambda)x'^2 + \frac{1}{16}(1-\lambda)x'$.

We have thus solved Problem 1.15 whenever $\ell \equiv 3 \pmod 4$:

**Proposition 1.17.** *Let $\ell \geq 11$ be a prime number such that $\ell \equiv 3 \pmod 4$, and let $\lambda \in \mathbb{Z}$ be such that*

- $\lambda \equiv -1 \pmod{\ell}$.
- $\lambda \equiv 1 \pmod{16}$.

*Then the equation $y^2 = x(x-1)(x-\lambda)$ satisfies the conditions of Problem 1.15.*

Let us now consider any prime $\ell \geq 11$. In order to make it easier to deal with the supersingularity condition applying Proposition 1.13, we shall look for a Weierstrass equation of the shape

$$y^2 = (x-b)(x-(c+i\sqrt{d}))(x-(c-i\sqrt{d})), \tag{1.7}$$

where $b, c, d \in \mathbb{Z}$. Our aim is to find some conditions that assure us that it defines a semistable elliptic curve.

A direct calculation yields that

$$\begin{cases} \Delta = -64d((b-c)^2+d)^2 \\ c_4 = 16((b-c)^2 - 3d) \end{cases}$$

The conditions on $b, c, d$ that we will require in order to apply Proposition 1.13 shall in particular imply that $\Delta$ is different from zero, so we will not consider that for the moment. We will turn to the issue of semistability.

If an odd prime $p$ divides both $\Delta$ and $c_4$, then it would have to divide $b-c$ and $d$. So to guarantee that the curve is semistable at all odd primes $p$, we must require that the greatest common divisor of $b-c$ and $d$ be a power of two.

Again, the strategy to deal with $p = 2$ is to find a suitable change of variables, so as to obtain an equation where one of the new quantities $c_4$ or $\Delta$ is odd. This assures us that it is minimal at 2, and that the elliptic curve it defines is semistable at 2. The idea to perform this is explained in the following remark.

**Remark 1.18.** Let us take any elliptic curve given by an equation of the form

$$y^2 = (x - b_0)(x - (c_0 + i\sqrt{d_0}))(x - (c_0 - i\sqrt{d_0})),$$

and satisfying that there exists a change of variables, preserving the Weierstrass form, which returns a new equation such that the quantity $\Delta'$ (or else $c_4'$) attached to it is odd. Then if we require $b, c, d$ to be congruent to $b_0, c_0, d_0$ modulo a high enough power of 2, the elliptic curve defined by Equation (1.7) will be semistable at 2. The reason why this holds is simply that the same change of variables, applied to Equation (1.7), will yield an equation such that the quantity $\Delta'$ (or else $c_4'$) attached to it is odd.

Let us consider the curve 17-A1 from Cremona's Tables [18],

$$y^2 + xy + y = x^3 - x^2 - x - 14. \tag{1.8}$$

This curve is semistable, and has good reduction at every prime save 17. The discriminant of this equation is $\Delta = -83521$, which is odd. Therefore this is a minimal model for $p = 2$. Through a change of variables, we can transform this equation into

$$y^2 = x^3 - 3x^2 - 8x - 880 = (x - 11)(x^2 + 8x + 80) \tag{1.9}$$

which has the desired shape with $b_0 = 11$, $c_0 = -4$, $d_0 = 64$. The change of variables from Equation (1.9) to Equation (1.8) is the following:

$$\begin{cases} x = 4x' \\ y = 8y' + 4x' + 4 \end{cases}$$

If we apply this change of variables to Equation (1.7), we obtain

$$\begin{aligned} y^2 + xy + y = x^3 - \left(\frac{1}{4} + \frac{b}{4} + \frac{c}{2}\right) x^2 + \\ + \left(-\frac{1}{2} + \frac{bc}{8} + \frac{c^2}{16} + \frac{d}{16}\right) x - \left(\frac{1}{4} + \frac{bc^2}{64} + \frac{bd}{64}\right). \end{aligned} \tag{1.10}$$

In order to be certain that all coefficients are integers, and moreover of the same parity than those of Equation (1.8) (so that the discriminant will also be odd), we need to ask $b, c, d$ to be congruent to $b_0, c_0, d_0$ modulo $2 \cdot 64 = 128$.

Finally we have all the ingredients to solve Problem 1.15.

**Theorem 1.19.** *Let $\ell \geq 11$ be a prime number. Assume $a \in \mathbb{Z}$ is such that, if $\overline{a}$ denotes its reduction modulo $\ell$, the factor $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$ in $\mathbb{F}_\ell[x]$.*

*Let us pick $b, c, d \in \mathbb{Z}$ satisfying:*

- *$b - c$ and $d$ are relatively prime.*
- *$b - c \equiv 4a - 1 \pmod{\ell}$, $d \equiv 4a - 1 \pmod{\ell}$.*
- *$b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$.*

*Then the equation*

$$y^2 = x^3 - (b + 2c)x^2 + (2bc + c^2 + d)x - (bc^2 + bd) \tag{1.11}$$

*defines a semistable elliptic curve with good supersingular reduction at $\ell$.*

*Proof.* First of all, note that $\ell$ does not divide the discriminant of Equation (1.11), and therefore it cannot be zero (see the proof of Proposition 1.13). Consequently Equation (1.11) defines an elliptic curve over $\mathbb{Q}$, say $E$.

Since $b - c$ and $d$ are relatively prime, it is easy to check that no odd prime number can divide both quantities $c_4$ and $\Delta$; thus $E$ is semistable at all these primes. To study the reduction at $p = 2$, let us apply to Equation (1.11) the change of variables (1.6). Now the congruence conditions modulo 128 allow us to check that the equation we obtain has integer coefficients and odd discriminant, and therefore $E$ has good reduction at $p = 2$.

Finally, since $\ell$ does not divide $\Delta$, Equation (1.11) is a minimal Weierstrass equation at $p = \ell$, and so the reduction of $E$ modulo $\ell$ can be expressed by means of the equation obtained reducing the coefficients in Equation (1.11). Hence Proposition 1.13 assures us that $E$ has good supersingular reduction at $\ell$.

□

Note that this theorem gives an explicit construction of infinitely many semistable elliptic curves with good supersingular reduction at the prime $\ell$.

Thus as a consequence of Theorem 1.3 and Theorem 1.19, we are able to state the following result.

**Theorem 1.20.** *For each prime number $\ell \geq 11$, there exists an elliptic curve $E/\mathbb{Q}$ such that the Galois extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified with Galois group* $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Note that Theorem 1.19 gives us infinitely many tamely ramified Galois extensions $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$.

## 1.4 Explicit construction for small primes

Theorem 1.19 allows us to obtain tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ provided $\ell \geq 11$. To complete this result, we can take specific curves that yield tame Galois realizations when $\ell = 2, 3, 5$ and 7.

**Example 1.21.**

- $\ell = 2$: The curve $19A3$ of Cremona's Tables [18] is semistable, has good supersingular reduction at 2, and the Galois representation attached to its group of 2-torsion points is surjective (cf. [66], Theorem 3.2).
- $\ell = 3$: The curve $17A1$ of Cremona's Tables [18] is semistable, has good supersingular reduction at 3, and the Galois representation attached to its group of 3-torsion points is surjective (cf. [66], Theorem 3.2).
- $\ell = 5$: The curve $14A1$ of Cremona's Tables [18] is semistable, has good supersingular reduction at 5, and the Galois representation attached to its group of 5-torsion points is surjective (cf. [66], Theorem 3.2).
- $\ell = 7$: The curve $15A1$ of Cremona's Tables [18] is semistable, has good supersingular reduction at 7, and the Galois representation attached to its group of 7-torsion points is surjective (cf. [66], Theorem 3.2).

In order to make our result completely satisfactory, we would like to be able to construct infinitely many elliptic curves which provide tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$, for each of the primes $\ell = 2, 3, 5, 7$. Of course, the main difference with regard to the previous section is that we cannot use Theorem 1.2 to prove surjectivity. Fortunately we shall be able to use some tricks, which shall depend on the value of $\ell$. Moreover, we shall rely on the examples presented above. First

of all, we will go through the four cases $\ell = 2, 3, 5, 7$ and show some conditions that ensure that the corresponding Galois representation is surjective and has good supersingular reduction at the prime $\ell$. At the end of the section we will explain how to construct elliptic curves which are semistable and, at the same time, satisfy the conditions we required.

### The prime $\ell = 2$

Let $E/\mathbb{Q}$ be an elliptic curve. The image of the Galois representation attached to the 2-torsion points of $E$ can be specified in terms of the discriminant and the rational 2-torsion points of $E$ (see Proposition 2.1 of [66] and § 5.3 of [77]). More precisely, the image of $\varphi_2$ is $\mathrm{GL}_2(\mathbb{F}_2)$ if and only if $E(\mathbb{Q})[2] = \{O\}$ and $\Delta_E$ is not a square.

Consider the curve 19A3 of Cremona's Tables [18], given by the equation

$$y^2 + y = x^3 + x^2 + x. \tag{1.12}$$

Let us change variables in order to obtain an equation of the shape $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, where the $b_i$ are obtained as usual from the coefficients $a_i$ of the original equation (see for instance [77], beginning of § 5). In this case, we apply the change of variables $y \mapsto \frac{1}{2}(y-1)$ and obtain the new equation

$$y^2 = 4x^3 + 4x^2 + 4x + 1.$$

The polynomial $4x^3 + 4x^2 + 4x + 1$ is irreducible modulo 5, and its discriminant is not a square modulo 3. Therefore, any elliptic curve $E$ given by an equation which is congruent to (1.12) modulo 3 and 5 will satisfy that the Galois representation attached to its 2-torsion points is surjective. Moreover, if the equation of $E$ is congruent to (1.12) modulo 2, its reduction (modulo 2) shall be given by $y^2 + y = x^3 + x^2 + x$, and therefore will be supersingular at 2.

### The prime $\ell = 3$

For this case, we will make use of the following result (see [66], Theorem 2.3-(iii)):

**Theorem 1.22.** *Let $E/\mathbb{Q}$ be an elliptic curve given by the equation*

$$y^2 = 4x^3 - g_2x - g_3, \tag{1.13}$$

*and let* $\Psi_3^E = 3x^4 - \frac{3}{2}g_2x^2 - 3g_3x - \frac{1}{16}g_2^2$. *Assume that* $\Psi_3^E$ *has no rational roots and the discriminant of* (1.13) *is not a cube. Then the Galois representation attached to the* 3*-torsion points of* $E$ *is surjective.*

Let us consider the curve 17A1 of Cremona's Tables [18], which is given by the equation $y^2 + xy + y = x^3 - x^2 - x - 14$. If we make the change of variables $y \mapsto \frac{1}{2}(y - x - 1)$, we obtain the equation $y^2 = 4x^3 - 3x^2 - 2x - 55$. In order to adjust it to the shape of the equation in the theorem, we must still make another change of variables, $x \mapsto x + \frac{1}{4}$, and we get

$$y^2 = 4x^3 - \frac{11}{4}x - \frac{445}{8}. \tag{1.14}$$

The discriminant of the polynomial $P(x) = 4x^3 - \frac{11}{4}x - \frac{445}{8}$ is $-1336336$, which is not a cube modulo 19.

On the other hand, the polynomial $\Psi_3^E = \frac{-121}{256} - \frac{1335}{8}x - \frac{33}{8}x^2 + 3x^4$ is irreducible modulo 5.

Therefore, any elliptic curve $E$ given by an equation congruent to (1.14) modulo 3, 5 and 19 satisfies that the Galois representation attached to the 3-torsion points is surjective. Moreover, its reduction at the prime $\ell = 3$ is supersingular.

### The prime $\ell = 5$.

In this case we will make use of the following result (see Proposition 19 of [77]).

**Proposition 1.23.** *Let* $\ell \geq 5$ *and let* $G$ *be a subgroup of* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *which contains three elements* $s, s', s''$ *satisfying the following properties:*

1. $\mathrm{tr}(s)^2 - 4\det(s)$ *is a non-zero square in* $\mathbb{F}_\ell$ *and* $\mathrm{tr}(s) \neq 0$.
2. $\mathrm{tr}(s')^2 - 4\det(s')$ *is not a square in* $\mathbb{F}_\ell$ *and* $\mathrm{tr}(s') \neq 0$.
3. *Let* $u = \mathrm{tr}(s'')^2/\det(s'')$. *Then* $u \neq 0, 1, 2, 4$ *and it satisfies that* $u^2 - 3u + 1 \neq 0$.

*Then* $G$ *contains* $\mathrm{SL}_2(\mathbb{F}_\ell)$. *In particular, if* $\det|_G$ *is surjective, then* $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Therefore, since we know that the representation $\varphi_\ell$ attached to the $\ell$-torsion points of an elliptic curve $E$ satisfies that $\det \varphi_\ell$ is the cyclotomic character, which is surjective, the previous proposition tells us that it suffices to find three elements $s, s', s''$ in $\mathrm{Im}(\varphi_\ell)$ satisfying the conditions above in order to prove that $\varphi_\ell$ is surjective.

Let us consider the curve 14A1 of Cremona's Tables [18], which is given by the equation

$$y^2 + xy + y = x^3 + 4x - 6. \tag{1.15}$$

We already know that the Galois representation $\varphi_5$ attached to the 5-torsion points of this curve is surjective. Therefore, it contains all the elements in $\mathrm{GL}_2(\mathbb{F}_5)$. In particular, it will contain three elements $s, s', s''$ satisfying the conditions of the proposition above. We are going to pick three such elements. To do so, we will look for primes $p$ where our elliptic curve has good reduction, and see whether the image of the Frobenius element at $p$ satisfies the conditions of the proposition.

- Let $p = 13$, and take $s = \varphi_5(\mathrm{Frob}_{13})$. We can check that $\mathrm{tr}(s) = 1 \neq 0$ and $\mathrm{tr}(s)^2 - 4\det(s) = 4$, which is a nonzero square in $\mathbb{F}_5$.
- Let $p = 3$, and take $s' = \varphi_5(\mathrm{Frob}_3)$. Then one can see that $\mathrm{tr}(s') = 3 \neq 0$ and $\mathrm{tr}(s')^2 - 4\det(s') = 2$, which is not a square in $\mathbb{F}_5$.
- Let $p = 3$ again, and call $s'' = \varphi_5(\mathrm{Frob}_3)$. One can check that $u(s'') = \mathrm{tr}(s'')^2/\det(s'') = 3$ and furthermore $u(s'')^2 - 3u(s'') + 1 = 1 \neq 0$.

Therefore, if we take any elliptic curve given by an equation congruent to (1.15) modulo 3, 5 and 13, we shall have that the Galois representation attached to the 5-torsion points of $E$ is surjective, and moreover the reduction at the prime 5 is supersingular.

### The prime $\ell = 7$

In this case we will proceed as above: we will use Proposition 1.23 in order to ensure surjectivity. Let us consider the curve 15A1 of Cremona's Tables [18], given by the equation

$$y^2 + xy + y = x^3 + x^2 - 10x - 10. \tag{1.16}$$

We know already that the Galois representation $\varphi_7$ attached to the 7-torsion points of this curve is surjective. Now we will look for primes $p$ of good reduction such that the image of the Frobenius at $p$ satisfies the conditions of Proposition 1.23.

- Let $p = 13$, and call $s = \varphi_7(\mathrm{Frob}_{13})$. It is easily verified that $\mathrm{tr}(s) = 5 \neq 0$ and $\mathrm{tr}(s)^2 - 4\det(s) = 1$, which is a nonzero square in $\mathbb{F}_7$.

- Let $p = 17$, and let $s' = \varphi_7(\mathrm{Frob}_{17})$. One can check that $\mathrm{tr}(s') = 2 \neq 0$ and $\mathrm{tr}(s')^2 - 4\det(s') = 6$, which is not a square in $\mathbb{F}_7$.

- Let $p = 13$, and call $s'' = \varphi_7(\mathrm{Frob}_{13})$. Then one can see that $u(s'') = \mathrm{tr}(s'')^2/\det(s'') = 3$ and $u(s'')^2 - 3u(s'') + 1 = 1 \neq 0$.

Therefore, if we take any elliptic curve $E$ given by an equation which is congruent to (1.16) modulo 7, 13 and 17, we shall have that the Galois representation attached to the 7-torsion points of $E$ is surjective, and furthermore it has good supersingular reduction at 7.

### Semistability

According to the previous paragraphs, given $\ell = 2, 3, 5$ or 7 we already can construct elliptic curves $E$ such that the Galois representation attached to the $\ell$-torsion points of $E$ is surjective, and the reduction of $E$ at $\ell$ is good and supersingular. We can achieve this by asking an equation defining $E$ to be congruent coefficientwise with the equations of the elliptic curves that we considered in Example 1.21, modulo a few suitable primes. What remains to be done is to show that, furthermore, we can choose these elliptic curves in such a way that they are semistable. Note that all the elliptic curves which appeared in Example 1.21 are semistable.

In order to settle the question, it will suffice to solve the following problem:

> Let us consider a semistable elliptic curve $E$, given by a minimal Weierstrass equation
>
> $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1.17)$$

and a set of primes $p_1, \ldots, p_r$ together with certain exponents $e_1, \ldots, e_r$. Can we construct infinitely many semistable elliptic curves defined by equations

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

satisfying that $a_i \equiv a_i'$ modulo $p_1^{e_1}, \ldots, p_r^{e_r}$?

Let us choose $a_i' = a_i$, $i = 1, \ldots, 4$, and leave $a_6'$ as a parameter. Since $c_4' = ({a_1'}^2 + 4a_2')^2 - 24(2a_4' + a_1'a_3')$ does not depend on $a_6'$, it is a fixed, concrete value (as a matter of fact, $c_4' = c_4$). Let $q_1, \ldots, q_s$ be the prime numbers which divide $c_4$. Our problem boils down to finding an infinite quantity of values of $a_6'$ which are congruent to $a_6$ modulo $p_1^{e_1}, \ldots, p_r^{e_r}$, and furthermore satisfying that

$$\begin{aligned}\Delta' = &-8(a_1'a_3' + 2a_4')^3 + 9({a_1'}^2 + 4a_2')(a_1'a_3' + 2a_4')({a_3'}^2 + 4a_6') \\ &-27({a_3'}^2+4a_6')^2-({a_1'}^2+4a_2')^2(-a_1'a_3'a_4'-{a_4'}^2+{a_1'}^2a_6'+a_2'({a_3'}^2+4a_6'))\end{aligned}$$

is not divisible by $q_1, \ldots, q_s$.

But note that the discriminant of equation (1.17) is not divisible by $q_1, \ldots, q_s$, since the initial elliptic curve $E$ is semistable (and the initial Weierstrass equation is minimal at all primes). Therefore it suffices to choose $a_6'$ so that it is congruent to $a_6$ modulo $q_1, \ldots, q_s, p_1^{e_1}, \ldots, p_r^{e_r}$.

In this way we obtain infinitely many different equations. And if we look at the expression of the $j$-invariant $j = c_4^3/\Delta$, it is clear that in fact we obtain infinitely many different elliptic curves (for the invariant $c_4$ is the same for all the curves, so if $\Delta$ differs, the $j$-invariant changes. And the discriminant $\Delta$ is a quadratic polynomial in $a_6$, with nonzero leading term).

## 1.5 Examples

The aim of this section is to display a few examples of elliptic curves, obtained by the method we have presented, which provide a tame Galois realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for several prime numbers $\ell$.

**Example 1.24.** Let us consider the prime $\ell = 11$. Since $11 = 4 \cdot 2 + 3$, we can make use of Proposition 1.17. That is to say, we must pick $\lambda \in \mathbb{Z}$ such that $\lambda \equiv -1 \pmod{11}$ and $\lambda \equiv 1 \pmod{16}$. The smallest

positive integer satisfying these conditions is $\lambda = 65$. Hence the curve $E$ defined by the equation

$$y^2 = x(x-1)(x-65) \tag{1.18}$$

is a semistable elliptic curve and has good supersingular reduction at $\ell = 11$.

Indeed, this curve is the one labeled 130B2 in Cremona's Tables [18]; it is therefore semistable (its conductor equals $2 \cdot 5 \cdot 13$) and we can easily check that the reduction at 11 is supersingular.

The Galois extension $\mathbb{Q}(E[11])/\mathbb{Q}$ yields a tame realization of the group $\mathrm{GL}_2(\mathbb{F}_{11})$ as Galois group over $\mathbb{Q}$.

**Example 1.25.** Let us consider the prime $\ell = 13$. According to Theorem 1.19, the first step is to find $a$. We compute the Deuring polynomial,

$$H_{13}(x) = (x^2 + 4x + 9)(x^2 + 7x + 1)(x^2 + 12x + 3).$$

Since the factor $x^2 + 12x + 3$ divides $H_{13}(x)$, we may take $a = 3$.

Therefore, we have to select $b, c, d \in \mathbb{Z}$ such that $\gcd(b - c, d) = 1$, $b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$, $b \equiv c + 11 \pmod{13}$, $d \equiv 11 \pmod{13}$.

For instance, we may take $c = -4$, $b = 267$, $d = 960$, and the elliptic curve $E$ we obtain is

$$y^2 = x^3 - 259x^2 - 1160x - 260592. \tag{1.19}$$

This is a semistable elliptic curve (its conductor is $N = 3 \cdot 5 \cdot 47 \cdot 1583$), and it has good supersingular reduction at 13.

Now we can claim that the Galois extension $\mathbb{Q}(E[13])/\mathbb{Q}$ gives rise to a tame realization of $\mathrm{GL}_2(\mathbb{F}_{13})$ as Galois group over $\mathbb{Q}$.

**Example 1.26.** Let us consider the prime $\ell = 17$. First of all, we must find a value for $a$ (cf. Theorem 1.19). Computing the Deuring polynomial, we obtain

$$H_{17}(x) = (x^2 + x + 16)(x^2 + 14x + 1)(x^2 + 16x + 1)(x^2 + 16x + 16).$$

Both factors $x^2 + 16x + 1$ and $x^2 + 16x + 16$ divide $H_{17}(x)$, so we can take either $a = 1$ or $a = -1$. Let us pick $a = -1$.

Therefore, we have to select $b, c, d \in \mathbb{Z}$ such that $\gcd(b - c, d) = 1$, $b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$, $b \equiv c - 5 \pmod{17}$, $d \equiv -5 \pmod{17}$.

For example, let us choose $c = -4$, $b = 1419$, $d = 1984$. We obtain the elliptic curve $E$ defined by

$$y^2 = x^3 - 1411x^2 - 9352x - 2838000. \tag{1.20}$$

This is a semistable elliptic curve (its conductor is $N = 7 \cdot 31 \cdot 289559$), and it has good supersingular reduction at 17.

The Galois extension $\mathbb{Q}(E[17])/\mathbb{Q}$ provides a tame realization of $\mathrm{GL}_2(\mathbb{F}_{17})$ as Galois group over $\mathbb{Q}$.

# Chapter 2

# Towards a generalization with base field $\mathbb{F}_{\ell^r}$

## 2.1 Elliptic curves and modular forms.

In the previous chapter we dealt with the problem of realizing the group $\mathrm{GL}_2(\mathbb{F}_\ell)$ as the Galois group of a tamely ramified extension of $\mathbb{Q}$, for every prime $\ell$. We tackled this problem by making use of the Galois representations attached to the $\ell$-torsion points of elliptic curves. Throughout this dissertation, we will take this result as our starting point and try to generalize it in several ways. More precisely, in this chapter we will replace elliptic curves with modular forms, in order to obtain tame Galois realizations of groups of the families $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ and $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ (cf. [23]).

First of all, let us explain how a modular form may help us in our task. Modular forms are holomorphic functions defined on the upper half plane $\mathfrak{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$, which satisfy certain symmetry relations. How can they provide an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on some arithmetic-geometric object?

In this chapter, we will consider modular forms with respect to the congruence subgroup $\Gamma_0(N)$, for some positive integer $N$. That is to say, the symmetries of the modular forms will be subject to the subgroup

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N|c\}.$$

Moreover, we will be concerned only with modular forms of weight two. In other words, the symmetries that a modular form $f$ shall

satisfy are given by

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

A holomorphic function on $\mathfrak{H}$ satisfying the condition above will be called a *modular form* if, in addition, it is "holomorphic at the cusps". We will not explain this hypothesis in detail, but refer the reader to [22], Definition 1.2.3. In particular, this condition implies that the modular form has a Fourier expansion at each cusp. If the independent term is zero for all these expansions, we will say that the modular form vanishes at the cusps, or, in short, that it is *cuspidal*. We will denote by $S_2(N)$ the set of cuspidal modular forms with respect to $\Gamma_0(N)$ and weight 2. This set is in fact a complex vector space, and it can be proved that its dimension is finite (see [22], Chapter 3).

For each natural number $n$, there is an operator $T_n : S_2(N) \to S_2(N)$, called the $n$-th Hecke operator (see [19], Chapter 1, § 3 for a definition). It can be proven that any two Hecke operators commute, that is to say, $T_n \circ T_m = T_m \circ T_n$ for all $n, m \in \mathbb{N}$. We will call $\mathbb{T}$ the subring of the ring of endomorphisms of $S_2(N)$ generated by the set $\{T_n : n \in \mathbb{N}\}$. Of particular interest will be the cuspidal modular forms that are eigenvectors for all the Hecke operators. Let us write the Fourier expansion of $f$ at $i\infty$ as

$$f(z) = \sum_{n \in \mathbb{N}} a_n e^{2\pi i n z}$$

Then if $f$ is an eigenvector for the Hecke operator $T_n$, say with eigenvalue $\lambda_n$, one can prove that from the formula $T_n f = \lambda_n \cdot f$ it follows that $a_n = \lambda_n \cdot a_1$. Assume that $f$ is a non-zero eigenvector for all the Hecke operators, and multiply it by $a_1^{-1}$ (if $a_1 = 0$, then all the $a_n$ would be compelled to vanish because of the relation $a_n = \lambda_n \cdot a_1$, so that $f$ would be zero). Then the Fourier coefficients of this modular form are precisely the different eigenvalues. We will say that $f$ is an *eigenform* if it is a non-zero cuspidal modular form which is an eigenvector for all Hecke operators, and we will always assume that $a_1 = 1$ (multiplying it if necessary by $a_1^{-1}$). The field generated over $\mathbb{Q}$ by adding all the Fourier coefficients, say $\mathbb{Q}_f = \mathbb{Q}[\{a_n\}_{n \in \mathbb{N}}]$, turns out to be a number field, which will play an important role in what follows (see Definition 6.5.3 of [22]).

On the other hand, in this setting it is natural to consider the modular curve $X_0(N)$, defined as the quotient of $\mathfrak{H}$ by $\Gamma_0(N)$, and

compactified by adding the cusps (see [22], chapter 2). Thus defined, this is a compact Riemann surface (over the complex numbers). But it turns out that it has a model defined over $\mathbb{Q}$. (This is a non-trivial fact. The proof relies on the fact that we can look at the quotient space $\mathfrak{H}/\Gamma_0(N)$ from a completely different point of view, namely, as the moduli space of elliptic curves with some extra structure. See [22], chapter 1, § 1.5). Furthermore, one might consider its Jacobian, denoted by $J_0(N)$. This is an abelian variety of dimension equal to the genus of $X_0(N)$. It can also be defined over $\mathbb{Q}$.

Now the point is that a construction due to Shimura allows one to attach an abelian variety $A_f$ to each eigenform. This abelian variety $A_f$ is defined as a quotient of $J_0(N)$, and also has a model over $\mathbb{Q}$. The dimension of $A_f$ is equal to the degree $r = [\mathbb{Q}_f : \mathbb{Q}]$. (The details of the construction can be looked up in [19], chapter 1, § 1.7). It is at the torsion points of this variety that we shall find a Galois representation. If we fix a prime $\ell$, we can consider, as in Section 1.1, the points of $\ell$-torsion of $A_f$. This set is a group, isomorphic to $(\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z})^r$. But this time the $\ell$-torsion points of $A$ will not suffice. For each $n$, we will consider the points of $\ell^n$-torsion of $A$, and take the inverse limit:

$$T_\ell(A_f) = \varprojlim_{n \in \mathbb{N}} A_f[\ell^n]$$

This is the Tate module, which is a $\mathbb{Z}_\ell$-module of rank $2r$. The action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\ell^n$-torsion points of $A_f$ extends to an action on the Tate module, giving rise to a Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, T_\ell(A_f) \simeq \mathrm{GL}_{2r}(\mathbb{Z}_\ell)$$

On the other hand, the relationship between $S_2(N)$ and $X_0(N)$ allows one to carry the action of the Hecke operators to $J_0(N)$. In turn, the abelian variety $A_f$ also inherits a certain action: the algebra $\mathbb{T}$ maps to a subring of $\mathrm{End}_{\mathbb{Q}}(A_f)$. More precisely, consider the map from $\mathbb{T}$ to $\mathbb{Q}_f$ defined by $T_n \mapsto a_n$ (that is to say, it attaches to each Hecke operator its eigenvalue). The image of this map is an order $H_f$ inside the ring of integers $\mathcal{O}_f$ of $\mathbb{Q}_f$, which can be viewed inside $\mathrm{End}_{\mathbb{Q}}(A_f)$. Furthermore, the action of the ring $H_f$ on $A_f$, induces an action of $H_{f,\ell} := H_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ in $\mathbb{T}_\ell(A_f)$, thus endowing it with a structure of $H_{f,\ell}$-module.

By tensoring everything by $\mathbb{Q}_\ell$, we will obtain an $\ell$-adic representation. Namely, call $\mathbb{Q}_{f,\ell} = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. We obtain that the $\mathbb{Q}_\ell$-vector

space $V_\ell(A_f)$ defined as $T_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has a structure of $\mathbb{Q}_{f,\ell}$-module. Moreover, one can prove that in fact $V_\ell(A_f)$ is a free module of rank 2 over this ring. Besides, this structure is compatible with the action of the elements of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In other words, if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $a \in \mathbb{Q}_{f,\ell}$ and $t \in T_\ell(A_f)$, then $\rho(\sigma)(a \cdot t) = a \cdot \rho(\sigma)(t)$. Therefore, fixing a $\mathbb{Q}_{f,\ell}$-base of $V_\ell(A_f)$, the representation $\rho$ above is remodeled into

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_{f,\ell}).$$

We can go one step further, and consider a prime $\lambda$ of $\mathbb{Q}_f$ above $\ell$. Since $\mathbb{Q}_{f,\ell}$ is the direct sum of the completions of $\mathbb{Q}_f$ at the different primes above $\ell$, taking the part corresponding to $\lambda$ we obtain a representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_{f,\lambda}),$$

where $\mathbb{Q}_{f,\lambda}$ is the completion of $\mathbb{Q}_f$ at the prime $\lambda$.

The relationship between this Galois representation and the modular form $f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$ we started with is made very explicit in the following way. Let us consider a prime number $p$ which does not divide the level $N$. Then the abelian variety $A_f$ has good reduction at $p$. Moreover, if $p \nmid \ell \cdot N$, then $\rho_{f,\lambda}$ is unramified at $p$, and the characteristic polynomial of the image of the Frobenius element at $p$, $\rho_{f,\lambda}(\mathrm{Frob}_p)$, is precisely $X^2 - a_p X + p$ (see Theorem 3.1, pg. 85 of [19]).

**Remark 2.1.** Since we will only deal with modular forms of weight 2, we have briefly outlined the classical construction, due to Shimura, of the Galois representation attached to a modular form. Further, we have left aside the modular forms with character, but this is not an essential restriction, and we did it only with the intention to simplify the presentation. In general, when the weight is $k > 1$, a result of Deligne [20] allows one to attach a Galois representation $\rho_{f,\ell}$ to a modular form $f$. When $k = 1$, the existence of the $\rho_{f,\ell}$ is proven by Deligne and Serre [21].

As a matter of fact, we did not intend to obtain a $\lambda$-adic representation, but a representation over a finite field. Therefore, we will consider the composition of $\rho_{f,\lambda}$ with the reduction modulo $\lambda$ on $\mathbb{Q}_{f,\lambda}$. In this way, we obtain a representation

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

Let us step back for a while and return to the point before we tensored by $\mathbb{Q}_\ell$. We had endowed the Tate module $T_\ell(A_f)$ with a structure of $H_{f,\ell}$-module. Now the index $(\mathcal{O}_f : H_f)$ is a finite number. If $\ell$ does not divide this index, then it is easy to see that from the fact that $V_\ell(A_f)$ is a free $\mathbb{Q}_{f,\ell}$-module of rank two, it follows that $T_\ell(A_f)$ is a free $H_{f,\ell}$-module of rank two. We will assume that $\ell \nmid (\mathcal{O}_f : H_f)$. Therefore, fixing a base of $T_\ell(A_f)$ as $H_{f,\ell}$-module, we obtain a representation

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(H_{f,\ell}) \subset \mathrm{GL}_2(\mathbb{Q}_{f,\ell}).$$

It can be proven that the determinant of the representation $\rho_{f,\ell}$ is equal to the cyclotomic character (see Proposition (2.2) of [67]). Therefore, the image of $\rho_{f,\ell}$ lies in

$$A_\ell = \{x \in \mathrm{GL}_2(H_{f,\ell}) : \det(x) \in \mathbb{Z}_\ell^*\}.$$

But is it possible to write a more precise statement?

First of all, we need to recall a couple of new concepts. On the one hand, from now on we will only consider modular forms $f \in S_2(N)$ which are *newforms* (the definition can be looked up in [19], Definition 1.21; in particular newforms are normalized eigenforms). On the other hand, recall that the notion of complex multiplication was essential in order to formulate a result about the image of the Galois representation attached to the $\ell$-torsion points of an elliptic curve. In our current setting, we also need to take this into account. More precisely, the definition of newform with complex multiplication is as follows (see [67], § 3): a newform $f$ has *complex multiplication* by a non-trivial Dirichlet character $\phi$ if, for all primes $p$ contained in a set of primes of density one, it holds that $\phi(p)a_p = a_p$. This kind of newforms shall have to be excluded when we formulate our result. But it will not be enough to exclude them; we must also take non-trivial inner twists into account. A newform $f$ has an *inner twist* by a Dirichlet character $\chi$ if there exists an embedding $\gamma : \mathbb{Q}_f \to \overline{\mathbb{Q}}$ such that $\gamma(a_p) = \chi(p)a_p$ for all but finitely many primes $p$ (see [68]).

When $f \in S_2(N)$ is a newform, a result of Ribet tells us that for all sufficiently large primes $\ell$ the image of $\rho_{f,\ell}$ coincides with $A_\ell$, provided that $f$ does not have complex multiplication or non-trivial inner twists (see Theorem 3.1 of [69]).

Now that we have a precise result about the image of the representation, we wish to carry out the reduction modulo $\ell$. Call $\mathcal{O}_{f,\ell} =$

$\mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Note that, since we are assuming that $\ell \nmid (\mathcal{O}_f : H_f)$, then $H_{f,\ell} \simeq \mathcal{O}_{f,\ell}$. Let $\lambda$ be any prime ideal of $\mathcal{O}_f$ above $\ell$, and call $\mathbb{F}_\lambda$ the residue field $\mathcal{O}_f/\lambda\mathcal{O}_f$. The following result follows from all the previous considerations (cf. [23], Theorem 2.2).

**Theorem 2.2.** *Let $f \in S_2(N)$ be a newform without complex multiplication or non-trivial inner twists. For all but finitely many primes $\ell$, the image of $\overline{\rho}_{f,\lambda}$ coincides with $\{x \in \mathrm{GL}_2(\mathbb{F}_\lambda) : \det(x) \in \mathbb{F}_\ell^*\}$.*

In order to get rid of the condition on the determinant above, we may consider the projection of the image inside the projective space, that is to say, we can compose $\overline{\rho}_{f,\ell}$ with the map $\mathrm{GL}_2(\mathbb{F}_\lambda) \to \mathrm{PGL}_2(\mathbb{F}_\lambda)$. The theorem above yields the following result:

**Corollary 2.3.** *Let $f \in S_2(N)$ be a newform without complex multiplication or non-trivial inner twists, and call $r$ the degree of the extension $\mathbb{F}_\lambda/\mathbb{F}_\ell$. For all but finitely many primes $\ell$, 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.*

*Proof.* The image of $\{x \in \mathrm{GL}_2(\mathbb{F}_{\ell^r}) : \det(x) \in \mathbb{F}_\ell^*\}$ through the projection $\mathrm{GL}_2(\mathbb{F}_{\ell^r}) \to \mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ is $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ if $r$ is even and $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ if $r$ is odd, according to Lemma 2.2 of [64]. □

At this point, it is already perceptible how the representations attached to modular forms generalize those considered in Chapter 1, as was claimed at the beginning of this section. Namely, let $f \in S_2(N)$ be a newform, and assume that the coefficient field $\mathbb{Q}_f$ coincides with $\mathbb{Q}$. In this situation, the abelian variety $A_f$ attached to $f$ has dimension $r = [\mathbb{Q}_f : \mathbb{Q}] = 1$, and is therefore an elliptic curve. Thus the Galois representation attached to the Tate module $T_\ell(E)$ has already been considered in Section 1.1. What does Theorem 2.2 tell us in this case? If we have a newform with rational Fourier coefficients and without complex multiplication, then the corresponding elliptic curve has no complex multiplication, and the result of Serre (Theorem 1.1) assures us that, for all but finitely many primes $\ell$, the image of the corresponding Galois representation equals $\mathrm{GL}_2(\mathbb{F}_\ell)$. To sum up, any Galois representation we obtain in this way could have been accomplished by the reasonings described in Chapter 1. Our aim now is to consider modular forms such that the corresponding abelian variety $A_f$ is not an elliptic curve, and in this way to generalize the techniques used in Chapter 1. There are two points which have to be settled, namely, to ensure that the ramification of the corresponding

extension is tame, and to guarantee that the image of the representation is as large as possible. The two following sections will deal with these points.

## 2.2 Ramification of the Galois representation attached to a modular form

Let $f \in S_2(N)$ be a newform without complex multiplication or non-trivial inner twists. In the previous section we saw how to attach to $f$ a Galois representation

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

Our aim in this section is to find conditions on $f$ which ensure that the ramification of the Galois extension that one obtains from $\overline{\rho}_{f,\ell}$ is tame. More precisely, we need to ensure that the image of the wild inertia group $I_{p,\mathrm{w}}$ by $\overline{\rho}_{f,\ell}$ is trivial, for all prime numbers $p$. We will split the section into two parts: in the first one, we will consider the primes $p \neq \ell$, and in the second one we will deal with the prime $p = \ell$.

- $p \neq \ell$

Given a continuous, odd, irreducible Galois representation

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

there is a way to measure the ramification away from $\ell$. In [79], 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 $\varepsilon(\overline{\rho}_\ell)$. In this section we are interested in the conductor $N(\overline{\rho}_\ell)$, because it 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 [79], § 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 $w$. 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

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

$$I_p = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_i \supset \cdots . \tag{2.1}$$

Note that the second group of this sequence, $G_1$, is already known to us: it coincides with the wild inertia group at $p$, $I_{p,\mathrm{w}}$.

Let $V$ be a 2-dimensional vector space over $\overline{\mathbb{F}}_\ell$, and consider the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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

$$n(p) = \sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{(G_0 : G_i)}, \tag{2.2}$$

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 2.4.** 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 (2.2).

Let $p$ be a prime number different from $\ell$. There exists a certain $s \in \mathbb{N}$ such that

$$n(p) = \dim(V/V_0) + \frac{\dim(V/V_1)}{(G_0 : G_1)} + \cdots + \frac{\dim(V/V_s)}{(G_0 : G_s)}$$

Note that all the terms in the sum above are positive. Moreover, the fact that (2.1) is decreasing implies that

$$\dim V/V_0 \geq \dim V/V_1 \geq \cdots \geq \dim V/V_s$$

Therefore, if $n(p) = 1$, then 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 $V$. In other words, $\overline{\rho}_\ell$ is tamely ramified at $p$. 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 the modular form $f \in S_2(N)$ we considered at the beginning of the section. According to Serre's conjecture, $\overline{\rho}_{f,\ell}$ comes from a modular form $g$ of level $N(\overline{\rho}_\ell)$ (and weight $k(\overline{\rho}_\ell)$, character $\varepsilon(\overline{\rho}_\ell)$). But it may well be that $N \neq N(\overline{\rho}_\ell)$. Luckily, there is a strong relationship between the two values: thanks to the work of Carayol and Livné (cf. [13], remark following Theorem 1 and [49], Proposition 0.1), we know that $N(\overline{\rho}_\ell)$ divides $N$ (when $\overline{\rho}_{f,\ell}$ is irreducible). Therefore, if $N$ is squarefree, then $N(\overline{\rho}_\ell)$ has no choice but to be squarefree too, and we will be certain that the ramification of $\overline{\rho}_{f,\ell}$ is tame at all primes $p \neq \ell$. Let us write this statement as a Proposition.

**Proposition 2.5.** *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 $p \neq \ell$.*

- $p = \ell$

Now that we have dealt with all primes $p \neq \ell$, we address the problem of obtaining some control of the ramification at the prime $\ell$. In the case of elliptic curves, this was achieved by asking the elliptic curve to have good supersingular reduction at $\ell$. 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 [70], Chapter 2, § 2.1). We will define these notions in general, that is to say, for a cusp form $f$ of weight $k$, level $N$ and character $\varepsilon$ (that is to say, $f \in S_k(N, \varepsilon)$), since the results of this subsection hold in this general setting.

**Definition 2.6.** Let $f \in S_k(N, \varepsilon)$ be a newform, and call $a_p$ the eigenvalue corresponding to the Hecke operator $T_p$. Let $\ell$ be a prime number. Fix a homomorphism $\varphi$ from the ring of integers of $\mathbb{Q}_f$ to $\overline{\mathbb{F}}_\ell$, and let $\overline{\rho}_{f,\ell}$ be the Galois representation attached to $f$ using the reduction map $\varphi$. We will say that $\overline{\rho}_{f,\ell}$ is *ordinary at* $\ell$ if $\varphi(a_\ell) \neq 0$. Otherwise we will say that $\rho_{f,\ell}$ is *supersingular at* $\ell$. We will say that the newform $f$ is *supersingular* at $\ell$ if there exists a homomorphism $\varphi$ such that the corresponding Galois representation is supersingular.

Fontaine has studied the image by $\overline{\rho}_{f,\ell}$ of the inertia group at $\ell$ when $f$ is supersingular. The following theorem, which is Theorem 2.6 of [25], seems to have appeared in a letter from Fontaine to Serre.

**Theorem 2.7** (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 $\ell$. 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 $\psi$ and $\psi'$ are the two fundamental characters of level* 2*.*

In particular, this result tells us that the image of the wild inertia group at $\ell$, $\overline{\rho}_{f,\ell}(I_{\ell,\mathrm{w}})$, is trivial (any character of the inertia group $I_\ell$ acts trivially on the wild inertia group, cf. Proposition 4 of § 1.6 of [77]). Therefore we can write the following proposition.

**Proposition 2.8.** *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 $\ell$.*

## 2.3 The image of the Galois representation attached to a modular form

In the previous section we tackled the question of finding sufficient conditions that assure us that the Galois representation $\overline{\rho}_{f,\ell}$ attached to a newform $f$ is tamely ramified. Now it is time to consider the image of this representation. As we explained at the beginning of the chapter, for all but finitely many primes $\ell$ 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, as we pointed out, is similar to that

of Serre about the image of the Galois representations attached to the $\ell$-torsion points of elliptic curves. But in the context of elliptic curves, this result was not enough for us, since it does not tell us whether, for a given prime $\ell$, it falls into the set of primes with large image. We had to resort to a theorem of Mazur (see Theorem 1.2), which allowed us to replace the condition "for all but finitely many primes $\ell$" by "for all primes $\ell \geq 11$", provided we also asked 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. Namely, there is a result of L. Dieulefait and N. Vila (see [23]), which 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 $\ell$.

Their method relies on some results of Ribet (see [69]). More precisely, they make use of the following theorem (cf. § 3 of [69]).

**Theorem 2.9.** *Let $f \in S_2(N)$ be a newform with coefficient field $\mathbb{Q}_f$ and ring of integers $\mathcal{O}$, $\ell$ a prime number and $\lambda$ a prime of $\mathcal{O}$ above $\ell$. Call $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Let $\rho_{f,\lambda}$ the $\lambda$-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) $\ell$ 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 $x_\ell$ such that $(\operatorname{trace} x_\ell)^2$ 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 $\lambda$ is an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_\lambda)$ whose order is divisible by $\ell$.*

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 $\ell$, and such that the coefficient $a_p$ enjoys some

suitable property involving $\lambda$. 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 [23].

## 2.4 Some examples of tame Galois realizations

The aim of this section is to combine the results presented in the previous sections in order to obtain tame Galois realizations of linear groups of the form $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$. But, unfortunately, we have not been able to obtain a procedure that, given a prime number $\ell$, constructs a suitable modular form yielding a tame Galois realization of the corresponding group. Two issues are responsible for this:

1. We do not (yet) have a procedure to construct, given a prime number $\ell$, a modular form (without complex multiplication or non-trivial inner twists) which is supersingular at $\ell$.

2. We do not have a set of generic conditions such that, whenever they are satisfied by a modular form, we are assured that the image of the corresponding Galois representation is large.

Concerning the first issue, we have tried several approaches. Of course, it is well known how to construct a modular form with complex multiplication possessing a zero coefficient at a given prime. Unfortunately, the image the Galois representation attached to such a modular form is not large, so it does not serve our purposes. Among other attempts, we tried to use some results of raising the level, and also some strategies involving Eisenstein primes. None have borne fruit for the time being.

With regard to the second issue, the algorithm of Dieulefait and Vila, while very effective at discerning whether, for a given modular form $f$, the Galois representation at a prime $\ell$ has large image, it is quite rigid, in the sense that one needs to know many features of the modular form in advance. For instance, in several places one must have the exact value of the level $N$. On the other hand, in the context of elliptic curves, we applied a result of Mazur, which told us that if the conductor $N$ of an elliptic curve $E$ was squarefree and $\ell \geq 11$, then the Galois representation attached to $E$ at $\ell$ was surjective. This left us great flexibility to pick the elliptic curve $E$, thus allowing us to

impose other conditions (to control the image of the inertia group at $\ell$, mostly).

Therefore, we have not managed to give an algorithm to construct tamely ramified extensions with Galois group $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ for a certain $r$. This problem remains a challenging issue for further investigation. Nevertheless, the results we have explained allow us to present a few concrete examples.

In [23], 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 2.2) whenever $\ell$ does not belong to this set. We present their results in the following table:

Table 2.1: 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 $\ell$. In order to ensure that they are also tamely ramified at $\ell$, we will make use of Proposition 2.8.

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 $a_\ell$, 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 $\ell$ is inert in the extension $\mathbb{Q}_{f_i}/\mathbb{Q}$ and $a_\ell \in (\ell)$:

Table 2.2: Inert supersingular primes

| Modular Form | Primes $\ell$ |
|---|---|
| $f_1$ | 43, 1033 |
| $f_2$ | |
| $f_3$ | 173 |
| $f_4$ | 23, 31, 4391 |
| $f_7$ | 59, 149, 1709 |
| $f_8$ | 47, 4799 |

As a consequence of Propositions 2.5, 2.8 and Tables 2.1 and 2.2, we obtain the following result.

**Proposition 2.10.** *The following groups occur as Galois groups of a tamely ramified extension of* $\mathbb{Q}$*:*

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

# Part II

# Part II: Tame Galois Realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$

# Chapter 3

# Tame Galois representations attached to abelian varieties

## 3.1 Statement of the problem

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

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

attached to the $\ell$-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 chapter we are interested in finding conditions over the variety $A$ that ensure that $K/\mathbb{Q}$ is tamely ramified.

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 $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. 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. The condition that $K/\mathbb{Q}$ be tamely ramified means that the action of the wild inertia group is trivial, for every prime $p$. We will address the problem of finding conditions that assure us that the image of $I_{p,\mathrm{w}}$ by $\rho_\ell$ is trivial.

First of all, let us note that it suffices to control the image by $\rho_\ell$ of $I_{p,\mathrm{w}}$ just for a finite quantity of primes $p$. Indeed, $I_{p,\mathrm{w}}$ is a pro-$p$-

group, that is, each finite quotient has cardinal equal to a power of $p$. Therefore the cardinal of $\mathrm{Im}(I_{p,\mathrm{w}})$ is a power of $p$. But this image must be contained in $\mathrm{GL}_{2n}(\mathbb{F}_\ell)$. Yet this group is finite, and has cardinal equal to

$$\ell^{\frac{2n(2n-1)}{2}} \prod_{i=1}^{2n} (\ell^i - 1).$$

Therefore, if $p$ does not divide this quantity, the cardinal of $\mathrm{Im}(I_{p,\mathrm{w}})$ must be $p^0 = 1$. We thus see that in order to obtain that the Galois extension $K/\mathbb{Q}$ is tamely ramified, it suffices to take into account the primes $p$ which divide $\mathrm{card}(\mathrm{GL}_{2n}(\mathbb{F}_\ell))$.

When the prime $p$ is different from $\ell$, a sufficient condition to guarantee that $\rho_\ell(I_{p,\mathrm{w}})$ is trivial will be to require that the abelian variety has semistable reduction. However, the control of the image of $I_{\ell,\mathrm{w}}$ by $\rho_\ell$ will be much more subtle.

## 3.2 Semistable reduction and the action of the inertia group

Let $K$ be a number field, and let us consider an abelian variety $A/K$. Let us consider a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of $K$. In order to define what it means for $A$ to have good or semistable reduction at the prime $\mathfrak{p}$, it is convenient to introduce the notion of Néron model (see Definition 1 of § 1.2, Chapter 1 of [8]).

**Definition 3.1.** A *Néron model* of $A$ is a scheme $\mathcal{A}$ over $\mathrm{Spec}\,\mathcal{O}_K$ which is smooth, separated and of finite type, such that its generic fibre $\mathcal{A}_K$ is equal to $A$, and such that the following universal property is satisfied:

For each smooth scheme $\mathcal{Y}$ over $\mathrm{Spec}\,\mathcal{O}_K$ and for each $K$-morphism $u_K : \mathcal{Y}_K \to \mathcal{A}_K$, there is a unique morphism of schemes over $\mathrm{Spec}\,\mathcal{O}_K$, $u : \mathcal{Y} \to \mathcal{A}$, extending $u_K$.

It is well known that all abelian varieties over a number field admit a Néron model (see for instance [8], chap. 1, § 1.4, Theorem 3). Because of the universal property it satisfies, this model is unique.

Let us consider a prime $\mathfrak{p}$ of $\mathcal{O}_K$. The Néron model $\mathcal{A}$ of $A$ allows us to consider the reduction of $A$ at the prime $\mathfrak{p}$, simply by taking the special fibre of $\mathcal{A}$ at $\mathfrak{p}$, which shall be denoted by $\mathcal{A}_\mathfrak{p}$. This fibre is a scheme over the residue field $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. If it is smooth, we say that

$A$ has *good reduction* at the prime $\mathfrak{p}$. In our setting, this is equivalent to saying that $\mathcal{A}_\mathfrak{p}$ is an abelian variety over $k_\mathfrak{p}$ (cf. [36], § A.9.4).

Recall that the set of primes of $\mathcal{O}_K$ where the reduction of $A$ is not good is finite (see [8], Chapter 1, § 1.4, Theorem 3).

In general, the special fibre $\mathcal{A}_\mathfrak{p}$ is an algebraic group, but it need not be connected. However, we may consider the connected component of $\mathcal{A}_\mathfrak{p}$ that contains the identity element of $\mathcal{A}_\mathfrak{p}$, say $\mathcal{A}_\mathfrak{p}^0$. This is a connected algebraic group, and therefore (see Theorem 16 of [72]) it is the extension of an abelian variety by a linear group. That is to say, there exists an abelian variety $B$ and an algebraic linear group $L$ such that we have the following short exact sequence:

$$0 \to L \to \mathcal{A}_\mathfrak{p}^0 \to B \to 0.$$

Now let us focus on the structure of this linear group. Recall the following two notions:

**Definition 3.2.** Let $k$ be a field and $\overline{k}$ an algebraic closure of $k$.

- A *torus* over $k$ is an algebraic group over $k$ which is isomorphic over $\overline{k}$ to a power of the multiplicative group over $\overline{k}$, that is to say, to an algebraic group of the form $\mathbb{G}^r_{m,\mathrm{Spec}\,\overline{k}}$ for some $r \in \mathbb{N}$.
- A commutative algebraic group $G$ is *unipotent* if there exists an ascending chain of subgroups

  $$0 = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

  such that $G_{i+1}/G_i$ is isomorphic over $\overline{k}$ to the additive group $\mathbb{G}_{a,\mathrm{Spec}\,\overline{k}}$, for each $i \in \{0, \dots n-1\}$.

For a definition of the additive and multiplicative group, see [48], Examples 4.35 and 4.36 of Chapter 7.

Now the structure theorem for commutative linear algebraic groups is the following one (see [8], Theorem 2, § 9.2, Chapter 9):

**Theorem 3.3.** *Let $k$ be a perfect field and let $G$ be a smooth and connected algebraic group over $k$ of finite type. Assume that $G$ is commutative and linear. Then $G$ is canonically an extension of an unipotent algebraic group by a torus.*

We will be interested in the case where there is no unipotent part. The following definition can be found in [36], § A.9.4.

**Definition 3.4.** We will say that $A/K$ has *semistable reduction* at a prime $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ if the connected component of the special fibre of $A$ at $\mathfrak{p}$, $\mathcal{A}^0_{\mathfrak{p}}$, is the extension of an abelian variety by a torus. In other words, if there exists an abelian variety $B$ and a torus $T$ such that we have the following exact sequence

$$0 \to T \to A^0_{\mathfrak{p}} \to B \to 0.$$

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. Let $\ell$ be a prime number, different from the characteristic of the residual field $k_{\mathfrak{p}}$, and let us denote by $T_\ell(A)$ the Tate module of $A$ at $\ell$. Let us also denote by $I_{\mathfrak{p}} \subset \operatorname{Gal}(\bar{K}/K)$ the inertia group at the prime $\mathfrak{p}$.

The following well-known criterion gives us a characterization of good reduction at the prime $\mathfrak{p}$ (see [75], Theorem 1):

**Theorem 3.5** (Néron-Ogg-Shafarevich)**.** *Let $A/K$ be an abelian variety, and $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$. Let $\ell$ be a prime number, different from the characteristic of the residual field $k_{\mathfrak{p}}$. Then $A$ has good reduction at $\mathfrak{p}$ if and only if $I_{\mathfrak{p}}$ acts trivially on $T_\ell(A)$.*

Moreover, a result of Grothendieck characterizes the case when the reduction is semistable in terms of the action of the inertia group at $\mathfrak{p}$ (see [31], Proposition 3.5 of Exposé IX, *Modeles de Néron et monodromie*).

**Theorem 3.6** (Grothendieck)**.** *Let $A/K$ be an abelian variety, and $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$. Let $\ell$ be a prime number, different from the characteristic of the residual field $k_{\mathfrak{p}}$. Then the following assertions are equivalent:*

- *$A$ has semistable reduction at $\mathfrak{p}$.*
- *There exists a submodule $T' \subset T_\ell(A)$, which is stable under the action of $I_{\mathfrak{p}}$, and such that $I_{\mathfrak{p}}$ acts trivially on both $T'$ and $T_\ell(A)/T'$.*

Let us now return to the situation at the beginning of this chapter. We have an abelian variety $A/\mathbb{Q}$, and a prime $\ell$, and we are considering the Galois representation $\rho_\ell$ attached to the $\ell$-torsion points of $A$. Let $p \neq \ell$ be a prime number, and assume that $A$ has semistable reduction at $p$. Theorem 3.6 guarantees that $\rho_\ell(I_{\mathrm{w},p})$ is trivial. For it is clear

that it suffices to ensure that $I_{p,\mathrm{w}}$ acts trivially on $T_\ell(A)$. And the theorem claims the existence of 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 $T_\ell(A)/T'$. Choosing a suitable basis of $T_\ell(A)$, the action of $I_p$ has the following shape

$$\begin{pmatrix} \mathrm{Id}_r & * \\ 0 & \mathrm{Id}_s \end{pmatrix}.$$

But the order of such a matrix is a divisor of $\ell$. Since $I_{p,\mathrm{w}}$ is a pro-$p$-group, its elements cannot act by a matrix of order $\ell$, and therefore they all act as the identity.

Let us state this claim as a theorem:

**Theorem 3.7.** *Let $A/\mathbb{Q}$ be an abelian variety, and let $\ell, p$ 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 $\rho_\ell$ is trivial.*

The previous theorem gives us a sufficient condition for the representation $\rho_\ell$ to be tamely ramified at a prime $p \neq \ell$. The following chapters are devoted to developing a strategy that allows us to obtain sufficient conditions for the representation to be tamely ramified at $\ell$. Of course, we will want these conditions to be effective. Since we will be interested in the behaviour of $\rho_\ell$ at the prime $\ell$, we will for the time being work in a local setting.

# Chapter 4

# Supersingular abelian varieties and the action of the inertia group at $\ell$

In the previous chapter, we found a condition that suffices to guarantee that the image of the wild inertia group at a prime $p \neq \ell$ by the Galois representation attached to the $\ell$-torsion points of an abelian variety is trivial. In this chapter we will address this issue when the prime $p$ coincides with $\ell$. Since we are interested in the behaviour at the prime $\ell$, we will work in a local setting. Namely, let us consider a local field $K$ of characteristic zero and residual characteristic $\ell$. Let $v$ be the corresponding discrete valuation, normalized so that $v(K^*) = \mathbb{Z}$, and denote by $\mathcal{O}$ the ring of integers of the valuation and by $k$ the residue field. Further, we will assume that $v(\ell) = 1$ (that is to say, $K$ is an unramified extension of $\mathbb{Q}_\ell$). Let us also fix an algebraic closure $\overline{K}$ of $K$, and keep calling $v$ the extension of $v$ to this algebraic closure. $\overline{k}$ shall denote the algebraic closure of $k$ obtained through the reduction of $\mathcal{O}_{\overline{K}}$, the ring of integers of $\overline{K}$ with respect to $v$, modulo its maximal ideal. Finally, we will denote by $I$ and $I_{\mathrm{w}}$ the inertia group and the wild inertia group of $\mathrm{Gal}(\overline{K}/K)$.

First of all, we will recall how the point was settled in Chapter 1, where the abelian variety was an elliptic curve. Afterwards, we will try to find a way to extend this situation to the general case.

We will see that the first part of the reasoning for an elliptic curve extends beautifully to the general case. However, in order to complete our task, we need to make an extra assumption (see Hypothesis 4.7).

The result we obtain is the content of Theorem 4.9.

## 4.1 Supersingular elliptic curves and the action of the inertia group at $\ell$

Let $E/K$ be an elliptic curve with good supersingular reduction. Then the extension $K(E[\ell])/K$ obtained by adjoining to $K$ the coordinates of the points of $\ell$-torsion is tamely ramified. Serre explains this result in [77], § 1. Let us briefly review his reasoning.

Let $E/K$ be an elliptic curve with good reduction at $\ell$. Then the curve we obtain by reducing modulo the maximal ideal of the valuation ring, say $\widetilde{E}/k$, is also an elliptic curve. There is a short exact sequence of abelian groups

$$0 \to E_1(\overline{K}) \to E(\overline{K}) \to \widetilde{E}(\overline{k}) \to 0,$$

where $E_1(\overline{K})$ denotes the points of $E$ with coordinates in $\overline{K}$ which reduce to the neutral element of the group of points of $E$, and $E(\overline{K}) \to \widetilde{E}(\overline{k})$ is the reduction map.

If $\widetilde{E}/k$ is a supersingular elliptic curve, then it has no non-zero $\ell$-torsion points. Therefore, all the points of $\ell$-torsion of $E$ must belong to $E_1(\overline{K})$. Consequently, it suffices to study this group. It is at this point that the formal group associated to the elliptic curve $E$ turns out to be very fruitful for us.

Recall that to the elliptic curve $E/K$ one can attach a commutative formal group law also defined over $K$, that is to say, a formal power series $F(X,Y) \in \mathcal{O}[[X,Y]]$ satisfying the following three properties:

- $F(0,X) = X = F(X,0)$.
- $F(F(X,Y),Z) = F(X,F(Y,Z))$.
- $F(X,Y) = F(Y,X)$.

(see [84], Chapter IV, for a detailed study of this).

To this formal power series one can attach a group, whose elements are those elements of $\overline{K}$ with positive valuation. On this set, which we shall denote $\overline{\mathfrak{m}}$, one can define an addition law $\oplus_F$ by

$$x \oplus_F y := F(x,y),$$

(which is well-defined since $F(x, y)$ converges to an element of $\overline{\mathfrak{m}}$). The set $\overline{\mathfrak{m}}$, endowed with this sum, turns out to be a group, which shall be denoted by $F(\overline{\mathfrak{m}})$.

Now this group turns out to be very useful to us, because there is a group isomorphism between $E_1(\overline{K})$ and $F(\overline{\mathfrak{m}})$. When our elliptic curve $E$ has good supersingular reduction, all $\ell$-torsion points of $E$ lie in $E_1(\overline{K})$, and therefore they can be viewed inside $F(\overline{\mathfrak{m}})$. Moreover, if we call $V$ the $\mathbb{F}_\ell$-vector space of the $\ell$-torsion points of $F(\overline{\mathfrak{m}})$, it is not difficult to prove that $E[\ell]$ is isomorphic (as $\mathbb{F}_\ell$-vector space) to $V$.

Besides, the absolute Galois group of $K$ acts over $F(\overline{\mathfrak{m}})$; the action of an element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is simply $x \mapsto \sigma(x)$, for all $x \in \overline{\mathfrak{m}}$. The expression of the isomorphism between $E_1(\overline{K})$ and $F(\mathfrak{m})$, which we have not made explicit here (but see [84], Prop. 2.2 of Chapter VII), makes it clear that it respects the Galois action. Therefore, the study of the Galois representation attached to the group of $\ell$-torsion points of $E$ is equivalent to the study of the Galois representation attached to the $\ell$-torsion points of the formal group $F(\overline{\mathfrak{m}})$.

In § 1.9 of [77], Serre studies the representation of the absolute Galois group of $K$ attached to the $\ell$-torsion points of a one-dimensional formal group of height two (which, in particular, includes the case we are concerned with, that is, a formal group attached to an elliptic curve with good supersingular reduction at $\ell$).

Let us have a quick look at his reasoning. Let $F(X, Y) \in \mathcal{O}[[X, Y]]$ be a formal group law of height 2, and $F(\overline{\mathfrak{m}})$ the group attached to it. Let $V$ be the $\mathbb{F}_\ell$-vector space of the points of $\ell$-torsion of $F(\overline{\mathfrak{m}})$. Since the height of the formal group law is 2, it is easy to prove that $V$ has in fact dimension 2 over $\mathbb{F}_\ell$ (see [29], Chap. IV, § 2). The main idea now would be, let us say, to try to embed $V$ into another vector space, one such that there is information available about the action of the inertia group. What follows can be found in [77], § 8 and 9, but we recall it here, since it will be essential to our further reasoning.

First of all, let us start by defining an auxiliary object. Let us fix a positive rational number $\alpha \in \mathbb{Q}$.

**Definition 4.1.** Consider the sets

$$\overline{\mathfrak{m}}_\alpha = \{x \in \overline{\mathfrak{m}} : v(x) \geq \alpha\} \quad \text{and} \quad \overline{\mathfrak{m}}_\alpha^+ = \{x \in \overline{\mathfrak{m}} : v(x) > \alpha\}.$$

We define $V_\alpha$ as the quotient group

$$V_\alpha := \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_\alpha^+.$$

In fact, $V_\alpha$ has a natural structure of $\overline{k}$-vector space. Namely, the multiplication is defined in the following way: take any element of $\overline{k}$, say $\mu + \overline{\mathfrak{m}}$, where $\mu \in \overline{K}$ is an element with $\ell$-adic valuation greater than or equal to zero, and let $x + \overline{\mathfrak{m}}_\alpha^+$ be any element in $V_\alpha$. Then

$$(\mu + \overline{\mathfrak{m}}) \cdot (x + \overline{\mathfrak{m}}_\alpha^+) := \mu \cdot x + \overline{\mathfrak{m}}_\alpha^+ \in V_\alpha.$$

The dimension of $V_\alpha$ as $\overline{k}$-vector space is clearly one.

The absolute Galois group of $K$ acts on $V_\alpha$ in the natural way, that is to say, for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and for each $x + \overline{\mathfrak{m}}_\alpha^+ \in \overline{\mathfrak{m}}_\alpha/\overline{\mathfrak{m}}_\alpha^+$, we have

$$\sigma(x + \overline{\mathfrak{m}}_\alpha^+) := \sigma(x) + \overline{\mathfrak{m}}_\alpha^+.$$

In general, this action does not respect the $\overline{k}$-vector space structure. If we take $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $\mu + \overline{\mathfrak{m}} \in \overline{k}$ and $x + \overline{\mathfrak{m}}_\alpha^+ \in V_\alpha$, then

$$\begin{aligned}\sigma((\mu + \overline{\mathfrak{m}}) \cdot (x + \overline{\mathfrak{m}}_\alpha^+)) &= \sigma(\mu \cdot x + \overline{\mathfrak{m}}_\alpha^+) = \sigma(\mu \cdot x) + \overline{\mathfrak{m}}_\alpha^+ = \\ &= \sigma(\mu) \cdot \sigma(x) + \overline{\mathfrak{m}}_\alpha^+ = (\sigma(\mu) + \overline{\mathfrak{m}}) \cdot (\sigma(x) + \overline{\mathfrak{m}}_\alpha^+) = \\ &= (\sigma(\mu) + \overline{\mathfrak{m}}) \cdot \sigma(x + \overline{\mathfrak{m}}_\alpha^+) \neq (\mu + \overline{\mathfrak{m}}) \cdot \sigma(x + \overline{\mathfrak{m}}_\alpha^+),\end{aligned}$$

save in the case when $\sigma$ belongs to the inertia group $I \subset \mathrm{Gal}(\overline{K}/K)$.

But this is precisely the case we are interested in. Specifically, and this is the key point, if we take an element $\sigma$ in the inertia group $I$, it induces a morphism of $\overline{k}$-vector space on $V_\alpha$. But since $V_\alpha$ is a one-dimensional vector space, such morphism must be the multiplication by an element of $\overline{k}^*$. That is to say, we obtain a character

$$\varphi_\alpha : I \to \overline{k}^*$$

such that, for all $\sigma \in I$

$$\sigma(x + \overline{\mathfrak{m}}_\alpha^+) = \varphi_\alpha(\sigma)(x + \overline{\mathfrak{m}}_\alpha^+).$$

But let us assume that $\sigma$ belongs to the wild inertia group $I_{\mathrm{w}}$. Since $I_{\mathrm{w}}$ is a pro-$\ell$-group, it holds that $\varphi_\alpha(\sigma)$, which has finite order in the multiplicative group $\overline{k}^*$ (for, by definition of local field, the residue class field $k$ is finite, and so any element of its algebraic closure has finite order), must have order equal to a power of $\ell$. Yet $\overline{k}^*$ has no element of order $\ell$. This proves that $I_{\mathrm{w}}$ acts trivially on $V_\alpha$. Let us state this as a lemma.

**Lemma 4.2.** *The wild inertia group $I_{\mathrm{w}}$ acts trivially on $V_\alpha$.*

Once this point is settled, the next step is to embed our $\mathbb{F}_\ell$-vector space $V$, which is the set of $\ell$-torsion points of the formal group $F(\overline{\mathfrak{m}})$, into $V_\alpha$, for a certain value of $\alpha$.

Let us first determine what this value $\alpha$ might be.

**Lemma 4.3.** *Let $x \in V \subset \overline{\mathfrak{m}}$ be a non-zero element. Then $v(x) = \frac{1}{\ell^2-1}$.*

*Proof.* This is explained in the proof of Proposition 9, § 1.9 of [77]. In any case, we will recall the details here, since we will need to generalize it in Chapter 7.

Since we are assuming that the formal group law has height two, the multiplication by $\ell$ map in the formal group $F(\overline{\mathfrak{m}})$ can be written as

$$[\ell](X) = \sum_{i=1}^{\infty} a_i X^i,$$

where $a_i \in \mathcal{O}$ for all $i \in \mathbb{N}$, and moreover $a_1 = \ell$, $\ell | a_i$ for all $i < \ell^2$, and $a_{\ell^2} \notin \mathfrak{m}$ (see Proposition 2.3 and Corollary 4.4 of chapter IV of [84]).

Now if $x \in V$ is a non-zero element, it must hold that

$$\sum_{i=1}^{\infty} a_i x^i = 0.$$

Call $\alpha = v(x)$, and let us compute the valuation of each of the terms in the previous equation.

- $v(a_1 x) = v(a_1) + v(x) = 1 + \alpha$.
- For all $i \in \{2, 3, \ldots, \ell^2 - 1\}$, $v(a_i x^i) = v(a_i) + v(x^i) > 1 + \alpha$, since $v(a_i) \geq 1$ and $v(x^i) > v(x) = \alpha$.
- $v(a_{\ell^2} x^{\ell^2}) = v(a_{\ell^2}) + \ell^2 v(x) = 0 + \ell^2 \alpha = \ell^2 \alpha$.
- For all $i > \ell^2$, $v(a_i x^i) = v(a_i) + v(x^i) > \ell^2 \alpha$, since $v(a_i) \geq 0$ and $v(x^i) > v(x^{\ell^2})$.

Therefore, since there must be (at least) two terms with minimal valuation (so that they compensate each other and the sum vanishes), the first and the $\ell^2$-th terms are constrained to satisfy that $v(a_1 x) = v(a_{\ell^2} x^{\ell^2})$, that is to say, $1 + \alpha = \ell^2 \alpha$, and this concludes the proof. □

This lemma tells us that we have an inclusion of sets $(V \setminus \{0\}) \subset \overline{\mathfrak{m}}_\alpha$, for $\alpha = \frac{1}{\ell^2-1}$. So we can consider the following map

$$\begin{aligned} \Phi : V &\to V_\alpha = \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_\alpha^+ \\ x &\mapsto x + \overline{\mathfrak{m}}_\alpha^+. \end{aligned}$$

This is obviously an injective map. Besides, it is a group morphism. For, from the definition of the formal group law $F$, it follows easily that its shape is the following:

$$F(X, Y) = X + Y + \text{terms of degree} \geq 2.$$

Therefore, for all $x, y \in \overline{\mathfrak{m}}_\alpha$, it holds that $F(x, y) - x - y \in \overline{\mathfrak{m}}_\alpha^+$. That is to say,

$$\Phi(x \oplus_F y) = (x \oplus_F y) + \overline{\mathfrak{m}}_\alpha^+ = (x + y) + \overline{\mathfrak{m}}_\alpha^+ = \Phi(x) + \Phi(y).$$

Finally, it is immediate to check that this morphism commutes with the Galois action: for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\Phi(\sigma(x)) = \sigma(x) + \overline{\mathfrak{m}}_\alpha^+ = \sigma(x + \overline{\mathfrak{m}}_\alpha^+) = \sigma(\Phi(x)).$$

This is enough to show that the wild inertia group acts trivially on $V$. For take any $\sigma \in I_{\mathrm{w}}$, and $x \in V$. Since $\Phi$ is injective, $\sigma(x) = x$ if and only if $\Phi(\sigma(x)) = \Phi(x)$. But this last claim follows from Lemma 4.2.

## 4.2 Generalization to supersingular abelian varieties

Our task now is to generalize all the steps we described in the previous section, when the abelian variety does not necessarily have dimension 1. We maintain the notation which was explained at the beginning of this chapter, thus remaining in the local setting.

Let us take an abelian variety $A/K$. The first step would be to reduce the study of the group $A[\ell]$ of $\ell$-torsion points to the study of a certain formal group.

First of all, let us recall what supersingularity means for an abelian variety (see Chapter 1, § 6 of [60]):

**Definition 4.4.** Let $k$ be a field of positive characteristic $\ell$. An abelian variety $A/k$ of dimension $n \geq 2$ is called *supersingular* if there exists a supersingular elliptic curve $E$ defined over an algebraic closure $\overline{k}$ of $k$ such that $A$ and $E^n$ are isogenous over $\overline{k}$.

It is well known that a supersingular abelian variety $A/k$ has no points of $\ell$-torsion. So, this far, everything occurs as we could wish.

On the other hand, the notion of formal group law generalizes to any dimension (see [34], Chapter II, § 9.1).

To ease notation, let us denote the following $d$-tuples of variables by $\mathbf{X} = (X_1, \ldots, X_d)$, $\mathbf{Y} = (Y_1, \ldots, Y_d), \mathbf{Z} = (Z_1, \ldots, Z_d)$. We shall denote by $\overline{\mathfrak{m}}^{\times d}$ the cartesian product of $\overline{\mathfrak{m}}$ with itself $d$ times.

**Definition 4.5.** A *$d$-dimensional formal group law* defined over $\mathcal{O}$ is a $d$-tuple of power series

$$(F_1(\mathbf{X}, \mathbf{Y}), \ldots, F_d(\mathbf{X}, \mathbf{Y})) \in \mathcal{O}[[X_1, \ldots, X_d, Y_1, \ldots, Y_d]]^{\times d}$$

satisfying:

- $F_i(\mathbf{X}, \mathbf{Y}) \equiv X_i + Y_i \pmod{\text{terms of degree two}}$, for all $i = 1, \ldots, d$.
- $F_i(F_1(\mathbf{X}, \mathbf{Y}), \ldots, F_d(\mathbf{X}, \mathbf{Y}), \mathbf{Z}) = F_i(\mathbf{X}, F_1(\mathbf{Y}, \mathbf{Z}), \ldots, F_d(\mathbf{Y}, \mathbf{Z}))$ for all $i = 1, \ldots, d$.

Besides, if $F_i(\mathbf{X}, \mathbf{Y}) = F_i(\mathbf{Y}, \mathbf{X})$ for all $i = 1, \ldots, d$, then the formal group law is said to be *commutative*.

As in the case of dimension 1, one can attach a group to a formal group law. The addition law $\oplus_{\mathbf{F}}$ defined by

$$\begin{aligned} \oplus_{\mathbf{F}} : \overline{\mathfrak{m}}^{\times d} \times \overline{\mathfrak{m}}^{\times d} &\to \overline{\mathfrak{m}}^{\times d} \\ (\mathbf{x}, \mathbf{y}) &\mapsto (F_1(\mathbf{x}, \mathbf{y}), \ldots, F_d(\mathbf{x}, \mathbf{y})) \end{aligned}$$

on $\overline{\mathfrak{m}}^{\times d}$ endows it with a group structure. We shall designate this group by $\mathbf{F}(\overline{\mathfrak{m}})$.

To an abelian variety $A/K$ of dimension $n$ one can attach a $n$-dimensional formal group (see the construction given in [36], Part C, Chapter C2).

Again, this far everything generalizes beautifully. Now our aim is to see that the study of the Galois action on the $\ell$-torsion points

of $A$ can be reduced to the study of the Galois action on this formal group. Fortunately, this is also a well-known fact (See Theorem C.2.6, Chapter C2, Part C of [36], taking into account that all the coordinates of the $\ell$-torsion points of $A$ are contained into a finite extension of $K$).

**Proposition 4.6.** *Let $A/K$ be an abelian variety with good reduction, and let $A_1(\overline{K})$ be the kernel of the reduction map*

$$A(\overline{K}) \to \widetilde{A}(\overline{k}).$$

*Then there is a group isomorphism between the formal group $\mathbf{F}(\overline{\mathfrak{m}})$ associated to the abelian variety $A$ and the group $A_1(\overline{K})$.*

*Moreover, this isomorphism commutes with the Galois action on both sides.*

If we take an abelian variety $A/K$ with good supersingular reduction, all its $\ell$-torsion points belong to $A_1(\overline{K})$ and the previous proposition tells us that they can be viewed inside the formal group $\mathbf{F}(\overline{\mathfrak{m}})$.

As in the preceding section, we will call $V$ the $\mathbb{F}_\ell$-vector space of the $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$. All the previous considerations imply that we have a group isomorphism

$$A[\ell] \simeq V$$

compatible with the action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$.

Thus, up to this point, everything happens analogously to the case of dimension one. If we recollect what we did in that case, the next step should be to embed $V$ into $V_\alpha$, for some value of $\alpha$. Yet in general we do not know how to accomplish this task. Our idea was to assume an extra hypothesis and try to follow the above line of reasoning wielding it. We will devote ourselves to this task in the following section.

The result we are aiming to obtain is Theorem 4.9.

## 4.3 Inertia action and the formal group law

In the previous section we began to tackle the Galois representations attached to the $\ell$-torsion points of an abelian variety. We were trying to emulate the case of dimension one, which was completed in Chapter 1. We were partly successful, but found the first important difficulty. Overcoming it shall be the aim of this section.

We remain in a local setting, as in the previous section. That is to say, $K$ is a local field of characteristic zero and residual characteristic $\ell$, $v$ the corresponding discrete valuation, normalized so that $v(K^*) = \mathbb{Z}$, $\mathcal{O}$ the ring of integers of the valuation and $k$ the residue field. Further, $v(\ell) = 1$ (for instance, we may take $K = \mathbb{Q}_\ell$). We fix an algebraic closure $\overline{K}$ of $K$, and call $v$ the extension of $v$ to this algebraic closure. Finally, $\overline{k}$ denotes the algebraic closure of $k$ obtained through the reduction of $\mathcal{O}_{\overline{K}}$, the ring of integers of $\overline{K}$ with respect to $v$, modulo its maximal ideal.

When the abelian variety $A/K$ has supersingular reduction and its dimension is 1, the dimension of the formal group law $F$ attached to it is also equal to 1 and its height is 2. This allowed us to embed the $\mathbb{F}_\ell$-vector space $V$ of $\ell$-torsion points of $F(\overline{\mathfrak{m}})$ into $V_\alpha$ (see Definition 4.1) for a certain value of $\alpha \in \mathbb{Q}$. The key point was that each of the points in $V \subset \overline{\mathfrak{m}}$ has $\ell$-adic valuation equal to $1/(\ell^2 - 1)$. This is the content of Lemma 4.3. But when the abelian variety has dimension $n > 1$, the points of $V \subset \overline{\mathfrak{m}}^{\times n}$ have $n$ coordinates, with room for different valuations.

Let $\mathbf{F}$ be a formal group law of dimension $n$, and let $V$ be the set of $\ell$-torsion points of $\mathbf{F}$. We need to devise a way of tackling the possibility that the valuations of the coordinates of the $\ell$-torsion points of $\mathbf{F}$ have different values. Our idea was to formulate a weaker assumption about the valuations of the coordinates, but which is strong enough to imply the desired result about the action of the wild inertia group $I_{\mathrm{w}}$ on $\mathbf{F}(\overline{\mathfrak{m}})$.

**Hypothesis 4.7.** *The $\mathbb{F}_\ell$-vector space $V$ is finite, and there exists a positive $\alpha \in \mathbb{Q}$ such that, for all non zero $(x_1, \ldots, x_n) \in V$, it holds that*

$$\min_{1 \le i \le n} \{v(x_i)\} = \alpha.$$

**Remark 4.8.** When the formal group law $\mathbf{F}$ is attached to an abelian variety, the $\mathbb{F}_\ell$-vector space of $\ell$-torsion points of $\mathbf{F}$ will always be finite. This will follow from the fact that the formal group law has finite height. We will recall the notion of height in Chapter 5.

Let us check that, under this hypothesis, we are able to achieve our aim:

**Theorem 4.9.** *Let $\mathbf{F}$ be a formal group law such that the $\mathbb{F}_\ell$-vector space $V$ of the $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$ satisfies Hypothesis 4.7. Then*

*the image of the wild inertia group $I_{\mathrm{w}}$ by the Galois representation attached to $V$ is trivial.*

*Proof.* Let $P = (x_1, \ldots, x_n) \in V$. We are going to show that each $\sigma \in I_{\mathrm{w}}$ acts trivially on $P$, that is, $\sigma(P) = P$.

According to Hypothesis 4.7, we have that, for each non-zero point $Q = (y_1, \ldots, y_n) \in V$,

$$\min_{1 \leq i \leq n} \{v(y_i)\} = \alpha.$$

Therefore, for each $n$-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, we know that either $\lambda_1 y_1 + \cdots \lambda_n y_n = 0$ or else it belongs to $\overline{\mathfrak{m}}_\alpha$. This allows us to consider the following map:

$$\begin{aligned} \varphi_{(\lambda_1,\ldots,\lambda_n)} : V &\to V_\alpha = \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_{\alpha^+} \\ (y_1, \ldots, y_n) &\mapsto \lambda_1 y_1 + \cdots \lambda_n y_n + \overline{\mathfrak{m}}_\alpha^+. \end{aligned}$$

It is clear that $\varphi_{(\lambda_1,\ldots,\lambda_n)}$ is a group morphism, when we consider on $V$ the sum given by the formal group law, and on $V_\alpha$ the sum induced by that of $\overline{K}$. As a matter of fact, it is a morphism of $\mathbb{F}_\ell$-vector spaces (for the structure of $\mathbb{F}_\ell$-vector space is determined by the sum). Besides, it is compatible with the Galois action. If we take an element $\tau \in \mathrm{Gal}(\overline{K}/K)$, then

$$\begin{aligned} \varphi_{(\lambda_1,\ldots,\lambda_n)}(\tau(Q)) &= \varphi_{(\lambda_1,\ldots,\lambda_n)}(\tau(y_1), \ldots, \tau(y_n)) = \\ &= (\lambda_1 \tau(y_1) + \cdots + \lambda_n \tau(y_n)) + \overline{\mathfrak{m}}_\alpha^+ = \\ &= \tau((\lambda_1 y_1 + \cdots + \lambda_n y_n) + \overline{\mathfrak{m}}_\alpha^+) = \tau(\varphi_{(\lambda_1,\ldots,\lambda_n)}(Q)). \end{aligned}$$

Now let us take an element $\sigma \in I_{\mathrm{w}}$. Then $\varphi_{(\lambda_1,\ldots,\lambda_n)}(\sigma(P)) = \sigma(\varphi_{(\lambda_1,\ldots,\lambda_n)}(P)) = \varphi_{(\lambda_1,\ldots,\lambda_n)}(P)$, where the last equation follows from Lemma 4.2. In other words, for each $n$-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, $\sigma(P) - P$ belongs to the kernel of $\varphi_{(\lambda_1,\ldots,\lambda_n)}$. But no point of $V$ can belong to all these kernels save the zero vector. This, again, is a consequence of Hypothesis 4.7. Any non-zero point $Q = (y_1, \ldots, y_n) \in V$ satisfies that there exists $j \in \{1, \ldots, n\}$ such that $v(y_j) = \alpha$. If we take $\lambda_i = 0$ for all $i \neq j$, $\lambda_j = 1$, then $\varphi_{(\lambda_1,\ldots,\lambda_n)}(P) = x_j + \overline{\mathfrak{m}}_\alpha^+ \neq 0 + \overline{\mathfrak{m}}_\alpha^+$.

To sum up, for each $P \in V$ and each $\sigma \in I_{\mathrm{w}}$, $\sigma(P) - P = (0, \ldots, 0)$, and so $\sigma$ acts trivially on $P$, as we wished to prove.

□

# Chapter 5

# Height of a formal group law

In this rather technical chapter we recall the notion of height of a formal group law. We shall also establish a few important points concerning the shape of homomorphisms between formal group laws. Let us start by recalling the definition of homomorphism.

**Definition 5.1.** Let $\mathbf{F} = (F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y}))$ and $\mathbf{G} = (G_1(\mathbf{X}, \mathbf{Y}), \dots G_n(\mathbf{X}, \mathbf{Y}))$ be two formal group laws over $\mathcal{O}$ of dimension $n$. A *homomorphism* $f$ is a $n$-tuple of formal power series in $\mathcal{O}[[Z_1, \dots, Z_n]]$ without constant term, say $(f_1(Z_1, \dots, Z_n), \dots, f_n(Z_1, \dots, Z_n))$, such that

$$\begin{aligned} f(F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y})) = \\ = (G_1(f_1(\mathbf{X}), \dots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \dots, f_n(\mathbf{Y})), \\ \dots, G_n(f_1(\mathbf{X}), \dots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \dots, f_n(\mathbf{Y}))). \end{aligned}$$

**Example 5.2.** For each $m \in \mathbb{N}$, one can define the multiplication by $m$ map in the following way:

$$\begin{cases} [0](\mathbf{Z}) = (0, 0, \dots, 0) \\ [1](\mathbf{Z}) = \mathbf{Z} \\ [m+1](\mathbf{Z}) = \mathbf{F}([1](\mathbf{Z}), [m](\mathbf{Z})) \text{ for } m \geq 1. \end{cases}$$

It is easy to prove by induction that the shape of the $n$ power series $[m]_i(\mathbf{Z})$ that constitute the multiplication by $m$ map is the following:

$$[m]_i(\mathbf{Z}) = m \cdot Z_i + \text{ terms of degree } \geq 2,$$

for all $i = 1, \ldots, n$.

We will now recall the notion of height of a formal group law (see [34], Chapter IV, (18.3.8)). Firstly, we need to define this concept for formal group laws defined over $k$, and then we will transfer this definition to formal group laws over $\mathcal{O}$ through the reduction map.

**Definition 5.3.** Let $\overline{\mathbf{F}}$ be a formal group law of dimension n over $k$, and let $\overline{[\ell]} = (\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z}))$ be the multiplication by $\ell$ map. Then $\overline{\mathbf{F}}$ is of *finite height* if the ring $k[[Z_1, \ldots, Z_n]]$ is finitely generated as a module over the subring $k[[\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z})]]$.

When $\overline{\mathbf{F}}$ is of finite height, it holds that $k[[Z_1, \ldots, Z_n]]$ is a free module over $k[[\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z})]]$ of rank equal to a power of $\ell$, say $\ell^h$. This $h$ shall be called the *height of* $\overline{\mathbf{F}}$.

**Definition 5.4.** Let $\mathbf{F}$ be a formal group law of dimension n over $\mathcal{O}$. We define the *height* of $\mathbf{F}$ as the height of the reduction $\overline{\mathbf{F}}$ of $\mathbf{F}$ modulo the maximal ideal of $\mathcal{O}$.

**Remark 5.5.** Before delving deeper in our problem by using this new tool, a few words about the way to compute it would be highly advisable. Let $\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})$ be $n$ formal power series in $k[[Z_1, \ldots, Z_n]]$ without constant term. We will prove below that the following statements are equivalent:

- $k[[Z_1, \ldots, Z_n]]$ is generated by $h$ elements as a module over the subring $k[[\overline{f}_1, \ldots, \overline{f}_n]]$.
- $k[[Z_1, \ldots, Z_n]]/\langle \overline{f}_1, \ldots, \overline{f}_n \rangle$ is a $k$-vector space of finite dimension less than or equal to $h$.

Therefore, to compute the height of $\overline{\mathbf{F}}$, one seeks the least $h$ that satisfies the last property, that is, the dimension of the $k$-vector space $k[[Z_1, \ldots, Z_n]]/\langle \overline{f}_1, \ldots, \overline{f}_n \rangle$. But this can be easily done by means of standard bases.

**Lemma 5.6.** *Let $f_1, \ldots, f_n$ be formal power series in $k[[Z_1, \ldots, Z_n]]$ without constant term. Call $I = \langle f_1, \ldots, f_n \rangle$ the ideal of $k[[Z_1, \ldots, Z_n]]$ they generate. Then $k[[Z_1, \ldots, Z_n]]$ is finitely generated as a module over $k[[f_1, \ldots, f_n]]$ if and only if $k[[Z_1, \ldots, Z_n]]/I$ is a finite dimensional $k$-vector space. Moreover,*

$$\operatorname{rank}(k[[Z_1, \ldots, Z_n]], k[[f_1, \ldots, f_n]]) = \dim(k[[Z_1, \ldots, Z_n]]/I).$$

*Proof.* Assume $k[[Z_1, \ldots, Z_n]]$ is generated by $a_1, \ldots, a_r$ as a module over $k[[f_1, \ldots, f_n]]$. Take any element of $k[[Z_1, \ldots, Z_n]]/I$, say $a + I$. We can express $a = b_1 a_1 + \cdots + b_r a_r$, for some $b_1, \ldots, b_r \in k[[f_1, \ldots, f_n]]$. That is to say, for each $i = 1, \ldots, r$, there is a formal power series $g_i(\mathbf{Z}) \in k[[Z_1, \ldots, Z_n]]$ such that $b_i = g_i(f_1, \ldots, f_n)$. So if $\lambda_i$ is the constant term of $g_i$, we may write $b_i = \lambda_i + c_i$, where $c_i \in I$. Therefore

$$a = b_1 a_1 + \cdots + b_r a_r = (\lambda_1 a_1 + \cdots + \lambda_r a_r) + (c_1 a_1 + \cdots + c_r a_r).$$

This shows that the $k$-vector space $k[[Z_1, \ldots, Z_n]]/I$ is generated by the elements $a_1 + I, \ldots, a_r + I$. Therefore it has finite dimension and furthermore

$$\operatorname{rank}(k[[Z_1, \ldots, Z_n]], k[[f_1, \ldots, f_n]]) \geq \dim(k[[Z_1, \ldots, Z_n]]/I).$$

Assume now that $k[[Z_1, \ldots, Z_n]]/I$ is a finite dimensional $k$-vector space, and fix a base $a_1 + I, \ldots, a_r + I$. We wish to see that $a_1, \ldots, a_r$ generate $k[[Z_1, \ldots, Z_n]]$ as a module over $k[[f_1, \ldots, f_n]]$. Take therefore some $a \in k[[Z_1, \ldots, Z_n]]$. Our assumption assures us that there exist $\lambda_1, \ldots, \lambda_r \in k$ such that $a - (\lambda_1 a_1 + \cdots \lambda_r a_r) \in I$. Therefore, there exist $a'_1, \ldots, a'_n \in k[[Z_1, \ldots, Z_n]]$ such that we can write

$$a = \sum_{j=1}^{r} \lambda_j a_j + \sum_{i=1}^{n} a'_i f_i. \tag{5.1}$$

Now we can apply the same procedure to each $a'_i$, and express it as $a'_i = \sum_{j=1}^{r} \lambda'_{i,j} a_j + \sum_{s=1}^{n} a''_{i,s} f_s$. Replacing this expression in (5.1), we get

$$a = \sum_{j=1}^{r} (\lambda_j + \sum_{i=1}^{n} \lambda'_{i,j} f_i) a_j + \sum_{i=1}^{n} \sum_{s=1}^{n} a''_{i,s} f_i f_s.$$

Iterating this procedure, we will express $a$ as a sum

$$a = \sum_{j=1}^{r} g_j(f_1, \ldots, f_n) a_j,$$

for some $g(\mathbf{Z}) \in k[[Z_1, \ldots, Z_n]]$, thus proving that $k[[Z_1, \ldots, Z_n]]$ is finitely generated as a module over $k[[f_1, \ldots, f_n]]$, and moreover that

$$\operatorname{rank}(k[[Z_1, \ldots, Z_n]], k[[f_1, \ldots, f_n]]) \leq \dim(k[[Z_1, \ldots, Z_n]]/I).$$

□

Let us recall briefly the definition and some properties of standard bases in power series rings (see [5]).

**Definition 5.7.** Let $k$ be a field, and $X_1, \ldots, X_n$ variables. Let $T = \{X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \cdots \cdot X_n^{\alpha_n} : (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$. An *admissible ordering* on $T$ is a total ordering $\leq$ on $T$ which satisfies:

- $1 < t$ for all $t \in T$.
- If $t_1 < t_2$ then $t_1 \cdot t < t_2 \cdot t$ for all $t_1, t_2, t \in T$.

**Definition 5.8.** Let $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in k[[X_1, \ldots, X_n]]$, and let $\leq$ be an admissible ordering on $T$. Let us denote by $\mathrm{T}(f) = \{a_\alpha X^\alpha : \alpha \in \mathbb{N}^n \text{ and } a_\alpha \neq 0\}$. The *leading term* of $f$ with respect to $\leq$, denoted $\mathrm{LT}(f)$, is the term $a_\alpha X^\alpha$ such that $a_\alpha \neq 0$ and, for all $a_\beta X^\beta \in \mathrm{T}(f)$, $X^\alpha \leq X^\beta$.

Now we have introduced the terminology required to define standard bases.

**Definition 5.9.** Let $\leq$ be an admissible ordering on $T$, and let $I$ be an ideal in $k[[X_1, \ldots, X_n]]$. A finite subset $S \subset I$ is called a *standard basis* of $I$ if, for every $f \in I$ there exists $g \in S$ such that $\mathrm{LT}(g) | \mathrm{LT}(f)$.

The main interest of standard bases lies in the fact that they provide us with a way to deal with division in $k[[X_1, \ldots, X_n]]$, as the following theorem shows.

**Theorem 5.10** (Hironaka division theorem)**.** *Let $\leq$ be an admissible ordering on $T$ and $I$ an ideal in $k[[X_1, \ldots, X_n]]$. Then*

- *There exists a standard basis $S$ of $I$.*
- *If $S = \{g_1, \ldots, g_m\}$ is a standard basis of $I$, then for all $f \in k[[X_1, \ldots, X_n]]$ there exists an unique $r \in k[[X_1, \ldots, X_n]]$ such that*
  - *There exist $q_1, \ldots, q_m \in k[[X_1, \ldots, X_n]]$ with*

$$f = \sum_{i=1}^{m} g_i \cdot q_i + r.$$

  - *For all term $t \in \mathrm{T}(r)$, and for all leading term $s \in \{\mathrm{LT}(g) : g \in S\}$, $s$ does not divide $t$.*

**Remark 5.11.** From the result above, it easily follows that, if $I$ is an ideal of $k[[X_1, \ldots, X_n]]$, then the dimension of $k[[X_1, \ldots, X_n]]/I$ as a $k$-vector space is determined in this way: Take a standard basis $S$ of $I$, and consider the set of terms $M = \{t \in T : \text{ for all } g \in S, \mathrm{LT}(g) \nmid t\}$. Then the cardinal of $M$ is the required dimension (of course, it need not be finite).

Now, if we have a formal group law $\overline{\mathbf{F}}$ over $k$ of dimension n, its height is the dimension of $k[[Z_1, \ldots, Z_n]]/\langle \overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z})\rangle$, so the previous considerations allow us to compute it in an explicit way.

In the case when the formal group law is of dimension 1, another definition of height is used (see for instance [84], Chapter IV, § 7). Namely, if $\overline{F}(X, Y)$ is a formal group law defined over $k$, the height of $\overline{F}$ is defined as the largest $r$ such that the multiplication by $\ell$ map, $\overline{[\ell]}(Z)$, can be expressed as $\overline{[\ell]}(Z) = \overline{g}(Z^{\ell^r})$, for some formal power series $\overline{g}(Z) \in k[[Z]]$. One can prove, following a simple reasoning, that the first term of $g$ with non-zero coefficient is precisely a constant times $Z^{\ell^r}$. Now what happens if we try to imitate this reasoning in dimension n?

**Proposition 5.12.** *Let $\overline{\mathbf{F}}$, $\overline{\mathbf{G}}$ be formal group laws over $k$ of dimension $n$, and $\overline{\mathbf{f}} : \overline{\mathbf{F}} \to \overline{\mathbf{G}}$ a non-zero homomorphism. Let us write*

$$\overline{\mathbf{f}}(\mathbf{Z}) = (\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})).$$

*If $u$ is the smallest exponent such that, in some $\overline{f}_i(\mathbf{Z})$, some variable $Z_j$ occurs in a non-zero monomial raised to the $u$-th power, then $u = \ell^r$ for some $r \geq 0$. Furthermore, there exist $\overline{g}_1(\mathbf{Z}), \ldots, \overline{g}_n(\mathbf{Z}) \in k[[Z_1, \ldots, Z_n]]$ such that*

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i(\mathbf{Z}^{\ell^r}), \text{ for all } i = 1, \ldots, n,$$

*where $\mathbf{Z}^{\ell^r} = (Z_1^{\ell^r}, \ldots, Z_n^{\ell^r})$.*

*Proof.* Since $\overline{\mathbf{f}}$ is a homomorphism of formal group laws, it holds that

$$\overline{\mathbf{f}}(\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})) = \overline{\mathbf{G}}(\overline{\mathbf{f}}(\mathbf{X}), \overline{\mathbf{f}}(\mathbf{Y})).$$

Coordinatewise, this means that

$$\begin{aligned} \overline{f}_i(\overline{F}_1(\mathbf{X}, \mathbf{Y}), \ldots, \overline{F}_n(\mathbf{X}, \mathbf{Y})) = \\ = \overline{G}_i(\overline{f}_1(\mathbf{X}), \ldots, \overline{f}_n(\mathbf{X}), \overline{f}_1(\mathbf{Y}), \ldots, \overline{f}_n(\mathbf{Y})), \end{aligned} \quad (5.2)$$

for each $i = 1, \ldots, n$.

Let us differentiate (5.2) with respect to $Y_j$. Applying the chain rule, we obtain

$$\sum_{m=1}^{n} \frac{\partial \overline{f}_i}{Z_m}(\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})) \cdot \frac{\partial \overline{F}_m}{\partial Y_j}(\mathbf{X}, \mathbf{Y}) = \sum_{m=1}^{n} \frac{\partial \overline{G}_i}{\partial Y_m}(\overline{\mathbf{f}}(\mathbf{X}), \overline{\mathbf{f}}(\mathbf{Y})) \cdot \frac{\partial \overline{f}_m}{\partial Z_j}(\mathbf{Y}),$$

for each $i = 1, \ldots, n$, $j = 1, \ldots, n$.

Substitute $\mathbf{Y} = (0, 0, \ldots, 0)$. We obtain that

$$\sum_{m=1}^{n} \frac{\partial \overline{f}_i}{Z_m}(\mathbf{X}) \cdot \frac{\partial \overline{F}_m}{\partial Y_j}(\mathbf{X}, 0, \ldots, 0) = \\ = \sum_{m=1}^{n} \frac{\partial \overline{G}_i}{\partial Y_m}(\overline{\mathbf{f}}(\mathbf{X}), 0, \ldots, 0) \cdot \frac{\partial \overline{f}_m}{\partial Z_j}(0, \ldots, 0), \quad (5.3)$$

for each $i = 1, \ldots, n$, $j = 1, \ldots, n$.

Equations (5.3), $i = 1, \ldots, n$, $j = 1, \ldots, n$, can be summarized in the following expression: if we denote by

$$A_{ij} = \frac{\partial \overline{f}_i}{\partial Z_j}(\mathbf{X}), \qquad F_{ij} = \tfrac{\partial \overline{F}_i}{\partial Y_j}(\mathbf{X}, 0, \ldots, 0)$$
$$a_{ij} = \frac{\partial \overline{f}_i}{\partial Z_j}(0, \ldots, 0), \quad G_{ij} = \tfrac{\partial \overline{G}_i}{\partial Y_j}(\overline{\mathbf{f}}(\mathbf{X}), 0, \ldots, 0))$$

then

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \cdot \begin{pmatrix} F_{11} & F_{12} & \cdots & F_{1n} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ F_{n1} & F_{n2} & \cdots & F_{nn} \end{pmatrix} = \\ \begin{pmatrix} G_{11} & G_{12} & \cdots & G_{1n} \\ G_{21} & G_{22} & \cdots & G_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ G_{n1} & G_{n2} & \cdots & G_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

If there exist $i, j \in \{1, \ldots, n\}$ such that $a_{ij} \neq 0$, then the formal power series $\overline{f}_i$ has a monomial $aZ_j$, where $a \in k^*$. Therefore $u = r^0$ and obviously all the formal power series $\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})$ can be expressed as formal power series in the variables $Z_1, \ldots, Z_n$, so there would be nothing to prove.

Assume that, on the contrary, all $a_{ij} = 0$. Then

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \cdot \begin{pmatrix} F_{11} & F_{12} & \cdots & F_{1n} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ F_{n1} & F_{n2} & \cdots & F_{nn} \end{pmatrix} = 0.$$

But the matrix

$$M_F = \begin{pmatrix} F_{11} & F_{12} & \cdots & F_{1n} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ F_{n1} & F_{n2} & \cdots & F_{nn} \end{pmatrix}$$

is invertible (Write $M_F = \mathrm{Id} + B$, where all entries of $B$ are formal power series without constant term. Then the sum $1 - B + B^2 - B^3 + \cdots$ defines a formal power series, which is the inverse of $M_F$). Therefore all the $A_{ij}$ must vanish. But this means that, for all $i = 1, \ldots, n$, the monomials of the power series $\overline{f}_i(\mathbf{Z})$, say $Z_1^{e_1} \cdot Z_2^{e_2} \cdots Z_n^{e_n}$, with some exponent $e_m$ not divisible by $\ell$, cannot occur with non-zero coefficient. Thus there exist $\overline{g}_i(\mathbf{Z})$, $i = 1, \ldots, n$, such that

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i(\mathbf{Z}^\ell).$$

We now wish to proceed by induction. To apply the same reasoning to the power series $\overline{\mathbf{g}}(\mathbf{Z}) = (\overline{g}_1(\mathbf{Z}), \ldots, \overline{g}_n(\mathbf{Z}))$, we must view $\overline{\mathbf{g}}$ as a homomorphism between formal group laws. Only the formal group laws will not be $\overline{\mathbf{F}}$ and $\overline{\mathbf{G}}$. Namely, if we consider the formal group law $\overline{\mathbf{F}}'(\mathbf{X}, \mathbf{Y})$, obtained from $\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})$ by raising all coefficients to the $\ell$-th power, then it is immediate to check that $(\overline{F}_i(\mathbf{X}, \mathbf{Y}))^\ell = \overline{F}'_i(\mathbf{X}^\ell, \mathbf{Y}^\ell)$ for $i = 1, 2, \ldots, n$. Therefore,

$$\overline{\mathbf{g}}(\overline{\mathbf{F}}'(\mathbf{X}^\ell, \mathbf{Y}^\ell)) = \overline{\mathbf{g}}(\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})^\ell) = \overline{\mathbf{f}}(\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})) = \overline{\mathbf{G}}(\overline{\mathbf{f}}(\mathbf{X}), \overline{\mathbf{f}}(\mathbf{Y})) = \overline{\mathbf{G}}(\overline{\mathbf{g}}(\mathbf{X}^\ell), \overline{\mathbf{g}}(\mathbf{Y}^\ell)).$$

Thus we conclude that

$$\overline{\mathbf{g}}(\overline{\mathbf{F}}'(\mathbf{X}, \mathbf{Y})) = \overline{\mathbf{G}}(\overline{\mathbf{g}}(\mathbf{X}), \overline{\mathbf{g}}(\mathbf{Y})),$$

which shows that the induction step can be taken.

This proves that there exist $\overline{g}_1(\mathbf{X}), \ldots, \overline{g}_n(\mathbf{Z}) \in k[[\mathbf{Z}]]$ and a natural number $r$ such that

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i(\mathbf{Z}^{\ell^r}),$$

for $i = 1, \ldots, n$.

Moreover, either $\overline{g}_1(\mathbf{Z})$ or $\overline{g}_2(\mathbf{Z})$ or $\ldots$ or $\overline{g}_n(\mathbf{Z})$ have a term of degree 1 with non-zero coefficient. That is to say, a monomial in some $Z_j^{\ell^r}$ does appear in at least one of the power series $\overline{f}_i(\mathbf{Z})$. And it is clear that it is the term of least degree of $\overline{f}_i(\mathbf{Z})$. □

**Remark 5.13.** We can apply this proposition to the homomorphism $\overline{[\ell]}$ of multiplication by $\ell$ in a formal group law $\overline{\mathbf{F}}$, and conclude that there exists an $r \geq 0$ (in fact $r$ will be greater or equal than 1) such that the formal power series $\overline{[\ell]}_i(\mathbf{Z})$, $i = 1, \ldots, n$, can be expressed as formal power series in the variables $Z_1^{\ell^r}, \ldots, Z_n^{\ell^r}$. But this $r$ might not be determined by the height of $\overline{\mathbf{F}}$. For instance, it might be the case that the height of $\overline{\mathbf{F}}$ is infinite, while the exponent $r$ must always be a finite number. This will cause some difficulties, which will have to be dealt with in the following chapters.

# Chapter 6

# Summary of results (abelian varieties)

The aim of this chapter is to gather all the results we have obtained up to this point and combine them to obtain tame Galois realizations of the image of the Galois representations attached to certain abelian varieties over $\mathbb{Q}$.

Let us consider an abelian variety $A/\mathbb{Q}$, and let us fix a prime number $\ell > 2$.

View $A$ as an abelian variety over $\mathbb{Q}_\ell$ through the natural immersion $\mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$. In Chapter 4, Section 4.1, we saw that to $A$ there corresponds a formal group law $\mathbf{F}$ over $\mathbb{Z}_\ell$. A few relevant, well-known facts about this formal group laws are collected in the following proposition.

**Proposition 6.1.** *Let $\mathbf{F}$ be the formal group law attached to an abelian variety $A/\mathbb{Q}_\ell$ of dimension $n$. Then the following holds:*

- *$\mathbf{F}$ is of finite height $h \leq 2n$.*
- *If $A/\mathbb{Q}_\ell$ has good supersingular reduction, then $h = 2n$.*

*Proof.* According to [87], Example (a) of (2.1), the $\ell$-divisible group attached to $A$ has height $2n$. In particular, if we consider the group scheme of $\ell$-torsion points of $A$, its order is $\ell^{2n}$. Therefore the order of its connected component is $\ell^h$ with $h \leq 2n$. But the exponent $h$ is equal to the height of $\mathbf{F}$ (see [87], (2.2)). In particular, if $A$ is supersingular, it has no non-zero $\ell$-torsion points over $\overline{\mathbb{F}}_\ell$. This

means that the group scheme of $\ell$-torsion points of $A$ is connected, and therefore the exponent $h$ coincides with $2n$.

□

The main result is the following.

**Theorem 6.2.** *Let $A/\mathbb{Q}$ be an abelian variety of dimension $n$. Let $\ell > 2$ be a prime number, and $\mathcal{P}$ be the set of prime numbers that divide the order of $\mathrm{GL}_{2n}(\mathbb{F}_\ell)$. Assume the following conditions hold:*

- *For all $p \in \mathcal{P}$ different from $\ell$, $A$ has semistable reduction at $p$.*
- *$A$ has good supersingular reduction at $\ell$ and the formal group law attached to $A$ at $\ell$ satisfies Hypothesis 4.7.*

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

*Proof.* As we reasoned in Section 3.1, it suffices to control the behaviour of the representation

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

at a finite number of primes, namely, the primes that divide the order of $\mathrm{GL}_{2n}(\mathbb{F}_\ell)$. The first assumption ensures that, at these primes (save possibly at $\ell$), $A$ has semistable reduction, so we can apply Theorem 3.6 and conclude that, at all primes $p \neq \ell$ that divide $\mathrm{card}(\mathrm{GL}_{2n}(\mathbb{F}_\ell))$, the representation $\rho_\ell$ is tamely ramified.

Therefore the problem boils down to studying the behaviour at $\ell$.

Firstly, since $A$ has good supersingular reduction at $\ell$, all its $\ell$-torsion points map to zero through the reduction map. Therefore, applying Proposition 4.6, we know that $A[\ell]$ is isomorphic to $V$, the $\mathbb{F}_\ell$-vector space of the $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$ endowed with the sum given by the formal group law, and this isomorphism commutes with the Galois action. Thus it is equivalent to studying the Galois action on $V$.

But, by assumption, Hypothesis 4.7 holds. Therefore we are able to apply Theorem 4.9, and conclude that the wild inertia group $I_{\ell,\mathrm{w}}$ acts trivially on $V$. This concludes the proof.

□

We are now equipped with a strong result that gives us sufficient conditions under which the Galois representation attached to the $\ell$-torsion points of certain abelian varieties is tamely ramified. Our

wish now is to give, wielding this theorem, some explicit examples of abelian varieties satisfying these conditions. In order to do this, we will restrict ourselves to the case of dimension $n = 2$ and we will consider the Jacobians of genus 2 curves. The next chapters study this case in great detail to find an explicit statement which guarantees that the conditions in Theorem 6.2 hold. We will again place ourselves in a local setting, thus following the notation introduced at the beginning of Chapter 4.

# Chapter 7

# Symmetric two-dimensional formal group laws

In this chapter we will restrict our attention to formal group laws of dimension $n = 2$ and finite height $h = 4$. The reason why this case is appealing to us will become clear in the next chapters, where we will apply this theory to the formal groups attached to the Jacobians of supersingular genus 2 curves (which, by Proposition 6.1, satisfy these conditions). Furthermore, we will take $K = \mathbb{Q}_\ell$, $v$ the normalized $\ell$-adic valuation, $\mathcal{O} = \mathbb{Z}_\ell$, $k = \mathbb{F}_\ell$. Our aim will be to find some conditions, more restrictive than those of Theorem 6.2 but which can be directly read on the equations which define the formal group law, so that in the particular case when its dimension is two, we can guarantee that the ramification of the corresponding Galois representation is tame.

Recall that we want to find a way to deal with the action of the wild inertia group upon the $\mathbb{F}_\ell$-vector space $V$ of the $\ell$-torsion points of a formal group law. In Section 4.1 we considered the case when the formal group law had dimension 1 and height 2. In this setting, we used Lemma 4.2, which claims that the action of the wild inertia group on $V_\alpha$ is trivial, for any $\alpha \in \mathbb{Q}$. Lemma 4.3 allowed us to embed $V$ into $V_\alpha$ for $\alpha = 1/(\ell^2 - 1)$, in a way compatible with the Galois action, thus solving our problem. More precisely, Lemma 4.3 claims that the valuation of the non-zero points of $V \subset \overline{\mathfrak{m}}$ is equal to $\alpha$. Have a quick glance at the proof of this lemma. The points $x \in V$ must

satisfy the equation $[\ell](x) = 0$, and our knowledge of the formal power series defining the multiplication by $\ell$ map allows one to compute the valuation of $x$.

In the case of dimension 2, several difficulties arise. On the one hand, the points of $V$ have two coordinates. Therefore, a point $(x, y) \in V$ satisfies two equations in two variables, $[\ell]_1(x, y) = 0$ and $[\ell]_2(x, y) = 0$. This complicates matters significantly. In Chapter 4 we stated some conditions, namely Hypothesis 4.7, under which we were able to hold in check the action of the wild inertia subgroup. Now we need to devise a way to ensure that these favourable conditions hold.

Moreover, our knowledge of the expression of the multiplication by $\ell$ map is not as complete as in the one dimensional case. We begin with a detailed study of the shape of this map.

We can apply Proposition 5.12 to the homomorphism $\overline{[\ell]}$ of multiplication by $\ell$ in a formal group law $\overline{\mathbf{F}}$, and conclude that there exists an $r \geq 0$ such that both formal power series $\overline{[\ell]}_1(Z_1, Z_2)$ and $\overline{[\ell]}_2(Z_1, Z_2)$ can be expressed as formal power series in the variables $Z_1^{\ell^r}$, $Z_2^{\ell^r}$. What is the relationship between this exponent $r$ and the height of $\overline{\mathbf{F}}$ as we defined it in Definition 5.3?

**Proposition 7.1.** *Let $\overline{\mathbf{F}}$ be a formal group law defined over $\mathbb{F}_\ell$, and assume that there exist two power series $\overline{f}_1, \overline{f}_2 \in \mathbb{F}_\ell[[Z_1, Z_2]]$ such that the formal power series that give multiplication by $\ell$ map $\overline{[\ell]}$ can be written as*

$$\begin{cases} \overline{[\ell]}_1(Z_1, Z_2) = \overline{f}_1(Z_1^{\ell^r}, Z_2^{\ell^r}), \\ \overline{[\ell]}_2(Z_1, Z_2) = \overline{f}_2(Z_1^{\ell^r}, Z_2^{\ell^r}). \end{cases}$$

*Then the height of $\overline{\mathbf{F}}$ is greater than or equal to $2r$.*

*Proof.* Let us write

$$\begin{cases} \overline{f}_1(Z_1, Z_2) = a_{11}Z_1 + a_{12}Z_2 + \text{terms of degree} \geq 2 \\ \overline{f}_2(Z_1, Z_2) = a_{21}Z_1 + a_{22}Z_2 + \text{terms of degree} \geq 2. \end{cases}$$

We know that one element (at least) of the set $\{a_{11}, a_{12}, a_{21}, a_{22}\}$ does not vanish. We may assume that the term $a_{11} \neq 0$ (the other cases are analogous).

Consider the graduated lexicographical ordering on $\mathbb{F}_\ell[[Z_1, Z_2]]$ with $Z_1 < Z_2$, that is to say, the relation $\leq$ determined by the following rules:

$$Z_1^a Z_2^b < Z_1^c Z_2^d \leftrightarrow \begin{cases} a + b < c + d \text{ or} \\ a + b = c + d \text{ and } a > c. \end{cases}$$

Let $I$ be the ideal generated by $\overline{f}_1(Z_1, Z_2)$ and $\overline{f}_2(Z_1, Z_2)$. In order to compute the height of $\overline{\mathbf{F}}$, we need to find a standard basis for $I$. Now the smallest monomial with respect to this ordering is $Z_1$. And this monomial appears in $\overline{f}_1(Z_1, Z_2)$. We can therefore use it to eliminate all monomials under a given degree of $\overline{f}_2(Z_1, Z_2)$, save those which are pure in $Z_2$. In fact, if $\overline{f}_2(Z_1, Z_2)$ is not a multiple of $\overline{f}_1(Z_1, Z_2)$, we will reach a point where the power series $\overline{g}_2(Z_1, Z_2)$ obtained from $\overline{f}_2$ by eliminating the terms divisible by $Z_1$ up to a certain degree has as leading term a monomial which is pure in $Z_2$, say $\overline{g}_2(Z_1, Z_2) = b_{0,t}Z_2^t +$ terms of degree $\geq t+1$. Then it is easily seen that $\{\overline{f}_1, \overline{g}_2\}$ is a standard basis for $I$, and the rank of $\mathbb{F}_\ell[[Z_1, Z_2]]/I$ as a $\mathbb{F}_\ell$-module is $t$.

Recall that the height of $\overline{\mathbf{F}}$ is the rank of $\mathbb{F}_\ell[[Z_1, Z_2]]/\langle\overline{[\ell]}_1, \overline{[\ell]}_2\rangle$. Clearly this rank is $\ell^r \cdot (\ell^r t) = \ell^{2r}t$. But we know that $t$ must be a power of $\ell$ (see Definition 5.3), say $t$ is of the form $\ell^s$ for some $s \in \mathbb{N}$. Hence the height of $\overline{\mathbf{F}}$ is $2r+s$, which is greater than (or equal to) $2r$, as we wished to show.

□

**Remark 7.2.** If the height of $\mathbf{F}$ is 4, only two possibilities might occur:

- The exponent $r$ in Proposition 5.12 is 2. By Proposition 7.1, there exists an $s \in \mathbb{N}$ such that $4 = 2r + s = 4 + s$. Hence $s = 0$.
- The exponent $r$ in Proposition 5.12 is 1. Then by Proposition 7.1, there exists an $s \in \mathbb{N}$ such that $4 = 2r + s = 2 + s$. Hence $s = 2$.

As was to be expected, the analysis that the first case requires is easier. We will therefore concentrate on this case. That is to say, from now on our statements will include this condition as a hypothesis. In Chapter 8 we shall state some sufficient conditions that guarantee that the exponent $r$ is equal to 2 (see Proposition 8.10).

Note that the condition $s = 0$ implies that, if we write the multiplication by $\ell$ map as

$$\begin{cases} \overline{[\ell]}_1(Z_1, Z_2) = \overline{a}Z_1^{\ell^2} + \overline{b}Z_2^{\ell^2} + \text{terms of degree} \geq \ell^2 \\ \overline{[\ell]}_2(Z_1, Z_2) = \overline{c}Z_1^{\ell^2} + \overline{d}Z_2^{\ell^2} + \text{terms of degree} \geq \ell^2 \end{cases}$$

then the determinant of the matrix $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ is non-zero.

Let $\mathbf{F}$ be a formal group law over $\mathbb{Q}_\ell$ of dimension 2 and height 4. Our aim is to analyze the valuation of the $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$. We now face the problem that the property of being of $\ell$-torsion provides us with two equations in two variables. In order to avoid this inconvenience, we are going to restrict our attention to a special kind of formal group laws. Namely, we will consider formal group laws such that the two equations have a certain relationship that allows us to reduce the problem to studying a single equation.

**Definition 7.3.** Let $\mathbf{F} = (F_1(X_1, X_2, Y_1, Y_2), F_2(X_1, X_2, Y_1, Y_2))$ be a formal group law of dimension 2 over $\mathbb{Q}_\ell$. We will say that $\mathbf{F}$ is a *symmetric formal group law* if the following relationship holds:

$$F_2(X_2, X_1, Y_2, Y_1) = F_1(X_1, X_2, Y_1, Y_2).$$

The symmetry is reflected in the power series $[\ell]_1(Z_1, Z_2)$ and $[\ell]_2(Z_1, Z_2)$.

**Lemma 7.4.** *Let $\mathbf{F}(\mathbf{X}, \mathbf{Y})$ be a symmetric formal group law of dimension 2. For all $n \geq 1$, it holds that*

$$[n]_2(Z_2, Z_1) = [n]_1(Z_1, Z_2).$$

*Proof.* We shall proceed by induction. The statement holds trivially for $n = 1$: $[1]_1(Z_1, Z_2) = Z_1 = [1]_2(Z_2, Z_1)$.

Now let us tackle the induction step $n \to n + 1$. Assume that $[n]_1(Z_1, Z_2) = [n]_2(Z_2, Z_1)$. By definition, we know that

$$\begin{aligned}
&[n+1]_1(Z_1, Z_2) = F_1(Z_1, Z_2, [n]_1(Z_1, Z_2), [n]_2(Z_1, Z_2)) \text{ and} \\
&[n+1]_2(Z_1, Z_2) = F_2(Z_1, Z_2, [n]_1(Z_1, Z_2), [n]_2(Z_1, Z_2)).
\end{aligned}$$

Hence

$$\begin{aligned}
[n+1]_2(Z_2, Z_1) = F_2(Z_2, Z_1, [n]_1(Z_2, Z_1), [n]_2(Z_2, Z_1)) = \\
F_1(Z_1, Z_2, [n]_2(Z_2, Z_1), [n]_1(Z_2, Z_1)) = \\
F_1(Z_1, Z_2, [n]_1(Z_1, Z_2), [n]_2(Z_1, Z_2)) = [n+1]_1(Z_1, Z_2).
\end{aligned}$$

□

From now on, our formal group law $\mathbf{F}$ will enjoy this extra condition.

Next we will establish two technical lemmas which will be useful.

**Lemma 7.5.** *Let $\ell > 2$ be a prime number, $r \in \mathbb{N}$, and let $f(Z_1, Z_2) \in \mathbb{Z}_\ell[[Z_1, Z_2]]$ be a formal power series such that $f(Z_2, Z_1) = -f(Z_1, Z_2)$, which can be written as:*

$$f(Z_1, Z_2) = \ell \cdot (Z_1 - Z_2) + \ell \cdot (\textit{terms of total degree} \geq 2 \textit{ and} < \ell^r) + a \cdot (Z_1^{\ell^r} - Z_2^{\ell^r}) + \textit{ terms of total degree} \geq \ell^r + 1,$$

*where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ with $x_0 \neq y_0$ satisfies $f(x_0, y_0) = 0$ and furthermore $v(x_0), v(y_0) \geq v(x_0 - y_0)$, then the $\ell$-adic valuation $v(x_0 - y_0)$ is $1/(\ell^r - 1)$.*

*Proof.* Let us call $\beta = v(x_0 - y_0)$. We will compute the valuations of the different terms that appear in the equality $f(x_0, y_0) = 0$.

- $v(\ell \cdot (x_0 - y_0)) = 1 + \beta$.
- Let us consider a term of total degree between 2 and $\ell^r - 1$, say $\ell \cdot c x_0^n y_0^m$. Compute its valuation: $v(\ell \cdot c x_0^n y_0^m) = 1 + v(c) + nv(x_0) + mv(y_0) \geq 1 + (n+m)\beta > 1 + \beta$, since $n + m \geq 2$.
- Let us consider the term $a(x_0^{\ell^r} - y_0^{\ell^r})$. Let us split it into the sum of two terms, in the following way:

  $$a \cdot (x_0^{\ell^r} - y_0^{\ell^r}) = a \cdot ((x_0 - y_0)^{\ell^r} - B) = a \cdot (x_0 - y_0)^{\ell^r} - a \cdot B,$$

  where $B = (x_0 - y_0)^{\ell^r} - (x_0^{\ell^r} - y_0^{\ell^r})$.

  On the one hand, $v(a \cdot (x_0 - y_0)^{\ell^r}) = v(a) + \ell^r \beta = \ell^r \beta$, since $\ell$ does not divide $a$.

  On the other hand, note that

  $$(x_0 - y_0)^{\ell^r} = x_0^{\ell^r} - \binom{\ell^r}{1} x_0^{\ell^r - 1} y_0 + \binom{\ell^r}{2} x_0^{\ell^r - 2} y_0^2 + \cdots - \binom{\ell^r}{2} x_0^2 y_0^{\ell^r - 2} + \binom{\ell^r}{1} x_0 y_0^{\ell^r - 1} - y_0^{\ell^r}.$$

  Therefore, each of the terms $\binom{\ell^r}{i}(-1)^i x_0^{\ell^r - i} y_0^i$ has a valuation strictly greater than $1 + \beta$. (For $v(x_0^{\ell^r - i} y_0^i) \geq \beta(\ell^r - i + i) = \ell^r \beta$, and hence $v(\binom{\ell^r}{i}(-1)^i x_0^{\ell^r - i} y_0^i) \geq 1 + \beta \ell^r > 1 + \beta$).
- Since $v(x_0), v(y_0) \geq \beta$, it is clear that the valuation of the terms of degree greater than $\ell^r$ is greater than $\ell^r \beta$.

But obviously there must be (at least) two terms with minimal valuation, since they must cancel out. Therefore $v(\ell \cdot (x_0 - y_0)) = v(a \cdot (x_0 - y_0)^{\ell^r})$, that is to say, $1 + \beta = \ell^r \beta$, hence $\beta = 1/(\ell^r - 1)$, as was to be proven.

□

**Lemma 7.6.** *Let $\ell > 2$ be a prime number, $r \in \mathbb{N}$, and let $f(Z_1, Z_2) \in \mathbb{Z}_\ell[[Z_1, Z_2]]$ be a formal power series such that $f(Z_2, Z_1) = f(Z_1, Z_2)$, which can be written as:*

$$\begin{aligned} f(Z_1, Z_2) = \ell \cdot (Z_1 + Z_2) + \ell \cdot (&\textit{terms of total degree} \geq 2 \textit{ and} < \ell^r) \\ &+ a \cdot (Z_1^{\ell^r} + Z_2^{\ell^r}) + \textit{ terms of total degree} \geq \ell^r + 1, \end{aligned}$$

*where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ satisfies $f(x_0, y_0) = 0$ and furthermore $v(x_0), v(y_0) \geq v(x_0 + y_0)$, then $v(x_0 + y_0)$ is $1/(\ell^r - 1)$.*

*Proof.* Analogous to that of Lemma 7.5. □

We will finally state and prove the main theorem of this section:

**Theorem 7.7.** *Let $\mathbf{F} = (F_1, F_2)$ be a two dimensional symmetric formal group law over $\mathbb{Z}_\ell$. Assume it has height 4 and the exponent in Proposition 5.12 is $r = 2$. Let us call $V$ the $\mathbb{F}_\ell$-vector space of $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$, $\alpha = 1/(\ell^2 - 1)$, and $v$ the $\ell$-adic valuation.*

*Then for all $(x_0, y_0) \in V$,*

$$\min\{v(x_0), v(y_0)\} = \alpha.$$

*Proof.* First of all, let us recall that, since the formal group law $\mathbf{F}$ is symmetric and of height 4 with $r = 2$, Remark 7.2 allows us to write the two formal power series that comprise the multiplication by $\ell$ map in the following way:

$$\begin{cases} [\ell]_1(Z_1, Z_2) = \ell Z_1 + \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) \\ \qquad\qquad + a \cdot Z_1^{\ell^2} + b \cdot Z_2^{\ell^2} + \text{ terms of degree} \geq \ell^2 + 1 \\ [\ell]_2(Z_1, Z_2) = \ell Z_2 + \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) \\ \qquad\qquad + b \cdot Z_1^{\ell^2} + a \cdot Z_2^{\ell^2} + \text{ terms of degree} \geq \ell^2 + 1 \end{cases}$$

with $\ell \nmid a^2 - b^2$.

Take a point $P = (x_0, y_0) \in V$. We split the proof in two cases.

**Case 1**: $v(x_0) \neq v(y_0)$. Assume that $v(x_0) < v(y_0)$ (otherwise we proceed analogously). Then $v(x_0 - y_0) = v(x_0)$. We will apply Lemma 7.5 with $r = 2$. The point $(x_0, y_0)$ satisfies both equations $[\ell]_1(x_0, y_0) = 0$ and $[\ell]_2(x_0, y_0) = 0$. Therefore it also satisfies that $f(x_0, y_0) = [\ell]_1(x_0, y_0) - [\ell]_2(x_0, y_0) = 0$. Furthermore, taking into account the previous considerations, we can write

$$\begin{aligned} f(Z_1, Z_2) &= \ell(Z_1 - Z_2) + \\ &+ \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) + (a - b) \cdot (Z_1^{\ell^2} - Z_2^{\ell^2}) + \\ &+ \text{ terms of degree greater than or equal to } \ell^2 + 1, \end{aligned}$$

and $\ell \nmid a - b$. Nothing prevents us now from applying Lemma 7.5 and concluding that $v(x_0 - y_0) = \alpha$. But then $\alpha = v(x_0) < v(y_0)$, hence $\min\{v(x_0), v(y_0)\} = \alpha$.

**Case 2:** $v(x_0) = v(y_0)$. Then either $v(x_0 - y_0) = v(x_0)$ or $v(x_0 + y_0) = v(x_0)$. (For both must be greater than or equal to $v(x_0)$. And taking into account that $\ell \neq 2$, we obtain $v(x_0) = v(2x_0) = v((x_0 + y_0) + (x_0 - y_0))$, so both $v(x_0 + y_0)$ and $v(x_0 + y_0)$ cannot be greater than $v(x_0)$). If $v(x_0 - y_0) = v(x_0)$, we can apply Lemma 7.5 as in the previous case and conclude that $v(x_0) = v(y_0) = \alpha$. If $v(x_0 + y_0) = v(x_0)$, we make use of Lemma 7.6 with $f = [\ell]_1 + [\ell]_2$ and $r = 2$, thus concluding that $v(x_0) = v(y_0) = \alpha$. This completes the proof.

□

Combining this theorem with Theorem 4.9, we obtain the following result:

**Theorem 7.8.** *Let $\mathbf{F} = (F_1, F_2)$ be a two dimensional symmetric formal group law over $\mathbb{Z}_\ell$. Assume it has height 4 and the exponent in Proposition 5.12 is $r = 2$. Then the wild inertia group $I_{\mathrm{w}}$ acts trivially on the $\mathbb{F}_\ell$-vector space of $\ell$-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$.*

# Chapter 8

# Jacobian of symmetric genus 2 curves

We concluded the previous chapter by stating a theorem which guarantees that the wild inertia group $I_{\mathrm{w}}$ acts trivially on the $\ell$-torsion points of the group attached to a two-dimensional formal group law over $\mathbb{Z}_\ell$ of height 4, provided some conditions are satisfied. These conditions were of a very explicit nature, in the sense that they could be checked directly on the equations that define the formal group law.

In this chapter we are going to present a certain kind of genus 2 curves such that the formal group law attached to their Jacobians satisfies these properties, and therefore the results of the previous chapter can be applied. Firstly, we will deal with the symmetry condition. To do so, we will need an explicit method to compute the formal group law of a genus 2 curve, starting from a hyperelliptic equation. In [15], such a method is described. The reasonings that we will bring into play will have a very explicit flavour, since they will be grounded on the computation of the formal group law. In the last section we will take care of the exponent $r$ in Proposition 5.12.

From now on, we will restrict our attention to the Jacobians of genus 2 curves $C/\mathbb{Q}$, represented through a hyperelliptic equation

$$C : y^2 = f(x), \tag{8.1}$$

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 which has no multiple factors.

## 8.1 Symmetric genus 2 curves

Given a hyperelliptic equation of a genus 2 curve $C$, say (8.1), one can define an embedding of the Jacobian surface attached to $C$ into a projective space of dimension 15. This embedding is detailed in [15]. Let us sketch the construction. First of all, we will identify the Jacobian surface, which is by definition the Picard group $\mathrm{Pic}^0(C)$, with the Picard group $\mathrm{Pic}^2(C)$ consisting of equivalence classes of degree 2 divisors on $C$. Namely, one can define a correspondence between $\mathrm{Pic}^2(C)$ and $\mathrm{Pic}^0(C)$ in the following way: Note that, if $P$ is a point of $C$ and we denote by $P'$ the conjugate of $P$ through the hyperelliptic involution, all the divisors of the form $P + P'$ are linearly equivalent, and therefore represent the same class in $\mathrm{Pic}^2(C)$. Call it $\mathcal{O}$. Then the correspondence sends each divisor $D$ of degree 2 to the divisor $D - \mathcal{O}$ of degree zero.

In this way, we have identified the Jacobian surface attached to $C$ with $\mathrm{Pic}^2(C)$. The embedding into a projective space can therefore be defined as a map from the symmetric product of two copies of $C$ (that is, the set of non-ordered pairs of points of $C$) into $\mathbb{P}^{15}$,

$$\mathbf{z} = (z_0, z_1, \ldots, z_{15}) : C^{(2)} \to \mathbb{P}^{15}$$

(the expressions of the $z_i$, $0 \leq i \leq 15$, are given in the first section of Chapter 2 of [15]). The projective locus of the image of $\mathbf{z}$, which shall be written as $J(C)$, is the Jacobian of $C$.

Now $J(C)$ can be expressed by means of equations as a variety of $\mathbb{P}^{15}$. Namely, one can consider 72 quadratic equations, which can be found at

`http://www2.maths.ox.ac.uk/ flynn/genus2/jacobian.variety/defining.equations`

Since we are going to make use of them, we also list them in Appendix A.

Let us consider a genus 2 curve $C/\mathbb{Q}$ given by a hyperelliptic equation (8.1). In [15] there is an explicit algorithm to compute the formal group law $\mathbf{F}$ of the Jacobian variety (that is, the abelian surface) attached to $C$ at the point $\mathcal{O}$, the group identity (see also [28]). This formal group is given by two power series

$$F_1(s_1, s_2, t_1, t_2) = s_1 + t_1 + 2f_4 s_1^2 t_1 + 2f_4 s_1 t_1^2 - f_1 s_2^2 t_2 - f_1 s_2 t_2^2 + \cdots$$
$$F_2(s_1, s_2, t_1, t_2) = s_2 + t_2 + 2f_2 s_2^2 t_2 + 2f_2 s_2 t_2^2 - f_5 s_2^2 t_1 - f_5 s_1 t_1^2 + \cdots$$

The idea of the symmetry emerged from the curious observation that if in the second equation we interchange $f_4$ by $f_2$, $f_1$ by $f_5$ and $s_1$ by $s_2$, $t_1$ by $t_2$, we obtain exactly the first equation.

Is this just mere chance?

Let us write a precise statement, and see if we can prove it. Let us consider the hyperelliptic equation

$$y^2 = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_4x^2 + f_5x + f_6. \tag{8.2}$$

Note that the following transformation

$$(x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^3}\right)$$

brings Equation (8.1) into Equation (8.2), and so this is just another equation that represents the curve $C$.

In any case, we can consider the formal group law $\widetilde{\mathbf{F}}$ computed from Equation (8.2), which shall be denoted by

$$\widetilde{\mathbf{F}} = (\widetilde{F}_1(\widetilde{s}_1, \widetilde{s}_2, \widetilde{t}_1, \widetilde{t}_2), \widetilde{F}_2(\widetilde{s}_1, \widetilde{s}_2, \widetilde{t}_1, \widetilde{t}_2)).$$

The result we are going to prove in the next section is the following:

**Theorem 8.1.** *With the notations introduced in this section, the following relations hold.*

$$\begin{cases} \widetilde{F}_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2) \\ \widetilde{F}_1(s_2, s_1, t_2, t_1) = F_2(s_1, s_2, t_1, t_2). \end{cases}$$

As a corollary, this statement follows easily.

**Theorem 8.2.** *Let $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ be a polynomial of degree 6 and non-zero discriminant, and let $\mathbf{F} = (F_1, F_2)$ be the formal group law attached to the Jacobian variety of the curve defined by $y^2 = f(x)$. Then*

$$F_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2).$$

We will work with this type of curves. Let us give them a name.

**Definition 8.3.** We shall call a genus 2 curve *symmetric* if it can be expressed through an equation $y^2 = f(x)$, where $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ is a polynomial of degree 6 and non-zero discriminant.

## 8.2 Comparison between formal group laws

This section is devoted to the proof of Theorem 8.1. Let us refer by $J(C)$ to the Jacobian variety attached to the curve $C$ through Equation (8.1) following the procedure described above. Of course, one can apply the same procedure to Equation (8.2). In order to avoid misunderstandings, let us denote by $\widetilde{J}(C)$ the Jacobian variety that arises in this way. Of course, they are isomorphic, but the set of equations that define them as algebraic varieties in $\mathbb{P}^{15}$ are different. The first step will be to define an isomorphism between them.

Consider the following automorphism $\Phi : \mathbb{P}^{15} \to \mathbb{P}^{15}$, defined as:

$$\begin{array}{llll} a_0 \mapsto a_0, & a_1 \mapsto -a_2, & a_2 \mapsto -a_1, & a_3 \mapsto a_5, \\ a_4 \mapsto a_4, & a_5 \mapsto a_3, & a_6 \mapsto -a_9, & a_7 \mapsto -a_8, \\ a_8 \mapsto -a_7, & a_9 \mapsto -a_6, & a_{10} \mapsto a_{14}, & a_{11} \mapsto a_{13}, \\ a_{12} \mapsto a_{12}, & a_{13} \mapsto a_{11}, & a_{14} \mapsto a_{10}, & a_{15} \mapsto a_{15} \end{array}$$

We wish to show that $\Phi$ induces an isomorphism of algebraic varieties between $J(C)$ and $\widetilde{J}(C)$. It will be enough to see that the image of any point $(a_0 : a_1 : \cdots : a_{15})$ in $J(C)$ lies in $\widetilde{J}(C)$ (for, because of the symmetry of our setting, the same proof, suitably changed, would show that any point in $\widetilde{J}(C)$ maps into $J(C)$, and this suffices for our purposes).

**Lemma 8.4.** *Let* $\{\mathrm{eqn}1, \mathrm{eqn}2, \ldots, \mathrm{eqn}72\}$ *be the equations defining* $J(C)$*, and* $\{\mathrm{eqn}'1, \mathrm{eqn}'2, \ldots, \mathrm{eqn}'72\}$ *be the equations defining* $\widetilde{J}(C)$*. Then the change of variables* $\Phi$ *induces the following transformations:*

$$\begin{array}{lll} \mathrm{eqn}1 \mapsto \mathrm{eqn}'5, & \mathrm{eqn}2 \mapsto \mathrm{eqn}'6, & \mathrm{eqn}3 \mapsto \mathrm{eqn}'3, \\ \mathrm{eqn}5 \mapsto \mathrm{eqn}'1, & \mathrm{eqn}6 \mapsto \mathrm{eqn}'2, & \mathrm{eqn}8 \mapsto \mathrm{eqn}'11, \\ \mathrm{eqn}9 \mapsto \mathrm{eqn}'14, & \mathrm{eqn}11 \mapsto \mathrm{eqn}'8, & \mathrm{eqn}12 \mapsto \mathrm{eqn}'13, \\ \mathrm{eqn}13 \mapsto \mathrm{eqn}'12, & \mathrm{eqn}14 \mapsto \mathrm{eqn}'9, & \mathrm{eqn}16 \mapsto \mathrm{eqn}'18, \\ \mathrm{eqn}17 \mapsto \mathrm{eqn}'17, & \mathrm{eqn}18 \mapsto \mathrm{eqn}'16, & \mathrm{eqn}19 \mapsto \mathrm{eqn}'19, \\ \mathrm{eqn}20 \mapsto \mathrm{eqn}'21, & \mathrm{eqn}21 \mapsto \mathrm{eqn}'20, & \mathrm{eqn}25 \mapsto \mathrm{eqn}'29, \\ \mathrm{eqn}26 \mapsto \mathrm{eqn}'30, & \mathrm{eqn}28 \mapsto \mathrm{eqn}'32, & \mathrm{eqn}29 \mapsto \mathrm{eqn}'25, \\ \mathrm{eqn}30 \mapsto \mathrm{eqn}'26, & \mathrm{eqn}32 \mapsto \mathrm{eqn}'28, & \mathrm{eqn}33 \mapsto \mathrm{eqn}'42, \\ \mathrm{eqn}34 \mapsto \mathrm{eqn}'41, & \mathrm{eqn}35 \mapsto \mathrm{eqn}'39, & \mathrm{eqn}38 \mapsto \mathrm{eqn}'38, \\ \mathrm{eqn}39 \mapsto \mathrm{eqn}'35, & \mathrm{eqn}41 \mapsto \mathrm{eqn}'34, & \mathrm{eqn}42 \mapsto \mathrm{eqn}'33, \\ \mathrm{eqn}44 \mapsto \mathrm{eqn}'47 & \mathrm{eqn}45 \mapsto \mathrm{eqn}'48, & \mathrm{eqn}47 \mapsto \mathrm{eqn}'44, \\ \mathrm{eqn}48 \mapsto \mathrm{eqn}'45 & \mathrm{eqn}49 \mapsto \mathrm{eqn}'55, & \mathrm{eqn}50 \mapsto \mathrm{eqn}'56, \\ \mathrm{eqn}51 \mapsto \mathrm{eqn}'57 & \mathrm{eqn}52 \mapsto \mathrm{eqn}'58, & \mathrm{eqn}53 \mapsto \mathrm{eqn}'59, \\ \mathrm{eqn}54 \mapsto \mathrm{eqn}'60 & \mathrm{eqn}55 \mapsto \mathrm{eqn}'49, & \mathrm{eqn}56 \mapsto \mathrm{eqn}'50, \\ \mathrm{eqn}57 \mapsto \mathrm{eqn}'51 & \mathrm{eqn}58 \mapsto \mathrm{eqn}'52, & \mathrm{eqn}59 \mapsto \mathrm{eqn}'53, \\ \mathrm{eqn}60 \mapsto \mathrm{eqn}'54 & \mathrm{eqn}61 \mapsto \mathrm{eqn}'64, & \mathrm{eqn}62 \mapsto \mathrm{eqn}'65, \end{array}$$

$$\begin{array}{lll}
\mathrm{eqn63} \mapsto \mathrm{eqn}'66 & \mathrm{eqn64} \mapsto \mathrm{eqn}'61, & \mathrm{eqn65} \mapsto \mathrm{eqn}'62, \\
\mathrm{eqn66} \mapsto \mathrm{eqn}'63 & \mathrm{eqn67} \mapsto \mathrm{eqn}'68, & \mathrm{eqn68} \mapsto \mathrm{eqn}'67, \\
\mathrm{eqn69} \mapsto \mathrm{eqn}'72 & \mathrm{eqn70} \mapsto \mathrm{eqn}'71, & \mathrm{eqn71} \mapsto \mathrm{eqn}'70, \\
\mathrm{eqn72} \mapsto \mathrm{eqn}'69 &&
\end{array}$$

$$\begin{aligned}
\mathrm{eqn4} \;\mapsto & \mathrm{eqn}'4 + f_2 f_6 \mathrm{eqn}'16 - f_1 f_6 \mathrm{eqn}'20 + f_0 f_5 \mathrm{eqn}'21 - \\
& - f_0 f_4 \mathrm{eqn}'18 + f_2(\mathrm{eqn}'12 - f_4 \mathrm{eqn}'17 + f_5 \mathrm{eqn}'20) + \\
& + f_4(\mathrm{eqn}'13 - f_1 \mathrm{eqn}'21 + f_2 \mathrm{eqn}'17) \\
\mathrm{eqn7} \;\mapsto & \mathrm{eqn}'7 + 4 f_0 f_5 \mathrm{eqn}'21 - 4 f_1 f_6 \mathrm{eqn}'20 - 2 f_1 \mathrm{eqn}'11 - \\
& - f_4 f_1 \mathrm{eqn}'21 - 3 f_1 f_4 \mathrm{eqn}'21 + 2 f_5 \mathrm{eqn}'8 + 4 f_2 f_5 \mathrm{eqn}'20 + \\
& + 4 f_4(\mathrm{eqn}'13 - f_1 \mathrm{eqn}'21 + f_2 \mathrm{eqn}'17) + 4 f_2(\mathrm{eqn}'12 - \\
& - f_4 \mathrm{eqn}'17 + f_5 \mathrm{eqn}'20) + 2 f_3(\mathrm{eqn}'9 + \mathrm{eqn}'14) \\
\mathrm{eqn10} \mapsto & \mathrm{eqn}'15 - 2 f_4 \mathrm{eqn}'17 + 2 f_5 \mathrm{eqn}'20 + 2(\mathrm{eqn}'12 - f_4 \mathrm{eqn}'17 + \\
& + f_5 \mathrm{eqn}'20) \\
\mathrm{eqn15} \mapsto & \mathrm{eqn}'10 + 2 f_2 \mathrm{eqn}'17 + 2 f_1 \mathrm{eqn}'21 + 2(\mathrm{eqn}'13 - f_1 \mathrm{eqn}'21 + \\
& + f_2 \mathrm{eqn}'17) \\
\mathrm{eqn22} \mapsto & \mathrm{eqn}'24 + 2 f_0 f_5 \mathrm{eqn}'14 + 4 f_0 f_2 f_5 \mathrm{eqn}'21 - f_0 f_5^2 \mathrm{eqn}'16 - \\
& - 4 f_1 f_6 \mathrm{eqn}'8 - 4 f_1^2 f_6 \mathrm{eqn}'17 - 8 f_1 f_2 f_6 \mathrm{eqn}'20 - \\
& - 8 f_0 f_3 f_6 \mathrm{eqn}'20 + 4 f_0 f_4 f_6 \mathrm{eqn}'16 \\
\mathrm{eqn23} \mapsto & \mathrm{eqn}'23 + 2 f_0 f_4 \mathrm{eqn}'11 - 3 f_0 f_3 f_5 \mathrm{eqn}'21 - 2 f_0 f_4 f_5 \mathrm{eqn}'17 - \\
& - 3 f_1^2 f_6 \mathrm{eqn}'21 + 3 f_0 f_5^2 \mathrm{eqn}'20 - 12 f_0 f_2 f_6 \mathrm{eqn}'21 + \\
& + 3 f_1 f_3 f_6 \mathrm{eqn}'20 + 4 f_1 f_2 f_6 \mathrm{eqn}'17 + 12 f_0 f_4 f_6 \mathrm{eqn}'20 + \\
& + 4 f_0 f_4^2 \mathrm{eqn}'21 + 4 f_1 f_6 \mathrm{eqn}'13 + 4 f_1^2 f_6 \mathrm{eqn}'21 - \\
& - 4 f_1 f_2 f_6 \mathrm{eqn}'17 - 2 f_2 f_6 \mathrm{eqn}'8 - 4 f_2^2 f_6 \mathrm{eqn}'20 - \\
& - 2 f_1 f_2 f_6 \mathrm{eqn}'17 + 4 f_0 f_5(\mathrm{eqn}'12 - f_4 \mathrm{eqn}'17 + f_5 \mathrm{eqn}'20) \\
\mathrm{eqn24} \mapsto & \mathrm{eqn}'22 - 2 f_6 f_1 \mathrm{eqn}'9 - 4 f_6 f_4 f_1 \mathrm{eqn}'20 + f_6 f_1^2 \mathrm{eqn}'18 + \\
& + 4 f_5 f_0 \mathrm{eqn}'11 + 4 f_5^2 f_0 \mathrm{eqn}'17 + 8 f_5 f_4 f_0 \mathrm{eqn}'21 + \\
& + 8 f_6 f_3 f_0 \mathrm{eqn}'21 - 4 f_0 f_2 f_6 \mathrm{eqn}'18 \\
\mathrm{eqn27} \mapsto & \mathrm{eqn}'31 + 2 f_2 f_3 \mathrm{eqn}'21 + 4 f_1 f_4 \mathrm{eqn}'21 - 4 f_2 f_4 \mathrm{eqn}'17 - \\
& - 2 f_3 f_4 \mathrm{eqn}'20 - 4 f_4(\mathrm{eqn}'13 - f_1 \mathrm{eqn}'21 + f_2 \mathrm{eqn}'17) \\
\mathrm{eqn31} \mapsto & \mathrm{eqn}'27 + (-2 f_4 f_3 \mathrm{eqn}'20 + 4 f_5 f_2 \mathrm{eqn}'20 - 4 f_4 f_2 \mathrm{eqn}'17 + \\
& + 2 f_3 f_2 \mathrm{eqn}'21) - 4 f_2(\mathrm{eqn}'12 - f_4 \mathrm{eqn}'17 + f_5 \mathrm{eqn}'20)
\end{aligned}$$

$$\begin{aligned}
\mathrm{eqn}36 \mapsto & \mathrm{eqn}'36 + f_2\mathrm{eqn}'21 - f_4\mathrm{eqn}'20 \\
\mathrm{eqn}37 \mapsto & \mathrm{eqn}'40 + \mathrm{eqn}'12 \\
\mathrm{eqn}40 \mapsto & \mathrm{eqn}'37 + \mathrm{eqn}'13 \\
\mathrm{eqn}43 \mapsto & -\mathrm{eqn}'46 - f_3\mathrm{eqn}'58 - f_1\mathrm{eqn}'63 - 3f_1\mathrm{eqn}'65 - \\
& - 4f_0f_5\mathrm{eqn}'68 - 4f_0f_5\mathrm{eqn}'70 + f_3\mathrm{eqn}'61 \\
\mathrm{eqn}46 \mapsto & -\mathrm{eqn}'43 + f_3\mathrm{eqn}'52 + f_5\mathrm{eqn}'66 + 3f_5\mathrm{eqn}'62 + \\
& + 4f_6f_1\mathrm{eqn}'67 + 4f_6f_1\mathrm{eqn}'71 - f_3\mathrm{eqn}'64
\end{aligned}$$

From this lemma, whose proof is mere algebraic computation, it follows at once that $\Phi : J(C) \to \widetilde{J}(C)$ is an algebraic isomorphism. And note that the zero element of the sum law of $J(C)$ (and also of $\widetilde{J}(C)$) as an abelian variety in $\mathbb{P}^{15}$ is $(1 : 0 : 0 : \cdots : 0) \in \mathbb{P}^{15}$. Therefore $\Phi$ maps the zero element of $J(C)$ into the zero element of $\widetilde{J}(C)$. It is well known that this causes $\Phi$ to be an isomorphism of abelian varieties (see for instance Corollary 1.2 of [55]).

We still need to deal with a few small details in order to be ready to prove Theorem 8.1.

First of all, we want to prove equalities between formal power series, namely $\widetilde{F}_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2)$ and $\widetilde{F}_1(s_2, s_1, t_2, t_1) = F_2(s_1, s_2, t_1, t_2)$, where $s_1, s_2, t_1, t_2$ are variables. We will not prove it directly. Instead, we will prove that, for all tuples $(s_1, s_2, t_1, t_2) \in \overline{\mathfrak{m}}^{\times 4}$, the equalities are satisfied. But this is enough to ensure that the equality between formal power series holds. More precisely, we can use the following result.

**Lemma 8.5.** *Let $G(X_1, \ldots, X_n) \in \mathbb{Z}_\ell[[X_1, \ldots, X_n]]$ be a formal power series. Assume that it holds that $G(x_1, \ldots, x_n) = 0$ for all tuples $(x_1, \ldots, x_n) \in \overline{\mathfrak{m}}^{\times n}$. Then $G(X_1, \ldots, X_n) = 0$ in $\mathbb{Z}_\ell[[X_1, \ldots, X_n]]$.*

*Proof.* We will proceed by induction. Assume first that the dimension $n$ is 1, that is to say, $G(X)$ is a formal power series in one variable with coefficients in $\mathbb{Z}_\ell$. Consider the formal power series $G_1(X) := G(\ell \cdot X)$. This is a restricted formal power series. By hypothesis, we know that, for all $x \in \overline{\mathfrak{m}}$, $G(x) = 0$. Therefore, the same is true for $G_1(X)$. Now we can apply a well-known result of Strassman (see [71], pg. 306), and conclude that $G_1(X)$ must be equal to zero. This implies that $G(X) = 0$.

Once we have settled the case of dimension 1 we are ready to tackle the induction step. Assume that the lemma is true for dimension $n$, and let us prove it for dimension $n+1$. Let $G(X_1, \ldots, X_n, X_{n+1})$ be a formal power series satisfying the hypothesis of the lemma. Fix any tuple $(x_1, \ldots, x_n) \in \overline{\mathfrak{m}}^{\times n}$. Now the formal power series in one variable $G(x_1, \ldots, x_n, X_{n+1})$ satisfies the hypothesis of the lemma for dimension 1. Therefore, by the considerations made at the beginning of the proof, we know that it vanishes in $\mathbb{Z}_\ell[[X_{n+1}]]$. In other words, if we consider $G(X_1, \ldots, X_n, X_{n+1}) \in \mathbb{Z}_\ell[[X_1, \ldots, X_n]][[X_{n+1}]]$ as a formal power series in $X_{n+1}$ with coefficients in $\mathbb{Z}_\ell[[X_1, \ldots, X_n]]$, the statement above means that all the coefficients satisfy the hypothesis of the lemma for dimension $n$. Therefore, by the induction hypothesis, they all vanish, and thus $G(X_1, \ldots, X_n, X_{n+1})$ vanishes in $\mathbb{Z}_\ell[[X_1, \ldots, X_n, X_{n+1}]]$. □

Next, we need to establish another technical lemma. Recall that we considered the formal group law $\mathbf{F} = (F_1, F_2)$ on $J(C)$, computed by means of the algorithm outlined in [15].

**Lemma 8.6.** *The following identities hold*

$$F_1(-s_1, -s_2, -t_1, -t_2) = -F_1(s_1, s_2, t_1, t_2)$$
$$F_2(-s_1, -s_2, -t_1, -t_2) = -F_2(s_1, s_2, t_1, t_2).$$

*Proof.* If we denote by $(z_0 : z_1 : \cdots : z_{15})$ the coordinates in $\mathbb{P}^{15}$, we can consider the localized coordinates, $s_i = z_i/z_0$. As a first step to compute the formal group law $\mathbf{F}$, in Chapter 7, Section 1 of [15] is proven that $(s_1, s_2)$ is a pair of local parameters for $J(C)$.

By Lemma 8.5, it suffices to show that, for any $s_1, s_2, t_1, t_2 \in \overline{\mathfrak{m}}$, $F_i(-s_1, -s_2, -t_1, -t_2) = -F_i(s_1, s_2, t_1, t_2)$, $i = 1, 2$. Let us take then any two points of $F(\overline{\mathfrak{m}})$, say $(s_1, s_2)$ and $(t_1, t_2)$. We can consider two points in $J(C)$,

$$A = (a_0 : a_1 : a_2 : \cdots : a_{15}) \text{ and } B = (b_0 : b_1 : b_2 : \cdots : b_{15}),$$

such that $a_0, b_0 \neq 0$ and $s_1 = a_1/a_0$, $s_2 = a_2/a_0$, $t_1 = b_1/b_0$, $t_2 = b_2/b_0$. Therefore, it suffices to show that

$$F_i(a_1/a_0, a_2/a_0, b_1/b_0, b_2/b_0) = -F_i(-a_1/a_0, -a_2/a_0, -b_1/b_0, -b_2/b_0).$$

The idea of the proof can be easily grasped by considering how the sum in the Jacobian of $C$ can be geometrically interpreted (generically)

in terms of these inverse images in $C$. Namely, recall that the Jacobian of $C$ was embedded in $\mathbb{P}^{15}$ through the map

$$\mathbf{z} = (z_0, z_1, \ldots, z_{15}) : C^{(2)} \to \mathbb{P}^{15},$$

which we did not write explicitly. Therefore, both points $A$ and $B$ have an inverse image, say the pairs $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$ of points of $C$. Assume that these points have coordinates $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q_1 = (u_1, v_1)$, $Q_2 = (u_2, v_2)$. Now consider the (only) cubic

$$Y = \alpha X^3 + \beta X^2 + \gamma X + \delta$$

that passes through the four points $P_1, P_2, Q_1, Q_2$. This cubic intersects $C$ in two additional points, say $R_1$ and $R_2$. Then the image through $\mathbf{z}$ of the pair $\{R_1, R_2\}$ is the opposite of sum of $A$ and $B$ in $J(C)$.

Consider now the images of $P_1$, $P_2$, $Q_1$, $Q_2$ through the hyperelliptic involution $Y \mapsto -Y$, say $P_1', P_2', Q_1', Q_2', R_1', R_2'$. Then the cubic given by the equation

$$Y = -\alpha X^3 - \beta X^2 - \gamma X - \delta$$

contains these six points, which means that the opposite of the sum of the points in $J(C)$ corresponding to the pairs $\{P_1', P_2'\}$ and $\{Q_1', Q_2'\}$ is the point corresponding to $\{R_1', R_2'\}$.

At this stage, it is necessary to make use of the explicit expressions of the maps $z_0$, $z_1$ and $z_2$ (which appear in the first section of Chapter 2 of [15]) in order to check that the following identities hold

$$\begin{cases} z_0(x_1, -y_1, x_2, -y_2) = z_0(x_1, y_1, x_2, y_2) \\ z_1(x_1, -y_1, x_2, -y_2) = -z_1(x_1, y_1, x_2, y_2) \\ z_2(x_1, -y_1, x_2, -y_2) = -z_2(x_1, y_1, x_2, y_2). \end{cases}$$

Therefore, if we consider the points $P_1' = (x_1, -y_1)$, $P_2' = (x_2, -y_2)$, $Q_1' = (u_1, -v_1)$ and $Q_2' = (u_2, -v_2)$ (which also belong to $C$), and call $A' = \mathbf{z}(x_1, -y_1, x_2, -y_2)$, $B' = \mathbf{z}(u_1, -v_1, u_2, -v_2)$, we obtain that the local parameters of $A'$ are $(-a_1/a_0, -a_2/a_0)$ and the local parameters of $B'$ are $(-b_1/b_0, -b_2/b_0)$.

Let us rephrase this reasoning by using the representation of the sum in $J(C)$ by means of divisors. To prove that the inverse of the sum of the points $A$ and $B$ is the sum of $A'$ and $B'$, it is enough to

show that their inverse images through the map $\mathbf{z}$ satisfy this property, that is to say, that the sum of the corresponding divisors in $\mathrm{Pic}^2(C)$ is zero. But this is immediate, since the divisor of the pair $\{P_1, P_2\}$ is $P_1 + P_2$, the divisor of the pair $\{Q_1, Q_2\}$ is $Q_1 + Q_2$, the divisor of the pair $\{P_1', P_2'\}$ is $P_1' + P_2'$ and the divisor of the pair $\{Q_1', Q_2'\}$ is $Q_1' + Q_2'$. Their sum is consequently $P_1 + P_2 + Q_1 + Q_2 + P_1' + P_2' + Q_1' + Q_2' = (P_1 + P_1') + (P_2 + P_2') + (Q_1 + Q_1') + (Q_2 + Q_2') = \mathcal{O}$. This completes the proof of the lemma.

□

We are now ready to prove Theorem 8.1.

*Proof.* We will prove that $\widetilde{F}_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2)$. The proof of the remaining identity is analogous.

As in the proof of the previous lemma, it suffices to show that, for any two points in $J(C)$ $A = (a_0 : a_1 : \cdots : a_{15})$ and $B = (b_0 : b_1 : \cdots : b_{15})$ with $a_0, b_0 \neq 0$, then $\widetilde{F}_2(a_2/a_0, a_1/a_0, b_2/b_0, b_1/b_0) = F_1(a_1/a_0, a_2/a_0, b_1/b_0, b_2/b_0)$. Let us call $D = (d_0 : d_1 : \cdots : d_{15})$ the point $A + B$ (Note that $d_0$ cannot vanish, since the sum given by the formal group law on $\overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ is closed and $\mathbf{F}(\overline{\mathfrak{m}}) \simeq A_1(\overline{K})$). By definition of the formal group law, we know that

$$F_1(a_1/a_0, a_2/a_0, b_1/b_0, b_2/b_0) = d_1/d_0. \tag{8.3}$$

On the other hand, since $\Phi$ is an isomorphism of abelian varieties, we have the identity $\Phi(A) + \Phi(B) = \Phi(D)$. In particular, calling $\Phi(A) = (\widetilde{a}_0 : \widetilde{a}_1 : \cdots : \widetilde{a}_{15})$ and similarly $\Phi(B) = (\widetilde{b}_0 : \widetilde{b}_1 : \cdots : \widetilde{b}_{15})$ and $\Phi(D) = (\widetilde{d}_0 : \widetilde{d}_1 : \cdots : \widetilde{d}_{15})$, we have that $\widetilde{F}_2(\widetilde{a}_1/\widetilde{a}_0, \widetilde{a}_2/\widetilde{a}_0, \widetilde{b}_1/\widetilde{b}_0, \widetilde{b}_2/\widetilde{b}_0) = \widetilde{d}_2/\widetilde{a}_0$. But now, recalling the definition of $\Phi$ coordinatewise, this identity can be expressed as

$$\widetilde{F}_2(-a_2/a_0, -a_1/a_0, -b_2/b_0, -b_1/b_0) = -d_1/d_0. \tag{8.4}$$

Combining Equation (8.3) with Equation (8.4), we obtain that

$$F_1(a_1/a_0, a_2/a_0, b_1/b_0, b_2/b_0) = \\ = -\widetilde{F}_2(-a_2/a_0, -a_1/a_0, -b_2/b_0, -b_1/b_0).$$

Applying Lemma 8.6, we conclude the proof.

□

## 8.3 Shape of the multiplication by $\ell$ map

In Chapter 5, we proved a Proposition about the shape of a homomorphism between formal group laws, namely Proposition 5.12. Let us recall the statement in the case of dimension 2. Given a homomorphism $\overline{\mathbf{f}} : \overline{\mathbf{F}} \to \overline{\mathbf{G}}$ between two formal group laws of dimension 2 over a finite field $k$ of characteristic $\ell$, the proposition claims the existence of an exponent $r$ such that the formal power series $\overline{f}_1, \overline{f}_2 \in k[[Z_1, Z_2]]$ which define $\overline{\mathbf{f}}$ can be written as formal power series in $Z_1^{\ell^r}$, $Z_2^{\ell^r}$. Furthermore, we saw that if we consider a formal group law $\overline{\mathbf{F}}$ of dimension 2 and height 4, and take $\overline{\mathbf{f}}$ to be the endomorphism of multiplication by $\ell$, then there are only two possibilities for the exponent $r$, namely, either $r = 2$ or $r = 1$ (see Remark 7.2). Through the remainder of Chapter 7, we assumed that the value of the exponent $r$ was two, and claimed that we would deal with such condition in this chapter. Let us do so now.

Our aim will be to prove that, under some suitable conditions, the formal group law satisfies the following hypothesis.

**Hypothesis 8.7.** *There exist two formal power series $\overline{g}_1(Z_1, Z_2)$ and $\overline{g}_2(Z_1, Z_2)$ such that the multiplication by $\ell$ map $\overline{[\ell]} = (\overline{[\ell]}_1, \overline{[\ell]}_2)$ in the 2-dimensional formal group law $\overline{\mathbf{F}}$ is given by*

$$\begin{cases} \overline{[\ell]}_1(Z_1, Z_2) = \overline{g}_1(Z_1^{\ell^2}, Z_2^{\ell^2}) \\ \overline{[\ell]}_2(Z_1, Z_2) = \overline{g}_2(Z_1^{\ell^2}, Z_2^{\ell^2}). \end{cases}$$

Our starting point is that the formal group law attached to a product of two supersingular elliptic curves trivially satisfies this claim, since in dimension 1 the exponent $r$ for a formal group law coincides with its height, which is 2 in the supersingular case. Furthermore, by definition a supersingular abelian surface $A$ over $k$ is isogenous over $\overline{k}$ to a product of two supersingular elliptic curves (recall Definition 4.4). Is there a way to transfer this property from the product of elliptic curves to the abelian surface through the isogeny?

First of all, note that if our isogeny is defined over the field $k$ and has degree prime to $\ell$, then it preserves this property.

**Lemma 8.8.** *Let $A$ and $B$ be abelian varieties defined over $k$, and $\Phi : B \to A$ an isogeny of degree prime to $\ell$. Assume moreover that the formal group law attached to $B$ satisfies Hypothesis 8.7. Then the formal group law attached to $A$ satisfies it too.*

*Proof.* Let $m$ be the degree of $\Phi$. By the considerations made on Chapter II, § 1 of [42], we know that there exists an isogeny $\Psi : A \to B$ (the dual isogeny of $\Phi$) such that $\Psi \circ \Phi = [m]_B$.

Consider the following commutative diagram:

$$\begin{array}{ccc} B & \xrightarrow{[\ell]_B} & B \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ A & \xrightarrow{[\ell]_A} & A \end{array}$$

We know that $\Phi \circ [\ell]_B = [\ell]_A \circ \Phi$. Therefore, $\Phi \circ [\ell]_B \circ \Psi = [\ell]_A \circ \Phi \circ \Psi$; and thus $\Phi \circ [\ell]_B \circ \Psi = [\ell]_A \circ [m]_A$.

Consider now the homomorphism these arrows induce on the formal group laws on $A$ and $B$ (we will not change their names). Since the reduction of $\overline{[\ell]}_B$ modulo $\ell$ can be expressed by means of formal power series in $Z_1^{\ell^2}, Z_2^{\ell^2}$, the same is true of the composition $\Phi \circ \overline{[\ell]}_B \circ \Psi = \overline{[\ell]}_A \circ \overline{[m]}_A$. But since the multiplication by $m$ map in the formal group law of $A$ is defined by

$$\begin{cases} \overline{[m]}_1(Z_1, Z_2) = mZ_1 + \cdots \\ \overline{[m]}_2(Z_1, Z_2) = mZ_2 + \cdots \end{cases}$$

it cannot happen that any of the two formal power series that define $[\ell]_A$ possesses a term of degree smaller than $\ell^2$ (for $m$ is invertible in $k$). Taking into account Proposition 5.12, we conclude that the multiplication by $\ell$ map in $A$ must also be expressible as a formal power series in $Z_1^{\ell^2}, Z_2^{\ell^2}$. □

The rest of the section is devoted to applying this lemma in a particular case. In Chapter 14 of [15], a kind of genus 2 curves is introduced, namely *bielliptic* curves, which are those which satisfy one of the equivalent conditions of Theorem 14.1.1 of [15]. For instance, condition (i) is that the curve can be expressed by a hyperelliptic equation without terms of odd degree in $x$, that is to say, an equation of the shape $y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0$. Also recall that at the beginning of this chapter we gathered that a symmetric curve would suit us. Therefore, we will consider symmetric bielliptic curves. Namely, we will focus on genus 2 curves $C$ which are given by a hyperelliptic equation

$$y^2 = x^6 + bx^4 + bx^2 + 1, \tag{8.5}$$

for a certain $b \in \mathbb{F}_\ell$, which moreover are supersingular. Whether for a given $\ell$ there exists such a curve is another issue, which will be dealt with in later chapters. For the moment, we will assume we have such a curve, and heed not the fact that we may be theorizing about the empty set.

Note that the Jacobian of $C$ is isogenous (over $\mathbb{F}_\ell$) to $E \times E$, where $E$ is the elliptic curve given by the Weierstrass equation $y^2 = x^3+bx^2+bx+1$. In order to check that the Jacobian of $C$ satisfies Hypothesis 8.7, one can explicitly compute the equations of the morphism of formal group laws that this isogeny induces. In fact, this is what we did at first, following the procedure described in Chapter 7 of [15]. Later, thanks to a remark of J. González, we found that this question we are considering is already treated in the literature. For instance, there is the following result (cf. Proposition 3 of [37]).

**Proposition 8.9.** *Let $E$ and $F$ be two elliptic curves over $\mathbb{F}_\ell$, let $A$ be the polarized abelian surface $E \times F$, and let $G \subset A[2](\overline{\mathbb{F}}_\ell)$ be the graph of a group isomorphism $\psi : E[2](\overline{\mathbb{F}}_\ell) \to F[2](\overline{\mathbb{F}}_\ell)$. Then $G$ is a maximal isotropic subgroup of $A[2](\overline{\mathbb{F}}_\ell)$, and furthermore the quotient polarized abelian variety $A/G$ is isomorphic to the Jacobian of a curve $C$ over $\overline{\mathbb{F}}_\ell$, unless $\psi$ is the restriction to $E[2](\overline{\mathbb{F}}_\ell)$ of an isomorphism $E \to F$ over $\overline{\mathbb{F}}_\ell$. Moreover, the curve $C$ and the isomorphisms are defined over $\mathbb{F}_\ell$ if $\psi$ is an isomorphism of* $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$*-modules.*

Let us consider the elliptic curve $E$ defined by the Weierstrass equation

$$y^2 = x^3 + bx^2 + bx + 1.$$

Then the 2-torsion points of $E$ are the following:

$$\begin{aligned} &O \\ &P_1 := (-1, 0) \\ &P_2 := (\frac{1}{2}(1 - b + \sqrt{-3 - 2b + b^2}), 0) \\ &P_3 := (\frac{1}{2}(1 - b - \sqrt{-3 - 2b + b^2}), 0). \end{aligned}$$

Let us consider the group morphism $\psi : E[2](\overline{\mathbb{F}}_\ell) \to E[2](\overline{\mathbb{F}}_\ell)$ defined as

$$O \mapsto O, \;\; P_1 \mapsto P_1, \;\; P_2 \mapsto P_3, \;\; P_3 \mapsto P_2.$$

Note that it is compatible with the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. In order to apply Proposition 8.9, we need to check that $\psi$ is not induced from an automorphism of $E$.

But the group of automorphisms of $E$ is well known (cf. [84], Chapter III, § 10). Namely, if $E$ is an elliptic curve with $j$-invariant different from 0 or 1728 (that is to say, with $b$ different from 0 or $-3/2$), then the group of automorphisms of $E$ has order 2, and the non-trivial automorphism corresponds to $(x, y) \mapsto (x, -y)$. Therefore, it cannot restrict to the morphism $\psi$. In the other cases, the order of $\mathrm{Aut}(E)$ is 4 or 6: it is easy to compute these automorphisms explicitly and check that they cannot restrict to $\psi$.

Therefore, for each $b \in \mathbb{F}_\ell$ such that the equation $y^2 = x^3 + bx^2 + bx + 1$ defines an elliptic curve $E$ (i.e., $b \neq 3, -1$), Proposition 8.9 tells us that there exists a genus 2 curve $C$ and an isogeny

$$\Phi : E \times E \to J(C)$$

which is separable (because of the definition of the quotient of abelian varieties, cf. § 7 Chapter 2, Theorem on p. 66 of [56]) of degree 4. Moreover, the isogeny can be defined over $\mathbb{F}_\ell$. Therefore, if $E$ is a supersingular elliptic curve we can apply Lemma 8.8 and conclude that the Jacobian of $C$ satisfies Hypothesis 8.7. But can $C$ be explicitly determined? Fortunately, Proposition 4 of [37] gives a very explicit recipe for computing $C$. As a conclusion, we can state the following result.

**Proposition 8.10.** *Let $b \in \mathbb{F}_\ell$ be such that the Weierstrass equation $y^2 = x^3 + bx^2 + bx + 1$ defines a supersingular elliptic curve over $\mathbb{F}_\ell$. Then the Jacobian of the genus 2 curve $C$ defined by the hyperelliptic equation*

$$y^2 = x^6 + bx^4 + bx^2 + 1$$

*satisfies Hypothesis 8.7.*

# Chapter 9

# Summary of results (abelian surfaces)

Once more, we will make a brief interlude and devote a chapter to collecting the results that we have already discussed. The tameness of the Galois extension obtained from the Galois representation attached to the $\ell$-torsion points of an abelian surface at a prime $p \neq \ell$ was already dealt with in Theorem 3.7. Regarding the tameness at $\ell$, we have proved that it suffices to ensure that Hypothesis 4.7 holds. From that point on, we have laboured to find explicit conditions that guarantee that this hypothesis holds. Put in a nutshell, we need that the formal group law of the abelian surface is symmetric and satisfies that the exponent in Proposition 5.12 is two. Note that these two conditions have a completely different nature: the first one involves characteristic 0; we need that the formal group law attached to $A/\mathbb{Q}_\ell$ is symmetric, whereas the second one is in fact a condition on the reduction of $A$ at $\ell$.

Firstly, we will write a statement about abelian surfaces which do not necessarily come from genus 2 curves, but which is valid in general:

**Theorem 9.1.** *Let $A/\mathbb{Q}$ be an abelian surface, and let $\ell > 2$ be a prime number. Let $\mathcal{P}$ be the set of prime numbers that divide the order of $\mathrm{GL}_4(\mathbb{F}_\ell)$. Assume that the following conditions hold:*

- *For all $p \in \mathcal{P}$ different from $\ell$, $A$ has semistable reduction at $p$.*
- *The formal group law attached to $A/\mathbb{Q}_\ell$ is symmetric.*

- *The reduction of $A$ at $\ell$ is a supersingular abelian variety such that there is an isogeny defined over $\mathbb{F}_\ell$, of degree prime to $\ell$, from $A$ to a product of two supersingular elliptic curves defined over $\mathbb{F}_\ell$.*

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

*Proof.* This result is a combination of Theorem 6.2, Theorem 7.8 and Lemma 8.8. □

Theorem 7.8 gave some conditions that ensured that the action of the wild inertia group at $\ell$ was trivial. These conditions were very explicit, in the sense that they could be checked simply by looking at the formal power series that define the formal group law. In Chapter 8, we restricted our attention to the Jacobians of genus 2 curves. We managed to find conditions which ensure that those of Theorem 7.8 will hold, and which can be read directly in the coefficients of a hyperelliptic equation of the curve. Therefore, a result of a very explicit nature like the one below was to be expected.

**Theorem 9.2.** *Let $C$ be a genus 2 curve defined by a hyperelliptic equation*

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

*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 $\mathrm{GL}_4(\mathbb{F}_\ell)$. Assume that the following conditions hold:*

- *For all $p \in \mathcal{P}$ different from $\ell$, $C$ has stable reduction at $p$.*
- *The reduction of $f(x)$ modulo $\ell$ 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.*

*Proof.* This result is a direct consequence of Theorem 6.2, Theorem 7.8, Theorem 8.2 and Proposition 8.10. Also one needs to recall that the genus 2 curve $C$ has stable reduction at a prime $p$ if and only if the Jacobian surface attached to it has semistable reduction at $p$ (see [48], Remark 4.26 of chapter 10). □

# Chapter 10

# Approximation to symmetry

An attentive reader might have been anxious to point out an objection before we go further. Namely, in order to obtain tame ramification at the prime $\ell$, we have resolved to consider the Jacobian of a very specific genus 2 curve. In particular, we asked that it be symmetric, that is to say, that it could be represented by a hyperelliptic equation of the form

$$y^2 = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

But, alas! the endomorphism ring of such a curve contains the involution $(x, y) \mapsto (1/x, y/x^3)$. In fact, the Jacobian of such a curve is reducible. Therefore, the image of the representation attached to the $\ell$-torsion points of this Jacobian cannot be $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (for, if the Jacobian splits into the product of $E_1$ and $E_2$, then the image of this representation is contained in $M_p = \{(s, s') \in \mathrm{Aut}(E_1[\ell]) \times \mathrm{Aut}(E_2[\ell]) : \det s = \det s'\}$, which is strictly smaller than $\mathrm{GSp}_4(\mathbb{F}_\ell)$; see [65]).

And in fact it is so. It will not do to take this curve in the hope of obtaining a representation with large image. Yet there is a way to get around this difficulty. Namely, we are going to take a curve which is "approximately symmetric", that is to say, symmetric up to a certain order with respect to the $\ell$-adic valuation.

Recall that we needed the symmetry in order to assert that the formal group attached to the Jacobian of our curve was symmetric in the sense of Definition 7.3. In turn, we used this symmetry in Theorem 7.7 to ensure that the formal group satisfies Hypothesis 4.7. So our aim in this chapter is the following: given a symmetric curve $C$,

to find another curve $C'$, which is not symmetric, but such that the corresponding formal group law still satisfies Hypothesis 4.7. More specifically, we wish to determine how close the coefficients of a hyperelliptic equation of $C'$ must be to those of a hyperelliptic equation of $C$ so that the condition in Hypothesis 4.7 is preserved. The main result of this chapter is the following.

**Theorem 10.1.** *Let $C$ be a genus 2 curve given by a hyperelliptic equation*

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

*where $f_0, \ldots, f_6 \in \mathbb{Z}_\ell$, and consider the genus 2 curve $C'/\mathbb{Q}_\ell$ given by the equation*

$$y^2 = f'_6x^6 + f'_5x^5 + f'_4x^4 + f'_3x^3 + f'_2x^2 + f'_1x + f'_0$$

*with $f'_0, \ldots, f'_6 \in \mathbb{Z}_\ell$ and satisfying $f_i - f'_i \in (\ell^4)$. Then if the formal group law attached to the Jacobian of $C$ satisfies Hypothesis 4.7, so does the formal group law attached to the Jacobian of $C'$.*

The rest of the chapter is devoted to proving it. Fix a genus 2 curve $C/\mathbb{Q}_\ell$, given by a hyperelliptic equation

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_0, \ldots, f_6 \in \mathbb{Z}_\ell$, and consider the genus 2 curve $C'/\mathbb{Q}_\ell$ given by the equation

$$y^2 = f'_6x^6 + f'_5x^5 + f'_4x^4 + f'_3x^3 + f'_2x^2 + f'_1x + f'_0$$

with $f'_0, \ldots, f'_6 \in \mathbb{Z}_\ell$.

Denote by $\mathbf{F} = (F_1, F_2)$ (resp. $\mathbf{F}' = (F'_1, F'_2)$) the formal group law attached to $C$ (resp. $C'$). It can be proven that the coefficients of $F_i$ (resp. $F'_i$) lie in $\mathbb{Z}[f_0, \ldots, f_6]$ (resp. $\mathbb{Z}[f'_0, \ldots, f'_6]$), $i = 1, 2$.

Therefore, if we assume that, for all $i = 0, \ldots, 6$, $f_i - f'_i \in (\ell^r)$, then the difference $F_i(s_1, s_2, t_1, t_2) - F'_i(s_1, s_2, t_1, t_2)$ has coefficients in $(\ell^r)$. Hence we may drop the curves and work in the formal group setting, since all we have to determine is the exponent $r$ which preserves Hypothesis 4.7 (once we know its value, it is simple to construct a genus 2 curve $C'$ whose corresponding formal group law satisfies Hypothesis 4.7 but which is not symmetric).

Denote by $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$, and $\overline{\mathfrak{m}} \subset \overline{\mathbb{Q}}_\ell$ the set of elements with positive valuation. Recall that Hypothesis 4.7 was a statement about the valuations of the coordinates of the $\ell$-torsion points of the group $\mathbf{F}(\overline{\mathfrak{m}})$ attached to the formal group law $\mathbf{F}$. Namely, call $[\ell]_1(Z_1, Z_2), [\ell]_2(Z_1, Z_2)$ (resp. $[\ell]'_1(Z_1, Z_2), [\ell]'_2(Z_1, Z_2)$) the equations defining the multiplication by $\ell$ map in $\mathbf{F}$ (resp. $\mathbf{F}'$). Then the hypothesis claims that for all non-zero pairs $(x, y) \in \overline{\mathfrak{m}}^2$, with $[\ell]_1(x, y) = [\ell]_2(x, y) = 0$ it holds that

$$\min\{v(x), v(y)\} = \alpha,$$

where $\alpha = 1/(\ell^2 - 1)$.

Now, if the coefficients of the power series $[\ell]_1(Z_1, Z_2), [\ell]_2(Z_1, Z_2)$ are close (with respect to the $\ell$-adic valuation) to the coefficients of the series $[\ell]'_1(Z_1, Z_2), [\ell]'_2(Z_1, Z_2)$, does this imply that the solutions of the system of equations $[\ell]_1(Z_1, Z_2) = [\ell]_2(Z_1, Z_2) = 0$ are close to the solutions of the system of equations $[\ell]'_1(Z_1, Z_2) = [\ell]'_2(Z_1, Z_2) = 0$?

A precise answer to this question can be found in [9], chapter III, § 4, n° 5. The reasoning is carried out in the context of restricted formal power series. For the sake of completeness, and since it will not take us too long, we will include here a (quite thorough) sketch of the reasoning, adapting it to this context.

For a while, we will change the setting, and introduce some notation. Let $A$ be a commutative ring, and fix an ideal $\mathfrak{m}$ of $A$. Assume that $A$ is separable and complete with respect to the $\mathfrak{m}$-adic topology, that is to say, that $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$ is equal to the neutral element of $A$ and $A$ is isomorphic to its completion with respect to this topology (see [9], Chapter 3, § 4, $n°5$, and also cf. [3], Chapter 10). For instance, we can take $A = \mathbb{Z}_\ell$, $\mathfrak{m} = \ell \cdot \mathbb{Z}_\ell$. As usual, we will denote in boldface the tuples of elements.

Consider a system of $n$ power series in $n$ variables,

$$\mathbf{f} = (f_1, \ldots, f_n), \quad f_i \in A[[X_1, \ldots, X_n]].$$

We will denote by $M_{\mathbf{f}}$ the Jacobian matrix, that is to say,

$$M_{\mathbf{f}} = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{X_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial f_n}{\partial X_1} & \cdots & \frac{\partial f_n}{X_n} \end{pmatrix},$$

and we will denote by $J_{\mathbf{f}}$ the determinant of $M_{\mathbf{f}}$. By $\mathfrak{m}^{\times n}$ we shall mean the cartesian product of $\mathfrak{m}$ with itself $n$ times. Furthermore we will denote $\mathbf{1}_n = (X_1, \ldots, X_n) \in A[[X_1, \ldots, X_n]]^{\times n}$.

We have the following proposition (see [9], chap. III, § 4):

**Proposition 10.2.** *Let $\mathbf{g} = (g_1, \ldots, g_n)$ be a system of power series in $A[[X_1, \ldots, X_n]]$, without constant term, such that $J_{\mathbf{g}}(0)$ is an invertible element of $A$. Then it holds:*

- *There exists another system of power series in $A[[X_1, \ldots, X_n]]$ without constant term, $\mathbf{h} = (h_1, \ldots, h_n)$, such that*

$$\mathbf{g} \circ \mathbf{h} = \mathbf{1}_n.$$

  *This system is unique and furthermore $\mathbf{h} \circ \mathbf{g} = \mathbf{1}_n$.*

- *For all $\mathbf{x} \in \mathfrak{m}^{\times n}$, we have that $\mathbf{g}(\mathbf{x}) \in \mathfrak{m}^{\times n}$, and $\mathbf{x} \mapsto \mathbf{g}(\mathbf{x})$ is a bijection from $\mathfrak{m}^{\times n}$to itself.*

This proposition allows us to prove the following theorem (cf. Theorem 2 of [9], chap. III, § 4):

**Theorem 10.3.** *Let $\mathbf{f} = (f_1, \ldots, f_n)$ be a system of elements in $A[[X_1, \ldots, X_n]]$, and let $\mathbf{a} \in \mathfrak{m}^{\times n}$. Call $J_{\mathbf{f}}(\mathbf{a}) = e$. There exists another system $\mathbf{g} = (g_1, \ldots, g_n)$ of elements of $A[[X_1, \ldots, X_n]]$ without constant term such that:*

*(i)* $M_{\mathbf{g}}(0) = I_n$.

*(ii) For all $\mathbf{x} \in A^n$, it holds that*

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{x}) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{g}(\mathbf{x})).$$

*(iii) Let $\mathbf{h} = (h_1, \ldots, h_n)$ be the system of formal power series without constant term such that $\mathbf{g} \circ \mathbf{h} = \mathbf{1}_n$ (see the proposition above). For all $\mathbf{y} \in \mathfrak{m}^{\times n}$, it holds that*

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{h}(\mathbf{y})) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{y}).$$

*Proof.* For each formal power series $f \in A[[X_1, \ldots, X_n]]$, one can always write

$$f(\mathbf{X} + \mathbf{Y}) = f(\mathbf{X}) + M_f(\mathbf{X})\mathbf{Y} + \sum_{1 \leq j \leq k \leq n} G_{jk}(\mathbf{X}, \mathbf{Y}) Y_j Y_k,$$

for certain $G_{jk} \in A[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]]$.

In particular, let us take $f = f_i$ (for $i = 1, \ldots, n$), $\mathbf{X} = \mathbf{a}$, $\mathbf{Y} = e \cdot \mathbf{x}$.

$$f_i(\mathbf{a}+e\cdot\mathbf{x}) = f_i(\mathbf{a})+M_{f_i}(\mathbf{a})\cdot(e\cdot\mathbf{x})+\sum_{1\le j\le k\le n} G_{jk}(\mathbf{a}, e\cdot\mathbf{x})(e\cdot x_j)(e\cdot x_k)$$
$$= f_i(\mathbf{a}) + M_{f_i}(\mathbf{a}) \cdot (e \cdot \mathbf{x}) + e^2 \cdot r_i(\mathbf{x}),$$

where $r_i$ is a formal power series whose terms have all degree at least two.

If we gather these equations for all $i$, we can write simply

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{x}) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{x}) + e^2 \cdot \mathbf{r}(\mathbf{x}).$$

Let $M'$ be the adjoint matrix of $M_{\mathbf{f}}(\mathbf{a})$. By definition, it satisfies that

$$M_{\mathbf{f}}(\mathbf{a})M' = e \cdot I_n.$$

If we insert this equation in the formula above, then we obtain

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{x}) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{x}) + M_{\mathbf{f}}(\mathbf{a})M' \cdot (e \cdot \mathbf{r}(\mathbf{x})).$$

Let us define $\mathbf{g} = \mathbf{1}_n + M'\mathbf{r}$. Since the terms of $\mathbf{r}$ have at least order 2, the second term does not alter the value of $M_{\mathbf{g}}(0)$, thus $M_{\mathbf{g}}(0) = M_{\mathbf{1}_n}(0) = I_n$. Moreover, we can write

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{x}) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{x}) + M_{\mathbf{f}}(\mathbf{a})M' \cdot (e \cdot \mathbf{r}(\mathbf{x})) =$$
$$\mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot e(\mathbf{x} + M'\mathbf{r}(\mathbf{x})) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot e(\mathbf{g}(\mathbf{x})).$$

This proves (i) and (ii). (iii) can be obtained by replacing $\mathbf{x}$ by $\mathbf{h}(\mathbf{y})$, where $\mathbf{h} = (h_1, \ldots, h_n)$ is given by Proposition 10.2.

□

We will say that two $n$-tuples $\mathbf{a}$ and $\mathbf{b}$ are congruent modulo an ideal $I$ of $A$ if they are so coordinatewise, that is to say, $a_i - b_i \in I$ for $i = 1, \ldots, n$. As a consequence of the theorem above, we have the following result:

**Corollary 10.4.** *Let $\mathbf{f} = (f_1, \ldots, f_n)$ be a system of elements in $A[[X_1, \ldots, X_n]]$, and let $\mathbf{a} \in \mathfrak{m}^{\times n}$. Call $e = J_{\mathbf{f}}(\mathbf{a})$. If $\mathbf{f}(\mathbf{a}) \equiv 0 \mod e^2\mathfrak{m}$, then there exists $\mathbf{b} \in \mathfrak{m}^{\times n}$ such that $\mathbf{f}(\mathbf{b}) = 0$ and $\mathbf{b} \equiv \mathbf{a} \mod e\mathfrak{m}$. Furthermore, assume that there exists another tuple $\mathbf{b}' \in \mathfrak{m}^{\times n}$ such that $\mathbf{f}(\mathbf{b}') = 0$ and $\mathbf{b}' \equiv \mathbf{a} \mod e\mathfrak{m}$. Then, if $A$ has no zero divisors, $\mathbf{b} = \mathbf{b}'$.*

*Proof.* If $e = 0$ the statement is obviously true, so we will assume that $e \neq 0$. Let us write $\mathbf{f}(\mathbf{a}) = e^2\mathbf{c}$, where $\mathbf{c} = (c_1, \ldots, c_n)$ is an $n$-tuple satisfying that $c_i \in \mathfrak{m}$, for all $i = 1, \ldots, n$. According to Theorem 10.3-(iii), we may claim that for all $\mathbf{y} \in \mathfrak{m}^{\times n}$,

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{h}(\mathbf{y})) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{y}) = e^2\mathbf{c} + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{y}),$$

where $\mathbf{h}$ is the $n$-tuple which pops up in Theorem 10.3.

Let us denote by $M'$ the adjoint matrix of $M_{\mathbf{f}}(\mathbf{a})$, so that $M_{\mathbf{f}}(\mathbf{a}) \cdot M' = eI_n$. For all $\mathbf{z} \in \mathfrak{m}^{\times n}$, we know that $M' \cdot \mathbf{z} \in \mathfrak{m}^{\times n}$. Picking $\mathbf{y} = M'\mathbf{z}$, the equality above yields

$$\mathbf{f}(\mathbf{a} + e \cdot \mathbf{h}(M'\mathbf{z})) = e^2\mathbf{c} + M_{\mathbf{f}}(\mathbf{a}) \cdot eM'\mathbf{z} = e^2 \cdot \mathbf{c} + e^2 \cdot \mathbf{z} = e^2 \cdot (\mathbf{c} + \mathbf{z}).$$

Choosing $\mathbf{z} = -\mathbf{c}$, we conclude that $\mathbf{b} = \mathbf{a} + e \cdot \mathbf{h}(M'(-\mathbf{c}))$ satisfies the conditions that were required.

With regard to uniqueness, assume that we have two $n$-tuples $\mathbf{b} = \mathbf{a} + e \cdot \mathbf{x}$, $\mathbf{b}' = \mathbf{a} + e \cdot \mathbf{x}'$ with $\mathbf{x}, \mathbf{x}' \in \mathfrak{m}^{\times n}$ and satisfying $\mathbf{f}(\mathbf{b}) = \mathbf{f}(\mathbf{b}') = 0$. Theorem 10.3-(ii) allows us to claim that

$$\mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{g}(\mathbf{x})) = \mathbf{f}(\mathbf{a}) + M_{\mathbf{f}}(\mathbf{a}) \cdot (e \cdot \mathbf{g}(\mathbf{x}')),$$

that is to say,

$$M_{\mathbf{f}}(\mathbf{a}) \cdot e \cdot (\mathbf{g}(\mathbf{x}) - \mathbf{g}(\mathbf{x}')) = 0.$$

Multiplying now on the left by $M'$, we obtain that

$$e^2 \cdot (\mathbf{g}(\mathbf{x}) - \mathbf{g}(\mathbf{x}')) = 0.$$

Since by assumption $A$ has no zero divisors, we may look at this equality coordinatewise and conclude that

$$\mathbf{g}(\mathbf{x}) - \mathbf{g}(\mathbf{x}') = 0.$$

But we know that the system of power series $\mathbf{g} = (g_1, \ldots, g_n)$ satisfies the hypotheses of Proposition 10.2. Therefore, the map

$$\mathbf{y} \mapsto \mathbf{g}(\mathbf{y})$$

is a bijection from $\mathfrak{m}^{\times n}$ to $\mathfrak{m}^{\times n}$. Thus if $\mathbf{g}(\mathbf{x}) = \mathbf{g}(\mathbf{x}')$, then it follows that $\mathbf{x} = \mathbf{x}'$.

□

Let us go back now to our approximation problem. We have two formal group laws $\mathbf{F}$, $\mathbf{F}'$, defined over $\mathbb{Z}_\ell$. Let us keep the notation we introduced at the beginning of this chapter. We consider the two systems of equations

$$\begin{cases} [\ell]_1(Z_1, Z_2) = 0 \\ [\ell]_2(Z_1, Z_2) = 0 \end{cases} \quad \text{and} \quad \begin{cases} [\ell]'_1(Z_1, Z_2) = 0 \\ [\ell]'_2(Z_1, Z_2) = 0 \end{cases} \tag{10.1}$$

where we know that for $i = 1, 2$, it holds that

$$[\ell]_i(Z_1, Z_2) - [\ell]'_i(Z_1, Z_2) \in \ell^r \cdot \mathbb{Z}_\ell[[Z_1, Z_2]].$$

Furthermore, since the systems of equations (10.1) describe the $\ell$-torsion points of the Jacobians of curves of genus 2, the set of solutions in $\overline{\mathfrak{m}}^{\times 2}$ is finite. We may thus consider a finite extension $K \supset \mathbb{Q}_\ell$ that contains all the coordinates of all the solutions of the systems in (10.1). Let us denote by $\mathcal{O}_K$ the ring of integers of $K$ and by $\mathfrak{m}$ its maximal ideal. It is clear that $\mathcal{O}_K$ is separable and complete with respect to the $\mathfrak{m}$-adic topology, and therefore all the previous reasonings are valid in this context.

Let us call $V'$ the set of pairs of $(x', y') \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ such that $[\ell]'_1(x', y') = [\ell]'_2(x', y') = 0$. Our first claim is the following:

**Lemma 10.5.** *For all $(x', y') \in V'$, $[\ell]_1(x', y'), [\ell]_2(x', y') \in \ell^r \mathfrak{m}$.*

*Proof.* Since $[\ell]'_1(x', y') = 0$, we can write

$$[\ell]_1(x', y') = [\ell]_1(x', y') - [\ell]'_1(x', y').$$

Furthermore, let us express $[\ell]_1(x, y) = \sum_{ij} a_{ij} x^i y^j$, $[\ell]'_1(x, y) = \sum_{ij} a'_{ij} x^i y^j$. Hence

$$[\ell]_1(x', y') = \sum_{ij} (a_{ij} - a'_{ij}) x'^i y'^j.$$

We know that $a_{ij} - a'_{ij} \in (\ell^r)$, and $x', y' \in \mathfrak{m}$, and also that $[\ell]_1(x, y)$ is a power series without constant term; thus it follows that $[\ell]_1(x', y') \in \ell^r \mathfrak{m}$. A similar reasoning shows that $[\ell]_2(x', y') \in \ell^r \mathfrak{m}$. □

In order to apply the corollary above to the system of equations $[\ell]_1(Z_1, Z_2) = [\ell]_2(Z_1, Z_2) = 0$, we need to compute the determinant of the Jacobian matrix attached to the system. But this is a simple

task (see Example 5.2); the Jacobian matrix $M_{([\ell]_1,[\ell]_2)}(x,y)$ is given by

$$\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix},$$

thus $e = \ell^2$.

This result suggests that we choose $r = 4$.

*Proof of Theorem 10.1.* Take $(x', y') \in \overline{\mathfrak{m}}^{\times 2}$ satisfying

$$[\ell]_1'(x', y') = [\ell]_2'(x', y') = 0.$$

We know that $[\ell]_1(x', y'), [\ell]_2(x', y') \in \ell^4 \cdot \mathfrak{m}$. Hence there exists a unique $(x, y) \in \overline{\mathfrak{m}}^{\times 2}$ such that $[\ell]_1(x, y) = [\ell]_2(x, y) = 0$ and furthermore

$$\begin{cases} x' \equiv x \mod \ell^2\mathfrak{m} \\ y' \equiv y \mod \ell^2\mathfrak{m}. \end{cases}$$

In particular, the two conditions $v(x' - x) \geq 2$, $v(y' - y) \geq 2$ are satisfied.

But $(x, y)$ is a point of $\ell$-torsion of the Jacobian of $C$, and therefore we know that

$$\min\{v(x), v(y)\} = \alpha.$$

But if $v(x) = \alpha$ and $v(x' - x) \geq 2 > \alpha$, then it follows that $v(x') = \alpha$. And similarly, if $v(y) = \alpha$, then $v(y') = \alpha$. Also if $v(x) > \alpha$, it cannot happen that $v(x') < \alpha$ (and the same applies to $y, y'$). We may conclude that

$$\min\{v(x'), v(y')\} = \alpha,$$

as we wished to prove. □

As a consequence of Theorem 10.1, we can formulate a slightly more general result than Theorem 9.2.

**Theorem 10.6.** *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 $\ell > 2$ 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 $\ell$, $C$ has stable reduction at $p$.*
- *The following congruences hold:*

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

- *The reduction of $f(x)$ modulo $\ell$ is of the form $x^6 + bx^4 + bx^2 + 1$, and the elliptic curve $E$ defined by $y^2 = x^3 + bx^2 + bx + 1$ is supersingular.*

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

# Chapter 11

# Image of the representation

In the previous chapters, we devoted ourselves to the tameness condition: we studied in detail some ways to guarantee that the Galois representation $\rho_\ell$ attached to the $\ell$-torsion points of certain abelian varieties is tamely ramified. But recall that our intention was to realize groups of the family $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ as Galois groups over $\mathbb{Q}$, with tame ramification. Therefore, some control of the image of the representation must be obtained.

Let us fix a prime $\ell$, let $A/\mathbb{Q}$ be an abelian variety of dimension $n$, and let us denote by $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2n}(\mathbb{F}_\ell)$ the Galois representation attached to the $\ell$-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 $\ell$-torsion points of $A$,

$$\langle \cdot, \cdot \rangle : A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*.$$

Furthermore, the elements of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ behave well with respect to this pairing. Namely, if we denote the cyclotomic character by $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*$, then for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for all $P_1, P_2 \in A[\ell]$,

$$\langle \sigma(P_1), \sigma(P_2) \rangle = \chi_\ell(\sigma) \cdot \langle P_1, P_2 \rangle. \tag{11.1}$$

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 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 is the whole general symplectic group (see Theorem 3 of *Lettre a Marie-France Vignéras* in [82]).

We are particulary interested in the case of abelian surfaces over $\mathbb{Q}$, since there are some explicit results in this context. In this case, the result of Serre boils down to:

**Theorem 11.1.** *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 $\ell$, it holds that*

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

There are two ways of thinking about the problem of determining whether in a specific example the image of the representation is as large as possible, that is to say, as large as the obvious restrictions (in this case, the behaviour of the image with respect to the Weil pairing) allow. Assume we have an abelian variety $A$ and we know that the image of the representation attached to it is, at most, equal to a certain group $G$. One way to proceed is to determine a small set of generators of $G$, and make sure that some element of the Galois group maps into each one of them. This method was first used by Shimura (see [83]).

A beautiful example of this procedure can be found in [77], § 5.2 (cf. [83]). Serre considers the elliptic curve $y^2+y = x^3-x$. It is known that the image of the Galois representation $\varphi_\ell$ attached to the $\ell$-torsion points of an elliptic curve is contained in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Now Proposition 19, § 2.8 in [77] claims that a subgroup $G$ of $\mathrm{GL}_2(\mathbb{F}_\ell)$ which contains three elements satisfying certain conditions generate $\mathrm{SL}_2(\mathbb{F}_\ell)$. Namely, if $\ell \geq 5$ and $G$ contains $s, s'$ and $s''$ satisfying:

- $\mathrm{Tr}(s)^2 - 4\det(s)$ is a non-zero square in $\mathbb{F}_\ell$ with $\mathrm{Tr}(s) \neq 0$,
- $\mathrm{Tr}(s')^2 - 4\det(s')$ is not a square in $\mathbb{F}_\ell$ and $\mathrm{Tr}(s') \neq 0$,
- The element $u = \mathrm{Tr}(s'')^2/\det(s'')$ is different from $0, 1, 2$ and $4$ and furthermore $u^2 - 3u + 1 \neq 0$,

then $G \supset \mathrm{SL}_2(\mathbb{F}_\ell)$, where Tr denotes the trace and det the determinant in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Moreover, if $G$ is the image of $\varphi_\ell$, then $G \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ implies that $G = \mathrm{GL}_2(\mathbb{F}_\ell)$, since it is known that $\det \circ \varphi_\ell = \chi_\ell$ is a surjective map.

Denote by $\mathrm{Frob}_2$ (resp. $\mathrm{Frob}_3$) a lift of the Frobenius element at 2 (resp. at 3) to the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (any lift will do; see the next section for further explanation of the choice of lifts of Frobenius

elements). Assume that $\ell \geq 13$ and furthermore $(11/\ell) = -1$. Then either the choice $s = \varphi_\ell(\mathrm{Frob}_2)$, $s' = \varphi_\ell(\mathrm{Frob}_3)$, $s'' = \varphi_\ell(\mathrm{Frob}_3)$ or $s = \varphi_\ell(\mathrm{Frob}_3)$, $s' = \varphi_\ell(\mathrm{Frob}_2)$, $s'' = \varphi_\ell(\mathrm{Frob}_3)$ (according to whether $(-1/\ell) = 1$ or not) will satisfy the conditions of the proposition, and lead to the conclusion that $\mathrm{Im}\varphi_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$.

The other way is to compute all the subgroups of $G$, and check that for each subgroup there is an element in the image of the representation which does not map inside it. Along these lines, for instance, one could look at the proof of Proposition 21, § 5.4 of [77]. As a consequence of this proposition, Serre shows that, save for $\ell = 5$ or $\ell = 11$, the image of the Galois representation $\varphi_\ell$ attached to the $\ell$-torsion points of the elliptic curve $y^2 + y = x^3 - x^2$ is the whole group $\mathrm{GL}_2(\mathbb{F}_\ell)$.

We will place ourselves in the situation where our abelian variety is the Jacobian of a genus 2 curve, hence an abelian surface. In this setting, a study of the image of the corresponding representations in the way we described first is carried out by P. Le Duff (see [44]). The other way is pursued by L. Dieulefait in [24]. In that paper, he manages to determine, given a fixed, principally polarized abelian surface $A/\mathbb{Q}$, a finite set of primes $\ell$ outside which the image of $\rho_\ell$ equals $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

In this chapter, we will take the results of Le Duff [44] 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.

When we first took thought on these matters, guided by the results of Le Duff, we obtained a result which was quite satisfactory, but unfortunately it depended on an unproven conjecture, due to Hardy and Littlewood (more precisely, Conjecture (F) of [33]). Given a prime number $\ell > 3$, we needed an auxiliary prime $q$ such that, among other conditions, satisfies that $4q - 3$ is a square. For concrete values of $\ell$, one could find this prime $q$, but to prove that it exists for all $\ell$ requires the use of the conjecture. Later, following a suggestion of L. Dieulefait, we managed to remodel our reasoning in order to obtain an unconditional result.

As we noted above, 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 [44]):

**Proposition 11.2.** *The symplectic group* $\mathrm{Sp}_4(\mathbb{F}_\ell)$ *is generated by a transvection and an element whose characteristic polynomial is irreducible.*

**Remark 11.3.** Recall that a transvection in $\mathrm{GL}_n(k)$ for any field $k$ is an element $\tau$ that fixes a hyperplane and such that $\mathrm{Im}(\mathrm{Id} - \tau)$ has dimension 1. (See Definition 4.1 of Chapter IV of [2]).

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 $\mathrm{GSp}_4(\mathbb{F}_\ell)$. This is because we have the following exact sequence

$$1 \longrightarrow \mathrm{Sp}_4(\mathbb{F}_\ell) \longrightarrow \mathrm{GSp}_4(\mathbb{F}_\ell) \xrightarrow{\pi} (\mathbb{Z}/\ell\mathbb{Z})^* \longrightarrow 1$$

and because the composition $\pi \circ \rho_\ell = \chi_\ell$ (due to Equation (11.1)) and is thus 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.

Firstly, let us concern ourselves with the transvection. The contents of Proposition 1.3 of [44] are the following:

**Proposition 11.4.** *Let $A$ be an abelian variety defined over a number field $K$ and $v$ a valuation of $K$. Assume that the reduction $\widetilde{A}_v$ of $A$ at $v$ is an extension of an abelian variety of dimension* $\dim(A) - 1$ *by a torus of dimension* 1.

*If $\ell$ is a prime number different from the residual characteristic of $v$, and such that it does not divide $(\widetilde{A}_v : \widetilde{A}_v^0)$ (which denotes the order of the group of connected components of the special fibre of the Néron model at $v$), then there exists an element in the inertia group $I_v$ such that its image by $\rho_\ell$ is a transvection.*

We are particularly interested in the case when the abelian variety $A$ is the Jacobian of a genus 2 curve $C$. In this case, the kind of reduction of $A$ at $p$, (that is, the classification of the connected component of the special fibre of the Néron model at a prime $p$) can be determined through the knowledge of the kind of reduction of a minimal regular proper model of C (the kind of reduction of such a model is classified in [57]).

For instance, it is well known 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 [48], Remark 4.26 of chapter 10).

Now if a genus 2 curve has stable reduction at a prime $p$, then this reduction must belong to one of the following seven types (labeled (I) to (VII)):

$$I_{0-0-0},\ I_{n-0-0},\ I_{n-p-0},\ I_{n-p-q},\ I_0-I_0-m,\ I_n-I_0-m,\ I_n-I_p-m$$

for some integers $n, m, q$.

In particular, Lemma 4.1 of [44] restates the condition in Proposition 11.4 in terms of the stable reduction of the curve $C$.

**Lemma 11.5.** *Let $C/\mathbb{Q}$ be a genus 2 curve and $J$ its Jacobian. Assume $C$ has stable reduction of type (II) or (VI) at $p$. Then the connected component of the special fibre at $p$ of the Néron model of $J$ which contains the neutral element is an extension of an elliptic curve by a torus.*

The kind of reduction of a genus 2 curve $C$ can be computed by means of the Igusa invariants attached to it. Therefore, the combination of the previous lemma and Proposition 11.4 provides us with an explicit way to guarantee that a transvection lies in $\mathrm{Im}\rho_\ell$.

Let us now try to approach the existence of an element with irreducible characteristic polynomial. The candidate elements we are going to look at are the images of the Frobenius elements at primes different from $\ell$, where $C$ has good reduction, since we have a great deal of information about their shape (as in the example of Serre we dwelt on at the beginning of the chapter).

Namely, let $q \neq \ell$ be a prime number, and assume that $J(C)$ has good reduction at $q$. Inside $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 reduction of the abelian variety $J(C)$ is also good at $q$, hence the image by $\rho_\ell$ of the inertia group at $q$ is trivial. Therefore, the image by $\rho_\ell$ 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 $\phi_q$ acting on the reduction $\widetilde{C}$ of $C$ at $q$. It is well known (see for instance [17], § 14.1.6, Theorem 14.16) that the characteristic polynomial of $\phi_q$ 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

$$\begin{cases} a := N_1 - q - 1 \\ b := (N_2 - q^2 - 1 + a^2)/2. \end{cases} \tag{11.2}$$

Furthermore, it can be proven (cf. Proposition 10.20 in [55]) that the polynomial obtained from $P(X)$ by reducing its coefficients modulo $\ell$ coincides with the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_q)$. This element need not be in $\mathrm{Sp}_4(\mathbb{F}_\ell)$, but luckily, any element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, raised to the $(\ell-1)$-th power does, and Lemma 3.3 in [44] shows that it suffices to prove that $P(X)$ is irreducible.

Up to this point, we have been following the steps of [44]. This is the way we approached the matter at first, trying to produce an element with irreducible characteristic polynomial. Choosing a prime $q$ in a suitable way and asking an equation of $C$ to satisfy certain congruences modulo $q$, we managed to ensure the existence of this element, but we needed to make use of a conjecture of Hardy and Littlewood (namely Conjecture (F) of [33]). But after consulting L. Dieulefait we have managed to devise a way to ensure a large image without resorting to this conjecture. We will now describe this new approach.

Since we have seen that asking the image of the Galois representation to contain a transvection is feasible, we will take advantage of this fact. The following result is Theorem 2.2 of [44]).

**Theorem 11.6.** *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 11.7.** 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 [44]). Therefore Proposition 11.2 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 11.8.** The second assertion in the previous 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 [44]). 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 [40]). 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 $P(1/\alpha) = 0$). Therefore, if $P(X)$ is not irreducible over $\mathbb{F}_\ell$, it will decompose in quadratic or linear factors since, if a root belongs to $\mathbb{F}_\ell$, then there is another root in $\mathbb{F}_\ell$.

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 labeled *"unrelated" 2-dimensional constituents* and the second one *"related" 2-dimensional constituents* in [24].

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 11.9.** *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 11.6 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 11.8). 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 $\alpha$ and $\beta$. Then the roots of the other factor are $1/\alpha$ and $1/\beta$.

Let us consider the polynomial $P_2(X) = (x-\alpha_2)(x-\beta_2)(x-1/\alpha_2)(x-1/\beta_2)$. Labeling the roots anew if necessary, we can assume that $\alpha_2$ and $\beta_2$ 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 11.8). 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 11.8), 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. □

**Remark 11.10.** Let us turn back to our Galois representation $\rho_\ell$ attached to the Jacobian of a genus 2 curve $C$. Let $q$ be a prime of good reduction of $C$. We already noted that the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_q)$, the image of the Frobenius element at $q$ has the shape $P(X) = X^4 + aX^3 + bX^2 + aqX + q^2$. If $q \equiv 1 \pmod{\ell}$, then $\rho_\ell(\mathrm{Frob}_q)$ belongs to $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and therefore it will suit our purposes.

This result, together with Proposition 11.4, fulfils our purpose. The following statement will be referred to many times.

**Theorem 11.11.** *Let $C$ be a genus 2 curve defined over $\mathbb{Q}$ with stable reduction of type $(II)$ or $(VI)$ at a prime number $p$. Let $c$ be the order of the group of connected components of the special fibre of the Néron model at $p$. Let $q_1$ and $q_2$ be different prime numbers at which $C$ has good reduction.*

*Call $P_i(X) = X^4 + a_i X^3 + b_i X^2 + a_i q_i X + {q_i}^2$ the characteristic polynomial of the Frobenius endomorphism acting on the reduction of $C$ at $q_i$, and define $\Delta_0(P_i) = a_i^2 - 4b_i + 8q_i$, $i = 1, 2$.*

*If $\ell > 2$ is a prime number which does not divide $2pq_1q_2c$ satisfying*

- $q_i \equiv 1 \pmod{\ell}, i = 1, 2.$
- *$\Delta_0(P_1)$ is not a square in $\mathbb{F}_\ell$ and $a_1 \not\equiv 0 \pmod{\ell}$.*
- *$\Delta_0(P_2)$ is a non-zero square in $\mathbb{F}_\ell$, and $P_2(X)$ does not decompose in linear factors in $\mathbb{F}_\ell$.*

*then the image of $\rho_\ell$ coincides with $\mathrm{GSp}_4(\mathbb{F}_\ell)$.*

# Chapter 12

# Explicit construction

In this chapter we will (at last!) face the problem of constructing, for a given prime number $\ell$, 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 chapters we have worked out some statements that give very accurate and explicit conditions for the Galois representation attached to the Jacobian surface of a genus 2 curve to satisfy the desired properties. To be more precise, 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 $A$ the Jacobian variety attached to $C$ and by $\rho_\ell$ the Galois representation attached to the $\ell$-torsion points of $A$, the following conditions are satisfied:
>
> - The Galois extension obtained by adjoining to $\mathbb{Q}$ the coordinates of the $\ell$-torsion points of $A$ is tamely ramified.
> - The image of $\rho_\ell$ coincides with the general symplectic group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.
>
> Then $\rho_\ell$ provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Now the first condition was settled in Theorem 9.2, and was polished afterwards in Theorem 10.6. The second condition was dealt

with in Theorem 11.11. If we collect all these results, we obtain the following theorem (of a rather clumsy length):

**Theorem 12.1.** *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 $\ell > 2$ 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 $\ell$, $C$ has stable reduction at $p$.*
- *The following congruences hold:*

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

- *The reduction of $f(x)$ modulo $\ell$ is of the form $x^6 + bx^4 + bx^2 + 1$, and the elliptic curve $E$ defined by $y^2 = x^3 + bx^2 + bx + 1$ is supersingular.*
- *There exists a prime number $p \neq \ell$ such that the reduction of $C$ at $p$ is stable of type (II) or (VI), and $\ell$ does not divide the order of the group of connected components of the special fibre of the Néron model at $p$.*
- *There exist two prime numbers $q_1, q_2$ with $q_i \equiv 1 \pmod{\ell}$ and such that $C$ has good reduction at $q_i$, $i = 1, 2$. Let $P_i(X) = X^4 + a_iX^3 + b_iX^2 + a_iq_iX + {q_i}^2$ be the characteristic polynomial of the Frobenius endomorphism acting on the reduction of $C$ at $q_i$, and define $\Delta_0(P_i) = a_i^2 - 4b_i + 8q_i$, $i = 1, 2$. Assume that*
  - *$\Delta_0(P_1)$ is not a square in $\mathbb{F}_\ell$ and $a_1 \not\equiv 0 \pmod{\ell}$.*
  - *$\Delta_0(P_2)$ is a non-zero square in $\mathbb{F}_\ell$, and $P_2(X)$ does not decompose in linear factors in $\mathbb{F}_\ell$.*

*Then the Galois extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$ provides a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.*

A quick glance at this theorem does not make it clear that for each prime number $\ell > 2$ such a genus 2 curve $C$ exists. On the contrary, there are a number of conditions that have to hold, and it is not clear whether they can all be simultaneously satisfied, or indeed whether they can be satisfied at all. Furthermore, some of the conditions involve the existence of primes, and it is not clear how to look for them.

Our aim in this chapter is to replace all these conditions with others, more restrictive, but which are simply congruences like the second condition of the Theorem above. In this way, it will be crystal clear (due to the Chinese Remainder Theorem) that such a curve exists. We shall tackle each of the conditions separately; thus the chapter will be split in several different sections. At the end, we shall state a theorem which will be a particular case of the Theorem above, but which will have a very explicit flavour.

In the course of this chapter, we will have to exclude the prime $\ell = 3$, since it will not be possible to find a supersingular symmetric elliptic curve over $\mathbb{F}_3$. This is a fundamental restriction, and in order to handle the case $\ell = 3$, another approach is required.

## 12.1 Good reduction at any given prime

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 $2g + 2$.

One can define the *discriminant* of this equation 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 [47], § 2).

The hyperelliptic equation defining $C$ is unique up to the following changes of variables

$$\begin{cases} x \mapsto \frac{ax+b}{cx+d} \\ y \mapsto \frac{ey+H(x)}{(cx+d)^3} \end{cases}$$

where $a, b, c, d, e \in k$ are such that $ad - bc \neq 0$, $e \neq 0$ and $H(x) \in k[x]$ has degree $\leq 3$ (see [47], § 2).

To ensure that a curve $C$, given by a hyperelliptic equation with integer coefficients, has good reduction at a prime $p$, we will use the discriminant. Namely, let us 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

$$y^2 = f(x), \tag{12.1}$$

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 (12.1), 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 12.2.** *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:*

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

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

*Proof.* Let us consider the following hyperelliptic equation:

$$y^2 = x^6 + x^4 + x^2 + 1.$$

Its discriminant is

$$\Delta = \left(\frac{1}{2}\right)^{12} \cdot \operatorname{disc}(4 \cdot (x^6 + x^4 + x^2 + 1)) = -4194304 \equiv 2 \pmod 3.$$

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 $\Delta$ modulo 3, thus it is not divisible by 3. □

In order to prove the following proposition, we will make use of a Lemma that will occur in Section 12.3, concerning the relationship between the exponent of the conductor of an abelian variety at a prime $p$ and the kind of reduction of the variety at $p$. These notions will be explained at the beginning of Section 12.3.

**Proposition 12.3.** *Let $C$ be a genus 2 curve given by the hyperelliptic equation*

$$y^2 = f(x), \tag{12.2}$$

*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:*

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

*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 (12.2), we obtain

$$y+x^3y+y^2 = \frac{f_6-1}{4}x^6+\frac{f_5}{4}x^5+\frac{f_4}{4}x^4+\frac{f_3-2}{4}x^3+\frac{f_2}{4}x^2+\frac{f_1}{4}x+\frac{f_0-1}{4}.$$

Let us define $b_0 = \frac{f_0-1}{4}$, $b_1 = \frac{f_1}{4}$, $b_2 = \frac{f_2}{4}$, $b_3 = \frac{f_3-2}{4}$, $b_4 = \frac{f_4}{4}$, $b_5 = \frac{f_5}{4}$, $b_6 = \frac{f_6-1}{4}$. Since $f_0 \equiv 1$ modulo 16, it follows that $b_0$ belongs to $\mathbb{Z}$. Likewise, the other congruences that are satisfied by hypothesis guarantee that $b_1$, $b_2$, $b_3$, $b_4$, $b_5$ and $b_6$ are integers. Moreover,

$$\begin{cases} b_0 \equiv b_6 \equiv 0 \pmod{4} \\ b_1 \equiv b_5 \equiv 0 \pmod{4} \\ b_2 \equiv b_4 \equiv 1 \pmod{4} \\ b_3 \equiv 0 \pmod{4}. \end{cases}$$

Therefore, we can compute the discriminant of the following equation modulo 4,

$$y + x^3y + y^2 = b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

We obtain that $\Delta = 2$: that is to say, it is divisible by 2, and once only. But the 2-adic valuation of the discriminant is always greater than or equal to the exponent at 2 of the conductor of the Jacobian surface attached to $C$ (see [46]). Therefore, Lemma 12.10 below ensures that the Jacobian surface attached to $C$ has either good reduction or bad semistable reduction at 2. □

**Remark 12.4.** We could have picked a curve such that the discriminant of some integer model is odd (say, for instance, the curve defined by the hyperelliptic equation $y^2 = x^6 + 2x^4 - 2x^3 - 3x^2 + 2x + 1$. After a suitable change of variables, it can be turned into the equation $y^2 + (x^3 + x + 1) \cdot y = -x^3 - x^2$, which has odd discriminant. cf. [86]). In this way, we would obtain a congruence condition which ensures that the initial curve $C$ has good reduction at 2. Nevertheless, we picked the curve in the proposition above for aesthetic reasons: we are trying to construct $C$ as symmetrical as possible.

## 12.2 Supersingular abelian surfaces

Our aim in this section is to construct, for a given (odd) prime number $\ell$, a genus 2 curve, defined over $\mathbb{Q}$, such that its Jacobian surface has good supersingular reduction at $\ell$. Moreover, we would ask that it is defined by an equation of the form $y^2 = f(x)$, 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 separable polynomial of degree 6 (In Chapter 8 it became clear that this is a highly convenient condition for our purposes). We shall say that a genus 2 curve defined over $\mathbb{F}_\ell$ is supersingular if its Jacobian is a supersingular abelian surface.

Assume that we have a genus 2 curve $C$ defined by an equation as above, satisfying that neither the leading coefficient nor the discriminant of $f(x)$ are divisible by $\ell$. Then the reduction of $C$ at $\ell$ is defined by the equation $y^2 = \overline{f}(x)$, where $\overline{f}(x) \in \mathbb{F}_\ell[x]$ is the polynomial of degree 6 obtained from $f(x)$ by reducing its coefficients modulo $\ell$. Therefore, what we shall construct is a supersingular genus 2 curve, defined over $\mathbb{F}_\ell$ by an equation $y^2 = \overline{f}(x)$, where

$\overline{f}(x) = \overline{f}_0 x^6 + \overline{f}_1 x^5 + \overline{f}_2 x^4 + \overline{f}_3 x^3 + \overline{f}_2 x^2 + \overline{f}_1 x + \overline{f}_0 \in \mathbb{F}_\ell[x]$ is a polynomial of degree 6 with non-zero discriminant. Lifting this equation to $\mathbb{Q}$ in a suitable way we will obtain the curve we were seeking.

There is a simple criterion which characterizes when a genus 2 curve is supersingular, in terms of the coefficients appearing on an equation defining the curve.

**Lemma 12.5.** *Let $C$ be a smooth projective genus 2 curve defined over a field $k$ of characteristic $\ell > 2$ by a hyperelliptic equation*

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

*where $f(x) \in k[x]$ is a separable polynomial of degree 5 or 6. Let us write*

$$f(x)^{\frac{\ell-1}{2}} = \sum_{j \geq 0} c_j x^j,$$

*and consider the matrices*

$$M = \begin{pmatrix} c_{\ell-1} & c_{\ell-2} \\ c_{2\ell-1} & c_{2\ell-2} \end{pmatrix}, \quad M^{(\ell)} = \begin{pmatrix} c_{\ell-1}^{\ell} & c_{\ell-2}^{\ell} \\ c_{2\ell-1}^{\ell} & c_{2\ell-2}^{\ell} \end{pmatrix}.$$

*Then $C$ is supersingular if and only if $M^{(\ell)} \cdot M = 0$.*

*Proof.* See [38], Lemma 1.1. □

We are concerned with equations $y^2 = f(x)$ where $f(x)$ is symmetric of degree 6. But in this case, $f(x)^{\frac{\ell-1}{2}}$ is also symmetric. That is to say, if we call $f(x)^{\frac{\ell-1}{2}} = \sum_{j=0}^{3(\ell-1)} c_j x^j$, then $c_0 = c_{3\ell-3}, c_1 = c_{3\ell-4}, \ldots, c_{\ell-2} = c_{2\ell-1}, c_{\ell-1} = c_{2\ell-2}$. Therefore, the supersingularity condition boils down to

$$\begin{pmatrix} c_{\ell-1}^{\ell} & c_{\ell-2}^{\ell} \\ c_{\ell-2}^{\ell} & c_{\ell-1}^{\ell} \end{pmatrix} \cdot \begin{pmatrix} c_{\ell-1} & c_{\ell-2} \\ c_{\ell-2} & c_{\ell-1} \end{pmatrix} = 0.$$

The four equations obtained by carrying out the products on the left turn out to be equal pairwise, and therefore we obtain just two conditions, namely

$$\begin{cases} c_{\ell-1}^{\ell+1} + c_{\ell-2}^{\ell+1} = 0 \\ c_{\ell-1} c_{\ell-2} (c_{\ell-1}^{\ell-1} + c_{\ell-2}^{\ell-1}) = 0. \end{cases}$$

Moreover, if we assume $f(x) \in \mathbb{F}_\ell$, then $c_{\ell-1}, c_{\ell-2} \in \mathbb{F}_\ell$ and thus $c_{\ell-1}^\ell = c_{\ell-1}$, $c_{\ell-2}^\ell = c_{\ell-2}$. Therefore the two conditions above reduce to

$$\begin{cases} c_{\ell-1}^2 + c_{\ell-2}^2 = 0 \\ 2c_{\ell-1}c_{\ell-2} = 0. \end{cases}$$

This shows that $c_{\ell-1} = c_{\ell-2} = 0$ must be satisfied. We can thus state the following proposition.

**Proposition 12.6.** *Let $\ell > 2$ be a prime number and let $C$ be a genus 2 curve defined over $\mathbb{F}_\ell$ by an equation of the form $y^2 = f(x)$, where $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_\ell[x]$ is a separable polynomial of degree 6 with non-zero discriminant. Let us write*

$$f(x)^{\frac{\ell-1}{2}} = \sum_{j=0}^{3(\ell-1)} c_j x^j.$$

*Then $C$ is supersingular if and only if $c_{\ell-1} = c_{\ell-2} = 0$.*

**Remark 12.7.** This result allows us to solve our problem for a family of odd primes $\ell$. Namely, let us consider the curve $C$ defined by the equation $y^2 = x^6 + 1$ over $\mathbb{F}_\ell$. The discriminant of this equation is $\Delta = -2^{14} \cdot 3^6$. Therefore, if $\ell \neq 2, 3$, $C$ is a smooth genus 2 curve.

Define now the polynomial $g(x) = (x^6 + 1)^{\frac{\ell-1}{2}}$. If we compute $g(x)$ by means of the binomial theorem, it is obvious that $g(x)$ is a polynomial in the variable $x^6$. That is to say, the only terms with non-zero coefficients must have index divisible by 6. Therefore, if $\ell - 1$ and $\ell - 2$ are not divisible by 6, then it follows that $c_{\ell-1}$ and $c_{\ell-2}$ are zero. But $\ell - 2$ cannot be divisible by 6 provided that $\ell$ is an odd number. Therefore, if $6 \nmid \ell - 1$, we obtain that $C$ is supersingular. Moreover, recall that, because of the symmetry of the equation defining $C$, $c_{\ell-1} = c_{2\ell-2}$. Therefore, if 6 does not divide $2\ell - 2$, $C$ is supersingular. These two formulations are equivalent.

As a conclusion, we can claim that, if $\ell$ is an odd prime congruent to 2 modulo 3, then the genus 2 curve $C$ defined by the equation $y^2 = x^6 + 1$ over $\mathbb{F}_\ell$ is supersingular.

Fix $\ell > 3$. In what follows, we will give a general construction of a supersingular genus 2 curve defined over $\mathbb{F}_\ell$. The key point will be to rely on the results on supersingularity obtained in Chapter1.

In Chapter 8 we saw that the genus 2 curve given by the hyperelliptic equation

$$y^2 = x^6 + bx^4 + bx^2 + 1 \tag{12.3}$$

is supersingular if the elliptic curve defined by

$$y^2 = x^3 + bx^2 + bx + 1 \tag{12.4}$$

is supersingular. Note that the discriminant $\Delta_f$ of $f(x) = x^6 + bx^4 + bx^2 + 1$ and the discriminant $\Delta_g$ of $g(x) = x^3 + bx^2 + bx + 1$ are related by the equation

$$\Delta_f = -64\Delta_g^2.$$

Therefore, if (12.4) defines an elliptic curve, then (12.3) will define a genus 2 curve whenever the characteristic of the base field is different from 2.

Therefore, our problem boils down to finding a supersingular elliptic curve defined by an equation of the form $y^2 = x^3 + bx^2 + bx + 1$ for a certain $b \in \mathbb{F}_\ell$.

Recall that an elliptic curve in Legendre form $y^2 = x(x-1)(x-\lambda)$ defined over a finite field of characteristic $\ell$ is supersingular if and only if $H_\ell(\lambda) = 0$, where $H_\ell(x)$ is the Deuring polynomial (see Proposition 1.7). Moreover, in Corollary 1.12 we noticed that, provided $\ell > 3$, there is always a quadratic factor of $H_\ell(x)$ of the form $x^2 - x + a$, for a certain $a \in \mathbb{F}_\ell^*$.

In Section 1.2, we looked for an elliptic curve given by a Weierstrass equation

$$y^2 = (x-b)(x-(c+\sqrt{-d}))(x-(c-\sqrt{-d})),$$

where $b, c, d \in \mathbb{F}_\ell$.

We sought $b, c, d \in \mathbb{F}_\ell$ such that

$$\frac{(b-c)}{\sqrt{-d}} = \pm\sqrt{1-4a}.$$

In Section 1.2, we chose

$$\begin{aligned} d &= 4a - 1 \\ b &= c + (4a - 1). \end{aligned}$$

But in this context, we want our elliptic curve to be defined by a symmetric equation. Therefore, we need some more flexibility to

choose $b, c, d$. Let us introduce a new parameter $e$: we shall seek $b, c, d, e$ such that

$$\begin{aligned} d &= e^2(4a-1) \\ b &= c + e(4a-1). \end{aligned} \tag{12.5}$$

As a matter of fact, if the resulting equation has to be of the form $y^2 = x^3 + b'x^2 + b'x + 1$ for a certain $b'$, the two following conditions must be satisfied.

$$\begin{aligned} -bc^2 - bd &= 1 \\ 2bc + c^2 + d &= -(b + 2c). \end{aligned}$$

For instance, a solution would be $b = -1, d = 1 - c^2$. Replacing these values in the equations (12.5), we obtain that

$$c = \frac{-1+2a}{2a}, e = \frac{-1}{2a}.$$

Recall that $a$ is non-zero because $x^2 - x + a$ divides $H_\ell(x)$. Therefore we can choose

$$\begin{aligned} b &= -1 \\ c &= 1 - \frac{1}{2a} \\ d &= \frac{-1+4a}{4a^2}. \end{aligned}$$

Under this choice, the polynomial $g(x)$ turns out to be

$$g(x) = x^3 + \frac{1-a}{a}x^2 + \frac{1-a}{a}x + 1.$$

The discriminant of this polynomial is $\Delta_g = -\frac{(-1+4a)^3}{a^4}$, which does not vanish (if $\Delta_g = 0$, then $a = 1/4$, and the polynomial $x^2 - x + a$ would have a double root). But the Deuring polynomial $H_\ell(x)$ does not have double roots; cf. Proposition 1.9).

Thus the equation

$$y^2 = x^3 + \frac{1-a}{a}x^2 + \frac{1-a}{a}x + 1$$

defines a supersingular elliptic curve over $\mathbb{F}_\ell$, and moreover it satisfies the symmetry condition. We can formulate this statement as a theorem:

**Theorem 12.8.** *Let $\ell > 3$ be a prime number. Let us choose $a \in \mathbb{F}_\ell$ such that the factor $x^2 - x + a$ divides the Deuring polynomial $H_\ell(x)$. Then the equation*

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

*defines a supersingular genus 2 curve.*

**Remark 12.9.** Assume $\ell = 3$. The only supersingular elliptic curve over $\mathbb{F}_3$ is given by the equation $y^2 = x(x-1)(x+1)$. We can study all the changes of variables which turn this equation into a symmetric one, but we only obtain the curve given by $y^2 = x^3 + 1$, which is a singular curve. Therefore, there is no symmetric polynomial $f(x) \in \mathbb{F}_3[x]$ such that the curve defined by $y^2 = f(x)$ is a supersingular elliptic curve. From now on, we shall have to exclude the prime $\ell = 3$ from our reasonings.

## 12.3 Stable reduction of type (II) at 5

One of the conditions in Theorem 12.1 is that there must exist a prime number $p \neq \ell$ such that the reduction of $C$ at $p$ must be stable of type (II). This leaves us great 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 ask that the order of the group of connected components of the special fibre of the Néron model at 5 is 1 (thus ensuring that $\ell$ does not divide it).

In Section 12.1 we stated some sufficient conditions that guarantee that a genus 2 curve $C$ defined over $\mathbb{Q}$ has good reduction at a given prime. We put to use the discriminant of a hyperelliptic equation with integer coefficients. But now our aim is more subtle; we will need a very precise control of the conductor, which is an invariant of the curve, far more refined than the discriminant of a hyperelliptic equation.

Before proceeding, let us say a few words about the definition of the conductor. Take a prime $p \neq \ell$, and consider a representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_{2n}(\mathbb{Q}_\ell)$$

which is continuous with respect to the Krull topology and the $\ell$-adic topology; in other words, an $\ell$-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. One can attach to $\rho_\ell$ a numerical invariant $f$, called the *conductor exponent at* $p$, that gives a measure of the ramification of $\rho_\ell$ (for an accurate description of the conductor exponent, see [76], § 2.1; cf. [12], Section 2).

In order to define the conductor of the genus 2 curve $C$, one attaches $\ell$-adic representations to $C$ by means of étale cohomology, for different primes $\ell$ (see [46], § 1.1). In this way we obtain, for all primes $p$, a conductor exponent $f_p$ (which does not depend on the choice of $\ell$). The conductor of $C$ is then defined as a product

$$N_C = \prod_{p \text{ prime}} p^{f_p}.$$

Similarly, one can define the conductor of an abelian variety, by considering the $\ell$-adic representations attached to the Tate module at different primes $\ell$. We will not dwell on the details here, but merely note that these $\ell$-adic representations obtained through étale cohomology are equivalent to the $\ell$-adic representations attached to the Tate module at different primes $\ell$ of the Jacobian variety attached to $C$ (cf. [46], § 1.1). Therefore, the conductor of $C$ coincides with the conductor of the Jacobian of $C$ as an abelian variety.

Incidentally, the conductor exponent of an abelian variety is capable of providing information about its reduction.

**Lemma 12.10.** *Let $A/\mathbb{Q}$ be an abelian variety and $p$ a prime number. If the conductor exponent at $p$ is less than or equal to 1, then $A$ has semistable reduction at $p$.*

*Proof.* The connected component of the special fibre of the Néron model at $p$, say $(\mathcal{A}_p)^0$, is the extension of an abelian variety $B$ by a linear group $H = T \times U$, where $T$ is a torus and $U$ and unipotent group (see [75]). Let us call their dimensions $t$ and $u$ respectively. The conductor exponent of $A$ at $p$ is equal to

$$f = t + 2u + \delta,$$

where $\delta$ is the measure of the wild ramification, also called Swan conductor (see [43], Chapter III, § 0). The following properties are satisfied:

- If $A$ acquires semistable reduction after a Galois extension of $\mathbb{Q}_p$ of degree prime to $p$, then $\delta = 0$.

- If $A$ has semistable reduction at $p$, then $u = 0$.

If $f = 0$, the Néron-Ogg-Shafarevich criterion assures us that $A$ has good reduction at $p$, so there is nothing to prove. Assume then that $f = 1$. In other words, assume that $1 = t + 2u + \delta$. Since $t, u, \delta$ are integer numbers greater than or equal to zero, the above relation directly implies that $u = 0$, and either $t = 1$ and $\delta = 0$ or $t = 0$ and $\delta = 1$. But this last possibility cannot hold, for if $u = t = 0$, then the connected component of the special fibre at $p$ of the Néron model of $A$ is the abelian variety $B$, that is to say, $A$ has good reduction and therefore, by the Néron-Ogg-Shafarevich criterion, the Galois representation attached to the Tate module $T_p(A)$ is unramified, thus $f = 0 \neq 1$.

Therefore, when $f = 1$, the connected component of the special fibre at $p$ of the Néron model is the extension of an abelian variety by a torus, that is to say, $A$ has semistable reduction, as was to be proven.

□

On the other hand, recall that if $A$ denotes the Jacobian variety attached to a smooth, projective and geometrically connected genus 2 curve $C$ defined over $\mathbb{Q}$, then the following conditions are equivalent (see [48], Remark 4.26 of chapter 10):

- $A$ has semistable reduction at 5.

- $C$ has stable reduction at 5.

Therefore, the previous lemma supplies a sufficient condition for $C$ to have stable reduction at $p$ in terms of the conductor exponent at $p$.

In general, controlling the conductor in a direct way is complicated, but it is easy to bound it. Namely, assume we have a hyperelliptic equation with coefficients in $\mathbb{Z}$, of discriminant $\Delta$, defining a genus 2 curve $C$. Then it holds that the $p$-adic valuation of $\Delta$ is greater than or equal to $f$ (see [46]). Therefore, if $p$ does not divide $\Delta$ or else it divides $\Delta$ just once, we can conclude that either $f = 0$ or $f = 1$. We will have to find a way to exclude the first case.

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 [48], 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 [45]). 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 $\mathbb{Q}_{p,\mathrm{nr}}$ (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 $\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{nr}}$, which in fact is the inertia group at $p$. In particular, it will be contained in the absolute Galois group of $\mathbb{Q}_p$, as we wish. 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 $\mathbb{Q}_{p,\mathrm{nr}}$ shall come into play; but since $\mathbb{Q}_{p,\mathrm{nr}}$ 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 $\mathbb{Q}_{p,\mathrm{nr}}$ 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.

The Igusa invariants can be considered as a generalization to genus 2 curves of the modular invariant $j$ of elliptic curves. Let us consider a polynomial

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

The Igusa invariants attached to $f$ are simply some elements belonging to the ring $\mathbb{Z}[\frac{1}{2}][a_0, a_1, a_2, a_3, a_4, a_5, a_6]$, defined as follows:

$$\begin{aligned}
J_2(a_0,&a_1, a_2, a_3, a_4, a_5, a_6) = -30a_0a_6 + 5a_1a_5 - 2a_2a_4 + \frac{3}{4}a_3^2,\\
J_4(a_0,&a_1, a_2, a_3, a_4, a_5, a_6) = \frac{165}{8}a_0^2a_6^2 - \frac{55}{8}a_0a_1a_5a_6 + \frac{41}{4}a_0a_2a_4a_6 -\\
&- \frac{25}{8}a_0a_2a_5^2 - \frac{21}{4}a_0a_3^2a_6 + \frac{15}{8}a_0a_3a_4a_5 - \frac{1}{2}a_0a_4^3 - \frac{25}{8}a_1^2a_4a_6 +\\
&+ \frac{15}{8}a_1^2a_5^2 + \frac{15}{8}a_1a_2a_3a_6 - \frac{7}{8}a_1a_2a_4a_5 - \frac{1}{16}a_1a_3^2a_5 + \frac{1}{8}a_1a_3a_4^2 -
\end{aligned}$$

$$
\begin{aligned}
&- \frac{1}{2}a_2^3a_6 + \frac{1}{8}a_2^2a_3a_5 + \frac{1}{8}a_2^2a_4^2 - \frac{1}{8}a_2a_3^2a_4 + \frac{3}{128}a_3^4,\\
J_6(a_0,&a_1,a_2,a_3,a_4,a_5,a_6) = 5a_0^3a_6^3 - \frac{5}{2}a_0^2a_1a_5a_6^2 - 14a_0^2a_2a_4a_6^2 +\\
&+ \frac{25}{4}a_0^2a_2a_5^2a_6 - \frac{159}{64}a_0^2a_3^2a_6^2 + \frac{165}{16}a_0^2a_3a_4a_5a_6 - \frac{125}{32}a_0^2a_3a_5^3 -\\
&- 4a_0^2a_4^3a_6 + \frac{25}{16}a_0^2a_4^2a_5^2 + \frac{25}{4}a_0a_1^2a_4a_6^2 - \frac{35}{16}a_0a_1^2a_5^2a_6 +\\
&+ \frac{165}{16}a_0a_1a_2a_3a_6^2 - \frac{51}{8}a_0a_1a_2a_4a_5a_6 + \frac{25}{16}a_0a_1a_2a_5^3 -\\
&- \frac{277}{64}a_0a_1a_3^2a_5a_6 + \frac{41}{16}a_0a_1a_3a_4^2a_6 + \frac{5}{8}a_0a_1a_3a_4a_5^2 -\\
&- \frac{3}{8}a_0a_1a_4^3a_5 - 4a_0a_2^3a_6^2 + \frac{41}{16}a_0a_2^2a_3a_5a_6 + a_0a_2^2a_4^2a_6 -\\
&- \frac{5}{8}a_0a_2^2a_4a_5^2 - \frac{49}{32}a_0a_2a_3^2a_4a_6 + \frac{5}{64}a_0a_2a_3^2a_5^2 + \frac{3}{16}a_0a_2a_3a_4^2a_5 +\\
&+ \frac{39}{128}a_0a_3^4a_6 - \frac{3}{64}a_0a_3^3a_4a_5 - \frac{125}{32}a_1^3a_3a_6^2 + \frac{25}{16}a_1^3a_4a_5a_6 -\\
&- \frac{5}{16}a_1^3a_5^3 + \frac{25}{16}a_1^2a_2^2a_6^2 + \frac{5}{8}a_1^2a_2a_3a_5a_6 - \frac{5}{8}a_1^2a_2a_4^2a_6 +\\
&+ \frac{1}{16}a_1^2a_2a_4a_5^2 + \frac{5}{64}a_1^2a_3^2a_4a_6 + \frac{11}{64}a_1^2a_3^2a_5^2 - \frac{7}{32}a_1^2a_3a_4^2a_5 +\\
&+ \frac{1}{16}a_1^2a_4^4 - \frac{3}{8}a_1a_2^3a_5a_6 + \frac{3}{16}a_1a_2^2a_3a_4a_6 - \frac{7}{32}a_1a_2^2a_3a_5^2 +\\
&+ \frac{1}{8}a_1a_2^2a_4^2a_5 - \frac{3}{64}a_1a_2a_3^3a_6 + \frac{7}{64}a_1a_2a_3^2a_4a_5 - \frac{1}{16}a_1a_2a_3a_4^3 -\\
&- \frac{7}{256}a_1a_3^4a_5 + \frac{1}{64}a_1a_3^3a_4^2 + \frac{1}{16}a_2^4a_5^2 - \frac{1}{16}a_2^3a_3a_4a_5 +\\
&+ \frac{1}{64}a_2^2a_3^3a_5 + \frac{1}{64}a_2^2a_3^2a_4^2 - \frac{1}{128}a_2a_3^4a_4 + \frac{1}{1024}a_3^6,\\
J_8 =&(1/4)\cdot(J_2\cdot J_6 - J_4^2),
\end{aligned}
$$

$$
\begin{aligned}
&J_{10}(a_0,a_1,a_2,a_3,a_4,a_5,a_6) =\\
&\quad = (1/2)^{12}\operatorname{disc}(a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0).
\end{aligned}
$$

I have computed these expressions with the help of Magma (see [54] for a brief review of the theory of the invariants and covariants of bilinear forms).

Moreover, we define

$$\begin{aligned} I_4 :=& J_2^2 - 2^3 \cdot 3 J_4, \\ I_{12} :=& -2^3 J_4^3 + 3^2 J_2 J_4 J_6 - 3^3 J_6^2 - J_2^2 J_8. \end{aligned}$$

We are able now to present Liu's characterization of the reduction type of a genus 2 curve in terms of the Igusa invariants (see Theorem 1 of [45]). As a matter of fact, we will just state the results concerning potential good reduction (that is to say, type (I)) and type (II).

**Theorem 12.11.** *Let $R$ be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and fraction 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 normalization of $\mathcal{C}_{\overline{s}}$ is an elliptic curve, of modular $j$-invariant $j = \overline{(I_4^3 I_{12}^{-1})}$.*

**Remark 12.12.** In the first case in the theorem, 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 12.13.** 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:

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

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. We must compute $J_{2i}^5 J_{10}^{-i}$, for $i = 1, 2, 3, 4, 5$. We obtain the following list:

$$\{\frac{-8587340257}{27380}, \frac{4053211077702843}{24565003059200}, \frac{-51543652195468685 75}{172182984642789376},$$
$$\frac{881034504963363427759250580048451}{617921920305669487313551360000}, 1\}.$$

If we compute the factorization of the numbers appearing on the list, we obtain:

$$\{-2^{-2}5^{-1}37^{-2}97^5, \quad 2^{-19}3^{15}5^{-2}7^{10}37^{-4},$$
$$-2^{-26}5^2 37^{-6}2903^5, \quad 2^{-48}5^{-4}17^5 19^5 37^{-8}61^5 197^5, 1\}.$$

It is plain 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 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). For if we compute the list of the $J_{2i}^6 I_{12}^{-i}$ for $i = 1, 2, 3, 4, 5$, we get

$$\{-2^{-6}37^{-1}97^6 29599^{-1}, \quad 2^{-30}3^{18}7^{12}37^{-2}29599^{-2},$$
$$-2^{-42}5^6 37^{-3}2903^6 29599^{-3},$$
$$2^{-72}17^6 19^6 37^{-4}61^6 197^6 29599^{-4}, \quad -2^{-18}5^6 37^7 29599^{-5}\}.$$

All these elements belong to $\mathbb{Z}_5$, and the last one is contained in the maximal ideal, and Theorem 12.11 allows us to conclude. Moreover, since $p = 5$ divides the discriminant of the equation just once, Lemma 12.10 tells us that the reduction is indeed stable.

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

**Theorem 12.14.** *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).*

*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 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 12.11 implies that the reduction is of type (II). □

On the other hand, we can compute the order of the group of connected components of the special fibre at $p$ of the Néron model of the Jacobian of a genus 2 curve $C$ in terms of Igusa invariants. Namely, the following proposition holds (see [45], Proposition 2-(ii)):

**Proposition 12.15.** *Let $R$ be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and fraction field $K$. Assume that the residual field $k$ is separably closed. Denote by $v$ the valuation in $R$. Let $C$ be a geometrically connected smooth projective curve of genus 2 defined over $K$ by the equation $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 6 without multiple roots. Then if the stable reduction of $C$ is of type (II), the group $\Phi$ of the connected components of the special fibre of the Néron model at $v$ is isomorphic to $\mathbb{Z}/e\mathbb{Z}$, where*

$$e = \frac{1}{6}v(J_{10}^6 I_{12}^{-5}).$$

**Remark 12.16.** Consider the curve $C$ in Example 12.13. We can compute

$$v_5(J_{10}^6 I_{12}^{-5}) = v_5\left(\left(\frac{6845}{256}\right)^6 \cdot \left(\frac{-1095163}{64}\right)^{-5}\right) = 6.$$

By the proposition above, the order of the group of connected components of the special fibre of the Néron model at $p = 5$ is 1. Therefore, we can add the following complement to Theorem 12.14.

**Theorem 12.17.** *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.*

## 12.4 Choosing the auxiliary primes

In this section we are going to deal with the last condition in Theorem 12.1. We wish to construct a genus 2 curve $C$ such that, at certain well chosen primes $q_1$ and $q_2$, it has good reduction and the characteristic polynomial of the Frobenius endomorphism at $q_i$, $i = 1, 2$, satisfies some properties concerning its factorization over $\mathbb{F}_\ell$.

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 $\ell$.

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? We need to recall the explicit conditions which reflect the relationship between the curve $C$ and the characteristic polynomial of the Frobenius endomorphism at any given prime $q$. Namely, if $N_1$ (resp. $N_2$) denotes the number of points of $C$ over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$), it holds that

$$\begin{cases} N_1 = q + 1 + a \\ N_2 = q^2 + 1 + 2b - a^2 \end{cases}$$

(see [17], Chapter 14, § 2, Theorem 14.17).

In [50], 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 [50]).

**Definition 12.18.** 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 the following inequalities are satisfied

$$|a| \leq 4\sqrt{q}$$
$$2|a|\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q.$$

**Remark 12.19.** 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 [50], we can state the following result:

**Theorem 12.20.** *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 the following conditions are satisfied:*

- *$\Delta_0$ is not a square in $\mathbb{Z}$.*
- *$q \nmid b$*
- *$a^2 \notin \{0, q + b, 2b, 3(b - q)\}$.*

*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 12.21.** The previous corollary 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 [26].

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

**Proposition 12.22.** *Let* $\ell$ *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* $q$*,* $P_1(X) = X^4+a_1X^3+b_1X^2+q_1a_1X+q_1^2$ *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 $\ell$, 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 12.20, 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 12.23.** *Let* $\ell$ *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 12.22, 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 $\ell$. This is possible for the same reason as in the proof of Proposition 12.22. 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 12.24. 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 12.20 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 would 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 $\alpha_2$ and $\beta_2$ 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 $\ell$. 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 $\mathbb{F}_\ell$, as we wished.

□

**Lemma 12.24.** *Let $A$ be a natural number, and let $\ell$ 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 get that $4\ell = x^2 - y^2 = (x + y)(x - y)$. Therefore $\ell = \frac{x+y}{2} \cdot \frac{x-y}{2}$. Since $\ell$ 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. □

## 12.5 Main result

In this section we will state the main result concerning tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. At the beginning of the chapter we stated a result, Theorem 12.1, that claims the existence of an abelian surface $A$ such that the Galois extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$ is tamely ramified with Galois group $\mathrm{GSp}_4(\mathbb{F}_\ell)$, provided that a certain set of conditions are satisfied. But from the looks of the conditions, we cannot be sure when they might be satisfied, or indeed if they can be satisfied at all. Throughout this chapter, 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 12.25.** *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* $b \in \mathbb{F}_\ell$ *be such that the elliptic curve defined by* $y^2 = x^3 + bx^2 + bx + 1$ *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:*

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

- *The following congruences mod* 3 *hold:*

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

- *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 $\ell^4$ 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,*

$$\begin{cases} f_6 \equiv 1 \pmod{\ell} \\ f_5 \equiv 0 \pmod{\ell} \\ f_4 \equiv b \pmod{\ell} \\ f_3 \equiv 0 \pmod{\ell}. \end{cases}$$

- *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 $\ell$, the following congruences hold:*

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

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

*Proof.* The existence of the element $b \in \mathbb{F}_\ell$ such that the elliptic curve defined by $y^2 = x^3 + bx^2 + bx + 1$ is supersingular is proved in Section 12.2. On the other hand, the existence of the genus 2 curves $C_1$ and $C_2$ is proved in Propositions 12.22 and 12.23. The theorem is thus a direct consequence of Theorem 12.1. □

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 12.26.** *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 12.27.** As we remarked at the beginning of Section 12.3, 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 following equation:

$$y^2 = x^6 + 391300x^4 + 1170x^3 + 1300x^2 + 1. \tag{12.6}$$

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, by Lemma 12.10, 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 12.3 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 $\ell = 5$.

How does this curve behave at the prime $\ell = 5$? Note that

$$\begin{cases} f_6 \equiv f_0 \pmod{5^4} \\ f_5 \equiv f_1 \pmod{5^4} \\ f_2 \equiv f_4 \equiv 50 \pmod{5^4}. \end{cases}$$

Therefore, the equation defining $C$ is congruent modulo $5^4$ with the 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 $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{F}_5)$ the Galois representation which arises from the action of the Galois group on the points of 5-torsion of the Jacobian variety attached to $C$. Now we want to determine its image.

The computation of the reduction data of $C$ at the prime $p = 27792683$ shows that the stable reduction at $p$ is of type (II), that is to say, of the kind $I_{\{1,0,0\}}$. Therefore, the prime $p = 27792683$ satisfies the hypothesis of Lemma 11.5. 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 11.2.

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 (11.2) 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 $\rho_5$ 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 12.26 without excluding the prime $\ell = 5$:

**Corollary 12.28.** *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 12.29.** *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 12.25. 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 (12.6) modulo a suitable power of the primes $2, 3, 5, 13, 27792683$ will provide a tamely ramified Galois realization of $\mathrm{GSp}_4(\mathbb{F}_5)$. □

## 12.6 Some examples

In this section we will present a few examples to illustrate how Theorem 12.25 allows us to compute explicitly genus 2 curves providing tame Galois realizations of the group $\mathrm{GSp}_4(\mathbb{F}_\ell)$. In fact, Theorem 12.25 can easily be turned into an algorithm to compute these genus 2 curves. Even though we have not explicitly formulated it in this way, the examples will thoroughly clarify how the algorithm works.

Before turning our attention to the examples, note the simple well-known result:

**Lemma 12.30.** *Let $q$ be a prime number. Then*

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

**Example 12.31.** Let us take $\ell = 7$. We will compute all the elements that appear in the statement of Theorem 12.25.

- 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 12.30 yields that $\mathrm{card}(\mathrm{GSp}_4(\mathbb{F}_\ell)) = 1659571200 = 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^4$. 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 $b \in \mathbb{F}_7$ such that the equation $y^2 = x^3 + bx^2 + bx + 1$ defines a supersingular elliptic curve. In order to do this, we compute the Deuring polynomial (see Section 12.2)

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

  Therefore, $x^2 - x + 5 = (x+1)(x+5)$ divides the Deuring polynomial, so we can take $b = (1-5)/5 = 2$ 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 12.22, we need to find $b_1$ such that $1-4\cdot b_1+8\cdot 29$ is not a square modulo $\ell$. 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 12.23, 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 12.25 replacing the elements that appear there by the ones we have chosen above:

**Proposition 12.32.** *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

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

**Example 12.33.** Now we will take $\ell = 11$. As before, we will start by determining an appropriate choice of the elements that occur in Theorem 12.25.

- We begin by computing the set $\mathcal{P}$ of primes dividing the order of $\mathrm{GSp}_4(\mathbb{F}_{11})$; applying Lemma 12.30, we can compute

$$\mathrm{card}(\mathrm{GSp}_4(F_{11})) = (11-1)11^{\frac{4^2}{4}} \prod_{j=1}^{2}(11^{2j}-1) = \\ = 257213088000 = 2^8 \cdot 3^2 \cdot 5^3 \cdot 11^4 \cdot 61.$$

  Therefore $\mathcal{P} = \{2, 3, 5, 11, 61\}$.

- The next step is to find a value $b \in \mathbb{F}_{11}$ such that the equation $y^2 = x^3 + b \cdot x^2 + b \cdot x + 1$ defines a supersingular elliptic curve. The way to locate this value is to compute the Deuring polynomial

$$H_{11}(t) = \sum_{j=0}^{5} \binom{5}{j}^2 t^j = t^5 + 3t^4 + t^3 + t^2 + 3t + 1 = \\ = (t+1)(t+5)(t+9)(t^2+10t+1).$$

  Therefore, we can take $b = (1-1)/1 = 0$.

- The next elements that we encounter are the primes $q_1$ and $q_2$. Recall that we must choose different $q_1, q_2 \equiv 1 \pmod{11}$ such that $q_2 > 3 \cdot 11$. For instance, we have taken $q_1 = 23$, $q_2 = 67$. Next, we have to find the genus 2 curves $C_1$ and $C_2$.

  - Choosing the curve $C_1$: Let us take $a_1 = 1$. According to Proposition 12.22, we must choose $b_1$ in such a way that $1 - 4b_1 + 8 \cdot 23$ is not a square modulo $\ell$. For instance, we

can pick $b_1 = 6$. Therefore, we can compute the quantities $N_1 = 23 + 1 + a_1 = 25$, $N_2 = 23^2 + 1 + 2b_1 - a_1^2 = 541$. Next, we must find a genus 2 curve $C_1$ with $N_1$ points over $\mathbb{F}_{23}$ and $N_2$ points over $\mathbb{F}_{23^2}$. The curve given by the hyperelliptic equation $y^2 = x^6 + x^5 + x^2 + 10x + 1$ satisfies these conditions.

– Choosing the curve $C_2$: Pick $a_2 = 1$. According to Proposition 12.23, the first step is to take an element $z$ such that $z^2 - 16 \cdot 67$ is not a square modulo $\ell$. We have taken $z = 1$. Next, we have to pick $b_2$ such that $1 - 4b_2 + 8 \cdot 67$ is congruent to $(z+1)^2 = 4$ modulo 67. For instance, $b_2 = 5$ satisfies this condition. Moreover, with this choice of $b_2$ it holds that $1 - 4 \cdot b_2 + 8 \cdot 67 = 517$ is not a square in $\mathbb{Z}$. Therefore we have the necessary ingredients to compute the quantities $N_1 = 67 + 1 + a_2 = 69$ and $N_2 = 67^2 + 1 + 2b_2 - a_2^2 = 4499$. Now we take the hyperelliptic equation $y^2 = x^6 + x^5 + 34x + 8$. It is easy to check that the curve $C_2$ defined by this equation has $N_1$ points over $\mathbb{F}_{67}$ and $N_2$ points over $\mathbb{F}_{67^2}$.

Once we have made all these choices, we can peruse Theorem 12.25 replacing the elements there by the ones we have determined. We obtain the following proposition:

**Proposition 12.34.** *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* $11^4$ *hold:*

$$\begin{cases} f_6 \equiv f_0 \pmod{11^4} \\ f_5 \equiv f_1 \pmod{11^4} \\ f_4 \equiv f_2 \pmod{11^4}. \end{cases}$$

*Furthermore,*

$$\begin{cases} f_6 \equiv 1 \pmod{11} \\ f_5 \equiv 0 \pmod{11} \end{cases} \quad \begin{cases} f_4 \equiv 0 \pmod{11} \\ f_3 \equiv 0 \pmod{11}. \end{cases}$$

- *The following congruences mod* 23 *hold:*

$$\begin{cases} f_6 \equiv 1 \pmod{23} \\ f_5 \equiv 1 \pmod{23} \\ f_4 \equiv 0 \pmod{23} \\ f_3 \equiv 0 \pmod{23} \end{cases} \quad \begin{cases} f_2 \equiv 1 \pmod{23} \\ f_1 \equiv 10 \pmod{23} \\ f_0 \equiv 1 \pmod{23}. \end{cases}$$

- *The following congruences modulo 61 hold:*

$$\begin{cases} f_0 \equiv f_6 \equiv 1 \pmod{61} \\ f_1 \equiv f_5 \equiv 0 \pmod{61} \end{cases} \quad \begin{cases} f_2 \equiv f_4 \equiv 0 \pmod{61} \\ f_3 \equiv 0 \pmod{61}. \end{cases}$$

- *The following congruences mod* 67 *hold:*

$$\begin{cases} f_6 \equiv 1 \pmod{67} \\ f_5 \equiv 1 \pmod{67} \\ f_4 \equiv 0 \pmod{67} \\ f_3 \equiv 0 \pmod{67} \end{cases} \quad \begin{cases} f_2 \equiv 0 \pmod{67} \\ f_1 \equiv 34 \pmod{67} \\ f_0 \equiv 8 \pmod{67}. \end{cases}$$

*Then the Galois extension* $\mathbb{Q}(J(C)[11])/\mathbb{Q}$ *provides a tamely ramified Galois realization of* $\mathrm{GSp}_4(\mathbb{F}_{11})$.

It is simple to construct curves satisfying the conditions of the proposition above. One such curve is defined by the hyperelliptic equation

$$y^2 = x^6 + 798661776 \cdot x^5 + 723807700 \cdot x^4 + 998854626 \cdot x^3 + \\ + 431555730100 \cdot x^2 + 1561224728976 \cdot x + 1059932266801.$$

# Appendix A

In Lemma 8.4, we make use of a set of equations defining the Jacobian of a genus 2 curve $C$. More precisely, we consider the set of 72 quadratic equations which define the Jacobian variety of $C$ as a subvariety of $\mathbb{P}^{15}$ that can be found at

`http://www2.maths.ox.ac.uk/ flynn/genus2/jacobian.variety/defining.equations`

Since the precise way in which they are labeled is essential to the statement of the Lemma, we will list them in this appendix, in order to avoid misunderstandings.

$$
\begin{aligned}
\mathrm{eqn}(1) :=& -a_0a_{11} + f_1a_{14}a_3 + f_3a_{10}a_5 + f_5a_3a_{10} + 2a_4a_3\\
\mathrm{eqn}(2) :=& -a_0a_{10} + a_3^2\\
\mathrm{eqn}(3) :=& -a_0a_{12} + a_3a_5\\
\mathrm{eqn}(4) :=& -f_0f_2a_{14}^2 - f_0a_{14}a_5 - 8f_0f_6a_{12}^2 - f_3f_5a_{12}a_{10} - f_1f_6a_{13}a_{10} -\\
&- f_2f_5a_{13}a_{10} - f_1f_5a_{13}a_{11} - 3f_5f_0a_{13}a_{12} - f_1f_3a_{14}a_{12} -\\
&- f_3f_0a_{14}a_{13} - f_0f_6a_{14}a_{10} - f_2f_4a_{14}a_{10} + a_4^2 - a_0a_{12} -\\
&- 6f_0f_6a_{12}a_{15} - f_2f_6a_{10}a_{15} - f_1f_6a_{11}a_{15} - f_5f_0a_{13}a_{15} -\\
&- f_1f_4a_{14}a_{11} - f_2a_{12}a_5 - f_4f_0a_{13}^2 - f_0f_6a_{15}^2 - f_4f_6a_{10}^2 -\\
&- f_6a_{10}a_3 - f_4a_{10}a_5 - f_3f_6a_{10}a_{11} - 4f_2f_6a_{10}a_{12} -\\
&- 2f_1f_6a_{11}a_{12}\\
\mathrm{eqn}(5) :=& -a_0a_{13} + f_1a_{14}a_5 + f_3a_{14}a_3 + f_5a_{10}a_5 + 2a_5a_4\\
\mathrm{eqn}(6) :=& -a_0a_{14} + a_5^2\\
\mathrm{eqn}(7) :=& -4f_0f_2a_{14}^2 - 4f_0a_{14}a_5 + a_0a_{15} - 36f_0f_6a_{12}^2 - 4f_3f_5a_{12}a_{10} -\\
&- 4f_1f_6a_{13}a_{10} - 4f_2f_5a_{13}a_{10} - 12f_5f_0a_{13}a_{12} -
\end{aligned}
$$

$$
\begin{aligned}
&- 2f_1f_3a_{14}a_{12} - 4f_3f_0a_{14}a_{13} - 4f_2f_4a_{14}a_{10} - 4f_5a_{10}a_4 -\\
&- f_5^2a_{10}^2 - 24f_0f_6a_{12}a_{15} - 4f_2f_6a_{10}a_{15} - 4f_1f_6a_{11}a_{15} -\\
&- 4f_5f_0a_{13}a_{15} - 4f_1f_4a_{14}a_{11} + f_3^2a_{14}a_{10} - 2f_3a_{11}a_5 -\\
&- 16f_1f_5a_{12}^2 - 2f_1a_{13}a_5 - 4f_2a_{12}a_5 - 4f_0f_6a_{15}^2 -\\
&- 4f_4f_6a_{10}^2 - 4f_6a_{10}a_3 - 4f_4a_{10}a_5 - 4f_3f_6a_{10}a_{11} -\\
&- 16f_2f_6a_{10}a_{12} - 8f_1f_6a_{11}a_{12} + f_1^2a_{14}^2 - 16f_0f_4a_{14}a_{12} -\\
&- 4f_1f_5a_{12}a_{15} - 4f_0f_4a_{14}a_{15}
\end{aligned}
$$

$$
\begin{aligned}
\text{eqn}(8) :=& - f_1a_{14}^2 - f_3a_{14}a_{12} + 2f_4a_{13}a_{12} - f_5a_{12}^2 - 2a_4a_{14} -\\
&- 2f_4a_{14}a_{11} + a_5a_{13}
\end{aligned}
$$

$$
\text{eqn}(9) := - f_1a_{14}a_{12} - f_3a_{14}a_{10} - f_5a_{12}a_{10} - 2a_4a_{12} + a_5a_{11}
$$

$$
\begin{aligned}
\text{eqn}(10) :=& 2f_4a_{14}a_{10} + 2f_5a_{12}a_{11} - 4a_5a_{12} - 2f_4a_{12}^2 - a_5a_{15} +\\
&+ f_1a_{14}a_{13} + f_3a_{14}a_{11} - f_5a_{13}a_{10} + 2a_4a_{13}
\end{aligned}
$$

$$
\begin{aligned}
\text{eqn}(11) :=& - f_5a_{10}^2 - f_3a_{10}a_{12} + 2f_2a_{11}a_{12} - f_1a_{12}^2 - 2a_4a_{10} -\\
&- 2f_2a_{13}a_{10} + a_3a_{11}
\end{aligned}
$$

$$
\text{eqn}(12) := f_2a_{12}^2 + f_1a_{13}a_{12} - a_5a_{10} - f_1a_{14}a_{11} - f_2a_{10}a_{14} + a_3a_{12}
$$

$$
\text{eqn}(13) := f_5a_{13}a_{10} + f_4a_{14}a_{10} - a_5a_{12} - f_4a_{12}^2 - f_5a_{12}a_{11} + a_3a_{14}
$$

$$
\text{eqn}(14) := - f_1a_{14}a_{12} - f_3a_{14}a_{10} - f_5a_{12}a_{10} - 2a_4a_{12} + a_3a_{13}
$$

$$
\begin{aligned}
\text{eqn}(15) :=& 4f_1a_{13}a_{12} - 2a_5a_{10} - 3f_1a_{14}a_{11} - a_3a_{15} - 2a_3a_{12} +\\
&+ f_5a_{10}a_{11} + f_3a_{10}a_{13} + 2a_4a_{11}
\end{aligned}
$$

$$
\text{eqn}(16) := - a_{14}a_{15} - 4a_{12}a_{14} + a_{13}^2
$$

$$
\text{eqn}(17) := - a_{10}a_{14} + a_{12}^2
$$

$$
\text{eqn}(18) := - a_{10}a_{15} - 4a_{10}a_{12} + a_{11}^2
$$

$$
\text{eqn}(19) := - a_{11}a_{13} + 2a_{10}a_{14} + a_{12}a_{15} + 2a_{12}^2
$$

$$
\text{eqn}(20) := - a_{12}a_{13} + a_{11}a_{14}
$$

$$
\text{eqn}(21) := - a_{11}a_{12} + a_{10}a_{13}
$$

$$
\begin{aligned}
\text{eqn}(22) :=& - a_{10}^2f_2f_5^2 - a_{11}^2f_0f_5^2 + a_1^2 - a_0a_3 + 8f_0f_6a_4a_{11} - a_{10}^2f_3^2f_6 -\\
&- f_4a_3^2 - f_0a_5^2 + 4a_{10}^2f_1f_5f_6 + 4a_{10}^2f_2f_4f_6 - a_{10}a_3f_3f_5 +\\
&+ 4a_{10}a_3f_2f_6 + 8f_1f_6a_{10}a_4 + f_1f_5a_{10}a_5 + 4a_{11}^2f_0f_4f_6 -\\
&- a_{10}a_{11}f_1f_5^2 + 4a_{10}a_{11}f_0f_5f_6 + 4a_{10}a_{11}f_1f_4f_6 +
\end{aligned}
$$

$$
\begin{aligned}
&+ 4f_0f_5a_{12}a_4 + 2a_{12}a_{10}f_0f_5^2 + 6a_{12}a_{10}f_1f_3f_6 + \\
&+ 8f_0f_3f_6a_{12}a_{11} + 4a_{14}a_{10}f_0f_2f_6 + 2a_{14}a_{10}f_0f_3f_5 + \\
&+ 3a_{14}a_{10}f_1^2f_6 + 4f_0f_1f_6a_{14}a_{11} + 2f_0f_1f_5a_{14}a_{12} \\
\text{eqn}(23) :=& a_1a_2 - a_0a_4 + 3a_{13}a_{10}f_0f_5^2 + a_{13}a_{10}f_1f_3f_6 + 2a_{10}^2f_2f_5f_6 + \\
&+ f_3f_6a_{10}a_3 + 4f_2f_6a_{10}a_4 + a_{10}a_5f_2f_5 + 5a_{10}a_5f_1f_6 + \\
&+ 4f_1f_6a_{12}a_3 + 20f_0f_6a_{12}a_4 + 10f_0f_5f_6a_{10}a_{12} + \\
&+ 2a_{12}^2f_1f_3f_5 + 28a_{12}^2f_0f_3f_6 + 4a_{12}^2f_1f_2f_6 + 3f_1f_5a_{12}a_4 + \\
&+ 2a_{12}a_{10}f_1f_4f_6 + 2a_{12}a_{10}f_2f_3f_6 + a_{12}a_{10}f_1f_5^2 - \\
&- 4f_0f_5^2a_{12}a_{11} - 4f_0f_6f_4a_{12}a_{11} + 2f_0f_4a_{13}a_5 + \\
&+ 8a_{10}a_{13}f_0f_4f_6 + 8a_{13}a_{12}f_0f_2f_6 + 3a_{13}a_{12}f_0f_3f_5 - \\
&- a_{13}a_{12}f_1^2f_6 + 9a_{14}a_3f_0f_5 + a_{14}a_3f_1f_4 + f_0f_3a_{14}a_5 - \\
&- 2f_1f_6f_2a_{14}a_{10} - 8f_0f_6f_3a_{14}a_{10} - 2f_0f_5f_3a_{14}a_{11} - \\
&- 4f_0f_6f_2a_{14}a_{11} + 10f_1f_6f_0a_{14}a_{12} + 2a_{14}a_{12}f_0f_2f_5 + \\
&+ a_{14}a_{12}f_1^2f_5 + 2f_1f_6a_3a_{15} + 4f_0f_6a_4a_{15} + 2f_0f_5a_5a_{15} + \\
&+ 2f_0f_5f_6a_{10}a_{15} + 4f_0f_3f_6a_{12}a_{15} + 2f_1f_6f_0a_{14}a_{15} \\
\text{eqn}(24) :=& - a_{14}^2f_0f_3^2 - a_{14}^2f_1^2f_4 + a_2^2 - a_0a_5 - f_6a_3^2 - f_2a_5^2 + \\
&+ 8a_{13}a_4f_0f_6 + 4f_0f_5a_{13}a_5 + 4a_{13}a_{10}f_0f_5f_6 - \\
&- 4a_{13}a_{10}f_1f_4f_6 + 4f_0f_4a_{14}a_5 + 4a_{10}a_{14}f_0f_4f_6 - \\
&- a_{10}a_{14}f_0f_5^2 + 4a_{10}a_{14}f_1f_3f_6 + 8f_1f_6a_{12}a_4 + \\
&+ 4f_1f_5f_6a_{12}a_{10} + 4f_1f_6f_4a_{12}a_{11} - 2f_1f_6a_{13}a_3 + \\
&+ 4a_{14}a_{13}f_0f_1f_6 + 4a_{14}a_{13}f_0f_2f_5 - a_{14}a_{13}f_1^2f_5 + \\
&+ 4a_{14}^2f_0f_2f_4 + f_1f_5a_{14}a_3 - a_{14}a_5f_1f_3 + 8a_{14}a_{11}f_0f_3f_6 + \\
&+ 16a_{14}a_{12}f_0f_2f_6 + 2a_{14}a_{12}f_0f_3f_5 + 4a_{14}f_0f_2f_6a_{15} - \\
&- a_{14}f_1^2f_6a_{15} \\
\text{eqn}(25) :=& - a_0a_{14} - f_2a_{14}a_5 - f_3a_{14}a_4 - 2f_4a_{14}a_3 - 3f_5a_4a_{12} - \\
&- f_6a_3a_{15} - 5f_6a_3a_{12} - f_1f_3a_{14}^2 - f_1f_4a_{14}a_{13} - \\
&- f_1f_5a_{14}a_{15} - 5f_1f_5a_{12}a_{14} - f_1f_6a_{13}a_{15} - 3f_1f_6a_{13}a_{12} - \\
&- 2f_2f_4a_{14}a_{12} - 2f_2f_5a_{13}a_{12} - 2f_2f_6a_{13}a_{11} - \\
&- 3f_3f_5a_{14}a_{10} - 2f_3f_6a_{12}a_{11} - 2f_4f_6a_{12}a_{10} - f_5^2a_{12}a_{10} +
\end{aligned}
$$

$$
\begin{aligned}
&+ a_2a_9 \\
\text{eqn(26)} := &- a_0a_{13} + f_1a_{14}a_5 + f_3a_5a_{12} - f_5a_{10}a_5 - 2f_6a_{11}a_3 + \\
&+ 2f_0f_3a_{14}^2 + 4f_0f_4a_{14}a_{13} + 4f_5f_0a_{14}a_{15} + 14f_5f_0a_{14}a_{12} + \\
&+ 4f_0f_6a_{13}a_{15} + 8f_0f_6a_{13}a_{12} + 4f_0f_6a_{14}a_{11} + \\
&+ 2f_1f_4a_{14}a_{12} + 2f_1f_5a_{13}a_{12} + 2f_1f_6a_{12}a_{15} + \\
&+ 8f_1f_6a_{12}^2 + 2a_2a_8 \\
\text{eqn(27)} := &2f_2a_3a_{14} - a_0a_{15} + 40f_0f_6a_{12}^2 + 6f_3f_5a_{12}a_{10} + \\
&+ 4f_2f_5a_{13}a_{10} + 8f_5f_0a_{13}a_{12} + 3f_1f_3a_{14}a_{12} + \\
&+ 2f_3f_0a_{14}a_{13} + 8f_0f_6a_{14}a_{10} + 4f_2f_4a_{14}a_{10} - 2a_0a_{12} + \\
&+ 4f_5a_{10}a_4 + f_5^2a_{10}^2 + 4f_3a_{12}a_4 + 28f_0f_6a_{12}a_{15} + \\
&+ 4f_1f_6a_{11}a_{15} + 4f_5f_0a_{13}a_{15} + 4f_1f_4a_{14}a_{11} + f_3^2a_{14}a_{10} + \\
&+ 4f_2f_6a_{11}^2 + 16f_1f_5a_{12}^2 + f_1a_{13}a_5 + 2a_2a_7 + 4f_0f_6a_{15}^2 + \\
&+ 4f_4f_6a_{10}^2 + 2f_6a_{10}a_3 + 4f_4a_{10}a_5 + 4f_3f_6a_{10}a_{11} + \\
&+ 14f_1f_6a_{11}a_{12} + 16f_0f_4a_{14}a_{12} + 4f_1f_5a_{12}a_{15} + \\
&+ 4f_0f_4a_{14}a_{15} + f_1f_5a_{14}a_{10} + 6a_{14}a_{11}f_0f_5 \\
\text{eqn(28)} := &- a_0a_{11} - 4f_0a_{13}a_5 - f_1a_{15}a_5 - 5f_1a_{12}a_5 - 2f_2a_{11}a_5 - \\
&- f_3a_{10}a_5 + f_5a_3a_{10} - 4f_0f_2a_{14}a_{13} - 2f_3f_0a_{15}a_{14} - \\
&- 10f_0f_3a_{14}a_{12} - 4f_0f_4a_{14}a_{11} - 2a_{15}a_{12}f_0f_5 - 6f_0f_5a_{12}^2 + \\
&+ f_1^2a_{14}a_{13} - f_1f_3a_{14}a_{11} - 2f_1f_4a_{12}^2 - f_1f_5a_{13}a_{10} + 2a_2a_6 \\
\text{eqn(29)} := &- a_0a_{10} - f_4a_3a_{10} - f_3a_4a_{10} - 2f_2a_{10}a_5 - 3f_1a_{12}a_4 - \\
&- f_0a_{15}a_5 - 5f_0a_{12}a_5 - f_5f_3a_{10}^2 - f_5f_2a_{10}a_{11} - \\
&- f_1f_5a_{15}a_{10} - 5f_1f_5a_{10}a_{12} - a_{15}a_{11}f_0f_5 - 3f_5f_0a_{11}a_{12} - \\
&- 2f_4f_2a_{10}a_{12} - 2f_4f_1a_{11}a_{12} - 2f_0f_4a_{13}a_{11} - \\
&- 3a_{14}a_{10}f_1f_3 - 2f_3f_0a_{13}a_{12} - 2f_0f_2a_{14}a_{12} - f_1^2a_{14}a_{12} + \\
&+ a_6a_1 \\
\text{eqn(30)} := &- a_0a_{11} + f_5a_3a_{10} + f_3a_3a_{12} - f_1a_{14}a_3 - 2f_0a_{13}a_5 + \\
&+ 2f_6f_3a_{10}^2 + 4f_2f_6a_{10}a_{11} + 4a_{10}f_1f_6a_{15} + 14a_{10}a_{12}f_1f_6 + \\
&+ 4f_0f_6a_{15}a_{11} + 8f_0f_6a_{12}a_{11} + 4f_0f_6a_{13}a_{10} + \\
&+ 2f_2f_5a_{12}a_{10} + 2f_1f_5a_{12}a_{11} + 2a_{15}a_{12}f_0f_5 + 8f_0f_5a_{12}^2 +
\end{aligned}
$$

$$
\begin{aligned}
&+ 2a_1a_7 \\
\text{eqn}(31) :=&4f_0f_2a_{14}^2 + 2f_0a_{14}a_5 + f_5a_3a_{11} - a_0a_{15} + 40f_0f_6a_{12}^2+ \\
&+ 3f_3f_5a_{12}a_{10} + 6f_1f_6a_{13}a_{10} + 14f_5f_0a_{13}a_{12}+ \\
&+ 6f_1f_3a_{14}a_{12} + 4f_3f_0a_{14}a_{13} + 8f_0f_6a_{14}a_{10} - 2a_0a_{12}+ \\
&+ 4f_3a_{12}a_4 + 28f_0f_6a_{12}a_{15} + 4f_2f_6a_{10}a_{15} + 4f_1f_6a_{11}a_{15}+ \\
&+ 4f_5f_0a_{13}a_{15} + 4f_1f_4a_{14}a_{11} + f_3^2a_{14}a_{10} + 2a_1a_8+ \\
&+ 16f_1f_5a_{12}^2 + 4f_2a_{12}a_5 + 4f_4f_0a_{13}^2 + 4f_0f_6a_{15}^2+ \\
&+ 2f_4a_{10}a_5 + 2f_3f_6a_{10}a_{11} + 16f_2f_6a_{10}a_{12} + 8f_1f_6a_{11}a_{12}+ \\
&+ f_1^2a_{14}^2 + 4f_1f_5a_{12}a_{15} + f_1f_5a_{14}a_{10} + 4f_2f_4a_{12}^2+ \\
&+ 4f_1a_{14}a_4 + 2a_{12}a_{11}f_3f_4 + 4f_2f_5a_{12}a_{11} - 2a_{10}a_{13}f_3f_4- \\
&- 2a_{13}a_{12}f_2f_3 + 2a_{14}a_{11}f_2f_3 \\
\text{eqn}(32) :=&- a_0a_{13} - 4f_6a_{11}a_3 - f_5a_3a_{15} - 5f_5a_3a_{12} - 2f_4a_{13}a_3- \\
&- f_3a_{14}a_3 + f_1a_{14}a_5 - 4f_6f_4a_{10}a_{11} - 2f_6f_3a_{10}a_{15}- \\
&- 10f_6f_3a_{10}a_{12} - 4f_2f_6a_{13}a_{10} - 2f_1f_6a_{12}a_{15} - 6f_1f_6a_{12}^2+ \\
&+ f_5^2a_{10}a_{11} - f_3f_5a_{13}a_{10} - 2f_5f_2a_{12}^2 - f_1f_5a_{14}a_{11} + 2a_1a_9 \\
\text{eqn}(33) :=&- a_5a_{14} - f_2a_{14}^2 - f_3a_{14}a_{13} - f_4a_{13}^2 - 3f_5a_{13}a_{12}- \\
&- f_5a_{13}a_{15} - f_6a_{14}a_{10} - 6f_6a_{12}a_{15} - 8f_6a_{12}^2 - f_6a_{15}^2 + a_9^2 \\
\text{eqn}(34) :=&a_9a_8 - a_4a_{14} - f_3a_{14}a_{12} - f_4a_{14}a_{11} - f_5a_{12}a_{15} - 4f_5a_{12}^2- \\
&- f_6a_{11}a_{15} - 2f_6a_{11}a_{12} - f_6a_{13}a_{10} \\
\text{eqn}(35) :=&2a_9a_7 - a_5a_{15} - 2a_5a_{12} + f_1a_{14}a_{13} + 2f_2a_{14}a_{12}+ \\
&+ f_3a_{14}a_{11} - f_5a_{13}a_{10} - 2f_6a_{15}a_{10} - 6f_6a_{10}a_{12} \\
\text{eqn}(36) :=&a_6a_9 - a_4a_{15} - a_4a_{12} + f_2a_{14}a_{11} + 2f_3a_{14}a_{10} + f_4a_{12}a_{11}+ \\
&+ f_1a_{14}a_{12} + f_5a_{12}a_{10} \\
\text{eqn}(37) :=&a_8^2 - a_5a_{12} - f_0a_{14}^2 - f_4a_{12}^2 - f_5a_{12}a_{11} - f_6a_{15}a_{10}- \\
&- 4f_6a_{10}a_{12} \\
\text{eqn}(38) :=&a_7a_8 - a_4a_{12} - f_0a_{14}a_{13} - f_1a_{14}a_{12} - f_5a_{12}a_{10} - f_6a_{10}a_{11} \\
\text{eqn}(39) :=&2a_6a_8 - a_3a_{15} - 2a_3a_{12} + f_5a_{10}a_{11} + 2f_4a_{12}a_{10}+ \\
&+ f_3a_{10}a_{13} - f_1a_{14}a_{11} - 2f_0a_{15}a_{14} - 6f_0a_{14}a_{12} \\
\text{eqn}(40) :=&a_7^2 - a_5a_{10} - f_0a_{15}a_{14} - 4f_0a_{14}a_{12} - f_1a_{14}a_{11} - f_2a_{10}a_{14}-
\end{aligned}
$$

$$
\begin{aligned}
&- f_6 a_{10}^2 \\
\text{eqn}(41) :=& a_6 a_7 - a_4 a_{10} - f_3 a_{10} a_{12} - f_2 a_{13} a_{10} - f_1 a_{12} a_{15} - 4 f_1 a_{12}^2 - \\
&- f_0 a_{15} a_{13} - 2 f_0 a_{13} a_{12} - f_0 a_{11} a_{14} \\
\text{eqn}(42) :=& - a_3 a_{10} - f_4 a_{10}^2 - f_3 a_{11} a_{10} - f_2 a_{11}^2 - 3 f_1 a_{11} a_{12} - \\
&- f_1 a_{15} a_{11} - f_0 a_{14} a_{10} - 6 f_0 a_{15} a_{12} - 8 f_0 a_{12}^2 - f_0 a_{15}^2 + a_6^2 \\
\text{eqn}(43) :=& - f_1 a_9 a_3 + a_{14} a_8 f_1^2 + 4 f_1 a_8 a_4 + 2 f_3 a_3 a_7 + a_3 a_1 - \\
&- f_3 a_2 a_{10} + 4 f_0 a_8 a_5 - a_6 a_0 + 2 f_2 a_8 a_3 - 2 f_0 f_5 a_{10} a_9 + \\
&+ 3 f_1 f_5 a_{10} a_8 + 2 f_1 f_6 a_{11} a_6 + 12 f_0 f_5 a_{12} a_7 + 12 f_0 f_6 a_{12} a_6 + \\
&+ 4 a_{12} a_8 f_0 f_4 + 2 a_{12} a_8 f_1 f_3 + 2 a_{12} a_7 f_1 f_4 + 2 a_{12} a_6 f_1 f_5 + \\
&+ 4 a_{14} a_8 f_0 f_2 + 4 f_0 f_3 a_{14} a_7 + 4 f_0 f_4 a_{14} a_6 + 4 f_0 f_5 a_7 a_{15} + \\
&+ 4 f_0 f_6 a_6 a_{15} \\
\text{eqn}(44) :=& - a_7 a_0 + 2 f_0 a_9 a_5 + f_1 a_8 a_5 + a_2 a_3 \\
\text{eqn}(45) :=& f_5 a_{10} a_2 + a_2 a_4 + a_{14} a_8 f_2^2 - a_0 a_8 + f_6 a_6 a_3 - f_2 a_9 a_4 - \\
&- f_2 f_4 a_{11} a_9 + a_{11} a_8 f_1 f_6 - a_{11} a_8 f_2 f_5 + 4 f_2 f_4 a_{12} a_8 + \\
&+ 4 a_{12} a_7 f_2 f_5 - 4 a_{12} a_7 f_1 f_6 + 3 f_2 f_6 a_{12} a_6 + f_0 f_5 a_{12} a_9 - \\
&- f_0 f_3 a_{14} a_9 - a_{14} a_8 f_1 f_3 + a_{14} a_7 f_2 f_3 - a_{14} a_7 f_1 f_4 - \\
&- f_1 f_5 a_{14} a_6 + f_2 f_4 a_8 a_{15} + a_7 f_2 f_5 a_{15} - a_7 f_1 f_6 a_{15} + \\
&+ f_2 f_6 a_6 a_{15} \\
\text{eqn}(46) :=& - f_3^2 a_{14} a_7 - 2 a_{10} a_7 f_5^2 + 4 f_6 a_7 a_3 + a_2 a_5 + 4 f_1 f_6 a_{11} a_9 - \\
&- a_0 a_9 + f_3 a_9 a_4 + 3 f_5 a_3 a_8 + 2 f_4 a_7 a_5 + 4 f_0 f_5 a_{13} a_9 - \\
&- 2 f_5 f_6 a_{10} a_6 + 4 a_{10} a_7 f_4 f_6 + 4 f_3 f_6 a_{10} a_8 + 4 f_2 f_6 a_{10} a_9 + \\
&+ 12 f_0 f_6 a_{12} a_9 - f_3 f_6 a_{12} a_6 + 4 a_{12} a_8 f_2 f_5 + 4 a_{12} a_9 f_1 f_5 + \\
&+ 4 a_{12} a_7 f_2 f_6 + 2 a_{12} a_7 f_3 f_5 - a_{12} a_8 f_3 f_4 - f_3 f_5 a_{13} a_6 + \\
&+ 2 f_1 f_5 a_{14} a_7 - a_{14} a_6 f_3 f_4 - a_{14} a_8 f_2 f_3 + 2 a_{14} a_6 f_1 f_6 + \\
&+ 4 f_0 f_6 a_9 a_{15} - f_3 f_6 a_6 a_{15} \\
\text{eqn}(47) :=& - a_0 a_8 + 2 f_6 a_6 a_3 + f_5 a_3 a_7 + a_5 a_1 \\
\text{eqn}(48) :=& f_0 a_9 a_5 + a_1 a_4 - f_4 f_2 a_{13} a_6 + a_{10} a_7 f_4^2 + f_1 a_{14} a_1 - \\
&- f_4 a_6 a_4 + f_6 f_1 a_{12} a_6 - a_7 a_0 + a_{13} a_7 f_0 f_5 - a_{13} a_7 f_1 f_4 - \\
&- f_6 f_3 a_{10} a_6 - a_{10} a_7 f_3 f_5 + a_{10} a_8 f_3 f_4 - a_{10} a_8 f_2 f_5 -
\end{aligned}
$$

$$
\begin{aligned}
&- f_5 f_1 a_{10} a_9 + 4 f_2 f_4 a_{12} a_7 + 4 a_{12} a_8 f_1 f_4 - 4 f_0 f_5 a_{12} a_8 + \\
&+ 3 f_4 f_0 a_{12} a_9 + f_2 f_4 a_7 a_{15} + a_8 f_1 f_4 a_{15} - f_0 f_5 a_8 a_{15} + \\
&+ f_4 f_0 a_9 a_{15} \\
\mathrm{eqn}(49) := &- a_9 a_5 + f_3 a_{14} a_8 + 2 f_4 a_{14} a_7 + 2 f_5 a_{14} a_6 + 2 f_6 a_{13} a_6 + \\
&+ f_5 a_8 a_{12} + a_2 a_{14} \\
\mathrm{eqn}(50) := &- 2 a_5 a_8 - f_1 a_{14} a_9 - 2 f_2 a_{14} a_8 - f_3 a_{14} a_7 + f_5 a_7 a_{12} + \\
&+ 2 f_6 a_{12} a_6 + a_2 a_{13} \\
\mathrm{eqn}(51) := &- a_5 a_7 + 2 f_0 a_{14} a_9 + f_1 a_{14} a_8 + a_2 a_{12} \\
\mathrm{eqn}(52) := &- a_3 a_7 + 2 f_0 a_{12} a_9 + f_1 a_{12} a_8 + a_2 a_{10} \\
\mathrm{eqn}(53) := &- 2 a_8 a_3 - f_1 a_{12} a_9 - 2 f_2 a_{12} a_8 - f_3 a_{12} a_7 + f_5 a_{10} a_7 + \\
&+ 2 f_6 a_{10} a_6 + a_2 a_{11} \\
\mathrm{eqn}(54) := &- 2 a_5 a_7 - f_1 a_{13} a_9 - 2 f_2 a_{14} a_7 - 2 f_2 a_{12} a_9 - f_3 a_{14} a_6 - \\
&- 3 f_3 a_8 a_{12} - 4 f_4 a_{12} a_7 - 3 f_5 a_{12} a_6 - f_5 a_{10} a_8 - 2 f_6 a_{11} a_6 + \\
&+ a_2 a_{15} + 2 a_2 a_{12} \\
\mathrm{eqn}(55) := &- a_3 a_6 + f_3 a_{10} a_7 + 2 f_2 a_{10} a_8 + 2 f_1 a_{10} a_9 + 2 f_0 a_{11} a_9 + \\
&+ f_1 a_{12} a_7 + a_1 a_{10} \\
\mathrm{eqn}(56) := &- 2 a_3 a_7 - f_5 a_{10} a_6 - 2 f_4 a_{10} a_7 - f_3 a_{10} a_8 + f_1 a_{12} a_8 + \\
&+ 2 f_0 a_{12} a_9 + a_1 a_{11} \\
\mathrm{eqn}(57) := &- a_8 a_3 + 2 f_6 a_{10} a_6 + f_5 a_{10} a_7 + a_1 a_{12} \\
\mathrm{eqn}(58) := &- a_5 a_8 + 2 f_6 a_{12} a_6 + f_5 a_7 a_{12} + a_1 a_{14} \\
\mathrm{eqn}(59) := &- 2 a_5 a_7 - f_5 a_{12} a_6 - 2 f_4 a_{12} a_7 - f_3 a_8 a_{12} + f_1 a_{14} a_8 + \\
&+ 2 f_0 a_{14} a_9 + a_1 a_{13} \\
\mathrm{eqn}(60) := &- 2 a_8 a_3 - f_5 a_{11} a_6 - 2 f_4 a_8 a_{10} - 2 f_4 a_{12} a_6 - f_3 a_{10} a_9 - \\
&- 3 f_3 a_{12} a_7 - 4 f_2 a_{12} a_8 - 3 f_1 a_{12} a_9 - f_1 a_{14} a_7 - 2 f_0 a_{13} a_9 + \\
&+ a_1 a_{15} + 2 a_1 a_{12} \\
\mathrm{eqn}(61) := &- a_9 a_4 + f_2 a_{14} a_8 + f_3 a_{14} a_7 + f_4 a_{14} a_6 + f_4 a_{12} a_8 + \\
&+ f_5 a_{13} a_6 + f_6 a_6 a_{15} + 3 f_6 a_{12} a_6 + a_5 a_8 \\
\mathrm{eqn}(62) := &- a_4 a_8 - f_0 a_{14} a_9 - f_1 a_{14} a_8 + f_4 a_{12} a_7 + f_5 a_{12} a_6 + \\
&+ f_6 a_{11} a_6 + a_5 a_7 \\
\mathrm{eqn}(63) := &- a_4 a_7 - f_0 a_{13} a_9 - f_1 a_{14} a_7 - f_1 a_{12} a_9 - f_2 a_{12} a_8 -
\end{aligned}
$$

$$
\begin{aligned}
&\quad - f_3a_{12}a_7 + f_6a_{10}a_6 + a_6a_5 \\
\text{eqn}(64) &:= - a_4a_6 + f_4a_{10}a_7 + f_3a_{10}a_8 + f_2a_{10}a_9 + f_2a_7a_{12} + \\
&\quad + f_1a_{11}a_9 + f_0a_{15}a_9 + 3f_0a_{12}a_9 + a_3a_7 \\
\text{eqn}(65) &:= - a_4a_7 - f_6a_{10}a_6 - f_5a_{10}a_7 + f_2a_{12}a_8 + f_1a_{12}a_9 + \\
&\quad + f_0a_{13}a_9 + a_8a_3 \\
\text{eqn}(66) &:= - a_4a_8 - f_6a_{11}a_6 - f_5a_{10}a_8 - f_5a_{12}a_6 - f_4a_{12}a_7 - \\
&\quad - f_3a_8a_{12} + f_0a_{14}a_9 + a_9a_3 \\
\text{eqn}(67) &:= - 4a_7a_{12} - a_7a_{15} + a_8a_{11} + a_6a_{13} \\
\text{eqn}(68) &:= - 4a_8a_{12} - a_8a_{15} + a_7a_{13} + a_9a_{11} \\
\text{eqn}(69) &:= - a_8a_{13} + a_7a_{14} + a_9a_{12} \\
\text{eqn}(70) &:= - a_7a_{13} + a_6a_{14} + a_8a_{12} \\
\text{eqn}(71) &:= - a_8a_{11} + a_9a_{10} + a_7a_{12} \\
\text{eqn}(72) &:= - a_7a_{11} + a_8a_{10} + a_6a_{12}
\end{aligned}
$$

# Resumen en castellano

Esta tesis se desarrolla en torno al Problema Inverso de la Teoría de Galois sobre el cuerpo de los números racionales. Este problema, que fue considerado por primera vez por D. Hilbert, tiene un enunciado muy simple (para un estudiante con nociones básicas de teoría de Galois). ¿Qué grupos finitos pueden realizarse como grupos de Galois sobre $\mathbb{Q}$? En otras palabras, dado un grupo finito $G$, ¿existe una extensión de Galois $K/\mathbb{Q}$ tal que $G \simeq \mathrm{Gal}(K/\mathbb{Q})$?

Este problema ha despertado el interés de muchos matemáticos y, sin embargo, aún es un problema abierto. En la actualidad se ha resuelto afirmativamente para muchos grupos finitos. El lector puede consultar [81] o [51] para hacerse una idea sobre el estado actual de la materia.

Sea $G$ un grupo finito, y supongamos que puede ser realizado como grupo de Galois sobre $\mathbb{Q}$, digamos mediante una extensión $K_1/\mathbb{Q}$. Podría ocurrir que estuviéramos interesados en extensiones del cuerpo de los racionales cuya ramificación tenga alguna característica especial, y la extensión $K_1/\mathbb{Q}$ no resulte adecuada. Podemos preguntarnos si existe otra extensión de Galois, $K_2/\mathbb{Q}$, cuyo grupo de Galois coincida con $G$ y además su ramificación posea esta característica. En esta dirección se han estudiado diversas variantes del Problema Inverso de la Teoría de Galois.

Por ejemplo, en la sección 2 de [7], B. Birch plantea la siguiente pregunta, a la que se refiere como "algo maliciosa".

**Problema 1.** [Problema Inverso de la Teoría de Galois Moderado] Sea $G$ un grupo finito. ¿Existe una extensión de Galois $K/\mathbb{Q}$, moderadamente ramificada, tal que $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$?

Este problema es una de las posibles variantes que han sido consideradas, pero hay muchas formas de refinar el Problema Inverso de la Teoría de Galois añadiendo condiciones de ramificación. Por ejemplo,

tenemos el siguiente problema. Fijemos un conjunto finito de primos, digamos $S$, y sea $G$ un grupo finito ¿Se puede realizar el grupo $G$ como grupo de Galois de una extensión de $\mathbb{Q}$ que no ramifique en $S$? Si $G$ puede realizarse como grupo de Galois con esta condición, sea cual sea el conjunto $S$ prefijado, entonces también puede realizarse como grupo de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada. De este modo puede probarse que el Problema 1 tiene una solución afirmativa para los grupos abelianos finitos, los grupos simétricos (y todos los grupos finitos de forma que el problema de Noether tenga solución afirmativa [73]), los grupos solubles finitos (ver [59], [41]) y los grupos alternados $A_n$ [62].

Por otra parte, los grupos de Mathieu $M_{11}$ y $M_{12}$, el grupo de automorfismos de $M_{22}$ (cf. [63]), y las extensiones centrales finitas de los grupos simétricos, alternados y de Mathieu $M_{11}$ y $M_{12}$ (cf. [61]) pueden realizarse como grupos de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada.

En esta tesis abordaremos el Problema 1 mediante el estudio de las representaciones del grupo de Galois absoluto $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ asociadas a objetos aritmético-geométricos.

En efecto, sea

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$$

una representación continua, donde $V$ es un espacio vectorial sobre un cuerpo finito $\mathbb{F}$ de característica $\ell$, y consideramos en $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ la topología de Krull y en $\mathrm{GL}(V)$ la topología discreta. Entonces el núcleo de $\rho$ es de la forma $\ker\rho = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, donde $K$ es una extensión de Galois finita de $\mathbb{Q}$. Por tanto,

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

Es decir, $\rho$ nos proporciona una representación de la imagen $\mathrm{Im}\rho$ como grupo de Galois sobre $\mathbb{Q}$.

Ante esta situación, nos planteamos dos preguntas.

- ¿Cuál es el grupo $\mathrm{Im}\rho$?
- ¿Qué características debe tener $\rho$ para que la extensión $K/\mathbb{Q}$ sea moderadamente ramificada?

En esta tesis consideraremos representaciones de Galois asociadas a curvas elípticas, formas modulares y variedades abelianas. Las

imágenes de estas representaciones han sido estudiadas en profundidad, como veremos más adelante. En cuanto a la segunda pregunta, podemos dar una respuesta en función de los grupos de ramificación superior.

Sea $p$ un número primo, y consideremos el cuerpo de los números $p$-ádicos $\mathbb{Q}_p$. Fijemos una clausura algebraica de $\mathbb{Q}_p$ y una inmersión $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. De este modo tenemos definida una inclusión $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Dentro del grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ podemos considerar el grupo de inercia $I_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{nr}})$ y el grupo de inercia salvaje $I_{p,\mathrm{w}} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{t}})$, donde $\mathbb{Q}_{p,\mathrm{nr}}$ (repectivamente $\mathbb{Q}_{p,\mathrm{t}}$) denotan la máxima extensión de $\mathbb{Q}_p$ no ramificada (respectivamente moderadamente ramificada).

**Lema 2.** *$K/\mathbb{Q}$ es no ramificada (respectivamente moderadamente ramificada) en $p$ si y sólo si $\rho(I_p) = \{\mathrm{Id}\}$ (respectivamente $\rho(I_{p,\mathrm{w}}) = \{\mathrm{Id}\}$).*

Por tanto, tendremos que buscar condiciones que garanticen que para todo primo $p$, $\rho(I_{p,\mathrm{w}})$ es trivial. Veremos que será mucho más fácil conseguir estas condiciones cuando $p$ sea distinto de la característica $\ell$ del cuerpo $\mathbb{F}$. La estrategia que vamos a utilizar, es decir, la construcción de representaciones de Galois de forma que la imagen del grupo de inercia salvaje sea trivial, se engloba en el problema de construir representaciones de Galois con un comportamiento local prefijado, que es en la actualidad un campo muy activo.

## Resultados fundamentales

Esta memoria está dividida en dos partes. El objetivo fundamental de la primera parte es la obtención de realizaciones de grupos lineales 2-dimensionales sobre un cuerpo finito como grupos de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada. En primer lugar, consideramos las representaciones de Galois asociadas a los puntos de $\ell$-torsión de curvas elípticas. El resultado principal que hemos obtenido es el siguiente (véanse los teoremas 1.19 y 1.20).

**Teorema 3.** *Sea $\ell$ un número primo. Existen infinitas curvas elípticas semiestables $E/\mathbb{Q}$ con buena reducción supersingular en $\ell$. La representación de Galois asociada a los puntos de $\ell$-torsión de $E$ da lugar a una realización de $\mathrm{GL}_2(\mathbb{F}_\ell)$ como grupo de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada.*

Además, este resultado es explícito, en el sentido de que damos un algoritmo que nos permite construir estas curvas.

A continuación se consideran las representaciones de Galois asociadas a formas modulares, con el fin de realizar grupos lineales de las familias $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ y $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ para $r \in \mathbb{N}$. Los resultados que hemos obtenido no son tan satisfactorios como en el caso anterior. Al final del Capítulo 2 obtenemos realizaciones de Galois moderadas para algunos de estos grupos (véase la Proposición 2.10).

El objetivo de la segunda parte es la obtención de realizaciones de los grupos lineales de la familia $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Con este propósito, consideramos las representaciones de Galois asociadas a superficies abelianas. El resultado principal de esta parte es el siguiente (ver Teorema 12.25 y Nota 12.27).

**Teorema 4.** *Sea $\ell \geq 5$ un número primo. Existen infinitas curvas $C$ de género 2 tales que la representación de Galois asociada a los puntos de $\ell$-torsión de la Jacobiana de $C$ proporciona una realización de $\mathrm{GSp}_4(\mathbb{F}_\ell)$ como grupo de Galois de una extensión moderadamente ramificada de $\mathbb{Q}$.*

## Contenido de la tesis

Vamos a detenernos en cada uno de los capítulos de esta memoria para resumir su contenido.

### Capítulo 1

En este capítulo estudiamos las representaciones de Galois $\varphi_\ell$ asociadas a los puntos de $\ell$-torsión de curvas elípticas. Nos centramos en dos puntos: la determinación de la imagen de esta representación y la imagen de los grupos de inercia salvaje.

En cuanto al primer punto, J-P. Serre [77] estudia detenidamente la imagen de estas representaciones. Concretamente, demuestra que si $E/\mathbb{Q}$ es una curva elíptica sin multiplicación compleja, entonces la imagen de $\varphi_\ell$ es isomorfa a $\mathrm{GL}_2(\mathbb{F}_\ell)$ salvo para un número finito de primos $\ell$. Combinando este resultado con otros, Mazur [53] prueba que, si $E/\mathbb{Q}$ es una curva elíptica semiestable, entonces la imagen de $\varphi_\ell$ coincide con $\mathrm{GL}_2(\mathbb{F}_\ell)$ siempre que $\ell \geq 11$. Una curva elíptica semistable verifica, además, que la imagen por $\varphi_\ell$ del grupo de inercia salvaje $I_{p,\mathrm{w}}$ es trivial siempre que $\ell \neq p$. Por tanto, lo único que nos falta

es controlar la ramificación en $\ell$. Ahora bien, en [77] Serre demuestra que, si $E$ es una curva elíptica con buena reducción supersingular en $\ell$, entonces $\varphi_\ell(I_{\ell,\mathrm{w}}) = \{\mathrm{Id}\}$.

En resumen, si $E$ es una curva elíptica semiestable definida sobre $\mathbb{Q}$ y $\ell \geq 11$ es un primo tal que $E$ tiene buena reducción supersingular en $\ell$, entonces la representación $\varphi_\ell$ asociada a los puntos de $\ell$-torsión de $E$ da lugar a una representación de $\mathrm{GL}_2(\mathbb{F}_\ell)$ como grupo de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada. El resto del capítulo está dedicado a la construcción de este tipo de curvas. Concretamente, para cada $\ell \geq 11$ construimos infinitas curvas que satisfacen estas condiciones. Uno de los puntos clave en la construcción es hallar, para cada primo $\ell$, una curva elíptica supersingular definida sobre $\mathbb{F}_\ell$, para lo cual utilizamos resultados de J. Brillhart y P. Morton [10] sobre el polinomio de Deuring.

Los primos $\ell = 2, 3, 5, 7$ los tratamos aparte, con razonamientos particulares adaptados para cada caso.

### Capítulo 2

En este capítulo se aborda el estudio de las representaciones de Galois asociadas a formas modulares de peso 2 respecto al grupo $\Gamma_0(N)$. Al igual que en el caso de las curvas elípticas, hay estudios sobre sus imágenes y su comportamiento local.

En primer lugar, realizamos una introducción donde exponemos la construcción clásica, desarrollada por G. Shimura, que a cada forma modular asocia una variedad abeliana definida sobre $\mathbb{Q}$, y, en consecuencia, una representación del grupo de Galois absoluto de $\mathbb{Q}$. Una vez que hemos introducido la representación $\overline{\rho}_{\ell,f}$ asociada a una forma modular $f$ en un primo $\ell$, nos centramos en exponer los resultados ya conocidos relevantes para la resolución de nuestro problema. K. Ribet [69] ha estudiado las imágenes de estas representaciones. Cuando $f$ es una forma modular sin multiplicación compleja ni "inner twists" no triviales, la imagen resulta ser grande salvo para un número finito de primos $\ell$. En este punto encontramos una dificultad, ya que no disponemos de un resultado análogo al resultado de Mazur para curvas elípticas. Sí que existe un algoritmo efectivo que, dada una forma modular, calcula un conjunto finito de primos fuera del cual la imagen de la representación es grande (véase [23]), pero para poder aplicarlo necesitamos una forma modular $f$ concreta, y no puede utilizarse de forma "genérica". Por otra parte, si el nivel $N$ de la forma modular

es libre de cuadrados, entonces la imagen del grupo de inercia salvaje $I_{p,\mathrm{w}}$ es trivial para todo primo $p \neq \ell$. De nuevo, el primo $\ell$ puede abordarse mediante una condición de supersingularidad: si la forma modular $f$ es supersingular, entonces un resultado de Fontaine (cf. [25]) garantiza que la imagen del grupo de inercia salvaje en $\ell$ es trivial. En este punto encontramos otra dificultad, ya que no conocemos un modo de construir formas modulares supersingulares en un primo prefijado $\ell$, que no tengan multiplicación compleja.

No obstante, reuniendo todos los resultados presentados en este capítulo, podemos dar algunos ejemplos de representaciones de grupos de la familia $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ como grupos de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada.

### Capítulo 3

En este capítulo comienza el estudio de las representaciones de Galois asociadas a variedades abelianas, que abarcará el resto de la memoria. Comenzamos introduciendo el objeto fundamental de estudio: dada una variedad abeliana $A$, consideramos la representación de Galois $\rho_\ell$ asociada a los puntos de $\ell$-torsión de $A$. En los primeros capítulos de esta parte, nos ocuparemos de controlar la ramificación de $\rho_\ell$. Concretamente, este capítulo trata la ramificación en los primos $p \neq \ell$. En este sentido, podemos generalizar de forma directa los razonamientos que aplicamos en el caso de curvas elípticas. Un resultado de Grothendieck [31] afirma que si $A$ es una variedad abeliana con reducción semiestable en un primo $p \neq \ell$, entonces la imagen de $I_{p,\mathrm{w}}$ por $\rho_\ell$ es trivial. A fin de definir el concepto de reducción semiestable en una variedad abeliana, recordamos algunos conceptos, como por ejemplo el modelo de Néron.

### Capítulo 4

En este capítulo comenzamos a abordar el problema de obtener un cierto control efectivo sobre la ramificación en $\ell$ de la representación de Galois. Como primera aproximación, tratamos de generalizar los razonamientos que se llevaron a cabo en el caso de curvas elípticas. Con este fin, comenzamos exponiendo con detalle los razonamientos de [77] que conducen a demostrar que una curva elíptica $E$ con buena reducción supersingular en $\ell$ induce una representación de Galois moderadamente ramificada en $\ell$. De este modo, podemos observar que la

ley de grupo formal $F$ asociada a $E$ en $\ell$ constituye un objeto fundamental en todo el razonamiento. Un lema clave estudia la valoración de los puntos de $\ell$-torsión del grupo $F(\overline{\mathfrak{m}})$ asociado a la ley de grupo formal $F$. Así pues, a continuación nos centramos en exponer cómo la noción de ley de grupo formal asociada a una curva elíptica puede generalizarse a variedades abelianas. Pero la ley de grupo formal asociada a una variedad abeliana de dimensión $n$ tiene a su vez dimensión $n$, lo cual nos impide reproducir los mismos razonamientos que en el caso de una curva elíptica (dimensión 1). Para solucionar este problema, introducimos una condición adicional, la Hipótesis 4.7, bajo la cual somos capaces de probar que la imagen de $I_{\ell,\mathrm{w}}$ por la representación $\rho_\ell$ es trivial. Nuestro objetivo en los próximos capítulos es obtener algunas condiciones de naturaleza explícita que nos permitan asegurar que la Hipótesis 4.7 se satisface.

### Capítulo 5

Este capítulo estudia el concepto de altura de una ley de grupo formal, que será necesario en los razonamientos que aparecen en capítulos posteriores. Exponemos la definición general tal y como aparece en [34], así como un rápido esquema sobre cómo se calcula en casos concretos. A continuación comparamos esta definición en la Proposición 5.12 con aquella, más simple, que se utiliza en el caso de dimensión 1. Esta proposición será clave en el razonamiento, ya que relaciona las propiedades que se utilizan en dimensión 1 para demostrar el resultado que buscamos con la definición general de altura.

### Capítulo 6

En este capítulo nos detenemos para reflexionar sobre los resultados que hemos obtenido hasta el momento y enunciar un resultado de carácter general sobre la ramificación de la representación asociada a los puntos de $\ell$-torsión de una variedad abeliana. Denotemos por $\mathbb{Q}(A[\ell])$ a la extensión de Galois finita de $\mathbb{Q}$ que se obtiene adjuntando las coordenadas de los puntos de $\ell$-torsión de $A$. El resultado más destacado es el siguiente.

**Teorema 5.** *Sea $A/\mathbb{Q}$ una variedad abeliana de dimensión $n$. Sea $\ell > 2$ un número primo, y $\mathcal{P}$ el conjunto de los primos que dividen al orden de $\mathrm{GL}_{2n}(\mathbb{F}_\ell)$. Supongamos que se verifican las siguientes condiciones:*

- *Para todo $p \in \mathcal{P}$ distinto de $\ell$, $A$ tiene reducción semiestable en $p$.*
- *$A$ tiene buena reducción supersingular en $\ell$ y la ley de grupo formal asociada a $A$ en $\ell$ satisface la Hipótesis 4.7.*

*Entonces la extensión de Galois $\mathbb{Q}(A[\ell])/\mathbb{Q}$ es moderadamente ramificada.*

### Capítulo 7

A partir de este capítulo, nos centramos en el caso en que $A$ es una superficie abeliana (es decir, la dimensión $n$ es 2). También supondremos a partir de ahora que la altura de la ley de grupo formal asociada a $A$ en $\ell$ es 4. Si $A$ es una superficie abeliana con buena reducción supersingular en $\ell$, esta última condición se verifica automáticamente.

El objetivo de este capítulo es introducir un tipo de ley de grupo formal, que denominamos simétrica, y demostrar que, si una ley de grupo formal simétrica satisface que el exponente $r$ que aparecen en la Proposición 5.12 es 2, entonces la Hipótesis 4.7 se verifica. Tanto la simetría como la condición sobre el exponente $r$ son condiciones que pueden leerse de forma directa en la expresión de la ley de grupo formal de $A$, es decir, tienen un carácter explícito, al contrario que la Hipótesis 4.7. Los resultados de este capítulo se basan en un par de lemas técnicos (7.5 y 7.6) que generalizan, dentro del contexto en que nos encontramos, el lema clave que se utilizó en el caso de curvas elípticas.

### Capítulo 8

En este capítulo tratamos de encontrar ejemplos de superficies abelianas que verifiquen las dos condiciones que aparecen en el capítulo anterior, es decir, de forma que la ley de grupo formal asociada sea simétrica y el exponente de la Proposición 5.12 sea 2. Para hallar estos ejemplos, consideraremos las superficies abelianas que se obtienen como Jacobianas de curvas de género 2.

La primera condición se verificará siempre que la correspondiente curva de género 2 sea simétrica (Definición 8.3). Para demostrar este hecho, necesitaremos probar un resultado (el Teorema 8.2). La demostración de este teorema utiliza el algoritmo explícito de cálculo de la ley de grupo formal asociado a la Jacobiana de una curva de género

2 que aparece en el Capítulo 7 de [15]. En esta demostración se utiliza un modelo explícito de la Jacobiana sumergida en un espacio proyectivo de dimensión 15. Las ecuaciones que lo definen se encuentran en la página web de V. Flynn, pero las hemos incluido en el Apéndice A para evitar confusiones.

Finalmente, centraremos nuestra atención en las curvas bielípticas, con el fin de encontrar curvas de género 2 simétricas de forma que, además, el exponente de la Proposición 5.12 de la ley de grupo formal asociada a la Jacobiana de la curva sea 2.

### Capítulo 9

De nuevo, consideramos conveniente dedicar un capítulo a reflexionar sobre los resultados obtenidos hasta el momento y enunciar de forma clara los teoremas fundamentales. Los resultados explícitos que se han obtenido en los dos capítulos anteriores nos permiten escribir el siguiente teorema.

**Teorema 6.** *Sea $C$ una curva de género 2 definida por una ecuación hiperelíptica de la forma*

$$y^2 = f(x), \tag{12.1}$$

*donde $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}[x]$ es un polinomio de grado 6 sin factores múltiples. Sea $\ell > 2$ un primo y $\mathcal{P}$ el conjunto de los primos que dividen al orden de $\mathrm{GL}_4(\mathbb{F}_\ell)$. Supongamos que se verifican las siguientes condiciones:*

- *Para $p \in \mathcal{P}$ distinto de $\ell$, $C$ tiene reducción estable en $p$.*
- *La reducción de $f(x)$ módulo $\ell$ es de la forma $x^6+bx^4+bx^2+1$, y la curva elíptica definida sobre $\mathbb{F}_\ell$ por $y^2 = x^3 + bx^2 + bx + 1$ es supersingular.*

*Entonces la extensión de Galois $\mathbb{Q}(A[\ell])/\mathbb{Q}$ es moderadamente ramificada.*

### Capítulo 10

El teorema que presentamos en el capítulo anterior, aunque aparentemente muy satisfactorio, esconde una dificultad esencial que nos impide utilizarlo para nuestros propósitos. La razón es la siguiente: la imagen de la representación de Galois asociada a la Jacobiana de

una curva de género 2 dada por una ecuación de la forma (12.1) con $f(x) = f_0x^6+f_1x^5+f_2x^4+f_3x^3+f_2x^2+f_1x+f_0$ no es grande. Es decir, esta representación no dará lugar a una realización del grupo $\mathrm{GSp}_4(\mathbb{F}_\ell)$ como grupo de Galois, sino de un subgrupo propio. Por tanto, necesitamos dar unas condiciones que garanticen que la representación $\rho_\ell$ es moderadamente ramificada, pero que sean lo suficientemente débiles como para permitir que la imagen de $\rho_\ell$ sea grande. Es decir, tenemos que suavizar las condiciones del Teorema 6.

Para esto utilizaremos algunos resultados de [9] que relacionan la proximidad de las soluciones de dos sistemas de ecuaciones $\{f_1 = 0, f_2 = 0\}$ y $\{g_1 = 0, g_2 = 0\}$, donde $f_1, f_2, g_1, g_2 \in \mathbb{Z}_\ell[[X_1, X_2]]$, con la proximidad de los coeficientes de $f_i$ y $g_i$. La medida de esta proximidad se realiza mediante la valoración $\ell$-ádica. Este capítulo cierra el estudio de la ramificación de la representación $\rho_\ell$.

### Capítulo 11

En este capítulo se estudia la imagen de la representación de Galois $\rho_\ell$ asociada a una superficie abeliana, con especial énfasis en el caso en que esta superficie es la Jacobiana de una curva de género 2.

Serre (cf. Teorema 3 de *Lettre a Marie-France Vignéras* en [82]) generaliza al contexto general de variedades abelianas el resultado de [77] sobre la imagen de la representación $\varphi_\ell$ asociada a los puntos de $\ell$-torsión de una curva elíptica. Concretamente, demuestra que si $A$ es una variedad abeliana definida sobre $\mathbb{Q}$ de dimensión $n$ impar, o bien igual a 2 ó 6, principalmente polarizada, cuyo anillo de endomorfismos coincide con $\mathbb{Z}$, entonces la imagen de la representación de Galois $\rho_\ell$ asociada a los puntos de $\ell$-torsión de $A$ es isomorfa al grupo general simpléctico $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$.

En el caso en que la variedad abeliana tenga dimensión 2, hay resultados explícitos que permiten determinar si la imagen de $\rho_\ell$ es isomorfa a $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (véanse [44] y [24]).

En una primera aproximación, adaptamos los resultados de P. Le Duff [44] a nuestros propósitos, y logramos construir, para cada $\ell \geq 5$, curvas de género 2 de forma que la representación de Galois asociada a los puntos de $\ell$-torsión de su Jacobiana tiene imagen grande. Sin embargo, esta construcción depende de una conjetura no demostrada (Conjetura F de [33]). Más adelante, siguiendo una sugerencia de L. Dieulefait, conseguimos dar otra construcción que no depende de esta conjetura.

En esencia, el resultado de Le Duff se basaba en la siguiente proposición.

**Proposición 7.** *El grupo simpléctico* $\mathrm{Sp}_4(\mathbb{F}_\ell)$ *está generado por una transvección y un elemento con polinomio característico irreducible.*

Imponer que la imagen de $\rho_\ell$ contenga una transvección es relativamente sencillo utilizando la relación entre la fibra especial del modelo de Néron en un primo $p \neq \ell$ y el tipo de reducción de la curva $C$ (véanse la Proposición 11.4 y el Lema 11.5). Por otra parte, Le Duff aborda la segunda condición pidiendo la existencia de un primo $q$, de buena reducción en $A$, de forma que el polinomio característico de la imagen del elemento de Frobenius $\mathrm{Frob}_q$ por $\rho_\ell$ sea irreducible. Es en este punto donde necesitamos refinar la condición de Le Duff. Nosotros pediremos la existencia de dos primos auxiliares, $q_1$ y $q_2$, de forma que sus polinomios característicos tengan un tipo concreto de factorización sobre $\mathbb{F}_\ell$. El resultado final es el siguiente (ver Teorema 11.11).

**Teorema 8.** *Sea $C$ una curva de género 2 definida sobre $\mathbb{Q}$ con reducción estable de tipo $(II)$ o $(VI)$ en un primo $p$. Sea $c$ el orden del grupo de las componentes conexas de la fibra especial del modelo de Néron en $p$. Sean $q_1$ y $q_2$ primos diferentes de forma que $C$ tiene buena reducción en ellos. Llamemos $P_i(X) = X^4 + a_i X^3 + b_i X^2 + a_i q_i X + {q_i}^2$ al polinomio característico del endomorfismo de Frobenius actuando sobre la reducción de $C$ en $q_i$, y definamos $\Delta_0(P_i) = a_i^2 - 4b_i + 8q_i$, $i = 1, 2$.*

*Supongamos que $\ell > 2$ es un primo que no divide a $2pq_1q_2c$ y satisface*

- $q_i \equiv 1 \pmod{\ell}$, $i = 1, 2$.
- $\Delta_0(P_1)$ *no es un cuadrado en* $\mathbb{F}_\ell$ *y* $a_1 \not\equiv 0 \pmod{\ell}$.
- $\Delta_0(P_2)$ *es un cuadrado no nulo en* $\mathbb{F}_\ell$*, y* $P_2(X)$ *no descompone en factores lineales en* $\mathbb{F}_\ell$.

*Entonces la imagen de $\rho_\ell$ coincide con* $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

### Capítulo 12

En este capítulo recogemos los resultados fundamentales de los capítulos anteriores y, utilizándolos como punto base, realizamos una

construcción explícita de curvas de género 2 que proporcionan realizaciones de $\mathrm{GSp}_4(\mathbb{F}_\ell)$ como grupo de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada. El capítulo está dividido en una serie de secciones que tratan las distintas construcciones que se requieren para llegar al resultado final.

Comenzamos exponiendo una construcción que garantiza que, en un primo $p \neq \ell$ dado, la curva $C$ de género 2 tiene buena reducción en $p$. A continuación nos centramos en la construcción de superficies abelianas supersingulares. Esta construcción, que utiliza curvas bielípticas, descansa sobre los resultados obtenidos en el Capítulo 1 sobre curvas elípticas supersingulares. A continuación se consideran los primos auxiliares que aparecen en el Teorema 8, es decir, $p$, $q_1$ y $q_2$, necesarios para garantizar que la imagen de la representación de Galois es suficientemente grande. Concretamente, tomamos como primo auxiliar $p = 5$, y, estudiando los invariantes de Igusa en un caso concreto, obtenemos una construcción general. En cuanto a los primos $q_1$ y $q_2$, proponemos un modo concreto y explícito de escogerlos, en función del primo $\ell$ de partida.

Finalmente, recogemos todos estos resultados en un teorema fundamental (Teorema 12.25). Dado un primo $\ell \geq 7$, este teorema afirma que cualquier curva $C$ de género 2 definida mediante una ecuación hiperelíptica $y^2 = f(x)$, donde $f(x) = f_6x^6+f_5x^5+f_4x^4+f_3x^3+f_2x^2+f_1x + f_0 \in \mathbb{Z}[x]$ es un polinomio de grado 6 sin factores múltiples, de forma que sus coeficientes satisfacen unas ciertas congruencias módulo algunas potencias de primos (concretamente, $2^4, 3, 5^2, \ell^4$, los primos auxiliares $q_1$ y $q_2$, y los primos que dividen al orden de $\mathrm{GSp}_4(\mathbb{F}_\ell)$), proporciona una realización de $\mathrm{GSp}_4(\mathbb{F}_\ell)$ como grupo de Galois de una extensión de $\mathbb{Q}$ moderadamente ramificada. Más aún, es fácil calcular infinitas curvas $C$ que satisfacen estas condiciones.

Tras considerar brevemente el caso $\ell = 5$, el capítulo concluye con unos ejemplos donde se utiliza el resultado fundamental para construir curvas de género 2 que proporcionen realizaciones moderadas de $\mathrm{GSp}_4(\mathbb{F}_\ell)$ para $\ell = 7, 11$.

# Bibliography


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

[3] Atiyah, M. F., Macdonald, I. G. *Introduction to Commutative Algebra*. Addison-Wesley, (1969).

[4] Auer, R., Top, J. *Legendre elliptic curves over finite fields*, J. Number Theory **95**, no. 2, pages 303–312 (2002).

[5] Becker, T. *Standard bases and some computations in rings of power series*. J. Symbolic Comput. **10** (1990), no. 2, pages 165–178.

[6] Bendel, C. P., Friedlander, E. M., Suslin, A. *Infinitesimal 1-parameter subgroups and cohomology*. J. Amer. Math. Soc. **10** (1997), no. 3, pages 693–728.

[7] 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).

[8] Bosch, S., Lütkebohmert, W., Raynaud, M. *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge·Band 21, Springer-Verlag (1990).

[9] Bourbaki, Nicolas *Èléments de mathématique. Fascicule XXVIII. Algèbre commutative*. Actualités Scientifiques et Industrielles, No. 1293 Hermann, Paris (1961).

[10] 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).

[11] Bröker, R. *Constructing supersingular elliptic curves*, to appear in Journal of Combinatorics and Number Theory.

[12] Brumer, A., Kramer, K. *The conductor of an abelian variety.* Compositio Math. **92** (1994), no. 2, pages 227–248.

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

[14] Carlitz, L. *Congruence properties of special elliptic functions.* Monatsh. Math. **58**, pages 77–90 (1954).

[15] 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).

[16] Childs, L. *A concrete introduction to higher algebra*, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg (1979).

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

[18] Cremona, J. E. *Algorithms for modular elliptic curves*, Cambridge Univ. Press (1992).

[19] Darmon, H., Diamond, F., Taylor, R. *Fermat's Last Theorem*, Current Developments in Mathematics 1, (1995), International Press, pages. 1–157. Reprinted in *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), pages 2–140, International Press, Cambridge, MA, (1997).

[20] Deligne, P. *Formes modulaires et représentations $\ell$-adiques*, Lecture Notes in Mathematics **179**, Springer (1971), pages 136–172.

[21] Deligne, P., Serre, J-P. *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. **7** (1974), pages 507–530.

[22] Diamond, F., Shurman, J. *A First Course in Modular Forms*. Graduate Texts in Mathematics 228, Springer-Verlag (2005).

[23] 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.

[24] 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).

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

[26] Eisenträger, K., Lauter, K. *A CRT algorithm for constructing genus* 2 *curves over finite fields*, math.NT/0405305, available at

`http://arxiv.org/PS_cache/math/pdf/0405/0405305v2.pdf`

[27] Elkies, N. D., *The existence of infinitely many supersingular primes for every elliptic curve over Q*. Invent. Math. **89**, no. 3, pages 561–567 (1987).

[28] 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.

[29] Fröhlich, A. *Formal Groups*, Lecture Notes in Math. 74, Berlin Heildelberg New York, Springer (1968).

[30] van der Geer, G., Moonen, B. *Abelian Varieties* (University of Amsterdam). Available at

`http://staff.science.uva.nl/ bmoonen/boek/BookAV.html`

[31] 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).

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

[33] Hardy, G. H., Littlewood, J. E. *Some problems of "partitio numerorum"; III: on the expression of a number as a sum of primes*, Acta Mathematica **44**, pages 1–70 (1923).

[34] Hazewinkel, M. *Formal Groups and Applications*. Academic Press (1978).

[35] Hilbert, D. *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. **110** (1892), pages 104–129.

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

[37] Howe, E. W., Leprévost, F., Poonen, B. *Large torsion subgroups of split Jacobians of curves of genus two or three*. Forum Math. **12** (2000), no. 3, pages 315–364.

[38] Ibukiyama, T., Katsura, T., Oort, F. *Supersingular curves of genus two and class numbers*. Compositio Math. **57** (1986), no. 2, pages 127–152.

[39] Katz, N. M., Mazur, B. *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N. J. (1985).

[40] Kawamura, T. *The effective surjectivity of mod $\ell$ Galois representations of* 1- *and* 2*-dimensional abelian varieties with trivial endomorphism ring*. Comment. Math. Helv. **78** (2003), no. 3, pages 486–493.

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

[42] Lang, S. *Abelian Varieties*. Interscience Tracts in Pure and Applied Mathematics **7**; Interscience Publishers, Inc. (1959).

[43] Lang, S. *Number Theory III: Diophantine Geometry*, Encyclopedia of Math. Sciences vol. 60, Springer-Verlag, (1991).

[44] Le Duff, Pierre *Représentations galoisiennes associées aux points d'ordre $\ell$ des jacobiennes de certaines courbes de genre* 2. Bull. Soc. Math. France **126**, no. 4, pages 507–524 (1998).

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

[46] Liu, Q. *Conducteur et discriminant minimal de courbes de genre* 2. Compositio Math. **94** (1994), no. 1, pages 51–79.

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

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

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

[50] Maisner, D., Nart, E. *Abelian Surfaces over Finite Fields as Jacobians*, Experimental Mathematics **11**, 3, pages 321–337 (2001).

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

[52] Masser, D. W., Wüstholz, G. *Galois properties of division fields of elliptic curves*. Bull. London Math. Soc. **25** (1993), no. 3, pages 247–254.

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

[54] Mestre, J-F. *Construction de courbes de genre* 2 *à partir de leurs modules*. In Mora, T. and Traverso, C., editors, *Effective methods in algebraic geometry*, volume **94** of Progr. Math., pages 313–334. Birkhäuser, (1991). Proc. Congress in Livorno, Italy, April 17–21, 1990.

[55] Milne, J. S., *Abelian varieties*. Version 2.0, March 16, 2008. Available at

`www.jmilne.org/math/`

[56] Mumford, D. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics, Bombay. Oxford University Press (1974).

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

[58] Neukirch, J. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften, Vol. 322, Springer-Verlag (1999).

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

[60] Oort, F., Li, K-Z. *Moduli of Supersingular Abelian Varieties*. Lecture Notes in Mathematics 1680, Springer (1998).

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

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

[63] 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).

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

[65] 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).

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

[67] Ribet, K. A. *Galois representations attached to eigenforms with Nebentypus*. Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pages 17–51. Lecture Notes in Math., Vol. **601**, Springer, Berlin, (1977).

[68] Ribet, K. A. *Twists of modular forms and endomorphisms of abelian varieties*. Math. Ann. **253** (1980), no. 1, pages 43–62.

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

[70] 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.

[71] Robert, A. M. *A Course in p-adic Analysis*, Springer Verlag, New York, (2000).

[72] Rosenlicht, M. *Some basic theorems on algebraic groups*. Amer. J. Math. **78** (1956), pages 401–443.

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

[74] Serre, J-P. *Groupes de Lie $\ell$-Adiques Attachés aux Courbes Elliptiques*, Colloque de Clermont-Ferrand, IHES (1964).

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

[76] Serre, J-P. *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisou-Poitou. Théorie des nombres, tome 11, $n°2$ (1969-1970), exp. $n°19$, pages 1–15.

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

[78] Serre, J-P. *Œuvres*, Vol. III. 1972–1984 Springer-Verlag, Berlin, (1986).

[79] 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.

[80] Serre, J-P. *Abelian $\ell$-Adic Representations and Elliptic Curves*, Addison Wesley Publishing Company (1989).

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

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

[83] Shimura, G. *A reciprocity law in non-solvable extensions*. J. Reine Angew. Math. **221** (1966) pages 209–220.

[84] Silverman, J. *The Arithmetic of Elliptic Curves*, Graduate texts in mathematics 106, Springer (1986).

[85] Stark, H. M. *An Introduction to Number Theory*, Cambridge (Mass.), MIT Press (1991).

[86] M. Stoll, *Genus* 2 *curves with small odd discriminant*, available at

`http://www.faculty.iu-bremen.de/stoll/data/`

[87] Tate, J. T. *p-divisible groups*. 1967 Proc. Conf. Local Fields (Driebergen, 1966) pages 158–183, Springer, Berlin.

[88] Waterhouse, W. *Introduction to Affine Group Schemes*. Graduate Texts in Mathematics, Vol. 66 Springer-Verlag (1979).

[89] Weber, H. *Lehrbuch der Algebra III*, Vieweg, Braunschweig, (1908).

[90] Weinstein, J. PhD thesis: *Automorphic representations with local constraints*, University of California, Berkeley, Spring 2007.