

**A Thesis Submitted for the Degree of PhD at the University of Warwick**

**Permanent WRAP URL:**

<http://wrap.warwick.ac.uk/94788>

**Copyright and reuse:**

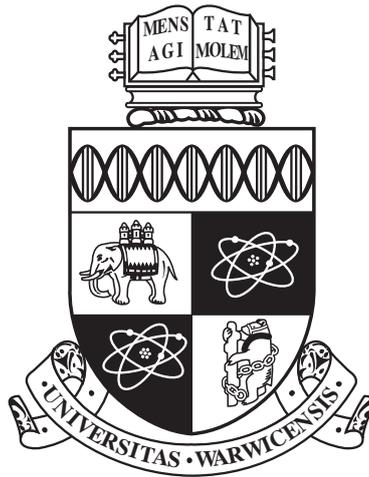
This thesis is made available online and is protected by original copyright.

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it.

Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: [wrap@warwick.ac.uk](mailto:wrap@warwick.ac.uk)



# Residual Representations of Abelian Varieties

by

**Pedro João Macedo Duarte Lemos**

**Thesis**

Submitted to the University of Warwick

for the degree of

**Doctor of Philosophy**

**Mathematics Institute**

April 2017

THE UNIVERSITY OF  
**WARWICK**

# Contents

<b>Acknowledgments</b>	<b>ii</b>
<b>Declarations</b>	<b>iii</b>
<b>Abstract</b>	<b>iv</b>
<b>Chapter 1 Representations of Semistable Abelian Varieties</b>	<b>1</b>
1.1 Symplectic Vector Spaces . . . . .	3
1.2 The Picard Group of an Abelian Variety . . . . .	5
1.3 The Dual of an Abelian Variety . . . . .	7
1.4 Polarized Abelian Varieties . . . . .	9
1.5 Fundamental Characters and a Theorem of Raynaud . . . . .	11
1.6 Néron Models . . . . .	14
1.7 Residual Representations of Semistable Principally Polarized Abelian Varieties . . . . .	15
1.8 Semistable Abelian Threefolds . . . . .	19
1.9 An Application . . . . .	26
<b>Chapter 2 Serre's Uniformity Conjecture</b>	<b>29</b>
2.1 Subgroups of $GL_2(\mathbb{F}_p)$ . . . . .	32
2.2 The Modular Curve $X_{0,ns}^+(r,p)$ . . . . .	33
2.3 Chen's Isogeny . . . . .	35
2.4 Formal Immersions . . . . .	39
2.5 Integrality of $j$ -invariant . . . . .	43
2.6 Proof of the main theorem . . . . .	45

# Acknowledgments

I would like to start by thanking my family — in particular my grandparents, parents and brother — for their constant support and encouragement, without which it would have not been possible for me to have come this far.

I want to acknowledge next all of my friends who accompanied me through these last four year and who made my time at Warwick both enjoyable and worthwhile. I must express my special gratitude to Samuele Anni, Chris Birkbeck, Matthew Bisatt, Florian Bouyer, Jamie Foronda, Céline Maistret, Vandita Patel, Matthew Spencer, Alex Torzewski, Gareth Tracey, George Turcas and Chris Williams for the mathematical discussions I had with some, the political arguments I had with others, and the fun moments I had with all of them. I would also like to thank Ana Beatriz, Ana Rita, António and Daniel, who, knowing me since I was a kid, have patiently put up with me all these years.

Finally, my greatest and most special “thank you” goes to my supervisor, Samir Siksek, who, with all his patience and brilliance, guided me through the dark wood that, sometimes, mathematics seems to be. The discussions we had and his shrewd insight were essential ingredients in the work I did during my PhD. I am perfectly convinced that I could hardly have had a better supervisor. Thank you very much!

# Declarations

The first chapter of this thesis is an extended version of [ALS16], a joint work of Samuele Anni, Samir Siksek and myself. Sections 1.1 to 1.6 are intended to provide the necessary background to the paper. As such, the results in these sections are not new: the source for sections 1.2 through 1.4 is [Mil86]; section 1.5 is based upon [Ser71] and a theorem by Raynaud [Ray74]; the results in section 1.6 can be found in [BLR90] and [ST68]. Unless otherwise stated, the results in the remainder of the chapter are a product of the collaboration among Samuele Anni, Samir Siksek and myself, which culminated in the article [ALS16] aforementioned.

The second chapter is an extended version of [Lem17]. As in the case above, I start the chapter with a few background sections: section 2.1 is concerned with Dixon's classification of maximal subgroups of  $\mathrm{GL}_2(\mathbb{F}_p)$ , and a proof of his result can be found in [Ser71]; sections 2.2 to 2.4 are based on [DM97]. The results in the remainder of the chapter (sections 2.5 and 2.6), unless otherwise stated, consist of original material and are a product of my own research.

# Abstract

This thesis is divided in two parts, corresponding to two papers in which I collaborated during the course of my PhD studies. Both of these parts are concerned with the question of surjectivity of residual Galois representations arising from abelian varieties defined over  $\mathbb{Q}$ . At the start of each chapter, a full introduction to the topic covered is provided.

In the first chapter, we prove the following theorem:

**Theorem.** Let  $A$  be a semistable principally polarized abelian variety of dimension  $d \geq 1$  over  $\mathbb{Q}$ . Let  $\ell \geq \max(5, d + 2)$  be a prime. Suppose that the image of

$$\bar{\rho}_{A,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GSp}_{2d}(\mathbb{F}_{\ell})$$

contains a transvection. Then  $\bar{\rho}_{A,\ell}$  is either reducible or surjective.

With this result in hand, we use it to study the surjectivity of the residual Galois representations modulo different primes of a specific abelian threefold. We are able to show the following:

**Proposition.** Let  $C/\mathbb{Q}$  be the genus 3 hyperelliptic curve

$$y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5,$$

and let  $J$  denote its Jacobian. Let  $\ell \geq 3$  be a prime. Then  $\bar{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_{\ell})$ .

In the second chapter, we prove the following special case of Serre's uniformity conjecture:

**Theorem.** Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $\text{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$ . Suppose, moreover, that  $E$  admits a non-trivial cyclic  $\mathbb{Q}$ -isogeny. Then, for  $p > 37$ , the residual mod  $p$  Galois representation  $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_p)$  is surjective.

# Chapter 1

## Representations of Semistable Abelian Varieties

In his 1972 paper [Ser71], Jean-Pierre Serre proved that, given an elliptic curve over a field  $K$  without complex multiplication over  $\bar{K}$ , the image of its mod  $\ell$  Galois representation is  $\mathrm{GL}_2(\mathbb{F}_\ell)$  for almost all primes  $\ell$ . The case of semistable elliptic curves over  $\mathbb{Q}$  is shown to be particularly easy to treat, and an explicit upper bound for the primes  $\ell$  for which  $\bar{\rho}_{E,\ell}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$  can be determined in this case. More precisely,

**Theorem 1** ([Ser71, Corollaire 1]). *Let  $E$  be a semistable elliptic curve over  $\mathbb{Q}$  and  $p$  the smallest prime number for which  $E$  has good reduction. Then, for every prime  $\ell > \#\tilde{E}(\mathbb{F}_p)$ , where  $\tilde{E}$  is the reduction of  $E$  mod  $p$ , we have  $\bar{\rho}_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_\ell)$ .*

Actually, in this case of semistable elliptic curves over  $\mathbb{Q}$ , much more is known. Indeed, using Mazur's description of  $X_0(\ell)(\mathbb{Q})$  ( $\ell$  prime) [MG78] and [Ser71, Proposition 21], we are able to conclude the following:

**Theorem 2** ([MG78, Theorem 4]). *Let  $E$  be a semistable elliptic curve over  $\mathbb{Q}$  and  $\ell \geq 11$  a prime number. Then the image of  $\bar{\rho}_{E,\ell}$  is  $\mathrm{GL}_2(\mathbb{F}_\ell)$ .*

Much more recently, in 2011, Chris Hall [Hal11] extended the famous surjectivity result by Serre to a certain class of higher dimensional abelian varieties.

**Theorem 3** ([Hal11, Theorem 1]). *Let  $A$  be a  $d$ -dimensional polarized abelian variety over a number field  $K$  without complex multiplication over  $\bar{K}$ . Suppose, moreover, that there exists a finite extension  $L/K$  such that the Néron model of  $A$  over  $\mathcal{O}_L$  has a semistable fibre with toric dimension 1. Then  $\bar{\rho}_{A,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$  for almost every prime  $\ell$ , where  $\bar{\rho}_{A,\ell}$  is the mod  $\ell$  Galois representation of  $A$ .*

One interesting question that one could ask oneself is if it is true that, for every prime  $\ell$  and every positive integer  $d$ ,  $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$  is a Galois group over  $\mathbb{Q}$ . As remarked in [AdRDW16], Hilbert’s irreducibility theorem can be used to give a positive answer to this question. However, it would be interesting to give examples of abelian varieties whose images of their mod  $\ell$  residual Galois representations are  $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$  for  $\ell$  larger than some “small” constant. Hall’s theorem above yields that, given an abelian variety  $A$  over  $K$  without complex multiplication over  $\bar{K}$ , there is a constant  $C$  for which  $\bar{\rho}_{A,\ell}$  surjects onto  $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$  for every prime  $\ell > C$ ; it does not, however, give us an estimation of  $C$ .

Already in 1998, some work was done towards this by Pierre Le Duff [LD98]. In his paper, he was able to conclude that, for  $2 < \ell < 500000$ ,  $\mathrm{GSp}_4(\mathbb{F}_\ell)$  is, in fact, realisable as the image of residual Galois representations of a single abelian variety. Building on his work, a 2014 joint work by Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas and Núria Vila [AdRAK<sup>+</sup>15] showed that the same happens with  $\mathrm{GSp}_6(\mathbb{F}_\ell)$  for every prime  $\ell$  in the interval  $[11, 500000]$ .

In this chapter, we will prove the following result:

**Theorem 4.** *Let  $A$  be a semistable principally polarized abelian variety of dimension  $d \geq 1$  over  $\mathbb{Q}$ . Let  $\ell \geq \max(5, d + 2)$  be a prime. Suppose that the image of*

$$\bar{\rho}_{A,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$$

*contains a transvection. Then  $\bar{\rho}_{A,\ell}$  is either reducible or surjective.*

A unipotent invertible linear map  $\varphi : \mathbb{F}_\ell^n \rightarrow \mathbb{F}_\ell^n$  is called a *transvection* if the linear map  $\varphi - \mathrm{Id}_n$  has rank 1.

After that, we will use this result to show that the image of the Galois representation associated to the Jacobian of the curve

$$C : y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5$$

is  $\mathrm{GSp}_6(\mathbb{F}_\ell)$  for every  $\ell \geq 3$ . We should here reference the work of David Zywina [Zyw15], where, independently, he gives an example of a plane quartic curve over  $\mathbb{Q}$  of genus 3 for which the Galois representation  $\rho_J : G_{\mathbb{Q}} \rightarrow \mathrm{GSp}_6(\hat{\mathbb{Z}})$  arising from the Galois action on the torsion points of its Jacobian  $J$  is surjective.

**Notation.** If  $A$  is an abelian variety, we will denote by  $m : A \times A \rightarrow A$  the associated operation morphism, by  $p : A \times A \rightarrow A$  the projection to the first coordinate, and by  $q : A \times A \rightarrow A$  the projection to the second coordinate. Throughout, whenever  $K$  is a number field, and  $v$  is a finite place of  $K$ , we will often write  $D_v \subseteq G_K := \text{Gal}(\bar{K}/K)$  for a decomposition subgroup over  $v$ ,  $I_v$  for the inertia subgroup of  $D_v$ , and  $I_v^w$  for the wild inertia subgroup of  $I_v$ . The tame inertia group, which is defined as the quotient  $I_v/I_v^w$ , will be denoted by  $I_v^t$ .

## 1.1 Symplectic Vector Spaces

Let  $V$  be a  $d$ -dimensional vector space over a field  $k$ . A bilinear pairing  $\langle \cdot, \cdot \rangle : V \times V \rightarrow k$  is said to be *symplectic* if it is alternating and non-degenerate. A vector space  $V$  equipped with such a pairing is called a *symplectic vector space*.

If  $(V, \langle \cdot, \cdot \rangle)$  is a symplectic vector space, a linear map  $L$  is *symplectic* if

$$\langle Lv, Lw \rangle = \langle v, w \rangle$$

for every  $v, w \in V$ . The group of symplectic invertible linear maps on  $V$  is denoted by  $\text{Sp}(V)$ . We define the *general symplectic group* on  $V$  as follows:

$$\text{GSp}(V) := \{L \in \text{GL}(V) : \text{for } v, w \in V, \exists c_L \in k^\times \text{ such that } \langle Lv, Lw \rangle = c_L \langle v, w \rangle\}.$$

It is evident that the map  $c : \text{GSp}(V) \rightarrow k^\times$  given by  $L \mapsto c_L$  is a homomorphism. We call  $c$  the *character of the symplectic pairing*.

**Proposition 5.** *Let  $(V, \langle \cdot, \cdot \rangle)$  be a symplectic vector space of dimension  $d$ . Then  $d$  is even.*

*Proof.* We may assume that  $V \neq 0$ . We will prove that if  $d$  is odd, then it is not possible to define a symplectic pairing on  $V$ . We proceed by induction.

If  $d = 1$ , then the result is evident, as the only possible alternating pairing is the trivial one, which is degenerate.

Let now  $d \geq 3$  be an odd integer, and suppose that the result was proved for  $d-2$ . Suppose, for the sake of contradiction, that it is possible to define a symplectic pairing on  $V$ . Let  $v \in V$  be a non-zero vector. Since the pairing is non-degenerate,



**Proposition 7.** *Let  $V$  be a symplectic vector space of dimension  $2d$ , and  $c$  the character associated to the symplectic pairing. Then, if  $L$  is an element of  $\mathrm{GSp}(V)$ , its determinant is  $c(L)^d$ .*

*Proof.* Choose a symplectic basis as in Proposition 6. Let  $M$  be the matrix of  $L$  with respect to this basis, and let  $G$  be the Gram matrix of the pairing with respect to this basis as well. We have just seen what  $G$  looks like. In particular,  $\det G = 1$ . Consider the matrix  $M' := \sqrt{c(L)}^{-1}M$ , defined over a quadratic extension of our base field  $k$ . The matrix  $M$  must satisfy

$$M^T G M = c(L)G.$$

Therefore,  $M'$  satisfies

$$M'^T G M' = G.$$

In other words,  $M'$  is a symplectic matrix. It is straightforward to conclude, just by taking determinants, that  $\det(M') = \pm 1$ . However, the proof that symplectic matrices have determinant 1 is more elaborated. We refer to [Art88, Theorem 3.25] for a proof of this fact.

Knowing that the determinant of a symplectic matrix is 1, it is now easy to finish the proof of our result:  $1 = \det(M') = \det(\sqrt{c(L)}^{-1}M)$  yields  $\det(M) = c(L)^d$ , as we wanted.  $\square$

## 1.2 The Picard Group of an Abelian Variety

Let  $X$  be a scheme. As a set, the *Picard group*  $\mathrm{Pic}(X)$  of  $X$  is defined to be the set of isomorphism classes of invertible sheaves on  $X$ ; the group structure is then obtained by defining the product of two classes  $[\mathcal{L}]$ ,  $[\mathcal{L}']$  of invertible sheaves to be the class  $[\mathcal{L} \otimes \mathcal{L}']$ . If  $A$  is an abelian variety over a field  $k$  — which, for simplicity, we will always assume to be perfect —, then it follows from the theorem of the square [Mil86, Theorem 6.7] that, for each  $k$ -scheme  $T$ , the map

$$\varphi_{\mathcal{L},T} : A(T) \rightarrow \mathrm{Pic}(A_T), \quad a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

is a homomorphism. The functor

$$K_{\mathcal{L}} : \mathbf{Sch}^{\mathrm{op}}/k \rightarrow \mathbf{Set}, \quad T \mapsto \ker \varphi_{\mathcal{L},T}$$

is representable, and its representing scheme will also be denoted by  $K_{\mathcal{L}}$ . It is easy to verify that it is the closed set

$$K_{\mathcal{L}} := \{a \in A : m^* \mathcal{L}|_{\{a\} \times A} \cong q^* \mathcal{L}|_{\{a\} \times A}\}.$$

**Proposition 8** ([Mil86, Proposition 9.2]). *Let  $\mathcal{L}$  be an invertible sheaf on  $A$ . Then the following conditions are equivalent:*

- (a)  $K_{\mathcal{L}} \cong A$ ;
- (b)  $t_a^* \mathcal{L} \cong \mathcal{L}$  on  $A_{\bar{k}}$  for all  $a \in A(\bar{k})$ ;
- (c)  $m^* \mathcal{L} \cong p^* \mathcal{L} \otimes q^* \mathcal{L}$ .

*Proof.* It is clear that (a) implies (b). It is also easy to see that (b) implies (a): indeed, the  $A(\bar{k})$  is dense in  $A$ , is contained in  $K_{\mathcal{L}}$  by assumption, and  $K_{\mathcal{L}}$  is a closed subset of  $A$ . We will then be done if we can prove that (a) is equivalent to (c).

It follows directly from the definitions that (c) yields (a). Assume that (a) holds, then. By definition of  $K_{\mathcal{L}}$ , we have

$$m^* \mathcal{L} \otimes q^* \mathcal{L}^{-1}|_{\{a\} \times A} \cong p^* \mathcal{L}|_{\{a\} \times A} \cong \mathcal{O}_{\{a\} \times A}$$

for all  $a \in A$ . Moreover,

$$m^* \mathcal{L} \otimes q^* \mathcal{L}^{-1}|_{A \times \{0\}} \cong \mathcal{L} \cong p^* \mathcal{L}|_{A \times \{0\}}.$$

Therefore, by the seesaw principle [Mil86, Corollary 5.2], we conclude that  $K_{\mathcal{L}} \cong A$ .  $\square$

We define  $\text{Pic}^0(A)$  to be the subgroup of  $\text{Pic}(A)$  consisting of the isomorphism classes of invertible sheaves on  $A$  which satisfy any of the equivalent conditions of Proposition 8. If  $T$  is a  $k$ -scheme, we define  $\text{Pic}^0(A_T)$  to be the isomorphism classes of invertible sheaves on  $A_T$  such that, if  $\mathcal{L}$  is a representative of such a class, then  $\mathcal{L}|_{\{0\} \times T}$  is trivial, and  $\mathcal{L}|_{A \times \{t\}}$  lies in  $\text{Pic}^0(A_{k(t)})$  for all  $t \in T$ .

**Proposition 9** ([Mil86, Proposition 10.1]). *Let  $\mathcal{L}$  be an invertible sheaf on  $A$ , and let  $T$  be a  $k$ -scheme. The image of  $\varphi_{\mathcal{L}, T}$  is contained in  $\text{Pic}^0(A_T)$ .*

*Proof.* Since  $\mathcal{L}$  is defined on  $A$ , we see that, for any  $a \in A(T)$ , the sheaf  $t_a^* \mathcal{L}_T \otimes \mathcal{L}_T^{-1}|_{\{0\} \times T}$  is trivial. Now, we have to show that  $t_a^* \mathcal{L}_{T,t} \otimes \mathcal{L}_{T,t}^{-1}$  lies in  $\text{Pic}^0(A_{k(t)})$  for

all  $t \in T$ . In order to do it, we will use part (b) of Proposition 8.

We aim to show that, given  $t \in T$ , we have

$$t_b^*(t_a^* \mathcal{L}_{T,t} \otimes \mathcal{L}_{T,t}^{-1}) \cong t_a^* \mathcal{L}_{T,t} \otimes \mathcal{L}_{T,t}^{-1}$$

for all  $b \in A(\overline{k(t)})$ . However,

$$t_b^*(t_a^* \mathcal{L}_{T,t} \otimes \mathcal{L}_{T,t}^{-1}) = t_{a+b}^* \mathcal{L}_{T,t} \otimes t_b^* \mathcal{L}_{T,t}^{-1},$$

and the theorem of the square yields that this is isomorphic to

$$t_a^* \mathcal{L}_{T,t} \otimes \mathcal{L}_{T,t}^{-1},$$

as we wanted. □

### 1.3 The Dual of an Abelian Variety

An abelian variety  $A^\vee$  is said to be the *dual* of an abelian variety  $A$ , and a sheaf  $\mathcal{P}$  on  $A \times A^\vee$  is called the *Poincaré sheaf*, if the following two conditions hold:

(a)  $\mathcal{P}$  lies in  $\text{Pic}^0(A_{A^\vee})$ ;

(b) if  $T$  is a  $k$ -scheme, and  $\mathcal{L}$  lies in  $\text{Pic}^0(A_T)$ , then there is a unique morphism  $f : T \rightarrow A^\vee$  such that  $(1 \times f)^* \mathcal{P} \cong \mathcal{L}$ .

**Theorem 10** ([Mil86, pp. 119-120]). *Let  $A$  be an abelian variety over a field  $k$ . The dual pair  $(A^\vee, \mathcal{P})$  exists and is unique up to unique isomorphism.*

**Remark.** If  $T$  is a  $k$ -scheme, then condition (b) of the definition of  $A^\vee$  gives us a functorial isomorphism between  $A^\vee(T)$  and  $\text{Pic}^0(A_T)$ . In other words, the functor

$$\mathbf{Sch}^{\text{op}}/k \rightarrow \mathbf{AbGrp}, \quad T \mapsto \text{Pic}^0(A_T)$$

is represented by the abelian variety  $A^\vee$ . As a consequence, the information contained in the homomorphisms  $\varphi_{\mathcal{L},T}$  can be synthesised in a single homomorphism

$$\varphi_{\mathcal{L}} : A \rightarrow A^\vee$$

of abelian varieties. It is clear that the map  $\text{Pic}(A) \rightarrow \text{Hom}(A, A^\vee)$  given by  $\mathcal{L} \mapsto \varphi_{\mathcal{L}}$

is a homomorphism with kernel  $\text{Pic}^0(A)$ . We define the *Néron–Severi group* of  $A$  to be  $\text{Pic}(A)/\text{Pic}^0(A)$ , and we denote it by  $\text{NS}(A)$ .

There is also a notion of *dual homomorphism*. In order to define this, we will firstly introduce the concept of *Cartier duality*.

Let **GrpSch** denote the category of group schemes, and let  $G$  be a finite flat commutative group scheme over a base scheme  $S$ . Consider the functor

$$\mathbf{Sch}^{\text{op}}/S \rightarrow \mathbf{Set}, \quad T \mapsto \text{Hom}_{\mathbf{GrpSch}}(G_T, \mathbb{G}_{m,T}).$$

This functor is represented by a finite flat  $S$ -group scheme  $G^\vee$ . We call  $G^\vee$  the *Cartier dual* of  $G$ .

If  $f : A \rightarrow B$  is a homomorphism of abelian varieties, let  $\mathcal{P}_B$  be the Poincaré sheaf on  $B \times B^\vee$ . Consider the invertible sheaf  $(f \times 1)^*\mathcal{P}_B$  on  $A \times B^\vee$ . By definition of dual abelian variety, there is a homomorphism  $f^\vee : B^\vee \rightarrow A^\vee$ , called the *dual* of  $f$ , such that

$$(1 \times f^\vee)^*\mathcal{P}_A \cong (f \times 1)^*\mathcal{P}_B.$$

**Theorem 11** ([Mil86, Theorem 11.1.]). *If  $f : A \rightarrow B$  is an isogeny with kernel  $N$ , then  $f^\vee : B^\vee \rightarrow A^\vee$  is an isogeny with kernel  $N^\vee$ , the Cartier dual of  $N$ .*

By definition of Cartier duality, if  $G$  is a finite flat group scheme over a base scheme  $S$ , then there is a bilinear pairing

$$G \times G^\vee \rightarrow \mathbb{G}_{m,S}.$$

Applying this to the multiplication-by- $N$  map on  $A$  (and noting that its dual is the multiplication-by- $N$  map on  $A^\vee$ ), we obtain a pairing

$$A[N] \times A^\vee[N] \rightarrow \mathbb{G}_m.$$

Moreover, if  $N$  is not divisible by the characteristic of the base field  $k$ , then we have a non-degenerate bilinear pairing of  $G_k$ -modules

$$\bar{e}_N : A[N](\bar{k}) \times A^\vee[N](\bar{k}) \rightarrow \bar{k}^\times.$$

It is clear that the image of this pairing is contained in  $\mu_N$ , the set of  $N$ th roots of unity of  $\bar{k}$ .

**Lemma 12** ([Mil86, Lemma 16.1.]). *Let  $m$  and  $n$  be integers not divisible by the characteristic of  $k$ . Then, for all  $P \in A[mn](\bar{k})$  and  $Q \in A^\vee[mn](\bar{k})$ , we have*

$$\bar{e}_{mn}(P, Q)^n = \bar{e}_m(nP, nQ).$$

Let  $\mu_m$  be the set of  $m$ -th roots of unity and, given a prime  $\ell$ , write

$$\mathbb{Z}_\ell(1) := \varprojlim \mu_{\ell^n}$$

for the  $G_k$ -module obtained by taking the projective limit of the system formed by the sets  $\mu_{\ell^n}$  and the maps  $\cdot^\ell : \mu_{\ell^{n+1}} \rightarrow \mu_{\ell^n}$ . By the previous lemma, we can define a pairing

$$e_\ell : T_\ell(A) \times T_\ell(A^\vee) \rightarrow \mathbb{Z}_\ell(1)$$

by setting  $e_\ell((P_n), (Q_n)) = (\bar{e}_{\ell^n}(P_n, Q_n))$ .

## 1.4 Polarized Abelian Varieties

A *polarization* of an abelian variety  $A$  is an isogeny  $\lambda : A \rightarrow A^\vee$  such that  $\lambda_{\bar{k}} = \varphi_{\mathcal{L}}$  for some ample invertible sheaf  $\mathcal{L}$  on  $A_{\bar{k}}$ . A *polarized abelian variety* is a pair  $(A, \lambda)$  consisting of an abelian variety  $A$  and a polarization  $\lambda$ . If the degree of a polarization is 1, we say that that polarization is *principal*.

**Example.** Elliptic curves are principally polarized. Indeed, let  $E$  be an elliptic curve defined over a field  $k$ . Consider the automorphism  $E \rightarrow E$  given by  $P \mapsto -P$ . Compose this with the isomorphism  $E \rightarrow \text{Pic}^0(E)$  given by  $P \mapsto [(O) - (P)]$ . The resulting map  $E \rightarrow \text{Pic}^0(E)$  is given by  $P \mapsto t_P^* \mathcal{O}_E(O) \otimes \mathcal{O}_E(O)^{-1}$  and is clearly principal.

The reason for our interest in polarized abelian varieties lies on the fact that, under some mild conditions, they come equipped with pairings defined on their Tate modules that share some useful properties with the well-known Weil pairings on elliptic curves. Indeed, if  $(A, \lambda)$  is a polarized abelian variety, then we can define pairings

$$\bar{e}_m^\lambda : A[m](\bar{k}) \times A[m](\bar{k}) \rightarrow \mu_m, \quad (P, Q) \mapsto \bar{e}_m(P, \lambda Q)$$

and

$$e_\ell^\lambda : T_\ell(A) \times T_\ell(A) \rightarrow \mathbb{Z}_\ell(1), \quad (P, Q) \mapsto e_\ell(P, \lambda Q).$$

If  $\lambda = \varphi_{\mathcal{L}}$  for some  $\mathcal{L} \in \text{Pic}(A)$ , we shall write  $\bar{e}_m^{\mathcal{L}}$  instead of  $\bar{e}_m^\lambda$ , and  $e_\ell^{\mathcal{L}}$  instead of  $e_\ell^\lambda$ .

**Proposition 13** ([Mil86, Proposition 16.6]). *Let  $k$  be an algebraically closed field. Assume that the characteristic of  $k$  is not 2 nor  $\ell$ , and let  $\lambda : A \rightarrow A^\vee$  be a homomorphism. We have  $\lambda = \varphi_{\mathcal{L}}$  for some  $\mathcal{L} \in \text{Pic}(A)$  if and only if  $e_\ell^\lambda$  is skew-symmetric.*

Therefore, if  $\ell$  is an odd prime and  $A$  is a principally polarized abelian variety of dimension  $g$  over a field of characteristic not dividing  $2\ell$ , the Galois action on  $A[\ell](\bar{k})$  gives rise to a representation

$$\bar{\rho}_{A,\ell} : G_{\mathbb{Q}} \rightarrow \text{GSp}_{2g}(\mathbb{F}_\ell).$$

From now on,  $\ell$  will always be assumed to be an odd prime.

**Remark.** Note that here, in opposition to what was done in Section 1.1, we regard pairings multiplicatively. Clearly, the results presented there have an obvious multiplicative counterpart.

Let  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_\ell^\times$  denote the mod  $\ell$  cyclotomic character. Since the pairing  $\bar{e}_\ell^{\mathcal{L}} : A[\ell](\bar{k}) \times A[\ell](\bar{k}) \rightarrow \mu_\ell$  is Galois-equivariant, we see that the character of this symplectic pairing is precisely  $\chi$ . Therefore, by Proposition 7, if  $\sigma$  is an element in  $G_{\mathbb{Q}}$ , then we have  $\det \bar{\rho}_{A,\ell}(\sigma) = \chi(\sigma)^g$  (where, as above,  $g = \dim A$ ).

In what follows, when given a polarized abelian variety, we will be interested in the action of the inertia subgroups of  $G_{\mathbb{Q}}$  on  $A[\ell](\bar{\mathbb{Q}})$ . We will make use of two important theorems concerning this question: one of them, that we will state after this paragraph, is Grothendieck's monodromy theorem, and it is concerned with the action of  $I_p$  when  $p \neq \ell$ ; the other theorem, which will be presented in the next section, is Raynaud's theorem, that deals with the case  $p = \ell$ .

**Theorem 14** (Grothendieck's monodromy theorem). *Let  $A$  be an abelian variety over  $\mathbb{Q}$  with semistable reduction at a prime  $p$ . If  $\ell$  is a prime different from  $p$ , then there is an  $\mathbb{F}_\ell$ -subspace  $V$  of  $A[\ell](\bar{\mathbb{Q}})$  on which  $I_p$  acts trivially and such that  $I_p$  acts trivially on the quotient  $A[\ell](\bar{\mathbb{Q}})/V$ .*

For a more general statement of this theorem, consult Theorem 6 in page 184 of [BLR90].

## 1.5 Fundamental Characters and a Theorem of Raynaud

Throughout this section, let  $K$  be a non-archimedean local field with residue field  $k$  of characteristic  $p$ . Let  $d \geq 1$  be an integer not divisible by  $p$ . We define

$$\mu_d := \{x \in K^{\text{nr}} : x^d = 1\}.$$

Moreover, fix a uniformiser  $\pi$  of  $K^{\text{nr}}$ , a  $d$ -th root  $\pi^{1/d}$  of  $\pi$ , and set  $K_d := K^{\text{nr}}(\pi^{1/d})$ . Since the characteristic of  $k$  does not divide  $d$ , it is clear that this extension is totally and tamely ramified.

**Lemma 15.** *The extension  $K_d/K^{\text{nr}}$  is Galois, and its Galois group is isomorphic to  $\mu_d$ .*

*Proof.* By Eisenstein's criterion, the polynomial  $X^d - \pi$  is irreducible in  $K^{\text{nr}}$ . Moreover, since the characteristic of  $k$  does not divide  $d$ , all the  $d$ -th roots of unity are contained in  $K^{\text{nr}}$ , from where it follows that  $K_d$  is the splitting field of the polynomial of  $X^d - \pi$  over  $K^{\text{nr}}$ , and that the extension  $K_d/K^{\text{nr}}$  is Galois of degree  $d$ . In order to prove that its Galois group is isomorphic to  $\mu_d$ , we are going to construct an isomorphism

$$\theta_d : \text{Gal}(K_d/K^{\text{nr}}) \rightarrow \mu_d.$$

If  $\sigma \in \text{Gal}(K_d/K^{\text{nr}})$ , then  $\sigma(\pi^{1/d}) = \zeta_d \pi^{1/d}$ , for some  $\zeta_d \in \mu_d$ . We then set

$$\theta_d(\sigma) := \frac{\sigma(\pi^{1/d})}{\pi^{1/d}}$$

and claim that this defines an isomorphism.

It is clear that  $\theta_d$  is injective. Since  $\mu_d$  has  $d$  elements, and the extension  $K_d/K^{\text{nr}}$  has degree  $d$ , surjectivity follows from injectivity.  $\square$

Note that the isomorphism  $\theta_d$  defined in the course of the proof of Lemma 15 is independent of the choice of uniformiser  $\pi$  and  $d$ -th root  $\pi^{1/d}$ . Indeed, if  $\varpi$  is another uniformiser of  $K^{\text{nr}}$ , and  $\varpi^{1/d}$  a  $d$ -th root of  $\varpi$ , then, writing  $\varpi = u\pi$ , where  $u$  is a unit, we have  $\varpi^{1/d} = u^{1/d}\pi^{1/d}$  for some  $d$ -th root of  $u$ . Since  $u^{1/d} \in K^{\text{nr}}$ , we find that

$$\sigma(\varpi^{1/d}) = \sigma(u^{1/d}\pi^{1/d}) = u^{1/d}\sigma(\pi^{1/d})$$

for every  $\sigma \in \text{Gal}(K_d/K^{\text{nr}})$ . Hence,

$$\frac{\sigma(\varpi^{1/d})}{\varpi^{1/d}} = \frac{u^{1/d}\sigma(\pi^{1/d})}{u^{1/d}\pi^{1/d}} = \frac{\sigma(\pi^{1/d})}{\pi^{1/d}},$$

as we wanted.

The Galois group  $\text{Gal}(K_d/K^{\text{nr}})$  is a quotient of  $I_K^t := \text{Gal}(K^t/K^{\text{nr}})$ , where  $K^t$  denotes the maximal tamely ramified extension of  $K$ . We call  $I_K^t$  the *tame inertia group* of  $K$ . By composing with the projection  $I_K^t \rightarrow \text{Gal}(K_d/K^{\text{nr}})$ , the homomorphism  $\theta_d$  induces a homomorphism on  $I_K^t$ . From now on, whenever we mention  $\theta_d$ , we are will be referring to this homomorphism just defined.

Fix an integer  $n \geq 1$  and set  $q := p^n$ . The characters  $\theta_{q-1}, \theta_{q-1}^p, \dots, \theta_{q-1}^{p^{n-1}}$  are known as the *fundamental characters of level  $n$* . Note that if we identify  $\mu_{q-1}$  with  $\mathbb{F}_q^\times$ , these are precisely the Galois conjugates of  $\theta_{q-1}$  over  $\mathbb{F}_p$ .

**Theorem 16** (Raynaud [Ray74]). *Let  $A$  be an abelian variety over  $\mathbb{Q}$ . Let  $p$  be a prime of semistable reduction of  $A$ . Regard  $A[p](\bar{\mathbb{Q}})$  as an  $I_p$ -module, and let  $V$  be a Jordan–Hölder factor of dimension  $n$  over  $\mathbb{F}_p$ . Then  $I_p^w$  acts trivially on  $V$ , and there is a structure of a 1-dimensional  $\mathbb{F}_{p^n}$ -vector space on  $V$  for which the action of  $I_p^t = I_p/I_p^w$  on it is given by a character  $\varpi : I_p^t \rightarrow \mathbb{F}_{p^n}^\times$ , where*

$$\varpi = \theta_{p^n-1}^{\sum_{i=0}^{n-1} a_i p^i},$$

with  $a_i \in \{0, 1\}$ .

Let  $\psi : V \rightarrow \mathbb{F}_{p^n}$  be an invertible  $\mathbb{F}_p$ -linear map that allows us to describe the action of  $I_p$  on  $V$  via the character  $\varpi$ . Moreover, let  $\sigma \in I_p^t$  be a topological generator of  $I_p^t$ . We claim that  $\varpi(\sigma) \in \mathbb{F}_{p^n}$  is an element of degree  $n$  over  $\mathbb{F}_p$ . In order to see this, let  $v$  be a non-zero vector of  $V$  and note that since  $V$  is irreducible for the action of  $I_p^t$ , it must be true that  $v, \sigma(v), \dots, \sigma^{n-1}(v)$  is an  $\mathbb{F}_p$ -basis for  $V$ . As  $\psi$  is an isomorphism of  $\mathbb{F}_p$ -vector spaces, we conclude that, for any  $\alpha \in \mathbb{F}_{p^n}$ , there exist  $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{F}_p$  such that

$$\begin{aligned} \alpha &= \lambda_0\psi(v) + \lambda_1\psi(\sigma(v)) + \dots + \lambda_{n-1}\psi(\sigma^{n-1}(v)) \\ &= (\lambda_0 + \lambda_1\varpi(\sigma) + \dots + \lambda_{n-1}\varpi(\sigma)^{n-1})\psi(v). \end{aligned}$$

But  $\psi(v) \neq 0$ , so this is equivalent to saying that, for any  $\alpha \in \mathbb{F}_{p^n}$ , there exist

$\lambda_0, \dots, \lambda_{n-1} \in \mathbb{F}_p$  such that

$$\alpha = \lambda_0 + \lambda_1 \varpi(\sigma) + \dots + \lambda_{n-1} \varpi(\sigma)^{n-1}.$$

Clearly, if the degree of  $\varpi(\sigma)$  over  $\mathbb{F}_p$  were not  $n$ , then  $\varpi(\sigma)$  would lie in a strictly smaller subextension of  $\mathbb{F}_{p^n}$ , making it impossible to generate every element of  $\mathbb{F}_{p^n}$  via  $\mathbb{F}_p$ -linear combinations of  $1, \varpi(\sigma), \dots, \varpi(\sigma)^{n-1}$ .

Keeping the notation from the paragraph above, we now claim that  $\varpi(\sigma)$  is an eigenvalue for the action of  $\sigma$  on  $V$ . Start by extending  $\psi$  to an  $\mathbb{F}_{p^n}$ -linear map  $V \otimes \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n} \otimes \mathbb{F}_{p^n}$  by mapping  $\sum_i v_i \otimes \alpha_i$  to  $\sum_i \psi(v_i) \otimes \alpha_i$ . Extend the action of  $I_p$  to  $V \otimes \mathbb{F}_{p^n}$  as well by setting  $\sigma(\sum_i v_i \otimes \alpha_i) = \sum_i (\sigma v_i) \otimes \alpha_i$ . Let  $\{\beta, \beta^p, \dots, \beta^{p^{n-1}}\}$  be a normal basis for the extension  $\mathbb{F}_{p^n}/\mathbb{F}_p$ . Then every element of  $V \otimes \mathbb{F}_{p^n}$  can be uniquely written in the form  $\sum_i v_i \otimes \beta^{p^i}$ . Similarly, every element of  $\mathbb{F}_{p^n} \otimes \mathbb{F}_{p^n}$  can be uniquely written in the form  $\sum_i \alpha_i \otimes \beta^{p^i}$ , where  $i \in \{0, \dots, n-1\}$  and  $\alpha_i \in \mathbb{F}_{p^n}$ . Let  $\lambda \in \mathbb{F}_{p^n}$  be an eigenvalue for the action of  $\sigma$  on  $V$ . Say that  $v := \sum_i v_i \otimes \beta^{p^i}$  is an eigenvector associated to  $\lambda$ . Then, for  $k \geq 1$ , we have

$$\sum_{i=0}^{n-1} (\sigma^k v_i) \otimes \beta^{p^i} = \sum_{i=0}^{n-1} v_i \otimes \lambda^k \beta^{p^i}.$$

Note that, by applying  $\psi$  to both sides, we obtain

$$\sum_{i=0}^{n-1} (\varpi(\sigma)^k \psi(v_i)) \otimes \beta^{p^i} = \sum_{i=0}^{n-1} \psi(v_i) \otimes \lambda^k \beta^{p^i}$$

Say that  $x^n + a_{n-1}x^{n-1} + \dots + a_0$  is the minimal polynomial of  $\varpi(\sigma)$  over  $\mathbb{F}_p$ , and that  $x^n + b_{n-1}x^{n-1} + \dots + b_0$  is the polynomial  $(x - \lambda)(x - \lambda^p) \dots (x - \lambda^{p^{n-1}})$ . Since the roots of these polynomials are  $\varpi(\sigma), \varpi(\sigma)^p, \dots, \varpi(\sigma)^{p^{n-1}}$  and  $\lambda, \lambda^p, \dots, \lambda^{p^{n-1}}$ , respectively, the elementary symmetric polynomials evaluated at  $\lambda, \dots, \lambda^{p^{n-1}}$  are going to be sums of powers of  $\lambda$ , and a similar situation occurs for the conjugates of  $\varpi(\sigma)$ . Therefore, by suitably combining some elements of the family (indexed by  $k$ ) of equalities above, we obtain, for each  $j \in \{0, \dots, n-1\}$ ,

$$\sum_{i=0}^{n-1} (a_j \psi(v_i)) \otimes \beta^{p^i} = \sum_{i=0}^{n-1} \psi(v_i) \otimes b_j \beta^{p^i}.$$

Since  $a_j, b_j \in \mathbb{F}_p$ , we must have  $a_j = b_j$  for every  $j \in \{0, \dots, n-1\}$ . This means that  $\varpi(\sigma)$  and  $\lambda$  have the same minimal polynomial, showing that they are, indeed,

conjugate. Note that, as a byproduct of this discussion, we concluded that the eigenvalues for the action of  $\sigma$  on  $V$  are of degree  $n$  over  $\mathbb{F}_p$ .

## 1.6 Néron Models

Let  $R$  be a discrete valuation ring with field of fractions  $K$ . Write  $S$  for the Dedekind scheme  $\text{Spec } R$ . Let  $X_K$  be a  $K$ -scheme. Any  $S$ -scheme  $X$  whose generic fibre is isomorphic to  $X_K$  is called an  $S$ -model of  $X_K$ . If  $X_K$  is a smooth and separated  $K$ -scheme of finite type, a *Néron model* of  $X_K$  over  $S$  is an  $S$ -model  $X$  of  $X_K$  which is smooth, separated and of finite type (over  $S$ ) and which satisfies the *Néron mapping property*: for each smooth  $S$ -scheme  $Y$  and each  $K$ -morphism  $\varphi : Y_K \rightarrow X_K$ , there is a unique  $S$ -morphism  $Y \rightarrow X$  extending  $\varphi$ .

**Proposition 17** ([BLR90, Section 1.2]). *Let  $X_K$  be a smooth and separated  $K$ -scheme of finite type. If there is a Néron model for  $X_K$  over  $S$ , then it is unique up to a unique isomorphism.*

*Proof.* Assume that  $X_K$  admits a Néron model over  $S$ . Let us denote it by  $X$ . Let  $X'$  be another Néron model over  $S$ . Since  $X$  and  $X'$  are both  $S$ -models for  $X_K$ , we have an isomorphism  $\varphi : X'_K \rightarrow X_K$ . By the Néron mapping property, there is a unique  $S$ -morphism  $\Phi : X' \rightarrow X$  which extends  $\varphi$ . Applying a similar reasoning to  $\varphi^{-1} : X_K \rightarrow X'_K$ , we conclude that there is a unique  $S$ -morphism  $\Psi : X \rightarrow X'$  which extends  $\varphi^{-1}$ . Since the  $S$ -morphisms that extend the identity morphisms  $X_K \rightarrow X_K$  and  $X'_K \rightarrow X'_K$  are the identity maps  $\text{id}_X : X \rightarrow X$  and  $\text{id}_{X'} : X' \rightarrow X'$ , we obtain the equalities

$$\Psi \circ \Phi = \text{id}_{X'} \quad \text{and} \quad \Phi \circ \Psi = \text{id}_X,$$

which prove the proposition. □

**Theorem 18** ([BLR90, Section 1.3]). *Let  $A$  be an abelian variety defined over a field of fractions  $K$  of a discrete valuation ring  $R$ . Then  $A$  admits a Néron model over  $\text{Spec } R$ .*

Another useful consequence of the Néron mapping property is the following:

**Lemma 19.** *Let  $X_K$  be a smooth and separated  $K$ -scheme of finite type. Assume that it admits a Néron model  $X$  over  $S$ . Then there exists a natural bijection between  $X(R)$  and  $X_K(K)$ .*

*Proof.* In order to prove this, we will define two maps,  $f : X(R) \rightarrow X_K(K)$  and  $g : X_K(K) \rightarrow X(R)$ , and then we will show that they are inverses of each other.

The map  $f$  is defined as follows. An element of  $X(R)$  is, by definition, an  $S$ -morphism  $S \rightarrow X$ . Precomposing with the morphism  $\text{Spec } K \rightarrow S$  obtained from the inclusion  $R \subseteq K$ , we obtain an element in  $X(K)$ . However, the image of any  $S$ -morphism  $\text{Spec } K \rightarrow X$  must land in the generic fibre of  $X$ . Therefore, we actually have an element in  $X_K(K)$ .

For the other direction, note that  $S$  is the Néron model of  $K$  over  $S$  itself. Therefore, if we are given a  $K$ -morphism  $\text{Spec } K \rightarrow X_K$ , the Néron mapping property yields the existence of a unique  $S$ -morphism  $S \rightarrow X$  extending it. This gives rise to our element in  $X(R)$ . It is now evident that these two maps are inverses of each other.  $\square$

Now let  $K$  be a number field, and  $A_K$  an abelian variety defined over  $K$ . Let  $v$  be a discrete valuation on  $K$ . Let  $K_v$  denote the completion of  $K$  at  $v$  and let  $\mathcal{O}_v$  denote the ring of integers. We will write  $k_v$  for the residue field associated to this local field. Also, let  $A$  denote the Néron model of  $A_K$  over  $\text{Spec } \mathcal{O}_v$ , and let  $\tilde{A}$  denote the special fibre.

Let  $K_v^{\text{nr}}$  denote the maximal unramified extension of  $K_v$  and let  $\mathcal{O}$  denote the ring of integers. Since  $A(\mathcal{O}) = A_K(K_v^{\text{nr}})$ , the reduction map  $\mathcal{O} \rightarrow \bar{k}_v$  induces a reduction on the  $K_v^{\text{nr}}$ -points of the abelian variety:

$$r_v : A_K(K_v^{\text{nr}}) \rightarrow \tilde{A}(\bar{k}_v).$$

Since  $A$  is smooth and  $\mathcal{O}$  is Henselian, we must have  $r_v$  surjective.

**Lemma 20** ([ST68, Lemma 2]). *Let  $m$  be a positive integer coprime to the characteristic of  $k_v$ . The reduction map  $r_v$  defines a  $G_{K_v}$ -equivariant isomorphism from  $A_K[m](K_v^{\text{nr}})$  onto  $\tilde{A}[m](\bar{k}_v)$ .*

## 1.7 Residual Representations of Semistable Principally Polarized Abelian Varieties

The main result we prove in this section is Theorem 4. Its proof uses two ingredients: one of them is Theorem 16 above, the other is the following classification of subgroups of  $\text{GSp}_{2d}(\mathbb{F}_\ell)$  containing a transvection.

**Theorem 21** ([AdRDW16]). *Let  $\ell \geq 5$  be a prime and let  $V$  be a symplectic  $\mathbb{F}_\ell$ -vector space of dimension  $2d$ . If  $G$  is a subgroup of  $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$  containing a transvection, then one of the following statements holds:*

- (i) *There is a non-trivial proper  $G$ -stable subspace  $W \subseteq V$ ;*
- (ii) *There are non-singular symplectic subspaces  $V_i \subseteq V$  ( $i = 1, \dots, h$ ) of dimension  $2m < 2d$ , and a homomorphism  $\phi : G \rightarrow S_h$  such that  $V = \bigoplus_{i=1}^h V_i$  and  $\sigma(V_i) = V_{\phi(\sigma)(i)}$  for  $\sigma \in G$  and  $1 \leq i \leq h$ . Moreover,  $\phi(G)$  is a transitive subgroup of  $S_h$ ;*
- (iii)  $\mathrm{Sp}(V) \subseteq G$ .

Before starting the proof of the main theorem, let us prove an auxiliary lemma.

**Lemma 22.** *Let  $k$  be an algebraically closed field and  $V \neq 0$  a finite-dimensional  $k$ -vector space. Let  $T$  be a linear map and suppose that there exist linear subspaces  $V_1, \dots, V_r$  of  $V$  such that  $V = \bigoplus_{i=1}^r V_i$  and  $T(V_i) = V_{i+1}$ , where the subscripts are to be interpreted mod  $r$ . If  $\alpha$  is an eigenvalue of  $T$ , and  $\zeta \in k$  is such that  $\zeta^r = 1$ , then  $\zeta\alpha$  is an eigenvalue of  $T$  as well.*

*Proof.* Let  $v$  be an eigenvector associated to  $\alpha$ . Let  $v_i \in V_i$  be such that  $v = \sum_{i=1}^r v_i$ . Then  $T(v_i) = \alpha v_{i+1}$ . Set  $v' := \sum_{i=1}^r \zeta^{-i} v_i$ . Then

$$T(v') = \sum_{i=1}^r \zeta^{-i} \alpha v_{i+1} = \zeta \alpha \sum_{i=1}^r \zeta^{-i-1} v_{i+1} = \zeta \alpha v',$$

which shows that  $\zeta\alpha$  is an eigenvalue for  $T$ . □

*Proof of Theorem 4.* For simplicity, we are going to write  $\bar{\rho}$  for  $\bar{\rho}_{A,\ell}$ . Let  $G := \bar{\rho}(G_{\mathbb{Q}})$  and consider the action of  $G$  on the symplectic vector space  $V := A[\ell]$ . Since, by assumption,  $G$  contains a transvection, we can apply Theorem 21. In order to prove the result, we only need to rule case (ii) out. Suppose, for the sake of contradiction, that case (ii) holds. Let  $\phi$  be as in the statement of Theorem 21. Let  $\pi := \phi \circ \bar{\rho} : G_{\mathbb{Q}} \rightarrow S_h$ . If we set  $H := \ker(\pi)$ , then there exists a number field  $K$  for which  $H = G_K$ . Moreover,  $\bar{\rho}|_{G_K}$  is reducible. We will now show that  $K/\mathbb{Q}$  is unramified at all the finite places, implying, by a famous result of Hermite, that  $K = \mathbb{Q}$ .

Throughout,  $I_p$  will stand for the inertia subgroup of a decomposition subgroup over the prime  $p$ .

Let  $p \neq \ell$  be a prime. Since we are assuming that  $A$  is semistable,  $I_p$  acts unipotently on  $V$  (see Theorem 14). Therefore, if  $\sigma \in I_p$ ,  $\bar{\rho}(\sigma)$  has  $\ell$ -power order.

However, the order of  $\bar{\rho}(\sigma)$  is divisible by the order of  $\pi(\sigma)$ , which, in turn, divides  $h!$ . As  $h = 2d/2m \leq d < \ell$ , we conclude that  $\pi(\sigma) = 1$ . Thus, if  $p \neq \ell$ , the extension  $K/\mathbb{Q}$  is unramified at  $p$ .

The next case we consider is that of  $\sigma \in I_\ell^w$ , the wild subgroup of  $I_\ell$ . This case is similar to the one above: as  $I_\ell^w$  is a pro- $\ell$ -group,  $\bar{\rho}(\sigma)$  has  $\ell$ -power order. Hence, as above, we conclude that  $\pi(\sigma) = 1$ .

Now let  $\sigma \in I_\ell$  be such that its image in  $I_\ell^t$  is a topological generator. Suppose, for the sake of contradiction, that  $\pi(\sigma) \neq 1$ . Reorder  $V_1, \dots, V_h$  so that  $\sigma(V_r) = V_1$  and, for  $i = 1, \dots, r-1$ ,  $\sigma(V_i) = V_{i+1}$ . Note that, since we are assuming that  $\pi(\sigma) \neq 1$ , we must have  $r > 1$ . Set  $\bar{V} := V \otimes \bar{\mathbb{F}}_\ell$  and  $\bar{V}_i := V_i \otimes \bar{\mathbb{F}}_\ell$ . Define  $\bar{W} := \bigoplus_{i=1}^r \bar{V}_i$ . Note that, by definition,  $\bar{W}$  is stable under the action of  $I_\ell$ . Let  $\alpha_0 \in \bar{\mathbb{F}}_\ell$  be an eigenvalue for the action of  $\sigma$  on  $\bar{W}$ . Since  $r \leq h \leq d < \ell$ , the field  $\bar{\mathbb{F}}_\ell$  has  $r$ th roots of unity distinct from 1 as long as  $r > 1$ . Let  $\zeta$  be a primitive  $r$ th root of unity and set  $\alpha_1 := \zeta \alpha_0$ . Lemma 22 now yields that  $\alpha_1$  is an eigenvalue for the action of  $\sigma$  on  $\bar{W}$  as well. By Raynaud's theorem (Theorem 16), there are integers  $n_0, n_1$  and characters  $\varpi_j : I_\ell \rightarrow \mathbb{F}_{\ell^{n_j}}^\times$  ( $j = 0, 1$ ) such that  $\alpha_j = \varpi_j(\sigma)$  and

$$\varpi_0 = \theta_{\ell^{n_0-1}}^{a_0+a_1\ell+\dots+a_{n_0-1}\ell^{n_0-1}}, \quad \varpi_1 = \theta_{\ell^{n_1-1}}^{b_0+b_1\ell+\dots+b_{n_1-1}\ell^{n_1-1}},$$

where, as in the statement of Raynaud's theorem,  $\theta_{\ell^n-1}$  stands for a fundamental character of level  $n$ , and  $a_i, b_i \in \{0, 1\}$ . Let  $m := \text{lcm}(n_0, n_1)$ . As  $n_0$  and  $n_1$  both divide  $m$ , the numbers

$$k_0 := \frac{\ell^m - 1}{\ell^{n_0} - 1} \quad \text{and} \quad k_1 := \frac{\ell^m - 1}{\ell^{n_1} - 1}$$

are integers. Moreover, we have  $\theta_{\ell^{n_0-1}}^{k_0} = \theta_{\ell^m-1}^{k_0}$  and  $\theta_{\ell^{n_1-1}}^{k_1} = \theta_{\ell^m-1}^{k_1}$ . Therefore,

$$\varpi_0 = \theta_{\ell^m-1}^{k_0(a_0+a_1\ell+\dots+a_{n_0-1}\ell^{n_0-1})}, \quad \varpi_1 = \theta_{\ell^m-1}^{k_1(b_0+b_1\ell+\dots+b_{n_1-1}\ell^{n_1-1})}.$$

Since  $\theta_{\ell^m-1}$  is surjective onto  $\mu_{\ell^m-1}$ , the element  $\theta_{\ell^m-1}(\sigma)$  must have order  $\ell^m - 1$ . However,  $\zeta = \varpi_1(\sigma)/\varpi_0(\sigma)$  has order  $r$ . Therefore,

$$r \left( k_0 \sum_{i=0}^{n_0-1} a_i \ell^i - k_1 \sum_{i=0}^{n_1-1} b_i \ell^i \right) \equiv 0 \pmod{\ell^m - 1}. \quad (1.1)$$

As  $a_i, b_i \in \{0, 1\}$ , it is evident that

$$-\frac{\ell^m - 1}{\ell - 1} = -\frac{\ell^m - 1}{\ell^{n_1} - 1} \sum_{i=0}^{n_1-1} \ell^i \leq k_0 \sum_{i=0}^{n_0-1} a_i \ell^i - k_1 \sum_{i=0}^{n_1-1} b_i \ell^i \leq \frac{\ell^m - 1}{\ell^{n_0} - 1} \sum_{i=0}^{n_0-1} \ell^i = \frac{\ell^m - 1}{\ell - 1}.$$

Therefore,

$$r \left| k_0 \sum_{i=0}^{n_0-1} a_i \ell^i - k_1 \sum_{i=0}^{n_1-1} b_i \ell^i \right| \leq r \frac{\ell^m - 1}{\ell - 1}.$$

Since  $r \leq d < \ell - 1$ , we have  $r \frac{\ell^m - 1}{\ell - 1} < \ell^m - 1$ . This, together with (1.1), implies

$$k_0(a_0 + a_1\ell + \dots + a_{n_0-1}\ell^{n_0-1}) = k_1(b_0 + b_1\ell + \dots + b_{n_1-1}\ell^{n_1-1}),$$

which means that  $\zeta = \varpi_1(\sigma)/\varpi_0(\sigma) = 1$ , yielding a contradiction. Hence,  $\pi(\sigma) = 1$ . As  $\pi(I_\ell^w) = 1$ , and as we chose  $\sigma$  to be a topological generator for  $I_\ell^t$ , we conclude, as we wanted, that  $\pi(I_\ell) = 1$ . This finishes the proof that  $K/\mathbb{Q}$  is unramified at  $\ell$ . Therefore,  $K/\mathbb{Q}$  is unramified at all finite places, forcing  $K = \mathbb{Q}$ , which contradicts the fact that  $\pi(G)$  is transitive.  $\square$

In order to apply Theorem 4, we need to know when the image of the residual Galois representation mod  $\ell$  of an abelian variety contains a transvection. The following lemma is a criterion for this to happen, and can be found in [Hal11].

**Theorem 23.** *Let  $A$  be a semistable abelian variety over  $\mathbb{Q}$  of dimension  $g$ . Assume that there is a prime  $q$  such that the special fibre of the Néron model for  $A$  at  $q$  has toric dimension 1. Let  $\ell \neq q$  be a prime not dividing the order of  $\Phi_q$ , the group of connected components of the special fibre of the Néron model for  $A$  at  $q$ . Then the image of the residual Galois representation*

$$\bar{\rho}_{A,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell)$$

*contains a transvection.*

*Proof.* Denote by  $A_\eta$  the generic fibre of the Néron model of  $A$  at  $q$ , and by  $A_s$  the special fibre. Let  $A_s^0$  be the connected component of the identity of  $A_s$ . It is well-known (see, for example, [Che60]) that  $A_s^0$ , being a connected algebraic group, is an extension of an abelian variety  $B$  by a linear group  $G$ , i.e., there is an (fppf)-exact sequence

$$0 \rightarrow G \rightarrow A_s^0 \rightarrow B \rightarrow 0.$$

Since we are assuming that  $A$  is semistable, we know that  $G$  is a torus. Moreover, by assumption, it must have dimension 1. Now,  $G(\bar{\mathbb{F}}_q)$  is  $\ell$ -divisible, which yields

the exactness of

$$0 \rightarrow G[\ell](\bar{\mathbb{F}}_q) \rightarrow A_s^0[\ell](\bar{\mathbb{F}}_q) \rightarrow B[\ell](\bar{\mathbb{F}}_q) \rightarrow 0.$$

As a consequence, we have

$$\dim_{\mathbb{F}_\ell} A_s^0[\ell](\bar{\mathbb{F}}_q) = 2g - 1.$$

Let  $D_q$  be a decomposition subgroup of  $G_{\mathbb{Q}}$  over  $q$  and let  $I_q$  be its inertia subgroup. By Lemma 20, reduction mod  $q$  defines an isomorphism

$$A_\eta[\ell](\bar{\mathbb{Q}}_q)^{I_q} \rightarrow A_s[\ell](\bar{\mathbb{F}}_q)$$

which is compatible with the  $D_q$ -action. Since  $\ell \nmid \#\Phi_q$ , we have  $A_s[\ell](\bar{\mathbb{F}}_q) = A_s^0[\ell](\bar{\mathbb{F}}_q)$ . Therefore,

$$\dim_{\mathbb{F}_q} A_\eta[\ell](\bar{\mathbb{Q}}_q)^{I_q} = 2g - 1.$$

Moreover,  $I_q$  acts unipotently on  $A_\eta[\ell](\bar{\mathbb{Q}}_q)$ . Hence, if  $\sigma \in I_q$  is an element which does not act trivially on  $A_\eta[\ell](\bar{\mathbb{Q}}_q)$ ,  $\bar{\rho}_{A,\ell}(\sigma)$  is unipotent and  $\bar{\rho}_{A,\ell}(\sigma) - I$  has rank 1; in other words,  $\bar{\rho}_{A,\ell}(\sigma)$  is a transvection.  $\square$

## 1.8 Semistable Abelian Threefolds

From now to the end of the chapter, unless otherwise specified,  $A$  will denote a semistable principally polarized abelian threefold over  $\mathbb{Q}$  for which there is a prime  $q$  such that the special fibre of the Néron model for  $A$  at  $q$  has toric dimension 1. If  $S$  stands for the set of such primes, then, according to Theorem 4 and Lemma 23, if  $\ell \geq 5$  is a prime which does not divide  $\gcd(\{q \cdot \#\Phi_q : q \in S\})$ , the representation  $\bar{\rho}_{A,\ell}$  is either reducible or surjective.

We are now going to describe a practical method to find a small integer  $B$  (depending on  $A$ ) such that, for  $\ell \nmid B$ , the representation  $\bar{\rho}_{A,\ell}$  is irreducible and, therefore, surjective. The idea is, for each  $n \in \{1, \dots, 5\}$ , to find an integer  $B_n \neq 0$  such that, possibly under certain mild conditions, the Galois representation  $\bar{\rho}_{A,\ell}$  does not admit an  $n$ -dimensional subrepresentation whenever  $\ell > B_n$ .

## Determinants of Jordan–Hölder factors

**Lemma 24.** *Any Jordan–Hölder factor  $W$  of the  $G_{\mathbb{Q}}$ -module  $A[\ell](\bar{\mathbb{Q}})$  has determinant  $\chi^r$  for some  $0 \leq r \leq \dim(W)$ , where  $\chi$  is the mod  $\ell$  cyclotomic character.*

*Proof.* Let  $W$  be a Jordan–Hölder factor of  $A[\ell](\bar{\mathbb{Q}})$  and  $\psi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}$  its determinant. As  $A$  is semistable, for primes  $p \neq \ell$ , the inertia group  $I_p \subseteq G_{\mathbb{Q}}$  acts unipotently on  $W$ . Thus,  $\psi|_{I_p} = 1$ . Now, considering  $W$  as an  $I_{\ell}$ -module, it follows from Raynaud’s Theorem that  $\psi|_{I_{\ell}} = \chi^r|_{I_{\ell}}$  for some  $0 \leq r \leq \dim(W)$ . Hence, the character  $\psi\chi^{-r}$  is unramified at all finite places, which forces  $\psi\chi^{-r} = 1$ .  $\square$

## 1-dimensional Jordan–Hölder factors

If  $p \neq \ell$  is a prime of good reduction for  $A$ , we shall write

$$P_p(x) = x^6 + \alpha_p x^5 + \beta_p x^4 + \gamma_p x^3 + p\beta_p x^2 + p^2\alpha_p x + p^3 \in \mathbb{Z}[x]$$

for the characteristic polynomial of Frobenius  $\sigma_p \in G_{\mathbb{Q}}$  at  $p$  acting on the Tate module  $T_{\ell}(A)$ . It is a well-known fact that  $P_p$  is independent of  $\ell$ . Moreover, the roots of  $P_p$  in  $\bar{\mathbb{F}}_{\ell}$  have the form  $u, v, w, p/u, p/v, p/w$ .

**Lemma 25.** *If  $P_p$  has a real root, then  $(x^2 - p)^2$  is a factor of  $P_p$ .*

*Proof.* We know that the complex roots of  $P_p$  have the form  $\omega_1, \omega_2, \omega_3, \bar{\omega}_1, \bar{\omega}_2, \bar{\omega}_3$ , where  $|\omega_i| = \sqrt{p}$  and  $\bar{\omega}$  denotes the complex conjugate of  $\omega$ . Suppose that  $\omega_1$  is real. Since  $|\omega_1| = \sqrt{p}$ , we conclude that  $\omega_1 = \pm\sqrt{p}$ . Therefore, either  $(x - \sqrt{p})^2$  divides  $P_p$ , or  $(x + \sqrt{p})^2$  divides  $P_p$ . As  $P_p \in \mathbb{Z}[x]$ , both of them must divide it. Hence,  $(x^2 - p)^2$  is a factor of  $P_p$ .  $\square$

Let  $T$  be a non-empty set of primes of good reduction for  $A$  and define

$$B_1(T) := \gcd\{p \cdot \#A(\mathbb{F}_p) : p \in T\}.$$

**Lemma 26.** *Suppose that  $\ell \nmid B_1(T)$ . The  $G_{\mathbb{Q}}$ -module  $A[\ell](\bar{\mathbb{Q}})$  does not have any 1-dimensional Jordan–Hölder factor.*

*Proof.* Suppose, for the sake of contradiction, that  $A[\ell](\bar{\mathbb{Q}})$  admits a 1-dimensional Jordan–Hölder factor; call it  $W$ . The action of  $G_{\mathbb{Q}}$  on  $W$  is then given by a character

$$\psi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}.$$

Lemma 24 asserts that  $\psi = 1$  or  $\chi$ . Now, if  $p \neq \ell$  is a prime of good reduction for  $A$ , we have that either  $P_p(1) \equiv 0 \pmod{\ell}$ , or, as  $\chi(\sigma_p) \equiv p \pmod{\ell}$ ,  $P_p(p) \equiv 0$

(mod  $\ell$ ). Since the roots of  $P_p$  are of the form  $u, v, w, p/u, p/v, p/w$ , we conclude that, in any case,  $P_p(1) \equiv 0 \pmod{\ell}$ . As  $\#A(\mathbb{F}_p) = P_p(1)$ , it follows that  $\ell$  must divide  $\#A(\mathbb{F}_p)$ , which yields  $\ell \mid B_1(T)$ . This contradiction proves the lemma.  $\square$

**Remark.** Note that the lemma still holds if, in its statement, we replace “1-dimensional” by “5-dimensional”. Indeed, as  $A[\ell](\bar{\mathbb{Q}})$  is a 6-dimensional  $\mathbb{F}_\ell$ -vector space, the existence of a 5-dimensional Jordan–Hölder factor implies the existence of a 1-dimensional one.

## 2-dimensional Jordan–Hölder factors

**Lemma 27.** *Suppose that the  $G_{\mathbb{Q}}$ -module  $A[\ell](\bar{\mathbb{Q}})$  does not have any 1-dimensional Jordan–Hölder factor, but has either a 2-dimensional or a 4-dimensional irreducible subspace  $U$ . Then  $A[\ell](\bar{\mathbb{Q}})$  has a 2-dimensional Jordan–Hölder factor  $W$  with determinant  $\chi$ .*

*Proof.* Suppose that  $\dim(U) = 2$ . If the restriction of the Weil pairing to  $U$  is non-degenerate, then  $\det(U) = \chi$  (see Proposition 7), and we can take  $W = U$ . We are then reduced to the case when the restriction of the Weil pairing to  $U$  is degenerate.

In this case,  $U \cap U^\perp \neq 0$ . The Galois invariance of the Weil pairing implies that  $U^\perp$  is a  $G_{\mathbb{Q}}$ -submodule of  $A[\ell](\bar{\mathbb{Q}})$ . But  $U$  is irreducible, and, therefore, we must have  $U \subseteq U^\perp$ . However,  $U^\perp$  is 4-dimensional. Since, by assumption,  $A[\ell](\bar{\mathbb{Q}})$  does not have any 1-dimensional Jordan–Hölder factor, each of the 2-dimensional quotients of

$$0 \subset U \subset U^\perp \subset A[\ell](\bar{\mathbb{Q}})$$

must be irreducible and have determinant 1,  $\chi$  or  $\chi^2$ . Since  $\det(A[\ell](\bar{\mathbb{Q}})) = \chi^3$ , we conclude that one of these quotients must have determinant  $\chi$ .

Now suppose that  $\dim(U) = 4$ . It is not possible for the restriction of the Weil pairing to  $U$  to be degenerate, as, if it were, then, as above, we would have  $U \subseteq U^\perp$ ; however,  $\dim(U^\perp) = 2 < \dim(U)$ . Therefore, the restriction of the Weil pairing to  $U$  is non-degenerate, and the determinant of  $U$  is  $\chi^2$ . As  $\det(A[\ell](\bar{\mathbb{Q}})) = \chi^3$ , we conclude that  $A[\ell](\bar{\mathbb{Q}})/U$  is an irreducible 2-dimensional  $G_{\mathbb{Q}}$ -module with determinant  $\chi$ .  $\square$

Let  $N$  be the conductor of  $A$ . Let  $W$  be a 2-dimensional Jordan–Hölder factor

of  $A[\ell](\bar{\mathbb{Q}})$  with determinant  $\chi$ . The representation

$$\tau : G_{\mathbb{Q}} \rightarrow \mathrm{GL}(W)$$

is odd, irreducible and 2-dimensional. By Serre's modularity conjecture [KW09],  $\tau$  arises from a newform  $f$  of level  $M \mid N$  and weight 2.

Let  $\mathcal{O}_f$  denote the ring of integers of the number field generated by the Hecke eigenvalues of  $f$ . Letting  $c_p(f)$  denote the  $p$ th Hecke eigenvalue of  $f$ , there is a prime  $\lambda \mid \ell$  of  $\mathcal{O}_f$  such that

$$\mathrm{Tr}(\tau(\sigma_p)) \equiv c_p(f) \pmod{\lambda}$$

for all primes  $p \nmid \ell N$ . Therefore, modulo  $\lambda$ , the polynomial  $x^2 - c_p(f)x + p$  is congruent to the characteristic polynomial of  $\tau(\sigma_p)$ . Thus, modulo  $\lambda$ , it is a factor of  $P_p$ .

Let  $H_{M,p}$  denote the  $p$ th Hecke polynomial for the new subspace  $S_2^{\mathrm{new}}(M)$  of cusp forms of level 2 and level  $M$ . This polynomial has the form

$$H_{M,p} = \prod_g (x - c_p(g)),$$

where  $g$  runs through the newforms of weight 2 and level  $M$ . Define

$$H'_{M,p} := x^d H_{M,p}(x + p/x) \in \mathbb{Z}[x],$$

where  $d := \dim(S_2^{\mathrm{new}}(M))$ . Note that, by definition,  $x^2 - c_p(f)x + p$  divides  $H'_{M,p}$ . Set

$$R(M, p) := \mathrm{Res}(P_p, H'_{M,p}) \in \mathbb{Z},$$

where  $\mathrm{Res}$  stands for the resultant. It is immediate that  $R(M, p) \equiv 0 \pmod{\lambda}$ . As  $R(M, p)$  is a rational integer, we must have  $\ell \mid R(M, p)$ . Therefore, if  $R(M, p) \neq 0$ , we obtain an upper bound on  $\ell$ . However, this integer  $R(M, p)$  can be very large. In order to find a smaller bound, we consider instead a set  $T$  of rational primes of good reduction for  $A$  and define

$$R(M, T) := \mathrm{gcd}\{p \cdot R(M, p) : p \in T\}.$$

Now let

$$B'_2(T) := \mathrm{lcm}\{R(M, T) : M \mid N \text{ and } \dim(S_2^{\mathrm{new}}(M)) \neq 0\}.$$

Finally, set

$$B_2(T) := \text{lcm}\{B_1(T), B'_2(T)\}.$$

**Lemma 28.** *Let  $T$  be a non-empty set of rational primes of good reduction for  $A$  and suppose that  $\ell \nmid B_2(T)$ . Then  $A[\ell](\overline{\mathbb{Q}})$  does not have 1-dimensional Jordan–Hölder factors, nor 2- or 4-dimensional irreducible subspaces.*

*Proof.* This follows from our discussion above.  $\square$

### 3-dimensional Jordan–Hölder factors

**Lemma 29.** *Suppose  $A[\ell]$  has Jordan–Hölder filtration  $0 \subset U \subset A[\ell]$  where both  $U$  and  $A[\ell]/U$  are irreducible and 3-dimensional. Moreover, let  $u_1, u_2, u_3$  be a basis for  $U$ , and let*

$$G_{\mathbb{Q}} \rightarrow \text{GL}_3(\mathbb{F}_{\ell}), \quad \sigma \mapsto M(\sigma)$$

*give the action of  $G_{\mathbb{Q}}$  on  $U$  with respect to this basis. Then we can extend  $u_1, u_2, u_3$  to a symplectic basis  $u_1, u_2, u_3, w_1, w_2, w_3$  for  $A[\ell]$  so that the action of  $G_{\mathbb{Q}}$  on  $A[\ell]$  with respect to this basis is given by*

$$G_{\mathbb{Q}} \rightarrow \text{GSp}_6(\mathbb{F}_{\ell}), \quad \sigma \mapsto \left( \begin{array}{c|c} M(\sigma) & * \\ \hline \mathbf{0} & \chi(\sigma)(M(\sigma)^t)^{-1} \end{array} \right).$$

*Proof.* In odd characteristic, any bilinear alternating pairing on an odd dimensional space must be degenerate (see Proposition 5). Therefore,  $U \subseteq U^{\perp}$ . As both spaces have dimension 3, we have  $U = U^{\perp}$ . Let  $u_1, u_2, u_3$  be a basis for  $U$ . Then  $\langle u_i, u_j \rangle = 0$ . Extend this to a symplectic basis  $u_1, u_2, u_3, w_1, w_2, w_3$  for  $A[\ell]$  (see Proposition 6). The lemma is now a consequence of the identity  $\langle u_i, \sigma w_j \rangle = \chi(\sigma) \langle \sigma^{-1} u_i, w_j \rangle$  for  $\sigma \in G_{\mathbb{Q}}$ .  $\square$

Now let  $U$  be as in Lemma 29. By Lemma 24, we have that  $\det(U) = \chi^r$  and  $\det(A[\ell]/U) = \chi^s$ , where  $0 \leq r, s \leq 3$ . Moreover, as  $\det(A[\ell]) = \chi^3$ , we have that  $r + s = 3$ .

**Lemma 30.** *Let  $p$  be a prime of good reduction for  $A$ . For ease, write  $\alpha, \beta$  and  $\gamma$  for the coefficients  $\alpha_p, \beta_p, \gamma_p$  of  $P_p$ . Suppose  $p + 1 \neq \alpha$  (this is certainly true for  $p \geq 36$ , as  $|\alpha| \leq 6\sqrt{p}$ ). Let*

$$\delta = \frac{-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma}{(p-1)(p+1-\alpha)} \in \mathbb{Q}, \quad \epsilon = \delta + \alpha \in \mathbb{Q}. \quad (1.2)$$

Let

$$g(x) = (x^3 + \epsilon x^2 + \delta x - p)(x^3 - \delta x^2 - p\epsilon x - p^2) \in \mathbb{Q}[x]. \quad (1.3)$$

Write  $k$  for the greatest common divisor of the numerators of the coefficients in  $P_p - g$  if  $P_p \neq g$ , and let  $k = 0$  otherwise. Let

$$K_p = p(p-1)(p+1-\alpha)k.$$

Then  $K_p \neq 0$ . Moreover, if  $\ell \nmid K_p$  then  $A[\ell]$  does not have a Jordan–Hölder filtration as in Lemma 29 with  $\det(U) = \chi$  or  $\chi^2$ .

**Lemma 31.** *Let  $p$  be a prime of good reduction for  $A$ . Write  $\alpha$ ,  $\beta$  and  $\gamma$  for the coefficients  $\alpha_p$ ,  $\beta_p$ ,  $\gamma_p$  of  $P_p$ . Suppose  $p^3 + 1 \neq p\alpha$  (this is true for  $p \geq 5$  as  $|\alpha| \leq 6\sqrt{p}$ ). Let*

$$\delta' = \frac{-p^5\alpha + p^4 + p^3\alpha^2 - p^3\beta - p^2\alpha + p\gamma + p - \beta}{(p^3 - 1)(p^3 + 1 - p\alpha)} \in \mathbb{Q}, \quad \epsilon' = p\delta' + \alpha \in \mathbb{Q}. \quad (1.4)$$

Let

$$g'(x) = (x^3 + \epsilon'x^2 + \delta'x - 1)(x^3 - p\delta'x^2 - p^2\epsilon'x - p^3) \in \mathbb{Q}[x]. \quad (1.5)$$

Write  $k'$  for the greatest common divisor of the numerators of the coefficients in  $P_p - g'$  if  $P_p \neq g'$ , and let  $k' = 0$  otherwise. Let

$$K'_p = p(p^3 - 1)(p^3 + 1 - p\alpha)k'.$$

Then  $K'_p \neq 0$ . Moreover, if  $\ell \nmid K'_p$  then  $A[\ell]$  does not have a Jordan–Hölder filtration as in Lemma 29 with  $\det(U) = 1$  or  $\chi^3$ .

*Proofs of Lemmas 30 and 31.* For now, let  $p$  be a prime of good reduction for  $A$ , and suppose that  $\ell \neq p$ . Suppose  $A[\ell]$  has a Jordan–Hölder filtration  $0 \subset U \subset A[\ell]$  where  $U$  and  $A[\ell]/U$  are 3-dimensional (i.e., as in Lemma 29). Then  $\det(U) = \chi^r$  with  $0 \leq r \leq 3$ . Let  $\sigma_p \in G_{\mathbb{Q}}$  denote a Frobenius element at  $p$ . Let  $M = M(\sigma_p)$  as in Lemma 29. Then  $\det(M) \equiv p^r \pmod{\ell}$ . Moreover, from the lemma,

$$P_p(x) \equiv \det(xI - M) \det(xI - pM^{-1}) \pmod{\ell}.$$

Write

$$\det(xI - M) \equiv x^3 + ux^2 + vx - p^r \pmod{\ell}.$$

Then

$$\begin{aligned} \det(xI - pM^{-1}) &= -p^{-r} \cdot x^3 \cdot \det(px^{-1}I - M) \\ &\equiv x^3 - p^{1-r}vx^2 - p^{2-r}ux - p^{3-r} \pmod{\ell}. \end{aligned}$$

Let

$$a = \begin{cases} u & \text{if } r = 0 \text{ or } 1 \\ -p^{-1}v & \text{if } r = 2 \\ -p^{-2}v & \text{if } r = 3 \end{cases} \quad b = \begin{cases} v & \text{if } r = 0 \text{ or } 1 \\ -u & \text{if } r = 2 \\ -p^{-1}u & \text{if } r = 3. \end{cases}$$

If  $r = 1$  or  $2$ , then

$$P_p(x) \equiv (x^3 + ax^2 + bx - p)(x^3 - bx^2 - pax - p^2) \pmod{\ell}. \quad (1.6)$$

If  $r = 0$  or  $3$  then

$$P_p(x) \equiv (x^3 + ax^2 + bx - 1)(x^3 - pbx^2 - p^2ax - p^3) \pmod{\ell}. \quad (1.7)$$

We now suppose that  $\ell \nmid K_p$  and prove Lemma 30 which corresponds to  $r = 1$  or  $2$ . We thus suppose that (1.6) holds. Comparing the coefficients of  $x^5$  in (1.6) we have that  $a \equiv b + \alpha \pmod{\ell}$ . Substituting this into (1.6) and comparing the coefficients of  $x^4$  and  $x^3$  we obtain

$$\begin{aligned} b^2 + (p + \alpha - 1) \cdot b + (p\alpha + \beta) &\equiv 0 \pmod{\ell} \\ (p + 1) \cdot b^2 + 2p\alpha \cdot b + (p^2 + p\alpha^2 + p + \gamma) &\equiv 0 \pmod{\ell}. \end{aligned}$$

Eliminating  $b^2$  we obtain the following congruence which is linear in  $b$ :

$$-(p - 1)(p + 1 - \alpha) \cdot b + (-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma) \equiv 0 \pmod{\ell}.$$

As  $\ell \nmid K_p$  we have  $\ell \nmid (p - 1)(p + 1 - \alpha)$ , and so we can solve for  $b \pmod{\ell}$ . It follows that  $b \equiv \delta$  and  $a \equiv b + \alpha \equiv \epsilon \pmod{\ell}$  where  $\delta$  and  $\epsilon$  are given by (1.2). Substituting into (1.6), we see that  $P_p \equiv g \pmod{\ell}$  where  $g$  is given by (1.3). Thus  $\ell$  divides the greatest common divisor of the numerators of the coefficients of  $P_p - g$  showing that  $\ell \mid k$  (in the notation of Lemma 30). As  $k \mid K_p$  and  $\ell \nmid K_p$  we obtain a contradiction. Thus if  $\ell \nmid K_p$  then  $A[\ell]$  does not have a Jordan–Hölder filtration as in Lemma 29 with  $\det(U) = \chi$  or  $\chi^2$ .

We need to show that  $K_p \neq 0$ . We are supposing that  $p + 1 \neq \alpha$  thus we need to show that  $P_p \neq g$ . Suppose  $P_p = g$ . As  $g$  is the product of two cubic polynomials, it follows that  $P_p$  has at least two real roots. By Lemma 25, we see that  $(x^2 - p)^2 \mid P_p$ . It follows that  $P_p = g$  must have two rational roots. Since all the roots have absolute value  $\sqrt{p}$ , this is a contradiction. We deduce that  $K_p \neq 0$  as required. This completes the proof of Lemma 30. The proof of Lemma 31 is practically identical.  $\square$

## Conclusion

The following theorem summarizes the results of this section.

**Theorem 32.** *Let  $A$  be a principally polarized abelian variety over  $\mathbb{Q}$ . Assume that there is a prime  $q$  for which the special fibre of the Néron model of  $A$  at  $q$  has toric dimension 1. Let  $S$  be a finite set of such primes. Let  $\ell$  be a prime number not dividing  $\gcd(\{q \cdot \#\Phi_q : q \in S\})$ . Let  $T$  be a non-empty set of primes of good reduction for  $A$ . Let*

$$B_3(T) = \gcd(\{K_p : p \in T\}), \quad B_4(T) = \gcd(\{K'_p : p \in T\}),$$

where  $K_p$  and  $K'_p$  are defined in Lemmas 30 and 31. Let

$$B(T) = \text{lcm}(B_2(T), B_3(T), B_4(T)),$$

where  $B_2(T)$  is defined in page 23. If  $\ell \nmid B(T)$ , then  $\bar{\rho}_{A,\ell}$  is surjective.

*Proof.* By Theorem 4, we know that  $\bar{\rho}_{A,\ell}$  is either reducible or surjective. Lemmas 28, 30 and 31 ensure that  $\bar{\rho}_{A,\ell}$  cannot be reducible. Hence, it must be surjective.  $\square$

## 1.9 An Application

As an application of the above, we will prove the following result:

**Proposition 33.** *Let  $C/\mathbb{Q}$  be the genus 3 hyperelliptic curve*

$$y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5,$$

and let  $J$  denote its Jacobian. Let  $\ell \geq 3$  be a prime. Then  $\bar{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \text{GSp}_6(\mathbb{F}_{\ell})$ .

*Proof.* We used `Magma` [BCP97] to implement the method described in this section. The model

$$y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5 \tag{1.8}$$

for the curve  $C$  has good reduction at 2. Let  $J$  be the Jacobian of  $C$ . This has conductor  $N = 8907 = 3 \times 2969$  (the algorithm used by `Magma` for computing the conductor and the component groups is described in [DDMM17]). As  $N$  is squarefree, the Jacobian  $J$  is semistable. Completing the square in (1.8), we see that the curve  $C$  has the following Weierstrass model:

$$y^2 = x^8 + 2x^7 + 5x^6 + 6x^5 + 4x^4 + 2x^3 + x^2 + 2x + 1.$$

Denote the polynomial on the right-hand side by  $f$ . Then

$$f \equiv (x+1)(x+2)^2(x^2+x+2)(x^3+2x^2+2x+2) \pmod{3}$$

and

$$f \equiv (x+1)(x+340)(x+983)^2(x^2+x+1)(x^2+663x+1350) \pmod{2969}.$$

Here the non-linear factors in both factorizations are irreducible. As  $f$  has precisely one double root in  $\bar{\mathbb{F}}_3$  and one double root in  $\bar{\mathbb{F}}_{2969}$  with all other roots simple, we see that the Néron models for  $J$  at 3 and 2969 have special fibres with toric dimension 1 (see the Appendix by Emmanuel Kowalski to [Hal11]). We found that  $\#\Phi_3 = \#\Phi_{2969} = 1$ . Thus the image of  $\bar{\rho}_{J,\ell}$  contains a transvection for all  $\ell \geq 3$ .

We now suppose  $\ell \geq 5$ . By Theorem 4, we know that  $\bar{\rho}_{J,\ell}$  is either reducible or surjective. Keeping up with the notation introduced above, we take our chosen set of primes of good reduction to be  $T = \{2, 5, 7\}$ . We note that

$$\#J(\mathbb{F}_2) = 2^5, \quad \#J(\mathbb{F}_5) = 2^7, \quad \#J(\mathbb{F}_7) = 2^6 \times 7.$$

It follows from Lemma 26 that  $J[\ell]$  does not have 1- or 5-dimensional Jordan–Hölder factors. Next we consider the existence of 2- or 4-dimensional irreducible subspaces. The possible values  $M \mid N$  such that  $S_2^{\text{new}}(M) \neq 0$  are  $M = 2969$  and  $M = 8907$ , where the dimensions are 247 and 495 respectively. The resultants  $R(M, p)$  are too large to reproduce here. For example, we indicate that  $R(8907, 7) \sim 1.63 \times 10^{2344}$ . However,

$$R(M, T) = \gcd(2 \cdot R(M, 2), 5 \cdot R(M, 5), 7 \cdot R(M, 7)) = \begin{cases} 2^4 & M = 2969, \\ 2^{22} & M = 8907. \end{cases}$$

It follows from Lemma 28 that  $J[\ell]$  does not have 2- or 4-dimensional irreducible subspaces. It remains to eliminate the possibility of a Jordan–Hölder filtration  $0 \subset U \subset J[\ell]$  where both  $U$  and  $J[\ell]/U$  are 3-dimensional. In the notation of Lemma 30,

$$K_2 = 14, \quad K_5 = 6900, \quad K_7 = 83202.$$

Then  $\gcd(K_2, K_5, K_7) = 2$ . Lemma 30 allows us to discard the case where  $\det(U) =$

$\chi$  or  $\chi^2$ . Moreover,

$$K'_2 = 154490, \quad K'_5 = 15531373270380, \quad K'_7 = 10908656905042386.$$

Then  $\gcd(K'_2, K'_3, K'_7) = 2$ . Using Lemma 31, we can conclude that the case where  $\det(U) = 1$  or  $\chi^3$  cannot happen. It follows that  $\bar{\rho}_{J,\ell}$  is irreducible, and hence surjective, for all  $\ell \geq 5$ .

It remains to show that  $\bar{\rho}_{J,3}$  is surjective. Denote  $\bar{\rho} = \bar{\rho}_{J,3}$ . Write  $G = \bar{\rho}(G_{\mathbb{Q}})$ . For a prime  $p$  of good reduction, let  $\sigma_p \in G_{\mathbb{Q}}$  denote a Frobenius element at  $p$  and  $\bar{P}_p \in \mathbb{F}_3[t]$  be the characteristic polynomial of  $\sigma_p$  acting on  $J[3]$ . Let  $N_p$  be the multiplicative order of the image of  $t$  in the algebra  $\mathbb{F}_3[t]/\bar{P}_p$ . It is immediate that  $N_p$  divides the order of  $\bar{\rho}(\sigma_p)$  and hence divides the order of  $G$ . We computed

$$N_2 = 2^3 \times 5, \quad N_5 = 2 \times 13, \quad N_{19} = 7, \quad N_{37} = 2 \times 3^2.$$

Thus the order of  $G$  is divisible by  $2^3 \times 3^2 \times 5 \times 7 \times 13$ . We checked that the only subgroups of  $\mathrm{GSp}_6(\mathbb{F}_3)$  with order divisible by this are  $\mathrm{Sp}_6(\mathbb{F}_3)$  and  $\mathrm{GSp}_6(\mathbb{F}_3)$ . As the mod 3 cyclotomic character is surjective on  $G_{\mathbb{Q}}$ , we have that  $G = \mathrm{GSp}_6(\mathbb{F}_3)$ . This completes the proof of the corollary.  $\square$

## Chapter 2

# Serre's Uniformity Conjecture

In [Ser71], Serre famously proved that, given an elliptic curve  $E$  defined over a number field  $K$  without complex multiplication, there exists a prime number  $p_{E,K}$  such that, for any prime  $p > p_{E,K}$ , the image of the residual mod  $p$  Galois representation  $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$  attached to  $E$  is the whole of  $\mathrm{GL}_2(\mathbb{F}_p)$ . In the very same paper, Serre raised the following question:

Given a number field  $K$ , is there a prime number  $p_K$  such that, for any elliptic curve  $E$  over  $K$  without complex multiplication, the residual mod  $p$  Galois representation  $\bar{\rho}_{E,p}$  is surjective onto  $\mathrm{GL}_2(\mathbb{F}_p)$ , whenever  $p$  is a prime larger than  $p_K$ ?

This conjecture remains open today, but, over the last forty years, there has been a lot of progress towards a proof for  $K = \mathbb{Q}$  — it is believed that, in this case,  $p_K = 37$ . The classification of maximal subgroups of  $\mathrm{GL}_2(\mathbb{F}_p)$  plays a central role in the general strategy used to tackle this problem: the aim is to try to show that, for  $p$  large enough, there are no elliptic curves without complex multiplication for which the image of  $\bar{\rho}_{E,p}$  is contained in any of these maximal subgroups. The maximal subgroups not containing  $\mathrm{SL}_2(\mathbb{F}_p)$  are the Borel subgroups, the normalisers of (split and non-split) Cartan subgroups and a few exceptional ones. The exceptional cases were treated by Serre in [Ser81]. Mazur, in [MG78], treated the Borel case, exhibiting all the possible prime degrees of rational isogenies admitted by elliptic curves over  $\mathbb{Q}$ : for elliptic curves over  $\mathbb{Q}$  without complex multiplication, the possible prime degrees of rational isogenies are 2, 3, 5, 7, 11, 13, 17 and 37. Finally, Bilu and Parent [BP11] and Bilu, Parent and Rebolledo [BPR13] studied the case of the normaliser of a split Cartan. In [BPR13], they proved that if  $E$  is an elliptic curve over  $\mathbb{Q}$ , and  $p \geq 11$  is a prime different from 13, then the image of  $\bar{\rho}_{E,p}$  is not contained

in the normaliser of a split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . The verification of the conjecture is thus reduced to the proof that, for  $p$  large enough, the image of the mod  $p$  Galois representation of any non-CM elliptic curve over  $\mathbb{Q}$  is not contained in the normaliser of any non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ .

For deep reasons, this last case seems, for the moment, out of reach. However, in the direction of such a result, we prove, in this chapter, the following:

**Theorem 34.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$ . Suppose, moreover, that  $E$  admits a non-trivial cyclic  $\mathbb{Q}$ -isogeny. Then, for  $p > 37$ , the residual mod  $p$  Galois representation  $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$  is surjective.*

Mazur [MG78] proved that if  $p \geq 11$  is a prime different from 13, then any elliptic curve over  $\mathbb{Q}$  with a  $\mathbb{Q}$ -rational  $p$  isogeny has potentially good reduction at every prime  $\ell > 2$ . In order to prove this, Mazur introduced the concept of *formal immersion*, a concept which will be central in our discussion. We say that a morphism  $f : X \rightarrow Y$  between two schemes is a *formal immersion at a point  $P \in X$*  if the induced morphism of completed local rings at  $P$

$$\hat{f}^* : \hat{\mathcal{O}}_{Y,f(P)} \rightarrow \hat{\mathcal{O}}_{X,P}$$

is surjective. We will briefly describe his method.

Say that  $E$  is an elliptic curve over  $\mathbb{Q}$  and that  $C$  is a  $\mathbb{Q}$ -rational subgroup of  $E(\bar{\mathbb{Q}})$  of order  $p$ , where  $p \geq 11$  is a prime different from 13. Then  $(E, C)$  is a representative of an isomorphism class of pairs which, by the moduli interpretation of  $X_0(p)$ , corresponds to a non-cuspidal rational point  $P$  of  $X_0(p)$ . Moreover, since  $E$  is assumed to have potentially multiplicative reduction at a prime  $\ell > 2$  (for simplicity, we will take  $\ell$  to be different from  $p$ ), the reduction of  $P$  mod  $\ell$  coincides with a cusp. By an application of the Atkin–Lehner involution if necessary, we may assume that this cusp is  $\infty$ . Mazur, in [Maz77] and [MG78], proves two fundamental claims that make the remainder of the argument work: firstly, he proves that  $J_0(p) := \mathrm{Jac}(X_0(p))$  has a non-trivial rank 0 quotient  $A$  defined over  $\mathbb{Q}$ ; secondly, he shows that the morphism

$$f : X_0(p)_{\mathbb{Z}_\ell} \rightarrow A_{\mathbb{Z}_\ell},$$

defined by composing the Abel–Jacobi map  $X_0(p)_{\mathbb{Z}_\ell} \rightarrow J_0(p)_{\mathbb{Z}_\ell}$  with the natural projection  $J_0(p)_{\mathbb{Z}_\ell} \rightarrow A_{\mathbb{Z}_\ell}$  is a formal immersion at  $\infty_\ell$ , the reduction of  $\infty$  to the special fibre. Here,  $X_0(p)_{\mathbb{Z}_\ell}$  stands for the minimal regular model of  $X_0(p)$  over  $\mathbb{Z}_\ell$ ,

and  $A_{\mathbb{Z}_\ell}$  and  $J_0(p)_{\mathbb{Z}_\ell}$  for the Néron models of  $A$  and  $J_0(p)$  over  $\mathbb{Z}_\ell$ . As we have seen,  $P$  reduces to  $\infty_\ell$ , which means that  $f(P)$  will reduce to  $0 \pmod{\ell}$ . However,  $f(P)$  is rational, and, since  $A(\mathbb{Q})$  is finite, it must be a torsion point of  $A$ . Now,  $\text{Tors } A(\mathbb{Q})$  injects, by reduction mod  $\ell$ , into  $A(\mathbb{F}_\ell)$ . Therefore,  $f(P) = 0$ . Let

$$s_\infty : \text{Spec } \mathbb{Z}_\ell \rightarrow X_0(p)_{\mathbb{Z}_\ell} \quad \text{and} \quad s_P : \text{Spec } \mathbb{Z}_\ell \rightarrow X_0(p)_{\mathbb{Z}_\ell}$$

be, respectively, the sections corresponding to  $\infty$  and  $P$ . We find that  $f \circ s_\infty = f \circ s_P$ . Therefore,

$$\hat{s}_\infty^* \circ \hat{f}^* = \hat{s}_P^* \circ \hat{f}^*,$$

where  $\hat{s}_\infty^*$ ,  $\hat{s}_P^*$  and  $\hat{f}^*$  are the induced maps on the completed local rings at  $\infty_\ell$ ,  $P_\ell$  and  $0_\ell$ , the mod  $\ell$  reductions of  $\infty$ ,  $P$  and  $0$ , respectively. But since  $\hat{f}^*$  is surjective, this yields  $\hat{s}_\infty^* = \hat{s}_P^*$ , implying that  $P = \infty$ . However, we asserted above that  $P$  is non-cuspidal, and, therefore, we have a contradiction.

We might try to apply this strategy to other modular curves, such as  $X_{\text{ns}}^+(p)$ . However, assuming the Birch and Swinnerton-Dyer conjecture, we can show that the Jacobian of  $X_{\text{ns}}^+(p)$  does not have a non-trivial rank 0 quotient defined over  $\mathbb{Q}$ . Indeed, by Chen [Che98] (see Theorem 40 in Section 2.3), the Jacobian of  $X_{\text{ns}}^+(p)$  is isogenous to the Jacobian of  $X_0^+(p^2) := X_0(p^2)/w_{p^2}$ , and the  $L$ -functions of every weight 2 cusp form of  $\text{Jac}(X_0^+(p^2))$  have sign  $-1$  in their functional equations. By the Birch and Swinnerton-Dyer conjecture, every non-trivial quotient of  $\text{Jac}(X_{\text{ns}}^+(p))$  will then have Mordell–Weil rank  $\geq 1$ . But, as we have seen, the existence of a non-trivial rank 0 quotient is necessary for Mazur’s method to work.

Nevertheless, using a result by Imin Chen [Che98], later generalized by de Smit and Edixhoven [dE00], Darmon and Merel [DM97] proved the following result.

**Theorem 35** ([DM97, Proposition 7.1]). *Let  $r = 2$  or  $3$ , and let  $p > 3$  be a prime. There exists a non-trivial optimal quotient  $A$  of the Jacobian  $J_{0,\text{ns}}^+(r, p)$  of the curve*

$$X_0(r) \times_{X(1)} X_{\text{ns}}^+(p)$$

*such that  $A(\mathbb{Q})$  is finite. Moreover, the kernel of the canonical projection  $J_{0,\text{ns}}^+(r, p) \rightarrow A$  is stable under the action of the Hecke operators  $T_n$  for  $n$  coprime to  $p$ .*

With it, they were able to show the following.

**Theorem 36** ([DM97, Theorem 8.1]). *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  admitting a  $\mathbb{Q}$ -rational  $r$ -isogeny, where  $r = 2$  or  $3$ . Suppose that there exists a prime  $p > 3$*

such that the image of  $\bar{\rho}_{E,p}$  is contained in the normaliser of a non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Then  $j(E) \in \mathbb{Z}[\frac{1}{p}]$ .

In fact, their methods work not only when  $r = 2$  or  $3$ , but whenever  $X_0(r)$  has genus 0; in other words, whenever  $r \in \{2, 3, 5, 7, 13\}$  (subject to the condition that, in the results aforementioned,  $p \notin \{2, 3, 5, 7, 13\}$ ). Therefore, we have

**Theorem 37.** *Set  $\Sigma := \{2, 3, 5, 7, 13\}$ . Let  $E$  be an elliptic curve over  $\mathbb{Q}$  admitting a  $\mathbb{Q}$ -rational  $r$ -isogeny for some  $r \in \Sigma$ . Suppose that there exists a prime  $p \notin \Sigma$  such that the image of  $\bar{\rho}_{E,p}$  is contained in the normaliser of a non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Then  $j(E) \in \mathbb{Z}[\frac{1}{p}]$ .*

The proof of this theorem is essentially the same as the one presented by Darmon and Merel [DM97] for Theorem 36. Sections 2.3 and 2.4 will provide an outline of it, the details being referred to [DM97].

There are essentially two steps in the proof of Theorem 34. The first one is to prove that, under the conditions of Theorem 37, we can actually conclude that  $j(E) \in \mathbb{Z}$ . The second one consists, firstly, in noting that, for  $p > 37$ , the image of the mod  $p$  Galois representation of any non-CM elliptic curve over  $\mathbb{Q}$  will be either contained in the normaliser of a non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ , or will be the whole of  $\mathrm{GL}_2(\mathbb{F}_p)$ ; and, secondly, in checking that, for  $r \in \{2, 3, 5, 7, 13\}$ , the non-CM elliptic curves corresponding to the rational points of  $X_0(r)$  with integral  $j$ -invariant have surjective mod  $p$  Galois representations. Separately, we check the same thing for the non-cuspidal rational points of  $X_0(11)$ ,  $X_0(17)$  and  $X_0(37)$ . This will yield the theorem.

## 2.1 Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

An essential ingredient used in the proof of Theorem 34 is Dixon's classification of the maximal subgroups of  $\mathrm{GL}_2(\mathbb{F}_p)$ . We start this section by introducing some terminology, namely the concepts of *Borel* and *Cartan subgroups*.

Let  $p$  be an odd prime number. A *Borel subgroup* of  $\mathrm{GL}_2(\mathbb{F}_p)$  is any conjugate to the subgroup of upper triangular matrices, while a *Cartan subgroup* is a maximal semi-simple commutative subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Cartan subgroups are usually divided in two classes: *split* and *non-split*. A subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$  is said to be a *split Cartan subgroup* if it is conjugate to the subgroup of non-singular diagonal matrices.

Consider now  $\mathrm{GL}_2(\mathbb{F}_p)$  as a subgroup of  $\mathrm{GL}_2(\mathbb{F}_{p^2})$ . A subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$  is said to be a *non-split Cartan subgroup* if it is conjugate (in  $\mathrm{GL}_2(\mathbb{F}_{p^2})$ ) to

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix} : \alpha \in \mathbb{F}_{p^2}^\times \right\}.$$

**Theorem 38** (Dixon). *Let  $p > 2$  be a prime and let  $G$  be a subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . If  $p \mid |G|$ , then one of the following is true:*

- (i)  $\mathrm{SL}_2(\mathbb{F}_p) \subseteq G$ ; or
- (ii)  $G$  is contained in a Borel subgroup.

*If, on the other hand,  $p \nmid |G|$ , then one of the following is true:*

- (iii)  $G$  is contained in the normalizer of a Cartan subgroup; or
- (iv) the image of  $G$  in  $\mathrm{PGL}_2(\mathbb{F}_p)$  is isomorphic to  $A_4$ ,  $S_4$  or  $A_5$ .

*Proof.* A proof can be found in [Ser71]. □

Subgroups of  $\mathrm{GL}_2(\mathbb{F}_p)$  falling in case (iv) of Theorem 38 are known as exceptional subgroups.

The general strategy used in the approach to Serre's question is to prove that, for  $p$  large enough, the image  $G$  of  $\bar{\rho}_{E,p}$  does not fall in cases (ii), (iii) and (iv). This would mean that  $\mathrm{SL}_2(\mathbb{F}_p) \subseteq G$ . However,  $\det \bar{\rho}_{E,p} = \chi_p$ , and  $\chi_p$ , the mod  $p$  cyclotomic character, is surjective. Hence,  $G = \mathrm{GL}_2(\mathbb{F}_p)$ .

## 2.2 The Modular Curve $X_{0,\mathrm{ns}}^+(r, p)$

As stated in the declaration, this section, section 2.3 and section 2.4 are based on [DM97]. In particular, no result in these three sections is new. However, we tried to include some details in some of the arguments that can be found there.

Let  $p$  be a prime. The modular curve  $X(p)$  parametrising isomorphism classes of pairs  $(E, (P, Q))$ , where  $E$  is an elliptic curve and  $(P, Q)$  is an  $\mathbb{F}_p$ -basis for  $E[p]$ , has a right action of  $\mathrm{GL}_2(\mathbb{F}_p)$ , as we now explain. If

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

then we set  $(E, (P, Q)) \cdot g := (E, (aP + cQ, bP + dQ))$ .

Now, let  $p$  be an odd prime. Denote by  $N_{\text{sp}}$  the normaliser of a split Cartan subgroup of  $\text{GL}_2(\mathbb{F}_p)$ , and by  $N_{\text{ns}}$  the normaliser of a non-split one. We set

$$X_{\text{sp}}^+(p) := X(p)/N_{\text{sp}} \quad \text{and} \quad X_{\text{ns}}^+(p) := X(p)/N_{\text{ns}}.$$

Clearly, the  $j$ -invariant map  $j : X(p) \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  factors through  $X_{\text{sp}}^+(p)$  and  $X_{\text{ns}}^+(p)$ . We shall denote the maps obtained from  $X_{\text{sp}}^+(p)$  and  $X_{\text{ns}}^+(p)$  to  $\mathbb{P}_{\mathbb{Q}}^1$  by  $j$  as well, and keep calling them  $j$ -invariant maps.

**Lemma 39.** *The curve  $X_{\text{ns}}^+(p)$  has  $(p-1)/2$  cusps. Each of these cusps is defined over  $\mathbb{Q}(\zeta_p)^+$ . They form a single Galois orbit under the action of  $\text{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})$ . Moreover, each of them has ramification degree  $p$  with respect to the  $j$ -invariant map.*

*Proof.* This is a direct application of the methods for computing cusps presented in Chapter 10 of [KM85].  $\square$

Let  $r$  be a prime. It is well-known that  $X_0(r)$  has two  $\mathbb{Q}$ -rational cusps: one of them with ramification degree  $r$ , the other with ramification degree 1. Analytically,  $X_0(r)$  can be described as the quotient of  $\mathcal{H}^*$  — the extended upper half complex plane — by the congruence subgroup  $\Gamma_0(r)$ . The cusps correspond to the classes of  $\infty$  and 0. The cusp  $\infty$  has ramification degree 1, while the cusp 0 has ramification degree  $r$ .

From now on, we will always assume that  $r \neq p$ . We define the following curves:

$$X_{0,\text{sp}}^+(r,p) := X_0(r) \times_{X(1)} X_{\text{sp}}^+(p) \quad \text{and} \quad X_{0,\text{ns}}^+(r,p) := X_0(r) \times_{X(1)} X_{\text{ns}}^+(p).$$

The discussion above leads us to the conclusion that  $X_{0,\text{ns}}^+(r,p)$  has  $p-1$  cusps, which we shall denote by

$$\infty_1, \dots, \infty_{\frac{p-1}{2}}, 0_1, \dots, 0_{\frac{p-1}{2}}.$$

These two sets of cusps  $(\infty_1, \dots, \infty_{\frac{p-1}{2}})$  and  $(0_1, \dots, 0_{\frac{p-1}{2}})$  are two Galois orbits for the action of  $\text{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})$ . The cusps corresponding to  $\infty$  have ramification degree  $p$ .

## 2.3 Chen's Isogeny

For ease of notation, write  $X_0^+(p^2)$  for the curve  $X_0(p^2)/w_{p^2}$ , where  $w_{p^2}$  is the Atkin–Lehner involution. In [Che98], Chen proved the following result:

**Theorem 40** ([Che98, Theorem 1]). *The Jacobian of  $X_{\text{ns}}^+(p)$  is isogenous to the new part of the Jacobian of  $X_0^+(p^2)$ .*

However, his proof, making use of the Selberg trace formula, was not constructive. It was later proven by Chen [Che00] that a construction by Darmon and Merel [DM97], which we now reproduce, is, in fact, an explicit construction of Chen's isogeny.

In order to describe this construction, we will need to introduce some notation. Let  $N_{\text{sp}}$  be the normaliser of a split Cartan subgroup of  $\text{GL}_2(\mathbb{F}_p)$ , and  $N_{\text{ns}}$  the normaliser of a non-split Cartan subgroup. Also, denote by  $B^+$  and  $B^-$  the subgroups of  $\text{GL}_2(\mathbb{F}_p)$  consisting of upper triangular matrices and lower triangular matrices, respectively. Define

$$X'(p) := X(p)/(N_{\text{sp}} \cap N_{\text{ns}}).$$

For  $r \in \{1, 2, 3, 5, 7, 13\}$ , there are two natural projections associated to  $X_0(r) \times_{X(1)} X'(p)$ :

$$X_0(r) \times_{X(1)} X'(p) \rightarrow X_{0,\text{sp}}^+(r, p) \quad \text{and} \quad X_0(r) \times_{X(1)} X'(p) \rightarrow X_{0,\text{ns}}^+(r, p).$$

We obtain a correspondence  $X_{0,\text{sp}}^+(r, p) \dashrightarrow X_{0,\text{ns}}^+(r, p)$ , which gives rise to a homomorphism

$$\phi : \text{Jac}(X_{0,\text{sp}}^+(r, p)) \rightarrow \text{Jac}(X_{0,\text{ns}}^+(r, p)).$$

Since we have an isomorphism between  $X_{\text{sp}}^+(p)$  and  $X_0^+(p^2)$ , we can substitute  $\text{Jac}(X_{0,\text{sp}}^+(r, p))$  by the Jacobian of  $X_0^+(r, p^2) := X_0(r) \times_{X(1)} X_0^+(p^2)$  in the homomorphism  $\phi$ .

**Lemma 41** ([DM97, Lemma 6.2 (a)]). *Under  $\phi$ , the image of the  $p$ -old part of  $\text{Jac}(X_0^+(r, p^2))$  is trivial.*

*Proof.* Define the  $p$ -old part of  $\text{Pic}(X_{0,\text{ns}}^+(r, p))$  as the image of

$$p^* : \text{Pic}(X_0(r)) \rightarrow \text{Pic}(X_{0,\text{ns}}^+(r, p)),$$

the pull-back of the projection to  $X_0(r)$ . Since  $X_0(r)$  has genus 0, the  $p$ -old part of  $\text{Jac}(X_{0,\text{ns}}^+(r, p))$  is trivial. Therefore, in order to prove the lemma, we only need to

show that the image under  $\phi$  of an old divisor is an old divisor.

Under our isomorphism between  $X_{0,\text{sp}}^+(r, p)$  and  $X_0^+(r, p^2)$ , an old divisor in the curve  $X_{0,\text{sp}}^+(r, p)$  has an inverse image in  $X_0(r) \times_{X(1)} X(p)$  which is the image of a  $B^+$  and a  $B^-$ -invariant divisor. Since

$$N_{\text{ns}}B^+ = N_{\text{ns}}B^- = \text{GL}_2(\mathbb{F}_p),$$

the image in  $X_{0,\text{ns}}^+(r, p)$  of such a divisor is  $\text{GL}_2(\mathbb{F}_p)$ -invariant, meaning that it must be an old divisor of  $X_{0,\text{ns}}^+(r, p)$ .  $\square$

We then obtain a homomorphism

$$\text{Jac}(X_0^+(r, p^2))^{p\text{-new}} \rightarrow \text{Jac}(X_{0,\text{ns}}^+(r, p)),$$

which, by Chen [Che00], is precisely Chen's isogeny. Moreover, it follows from this explicit description that if  $n \geq 1$  is an integer coprime to  $p$ , then Chen's isogeny commutes with the Hecke operators  $T_n$ . Summing up,

**Theorem 42** ([DM97, Theorem 6.1]). *If  $r \in \{1, 2, 3, 5, 7, 13\}$ , there is an isogeny between  $J_{0,\text{ns}}^+(r, p)$  and  $\text{Jac}(X_0^+(r, p^2))^{p\text{-new}}$  which, for any integer  $n \geq 1$  coprime to  $p$ , commutes with the action of  $T_n$ .*

The existence of such an isogeny is of fundamental importance to prove the following result:

**Theorem 43** ([DM97, Proposition 7.1]). *Let  $r \in \{2, 3, 5, 7, 13\}$  and let  $p$  be a prime number not in there. There exists a non-trivial optimal quotient  $A$  of  $J_{0,\text{ns}}^+(r, p)$ , defined over  $\mathbb{Q}$ , such that  $A(\mathbb{Q})$  is finite. Moreover, if  $n \geq 1$  is an integer coprime to  $p$ , the kernel of the canonical projection  $J_{0,\text{ns}}^+(r, p) \rightarrow A$  is stable under the Hecke operators  $T_n$ .*

In order to prove this result, we will introduce some notation.

Let  $\mathbb{T}_{\mathbb{Q}}$  denote the semi-simple  $\mathbb{Q}$ -subalgebra of  $\text{End}(\text{Jac}(X_0^+(r, p^2))^{\text{new}}) \otimes \mathbb{Q}$  generated by the Hecke operators  $T_\ell$ , with  $\ell \nmid rp$ . Also, write  $S$  for the vector space  $S_2^{\text{new}}(\Gamma_0(rp^2), \mathbb{Q})^{w_{p^2}}$ , i.e., the space of weight 2 cusp forms of level  $\Gamma_0(rp^2)$  with rational expansion at  $\infty$  and fixed by the action of  $w_{p^2}$ .

We define a pairing  $\langle \cdot, \cdot \rangle : \mathbb{T}_{\mathbb{Q}} \times S \rightarrow \mathbb{C}$  by setting  $\langle T, f \rangle := a_1(Tf)$ . We claim that this pairing is non-degenerate. Indeed, if  $T \in \mathbb{T}_{\mathbb{Q}}$  is such that  $\langle T, f \rangle = 0$  for

every element  $f$  of  $S$ , then this means that  $a_1(Tf) = 0$  for every  $f \in S$ . However,  $\mathbb{T}_{\mathbb{Q}}$  is defined as a subspace of  $\text{End}(\text{Jac}(X_0^+(r, p^2))^{\text{new}}) \otimes \mathbb{Q}$ , which means that  $T$  must equal 0. On the other hand, if  $f \in S$  is that  $a_1(Tf) = 0$  for every  $T \in \mathbb{T}_{\mathbb{Q}}$ , then it is well-known that  $f$  must be 0 (see section 5.8 in [DS05]).

Now, let  $H$  denote the subspace of  $H_1(\text{Jac}(X_0^+(r, p^2))^{\text{new}}(\mathbb{C}), \mathbb{Q})$  fixed by complex conjugation. We define the pairing  $(\cdot, \cdot) : S \times H \rightarrow \mathbb{C}$  by

$$(f, \gamma) \mapsto 2\pi i \int_{\gamma'} f(z) dz,$$

where  $\gamma'$  is any lift of  $\gamma$  to  $H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})$ . This pairing is non-degenerate and the Hecke operators are self-adjoint with respect to it (see [DM97]). Moreover,  $H$  is a  $\mathbb{T}_{\mathbb{Q}}$ -module of rank 1 (we refer, once again, to [DM97]).

Consider the geodesic in  $\mathcal{H}^*$  that connects 0 to  $\infty$  and the path  $e$  it defines in  $X_0^+(r, p^2)$ . According to the Drinfeld–Manin theorem [Cre97, Theorem 2.1.3],  $e \in H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})$ . Moreover, it is fixed under complex conjugation. Hence,  $e \in H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})^+$ .

**Lemma 44** ([DM97, Proposition 7.2]). *The path  $e$  described above does not belong to the old part of  $H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})$ .*

Before proving Theorem 43, let us define the concept of *optimal quotient*. Let  $A$  and  $B$  be abelian varieties and let  $p : A \rightarrow B$  be a surjective homomorphism of abelian varieties. We say that  $B$  is an *optimal quotient* of  $A$  if the kernel of  $p$  is connected.

*Proof of Theorem 43.* As was discussed above, there is an isogeny between  $J_{0, \text{ns}}^+(r, p)$  and  $\text{Jac}(X_0^+(r, p^2))^{p\text{-new}}$  which commutes with the Hecke operators  $T_n$ , whenever  $n$  is coprime to  $p$ . Thus, we are reduced to proving the result for  $\text{Jac}(X_0^+(r, p^2))^{p\text{-new}}$ . Note that  $\text{Jac}(X_0^+(r, p^2))^{\text{new}}$  is an optimal quotient of  $\text{Jac}(X_0^+(r, p^2))^{p\text{-new}}$ . Given an optimal quotient  $B$  of  $J_0^{\text{new}}(N)$ , and writing  $p : J_0^{\text{new}}(N) \rightarrow B$  for the canonical projection, we know, by a result of Ribet (see, for example, section 2 of [MG78]), that  $\ker p$  is stable under the action of Hecke operators. Therefore, the same will be true for any optimal quotient of  $\text{Jac}(X_0^+(r, p^2))^{\text{new}}$ . Hence, we only need to show that  $\text{Jac}(X_0^+(r, p^2))^{\text{new}}$  has a non-trivial optimal quotient with only finitely many rational points.

For ease of notation, set  $J := \text{Jac}(X_0^+(r, p^2))^{\text{new}}$ . Consider the geodesic in  $\mathcal{H}^*$  that connects 0 to  $\infty$  and the path  $e$  it defines in  $X_0^+(r, p^2)$ . According to the Drinfeld–Manin theorem,  $e \in H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})$ . Moreover, it is fixed under complex conjugation. Hence,  $e \in H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})^+$ . Write  $e'$  for the image of  $e$  in  $H$ . Define  $I_e$  to be the annihilator of  $e'$  in  $\mathbb{T}_{\mathbb{Z}}$ , i.e.,

$$I_e := \{T \in \mathbb{T}_{\mathbb{Z}} : Te' = 0\}.$$

Set  $A := J/I_e J$ . We now aim to prove that  $A(\mathbb{Q})$  is finite and that  $A$  is not trivial. We start by proving the finiteness of  $A(\mathbb{Q})$ .

Let  $f$  be a normalized eigenform. We define  $I_f$  to be the kernel of the map  $\varphi_f : \mathbb{T}_{\mathbb{Z}} \rightarrow \mathbb{C}$  given by  $\varphi_f(T) = a_1(Tf)$ . Since the pairing  $\langle \cdot, \cdot \rangle$ , defined above, is non-degenerate, we conclude that  $I_f$  is submodule of  $\mathbb{T}_{\mathbb{Z}}$  of rank (as a  $\mathbb{Z}$ -module)  $\text{rk } \mathbb{T}_{\mathbb{Z}} - 1$ . For each  $G_{\mathbb{Q}}$ -equivalence class  $[f]$  of normalized eigenforms in  $S_{\mathbb{C}} := S \otimes_{\mathbb{Q}} \mathbb{C}$ , denote by  $A_f$  the quotient  $J/I_f J$ . Since  $J$  is isogenous to  $\prod_{[f]} A_f$ , where  $[f]$  runs through the  $G_{\mathbb{Q}}$ -equivalence classes of normalized eigenforms in  $S_{\mathbb{C}}$ , we get

$$L(J, s) = \prod_{[f]} L(A_f, s).$$

Moreover, we have the following relationship between the  $L$ -functions of  $A_f$  and  $f$ :

$$L(A_f, s) = \prod_{\sigma} L(f^{\sigma}, s),$$

where  $\sigma$  runs through the embeddings of  $K_f$  in  $\mathbb{C}$ . In particular,  $L(A_f, 1) = 0$  if and only if  $L(f^{\sigma}, 1) = 0$  for some embedding  $\sigma$ . This is useful because we have a functional equation for  $L(f, s)$ :

$$(2\pi)^{-s} \Gamma(s) (rp^2)^{s/2} L(f, s) = (rp^2)^{s/2} \int_0^{\infty} f(it) t^{s-1} dt.$$

Therefore,

$$L(f, 1) = 2\pi \int_0^{\infty} f(it) dt.$$

Thus,

$$L(f, 1) = 2\pi i \int_e f(z) dz = (f, e'),$$

where the pairing  $(\cdot, \cdot)$  was extended to  $S_{\mathbb{C}} \times H \rightarrow \mathbb{C}$ . We then have  $L(f, 1) = 0$  if and only if  $(f, e') = 0$ .

Suppose that  $f$  is a normalized eigenform such that  $(f, e') \neq 0$ . Let  $T \in I_e$ . Since  $f$  is an eigenform, there is a constant  $c \in \mathbb{C}$  such that  $Tf = cf$ . Hence,

$$c(f, e') = (Tf, e') = (f, Te') = 0.$$

As  $(f, e') \neq 0$ , by assumption, we conclude that  $c = 0$ . Therefore,  $I_e \subseteq I_f$ .

Suppose now that  $f$  is a normalized eigenform such that  $(f, e') = 0$ . Note that  $H = I_e H \oplus \mathbb{T}_{\mathbb{Q}} e'$ . Since the pairing  $(\cdot, \cdot)$  is non-degenerate, there must exist some  $T \in I_e$  such that  $Tf \neq 0$ . This means that  $I_e \otimes_{\mathbb{Z}} \mathbb{Q} \not\subseteq I_f \otimes_{\mathbb{Z}} \mathbb{Q}$ . As  $\text{rk } I_f = \text{rk } \mathbb{T}_{\mathbb{Z}} - 1$ , the subspace generated by  $I_e \otimes_{\mathbb{Z}} \mathbb{Q}$  and  $I_f \otimes_{\mathbb{Z}} \mathbb{Q}$  must be the whole of  $T_{\mathbb{Q}}$ .

These considerations lead us to the conclusion that

$$A \sim \prod_{L(f,1) \neq 0} A_f.$$

A theorem of Kolyvagin and Logachev [KL89] now tells us that, whenever  $L(f, 1) \neq 0$ ,  $A_f(\mathbb{Q})$  is finite. Therefore,  $A(\mathbb{Q})$  is finite as well.

Now, if  $A$  were trivial, we would have  $(f, e') = 0$ , for all  $f \in S_{\mathbb{C}}$ . However, the non-degeneracy of this pairing means that  $e'$  would be 0 in  $H$ , i.e., it would be in the old part of  $H_1(X_0^+(r, p^2)(\mathbb{C}), \mathbb{Q})$ , which we know is not true.  $\square$

## 2.4 Formal Immersions

We will say that a morphism  $\varphi : X \rightarrow Y$  of schemes is a *formal immersion* at a point  $x \in X$  if the induced homomorphism of the completed local rings  $\hat{\varphi} : \hat{\mathcal{O}}_{Y, \varphi(x)} \rightarrow \hat{\mathcal{O}}_{X, x}$  is surjective.

**Lemma 45.** *Let  $\varphi : X \rightarrow Y$  be a morphism of Noetherian schemes,  $x$  a point of  $X$  and  $y := \varphi(x)$ . Then  $\varphi$  is a formal immersion at  $x$  if and only if the following two conditions are satisfied:*

- (1) *the induced map  $k(y) \rightarrow k(x)$  of residue fields is an isomorphism;*
- (2) *the induced map  $\text{Cotg}_y(Y) \rightarrow \text{Cotg}_x(X)$  of cotangent spaces is surjective.*

*Proof.* It is easy to check that if  $\varphi$  is a formal immersion, then (1) and (2) hold. In order to prove the converse, we are going to show, by induction, that  $\hat{\mathfrak{m}}_x^n =$

$\hat{\varphi}(\hat{\mathfrak{m}}_y^n) + \hat{\mathfrak{m}}_x^{n+1}$  for all  $n \geq 0$ , where  $\hat{\varphi}$  denotes the map on local rings induced by  $\varphi$ .

Clearly, by assumption, we have  $\hat{\mathcal{O}}_{X,x} = \hat{\varphi}(\hat{\mathcal{O}}_{Y,y}) + \hat{\mathfrak{m}}_x$  and  $\hat{\mathfrak{m}}_x = \hat{\varphi}(\hat{\mathfrak{m}}_y) + \hat{\mathfrak{m}}_x^2$ . Let  $n$  be an integer greater than 1 and suppose that we proved the result for all values smaller than  $n$ . Then, if  $\alpha \in \hat{\mathfrak{m}}_x^n$ , we can write  $\alpha = \sum_i \beta_i \gamma_i$ , where  $\beta_i \in \hat{\mathfrak{m}}_x$  and  $\gamma_i \in \hat{\mathfrak{m}}_x^{n-1}$ . Therefore,

$$\beta_i = \hat{\varphi}(s_i) + b_i$$

and

$$\gamma_i = \hat{\varphi}(t_i) + c_i,$$

where  $s_i \in \hat{\mathfrak{m}}_y$ ,  $b_i \in \hat{\mathfrak{m}}_x^2$ ,  $t_i \in \hat{\mathfrak{m}}_y^{n-1}$  and  $c_i \in \hat{\mathfrak{m}}_x^n$ . Thus,

$$\beta_i \gamma_i = (\hat{\varphi}(s_i) + b_i)(\hat{\varphi}(t_i) + c_i) = \hat{\varphi}(s_i t_i) + b_i \hat{\varphi}(t_i) + c_i \hat{\varphi}(s_i) + b_i c_i \in \hat{\varphi}(\hat{\mathfrak{m}}_y^n) + \hat{\mathfrak{m}}_x^{n+1}.$$

Therefore,  $\hat{\varphi}(\hat{\mathfrak{m}}_y^n / \hat{\mathfrak{m}}_y^{n+1}) = \hat{\mathfrak{m}}_x^n / \hat{\mathfrak{m}}_x^{n+1}$  for all  $n \geq 0$ . Hence, if  $a \in \hat{\mathcal{O}}_{X,x}$ , let  $b_0 \in \hat{\mathcal{O}}_{Y,y}$  be such that  $a - \hat{\varphi}(b_0) \in \hat{\mathfrak{m}}_x$ ,  $b_1 \in \hat{\mathfrak{m}}_y$  be such that  $a - \hat{\varphi}(b_0 + b_1) \in \hat{\mathfrak{m}}_x^2$ , and so on. Then, setting  $b = \sum_i b_i$ , we have  $\hat{\varphi}(b) = a$ , which proves the result.  $\square$

Recall that  $X_{0,\text{ns}}^+(r, p)$  has  $(p-1)/2$  cusps corresponding to the cusp  $\infty$  of  $X_0(r)$ . Choose one of them and call it  $\infty$ . Consider the Abel–Jacobi map  $f : X_{0,\text{ns}}^+(r, p) \rightarrow J_{0,\text{ns}}^+(r, p)$  normalized by mapping  $\infty$  to 0. Note that this morphism is not defined over  $\mathbb{Q}$ , but only over  $\mathbb{Q}(\zeta_p)^+$ . From now on,  $\ell$  will denote a prime satisfying  $\ell \equiv \pm 1 \pmod{p}$ . We remark that, in this case,  $\zeta_p + \zeta_p^{-1} \in \mathbb{Z}_\ell$ , and so  $f$  is defined over  $\mathbb{Q}_\ell$ . Therefore, we obtain a morphism

$$f_{\mathbb{Z}_\ell} : X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \rightarrow J_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}.$$

We shall write  $f_s$  for the morphism induced by  $f_{\mathbb{Z}_\ell}$  on the special fibres. Similarly, we shall write  $X_{0,\text{ns}}^+(r, p)_s$  and  $J_{0,\text{ns}}^+(r, p)_s$  for the special fibres of  $X_{0,\text{ns}}^+(r, p)$  and  $J_{0,\text{ns}}^+(r, p)$ , respectively.

**Theorem 46** ([DM97, Lemma 8.2]). *Let  $\Sigma := \{2, 3, 5, 7, 13\}$ ,  $r \in \Sigma$ ,  $p$  a prime number not in  $\Sigma$  and  $\ell$  a prime number such that  $\ell \equiv \pm 1 \pmod{p}$ . Also, let  $\infty \in X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$  be the section associated to the cusp  $\infty$  and  $\infty_\ell \in X_{0,\text{ns}}^+(r, p)_s(\mathbb{F}_\ell)$  the reduction of  $\infty$  mod  $\ell$ . Then the morphism  $f_{\mathbb{Z}_\ell} : X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \rightarrow A_{\mathbb{Z}_\ell}$  is a formal immersion at  $\infty_\ell$ .*

*Proof.* Note that both  $X := X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}$  and  $A_{\mathbb{Z}_\ell}$  are smooth over  $\mathbb{Z}_\ell$ . Then,  $\hat{\mathcal{O}}_{X, \infty_\ell} \cong \mathbb{Z}_\ell[[T]]$  and  $\hat{\mathcal{O}}_{A, 0_\ell} \cong \mathbb{Z}_\ell[[T_1, \dots, T_d]]$ , where  $d = \dim A_{\mathbb{F}_\ell}$ . The closed

immersions  $X_{0,\text{ns}}^+(r,p)_s \hookrightarrow X_{0,\text{ns}}^+(r,p)_{\mathbb{Z}_\ell}$  and  $A_s \hookrightarrow A_{\mathbb{Z}_\ell}$  correspond to the canonical projections

$$\mathbb{Z}_\ell[[T]] \rightarrow \mathbb{F}_\ell[[T]]$$

and

$$\mathbb{Z}_\ell[[T_1, \dots, T_d]] \rightarrow \mathbb{F}_\ell[[T_1, \dots, T_d]].$$

It is then easy to see that the surjectivity of the map  $\mathbb{F}_\ell[[T_1, \dots, T_d]] \rightarrow \mathbb{F}_\ell[[T]]$  induced by  $f$  implies the surjectivity of  $\mathbb{Z}_\ell[[T_1, \dots, T_d]] \rightarrow \mathbb{Z}_\ell[[T]]$ . Hence, we only need to show that  $f_s : X_s \rightarrow A_s$  is a formal immersion at  $\infty_\ell$ .

We will make use of Lemma 45. We only need to show that the map on cotangent spaces  $\text{Cotg}(A_s) \rightarrow \text{Cotg}_{\infty_\ell}(X_s)$  is surjective.

Note that we have a commutative diagram

$$\begin{array}{ccc} \text{Cotg}(A_s) & \xrightarrow{\pi} & \text{Cotg}(J_{0,\text{ns}}^+(r,p)_s) \\ & \searrow f_s^* & \downarrow \alpha \\ & & \text{Cotg}_{\infty_\ell}(X_s) \end{array}$$

where  $\pi$  is an injection.

Since  $A_s$  is not trivial,  $\text{Cotg}(A_s) \neq 0$ . Let  $\theta \in \text{Cotg}(A_s)$  be a non-zero element and consider its image via  $\pi$  — call it  $\omega$ . We can write

$$\omega = \sum_{n=1}^{\infty} a_n(\omega) q^{\frac{n}{p}} \frac{dq^{\frac{1}{p}}}{q^{\frac{1}{p}}},$$

and we already know that  $a_1(T_n(\omega)) = a_n(\omega)$  for  $n$  coprime to  $p$ . Suppose, for contradiction, that  $a_n(\omega) = 0$  for all  $n$  coprime to  $p$ . We claim that, under this assumption, we are forced to conclude that  $\omega$  lies in  $H^0(X_0(r)_s, \Omega_{X_0(r)/\mathbb{F}_\ell}^1)$ , which yields a contradiction, as this vector space is trivial.

In order to prove this claim, let us write  $K$  for the function field of  $X_0(r)_s$  and  $L$  for the one of  $X_s$ . The function field  $L$  is then a finite Galois extension of  $K$  of degree  $\frac{p(p-1)}{2}$ . Denote by  $\infty_1, \dots, \infty_{\frac{p-1}{2}}$  the  $\frac{p-1}{2}$  cusps of  $X_s$  over the cusp  $\infty$  of  $X_0(r)_s$ . For each  $i \in \{1, \dots, \frac{p-1}{2}\}$ , let  $s_i \in L$  be a uniformizer at  $\infty_i$ . Also, let  $t \in K$

be a uniformizer at the cusp  $\infty$  of  $X_0(r)_s$ . Since  $\Omega_{K/\mathbb{F}_\ell}^1$  is a 1-dimensional  $K$ -vector space and  $\Omega_{L/\mathbb{F}_\ell}^1 = \Omega_{K/\mathbb{F}_\ell}^1 \otimes_K L$ , we can write any element of  $\Omega_{L/\mathbb{F}_\ell}^1$  as the product of an element in  $L$  by  $dt$ .

Now, note that the slash operators  $|_2 \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ ,  $n \in \{0, \dots, p-1\}$ , induce automorphisms of  $X_s$  over  $X_0(r)_s$ . Therefore, these give rise to elements in  $\text{Gal}(L/K)$ . Moreover, it is easily checked (using the Orbit–Stabilizer theorem, or otherwise) that, actually, these operators fix the cusps  $\infty_1, \dots, \infty_{\frac{p-1}{2}}$ . Thus, the corresponding automorphisms in  $\text{Gal}(L/K)$  are contained in every decomposition group  $\text{Gal}(L_{s_i}/K_t)$ ,  $i = 1, \dots, \frac{p-1}{2}$ , where  $K_t$  is the  $t$ -adic completion of  $K$  and, similarly, for each  $i$ ,  $L_{s_i}$  is the  $s_i$ -adic completion of  $L$ .

Writing  $\omega = f dt$ , for some  $f \in L$ , we have

$$\text{Tr } \omega = \text{Tr}_K^L(f) dt = \sum_{i=1}^{\frac{p-1}{2}} \text{Tr}_{K_t}^{L_{s_i}}(f) dt = \sum_{i=1}^{\frac{p-1}{2}} \sum_{n=0}^{p-1} f |_2 \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} dt.$$

Since we are assuming that  $a_n(\omega) = 0$  for any  $n$  coprime to  $p$ , we conclude that  $f$  is invariant under these slash operators. Hence,

$$\text{Tr } \omega = \sum_{i=1}^{\frac{p-1}{2}} p\omega = \frac{p(p-1)}{2}\omega.$$

Now, since  $\ell$  does not divide  $\frac{p(p-1)}{2}$ , we conclude that  $\omega$  is a holomorphic differential in  $X_0(r)_s$ , as we wanted. However, as noted above, this yields a contradiction. Hence, there must exist some  $n$  coprime to  $p$  such that  $a_n(\omega) \neq 0$ .

Consider  $T_n\omega$  now. We have  $\alpha(T_n\omega) = a_1(T_n\omega) = a_n(\omega) \neq 0$ . Since  $\text{Cotg}_{\infty_\ell}(X_s) \cong \mathbb{F}_\ell$ , we conclude that  $f_s^*$  is surjective.  $\square$

**Corollary 47** ([DM97, Theorem 8.1]). *Let  $\Sigma := \{2, 3, 5, 7, 13\}$ ,  $r \in \Sigma$  and  $p$  a prime number not in  $\Sigma$ . Let  $E$  be an elliptic curve over  $\mathbb{Q}$  admitting a  $\mathbb{Q}$ -rational  $r$ -isogeny and such that  $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$  is contained in the normalizer of a non-split Cartan subgroup of  $\text{GL}_2(\mathbb{F}_p)$ . Then, if  $\ell \equiv \pm 1 \pmod{p}$ ,  $v_\ell(j(E)) \geq 0$ .*

*Proof.* This elliptic curve gives rise to a  $\mathbb{Q}$ -rational point  $P \in X_{0,\text{ns}}^+(r, p)$ . Let  $Q$  denote its image in  $A$ . Note that  $Q$  is a point defined over  $\mathbb{Q}(\zeta_p)^+$ . We start by proving that  $Q$  is a torsion point. In order to prove this, start by noting

that we have  $Q = (P) - (\infty)$ . Recall that  $X_{0,\text{ns}}^+(r, p)$  has  $m := (p - 1)/2$  cusps  $\infty_1 (= \infty), \infty_2, \dots, \infty_m$  over the cusp  $\infty$  of  $X_0(r)$  and that they form a single orbit under the Galois action. Now, given  $\sigma \in G_{\mathbb{Q}}$ , set  $Q^\sigma := \sigma(Q) = (P) - (\infty_{\sigma(1)})$ . Thus,  $Q^\sigma - Q = (\infty_1) - (\infty_{\sigma(1)})$ . The Drinfeld–Manin theorem now yields that  $Q^\sigma - Q$  has finite order, i.e., there is an integer  $N$  for which  $N(Q^\sigma - Q) = 0$ . Since  $\sigma$  is an arbitrary element of  $G_{\mathbb{Q}}$ , we conclude that there is an integer  $M$  such that  $\sigma(MQ) = MQ$ , for all  $\sigma \in G_{\mathbb{Q}}$ . Therefore,  $MQ$  is a  $\mathbb{Q}$ -point in  $A$ . However, Theorem 43 says that  $A(\mathbb{Q})$  is finite. Hence,  $MQ$  is torsion, and so is  $Q$ .

Suppose, for the sake of contradiction, that there is some  $\ell \equiv \pm 1 \pmod{p}$  for which  $v_\ell(j(E)) < 0$ . We know that the torsion subgroup of  $A(\mathbb{Q}_\ell)$  injects into  $A_s(\mathbb{F}_\ell)$ . Also, because of our assumption on the  $j$ -invariant, we conclude that  $P_\ell$ , the reduction of  $P \in X_{0,\text{ns}}^+(r, p)(\mathbb{Q}_\ell) \pmod{\ell}$ , coincides with the reduction of a cusp  $\pmod{\ell}$ . Without loss of generality, we may assume that this cusp is  $\infty$ . Thus,  $0 = f(\infty)$  and  $Q = f(P)$  reduce to the same cusp  $\pmod{\ell}$ . Since the torsion part of  $A(\mathbb{Q}_\ell)$  injects into  $A_s(\mathbb{F}_\ell)$ , we must have  $Q = 0$ . However,  $P$  is necessarily different from  $\infty$ . Since they both reduce to  $\infty_\ell$ , we have two distinct homomorphisms

$$g_P, g_\infty : \hat{\mathcal{O}}_{X_{0,\text{ns}}^+(r, p), \infty_\ell} \rightarrow \mathbb{Z}_\ell$$

corresponding to the respective  $\mathbb{Z}_\ell$ -points defined in  $X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}$  by  $P$  and  $\infty$ . Since  $P$  and  $\infty$  are both mapped, via  $f_{\mathbb{Z}_\ell}$ , to 0, we conclude that  $g_P \circ \hat{f}_{\mathbb{Z}_\ell}^\# = g_\infty \circ \hat{f}_{\mathbb{Z}_\ell}^\#$ , where  $\hat{f}_{\mathbb{Z}_\ell}^\# : \hat{\mathcal{O}}_{A, 0_\ell} \rightarrow \hat{\mathcal{O}}_{X_{0,\text{ns}}^+(r, p), \infty_\ell}$  is the homomorphism induced by the morphism  $f_{\mathbb{Z}_\ell}$  on the completed local rings. However,  $f_{\mathbb{Z}_\ell}$  is a formal immersion at  $\infty_\ell$ , which precisely says that  $\hat{f}_{\mathbb{Z}_\ell}^\#$  is surjective. Thus,  $g_P$  must equal  $g_\infty$ , which yields a contradiction.  $\square$

## 2.5 Integrality of $j$ -invariant

One of the fundamental observations of this section is the following improvement of Theorem 37:

**Proposition 48.** *Set  $\Sigma := \{2, 3, 5, 7, 13\}$ . Let  $E$  be an elliptic curve over  $\mathbb{Q}$  admitting a  $\mathbb{Q}$ -rational  $r$ -isogeny for some  $r \in \Sigma$ . Suppose that there exists a prime  $p \notin \Sigma$  such that the image of  $\bar{\rho}_{E, p}$  is contained in the normaliser of a non-split Cartan subgroup of  $\text{GL}_2(\mathbb{F}_p)$ . Then  $j(E) \in \mathbb{Z}$ .*

This proposition is actually a corollary of the following result.

**Proposition 49.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and  $p \geq 5$  a prime number such that  $\bar{\rho}_{E, p}(G_{\mathbb{Q}})$  is contained in the normaliser of a non-split Cartan*

subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Then, for any prime  $\ell \not\equiv \pm 1 \pmod{p}$ , the elliptic curve  $E$  has potentially good reduction at  $\ell$ .

**Remark.** Note that the case  $\ell = p$  is included in the proposition.

*Proof.* Suppose  $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$  is contained in the normaliser  $N_{\mathrm{ns}}$  of a non-split Cartan subgroup  $C_{\mathrm{ns}}$  of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Let  $\ell$  be a prime of potentially multiplicative reduction. For the remainder of this proof, we will write  $E$  for  $E_{\mathbb{Q}_\ell}$ , the elliptic curve obtained from  $E$  by extension of scalars to  $\mathbb{Q}_\ell$ . Also, we fix an embedding  $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ , which amounts to a choice of decomposition subgroup  $G_{\mathbb{Q}_\ell} \hookrightarrow G_{\mathbb{Q}}$  over  $\ell$ .

Since  $E$  has potentially multiplicative reduction, it is a quadratic twist of a Tate curve  $E_q$ ,  $q \in \mathbb{Q}_\ell^\times$ . Let  $\psi$  be the quadratic character associated to this twist ( $\psi$  may well be the trivial character). Then  $\bar{\rho}_{E,p} \cong \bar{\rho}_{E_q,p} \otimes \psi$ . Since we have

$$\bar{\rho}_{E_q,p} \sim \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix},$$

where  $\chi_p : G_{\mathbb{Q}_\ell} \rightarrow \mathbb{F}_p^\times$  is the mod  $p$  cyclotomic character, we conclude that

$$\bar{\rho}_{E,p} \sim \begin{pmatrix} \psi\chi_p & * \\ 0 & \psi \end{pmatrix}.$$

Now, note that  $C_{\mathrm{ns}}$ , as a subgroup of  $\mathrm{GL}_2(\mathbb{F}_{p^2})$ , is conjugate to the subgroup

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a^p \end{pmatrix} : a \in \mathbb{F}_{p^2}^\times \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2}) \quad (2.1)$$

Since  $[N_{\mathrm{ns}} : C_{\mathrm{ns}}] = 2$ , we have  $\bar{\rho}_{E,p}(\sigma)^2 \in C_{\mathrm{ns}}$  for all  $\sigma \in G_{\mathbb{Q}_\ell}$ . Also, since  $\psi$  is quadratic, the eigenvalues of  $\bar{\rho}_{E,p}(\sigma)^2$  are  $\chi_p(\sigma)^2$  and 1. It then follows from (2.1) that  $\chi_p(\sigma)^2 = 1$  for all  $\sigma \in G_{\mathbb{Q}_\ell}$ . If  $\ell = p$ , then we know that  $\chi_p$  surjects onto  $\mathbb{F}_p^\times$ , which forces  $p \leq 3$ . If  $\ell \neq p$ , then we have  $\ell^2 \equiv 1 \pmod{p}$ .  $\square$

*Proof of Proposition 48.* Let  $E$  be an elliptic curve and  $p$  a prime as in the statement of the proposition. Then we already know, due to Corollary 47, that if  $\ell \equiv \pm 1 \pmod{p}$ , then  $v_\ell(j(E)) \geq 0$ . Note that  $E$  and  $p$  satisfy the conditions of Proposition 49. It follows that  $E$  has potentially good reduction at any prime  $\ell \not\equiv \pm 1 \pmod{p}$ , which means that  $v_\ell(j(E)) \geq 0$  for primes  $\ell \not\equiv \pm 1 \pmod{p}$  as well. Therefore,  $j(E) \in \mathbb{Z}$ .  $\square$

## 2.6 Proof of the main theorem

With Proposition 48 proven, we have the most important ingredients for the proof of the main result of this paper.

*Proof of Theorem 34.* Let  $E$  is an elliptic curve over  $\mathbb{Q}$  without CM which admits a cyclic  $\mathbb{Q}$ -rational isogeny, which we may assume to be of prime degree  $r$ . By Mazur [MG78], we have  $r \in \{2, 3, 5, 7, 11, 13, 17, 37\}$ . Suppose, for the sake of contradiction, that there exists a prime number  $p > 37$  such that  $\bar{\rho}_{E,p}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{F}_p)$ . For each prime number  $r$ , define

$$S_r = \{j(P) : P \in Y_0(r)(\mathbb{Q})\}.$$

We will distinguish two cases: we can either have  $r \in \{2, 3, 5, 7, 13\}$ , or  $r \in \{11, 17, 37\}$ . For  $r = 11, 17$ , the modular curve  $X_0(r)$  is an elliptic curve over  $\mathbb{Q}$  of rank 0; and for  $r = 37$ ,  $X_0(r)$  is a curve of genus 2 whose Jacobian has rank 1. This makes it easy to determine the rational points of  $X_0(r)$  for  $r \in \{11, 17, 37\}$ , which are, in fact, known. From [Cre97, p. 98], we know that

$$\begin{aligned} S_{11} &= \{-11 \cdot 131^3, -2^{15}, -11^2\}; \\ S_{17} &= \left\{ -\frac{17^2 \cdot 101^3}{2}, -\frac{17 \cdot 373^3}{2^{17}} \right\}; \\ S_{37} &= \{-7 \cdot 137^3 \cdot 2083^3, -7 \cdot 11^3\}. \end{aligned}$$

Therefore, if  $r \in \{11, 17, 37\}$ , the  $j$ -invariant of  $E$  is one of the values in  $S_{11} \cup S_{17} \cup S_{37}$ . Since any two elliptic curves over  $\mathbb{Q}$  without CM and with the same  $j$ -invariant are related by a quadratic twist, the surjectivity of  $\bar{\rho}_{E,p}$  only depends on the  $j$ -invariant. The LMFDB [LMF16] provides a long list of elliptic curves over  $\mathbb{Q}$ , together with information about the surjectivity of the mod  $p$  Galois representations attached to them, such as the largest non-surjective prime — which is computed using an algorithm of Sutherland [Sut16]. For each of the seven values in  $S_{11} \cup S_{17} \cup S_{37}$ , we found an elliptic curve over  $\mathbb{Q}$  in this database with this  $j$ -invariant, we verified that  $-2^{15}$  is the only CM  $j$ -invariant, and checked that the largest non-surjective prime of each of the other six  $j$ -invariants is  $\leq 37$ . Therefore, if an elliptic curve  $E$  defined over  $\mathbb{Q}$  without CM admits a  $\mathbb{Q}$ -rational isogeny of degree  $r \in \{11, 17, 37\}$ , then the image of  $\bar{\rho}_{E,p}$  is  $\mathrm{GL}_2(\mathbb{F}_p)$  for all  $p > 37$ .

Keeping up with the notation introduced at the beginning of this proof, we suppose that  $r \in \{2, 3, 5, 7, 13\}$ . Now,  $X_0(r)$  is a smooth curve of genus 0 with

rational points (the cusps, for instance), which means that  $X_0(r)$  will have infinitely many rational points. Therefore, we will not be able to use the same strategy we applied to treat the case  $r \in \{11, 17, 37\}$ . Instead, we are going to start by showing that if  $\bar{\rho}_{E,p}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{F}_p)$ , then  $j(E) \in \mathbb{Z}$ . We are only a step away from proving this. After the successive works mentioned in the introduction, we have the following theorem:

**Theorem 50** (Bilu–Parent–Rebolledo [BPR13], Mazur [MG78], Serre [Ser81, Lemme 18]). *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$ . If  $p > 37$  is a prime such that  $\bar{\rho}_{E,p}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{F}_p)$ , then the image of  $\bar{\rho}_{E,p}$  is contained in the normaliser of a non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ .*

This result, together with Proposition 48, yields  $j(E) \in \mathbb{Z}$ .

This would be of no use for us if  $S_r \cap \mathbb{Z}$  were infinite; but it turns out that, for  $r \in \{2, 3, 5, 7, 13\}$ , this set is finite. In order to prove this, we can directly compute these sets, and that is what we will do now.

For an appropriate choice of local coordinate  $t$  on  $X_0(r) \cong \mathbb{P}_{\mathbb{Q}}^1$ , the  $j$ -invariant map is explicitly given by a map of the form

$$t \mapsto \frac{f(t)}{t},$$

where  $f(t) \in \mathbb{Z}[t]$  is a monic polynomial of degree  $r+1$  and non-zero constant term. The values of  $f(t)$  can be found in the following table:

$r$	$f(t)$
2	$(t+16)^3$
3	$(t+27)(t+3)^3$
5	$(t^2+10t+5)^3$
7	$(t^2+5t+1)^3(t^2+13t+49)$
13	$(t^4+7t^3+20t^2+19t+1)^3(t^2+5t+13)$

For  $r = 2, 3$ , they are easy to check (see [Bir73, pp. 179-180]); for  $r = 5, 7, 13$ , we refer to [Dah08, p. 54]. If  $t$  corresponds to a  $\mathbb{Q}$ -point in  $X_0(r)$ , then we can write  $t = a/b$ , where  $a, b \in \mathbb{Z}$ ,  $b > 0$  and  $\mathrm{gcd}(a, b) = 1$ . Now, if the  $j$ -invariant of this point is integral, we have

$$\frac{b^{r+1}f(a/b)}{ab^r} \in \mathbb{Z}.$$

Therefore,  $b \mid b^{r+1}f(a/b)$ . But  $b^{r+1}f(a/b) = a^{r+1} + bG(a, b)$ , where  $G \in \mathbb{Z}[s, t]$  is a homogeneous polynomial. Since  $\gcd(a, b) = 1$ , we must have  $b = 1$ . Hence,  $t \in \mathbb{Z}$  and  $t$  must divide the constant term of  $f(t)$ . Substituting  $t$  in  $f(t)/t$  by all integers that divide the constant term of  $f(t)$ , we obtain  $S_r \cap \mathbb{Z}$ :

$$\begin{aligned} S_2 \cap \mathbb{Z} &= \{ -3^3 \cdot 5^3, -2^2 \cdot 7^3, -2^4 \cdot 3^3, -2^6, 0, 2^7, 2^6 \cdot 3^3, 2^4 \cdot 5^3, 2^{11}, 2^2 \cdot 3^6, 2^7 \cdot 3^3, 17^3, \\ &\quad 2^6 \cdot 5^3, 2^5 \cdot 7^3, 2^5 \cdot 3^6, 2^4 \cdot 3^3 \cdot 5^3, 2^4 \cdot 17^3, 2^3 \cdot 31^3, 2^3 \cdot 3^3 \cdot 11^3, 2^2 \cdot 3^6 \cdot 7^3, \\ &\quad 2^2 \cdot 5^3 \cdot 13^3, 2 \cdot 127^3, 2 \cdot 3^3 \cdot 43^3, 3^3 \cdot 5^3 \cdot 17^3, 257^3 \}; \\ S_3 \cap \mathbb{Z} &= \{ -2^4 \cdot 11^6 \cdot 13, -2^{15} \cdot 3 \cdot 5^3, -2^4 \cdot 3^2 \cdot 13^3, -2^4 \cdot 13, 0, 2^4 \cdot 3^3, 2^8 \cdot 7, 2^4 \cdot 3^3 \cdot 5, \\ &\quad 2^8 \cdot 3^3, 2^4 \cdot 3^3 \cdot 5^3, 2^8 \cdot 3^2 \cdot 7^3, 2^4 \cdot 3 \cdot 5 \cdot 41^3, 2^8 \cdot 7 \cdot 61^3 \}; \\ S_5 \cap \mathbb{Z} &= \{ -2^6 \cdot 719^3, -2^6 \cdot 5 \cdot 19^3, 2^6, 2^6 \cdot 5^2, 2^{12}, 2^{12} \cdot 5^2, 2^{12} \cdot 5 \cdot 11^3, 2^{12} \cdot 211^3 \}; \\ S_7 \cap \mathbb{Z} &= \{ -3^3 \cdot 37 \cdot 719^3, -3^3 \cdot 5^3, 3^3 \cdot 37, 3^2 \cdot 7^4, 3^3 \cdot 5^3 \cdot 17^3, 3^2 \cdot 7 \cdot 2647^3 \}; \\ S_{13} \cap \mathbb{Z} &= \{ -2^6 \cdot 3^2 \cdot 4079^3, 2^6 \cdot 3^2, 2^{12} \cdot 3^3 \cdot 19, 2^{12} \cdot 3^3 \cdot 19 \cdot 991^3 \}. \end{aligned}$$

Resorting once again to the elliptic curve database of the LMFDB [LMF16], we verified that the largest non-surjective prime of each of the non-CM  $j$ -invariants in

$$(S_2 \cup S_3 \cup S_5 \cup S_7 \cup S_{13}) \cap \mathbb{Z}$$

is not larger than 37. This concludes the proof of Theorem 34.  $\square$

**Remark.** During the proof of Theorem 34, we computed the sets  $S_r \cap \mathbb{Z}$ , for  $r \in \{2, 3, 5, 7, 13\}$ , using an explicit description of the  $j$ -invariant map. There is, however, a nice proof of the finiteness of the sets  $S_r \cap \mathbb{Z}$ , pointed out to me by Samir Siksek. Since this proof is interesting in its own right, we include it here.

**Proposition 51.** *Let  $p$  be a prime number. Then the set  $S_p \cap \mathbb{Z}$  is finite.*

*Proof.* If the genus of  $X_0(p)$  is at least 1, then it is known that there are only finitely many points in  $X_0(p)(\mathbb{Q})$ . Therefore, we may assume that the genus of  $X_0(p)$  is 0, i.e., that  $p \in \{2, 3, 5, 7, 13\}$ .

Fix an isomorphism  $\psi : \mathbb{P}_{\mathbb{Z}[\frac{1}{p}]}^1 \rightarrow X_0(p)_{\mathbb{Z}[\frac{1}{p}]}$  over  $\mathbb{Z}[\frac{1}{p}]$ , and choose projective coordinates in such a way that  $(0 : 1)$  is mapped to the cusp 0 and  $(1 : 0)$  to the cusp  $\infty$ . The  $j$ -invariant map is then a morphism

$$j : \mathbb{P}_{\mathbb{Z}[\frac{1}{p}]}^1 \rightarrow \mathbb{P}_{\mathbb{Z}[\frac{1}{p}]}^1$$

mapping  $(1 : 0)$  and  $(0 : 1)$  to  $(1 : 0)$ . For a point in  $X_0(p)$  to have integral  $j$ -invariant, it is necessary that its image under the  $j$ -invariant map does not intersect

$(1 : 0)$  in any special fibre of  $\mathbb{P}_{\mathbb{Z}[\frac{1}{p}]}^1$ . Therefore, such a point must not intersect  $(0 : 1)$  nor  $(1 : 0)$  in any special fibre of  $\mathbb{P}_{\mathbb{Z}[\frac{1}{p}]}^1 \cong X_0(p)_{\mathbb{Z}[\frac{1}{p}]}$ . This means that it must be of the form  $(p^k : 1)$ , for some  $k \in \mathbb{Z}$ .

Consider now  $X_0(p)(\mathbb{C}_p)$  and  $\mathbb{P}^1(\mathbb{C}_p)$  equipped with the  $p$ -adic topology. Consider the  $\mathbb{Q}$ -isomorphism between  $X_0(p)$  and  $\mathbb{P}_{\mathbb{Q}}^1$  obtained by restricting the isomorphism of the paragraph above to the general fibres. Let  $B$  be the open ball of radius  $1/p$  centered at the point  $(1 : 0)$  of  $\mathbb{P}^1(\mathbb{C}_p)$ ; the integral points of  $\mathbb{P}^1(\mathbb{C}_p)$  lie outside of  $B$ . Since our isomorphism between  $X_0(p)$  and  $\mathbb{P}_{\mathbb{Q}}^1$  and the  $j$ -invariant morphism  $j : X_0(p)(\mathbb{C}_p) \rightarrow \mathbb{P}^1(\mathbb{C}_p)$  are  $p$ -adically continuous,  $U := j^{-1}(B)$  is an open subset of  $\mathbb{P}^1(\mathbb{C}_p)$  containing  $(1 : 0)$  and  $(0 : 1)$ . Clearly, among the points  $(\pm p^k : 1)$ ,  $k \in \mathbb{Z}$ , only finitely many lie outside of  $U$ . This concludes the proof of the lemma.  $\square$

# Bibliography

- [AdRAK<sup>+</sup>15] Sara Arias-de Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. Galois representations and Galois groups over  $\mathbb{Q}$ . In *Women in numbers Europe*, volume 2 of *Assoc. Women Math. Ser.*, pages 191–205. Springer, Cham, 2015.
- [AdRDW16] Sara Arias-de Reyna, Luis Dieulefait, and Gabor Wiese. Classification of subgroups of symplectic groups over finite fields containing a transvection. *Demonstr. Math.*, 49(2):129–148, 2016.
- [ALS16] Samuele Anni, Pedro Lemos, and Samir Siksek. Residual representations of semistable principally polarized abelian varieties. *Res. Number Theory*, 2:Art. 1, 12, 2016.
- [Art88] E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1988. Reprint of the 1957 original, A Wiley-Interscience Publication.
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [Bir73] B. J. Birch. Some calculations of modular relations. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 175–186. Lecture Notes in Mathematics, Vol. 320. Springer, Berlin, 1973.
- [BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

- [BP11] Yuri Bilu and Pierre Parent. Serre’s uniformity problem in the split cartan case. *Annals of Mathematics*, 173:569–584, 2011.
- [BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on  $X_0^+(p^r)$ . *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.
- [Che60] C. Chevalley. Une démonstration d’un théorème sur les groupes algébriques. *J. Math. Pures Appl. (9)*, 39:307–317, 1960.
- [Che98] I. Chen. The jacobians of non-split cartan modular curves. *Proceedings of the London Mathematical Society*, 77(1):1–38, 1998.
- [Che00] Imin Chen. On relations between Jacobians of certain modular curves. *J. Algebra*, 231(1):414–448, 2000.
- [Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.
- [Dah08] S. R. Dahmen. *Classical and modular methods applied to Diophantine equations*. PhD thesis, Universiteit Utrecht, 2008.
- [DDMM17] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Arithmetic of hyperelliptic curves over local fields. 2017. in preparation.
- [dE00] Bart de Smit and Bas Edixhoven. Sur un résultat d’Imin Chen. *Mathematical Research Letters*, 7(2):147–153, 2000.
- [DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat’s last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.
- [DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.
- [Hal11] Chris Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.
- [KL89] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.
- [KM85] N.M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Annals of mathematics studies. Princeton University Press, 1985.

- [KW09] Chandrashekhara Khare and Jean-Pierre Wintenberger. Serre’s modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.
- [LD98] Pierre Le Duff. Représentations galoisiennes associées aux points d’ordre  $l$  des jacobiniennes de certaines courbes de genre 2. *Bull. Soc. Math. France*, 126(4):507–524, 1998.
- [Lem17] Pedro Lemos. Serre’s Uniformity Conjecture for Elliptic Curves with Rational Cyclic Isogenies. *ArXiv e-prints*, February 2017.
- [LMF16] The LMFDB Collaboration. The L-functions and modular forms database. <http://www.lmfdb.org>, 2016. [Online; accessed 11 November 2016].
- [Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.
- [MG78] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.
- [Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.
- [Ray74] Michel Raynaud. Schémas en groupes de type  $(p, \dots, p)$ . *Bull. Soc. Math. France*, 102:241–280, 1974.
- [Ser71] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971.
- [Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
- [ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
- [Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.
- [Zyw15] D. Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. *ArXiv e-prints*, August 2015.