UNIVERSITAT DE BARCELONA

ADVANCED MATHEMATICS
MASTER'S FINAL PROJECT

Comparing Galois representations and the Faltings-Serre-Livné method

Author:
Ignasi Sánchez Rodríguez

Supervisor:
Dr. Luís Dieulefait
Dr. Nuno Freitas

Facultat de Matemàtiques i Informàtica

September 7th, 2020

Contents

UNIVERSITAT DE BARCELONA

Abstract

Facultat de Matemàtiques i Informàtica

MSc

Comparing Galois representations and the Faltings-Serre-Livné method

by Ignasi Sánchez Rodríguez

In 1984, Jean-Pierre Serre, based on the ideas of Gerd Faltings, explained in his course at the *Collège de France* a method for comparing irreducible ℓ-adic Galois representations. This method would later be anointed as the *Faltings-Serre method* by the mathematical community. In 1987 Ron Livné gave an algorithm to compare the case of 2-dimensional 2-adic Galois representations with even trace. In 2008 Gabriel Chênevert generalised it erasing the condition on the traces. In this thesis we are going to draw on his work to explore and formalise Serre's ideas. In addition, we are going to collect some examples from Serre himself in the case of 2-dimensional 2-adic Galois representations from elliptic curves to understand the use of it and we are going to explain them in detail. Finally, we are also going to study Livné's approach and give an example of this as well.

Acknowledgements

M'agradaria primer donar les gràcies als meus dos tutors, Luís Dieulefait i Nuno Freitas, per la seva inestimable ajuda durant tot el treball. En especial, durant aquestes últimes setmanes del mes d'agost, que rebien un correu meu cada dia amb incessants dubtes i sempre contestaven amb la major rapidesa i detall. Moltes gràcies per tot el que heu fet per mi.

També voldria agrair a totes les professores de la Facultat de Matemàtiques i Informàtica, qui m'han obert les portes al món de les matemàtiques, del qual no puc ni vull escapar. Especialment, m'agradaria agrair a la Teresa Crespo, qui ha sigut una ajuda constant durant els meus anys de grau i qui em va obrir les portes a la teoria de nombres i a la teoria de Galois.

Agrair també a en Santi Seguí, en Jordi Vitrià i n'Oriol Pujol per apropar-me a la banda de Ciència de Dades i fer-me sentir una persona molt vàlida en aquest àmbit. Treballar i, sobretot, aprendre d'ells ha estat una de les millors experiències que un pot desitjar de la universitat.

Finalment, agrair a la meva família: als meus pares, Josep i Lupe, als meus germans, Albert i Gemma i als meus amics, els quals han escotat queixes constants de què no arribava a acabar i han suportat el meu mal humor quan no em sortien els resultats (ho sento!). Gràcies a l'Enric per pensar amb mi i oferir rutes alternatives a qualsevol raonament que no sortia bé. I gràcies a l'Aina per escoltar-me dia a dia, animar-me quan no sortien les coses i estar amb mi quan no em trobava bé. T'agraeixo tot el que fas cada dia per mi.

Introduction

In the past century, there has been an increasing trend in mathematics to study complex objects by how they act on spaces sharing common features. This is, in a broad sense, what we call a *representation*. Particularly, mathematicians are highly interested in representations arising from the action of a group G on vector spaces over a field E. Such representations give rise to group homomorphisms from G to the invertible matrices with coefficients in E and are called *linear representations of G over E*. In this thesis we study certain representations of this kind arising naturally in Number Theory.

The central object of study in Algebraic Number Theory is the *absolute Galois group of* $\mathbb{Q}$, denoted as $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, consisting of all field automorphisms of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The representations of $\mathrm{Gal}_{\mathbb{Q}}$ and of its subgroups are called *Galois representations*. The 1-dimensional representations of $\mathrm{Gal}_{\mathbb{Q}}$ are well understood via Class Field Theory, but understanding the representations of dimension $n \geq 2$ is an extremely difficult problem. A general approach to this end is to "visualise" pieces of $\mathrm{Gal}_{\mathbb{Q}}$ via its action on certain geometric objects. This idea, in the particular case of 2-dimensional representations, has seen a lot of research done during the last decades, and has yielded some fantastic results. The most famous of which being the proof by Wiles *et al.* (chronologically: [34], [33] and [5]) of one of the most famous theorems in mathematics: Fermat's Last Theorem. More recently, a full proof of Serre's conjecture was found by Khare and Wintenberger [16, 17]. These are however only the first steps into what is known as the Langlands program, that consists of a web of conjectures, according to which all Galois representations arising from geometry should be automorphic. In view of these conjectures a natural question arises: given two Galois representations that should be isomorphic according to the Langlands program can we show they are actually isomorphic?

In this thesis we study methods that allow us to give a positive answer to the previous question under certain hypothesis. For us, the study of isomorphisms of Galois representations taking values on a finite extension of $\mathbb{Q}_\ell$, the field of ℓ-adic numbers, starts with Gerd Faltings, in his 1983 paper [12]. In 1984, Jean-Pierre Serre gave a course in the Collège de France, in which he implemented Falting's ideas into a computable method for the case of 2-dimensional representations taking values in $\mathbb{Q}_2$. Around the same time, using Serre's method, François Mestre [19], gave an example of how to prove that a particular elliptic curve, the one of conductor 5077, was modular. Unfortunately, we do not know of any available notes of Serre's course, except for a short summary [29] and a letter he wrote to Tate [27] describing it. In 1987, Ron Livné [18] gave a further refinement of Serre's method and, in 2008, Gabriel Chênevert [8] made a generalization of Livné's method. There are other articles applying variants of the method, for example, in [11] it is used to prove the modularity of elliptic curves over imaginary quadratic fields and in [14] it is used to prove the modularity of Calabi-Yau surfaces and threefolds. However only in very recent works a more systematic approach to the method has been detailed. Indeed, there has been a systematic study by two PhD students of John Cremona: Alejandro Argáez [2] and

Mattia Sanna [26] in the 2-dimensional 2-adic and 3-adic cases respectively; moreover, in [7] the authors describe the method applied to representations valued in the symplectic group $\mathrm{GSp}(\overline{\mathbb{Q}}_2)$ with absolutely irreducible residual image and remarkably estabilsh 'paramodularity' of the abelian surface of conductor 277 as a consequence. Despite of these latest efforts, there are still aspects of Serre's method whose details are not available in the literature. The objective of this thesis is to understand the method proposed by Serre [27, 29], describe it in a more modern and general manner, following [8], and to fill in the missing details of his computations and arguments.

The thesis is structured in the following way: In Chapter 1 we are going to give the basic definitions from Algebraic Number Theory to follow the main statements of the theorems. We are also going to introduce linear group representations, giving the example of linear representations of a finite group G over the field of complex numbers $\mathbb{C}$. Then, we are going to define ℓ-adic Galois representations, and give the definition of representations arising from elliptic curves and modular forms. This will be used afterwards in the examples by Serre.

In Chapter 2, we are going to introduce the essential tool when comparing Galois representations, the deviation group $\delta(G)$. Then we are going to see Serre's method, *the method of quartic fields* or *the Faltings-Serre method*, for comparing two ℓ-adic representations with irreducible residual representation. Particularly, we are going to detail the 2-dimensional 2-adic case. Then we are going to study the examples that Serre talks about in his letter to Tate [27]. These are the following:

- There is only one $\mathbb{Q}$-isogeny class of $\mathbb{Q}$-elliptic curves of conductor 11.
- There is only one $\mathbb{Q}$-elliptic curve of conductor 5077 which is modular.

Finally, in Chapter 3 we are going to present the generalisation by Ron Livné [18] which covers the case of the two representations having reducible residual image using Faltings' and Serre's ideas. We are also going to look at a concrete example: we are going to prove that the elliptic curve of conductor 33 is modular.

Chapter 1

Basic concepts

In this chapter we are going to introduce basic concepts from Algebraic Number Theory and the necessary theory of linear representations that we are going to need for this thesis.

1.1 Algebraic Number Theory

Any book on Algebraic Number Theory covers the topics we are going to talk about. To cite a few, [20], [25] or [28].

1.1.1 Primes and ramification

Let K be a number field, let $\mathcal{O}_K$ be its ring of integers and let L/K be a finite extension with $\mathcal{O}_L$ the ring of integers of L.

Since $\mathcal{O}_L$ is a Dedekind domain, for any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ (which we call *a finite prime of* K), we can consider the prime decomposition of the ideal of $\mathcal{O}_L$, namely $\mathfrak{p}\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

where the $\mathfrak{P}_i$ are different prime ideals of $\mathcal{O}_L$ which we call *primes above* $\mathfrak{p}$, *primes lying over* $\mathfrak{p}$ or *primes dividing* $\mathfrak{p}$. More in general, a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ is said to divide $\mathfrak{p}$ if $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Also, $g =: g_{L/K}(\mathfrak{p})$ is a positive integer and the $e_j =: e(\mathfrak{P}_j/\mathfrak{p})$ are also positive integers called the *ramification index for* $\mathfrak{P}_j/\mathfrak{p}$. In a Dedekind domain, every nonzero prime ideal is a maximal ideal, hence $k_{\mathfrak{P}_j} := \mathcal{O}_L/\mathfrak{P}_j$ and $k_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ are fields, which we call *residue fields.* They are finite fields of characteristic p, being p a rational prime satisfying $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. We may view $k_{\mathfrak{p}}$ as a subfield of $k_{\mathfrak{P}_j}$. Particularly, we define the *residual degree* as their field extension degree, i.e.

$$f(\mathfrak{P}_j/\mathfrak{p}) := [k_{\mathfrak{P}_j} : k_{\mathfrak{p}}].$$

If the extension L/K is Galois, then $\mathrm{Gal}(L/K)$ acts transitively on the set of primes lying over $\mathfrak{p}$ by permutation, so every ramification index and residual degree are equal, independent of $\mathfrak{P}_j$.

In general, for any finite extension L/K and any prime $\mathfrak{p}$ in $\mathcal{O}_K$, one has the formula

$$\sum_{i=1}^{g_{L/K}(\mathfrak{p})} e(\mathfrak{P}_j/\mathfrak{p})f(\mathfrak{P}_j/\mathfrak{p}) = [L : K].$$

Particularly, in the Galois case the formula is simplified to $efg = [L : K]$.

For $\mathfrak{p}$ a finite prime of K we differentiate between three possible situations:

1. If $e(\mathfrak{P}_j/\mathfrak{p}) = 1$ for $1 \leq j \leq g$, we say that $\mathfrak{p}$ *is unramified in* L/K. Otherwise we say that $\mathfrak{p}$ *ramifies.*

2. If $g_{L/K}(\mathfrak{p}) = 1$ and $e(\mathfrak{P}_1/\mathfrak{p}) = 1$, i.e. if $\mathfrak{p}$ stays prime in $\mathcal{O}_L$, we say that $\mathfrak{p}$ *is inert in* L/K

3. If $g_{L/K}(\mathfrak{p}) = [L : K]$, we say that $\mathfrak{p}$ *is totally split in* L/K.

There is different way of defining ramification in the Galois case, which will be more useful to us. Let L/K be a Galois extension. Then for a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ and $\mathfrak{P} \subseteq \mathcal{O}_L$ a prime lying over it, we define the *decomposition group at* $\mathfrak{P}/\mathfrak{p}$ as the stabiliser at $\mathfrak{P}$ of the action of $\mathrm{Gal}(L/K)$ on the set of primes above $\mathfrak{p}$. That is,

$$D(\mathfrak{P}/\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

The decomposition group acts on $\mathcal{O}_L/\mathfrak{P}$ by $\sigma(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$, so particularly, it surjects onto $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$, the Galois group of the residual extensions. This yields a short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & I(\mathfrak{P}/\mathfrak{p}) \arrow[r] & D(\mathfrak{P}/\mathfrak{p}) \arrow[r] & \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \arrow[r] & 1 \end{tikzcd} \tag{1.1}$$

where the kernel of the surjection, $I(\mathfrak{P}/\mathfrak{p})$, called the *inertia group* can be explicitly written as

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) \mid \sigma(x) \equiv x \pmod{\mathfrak{P}},\ \forall x \in \mathcal{O}_L\}.$$

When $I(\mathfrak{P}/\mathfrak{p}) = 1$, the prime $\mathfrak{p}$ is unramified. Also, looking at the definitions of both groups, it can be seen that for any $\sigma \in \mathrm{Gal}(L/K)$ the following identities are satisfied

$$\sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1} = D(\sigma(\mathfrak{P})/\mathfrak{p}) \quad \text{and} \quad \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1} = I(\sigma(\mathfrak{P})/\mathfrak{p})$$

When L/K is Galois and finite, we can compute the order of the decomposition and inertia groups.

The order of the decomposition group can be computed using the fact that it is the stabiliser at $\mathfrak{P}$ of $\mathrm{Gal}(L/K)$ acting on the set of primes above $\mathfrak{p}$. By the formula above, $efg = [L : K] = |\mathrm{Gal}(L/K)|$. Particularly, $g = |\mathrm{Gal}(L/K)|/ef$. Now, by the orbit-stabiliser theorem, we have that the order of an orbit of an element is equal to the index between the group and the stabiliser. In this case, g is the order of the orbit of a prime $\mathfrak{P}$ lying over $\mathfrak{p}$, $\mathrm{Gal}(L/K)$ is the group and $D(\mathfrak{P}/\mathfrak{p})$ is the stabiliser. Hence, we have

$$g = \frac{|\mathrm{Gal}(L/K)|}{ef} \qquad \text{and} \qquad g = \frac{|\mathrm{Gal}(L/K)|}{|D(\mathfrak{P}/\mathfrak{p})|}.$$

Particularly, $|D(\mathfrak{P}/\mathfrak{p})| = ef$.

To find the order of the inertia group, using the exact sequence (1.1), we have that

$$|I(\mathfrak{P}/\mathfrak{p})| = \frac{|D(\mathfrak{P}/\mathfrak{p})|}{|\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})|} = \frac{ef}{f} = e.$$

1.1.2 Frobenius element

Following from the definition of the decomposition group, let L/K be a Galois extension of a number field K and let $\mathfrak{p}$ be a finite prime of K and $\mathfrak{P}$ a finite prime of L lying over it.

If $\mathfrak{p}$ is unramified, then $I(\mathfrak{P}/\mathfrak{p}) = 1$, hence the exact sequence (1.1) gives an isomorphism between $D(\mathfrak{P}/\mathfrak{p})$ and $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. The group $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is cyclic of order a power of p and it is generated by the Frobenius homomorphism $x \mapsto x^p$. So, there is a unique element of $\mathrm{Gal}(L/K)$ which is contained in $D(\mathfrak{P}/\mathfrak{p})$ and maps to the Frobenius homomorphism by the isomorphism between the two groups. We call this element the *Frobenius element at* $\mathfrak{P}/\mathfrak{p}$ and denote it by $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$. Now, for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma\,\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})\sigma^{-1}.$$

So, we can define a conjugacy class in $\mathrm{Gal}(L/K)$ which contains $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$. We call it the *Frobenius element at* $\mathfrak{p}$ and denote it by $\mathrm{Frob}_{\mathfrak{p}}$. Explicitly,

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \mid \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}\}.$$

There is a concrete characterisation of the Frobenius element:

Proposition 1.1.1. *Let L/K be a Galois extension, $\mathfrak{p}$ a non-zero finite prime of K unramified in L/K and $\mathfrak{P}$ a finite prime of L lying over $\mathfrak{p}$. Then* $\mathrm{Frob}_{\mathfrak{p}}$ *is the unique $\sigma \in \mathrm{Gal}(L/K)$ that satisfies*

$$\sigma(\alpha) \equiv \alpha^{N_{L/K}(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

A very important theorem for us is the following

Theorem 1.1.2 (Weak Chebotarev)**.** *Let L/K be a Galois extension, unramified outside a finite set of primes S. Then the Frobenius elements of unramified primes in L/K are dense in* $\mathrm{Gal}(L/K)$.

1.2 Linear representations

We are going to state some basic definitions and properties of linear group representations over a field K of characteristic 0. We are then going to briefly look at the classification of linear representations of a finite group over $\mathbb{C}$, which will serve as a clarifying example for the definitions given before, and finally we are going to define and give some important examples of Galois representations, the main object of interest in this thesis.

Definition 1.2.1. Let K be a field of characteristic 0, let G be a group and let V be a finite dimensional vector space over K. Any K-linear action of G onto V, $\rho\colon G \longrightarrow \mathrm{GL}(V)$, is called a *$K$-valued representation of G.*

The representation is usually denoted as the linear action and the vector space, i.e. it is the pair (ρ, V). Sometimes, when the space V and the field K are well understood, they are omitted and the representation is just denoted as ρ.

Since we are asking for the vector space V to be finite dimensional, let $n = \dim_K V$. In this case, we say that the representation ρ is *of dimension* n. Choosing a basis for V

gives an isomorphism $\mathrm{GL}(V) \cong \mathrm{GL}_n(K)$. This allows us to denote the representation as (ρ, V) or (ρ, K, n). For example, when $K = \mathbb{C}$, the complex numbers, we are going to say that we have a *complex representation of dimension n of G*, $\rho\colon G \longrightarrow \mathrm{GL}_n(\mathbb{C})$.

There is no harm in asking for G, V and K to have an endowed topology respecting their algebraic structure and that the homomorphism $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is continuous, since we could always endow everything with the discrete topology. In this work, we are always going to assume that the representations are continuous.

If we have $W \subseteq V$ a vector subspace, stable under the action of G, that is,

$$\rho(g)(w) \in W, \quad \forall g \in G,\ \forall w \in W,$$

we call the representation $\rho\colon G \longrightarrow \mathrm{GL}(W)$ a *subrepresentation of ρ*. In particular, this gives the following definition:

Definition 1.2.2. A representation $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is called *simple* or *irreducible* if its only possible subrepresentations are $W = \{0\}$ and $W = V$.

We say that a representation $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is *semisimple* if it can be written as a direct sum of simple subrepresentations.

Definition 1.2.3. Consider two representations (ρ_1, V_1) and (ρ_2, V_2), where V_1, V_2 are two vector spaces over K. A *homomorphism of representations* is a K-linear map $f\colon V_1 \longrightarrow V_2$ such that

$$f \circ \rho_1(g) = \rho_2(g) \circ f.$$

If the homomorphism f is invertible, we say that ρ_1 is isomorphic to ρ_2 and write $\rho_1 \cong \rho_2$.

Every representation $\rho\colon G \longrightarrow \mathrm{GL}(V)$ admits a *Jordan-Hölder composition series*, i.e. a decreasing filtration

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_m = 0.$$

where V_{i+1} is a maximal proper G-stable subspace of V_i or equivalently, V_i/V_{i+1} is simple. Let us write $JH(\rho)$ for the set of isomorphism classes of the simple quotients V_i/V_{i+1} with multiplicities. It is a standard fact in representation theory that $JH(\rho)$ does not depend on the choice of Jordan-Hölder composition series for ρ. This allows us to define an equivalence relation on the set of representations which is coarser than being isomorphic:

Definition 1.2.4. We say that two representations of G, (ρ_1, V_1), (ρ_2, V_2) are *equivalent* and write $\rho_1 \sim \rho_2$ if $JH(\rho_1) = JH(\rho_2)$.

Theorem 1.2.5. *Let (ρ_1, V_1) and (ρ_2, V_2) be two representations of G. Then*

1. *If $\rho_1 \cong \rho_2$, then $\rho_1 \sim \rho_2$.*
2. *If ρ_1, ρ_2 are semisimple, then $\rho_1 \cong \rho_2$ if and only if $\rho_1 \sim \rho_2$.*
3. *For every representation ρ, there exists a unique (up to isomorphism) semisimple representation ρ^{ss} such that $\rho \sim \rho^{ss}$. Concretely, if*

   $$JH(\rho) = \{(W_1, m_1), \ldots, (W_r, m_r)\},$$

   then ρ^{ss} is the action of G on $W_1^{m_1} \oplus \cdots \oplus W_r^{m_r}$.

The isomorphism class of the semisimple representation ρ^{ss} is called the *semisimplification of* ρ. From 2 and 3, we deduce

$$\rho_1 \sim \rho_2 \iff \rho_1^{ss} \cong \rho_2^{ss}.$$

The problem of deciding when two semisimple representations in characteristic 0 are isomorphic is completely determined by their trace. Given a representation $\rho\colon G \longrightarrow \mathrm{GL}(V)$, its *trace* is the continuous function

$$\mathrm{tr}(\rho)\colon G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{\mathrm{tr}} K.$$

Proposition 1.2.6. *Let ρ_1 and ρ_2 be two semisimple representations of a group G with values in K. Then,*

$$\rho_1 \cong \rho_2 \iff \mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2).$$

Particularly, from the theorem above it follows that

$$\rho_1 \sim \rho_2 \iff \rho_1^{ss} \cong \rho_2^{ss} \iff \mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2).$$

Notice that we write $\mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$ instead of $\mathrm{tr}(\rho_1^{ss}) = \mathrm{tr}(\rho_2^{ss})$, which is the equality that one would expect. This is because the trace does not distinguish a representation ρ from its semisimplification ρ^{ss}, since it is additive on short exact sequences whether they are split or not.

1.2.1 Linear representation of finite groups

Suppose now we are on the setting of G a finite group and $K = \mathbb{C}$. We are going to see that the representations of G are determined by the group of characters of G.

Theorem 1.2.7. *Every representation of a finite group G, $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is semisimple.*

The proof of this theorem can be found on any book on representations. It usually involves the construction of a Hermitian product $H(\cdot,\cdot)$ and then for any subrepresentation W, we can find the orthogonal space to W using the product. This gives a decomposition of V as $W \oplus W^{\perp}$.

This tells us that classifying representations modulo $\cong$ or modulo $\sim$ is indifferent in the finite case. Of course, this is not true in general:

- If G is infinite, let $\rho\colon \mathbb{Z} \longrightarrow \mathrm{GL}_2(\mathbb{C})$ the representation defined by

  $$\rho(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

  The only subrepresentation of dimension 1 is the subspace spanned by $(1\ 0)^T$.

- If the characteristic of the field where the vector space is defined divides the order of the group. For example, let p be a prime and let $\rho\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ the representation defined by

  $$\rho(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then, as before, the only subrepresentation of dimension 1 is the subspace spanned by $(1\ 0)^T$.

Given ρ, a complex n-dimensional representation of a finite group G, we define the *character attached to* ρ, denoted as $\chi\colon G \longrightarrow K$, as the trace of the representation.

It can be proved that for any $g \in G$, the image of g, $\rho(g) \in \mathrm{GL}_n(\mathbb{C})$ is diagonalizable and the eigenvalues of the matrix are the roots of unity dividing the order of the group. Particularly,

$$\chi(g) = \sum_{\lambda \in \mathrm{Spec}(\rho(g))} \lambda = \sum_{d \| G|} e^{2\pi i |G|/d}.$$

Let us see some properties that characters satisfy in this setting. Let $\rho\colon G \longrightarrow \mathrm{GL}(V)$ be a representation of dimension n and let χ be its character. Then, for every $g \in G$,

1. χ is constant in the conjugacy classes of G.
2. $\chi(g)$ is an algebraic integer, i.e. $\chi(g) \in \overline{\mathbb{Q}}$.
3. $|\chi(g)| \leq n$ and $|\chi(g)| = n \iff \rho(g) = \mathrm{Id}$. Particularly, $\chi(\mathrm{id}_G) = n$.

We want to classify the representations of G modulo isomorphism. In the vector space of functions $\phi\colon G \longrightarrow \mathbb{C}$ we define the Hermitian product

$$(\phi, \psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

Let $\mathcal{C}$ be the subspace of all the functions $G \longrightarrow \mathbb{C}$ which are constant in the conjugacy classes defined with the same Hermitian product. Such a function is called a *class function.* As we saw in the properties of the characters of a representation above, a character χ is a class function.

Theorem 1.2.8. *The set of characters of the irreducible representations of G define an orthonormal basis for $\mathcal{C}$.*

In particular, if $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is a representation of dimension n, one has the following remarks:

- The number of non-isomorphic irreducible representations of G is equal to the number of conjugacy classes of G.
- Let $JH(\rho) = \{(U_1, m_1), \ldots, (U_r, m_r)\}$ be a list of all the non-isomorphic irreducible representations of G. Let ρ_i be the induced representation of U_i and χ_i the attached character. Then V can be written as

  $$V = U_1^{m_1} \oplus \cdots \oplus U_r^{m_r},$$

  and the m_i satisfy

  $$\chi = m_1\chi_1 + \cdots + m_r\chi_r.$$

Therefore, all the necessary information to decompose representations of a finite group G in irreducible sums is given in the character table for G. This table is an $r \times r$ matrix with values $\chi_i(c_j)$, where the c_j are the representatives of the conjugacy classes of G.

Example 1.2.9. The standard example is to give the conjugacy classes of the group S_m. To make it easy, we can choose $G = S_4$.

The conjugacy classes of a symmetric group S_m are given by the partition numbers of m. For $m = 4$, we have the following cases:

Partition of 4	Associated c_i
$1+1+1+1$	id
$2+1+1$	(12)
$3+1$	(123)
$2+2$	$(12)(34)$
4	(1234)

1.2.2 Galois Representations

Definition 1.2.10. Let L/K be a Galois extension of number fields, let E be a field of characteristic 0 and let V be a finite dimensional vector space over E. A *Galois representation* is a linear representation of $\mathrm{Gal}(L/K)$ over V

$$\rho\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}(V).$$

First of all, let us remark that the usual definition of a Galois representation is by using the absolute Galois group Gal_K. Both definitions are equivalent, since given

$$\rho\colon \mathrm{Gal}_K \longrightarrow \mathrm{GL}(V),$$

such that $\mathrm{Ker}(\rho) = \mathrm{Gal}(\overline{K}/L)$, by the isomorphism theorem and Galois theory one has

$$\mathrm{Im}(\rho) \cong \mathrm{Gal}_K / \mathrm{Ker}(\rho) \cong \mathrm{Gal}(\overline{K}/K)/\,\mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K).$$

Let us look at one of the simpler examples, the representation given by a cyclotomic character.

Example 1.2.11. (Complex cyclotomic character). Let $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ be a primitive Dirichlet character. Let ζ_N be a primitive Nth root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Particularly, $\mathrm{Gal}_{\mathbb{Q}}$ can be restricted to $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, which gives the commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}_{\mathbb{Q}} \arrow[d, "\pi_N"] & & \\
\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \arrow[rr, "\sim"] \arrow[dr, dashed, "\rho_{\chi,N}"'] & & (\mathbb{Z}/N\mathbb{Z})^\times \arrow[dl, "\chi"] \\
& \mathbb{C}^\times &
\end{tikzcd}$$

The Dirichlet character χ determines a homomorphism

$$\rho_\chi = \rho_{\chi,N} \circ \pi_N\colon\ \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathbb{C}^\times.$$

It satisfies that $\rho_\chi(\mathrm{conj}) = \chi(-1)$ and for any prime $\mathfrak{p} \subseteq \mathcal{O}_{\overline{\mathbb{Q}}} = \widehat{\mathbb{Z}}$ lying over a rational prime p with $p \nmid N$, i.e. p does not ramify in $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, then $\rho_\chi(\mathrm{Frob}_{\mathfrak{p}}) = \chi(p)$. To show that the homomorphism is continuous, it suffices to check that ρ_χ^{-1} is open, and this holds because the anti-image is $\mathrm{Gal}(K/\mathbb{Q})$ for some Galois number field $K \subseteq \mathbb{Q}(\zeta_N)$.

Any continuous homomorphism $\rho\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(\mathbb{C})$ factors through $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ for some Galois number field K. Particularly, the representation ρ has finite image. For a 1-dimensional representation $\rho\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathbb{C}^{\times}$, having finite image implies, by the Kronecker-Weber theorem, factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ for some N. Thus all complex 1-dimensional representations factor through ρ_χ for a primitive Dirichlet character χ whose N has to be chosen properly.

However, the representations we are interested in, for example those that arise from $\mathbb{Q}$-abelian varieties, have E a finite extension of $\mathbb{Q}_\ell$ for a rational prime ℓ. Hence, let E be a local number field, i.e. a finite extension of $\mathbb{Q}_\ell$, with ring of integers $\mathcal{O}_\lambda$ having maximal ideal λ.

Definition 1.2.12. Let V be a vector space over E and let ρ be a continuous linear action of $\mathrm{Gal}(L/K)$ on V,

$$\rho\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}(V).$$

We call the couple (ρ, V) a *λ-adic Galois representation* of the group $\mathrm{Gal}(L/K)$.

We can also look at the ℓ-adic cyclotomic character

Example 1.2.13. (ℓ-adic cyclotomic character). Let K be a number field and let ζ_{ℓ^n} be a primitive ℓ^n-root of unity in $\overline{K}$ with $(\zeta_{\ell^n})^\ell = \zeta_{\ell^{n-1}}$. For $\sigma \in \mathrm{Gal}_K$ and $i \geq 0$, define a sequence of integers $a_i \in \mathbb{F}_\ell$,

$$\begin{array}{rcl} \sigma(\zeta_\ell) & = & \zeta_\ell^{a_1} \\ \sigma(\zeta_{\ell^2}) & = & \zeta_{\ell^2}^{a_1+a_2\ell} \\ & \vdots & \\ \sigma(\zeta_{\ell^n}) & = & \zeta_\ell^{a_1+a_2\ell+\cdots+a_n\ell^{n-1}}. \\ & \vdots & \end{array}$$

Then we define the ℓ-adic cyclotomic character $\chi_\ell\colon \mathrm{Gal}_K \longrightarrow \mathbb{Z}_\ell^\times \subseteq \mathrm{GL}_1(\mathbb{Q}_\ell)$ as

$$\chi_\ell(\sigma) = a_1 + a_2\ell + \cdots + a_n\ell^{n-1} + \ldots.$$

Notice that the value $\chi_\ell \pmod{\ell^n}$ simply says what σ does to the ℓ^n roots of unity. It is easy to check that the cyclotomic character is multiplicative. It is also easy to check that it is continuous: taking $F_n = K(\zeta_{\ell^n})$, then $\mathrm{Gal}(\overline{K}/F_n) \mapsto 1 \pmod{\ell^n}$ so χ_ℓ is continuous. Hence, it defines a 1-dimensional ℓ-adic representation.

This representation also satisfies that $\chi_\ell(\mathrm{conj}) = -1$ and as before $\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = p$ when $p \neq \ell$.

We are now going to see that any λ-adic representation can be seen as having values in $\mathcal{O}_\lambda$.

Definition 1.2.14. Let V be a finite dimensional vector space over E. An $\mathcal{O}_\lambda$-lattice Λ is a $\mathcal{O}_\lambda$-submodule of V spawned by E-linearly independent vectors. If the vectors of the basis of V over E, then we call Λ a *full $\mathcal{O}_\lambda$-lattice.*

Since we are considering ρ to be continuous, we have the following proposition:

Proposition 1.2.15. *Let (ρ, V) be a λ-adic Galois representation of a Galois group $G = \mathrm{Gal}(L/K)$. Then ρ stabilizes a full $\mathcal{O}_\lambda$-lattice of V.*

Proof. Let Λ be a full lattice of V. Then $\rho(G)(\Lambda) = \{\rho(g)(v) \mid \forall g \in G,\ \forall v \in \Lambda\}$ is a lattice. Consider the subgroup H of G that stabilizes Λ, i.e. $H = \{g \in G \mid \rho(g)\Lambda = \Lambda\}$. By continuity of ρ, H is open, and being G profinite (hence compact), H has finite index. Indeed, Λ is open and compact by definition, so its stabilizer in $\mathrm{GL}(V)$ is open. Therefore, the lattice T generated by the lattices $\rho(\sigma)\Lambda$, for $\sigma \in G/H$ is stable under the action of the Galois group. □

Corollary 1.2.16. *Choosing a E-basis of V which is a $\mathcal{O}_\lambda$-basis for a full lattice Λ under ρ, we have $\rho\colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}_\lambda) \subseteq \mathrm{GL}_n(E)$.*

Remark 1.2.17. We have seen in Definition 1.2.3 that two K-valued representations are isomorphic if and only if they are conjugated, i.e., there exists $P \in \mathrm{GL}_n(K)$ such that $P\rho_1P^{-1} = \rho_2$. This is not true when we are considering the representations with values on $\mathcal{O}_\lambda$. For example, let $G = C_2$ the cyclic group of 2 elements and let $K = \mathbb{Q}_2$. Consider the following representations

$$\rho_1(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho_2(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The matrix

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

satisfies $P\rho_1P^{-1} = \rho_2$. However, if ρ_1 and ρ_2 were conjugate over $\mathcal{O}_\lambda = \mathbb{Z}_2$, then they would be conjugated modulo 2, but this is impossible since the reduction modulo 2 of $\rho_2(\sigma)$ is the identity and the one of $\rho_1(\sigma)$ isn't.

Definition 1.2.18. A homomorphism $\rho\colon \mathrm{Gal}(L/K) \longrightarrow H$ is *unramified* at a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ if

$$I(\mathfrak{P}/\mathfrak{p}) \subseteq \mathrm{Ker}(\rho),$$

for any prime $\mathfrak{P} \subseteq \mathcal{O}_L$ above $\mathfrak{p}$.

Given S a finite set of primes of K, let I_S be the closed normal subgroup of $\mathrm{Gal}(L/K)$ generated by all the inertia subgroups $I(\mathfrak{P}/\mathfrak{p})$ for $\mathfrak{p} \notin S$. Then the quotient

$$\mathrm{Gal}(L/K)_S := \mathrm{Gal}(L/K)/I_S$$

is the largest continuous quotient of $\mathrm{Gal}(L/K)$ which is unramified outside S. By the Galois correspondence, there exists a subextension L_S of L/K such that

$$I_S = \mathrm{Gal}(L/L_S)$$

is the maximal subextension of L unramified outside S. More generally, for any topological group H, the continuous homomorphisms $\rho\colon \mathrm{Gal}(L/K) \longrightarrow H$ that are unramified outside S are precisely those that factor through the quotient

$$\mathrm{Gal}(L/K)_S = \mathrm{Gal}(L_S/K).$$

Proposition 1.2.19. *Let E be a local number field and V a finite dimensional vector space over E. Let ρ_1 and ρ_2 be two representations of the absolute Galois group Gal_K into $\mathrm{GL}(V)$ which are unramified outside S. Then*

$$\rho_1 \sim \rho_2 \iff \mathrm{tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_\mathfrak{p})), \quad \forall \mathfrak{p} \notin S.$$

Note that the trace is constant on conjugacy classes, so the right hand side makes sense.

Proof. The equivalence class of a continuous representation $\rho\colon \operatorname{Gal}(L/K) \longrightarrow \operatorname{GL}(V)$ unramified outside S is determined by its trace. In particular, we may view the trace map as a continuous function on $\operatorname{Gal}(L_S/K)$, which is determined by its restriction to a dense subset. □

In addition to considering a single λ-adic Galois representation, sometimes is needed to vary λ and consider families of representations satisfying a compatibility condition.

Given K and E two number fields, and λ a prime of E, let S_λ denote the set of primes of K which divide $N(\lambda)$.

Definition 1.2.20. An E-rational compatible system of λ-adic representations of degree n of Gal_K is a family indexed by the finite places λ of E,

$$\rho = \{\rho_\lambda\colon \operatorname{Gal}_K \longrightarrow \operatorname{GL}_n(E_\lambda)\}_\lambda,$$

where E_λ is the completion of E at λ, for which there exists a finite set S of primes of K such that for every λ:

- ρ_λ is unramified outside $S \cup S_\lambda$.
- for every prime $\mathfrak{p} \notin S \cup S_\lambda$ of K, the characteristic polynomial

  $$\det(1 - t\rho_\lambda(\operatorname{Frob}_\mathfrak{p})) \in E_\lambda[t]$$

  has coefficients in E and does not depend on λ.

The minimal set S satisfying these two conditions will be denoted $\operatorname{Ram}(\rho)$.

For the purposes of this thesis, we are interested in the following type of compatible system: Given a representation $\rho\colon \operatorname{Gal}_K \longrightarrow \operatorname{GL}_n(E)$ with finite ramification, we can associate a compatible system

$$\rho_\lambda := \rho \otimes E_\lambda.$$

Particularly, given a representation ρ as above, we can define the set $\operatorname{Ram}(\rho)$ as the finite set for this compatible system.

Example 1.2.21. An example for this is $E = \mathbb{Q}$ and then for every rational prime ℓ, define the system of representations $\rho_\ell = \rho \otimes_\mathbb{Q} \mathbb{Q}_\ell$. The condition on the characteristic polynomial in this case is that it is an element of $\mathbb{Q}[t]$. We are going to see another example in the case of representations arising from an elliptic curve $E/\mathbb{Q}$.

Galois representations attached to an elliptic curve

Let E be an elliptic curve defined over a number field K. Then one may define Galois representations attached to the elliptic curve by letting the absolute Galois group Gal_K act on sets of torsion points of E.

Let $\sigma \in \operatorname{Gal}_K$ and let E be an elliptic curve defined over K. Let $P = (x, y)$ be a point on $E(\overline{K})$. The automorphism σ acts on P coordinate wise, so if P satisfies the defining Weierstrass equation for E, so does $\sigma(P) = (\sigma(x), \sigma(y))$. Particularly, for every $P, Q \in E$, $\sigma(P + Q) = \sigma(P) + \sigma(Q)$. So, σ induces a group homomorphism $E(\overline{K}) \longrightarrow E(\overline{K})$ and furthermore, it induces a map of the m-torsion points $E[m](\overline{K})$ by restriction, $\sigma_m\colon E[m](\overline{K}) \longrightarrow E[m](\overline{K})$.

Since $E[m](\overline{K}) \cong (\mathbb{Z}/m\mathbb{Z})^2$, we can choose two points $P, Q \in E[m](\overline{K})$ which span it. Particularly, every point in $E[m](\overline{K})$ can be written as a $\mathbb{Z}/m\mathbb{Z}$-linear combination of P and Q. So, since we have a basis of this space, we can write σ_m as a 2×2 matrix

$$A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$$

which satisfies

$$\begin{pmatrix} \sigma_m(P) \\ \sigma_m(Q) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}.$$

This gives a group homomorphism

$$\begin{array}{rccl} \rho_m\colon & \mathrm{Gal}_K & \longrightarrow & \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ & \sigma & \longmapsto & A_\sigma \end{array}.$$

This is Galois representation which we call the *mod m Galois representation attached to E* or the *residual representation of E mod m.*

Notice that the kernel of this map are those $\sigma \in \mathrm{Gal}_K$ such that $A_\sigma = \mathrm{Id}$. That is, the σ which leave fixed the m-torsion points of E, namely the subgroup $\mathrm{Gal}(\overline{K}/K(E[m](\overline{K})))$. So, we have

$$\rho_m(\mathrm{Gal}_K) \cong \mathrm{Gal}_K / \mathrm{Ker}(\rho_m) \cong \mathrm{Gal}_K / \mathrm{Gal}(\overline{K}/K(E[m](\overline{K}))) \cong \mathrm{Gal}(K(E[m](\overline{K}))/K), \tag{1.2}$$

Example 1.2.22. The 2-torsion points of a rational elliptic curve can be easily described. We are going to see some results on Chapter 2, §2.2. For now, let us state some results without proof.

Let E be an elliptic curve over $\mathbb{Q}$. Its 2-torsion subgroup, $E[2] \cong \mathbb{F}_2^2$ is given by 4 points. Particularly, if E is given by a Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

then a point $(x, y) \in E[2]$ must satisfy $y^2 = 0$, hence, the 2-torsion points consist of points of the form $(x, 0)$. Consequently, let $E[2] = \{\mathcal{O}, (a, 0), (b, 0), (c, 0)\}$, with $a, b, c \in \overline{Q}$ and $\mathcal{O}$ the identity element of E seen as a group. Then the 2-torsion field $\mathbb{Q}(E[2]) = \mathbb{Q}(a, b, c)$.

Since a, b, c are solution to an equation with rational coefficients, we can have 1 or 3 rational roots. If $a, b, c \in \mathbb{Q}$, then $\mathbb{Q}(E[2]) = \mathbb{Q}$ and the representation ρ_2 is trivial by (1.2).

If we have two or more roots in $\overline{\mathbb{Q}} \setminus \mathbb{Q}$, then $\mathbb{Q}(E[2])/\mathbb{Q}$ is an extension with irreducible polynomial of degree at most 3, so $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is a transitive subgroup of S_3, which can only be the alternating group A_3 or S_3 itself. It is a simple exercise of Galois theory to check that the condition for one or the other is whether the discriminant of the polynomial $x^3 + Ax + B$ is a square in $\mathbb{Q}$ (in which case $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong A_3$) or not (in which case $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$).

In fact, since $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, whenever the discriminant of $x^3 + Ax + B$ is not a square in $\mathbb{Q}$, the representation $\rho_2\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_2)$ is surjective.

Surjectivity in the case of residual representations (in the non CM case at least) is not that “rare”. In [30], Serre proves the following theorem:

Theorem 1.2.23. *Let K be an algebraic number field and E an elliptic curve defined over K without complex multiplication. Then, for all but finitely many primes ℓ, the residual representation*

$$\rho_\ell \colon \operatorname{Gal}_K \longrightarrow \operatorname{GL}_2(\mathbb{F}_\ell)$$

is surjective.

One is usually interested in a broader picture than the m-torsion points of an elliptic curve. Recall that given an elliptic curve over a number field K and given a rational prime ℓ, we can define the Tate module of E,

$$T_\ell(E) = \varprojlim_m E[\ell^m].$$

The inverse limit is given by the multiplication by ℓ isogeny, $[\ell] \colon E[\ell^{n+1}] \longrightarrow E[\ell^n]$. The Tate module is a free $\mathbb{Z}_\ell$-module of rank 2; this can be easily seen, since $E_{\ell^n} \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$ and $\varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} = \mathbb{Z}_\ell$. Denote by $V_\ell(E)$ the finite dimensional $\mathbb{Q}_\ell$-vector space obtained by extension of scalars from $T_\ell(E)$, i.e.,

$$V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Then one defines the ℓ-adic representation of E as

$$\rho_{E,\ell} \colon \operatorname{Gal}_K \longrightarrow \operatorname{Aut}(V_\ell(E)).$$

Choosing a basis of $T_\ell(E)$ in the natural manner (i.e. choosing the basis for $E[\ell^n]$ as above) gives a $\mathbb{Z}_\ell$-basis in $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, which gives the isomorphism $\operatorname{GL}_2(\mathbb{Q}_\ell) \cong \operatorname{Aut}(V_\ell(E))$ and also this basis forms a full $\mathbb{Z}_\ell$-lattice of $V_\ell(E)$. We know that $\rho_{E,\ell}$ stabilises a full $\mathcal{O}_\lambda$-lattice of V, by Proposition 1.2.15, but we would like to prove that this particular $\mathbb{Z}_\ell$-lattice is the one being stabilised. This requires some computations.

For ease of reading during this part, let $T_\ell = T_\ell(E)$ and $V_\ell = V_\ell(E)$. We can write V_ℓ as the localisation of T_ℓ at $1/\ell$, $V_\ell = T_\ell[1/\ell]$. Then,

$$V_\ell/T_\ell = T_\ell[1/\ell]/T_\ell = \bigcup_n \ell^{-n}T_\ell/T_\ell.$$

Note that $\ell^{-n}T_\ell/T_\ell \cong T_\ell/\ell^nT_\ell \cong E[\ell^n]$. Hence,

$$V_\ell/T_\ell \cong \bigcup_n E[\ell^n].$$

This induces an isomorphism $\operatorname{Aut}(V_\ell/T_\ell) \cong \operatorname{Aut}(\bigcup_n E[\ell^n])$. We want to see that there is an isomorphism between $\operatorname{Aut}(T_\ell)$ and $\operatorname{Aut}(V_\ell/T_\ell)$. We have the commutative diagram

$$\begin{tikzcd}
\vdots & \vdots & \vdots \\
\ell^{-n}T_\ell/T_\ell \arrow[u, "{[\ell]}"] \arrow[r, "\sim"] & T_\ell/\ell^n T_\ell \arrow[u, "\mathrm{proj}"] \arrow[r, "\sim"] & E[\ell^n] \arrow[u, "{[\ell]}"] \\
\ell^{-n-1}T_\ell/T_\ell \arrow[u, "{[\ell]}"] \arrow[r, "\sim"] & T_\ell/\ell^{n+1} T_\ell \arrow[u, "\mathrm{proj}"] \arrow[r, "\sim"] & E[\ell^{n+1}] \arrow[u, "{[\ell]}"] \\
\vdots \arrow[u, "{[\ell]}"] & \vdots \arrow[u, "\mathrm{proj}"] & \vdots \arrow[u, "{[\ell]}"]
\end{tikzcd}$$

where $[\ell]$ denotes the multiplication by ℓ isogeny. These give a natural inclusion map $\ell^{-(n+1)}T_\ell/T_\ell \longrightarrow \ell^{-n}T_\ell/T_\ell$ which give V_ℓ/T_ℓ as a projective limit. Taking inverse limit on $T_\ell/\ell^n T_\ell \cong E[\ell^n]$ gives again the Tate module T_ℓ. And obviously, since $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$, taking projective limits gives $\mathbb{Z}_\ell^2$. So we can redraw the diagram above as:

$$\begin{tikzcd}
\vdots & \vdots & \vdots \\
\ell^{-n}T_\ell/T_\ell \arrow[u, "{[\ell]}"] \arrow[r, "\sim"] & T_\ell/\ell^n T_\ell \arrow[u, "\mathrm{proj}"] \arrow[r, "\sim"] & E[\ell^n] \arrow[u, "{[\ell]}"] \\
\ell^{-n-1}T_\ell/T_\ell \arrow[u, "{[\ell]}"] \arrow[r, "\sim"] & T_\ell/\ell^{n+1} T_\ell \arrow[u, "\mathrm{proj}"] \arrow[r, "\sim"] & E[\ell^{n+1}] \arrow[u, "{[\ell]}"] \\
\vdots \arrow[u, "{[\ell]}"] & \vdots \arrow[u, "\mathrm{proj}"] & \vdots \arrow[u, "{[\ell]}"] \\
V_\ell/T_\ell \arrow[u] \arrow[r, "\sim"] & T_\ell \arrow[u] \arrow[r, "\sim"] & \mathbb{Z}_\ell^2 \arrow[u]
\end{tikzcd}$$

Finally, the same diagram is given when taking automorphisms,

$$\begin{tikzcd}
\vdots & \vdots & \vdots \\
\mathrm{Aut}(\ell^{-n}T_\ell/T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{Aut}(T_\ell/\ell^n T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[u] \\
\mathrm{Aut}(\ell^{-n-1}T_\ell/T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{Aut}(T_\ell/\ell^{n+1} T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \arrow[u] \\
\vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] \\
\mathrm{Aut}(V_\ell/T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{Aut}(T_\ell) \arrow[u] \arrow[r, "\sim"] & \mathrm{GL}_2(\mathbb{Z}_\ell) \arrow[u]
\end{tikzcd}$$

So, denoting by $E[\ell^\infty] = \bigcup_n E[\ell^n]$, we have an ℓ-adic representation

$$\phi_{E,\ell^\infty} \colon \operatorname{Gal}_K \longrightarrow \operatorname{Aut}(E[\ell^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Considering the inclusion $\mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$, then the representations ϕ_{E,ℓ^∞} and $\rho_{E,\ell}$ give the same representation: the action of Gal_K on V_ℓ is determined by the action of Gal_K on T_ℓ.

Again in [30], Serre gives a theorem for surjectivity in the non-CM case:

Theorem 1.2.24. *Let K be a number field and E an elliptic curve without complex multiplication. Then for all but finitely many primes ℓ, we have $\rho_{E,\ell}(\operatorname{Gal}_K) = \operatorname{Aut}(E[\ell^\infty])$.*

Our interest in this thesis is to compare Galois representations, i.e. to determine when two representations are equivalent. As we have seen in Proposition 1.2.19, a way to do so is by comparing the traces of the representations in the Frobenius elements at unramified primes. The following proposition is going to help us to compute these traces in the case of elliptic curves:

Proposition 1.2.25. *Let ℓ be a prime and let E be an elliptic curve over $\mathbb{Q}$ with conductor N. The Galois representation $\rho_{E,\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathfrak{p}$ be a prime above it. Then, one has*

$$\operatorname{tr}(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = a_p(E) \quad \text{and} \quad \det(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = \chi_\ell(\mathrm{Frob}_\mathfrak{p}) = p,$$

where χ_ℓ is the ℓ-adic cyclotomic character. In particular, the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ is:

$$x^2 - a_p(E)x + p.$$

Remark 1.2.26. For E an elliptic curve defined over a number field K, one can consider the system of ℓ-adic representations

$$\rho_{E,\bullet} := \{\rho_{E,\ell} \colon \operatorname{Gal}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)\}_{\ell \text{ prime number}}$$

Even though they are representations into different groups, they share many properties, since they come from the elliptic curve E. For example, for each finite prime $\mathfrak{p}$ of K, the type of reduction of E at $\mathfrak{p}$ carrier information about the image of the decomposition group at this prime by the representation $\rho_{E,\ell}$. An application of this observation is the Néron-Ogg-Shafarevich criterion [32, Ch. 7, Thm. 7.1].

This allows us to generalise the proposition above:

Proposition 1.2.27. *Let E be an elliptic curve defined over a number field K, let ℓ be a rational prime and let $\mathfrak{p}$ be a finite place of K of good reduction for E such that $\mathfrak{p} \nmid \ell$. Let $\mathrm{Frob}_\mathfrak{p}$ be an element of Gal_K projecting onto the Frobenius map in $\operatorname{Gal}(\bar{k}_\mathfrak{p}/k_\mathfrak{p})$, the absolute Galois group of the residue field $k_\mathfrak{p}$. Then,*

$$\operatorname{tr}(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = a_\mathfrak{p} = 1 + N_{K/\mathbb{Q}}(\mathfrak{p}) - \#E(k_\mathfrak{p})$$

$$\det(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p}) = N_{K/\mathbb{Q}}(\mathfrak{p}),$$

where $N_{K/\mathbb{Q}}(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in $K/\mathbb{Q}$ which is equal to the cardinal of the residual field $k_\mathfrak{p}$. Particularly, the characteristic polynomial is

$$x^2 - a_\mathfrak{p}x + N_{K/\mathbb{Q}}(\mathfrak{p}).$$

Finally, one might consider what is the representation of the full torsion group of E, that is, $E_{tors} = \bigcup_n E[n]$. One can define the automorphisms of E_{tors} as the projective limit

$$\operatorname{Aut}(E_{tors}) = \varprojlim_n \operatorname{Aut}(E[n])$$

Since $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, $\operatorname{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, so taking projective limits on both sides yields

$$\operatorname{Aut}(E_{tors}) = \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

where $\widehat{\mathbb{Z}}$ is the Prüfer ring, $\varprojlim \mathbb{Z}/n\mathbb{Z}$. The Galois group Gal_K acts continuously on $\operatorname{Aut}(E[n])$, hence, it acts continuously on $\operatorname{Aut}(E_{tors})$, giving the representation

$$\rho_E \colon \mathrm{Gal}_K \longrightarrow \operatorname{Aut}(E_{tors}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Galois representations and modular forms

We are going to associate a Galois representation to a modular curve $X_1(N)$ and we are going to see that we can decompose them into 2-dimensional representations associated to modular forms. This will give the desired representation $\rho_{f,\ell}$ for a given modular form f.

Let N be a positive integer and let ℓ be a rational prime. The modular curve $X_1(N)$ is a projective nonsingular algebraic curve over $\mathbb{Q}$. Let g denote its genus. The complexification $X_1(N)_{\mathbb{C}}$ defined by the same equations but viewing the curve over $\mathbb{C}$, can also be viewed as a compact Riemann surface. The Jacobian of a modular curve is a g-dimensional complex torus:

$$J_1(N) = \operatorname{Jac}(X_1(N)_{\mathbb{C}}) \cong \mathbb{C}^g/\Lambda_g.$$

The Picard group of the modular curve is the Abelian group of divisor classes of the points of $X_1(N)$,

$$\operatorname{Pic}^0(X_1(N)) = \operatorname{Div}(X_1(N))/\operatorname{Div}^{\ell}(X_1(N)).$$

The group $\operatorname{Pic}^0(X_1(N))$ can be identified with a subgroup of $\operatorname{Pic}^0(X_1(N)_{\mathbb{C}})$ and the complex Picard group is naturally isomorphic to the Jacobian by Abel's theorem. Thus, there is an inclusion of ℓ^n-torsion,

$$i_n \colon \operatorname{Pic}^0(X_1(N))[\ell^n] \longrightarrow \operatorname{Pic}^0(X_1(N)_{\mathbb{C}})[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}.$$

Igusa's theorem states that $X_1(N)$ has good reduction at primes $p \nmid N$, so also there is a natural surjective reduction map $\operatorname{Pic}^0(X_1(N)) \longrightarrow \operatorname{Pic}^0(\widetilde{X}_1(N))$ which restricts to

$$\pi_n \colon \operatorname{Pic}^0(X_1(N))[\ell^n] \longrightarrow \operatorname{Pic}^0(\widetilde{X}_1(N)[\ell^n].$$

From algebraic geometry, let X be a curve of genus g over a field K and let M be an integer coprime to the characteristic of K. Then $\operatorname{Pic}^0(X)[M] \cong (\mathbb{Z}/M\mathbb{Z})^{2g}$ and if X has good reduction at a prime $p \nmid M$ over $\mathbb{Q}$, then the reduction map is injective on $\operatorname{Pic}^0(X)[M]$. Particularly, the inclusion i_n is an isomorphism and so is the surjection π_n for $p \nmid \ell N$.

Now we define the *ℓ-adic Tate module of* $X_1(N)$ as

$$T_\ell(\operatorname{Pic}^0(X_1(N))) = \varprojlim_n \operatorname{Pic}^0(X_1(N))[\ell^n].$$

Much in the same way as in the previous section, choosing a basis for $\mathrm{Pic}^0(X_1))[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ gives an isomorphims

$$T_\ell(\mathrm{Pic}^0(X_1(N))) \cong \mathbb{Z}_\ell^{2g}.$$

Any $\sigma \in \mathrm{Gal}_\mathbb{Q}$ defines an automorphism in $\mathrm{Div}^0(X_1(N))$,

$$\sigma\left(\sum n_P(P)\right) = \sum n_P(\sigma(P)),$$

i.e. it acts on the points. Since $\sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f))$ for any $f \in \overline{\mathbb{Q}}(X_1(N))$, the automorphism descends to $\mathrm{Pic}^0(X_1(N))$, giving an action,

$$\mathrm{Pic}^0(X_1(N)) \times \mathrm{Gal}_\mathbb{Q} \longrightarrow \mathrm{Pic}^0(X_1(N)).$$

Said action restricts to the ℓ^n-torsion (this is because the extension over $\mathbb{Q}$ obtained by attaching the ℓ^n torsion of the Picard group is Galois). This gives a commutative diagram

$$\begin{tikzcd}
 & \mathrm{Gal}_\mathbb{Q} \arrow[dl] \arrow[dr] & \\
\mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^n]) & & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^{n+1}]) \arrow[ll]
\end{tikzcd}$$

which allows us to take inverse limits and define the *$2g$-dimensional ℓ-adic Galois representation associated to $X_1(N)$*,

$$\rho_{X_1(N),\ell} \colon \mathrm{Gal}_\mathbb{Q} \longrightarrow \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

We could have defined $V_\ell(X_1(N)) = T_\ell(X_1(N)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ as we did in the previous section and by a similar argument, deduce that the representation over $V_\ell(X_1(N))$ has actually values on $\mathbb{Z}_\ell$, since the Galois groups acting on $V_\ell(X_1(N))$ actually acts on $T_\ell(X_1(N))$. Or viceversa, we could have given the arguments we have given in this section in the previous one. In fact, this latter approach is the one taken in [10].

Now we want to restrict this representation to be the representation of a modular form f.

Recall that the Hecke algebra $\mathbb{T}_\mathbb{Z}$ is the algebra is the algebra of $\mathrm{End}(S_2(\Gamma_1(N)))$ generated over $\mathbb{Z}$ by the Hecke operators. It acts on $\mathrm{Pic}^0(X_1(N))$ linearly, which restrictrs to the ℓ^n torsion and so the action extends to $T_\ell(\mathrm{Pic}^0(X_1(N)))$. The Galois action and the Hecke action on $\mathrm{Pic}^0(X_1(N))$ commute and therefore so do the two actions on $T_\ell(\mathrm{Pic}^0(X_1(N)))$.

We have similar proposition to Proposition 1.2.25:

Proposition 1.2.28. *Let ℓ be a prime and let N be a positive integer. The Galois representation $\rho_{X_1(N),\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathfrak{p}$ be a prime above it. Then the characteristic polynomial of $\rho_{X_1(N),\ell}(\mathrm{Frob}_\mathfrak{p})$ is*

$$x^2 - T_p x + \langle p \rangle p.$$

Consider a normalized eigenform $f \in S_2(N,\chi)$. The Hecke algebra contains an ideal associated to f, the kernel of the eigenvalue map

$$I_f = \{T \in \mathbb{T}_\mathbb{Z} \mid Tf = 0\},$$

and the Abelian variety attached to f is defined as

$$A_f = J_1(N)/I_f J_1(N).$$

There is an isomorphism

$$\mathbb{T}_{\mathbb{Z}}/I_f \cong \mathcal{O}_f := \bigoplus_{n\geq 0} \mathbb{Z}[a_n(f)].$$

Under this isomorphism, the Fourier coefficients $a_p(f)$ act on A_f as $T_p + I_f$. Also, $\mathcal{O}_f$ contains the values χ_n for positive n and $\chi(p)$ acts on A_f as $\langle p\rangle + I_f$.

Let K_f denote the fraction field of the ring $\mathcal{O}_f$. It is a number field whose extension degree $d = [K_f : \mathbb{Q}]$ is also the dimension of A_f as a complex torus. As with elliptic curves and modular curves, the Abelian variety has an ℓ-adic Tate module (as a matter of fact, elliptic curves' is just an example of this one),

$$T_\ell(A_f) = \varprojlim_n A_f[\ell^n] \cong \mathbb{Z}_\ell^{2d}.$$

The action of $\mathcal{O}_f$ on A_f is defined on the ℓ^n-torsion and extends to an action of $T_\ell(A_f)$. The following lemma shows that $\mathrm{Gal}_{\mathbb{Q}}$ acts on $T_\ell(A_f)$.

Lemma 1.2.29. *The map* $\mathrm{Pic}^0(X_1(N))[\ell^n] \longrightarrow A_f[\ell^n]$ *is surjective. Its kernel is stable under the action of* $\mathrm{Gal}_{\mathbb{Q}}$.

Proof. The proof is more involved than we would like to get, since it uses the homology of $X_1(N)_{\mathbb{C}}$. It can be seen in [10], Lemma 9.5.2. □

So, $\mathrm{Gal}_{\mathbb{Q}}$ acts on $A_f[\ell^n]$ and therefore on $T_\ell(A_f)$. The action commutes with the action of $\mathcal{O}_f$ since the action of $\mathrm{Gal}_{\mathbb{Q}}$ and the one from $\mathbb{T}_{\mathbb{Z}}$ commute on $T_\ell(\mathrm{Pic}^0(X_1(N)))$. Choosing coordinates appropriately gives a Galois representation

$$\rho_{A_f,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{2d}(\mathbb{Q}_\ell).$$

The representation is unramified at primes $p \nmid \ell N$ since its kernel contains $\mathrm{Ker}(\rho_{X_1(N),\ell})$. For any such prime p, let $\mathfrak{p}$ be a prime above it. Then at the level of Abelian varieties we have that T_p acts as $a_p(f)$, the pth Fourier coefficient of f, and $\langle p\rangle$ acts as $\chi(p)$, the character of the space of cusp forms where f is, $S_2(N,\chi)$, hence Proposition 1.2.28 says that the characteristic polynomial of $\rho_{A_f,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ is

$$x^2 - a_p(f)x + \chi(p)p.$$

The Tate module $T_\ell(A_f)$ has rank $2d$ over $\mathbb{Z}_\ell$. Since it is an $\mathcal{O}_f$-module, the tensor product $V_\ell(A_f) = T_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a module over $\mathcal{O}_f \otimes \mathbb{Q}_\ell = K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. The absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$ acts $(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$-linearly on $V_\ell(A_f) \cong (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^2$. Choosing a basis B of $V_\ell(A_f)$ gives an isomorphism $\mathrm{GL}_2(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \cong \mathrm{Aut}(V_\ell(A_f))$.

Remark 1.2.30. We recall the following result from Algebraic Number Theory. Let E be a number field and $\mathcal{O}_K$ its ring of integers. Completing E by a prime $\lambda \subset \mathcal{O}_E$ gives the field E_λ with ring of integers

$$\mathcal{O}_{E,\lambda} = \varprojlim_n \mathcal{O}_E/\lambda^n.$$

If ℓ is a rational prime such that λ is above ℓ, then $\mathbb{Z}_\ell$ is a subring of $\mathcal{O}_{E,\lambda}$ and $\mathbb{Q}_\ell$ a subfield of E_λ. Let f_λ be the residual degree $f(\lambda/\ell) = [k_\lambda : \mathbb{F}_\ell]$ and e_λ the ramification index $e(\lambda/\ell)$. Then $[E_\lambda : \mathbb{Q}_\ell] = e_\lambda f_\lambda$ and there is a ring isomorphism

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} E_\lambda.$$

Then, $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_{f,\lambda}$, so for each λ we have

$$\rho_{f,\lambda}\colon \operatorname{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

This proves that for every normalised eigenform $f \in S_2(N, \chi)$ with number field K_f, ℓ a prime, for each λ maximal ideal of $\mathcal{O}_{K_f}$ lying over ℓ, there exists a 2-dimensional Galois representation

$$\rho_{f,\lambda}\colon \operatorname{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

This representation is unramified at every prime $p \nmid \ell N$ and for any such p with $\mathfrak{p}$ a prime lying over it, the image of the Frobenius at $\mathfrak{p}$ has characteristic polynomial

$$x^2 - a_p(f)x + \chi(p)p.$$

To finish off both examples, we have two theorems which are going to be very important for the examples of representations arising from abelian varieties.

Theorem 1.2.31. *If A is an abelian variety defined over a number field K, then $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$ is a semisimple representation for the absolute Galois group Gal_K of K.*

Theorem 1.2.32. *Let A and A' be two abelian varieties defined over a number field K. Then A and A' are K-isogenous if and only if $V_\ell(A) \sim V_\ell(A')$.*

Chapter 2

Comparing Galois representations: the residually irreducible case.

2.1 The deviation group $\delta(G)$

Let G be an arbitrary group and let E be a local field with ring of integers $\mathcal{O}_\lambda$, maximal ideal λ and residue field k. Let $\rho_1, \rho_2 \colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}_\lambda)$ be two λ-adic representations. We are interested in deciding when $\rho_1 \sim \rho_2$, that is, when the semisimplifications of ρ_1 and ρ_2 are isomorphic. In order to do this, we are going to construct a group $\delta(G)$ in which we will be able to find a finite set of elements where, if the representations coincide, then their semisimplifications will be isomorphic, otherwise, they won't.

Let us start by extending the map $\rho_1 \times \rho_2 \colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}_\lambda) \times \mathrm{GL}_n(\mathcal{O}_\lambda)$ to an homomorphism of $\mathcal{O}_\lambda$-modules

$$\rho\colon \mathcal{O}_\lambda[G] \longrightarrow M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda).$$

Recall that $\mathcal{O}_\lambda[G]$ is the group $\mathcal{O}_\lambda$-module for G, i.e. it is the $\mathcal{O}_\lambda$-module with basis the elements of G, which can be described as:

$$\mathcal{O}_\lambda[G] = \left\{ \sum_{\substack{i\in I\\ \#I<\infty}} a_i g_i \;\middle|\; a_i \in \mathcal{O}_\lambda,\ g_i \in G \right\}.$$

For $x = \sum a_i g_i \in \mathcal{O}_\lambda[G]$, we set

$$\rho\left(\sum g_i a_i\right) = \left(\sum a_i \rho_1(g_i), \sum a_i \rho_2(g_i)\right).$$

Notice that it is only natural that the image is not in $\mathrm{GL}_n(\mathcal{O}_\lambda) \times \mathrm{GL}_n(\mathcal{O}_\lambda)$ since, in general, it is not true that $\mathrm{GL}_n(\mathcal{O}_\lambda)$ is closed under $\mathcal{O}_\lambda$-linear combinations.

Remark. Notice that $\mathcal{O}_\lambda[G]$ and $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$ are rings, and also $\mathcal{O}_\lambda$ is contained in the center of $\mathcal{O}_\lambda[G]$ and $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$, then we can see them both as $\mathcal{O}_\lambda$ associative algebras. Particularly, ρ is an $\mathcal{O}_\lambda$-algebra homomorphism.

Now let M be the image of ρ in $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$ and consider the composition

$$\delta\colon G \longrightarrow M^\times \longrightarrow (M/\lambda M)^\times.$$

Definition 2.1.1. The image $\delta(G)$ of G in $(M/\lambda M)^\times$ is called the *deviation group* of the pair (ρ_1, ρ_2).

Remark. Consider the short exact sequence associated to the reduction modulo λ:

$$0 \longrightarrow M_n(\lambda) \longrightarrow M_n(\mathcal{O}_\lambda) \longrightarrow M_n(k) \longrightarrow 0.$$

This short exact sequence identifies $M_n(k) \oplus M_n(k)$ with $R/\lambda R$, where $R = M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$ (recall that given M, N two A-modules, for a commutative ring A, and $I \subseteq A$ an ideal, $(M \oplus N)/I(M \oplus N) \cong M/IM \oplus N/IN$). Since $\delta(G)$ is a subgroup of $(M/\lambda M)^\times$ and $M \subseteq R$, it might be tempting to think that $\delta(G)$ is a subgroup of $(R/\lambda R)^\times = \mathrm{GL}_n(k) \times \mathrm{GL}_n(k)$. To show that this is not the case, let

$$\overline{M} = M/(M \cap \lambda R).$$

Since $\lambda M \subseteq M \cap \lambda R$, we have a short exact sequence involving $M/\lambda M$:

$$0 \longrightarrow (M \cap \lambda R)/\lambda M \longrightarrow M/\lambda M \longrightarrow \overline{M} \longrightarrow 0.$$

Writing $\overline{G}$ for the image of G in $\overline{M}^\times \subseteq (R/\lambda R)^\times$, we have a short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1, \tag{2.1}$$

where the kernel $N(G)$ is the image of $\rho(G) \cap (1 + \lambda R)$ in $(M/\lambda M)^\times$, and in general its nonzero.

Proposition 2.1.2. *The group $\delta(G)$ is finite. More precisely,*

$$|\delta(G)| < |k|^{2n^2}.$$

Proof. M is a submodule of the free $\mathcal{O}_\lambda$-module $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$. Since $\mathcal{O}_\lambda$ is a local ring, M itself is free of rank r, where r satisfies the inequality

$$r \leq \operatorname{rank}(M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)) = 2n^2.$$

Since M is an $\mathcal{O}_\lambda$-module, $M/\lambda M$ is a $k = \mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda$-algebra of dimension r, hence:

$$|\delta(G)| \leq |(M/\lambda M)^\times| < |k|^r \leq |k|^{2n^2}.$$

□

The following proposition is a step towards deciding when $\rho_1 \sim \rho_2$.

Proposition 2.1.3. *Let Σ be a subset of G surjecting onto $\delta(G)$. Then,*

$$\rho_1 \otimes E \sim \rho_2 \otimes E \iff \mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g)),\ \forall g \in \Sigma.$$

Proof. The implication $\rho_1 \otimes E \sim \rho_2 \otimes E \Rightarrow \mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g))$ is obvious.

For the other implication, suppose that $\rho_1 \not\sim \rho_2$. Then $\mathrm{tr}(\rho_1) \neq \mathrm{tr}(\rho_2)$ for some $g \in G$. Since this is an inequality in $\mathcal{O}_\lambda$, it implies that there exists an integer $\alpha \geq 1$ such that

$$\mathrm{tr}(\rho_1(g)) \equiv \mathrm{tr}(\rho_2(g)) \pmod{\lambda^\alpha} \quad \text{and} \quad \mathrm{tr}(\rho_1(g)) \not\equiv \mathrm{tr}(\rho_2(g)) \pmod{\lambda^{\alpha+1}}.$$

Choose an uniformiser π, i.e. choose $\pi \in \mathcal{O}_\lambda$ such that $\lambda = \pi\mathcal{O}_\lambda$. We can define the map

$$\begin{array}{rccl} \widetilde{\phi}\colon & G & \longrightarrow & \mathcal{O}_\lambda \\ & g & \longmapsto & \pi^{-\alpha}[\mathrm{tr}(\rho_2(g)) - \mathrm{tr}(\rho_1(g))] \end{array}$$

Our objective now is to descend $\widetilde{\phi}$ to map Φ from $\delta(G)$ instead of G. Since Σ surjects into $\delta(G)$, then we are going to be able to find an element g' of this set such that $\Phi(\delta(g'))$ is not in λM, and hence, the traces restricted to the set Σ will also be non-equal, which is what we want to prove.

This map can be extended to an $\mathcal{O}_\lambda$-linear map

$$\phi\colon M \longrightarrow \mathcal{O}_\lambda, \quad \phi(M) \nsubseteq \lambda.$$

Following the same steps as in the definition of $\delta(G)$, we have the following commutative diagram:

$$\begin{tikzcd}
G \arrow[r, "\widetilde{\phi}"] \arrow[d, hook, "i"'] & \mathcal{O}_\lambda \\
\mathcal{O}_\lambda[G] \arrow[r, two heads, "\rho"] & M \arrow[u, dashed, "\phi"']
\end{tikzcd}$$

To see that $\phi(M) \nsubseteq \lambda$, notice that $\phi(\rho(i(g))) = \pi^{-\alpha}[\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g))] \notin \lambda$, since $\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g)) \not\equiv 0 \pmod{\lambda^{\alpha+1}}$.

The map ϕ descends to a non-zero k-linear map $M/\lambda M \longrightarrow k$, hence to a function

$$\Phi\colon \delta(G) \longrightarrow k$$

which is non-zero because $\delta(G)$ spans $M/\lambda M$ (since $\rho(G)$ spans M and $\delta(G) \subseteq (M/\lambda M)^\times \subseteq M/\lambda M$ is the image of $\rho(G)$).

Hence, since Σ surjects onto $\delta(G)$, there exists a $g' \in \Sigma$ such that $\Phi(\delta(g')) \neq 0$, i.e.

$$\phi(g) = \pi^{-\alpha}[\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g))] \notin \lambda.$$

In particular, $\operatorname{tr}(\rho_1(g')) \neq \operatorname{tr}(\rho_2(g'))$, so $\operatorname{tr}(\rho_1)|_\Sigma \neq \operatorname{tr}(\rho_2)|_\Sigma$. □

Remark. When $E = \mathbb{Q}_\ell$, for a prime ℓ, then we can choose ℓ as the uniformizer, hence the map ϕ can be written as

$$\phi(g) = \frac{\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g))}{\ell^\alpha}.$$

Corollary 2.1.4. *Let $\mathcal{R}$ be a class of representations of G defined over $\mathcal{O}_\lambda$ and Σ be a subset of G surjecting onto all the deviation groups of pairs $\rho_1, \rho_2 \in \mathcal{R}$. Then, given two representations ρ_1 and ρ_2,*

$$\rho_1 \sim \rho_2 \iff \operatorname{tr}\rho_1|_\Sigma = \operatorname{tr}\rho_2|_\Sigma.$$

In particular, if $\mathcal{R}$ is the class of representations of degree n, it is enough to ask that Σ surjects onto all quotients of G of size bounded by $|k|^{2n^2}$. If G has only a finite number of such quotients, this gives an algorithm to decide the equivalence of n-dimensional λ-adic representations of G.

Application to Galois representation

Given a number field K, we specialize now to the case $G = \operatorname{Gal}(\overline{K}/K) = \operatorname{Gal}_K$, the absolute Galois group of K.

Lemma 2.1.5. *Let ρ_1 and ρ_2 be two λ-adic representations of Gal_K. Then $\delta(\operatorname{Gal}_K)$ is unramified outside of $\operatorname{Ram}(\rho_1) \cup \operatorname{Ram}(\rho_2)$.*

Proof. For a prime $\mathfrak{p} \notin \mathrm{Ram}(\rho_1) \cup \mathrm{Ram}(\rho_2)$, we have $I(\mathfrak{p}) \subseteq \mathrm{Ker}(\rho_1) \cap \mathrm{Ker}(\rho_2)$. Hence, $I(\mathfrak{p}) \subseteq \mathrm{Ker}(\rho)$, where recall that $\rho = \rho_1 \times \rho_2$. That is, the image of $\rho(\mathrm{Gal}_K)$ is unramified at $\mathfrak{p}$. Hence, $\delta(\mathrm{Gal}_K)$ being a finite quotient of $\rho(\mathrm{Gal}_K)$, is also unramified at $\mathfrak{p}$. □

This is a better version of Proposition 1.2.19. This lemma is telling us that since $\delta(G)$ is a finite group, it can be identified with a finite extension F/K unramified outside of $\mathrm{Ram}(\rho_1) \cup \mathrm{Ram}(\rho_2)$.

Corollary 2.1.6. *Given a finite set S of places of K and an integer $n \geq 1$, there exists a finite set of primes T disjoint from S such that if ρ_1 and ρ_2 are any λ-adic representations of degree n of Gal_K, unramified outside S, then*

$$\rho_1 \sim \rho_2 \iff \operatorname{tr} \rho_1|_\Sigma = \operatorname{tr} \rho_2|_\Sigma,$$

where $\Sigma = \{\mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \in T\}$.

Proof. By the Minkowski theorem, there are only a finite number of Galois extensions L/K unramified outside S and of degree bounded by $|k|^{2n^2}$. One can take for T the finite set of primes $\mathfrak{p}$ for which the Frobenius elements $\mathrm{Frob}_\mathfrak{p}$ exhaust all conjugacy classes of $\mathrm{Gal}(L/K)$ for such extensions L/K. □

2.2 The method of the quartic fields

In 1984-1985, Serre [27, 29], based on Falting's ideas of the deviation group we have introduced, made a computable method for these. He focused on the case of 2-adic representations of dimension 2. Particularly, in [27] Serre explicitly uses the method to solve two problems:

(a) Every elliptic curve over $\mathbb{Q}$ of conductor 11 is $\mathbb{Q}$-isogenous to an already known curve.

(b) (Following Mestre [19]) The known elliptic curve of conductor 5077 is “of Weil”, i.e. modular.

We are going to develop the required theory for a general λ-adic representation of dimension n and then we are going to specialise to the case $\lambda = n = 2$. After that, we are going to explain in detail both examples above.

Let $\rho_1, \rho_2 \colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}_\lambda)$ be two semisimple λ-adic representations of dimension n and let $\delta(G)$ be the associated deviation group to the pair. Let us suppose that the residual representations $\overline{\rho_1}, \overline{\rho_2} \colon G \longrightarrow \mathrm{GL}_n(k)$ are equal, but that the representations $\rho_1 \otimes E$ and $\rho_2 \otimes E$ are not isomorphic, i.e. conjugated by an element of $\mathrm{GL}_n(E)$.

Let β be the maximal integer such that ρ_1 and ρ_2 are conjugated modulo λ^β. We know that $\beta \geq 1$, since $\overline{\rho_1} = \overline{\rho_2}$. We have also seen in the proof of Proposition 2.1.3, there exists a maximal α such that $\mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \pmod{\lambda^\alpha}$ and $\mathrm{tr}(\rho_1) \not\equiv \mathrm{tr}(\rho_2)$ $\pmod{\lambda^{\alpha+1}}$. Particularly, ρ_1 and ρ_2 are not conjugated modulo $\lambda^{\alpha+1}$, hence $\beta \leq \alpha$. In particular, β is finite.

Now, replacing ρ_2 by a conjugate if necessary, we can assume

$$\rho_1 \equiv \rho_2 \pmod{\lambda^\beta}, \quad \rho_1 \not\equiv \rho_2 \pmod{\lambda^{\beta+1}}.$$

Hence, for every $g \in G$, we have

$$\rho_1(g) - \rho_2(g) \equiv 0 \pmod{\lambda^\beta} \Longrightarrow \rho_1(g) - \rho_2(g) = \theta_g \pi^\beta,$$

for some $\theta_g \in M_n(\mathcal{O}_\lambda)$ and π an uniformiser of λ. We can still simplify this equation one more step:

$$\rho_1(g) - \rho_2(g) = \theta_g \pi^\beta \Longrightarrow \rho_1(g) = (1 + \pi^\beta \theta_g \rho_2(g)^{-1})\rho_2(g).$$

Now, let $\theta \colon G \longrightarrow M_n(\mathcal{O}_\lambda)$ be the map $g \longmapsto \theta_g \rho_2(g)^{-1}$. We can write

$$\rho_2 = (1 + \pi^\beta \theta)\rho_1. \tag{2.2}$$

As a remark, notice that $\theta(G) \not\subseteq M_n(\lambda)$, since $\rho_1 \not\equiv \rho_2 \pmod{\lambda^{\beta+1}}$.

Whenever we have $\alpha = \beta$, the α defined in Proposition 2.1.3, this particular expression allows us to write the map defined in that as:

$$\phi(g) = \frac{\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g))}{\pi^\beta} = \operatorname{tr}(\theta(g)\rho_1(g)),$$

which defines a map from the group G to $M_n(\mathcal{O}_\lambda) \times \mathrm{GL}_n(\mathcal{O}_\lambda)$, $g \longmapsto (\theta(g), \rho_1(g))$. This map does not require of $\alpha = \beta$, it works in general, but it is a natural deduction when it is the case. We are going to see that when $n = \lambda = 2$, Serre proves (in the letter to Tate [27] which gave birth to this method) that $\alpha = \beta$, and hence the function defined in Proposition 2.1.3 descends to this function we just defined.

Restricting ourselves to the field k (we want it to factor through the deviation group $\delta(G)$), this map is a group homomorphism when we endow the image with the semidirect product

$$(A, B) \star (C, D) = (A + CBC^{-1}, BD).$$

The following proposition proves it.

Proposition 2.2.1. *If $\rho_1 \not\simeq \rho_2$, the function*

$$\begin{array}{rccl} \varphi\colon & G & \longrightarrow & M_n(k) \rtimes \mathrm{GL}_n(k) \\ & g & \longmapsto & (\theta(g) \pmod{\lambda}, \rho_1(g) \pmod{\lambda}) \end{array}$$

is a group homomorphism which factors through the deviation group $\delta(G)$.

Proof. First let us show that φ is a group homomorphism. That is, given $g, h \in G$ we want to show that

$$\varphi(gh) = (\theta(gh) \pmod{\lambda}, \rho_1(gh) \pmod{\lambda}) =$$

$$= (\theta(g) + \rho_1(g)\theta(h)\rho_1(g)^{-1} \pmod{\lambda}, \rho_1(g)\rho_2(h) \pmod{\lambda} = \varphi(g)\varphi(h),$$

where the product is the group operation in the semidirect product coming from the action of $\mathrm{GL}_n(k)$ on $M_n(k)$ by conjugation. We already know that the second component is that way, since ρ_1 is already a group homomorphism. Hence, we need to show that

$$\varphi(gh)_1 = \theta(g) + \rho_1(g)\theta(h)\rho_1(g)^{-1} \pmod{\lambda}.$$

For us to do so, using (2.2),

$$\rho_2(g) = (1 + \pi^\beta \theta(g))\rho_1(g) \quad \text{and} \quad \rho_2(h) = (1 + \pi^\beta \theta(h))\rho_1(h).$$

Then, we also have

$$\rho_2(gh) = \rho_2(g)\rho_2(h), \tag{1}$$

for being ρ_2 a group homomorphism, and again from (2.2),

$$\rho_2(gh) = (1 + \pi^\beta\theta(gh))\rho_1(gh). \tag{2}$$

Now, (1) can be expanded using (2.2) on each term, which yields

$$\rho_2(gh) = (1 + \pi^\beta\theta(g))\rho_1(g)(1 + \pi^\beta\theta(h))\rho_1(h) =$$

$$= \rho_1(g)\rho_1(h) + \pi^\beta(\theta(g)\rho_1(g)\rho_1(h) + \rho_1(g)\theta(h)\rho_1(h)) + \pi^{2\beta}\theta(g)\rho_1(g)\theta(h)\rho_1(h).$$

Equaling the right hand side of the equation above with the right hand side of (2), we obtain

$$\rho_1(g)\rho_1(h) + \pi^\beta\theta(gh)\rho_1(g)\rho_1(h) =$$

$$= \rho_1(g)\rho_1(h) + \pi^\beta(\theta(g)\rho_1(g)\rho_1(h) + \rho_1(g)\theta(h)\rho_1(h)) + \pi^{2\beta}\theta(g)\rho_1(g)\theta(h)\rho_1(h)$$

Multiplying by $\rho_1(gh)^{-1} = \rho_1(h)^{-1}\rho_1(g)^{-1}$ on the right and by $\pi^{-\beta}$, we obtain an equation for $\theta(gh)$:

$$\theta(gh) = \theta(g) + \rho_1(g)\theta(h)\rho_1(g)^{-1} + \pi^\beta\theta(g)\rho_1(g)\theta(h)\rho_1(g)^{-1}.$$

Hence, since $\beta \geq 1$, reducing modulo $\lambda = \pi\mathcal{O}_\lambda$, the desired equality.

$$\varphi_1(gh) = \theta(gh) \pmod{\lambda} = \theta(g) + \rho_1(g)\theta(h)\rho_1(g)^{-1} \pmod{\lambda}.$$

Now, let us show that φ factors through $\delta(G)$, i.e. let us show that $\mathrm{Ker}(\delta) \subseteq \mathrm{Ker}(\varphi)$. Let $g \in \mathrm{Ker}(\delta)$. Since $\rho_1 \times \rho_2(g) = \rho(g) \in 1 + \lambda M$, i.e. there exists $\{a_h\}_{h\in G} \subseteq \mathcal{O}_\lambda$ with $a_h = 0$ for almost all $h \in G$ such that

$$\rho(g) = 1 + \pi \sum_{h\in G} a_h\rho(h).$$

Since this is a cartesian product $\rho_1 \times \rho_2(g)$, the equation above is actually a pair of equations

$$\rho_i(g) = 1 + \pi \sum_{h\in G} a_h\rho_i(h).$$

For $i = 1$, this implies $\rho_1(g) \equiv 1 \pmod{\lambda}$. This gives us that the second component of $\varphi(g)$ is the identity element in $\mathrm{GL}_n(k)$. Moreover, using (2.2), the equation for $i = 2$ can be rewritten as

$$\rho_1(g) + \pi^\beta\theta(g)\rho_1(g) = 1 + \pi \sum_{h\in G} a_h\rho_1(h) + \pi^{\beta+1} \sum_{h\in G} a_h\theta(h)\rho_1(h).$$

Subtracting $\rho_1(g) = 1 + \pi\sum_{h\in G} a_h\rho_1(h)$ and multiplying by $\pi^{-\beta}$ to both sides, we obtain

$$\theta(g)\rho_1(g) = \pi^\beta \sum_{h\in G} a_h\theta(h)\rho_1(h).$$

Hence,

$$\theta(g) = \pi^\beta \sum_{h\in G} a_h\theta(h)\rho_1(hg^{-1}) \equiv 0 \pmod{\lambda}.$$

Therefore, the first component of $\varphi(g)$ is the identity element in $M_n(k)$. Which finishes the proof, since $\varphi(g) = (0, 1)$, hence $g \in \operatorname{Ker}(\varphi)$. □

Recall the short exact sequence (2.1). We can refine it to include $\varphi(G)$, the image of G in $M_n(k) \rtimes \mathrm{GL}_n(k)$, such that

$$\begin{tikzcd}
\delta(G) \arrow[r, two heads] & \varphi(G) \arrow[r, two heads] & \overline{G} .
\end{tikzcd}$$

Particularly, we can draw the full diagram

$$\begin{tikzcd}
0 \arrow[r] & (M \cap \lambda R)/\lambda M \arrow[r] & M/\lambda M \arrow[r] & \overline{M} \arrow[r] & 0 \\
1 \arrow[r] & N(G) \arrow[r] \arrow[u, hook] & \delta(G) \arrow[r] \arrow[u, hook] \arrow[d, two heads] & \overline{G} \arrow[r] \arrow[u, hook] & 1 \\
 & & \varphi(G) \arrow[ur, two heads] & &
\end{tikzcd}$$

Remark 2.2.2. In general, one does not have that the map $\delta(G) \twoheadrightarrow \varphi(G)$ is a monomorphism. From the proof of the Proposition above, we have that an element $g \in G$ lies in $\operatorname{Ker}(\delta)$ if and only if

$$\rho_1(g) = 1 + \pi \sum_{h \in G} a_h \rho_1(h),$$

$$\theta(g) = \pi \sum_{h \in G} a_h \theta(h) \rho_1(hg^{-1})$$

for some $a_h \in \mathcal{O}_\lambda$, all zero except a finite amount of them.

Also, from (2.2), and the following lemma, we have

$$\det(\rho_1) = (1 + \pi^\beta \operatorname{tr}(\theta) + O(\pi^{\beta^2})) \det(\rho_2). \tag{2.3}$$

Lemma 2.2.3. *Let R be a commutative ring and let $A \in \mathrm{GL}_n(R)$. Then, for $k \in R$,*

$$\det(1 + kA) = 1 + k \operatorname{tr}(A) + O(k^2).$$

Proof. This is straightforward to prove by induction. Start with $n = 2$, since the case $n = 1$ is uninteresting. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad 1 + kA = \begin{pmatrix} 1 + ka & kb \\ kc & 1 + kd \end{pmatrix}.$$

Then

$$\det(1 + kA) = \begin{vmatrix} 1 + ka & kb \\ kc & 1 + kd \end{vmatrix} = (1 + ka)(1 + kd) - k^2 bc = 1 + k \operatorname{tr}(A) + k^2 \det(A).$$

Suppose then the result to hold for $n - 1$ and let us prove the case n. Let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

We denote by A_{ij} the matrix in $\mathrm{GL}_{n-1}(R)$ which is the matrix A without the ith row and without the jth column. Then,

$$\det(1+kA) = (1+ka_11)\det(1+kA_{11}) + \sum_{i=2}^{n}(-1)^{i+1}ka_{i1}\det(1+kA_{i1}) =$$

$$= \det(1+kA_{11}) + k\sum_{i=1}^{n}(-1)^{i+1}a_{i1}\det(1+kA_{i1}).$$

Using the induction hypothesis on A_{i1} for $1 \leq i \leq n$, we have

$$\det(1+kA) = 1 + k\operatorname{tr}(A_{11}) + O(k^2) + ka_{11} = 1 + \operatorname{tr}(A) + O(k^2).$$

□

So, in addition, by (2.3), if we require $\det(\rho_2) = \det(\rho_1)$, then $0 = \pi^{\beta}\operatorname{tr}(\theta) + O(\pi^{\beta^2})$ which multiplying by $\pi^{-\beta}$ implies:

$$\operatorname{tr}(\theta) \equiv 0 \pmod{\lambda^{\beta}}$$

In particular, φ takes values in

$$M_n^0(k) \rtimes \mathrm{GL}_n(k)$$

where $M_n^0(k)$ denotes the set of $n \times n$ matrices of trace 0.

Gabriel Chênevert in [8, p.114] has a remark in which he explains that in conversations with Serre, he showed in [27] that ρ_1 and ρ_2 are conjugated modulo 2^{α} if and only if $\operatorname{tr}(\rho_1) \equiv \operatorname{tr}(\rho_2) \pmod{2^{\alpha}}$. Particularly, $\alpha = \beta$. This would mean that the function ϕ considered in Proposition 2.1.3 defined as

$$\phi(g) = 2^{-\alpha}(\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g)) \pmod{2}$$

descends to $\varphi(G)$. Consequently, $\varphi(G)$ can be used in place of $\delta(G)$ in Corollary 2.1.4, which makes the application to decide whether two representations satisfying the hypothesis of Serre are equivalent or not a lot easier. Namely, if $\rho_1 \not\sim \rho_2$, $\alpha = \beta$ and $\Sigma \subseteq G$ surjecting onto $\varphi(G)$, then there exists $g \in \Sigma$ such that

$$\operatorname{tr}(\rho_1(g)) \neq \operatorname{tr}(\rho_2(g)).$$

Particularly,

$$\operatorname{tr}(\theta(g)\rho_1(g)) \equiv \operatorname{tr}(\overline{\theta}(g)\overline{\rho_1}(g)) \not\equiv 0 \pmod{\lambda}.$$

In this case, the image of φ can be computed. Let $\rho_1, \rho_2 \colon G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_2)$ two 2-adic representations such that $\det(\rho_1) = \det(\rho_2)$ and the residual representations are equal and surjective. Then, seeing $M_2(\mathbb{F}_2)$ as an S_3-module under the action by conjugation of $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, we have[1]

$$M_2(\mathbb{F}_2) \cong \mathbb{F}_2^2 \oplus V_4,$$

[1] A proof of both isomorphisms above can be found in Appendix B. The second one is straightforward from the restriction of having trace zero.

where V_4 is the Klein group, which is isomorphic to $\mathbb{F}_2^2$. Likewise,

$$M_2^0(\mathbb{F}_2) \cong \mathbb{F}_2 \oplus V_4, \quad \mathbb{F}_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Then, if $\overline{\rho_1} = \overline{\rho_2}$ and its surjective, the second component of $\varphi(G)$ is the full S_3. That is,

$$\mathrm{Im}(\varphi) = N \rtimes S_3,$$

where N is a subgroup of $\mathbb{F}_2 \oplus V_4 \cong \mathbb{F}_2^3$. So, the index $[\mathbb{F}_2 \oplus V_4 : N]$ is either 1, 2 or 4. We know it can not be 8, because then it would imply that $\theta(g) = 0$ for every $g \in G$, i.e. $\mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \pmod{2^{\alpha+1}}$, which is not true by hypothesis. Then, we the only possibilities for $M_2(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)$ are:

$$\mathbb{F}_2 \rtimes S_3 \cong \{\pm 1\} \times S_3, \quad V_4 \rtimes S_3 \cong S_4, \quad (\mathbb{F}_2 \oplus V_4) \rtimes S_3 \cong \{\pm 1\} \times S_4.$$

2.2.1 Rational elliptic curves of conductor 11.

We let $E_{11}/\mathbb{Q}$ be the elliptic curve of conductor 11 defined by the Weierstrass equation

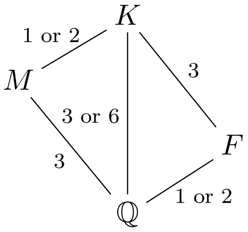
$$E_{11} \; : \; y^2 - y = x^3 - x^2.$$

We aim to show that every elliptic curve over $\mathbb{Q}$ of conductor 11 is $\mathbb{Q}$-isogenous to E_{11}. This result was first obtained by Agrawal, Coates, Hunt, and van der Poorten in [1] with a method that involved lots of computations. Later on, Serre on a letter to Tate on the 26th of October of 1984 [27] and simultaneously on his course of 1984-1985 at the Collège de France [29], gave a method applying Faltings' ideas to prove this result in a much shorter way, which is now known as *the method of quartic fields.*

We start with a general treatment of elliptic curves of prime conductor. Let E be an elliptic curve over $\mathbb{Q}$ with prime conductor $p \neq 2, 3$. We can assume that E is given by a Weierstrass model of the form

$$y^2 = f(x) := x^3 + a_2 x^2 + a_4 x + a_6, \qquad a_i \in \mathbb{Q}.$$

Suppose that E has no rational 2-torsion points. Since the 2-torsion points satisfy $y = 0$ in the above model, it follows the cubic $f(x)$ is irreducible over $\mathbb{Q}$. Let K be the splitting field of $f(x)$, that is, K is the 2-torsion field of E. Let M be the subfield of K generated by a root of $f(x)$ and let F be a field such that K/F is a cubic cyclic extension. This is possible because $K/\mathbb{Q}$ has degree 3 or 6, since $f(x)$ is irreducible and so $\mathrm{Gal}(K/\mathbb{Q})$ is embedded in a transitive subgroup of S_3, the symmetric group on 3 elements. The only possible options are S_3 or A_3, the alternating subgroup of S_3. (Note that in the case $[K : \mathbb{Q}] = 3$, we would have $K = M$ and $F = \mathbb{Q}$.) Hence, we have the following field extension diagram:



The following lemma is due to Setzer [31].

Lemma 2.2.4. *Keep the notation above.*

(1) *The Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ *is* S_3.

(2) $F = \mathbb{Q}(\sqrt{p}) \subset K$ *or* $F = \mathbb{Q}(\sqrt{-p}) \subset K$.

(3) *The extension* K/F *is unramified outside the primes dividing* 2.

Proof. We first show that p must factor in M as $\mathfrak{p}\mathfrak{q}^2$. Since E has prime conductor p it has multiplicative reduction at p and good reduction away from p. There is an integral model of E, i.e. an equation for E of the form $y^2 = f(x) := x^3 + b_2x^2 + b_4x + b_6$ with $b_i \in \mathbb{Z}$, where $f(x)$ is irreducible and has a double and a simple root modulo p. The splitting field of this new f is also K, and we let $M \subset K$ be the subfield generated by a root of $f(x)$. Thus at least two primes of M divide p. Moreover, the model for E can be chosen such that its discriminant is $\Delta = \pm 2^{12}p^n$, for some $n \geq 1$. (The explicit computations can be found in Setzer's article.) Hence, the only primes that may ramify in M are those dividing 2 and p. However, there are no cubic extensions of $\mathbb{Q}$ ramifying only at 2[2]. Thus, some prime of M dividing p must ramify in $M/\mathbb{Q}$, which proves the factorization of p. In particular, $M/\mathbb{Q}$ cannot be Galois, proving (1).

Since the discriminant of $f(x)$ is $\pm 2^8 p^n$, it differs from Δ by a square factor. Hence $F = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\pm p^n})$ and part (2) follows if we show that p ramifies in $F/\mathbb{Q}$. Let e be the ramification index of a prime of K lying over p, and let f be its residual degree. Let g be the number of primes dividing p in K, so that $gfe = 6$. But $g \geq 2$ and $2 \mid e$, from the factorization of p in M, thus $g = 3$, $e = 2$ and $f = 1$. Since K/F is cubic it follows that all the ramification of p occurs in $F/\mathbb{Q}$, proving (2). Further, no other primes besides those dividing 2 and p can ramify in K/F, so (3) holds. □

Corollary 2.2.5. *Let* $E/\mathbb{Q}$ *be an elliptic curve of prime conductor* p. *Assume* E *has no 2-torsion point defined over* $\mathbb{Q}$. *Then* $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{p})$ *or* $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-p})$, *where* Δ *is the discriminant of a model for* E.

Proof. This follows from the proof of part (2) in Lemma 2.2.4 and the fact that the discriminant of different models for E differ by a square in $\mathbb{Q}$. □

We can deduce further properties of E from the work of Brumer and Kramer. The following is [6, Cor. 5.3].

Lemma 2.2.6. *Let* $E/\mathbb{Q}$ *be a semistable elliptic curve of discriminant* Δ. *Suppose that* E *has no rational points of order 2.*

(1) *If E has good ordinary reduction or multiplicative reduction at 2, then 3 divides the order of the class group of* $\mathbb{Q}(\sqrt{\Delta})$ *modulo the subgroup generated by the classes of the ideals lying over 2. Particularly,* $3 \mid h(\mathbb{Q}(\sqrt{\Delta}))$.

(2) *If E has good supersingular reduction at 2, then:*

(a) $\Delta \equiv 5 \pmod 8$.

(b) For every $\alpha \in \mathbb{Q}(\sqrt{\Delta})$, *for which the ideal generated by* α *is a cube of an ideal prime to* 2, *we have* $\alpha \equiv 1 \pmod 2$.

[2] https://www.lmfdb.org/NumberField/?degree=3&ram_quantifier=exactly&ram_primes=2&search_type=List

(3) *Neither of* $\pm\Delta$ *is a perfect square.*

In our setting, the conductor of E is a prime p so E is semistable. A key hypothesis in the previous results is $E[2](\mathbb{Q}) = \emptyset$. For curves with prime conductor this is described by the following result (see [31, Thm. 2]).

Lemma 2.2.7. *Let* $p \neq 2, 3, 17$ *be a prime. There is an elliptic curve of conductor* p *over* $\mathbb{Q}$ *with a rational 2-torsion point if and only if* $p = u^2 + 64$ *for some integer* u.

The following theorem describes the 2-torsion field of certain elliptic curves with prime conductor for some primes.

Theorem 2.2.8. *Let* $N \equiv 3 \pmod 8$ *be a prime such that* 3 *does not divide the class number of* $\mathbb{Q}(\sqrt{N})$ *nor* $\mathbb{Q}(\sqrt{-N})$*. Let* $E/\mathbb{Q}$ *be an elliptic curve of conductor* N *and denote by* K *its 2-torsion field. Then, the following holds:*

(a) $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$*;*

(b) K *is the unique cubic cyclic extension of* $\mathbb{Q}(\sqrt{-N})$ *of conductor* (2)*;*

(c) E *has good supersingular reduction at 2.*

Before proving it, we need a lemma.

Lemma 2.2.9. *Let* $N > 3$ *be a prime such that* 3 *does not divide the class number of* $\mathbb{Q}(\sqrt{N})$ *nor* $\mathbb{Q}(\sqrt{-N})$*. Then there exists a unique cubic cyclic Galois extension of* $\mathbb{Q}(\sqrt{-N})$ *which is a subfield of the ray class field with modulus* (2)*.*

Proof. Let $L/\mathbb{Q}(\sqrt{-N})$ be the extension corresponding to the ray class group of modulus (2) (note that $\mathbb{Q}(\sqrt{-N})$ is totally complex so we don't have to allow ramification at the primes at ∞). From [21, Ch. V, Thm. 1.7], we know that the degree $[L : \mathbb{Q}(\sqrt{-N})] = h_{(2)}$ is given by the formula

$$h_{(2)} = h \cdot (U : U_{(2),1})^{-1} 2^{r_0} N_{\mathbb{Q}(\sqrt{-N})/\mathbb{Q}}((2)) \left(1 - \frac{1}{N_{\mathbb{Q}(\sqrt{-N})/\mathbb{Q}}((2))}\right),$$

where h is the class number of $\mathbb{Q}(\sqrt{-N})$, $r_0 = 0$ is the number of real places in the modulus (2), U is the group of units in $\mathbb{Q}(\sqrt{-N})$ and $U_{(2),1}$ is the elements of $a \in U$ which satisfy $\mathrm{ord}_2(a-1) \geq 1$. The units of $\mathbb{Q}(\sqrt{-N})$ are $\{\pm 1\}$ (since N is a prime greater than 3), hence $(U : U_{(2),1})^{-1} = 1$. We also have $N_{\mathbb{Q}(\sqrt{-N})/\mathbb{Q}}((2)) = 4$, thus $h_{(2)} = 3h$. By hypothesis, $3 \nmid h$ so 3 divides $h_{(2)}$ exactly once, which implies there is a unique degree 3 cyclic extension of $\mathbb{Q}(\sqrt{-N})$ inside L. □

Now we can prove the theorem.

Proof of Theorem 2.2.8. Recall that for any number field its narrow class number is of the form $2^s h$ where h is its class number. From our hypotheses, it follows that the narrow class numbers of $\mathbb{Q}(\sqrt{N})$ and $\mathbb{Q}(\sqrt{-N})$ are not divisible by 3.

From Lemma 2.2.7 we see that E has no 2-torsion point defined over $\mathbb{Q}$; indeed, if $N = u^2+64$, then $N \equiv u^2 \pmod 8$ but $N \equiv 3 \pmod 8$ and 3 is not a square modulo 8, a contradiction. By Lemma 2.2.4 we conclude that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, proving (a).

From Corollary 2.2.5 we know that either $F = \mathbb{Q}(\sqrt{N}) \subset K$ or $F = \mathbb{Q}(\sqrt{-N}) \subset K$ and, from part (3) of Lemma 2.2.4, all the ramification of K at p occurs in this quadratic subfield. Suppose that the common ramification index of the primes in K above 2 is $e_2 = 2$, then this ramification occurs also in F because K/F is cubic and so K/F is unramified at all finite places, contradicting the assumption on the narrow class number; if 2 is unramified in K we get a similar contradiction. Thus $e_2 = 3$ because an S_3-extension does not allow for totally ramified primes. Moreover, F is unramified at 2, so $F = \mathbb{Q}(\sqrt{-N})$ because $N \equiv 3 \pmod 8$.

Using Lemma 2.2.9, one proves (b), since N satisfies the hypothesis.

Finally, from Serre [30] and the fact that inertia at 2 has order 3, we conclude that E has good supersingular reduction at 2, proving (c). □

Proposition 2.2.10. *Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be non-isogenous elliptic curves with odd conductor N satisfying $a_2(E_1) = a_2(E_2) \in \{-2, 0, 2\}$. Suppose that $\bar{\rho}_{E_1,2} \simeq \bar{\rho}_{E_2,2}$ so that we can consider the map $\varphi\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow M_2^0(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)$ defined in Proposition 2.2.1,*

$$\varphi(g) = \left(2^{-\beta}(\rho_{E_1,2}(g) - \rho_{E_2,2}(g)) \pmod 2, \bar{\rho}_{E_1,2}(g)\right).$$

Write K for the common 2-torsion field of E_1 and E_2 and, let $\tilde{K}$ be the field fixed by φ. Then the extension $\tilde{K}/K$ is unramified outside N. Moreover, if $N = p$ is prime then $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq S_4$.

Proof. Suppose $\rho_{E_i,2}$ is unramified at p for both $i = 1, 2$, then any inertia subgroup $I_p \subseteq \mathrm{Gal}_{\mathbb{Q}}$ is contained in $\mathrm{Ker}(\rho_{E_i,2})$ for $i = 1, 2$. Thus $\varphi(g) = (0, 1)$ for all $g \in I_p$. Therefore, the primes that may ramify in $\tilde{K}$ are a subset of those for which $\rho_{E_1,2}$ or $\rho_{E_2,2}$ ramify. Moreover, from Proposition 1.2.25 it follows that $\tilde{K}$ may ramify only at primes $p \mid 2N$. So, the first statement follows if we show that $\tilde{K}/K$ is unramified at all primes of K above 2.

Since E_1 and E_2 have even trace of Frobenius at 2 they both have good supersingular reduction at 2. The theorem of Honda-Hill-Cartier [13] implies that the polynomial of the formal group associated to E_i at 2 is the same as the characteristic polynomial of the system of ℓ-adic representations at 2. This says that $a_2(E_i)$ determines the formal group of E_i at 2, which determines the 2-adic representation restricted to a decomposition group D_2 at 2. By assumption, we have $a_2(E_1) = a_2(E_2)$ therefore $\rho_{E_1,2}|_{D_2} \cong \rho_{E_2,2}|_{D_2}$, hence for all $x \in D_2$ we have $\varphi(x) = (0, \overline{\rho}_{E_1,2}(x))$. In particular, for $x \in I_2 \cap \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we have $\varphi(x) = (0, 1)$, hence $\tilde{K}/K$ is unramified at all primes $\mathfrak{p} \mid 2$ in K, as desired.

We will now prove the second statement. Assume $N = p$ is a prime. Since the curves are non-isogenous, $\tilde{K}/K$ is non-trivial and we know that $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ is isomorphic to one of $C_2 \times S_3$, S_4 or $C_2 \times S_4$. Moreover, the first part of the proof shows that the size of the inertia subgroups at 2 in $\tilde{K}$ is the same as in K which we know to be 3 because the curves have good supersingular reduction at 2. Therefore, $\varphi(I_2)$ is isomorphic to $\{0\} \times C_3$ in the cases $C_2 \times S_3$ and $C_2 \times S_4$. In the former case $\varphi(I_2)$ is a normal subgroup fixing a biquadratic extension of $\mathbb{Q}$ ramified only at p, which does not exist. In the latter case, we have $\varphi(I_2)$ is contained in the normal subgroup $\{0\} \times A_4$; thus $\{0\} \times A_4$ fixes also a biquadratic extenstion ove $\mathbb{Q}$ ramified only at p, a contradiction. Thus $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq S_4$. □

We now resume the discussion about elliptic curves of conductor 11 by Serre. First, an easy `Magma` calculation shows that the 2-torsion field of the curve E_{11} is

$$K_{11} := \mathbb{Q}(\theta), \qquad \text{where} \qquad \theta^6 - \theta^5 + 2\theta^4 - 3\theta^3 + 2\theta^2 - \theta + 1 = 0.$$

We now prove the main theorem in Serre's letter [27]

Theorem 2.2.11. *Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from* 11 *and* 2*-torsion field equal to* K_{11}. *Then, one of the following holds:*

(i) $a_2(E) = -2$ *and* E *is* $\mathbb{Q}$*-isogenous to* E_{11}*;*

(ii) $a_2(E) = 0$ *and* E *is* $\mathbb{Q}$*-isogenous to* $y^2 + y = x^3 - x^2 - 7x + 10$ *of conductor* 11^2*;*

(iii) $a_2(E) = 2$ *and* E *is* $\mathbb{Q}$*-isogenous to* $y^2 + y = x^3 - x^2 - 40x - 221$ *of conductor* 11^2.

In particular, there is only one $\mathbb{Q}$*-isogeny class of rational elliptic curves with conductor 11 and it satisfies* $a_2 = -2$.

Proof. Since $K_{11}/\mathbb{Q}$ has inertia of order 3 at all primes dividing 2, it follows as in the proof of Theorem 2.2.8 that $E/\mathbb{Q}$ has good supersingular reduction at 2, so $a_2(E) \equiv 0 \pmod 2$. By the Hasse bound $|a_p(E)| \leq 2\sqrt{p}$ for $p = 2$ we obtain $a_2(E) \in \{-2, 0, 2\}$.

(i) Suppose first $a_2(E) = -2$. Arguing by contradiction, we will show that the Galois representations $\rho_{E,2}$, $\rho_{E_{11},2} \colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_2)$ attached to E and E_{11} are equivalent.

Since both mod 2 residual representations $\bar{\rho}_{E,2}$ and $\bar{\rho}_{E_{11},2}$ cut out the field K_{11}, they are both surjective, and hence equivalent.

Suppose that $\rho_{E,2} \not\sim \rho_{E_{11},2}$ and consider the map $\varphi \colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow M_2^0(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)$ defined in Proposition 2.2.1, where $\rho_1 := \rho_{E,2}$ and $\rho_2 := \rho_{E_{11},2}$. More precisely,

$$\varphi(g) = \left(2^{-\alpha}(\rho_1(g) - \rho_2(g)) \pmod 2, \bar{\rho}_1(g)\right).$$

and we let $\widetilde{K} = \overline{\mathbb{Q}}^{\mathrm{Ker}(\varphi)} \supset K_{11}$ be the fixed field by $\mathrm{Ker}(\varphi)$. The assumption $\rho_1 \not\sim \rho_2$ implies that $\widetilde{K}/K_{11}$ is a non-trivial extension. We will show that $\widetilde{K}/K_{11}$ is trivial, obtaining a contradiction.

An easy calculation shows that $a_2(E_{11}) = -2$. Since $a_2(E) = a_2(E_{11})$, by Proposition 2.2.10, we have that $\widetilde{K}/K_{11}$ is unramified at 2 and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_4$. Using the `Number Field Database` (NFDB) [15], we obtain the complete list of degree 4 extensions of $\mathbb{Q}$ unramified at outside $\{2, 11\}$ and having Galois group S_4. The resulting fields are listed in Table 2.1 and $\widetilde{K}$ must be one of them.

rd	*grd*	D	h	G	Polynomial
12.08	13.56	$-2^4 11^3$	1	S_4	$x^4 - 2x^3 - 4x^2 - 6x - 2$
7.28	14.89	$-2^8 11^1$	1	S_4	$x^4 - 2x^2 - 4x - 1$
9.38	19.78	$-2^6 11^2$	1	S_4	$x^4 - 2x^3 - 3x^2 + 2$
24.16	27.12	$-2^8 11^3$	1	S_4	$x^4 - 44x + 22$
18.76	33.27	$-2^{10} 11^2$	2	S_4	$x^4 - 6x^2 - 8x - 25$
18.76	33.27	$-2^{10} 11^2$	2	S_4	$x^4 - 8x^2 - 16x + 24$

Table 2.1: Table of possible fields with the following search restrictions: *degree* = 4; *Galois T-number* = 5; *Ramifying primes limited to* $\{2, 11\}$; $p = 2$ *has c in* 0..Infinity; $p = 11$ *has c in* 0..Infinity.

Using the `Magma` code in Appendix A.1.1 one checks that, for all fields in Table 2.1 containing K_{11}, the ramification at 2 in $\widetilde{K}/K_{11}$ is non-trivial, a contradiction.

(ii) Suppose now $a_2(E) = 0$. Let E' be the conductor 11^2 elliptic curve with CM given by the Weierstrass equation $E' : y^2 + y = x^3 - x^2 - 7x + 10$. It is easy to check that the 2-torsion field of E' is also K_{11} and $a_2(E') = 0$. Thus $a_2(E) = a_2(E')$

and a perfectly analogous argument to the case $a_2(E) = -2$ (it gives the same list of possible fields $\tilde{K}$) shows that $\rho_{E,2} \sim \rho_{E',2}$, hence E and E' are $\mathbb{Q}$-isogenous.

(iii) For $a_2(E) = 2$, we let E' be the conductor 11^2 elliptic curve given by the Weierstrass equation $E' : y^2 + y = x^3 - x^2 - 40x - 221$. Again, it is easy to check that the 2-torsion field of E' is K_{11} and $a_2(E') = 2$. The conclusion follows as above.

Note that Theorem 2.2.8 implies that every elliptic curve of conductor 11 has 2-torsion field K_{11}. Thus, the last statement follows because the previous three cases are exhaustive. □

Next we give a generalization by Nigel Boston [4] of part (i) of Theorem 2.2.11. For it, we require of two auxiliary lemmas.

Lemma 2.2.12. *Let $K/\mathbb{Q}_\ell$ a local number field with $[K : \mathbb{Q}_\ell] = d$. Then, the index of the groups $[K^\times : {K^\times}^n]$ and $[U : U^n]$ is*

$$[K^\times : {K^\times}^n] = n[U : U^n] = n\ell^{dv_\ell(n)}|\mu_n(K)|,$$

where $|\mu_n(K)|$ is the order of the group of n-th roots in K.

Proof. This is [25, Ch. 2, Cor. 5.8]. □

Lemma 2.2.13. *Let $N > 3$ be a prime such that 3 does not divide the class number of $\mathbb{Q}(\sqrt{N})$ nor $\mathbb{Q}(\sqrt{-N})$, let K be the unique cubic cyclic extension of $\mathbb{Q}(\sqrt{-N})$ and suppose that $h(K)$ is odd. Then, there exists an exact sequence of $\mathbb{F}_2[\mathrm{Gal}(K/\mathbb{Q})]$-modules as follows:*

$$0 \xrightarrow{\delta_0} B \xrightarrow{\delta_1} \overline{U} \xrightarrow{\delta_2} \bigoplus_{\wp|N} \overline{U}_\wp \xrightarrow{\delta_3} \overline{P} \xrightarrow{\delta_4} 0,$$

where $\overline{U}$ is the units of K modulo squares, $\overline{U}_\wp$ is the units in $K_\wp$ (the completion of K at the prime $\wp$) modulo squares, and $\overline{P} = \mathrm{Gal}(L/K)$, where L/K is the maximal elementary 2-abelian extension of K unramified outside the primes in K above N.

Proof. We will deduce the exact sequence from well known facts of class field theory. From [21, Ch. V, Thm. 1.7] or [9, Ch. 3, Prop. 3.2.3], given the modulus $\mathfrak{m} = \wp_1\wp_2\wp_3 \subseteq \mathcal{O}_K$, where the $\wp_i$ are the primes above N in K, one has the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & U_\mathfrak{m} \arrow[r] & \mathcal{O}_K^\times \arrow[r] & (\mathcal{O}_K/\mathfrak{m})^\times \arrow[r] & Cl_\mathfrak{m}(K) \arrow[r] & Cl(K) \arrow[r] & 0 \end{tikzcd}$$

Notice that $(\mathcal{O}_K/\mathfrak{m})^\times = \prod_{\wp_i}(\mathcal{O}_K/\wp_i)^\times \hookrightarrow \bigoplus_{\wp_i} \mathcal{O}_{\wp_i}^\times$, where $\mathcal{O}_{\wp_i}^\times$ is the group of units in the completions by $\wp_i$ of K, namely $K_{\wp_i}$. So the map $(\mathcal{O}_K/\mathfrak{m})^\times \longrightarrow Cl_\mathfrak{m}(K)$ factors through $\bigoplus_{\wp_i} \mathcal{O}_{\wp_i}^\times$, which yields the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & U_\mathfrak{m} \arrow[r] & \mathcal{O}_K^\times \arrow[r] & \bigoplus_{\wp|N} \mathcal{O}_\wp^\times \arrow[r] & Cl_\mathfrak{m}(K) \arrow[r] & Cl(K) \arrow[r] & 0 \end{tikzcd}$$

Notice that $Cl(K)$ is killed modulo squares since it is an abelian group of order $|Cl(K)| = h(K)$, which is odd. □

Boston's theorem states:

Theorem 2.2.14. *Let $N \equiv 3 \pmod 8$ be a prime such that 3 does not divide the class number of $\mathbb{Q}(\sqrt{N})$ nor $\mathbb{Q}(\sqrt{-N})$, so that there is a unique cubic cyclic extension K of $\mathbb{Q}(\sqrt{-N})$ of conductor (2). Let $M \subset K$ a cubic subfield. Suppose that $h(M)$ is odd and that the minimum polynomial of a fundamental unit of M has a quadratic residue and a quadratic non-residue root modulo N.*

Then there is at most one $\mathbb{Q}$-isogeny class of elliptic curves over $\mathbb{Q}$ of conductor N with given trace of Frobenius at 2.

Proof. Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves of conductor N. By Theorem 2.2.8 it follows that $\bar{\rho}_{E_1,2}$ and $\bar{\rho}_{E_2,2}$ are isomorphic, cut out the field K and both have good supersingular reduction at 2, hence $a_2(E_i) \in \{-2, 0, 2\}$.

Suppose that $a_2(E_1) = a_2(E_2)$ and that E_1 and E_2 are not $\mathbb{Q}$-isogenous. By Proposition 2.2.10 there is an extension $\tilde{K}/K$ unramified outside N and such that $\mathrm{Gal}(\tilde{K}/K) \simeq S_4$. In particular, $\tilde{K} \subset L$ where L/K is the maximal elementary 2-abelian extension of K unramified outside the primes in K above N.

We will reach a contradiction by showing L/K is trivial. The key idea is to use two results of Nicole Moser. The first one, [23, Theorem IV.1], states

$$h(K) = \frac{a}{3} h(M)^2 h(\mathbb{Q}(\sqrt{-N})), \quad a \in \{1, 3\}.$$

Since $h(M)$ is odd by assumption and, from Genus theory, $h(\mathbb{Q}(\sqrt{-N}))$ is also odd then $h(K)$ is also odd. The second one is [23, Proposition II.2], stating that K has a Minkowski unit, i.e. a single generator of its unit group modulo torsion as a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module. From Lemma 2.2.13, using the fact that $h(K)$ is odd, there is an exact sequence of $\mathbb{F}_2[\mathrm{Gal}(K/\mathbb{Q})]$-modules:

$$0 \xrightarrow{\delta_0} B \xrightarrow{\delta_1} \overline{U} \xrightarrow{\delta_2} \bigoplus_{\wp | N} \overline{U}_\wp \xrightarrow{\delta_3} \overline{P} \xrightarrow{\delta_4} 0,$$

We now analyze the terms in this sequence:

- We have $\dim_{\mathbb{F}_2}(\overline{U}) = 3$. Indeed, Dirichlet's unit theorem states that the group of units is $U = \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K is the group of roots of unity in K, r is the number of real embeddings of K and s is half the number of complex embeddings of K. Note that $\mu_K = \{\pm 1\}$ and K is totally complex (it contains $\mathbb{Q}(\sqrt{-N})$). Therefore, $r = 0$, $s = 3$ and $U \simeq \{\pm 1\} \times \mathbb{Z}^2$; so taking U modulo squares yields $\overline{U} \simeq \{\pm 1\}^3$, as desired.

- We have $\dim_{\mathbb{F}_2}(\overline{U}_\wp) = 1$ by Lemma 2.2.12. Indeed, in the notation of that lemma, we have $\ell = N$, $K = K_\wp$, $U = U_\wp$, $d = e(\wp/N)f(\wp/N) = 2$, $n = 2$, $v_N(2) = 0$ and $|\mu_2(K_\wp)| = |\pm 1| = 2$. Thus $[U_\wp : U_\wp^2] = N^{2v_N(2)}2 = 2$, as desired. Since $N = \wp_1\wp_2\wp_3$ in K, we also have

$$\dim_{\mathbb{F}_2}\left(\bigoplus_{\wp | N} \overline{U}_\wp\right) = 3 = \dim_{\mathbb{F}_2}(\overline{U}).$$

- We have $\dim_{\mathbb{F}_2}(\overline{P}) = \dim_{\mathbb{F}_2}(B)$. Indeed, we have an exact sequence of $\mathbb{F}_2$-vector spaces (with an action of $\mathrm{Gal}(K/\mathbb{Q})$), hence

$$\dim_{\mathbb{F}_2}\left(\bigoplus_{\wp | N} \overline{U}_\wp\right) = \dim_{\mathbb{F}_2}(\mathrm{Ker}(\delta_3)) + \dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_3)).$$

By exactness, $\dim_{\mathbb{F}_2}(\mathrm{Ker}(\delta_3)) = \dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_2))$ and since δ_3 is surjective, $\mathrm{Im}(\delta_3) = \overline{P}$. So, one has

$$\dim_{\mathbb{F}_2}\left(\bigoplus_{\wp|N}\overline{U}_{\wp}\right) = \dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_2)) + \dim_{\mathbb{F}_2}(\overline{P}).$$

Now, $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_2)) = \dim_{\mathbb{F}_2}(\overline{U}) - \dim_{\mathbb{F}_2}(\mathrm{Ker}(\delta_2))$, and since δ_1 is injective and exactness, $\mathrm{Ker}(\delta_2) = \mathrm{Im}(\delta_1) = B$. So, we can write the equality of dimensions as:

$$\dim_{\mathbb{F}_2}\left(\bigoplus_{\wp|N}\overline{U}_{\wp}\right) + \dim_{\mathbb{F}_2}(B) = \dim_{\mathbb{F}_2}(\overline{U}) + \dim_{\mathbb{F}_2}(\overline{P}).$$

Finally, since $\dim_{\mathbb{F}_2}\left(\bigoplus_{\wp|N}\overline{U}_{\wp}\right) = \dim_{\mathbb{F}_2}(\overline{U})$, we are left with the equality we were searching for,

$$\dim_{\mathbb{F}_2}(\overline{P}) = \dim_{\mathbb{F}_2}(B).$$

Recall that, to finish the proof, we want to show that L/K is trivial. By the previous equality of dimensions this follows if we show $B = 0$. Since $B = \mathrm{Ker}(\delta_2) = \mathrm{Im}(\delta_1)$, to see that $\mathrm{Ker}(\delta_2) = 0$ we need to see that no non-trivial element of $\overline{U}$ maps to zero via δ_2. The existence of a Minkowski unit implies that $\overline{U} \cong \{\pm 1\} \oplus V$, where V is an irreducible 2-dimensional $\mathbb{F}_2[\mathrm{Gal}(K/\mathbb{Q})]$-module. Since $N \equiv 3 \pmod 8$, then -1 can not be a square modulo N, so particularly it is non trivial in $\overline{U}_{\wp_i}$ for $1 \le i \le 3$. So, what we need to do is find an element of V which is not a square mod $\wp_i$ for some i and therefore is not in the ith component of the kernel of the map δ_2. This will finish the proof since V is irreducible.

One of the hypothesis of the theorem is that the minimum polynomial of a fundamental unit ω of M has a root that is a quadratic residue and another which is a quadratic non-residue modulo N. From the proof of Setzer's Lemma, we know that

$$N\mathcal{O}_M = \mathfrak{p}\mathfrak{q}^2,$$

for $\mathfrak{p}, \mathfrak{q}$ primes of $\mathcal{O}_M$. We know that the residual fields $\mathcal{O}_M/\mathfrak{p} \cong \mathcal{O}_M/\mathfrak{q} \cong \mathbb{F}_N$ (since $f(\mathfrak{p}/N) = f(\mathfrak{q}/N) = 1$). The irreducible polynomial of ω, namely f_ω, is a degree 3 polynomial (since there are no subextensions of M and $\omega \notin \mathbb{Q}$). And, by hypothesis, it splits like

$$f_\omega \pmod{\mathfrak{p}} \equiv f_\omega \pmod{\mathfrak{q}} \equiv (x - b_1)(x - b_2)^2 \pmod{N},$$

with $b_i \in \mathbb{F}_N$ and one of them being a square mod N and the other not. Moreover,

$$\omega \equiv b_1 \pmod{\mathfrak{p}}, \quad \omega \equiv b_2 \pmod{\mathfrak{q}}.$$

Now we can think of ω as an element of K. The irreducible polynomial of ω in K is still f_ω. Moreover, we have seen above that

$$N\mathcal{O}_K = \wp_1^2\wp_2^2\wp_3^2.$$

So, since $\mathfrak{p}$ and $\mathfrak{q}^2$ must divide $N\mathcal{O}_K$, we have that $\mathfrak{p}$ is totally ramified and $\mathfrak{q}$ is totally split in K/M. Moreover, we have for every $1 \le i \le 3$ one of the two following possibilities:

$$\omega \pmod{\wp_i} \equiv \omega \pmod{\mathfrak{p}} \equiv b_1, \ \mathit{or}$$

$$\omega \pmod{\wp_i} \equiv \omega \pmod{\mathfrak{q}} \equiv b_2.$$

Since we cannot be in the same case for the three i, there is a $\wp_i$ such that $\omega \pmod{\wp_i}$ is not a square. Particularly, $\delta_2(\omega)_i \in \overline{U}_{\wp_i}$ is non-trivial. Hence, $\omega \notin \mathrm{Ker}(\delta_2)$. □

Finally, to finish this example, we have written some code in Magma to check which primes N satisfy the hypothesis of Boston's theorem. It can be found on Appendix A.1.2.

2.2.2 Another application of the method of quartic fields: There is a unique modular elliptic curve over $\mathbb{Q}$ of conductor 5077.

Nowadays we know that every elliptic curve defined over $\mathbb{Q}$ is modular due to the work of Breuil, Conrad, Diamond, and Taylor [5] which extends the groundbreaking work of Andrew Wiles [34] on modularity of semistable elliptic curves over $\mathbb{Q}$. Before the proof of these general results, mathematicians were interested in providing evidence towards them. In particular, Mestre [19] showed there exists a unique modular elliptic curve over $\mathbb{Q}$ of conductor 5077. This was a proof of existence without an explicit equation for the curve. Then, adapting Serre's approach for conductor 11 described above, Mestre also shows that the curve given by equation (2.4) is modular, by showing it is $\mathbb{Q}$-isogenous to the unique modular elliptic curve of conductor 5077.

In this section, we give a slightly modified proof of Mestre's computations with the aid of Magma. Indeed, we will show that the elliptic curve E[3] of conductor 5077 defined by the Weierstrass equation

$$E \;:\; y^2 - y = x^3 - 7x + 6 \tag{2.4}$$

is modular. More precisely, let $f \in S_2(5077)$ be the newform with q-expansion

$$f(q) = q - 2q^2 - 3q^3 + 2q^4 - 4q^5 + 6q^6 - 4q^7 + 6q^9 + O(q^{10}).$$

This is the unique newform in $S_2(5077)$ with field of coefficients $K_f = \mathbb{Q}$[4]. From Chapter 1, we know that, for every prime ℓ, the curve E and the newform f have attached ℓ-adic Galois representations, respectively,

$$\rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \quad \text{and} \quad \rho_{f,\ell}\colon \mathrm{Gal}_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Futhermore, the curve E is *modular* if $\rho_{E,\ell} \sim \rho_{f,\ell}$ for one (hence all) prime ℓ and we will estabilsh this for $\ell = 2$. To this end, Mestre [19] states the following theorem which he attributes to Serre from his course in the Collège de France in 1984-85, [29].

Theorem 2.2.15. *Let E and E' be two elliptic curves defined over $\mathbb{Q}$ having prime conductor N and such that the 2-torsion field of both curves is the same S_3-extension $K/\mathbb{Q}$. Suppose that $a_2(E) = a_2(E')$ is even and that E and E' are not $\mathbb{Q}$-isogenous.*

Then, there exists a unramified extension $\widetilde{K}/K$ such that $\widetilde{K}/\mathbb{Q}$ is a S_4-extension. Furthermore, $a_p(E) \neq a_p(E')$ for every prime p where the Frobenius at p in $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ has order 4.

We were not able to find a detailed proof of this theorem and we don't know that the theorem is correct, so we are not going to use it. The potential issue is that it claims the extension $\widetilde{K}/K$ is unramified. We can only show it is unramified at

[3] https://www.lmfdb.org/EllipticCurve/Q/5077/a/1

[4] https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/5077/2/a/a/

primes above 2 and not necessarily at primes above N. Nevertheless, we will reprove Mestre's example using this weaker version; this will require additional computational arguments. Let us first translate the general picture of the theorem into the language of Galois representations. Let

$$\rho,\ \rho'\colon \operatorname{Gal}_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(\mathbb{Z}_2)$$

be the two irreducible 2-adic representations of E and E' respectively.

- The condition on the 2-torsion fields implies that $\overline{\rho} = \overline{\rho'}$, since the 2-torsion fields are the ones cut out by the residual representations. Particularly, it is the field cut out by the second component of the map φ defined in Proposition 2.2.1.
- The condition $a_2(E) = a_2(E')$ is even and implies that the 2-adic representations coincide in the inertia group at 2. This comes from the Honda-Cartier-Hill theorem [13], which tells us that, since the curve E has supersingular reduction at 2, $\rho|_{D_2} \cong \rho'|_{D_2}$, where D_2 is the decomposition group at 2. The argument is similar to the one in Proposition 2.2.10.

The extension $\widetilde{K}/K$ comes from applying the Faltings-Serre method as for $N = 11$. Indeed, it is $\widetilde{K} = \overline{\mathbb{Q}}^{\operatorname{Ker}(\varphi)}$ of and it has Galois group S_4 over $\mathbb{Q}$. To see that the extension $\widetilde{K}/K$ is unramified at 2 we argue as in the proof of Proposition 2.2.10, but we are unable to prove it is also unramified at 5077. (A soft reason for the possibility of this being false is that Boston, almost 10 years later, published his paper which we used above and he did not mention this result nor use it). Nevertheless, this is the only step of the theorem that we don't know that it is true, everything else follows from Serre [27]. To see that $\operatorname{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_4$ we use the same argument as in the case of conductor 11, by looking at the inertia at 2, we discard the cases $\operatorname{Gal}(\widetilde{K}/\mathbb{Q}) \cong C_2 \times S_i$, with $i = 3, 4$.

Finally, we need to see that for every prime p, and $\mathfrak{p}$ a prime lying over it in $\widetilde{K}$, where $\operatorname{Frob}_{\mathfrak{p}} \in \operatorname{Gal}(\widetilde{K}/\mathbb{Q})$ has order 4, $a_p(E) \neq a_p(E')$. Recall from Proposition 1.2.25, that $\operatorname{tr}(\rho(\operatorname{Frob}_{\mathfrak{p}})) = a_p(E)$, so $a_p(E) \neq a_p(E')$ implies $\operatorname{tr}(\rho(\operatorname{Frob}_{\mathfrak{p}})) \neq \operatorname{tr}(\rho'(\operatorname{Frob}_{\mathfrak{p}}))$. We have seen before Proposition 2.2.1, that if we have an element $(M, N) \in M_2^0(\mathbb{F}_2) \rtimes \operatorname{GL}_2(\mathbb{F}_2)$ (particularly, in the image of φ), then the map $\phi = \operatorname{tr}(MN)$ is enough to determine when the two representations are equivalent.

Lemma 2.2.16. *An element $(M, N) \in M_2(\mathbb{F}_2) \rtimes GL_2(\mathbb{F}_2)$ satisfies $\phi(MN) \neq 0$ if and only if it has order 4 or 6.*

Proof. Recall that we can identify $\operatorname{GL}_2(\mathbb{F}_2)$ with S_3 (as given in Appendix B). Then the elements $(M, \sigma) \in M_2^0(\mathbb{F}_2) \rtimes S_3$ contained in the one of the following subgroups

$$\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} \times S_3, \quad M_2^0(\mathbb{F}_2) \times \{\operatorname{id}_{S_3}\}, \quad \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \times \{\sigma \in S_3 \mid \sigma^2 = \operatorname{id}_{S_3}\}$$

satisfy $\phi(M\sigma) = 0$. All the other elements, the ones that have non-trivial image by ϕ, correspond to elements of order 4 or 6 in $M_2^0(\mathbb{F}_2) \rtimes S_3 \cong \mathbb{F}_2^3 \rtimes S_3 \cong C_2 \times S_4$. Particularly, the elements of order 4 correspond to elements of $\{1\} \times S_4$ or $\{-1\} \times S_4$ and the elements of order 6 correspond to elements of order 3 of S_4 and C_2, since there are no elements of order 6 in S_4. □

Particularly, since we have seen that $\operatorname{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_4$, it is enough to search for the elements of order 4 in the image of φ, and these are the ones coming from a Frobenius element of order 4, as we wanted. This completes the proof of Theorem 2.2.15, except for claim about the ramification at N.

As mentioned in the beginning of this section, we will prove modularity of E by comparing its 2-adic representation to that of f. The arguments we have seen above were mostly using properties of the Galois representations attached to the elliptic curves E and E', so it is natural to expect that we can proceed similarly with the representation attached to f. This however, introduces some additional challenges as we shall explain next.

Step 1. Firstly, we have to show that both residual representations

$$\overline{\rho}_{E,2},\ \overline{\rho}_{f,2}\colon \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_2)$$

determine the same S_3-extension $K/\mathbb{Q}$, which implies they are isomorphic. Note that the image of these residual representations is a subgroup of $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, so the extension $K/\mathbb{Q}$ has Galois group isomorphic to one of the groups in the set $\{1, C_2, C_3, S_3\}$. The case of $\overline{\rho}_{E,2}$ is simpler. From Lemma 2.2.4, we already know that the fixed field by $\overline{\rho}_{E,2}$ has Galois group S_3. We can easily compute it using `Magma`. It is the field K_E given by the polynomial

$$x^6 + 2x^5 - 163x^4 + 284x^3 + 2095x^2 - 6274x + 4483.$$

To find the field K defined by $\overline{\rho}_{f,2}$ we need to do a bit more of work. First, we discard the cases $\mathrm{Gal}(K/\mathbb{Q}) \in \{1, C_2\}$ as follows. Finding a prime p such that the characteristic polynomial of $\overline{\rho}_{f,2}(\mathrm{Frob}_p)$ is irreducible over $\mathbb{F}_2$ implies that $\overline{\rho}_{f,2}(\mathrm{Frob}_p)$ is diagonalizable over the quadratic extension of $\mathbb{F}_2$, hence $\overline{\rho}_{f,2}(\mathrm{Frob}_p)$ has order 3 or 6. This implies that the image of $\overline{\rho}_{f,2}$ cannot be trivial or C_2. In our example, $p = 3$ satisfies the conditions and the computations can be found in Appendix A.2.1.

To deal with the cases C_3 and S_3 we will find a finite list of candidate fields using ramification properties of $\overline{\rho}_{f,2}$ and then exclude all possibilities except one, which turns out to be the field K_E above. Indeed, the representation $\rho_{f,2}$ is unramified outside $\{2, 5077\}$ by Proposition 1.2.28. Moreover, the residual representation $\overline{\rho}_{f,2}$ is a quotient of $\rho_{f,2}$, so its ramification set is a subset of $\{2, 5077\}$, hence the extension $K/\mathbb{Q}$ cut out by $\overline{\rho}_{f,2}$ is also unramified outside $\{2, 5077\}$.

To obtain a complete list of possible fields we need to first bound the discriminant of $K/\mathbb{Q}$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is C_3 or S_3, an inertia group at 2, denoted I_2, has order dividing 6. When $|I_2| = 1$, then 2 does not ramify so the exponent of 2 in the discriminant is 0. When $|I_2| = 3$, the extension $K/\mathbb{Q}$ is tamely ramified at 2 and by [28, Ch. III, Prop. 13], we have $v_{\mathfrak{P}}(\mathfrak{D}_{K/\mathbb{Q}}) = |I_2| - 1 = 2$, where $\mathfrak{D}_{K/\mathbb{Q}}$ denotes the different of $K/\mathbb{Q}$ and $\mathfrak{P}$ is any prime in K dividing 2.

When $K/\mathbb{Q}$ is wildly ramified at 2, i.e. then $|I_2| \in \{2, 6\}$, we apply a result of Moon and Taguchi (see [22, Th. 3]). Following the notation of this theorem, in our setting, we have $p = \widetilde{k} = 2$ and $m = d = 1$, we obtain

$$v_2(\mathfrak{D}_{K/\mathbb{Q}_2}) = 1 + \frac{\widetilde{k} - 1}{p - 1} - \frac{\widetilde{k} - 1 + d}{(p-1)p^m} = 1 + 1 - 2^{1-m} = 2$$

So at most, the maximal exponent of the primes of K above 2 in the different $\mathfrak{D}_{K/\mathbb{Q}}$ is 2. Now, the discriminant is the norm of the different, i.e.

$$\mathfrak{d}_{K/\mathbb{Q}} = N_{K/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}}).$$

Particularly, since the norm is multiplicative, the factors of the discriminant are the norm of the factors of the different. i.e., if v is the maximal exponent of the different at a prime of K, namely $\mathfrak{p}$ above a prime $p \in \mathbb{Q}$, then

$$N_{K/\mathbb{Q}}(\mathfrak{p}^v) = p^{fv},$$

where f is the residual degree $f(\mathfrak{p}/p)$. Now, if the prime p satisfies $p \mid \mathfrak{d}_{K/\mathbb{Q}}$ and $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^e$, then $\mathfrak{p}_i \mid \mathfrak{D}_{K/\mathbb{Q}}$ for $1 \leq i \leq g$. Particularly, if α is the maximal exponent of p such that $p^\alpha \mid \mathfrak{d}_{K/\mathbb{Q}}$, then

$$p^\alpha \leq \prod_{i=1}^{g} p^{fv} = p^{gfv}.$$

Hence, in our case, since $v = 2 = |I_2| - 1 = e(\mathfrak{P}/2) - 1$, multiplying and dividing by $e := e(\mathfrak{P}/2)$ on both sides of the inequality gives

$$\alpha \leq egf\left(1 - \frac{1}{e}\right) = [K : \mathbb{Q}]\left(1 - \frac{1}{e}\right) = 6 - 2 = 4.$$

We now bound the exponent of 5077. Since 5077 does not divide 6 the ramification is tame. Hence, again by [28, Ch. III, Prop. 13], the maximal exponent v of the primes of K lying over 5077, namely $\mathfrak{P}$, such that $\mathfrak{P}^v$ divides $\mathfrak{D}_{K/\mathbb{Q}}$ is $v = |I_{5077}| - 1$. Moreover, the modular form f is Steinberg at 5077, and it is well known that this implies that the image of inertia at 5077 via $\bar{\rho}_{f,2}$ has order 1 or 2. Hence, the maximal exponent α such that 5077^α divides $\mathfrak{d}_{K/\mathbb{Q}}$ is

$$\alpha \leq [K : \mathbb{Q}]\left(1 - \frac{1}{|I_{5077}|}\right) = 6 - 3 = 3.$$

So the root discriminant of K is at most

$$2^{2/3}5077^{1/2} = 113.1072.$$

Using this bound on the NFDB, and discarding the fields with Galois group C_2, one obtains the fields in Table 2.2.

rd	grd	D	h	G	Polynomial
27.28	113.11	$2^2 5077^1$	2	S_3	$x^3 - 28x - 50$
295.40	295.40	5077^2	1	C_3	$x^3 - x^2 - 1692x + 5265$

Table 2.2: Table of possible fields with the following search restrictions: *degree in the range* 1,2,3; *root discriminant in the range* 1..114; *Galois T-number in the range* 1,2; *Ramifying primes limited to* $\{2, 5077\}$; *p = 2 has c in* 0..Infinity; and *p = 5077 has c in* 0..Infinity.

We note that the spliting field of the polynomial in the first line of Table 2.2 is isomorphic to the field K_E. To discard the field with Galois group isomorphic to C_3, we use the functions defined in Appendix A.2.1 to compute the order of $\bar{\rho}_{f,2}(\mathrm{Frob}_{\mathfrak{p}})$ for some $\mathfrak{p} \in \mathcal{O}_K$ above p (similarly to what has been done to prove that the Galois group could not be trivial nor C_2) and compare it with the Frobenius element at p of the Galois group $\mathrm{Gal}(\mathbb{Q}(x^3 - x^2 - 1692x + 5265)/\mathbb{Q}) \cong C_3$. We find that for $p = 3$, the orders differ, hence this extension with Galois group C_3 can not be the extension

K. We conclude that $\bar{\rho}_{E,2}$ and $\bar{\rho}_{f,2}$ cut the same field and so are isomorphic. The code to check these claims is the following:

```
ff := Newform("G0N5077k2A"); // Gamma_0(N) of lvl 5077 & wt 2 & iso class A
Kf<a> := SplittingField(x^3-x^2-1692*x+5265);
p := 3;
apf := Coefficient(ff,p);
charpoly := x^2 - apf*x + p;
M := diagMatrix(charpoly);
ordF := matOrder(M);
ordK := Order(FrobeniusElement(Kf,p));

print "Order of rho(frob):", ordF, "||", "Order of Frob_p:", ordK;
```

And it prints:

```
Order of rho(frob): 3 || Order of Frob_p: 1
```

Step 2. We will determine a finite list of possible extensions $\tilde{K}/K$. Since 2 does not divide the level 5077 of f and $\bar{\rho}_{f,2}(I_2)$ has order 3 from Step 1, we conclude that $\rho_{f,2}|_{D_2}$ is non-ordinary representation determined by the trace of Frobenius at 2. Moreover, since $a_2(f) = -2 = a_2(E)$ we also conclude $\rho_{f,2}|_{D_2} \simeq \rho_{E,2}|_{D_2}$. (This conclusions uses a deep result about Galois representations outside the scope of this work.) This is analogous conclusion to Serre's argument and following the arguments above, we conclude that $\mathrm{Gal}(\widetilde{K}/K) \cong S_4$. Moreover, we know that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ thus $\widetilde{K}/K$ is a biquadratic extension which only ramifies at the primes of K above 5077 (and possibly at some primes at infinity, since the extension $K/\mathbb{Q}$ is totally real). To compute $\tilde{K}$ we introduce the p-Selmer group. Let S be a finite set of prime ideals in K. For an integer p, the *p-Selmer group of S* is defined as

$$K_p(S) := \{x \in K^\times/(K^\times)^p \mid v_q(S) \equiv 0 \pmod{p}\ \forall q \notin S\}.$$

The set $K_p(S)$ is a finite abelian group of exponent p and it can be computed using Magma. We are interested in the 2-Selmer group of primes of K dividing 5077, since we are searching for biquadratic extensions of K ramifying only on primes above 5077. Let $S = \{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \mid 5077\}$, then for any $\alpha \in K_2(S)$, it satisfies that it is not a square in K and the quadratic extension $K(\sqrt{\alpha})/K$ ramifies only at the primes in S. Since we are searching for biquadratic extension of K, we have to choose two elements $\alpha, \beta \in K_2(S)$ and consider the extension

$$K(\sqrt{\alpha}, \sqrt{\beta})/K.$$

Note that *a priori* such an extension can ramify at 2 and does not have to be Galois over $\mathbb{Q}$. Using Magma, we can find all such extensions with Galois group $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq S_4$ and the correct ramification properties. We found seven of them. The code for this is available on Appendix A.2.2. The polynomials defining the possible fields are in Appendix A.2.4.

Step 3. To finish the proof, we need to check that none of the extensions computed in Step 2 is compatible with our setting. Observe that the argument at the end of the sketch of proof of Theorem 2.2.15 giving that the Frobenius elements in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ of order four allow to discard the possibilities for $\tilde{K}$ also applies here. This is because that argument depends only on the group structure of $M_2^0(\mathbb{F}_2) \rtimes S_3$ and not on the representations involved arising from elliptic curves. Thus, for each of the seven $\widetilde{K}$, we find a prime p such that $\mathrm{Frob}_p \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ has order 4 and $\mathrm{tr}(\rho_{E,2}(\mathrm{Frob}_p)) = \mathrm{tr}(\rho_{f,2}(\mathrm{Frob}_p))$, discarding $\widetilde{K}$. The code in Appendix A.2.3 finds such a prime p for each extension $\widetilde{K}$ and we find that the primes $p = 5, 11, 13$ suffice. More precisely, we get the following output

```
p = 5 || ap(f) =  -4 | ap(E) =  -4
p = 13 || ap(f) =  -4 | ap(E) =  -4
p = 11 || ap(f) =  -6 | ap(E) =  -6
p = 5 || ap(f) =  -4 | ap(E) =  -4
p = 5 || ap(f) =  -4 | ap(E) =  -4
p = 5 || ap(f) =  -4 | ap(E) =  -4
p = 11 || ap(f) =  -6 | ap(E) =  -6
```

We conclude that the extension $\widetilde{K}/K$ is trivial and so $\rho_{E,2} \sim \rho_{f,2}$ as desired.

To conclude this chapter, we mention that nowadays there is an easier method to prove that two elliptic curves over $\mathbb{Q}$ are $\mathbb{Q}$-isogenous, that follows by the Modularity theorem.

Theorem 2.2.17. *Two elliptic curves E, E' over $\mathbb{Q}$ are $\mathbb{Q}$-isogenous if and only if they have the same conductor $N(E_1) = N(E_2) = N$ and $|E_1(\mathbb{F}_p)| = |E_2(\mathbb{F}_p)|$ for all primes $p \nmid N$ such that*

$$p \leq \frac{N}{6} \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proof. Let ρ_i be the compatible system of 2-dimensional Galois repserentations associated to E_i and f_i the corresponding modular form (from the Modularity theorem), for $i = 1, 2$. Then,

$$E_1 \equiv E_2 \iff \rho_1 \sim \rho_2 \iff f_1 = f_2.$$

By [24, Th. 1], a cusp form f of weight 2 and level N is determined by its first

$$\frac{N}{6} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Fourier coefficients $a_n(f)$. For eigenforms, we can restrict out attention to Fourier coefficients $a_p(f)$ where p is prime.

In our situation, if $p \mid N$, from multiplicity 1 it is automatic that $a_p(f_1) = a_p(f_2)$, since f_1 and f_2 are newforms of the same level N.

If $p \nmid N$, sice $a_p(f_i) = \mathrm{tr}(\rho_i(\mathrm{Frob}_p)) = 1 - |E_i(\mathbb{F}_p)| + p$, the result follows. □

Notice that this does not mean that the method is useless after the proof of the modularity theorem, but that it is useless in the case of $\mathbb{Q}$-isogenies of elliptic curves over $\mathbb{Q}$. For example, the method is still valid when the elliptic curves are defined over a quadratic imaginary field, such as in [11].

Chapter 3

Comparing Galois representations: the residually reducible case.

3.1 The Faltings-Serre-Livné criterion

In this section we focus our attention on 2-dimensional λ-adic representations

$$\rho_1, \rho_2 \colon G \longrightarrow \mathrm{GL}_2(\mathcal{O}_\lambda)$$

where $\mathcal{O}_\lambda$ has residual characteristic 2 and, moreover,

$$\operatorname{tr}(\rho_1) \equiv \operatorname{tr}(\rho_2) \equiv 0 \pmod{\lambda} \quad \text{and} \quad \det(\rho_1) \equiv \det(\rho_2) \equiv 1 \pmod{\lambda}. \tag{3.1}$$

The above condition on the traces show that the residual representations are not surjective and, in fact, can be reducible. This is in contrast with the method of quartic fields from the previous chapter which requires the residual representation to be absolutely irreducible. Nevertheless, the basis for comparing representations has been set in general using the deviation group introduced in 2.1. Here we present the Faltings-Serre-Livné criterion which allows to have control over the deviation group and decide whether $\rho_1 \sim \rho_2$ in the residually reducible case.

The following set will play a crucial role.

Definition 3.1.1. Define Ξ to be the set of elements $g \in G$ for which the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ coincide.

The results of this chapter are very reliant on group-theoretical results. Before starting with those, let us recall some definitions that we are going to use and that are maybe not standard for a group theory course.

Definition 3.1.2.

1. Let G be a group. We define the ideal of $\mathbb{Z}$,

$$I = \{z \in \mathbb{Z} \mid \forall g \in G,\ g^z = 1\}.$$

Since its an ideal of $\mathbb{Z}$, it is of the form $e\mathbb{Z}$, for some $e \in \mathbb{Z}$. Particularly, the *exponent of* G is the minimal e such that $e\mathbb{Z} = I$.

2. Let G be a group. We say that G is a *p-group* if all elements have order a power of p.

3. Let G be a profinite group. We say that G is a *pro-p-group* if for every normal subgroup N, the quotient G/N is a p-group.

4. A subgroup H of a group G is called a *characteristic subgroup* if for every $\varphi \in \mathrm{Aut}(G)$, $\varphi(H) \subseteq H$.

With all these definitions, let us continue with comparing Galois representations. The following proposition characterises the elements of Ξ.

Proposition 3.1.3. *If $g \in \Xi$, then $\delta(g)^2 = 1$ in $\delta(G)$.*

Proof. The characteristic polynomial of a 2-dimensional representation ρ is given by

$$x^2 - \operatorname{tr}(\rho)x + \det(\rho).$$

Particularly, if $g \in \Xi$, the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ are equal, hence $\operatorname{tr}(\rho_1(g)) = \operatorname{tr}(\rho_2(g))$ and $\det(\rho_1(g)) = \det(\rho_2(g))$. Denote them by $\operatorname{tr}(g)$ and $\det(g)$ respectively. Using the Cayley-Hamilton theorem, one has for $i = 1, 2$,

$$0 = \rho_i(g)^2 - \operatorname{tr}(g)\rho_i(g) + \det(g)\rho_i(1) \implies \rho_i(g)^2 = \operatorname{tr}(g)\rho_i(g) - \det(g)\rho_i(1).$$

Making use of the hypothesis (3.1), one has that $\operatorname{tr}(g)\rho_i(g) \in \lambda\rho_i(g)$ and $\det(g)\rho_i(1) \in (1+\lambda)\rho_i(1)$. In particular, subtracting $\rho_i(1)$ to both sides of the equation above, we have

$$\rho_i(g)^2 - \rho_i(1) = \operatorname{tr}(g)\rho_i(g) - (\det(g)+1)\rho_i(1) \in \lambda\rho_i(g) + (2+\lambda)\rho(1) \subseteq \lambda M.$$

Hence,

$$\rho(g)^2 \equiv \rho(1) \pmod{\lambda M} \implies \delta(g)^2 = \delta(1) = 1.$$

□

This gives us the following characterisation of $\delta(G)$ when both representations are equivalent:

Corollary 3.1.4. *If $\rho_1 \sim \rho_2$, then $\delta(G)$ is an abelian group of exponent 2.*

Proof. When $\rho_1 \sim \rho_2$ we have $\Xi = G$. Particularly, $\delta(G) = \delta(\Xi)$, has exponent 2. □

In general, however, we can not say much more than the folowing.

Proposition 3.1.5. *The deviation group $\delta(G)$ is a 2-group.*

This gives, using Proposition 2.1.2, $\delta(G) = 2^r$, with $0 \leq r \leq 7$.

Proof. The strategy is the following: recall that $\delta(G)$ fits into the short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1,$$

where $N(G)$ is a finite quotient of $\rho(G) \cap (1+\lambda R)$, where $R = M_2(\mathcal{O}_\lambda) \oplus M_2(\mathcal{O}_\lambda)$ and $\rho = \rho_1 \times \rho_2$. If we prove that $\overline{G}$ and $N(G)$ are 2-groups, then so will be $\delta(G)$.

To see that $N(G)$ is a 2-group first notice that the multiplicative group $1+\lambda R$ embeds via the logarithm into the additive group λR, hence its a pro-2-group. It is a known fact [3, Ch.10] that if $\{G_n\}$ is a sequence of subgroups defining the topology on G, then the completion $\widetilde{G}/\widetilde{G_n} \cong G/G_n$. Particularly, since $N(G)$ is a finite quotient of $\rho(G) \cap (1+\lambda R)$, then it is a 2-group.

Moreover, by the hypothesis on this section, (3.1), the characteristic polynomial of ρ_i, for $i = 1, 2$, satisfies

$$x^2 - \operatorname{tr}(\rho_i)x + \det(\rho_i) \equiv x^2 + 1 \pmod{\lambda}.$$

Again, using Cayley-Hamilton, for every $g \in G$, one has

$$\rho_i(g)^2 \equiv -1 \equiv 1 \pmod{\lambda}.$$

It follows that $\rho_1 \times \rho_2(g) \equiv 1 \pmod{\lambda}$, hence $\overline{G}$ has exponent 2, and in particular it is an abelian 2-group. □

We are going to state the group theory results we need to prove the theorem at the end of the section.

Definition 3.1.6. For any group G, we define the subgroup generated by the squares

$$N_2(H) := \langle g^2 \mid g \in G \rangle.$$

It is easy to see that $N_2(G)$ is a characteristic subgroup of G: for any $\varphi \in \mathrm{Aut}(G)$, it is enough to see that the image of the generators of $N_2(G)$ is invariant under φ. Particularly, for any $g \in G$, $\varphi(g^2) = \varphi(g)^2 \in N_2(G)$. Since it is characteristic, then it is normal, and we can therefore consider the *2-quotient* $G_2 := G/N_2(G)$ of G.

Proposition 3.1.7. *G_2 is the greatest quotient of G of exponent 2. Moreover, if N is a normal subgroup of G, then*

$$(G/N)_2 \cong G/(N_2(G) \cdot N).$$

In particular, $(G/N)_2 = G_2$ if and only if $N \subseteq N_2(G)$.

Proof. G/N is a quotient of G of exponent 2 if and only if N is a normal subgroup which contains all the squares, i.e. $N_2(G) \subseteq N$. Hence, G_2 is the greatest quotient of G of exponent 2, since $N_2(G)$ is normal.

To prove the isomorphism, we need to how that if N is a normal subgroup of G, then $N_2(G/N) = (N_2(G) \cdot N)/N$. This is an easy exercise using the definition of quotient group, and then the conclusion follows. □

As a final definition, let $G[2] := \{g \in G \mid g^2 = 1\}$, the set of elements of 2-torsion of G. This need not be a subgroup when G is not abelian: for example, if $G = S_3$, $G[2] = \{1, (1,2), (1,3), (2,3)\}$, but this is not a subgroup (it has order 4 which does not divide 6).

Lemma 3.1.8. *Let G be a 2-group such that every element in G_2 has a lift to an element of $G[2]$. Then G has exponent 2, i.e. $G = G_2$.*

Proof. Consider the short exact sequence for G_2,

$$1 \longrightarrow N_2(G) \longrightarrow G \longrightarrow G_2 \longrightarrow 1.$$

Let us argue by contradiction. Suppose that $N_2(G) \neq 1$.

Without loss of generality we can assume that $N_2(G)$ is cyclic of order 2: Let Ω be the set of subgroups of index 2 of $N_2(G)$. Writing the abelianisation of the 2-group $N_2(G)$ as

$$N_2(G)_{ab} = \bigoplus_{i=1}^{k} \mathbb{Z}/2^{a_i}\mathbb{Z}, \quad k, a_i \geq 1,$$

we see that $|\Omega| = 2^k - 1$ is off, so G acts on Ω by conjugation with at least one fixed point $N \in \Omega$. Replacing G by G/N (which doesn't change its 2-quotients by Proposition 3.1.7), we obtain the supposition.

Hence, we can assume that $N_2(G) = \langle n \rangle \cong C_2$. Then, necessarily, $N_2(G) \subseteq Z(G)$: for $g \in G$, gng^{-1} must be an element of order 2 in $N_2(G)$, hence $gng^{-1} = n$.

The elements of order 2 in G commute: for $g, g' \in G$ of order 2, consider gg'. Then its either of the form g'' or $g''n$, with g'' of order 2. In both cases, $gg' = 1$.

Finally, using this last remark, we can find a section of $G \longrightarrow G_2$ by choosing generators of G_2 and sending them to lifts of order 2 in H. This implies that $G \cong N_2(G) \times G_2$, which contradicts the definition of the 2-quotient. □

Using this lemma we can derive a criterion for the equivalence between two representations:

Theorem 3.1.9. *Let $\rho_1, \rho_2 \colon G \longrightarrow \mathrm{GL}_2(\mathcal{O}_\lambda)$ be two λ-adic representations satisfying the conditions (3.1),*

$$\mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \equiv 0 \pmod{\lambda} \quad \textit{and} \quad \det(\rho_1) \equiv \det(\rho_2) \equiv 1 \pmod{\lambda}.$$

and also let

$$\Xi = \{g \in G \mid \mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g)), \det(\rho_1(g)) = \det(\rho_2(g))\}.$$

Then $\rho_1 \sim \rho_2$ if and only if Ξ surjects onto G_2.

Proof. The implication to the right has nothing to prove since if $\rho_1 \sim \rho_2$, then $\Xi = G$.

For the left implication, suppose that Ξ surjects onto G_2 and consider the following diagram of quotients of G

$$\begin{tikzcd}
 & \Xi \arrow[d, two heads] \\
G \arrow[r, two heads] \arrow[d, two heads] & G_2 \arrow[d, two heads] \\
\delta(G) \arrow[r, two heads] & \delta(G)_2
\end{tikzcd}$$

By Proposition 3.1.3, we have that for any $g \in \Xi$, $\delta(g)^2 = 1$, hence $g \in \delta(G)[2]$, hence, we can apply the lemma to $\delta(G)$ to conclude $\delta(G) = \delta(G)_2$. In particular, it follows that Ξ surjects onto $\delta(G)$, which implies $\rho_1 \sim \rho_2$ by Corollary 2.1.4. □

We can apply this theorem to the case of Galois representations:

Theorem 3.1.10. *Let K be a number field and E_λ a finite extension of $\mathbb{Q}_2$ with ring of integers $\mathcal{O}_\lambda$ and maximal ideal λ. Let*

$$\rho_1, \rho_2 \colon \mathrm{Gal}_K \longrightarrow \mathrm{GL}_2(E_\lambda),$$

be two continuous representations unramified outside a finite set S of primes of K, and such that (3.1) are satisfied, i.e.,

$$\mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \equiv 0 \pmod{\lambda} \quad \textit{and} \quad \det(\rho_1) \equiv \det(\rho_2) \equiv 1 \pmod{\lambda}.$$

Let $K_{2,S}$ be the compositum of all quadratic extensions of K unramified outside S and suppose that there exists a set of primes T disjoint from S such that

1. $\{\mathrm{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \in T\} \twoheadrightarrow \mathrm{Gal}(K_{2,S}/K)$.
2. $\mathrm{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ *and* $\det(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \det(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ *for all* $\mathfrak{p} \in T$.

Then $\rho_1 \sim \rho_2$.

Proof. Since Gal_K is compact, ρ_1 and ρ_2 preserve an $\mathcal{O}_\lambda$-lattice in E_λ^2, so that we may view them as taking values in $\mathrm{GL}_2(\mathcal{O}_\lambda)$ (this is Proposition 1.2.15). Then we only need to apply Theorem 3.1.9 to $\mathrm{Gal}(\overline{K}/K)_S = \mathrm{Gal}(K_S/K)$, where K_S is the maximal unramified extension outside S of K, since then $\mathrm{Gal}(\overline{K}/K)_2 = \mathrm{Gal}(K_{2,S}/K)$. □

To apply this criterion one needs to describe explicitly the compositum $K_{2,S}$, together with its Galois group. As an example, when $K = \mathbb{Q}$, the situation is particularly simple. For each prime $p \in \mathbb{Q}$, we need to describe the field $\mathbb{Q}_{2,p}$, i.e. the quadratic field unramified outside p. Since we are dealing with quadratic extensions, we need to differentiate between $p = 2$ and $p \neq 2$.

- For $p \neq 2$, let $d_p = \left(\frac{-1}{p}\right) p = (-1)^{p(p-1)/2}p$. Then $\mathbb{Q}_{2,p} = \mathbb{Q}(\sqrt{d_p})$. To describe the Galois group $\mathrm{Gal}(\mathbb{Q}_{2,p}/\mathbb{Q})$, define the Frobenius at the primes $q \neq 2, p$, which maps to $\left(\frac{d_p}{q}\right) = \left(\frac{q}{p}\right)$ under
$$\varepsilon_p\colon\ \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{2,p}) \cong \{\pm 1\}.$$
- For $p = 2$, $\mathbb{Q}_{2,2} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$ and Frob_q, for $q \neq 2$ goes to $q \pmod 8$ under
$$\varepsilon_2\colon\ \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{2,2}/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times.$$
- For a general S, $\mathbb{Q}_{2,S} = \prod_{p\in S} \mathbb{Q}_{2,p}$ and
$$\varepsilon_s = \prod_{p\in S} \varepsilon_p\colon\ \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{2,S}/\mathbb{Q}) \cong \prod_{p\in S} \mathrm{Gal}(\mathbb{Q}_{2,p}/\mathbb{Q}).$$

So, applying the criterion requires to compare the traces of ρ_1 and ρ_2 at $2^{|S|+1}$ primes at most.

Example 3.1.11. We are going to prove that the elliptic curve E of conductor 33[1] with Weierstrass equation

$$y^2 + xy = x^3 + x^2 - 6x - 9$$

is modular. For that, we are going to compare it with the newform $f \in S_2(33)$[2] having rational coefficients, trivial character, and q-expansion

$$f(q) = q + q^2 - q^3 - q^4 - 2q^5 - q^6 + 4q^7 - 3q^8 + q^9 + O(q^{10}).$$

From Chapter 1, we can associate a 2-adic Galois representation to both objects, $\rho_{E,2}$ and $\rho_{f,2}$ respectively. We want to see that $\rho_{E,2} \sim \rho_{f,2}$. Recall also that the characteristic polynomial for any $\mathfrak{p}$ above a prime p which does not ramify in $\rho_{E,2}$, i.e. $p \nmid 2 \cdot 33$, is of the form

$$x^2 - a_p(E)x + p \in \mathbb{Q}[x] \Longrightarrow \mathrm{tr}(\rho_{E,2}(\mathrm{Frob}_{\mathfrak{p}})) = a_p(E), \quad \det(\rho_{E,2}(\mathrm{Frob}_{\mathfrak{p}})) = p.$$

[1] Any elliptic curve in the isogeny class `https://www.lmfdb.org/EllipticCurve/Q/33a/`

[2] `https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/33/2/a/a/`

Similarly, for $\rho_{f,2}$ and the same $\mathfrak{p}$,

$$x^2-a_p(f)x+\chi(p)p \in \mathbb{Q}[x] \Longrightarrow \mathrm{tr}(\rho_{E,2}(\mathrm{Frob}_{\mathfrak{p}})) = a_p(f), \quad \det(\rho_{E,2}(\mathrm{Frob}_{\mathfrak{p}})) = \chi(p)p = p,$$

since χ is a trivial character.

We are going to apply Livné's method, i.e. Theorem 3.1.10, so we need to check that

$$\mathrm{tr}(\rho_{E,2}) \equiv \mathrm{tr}(\rho_{f,2}) \equiv 0 \pmod 2 \quad \text{and} \quad \det(\rho_{E,2}) \equiv \det(\rho_{f,2}) \equiv 1 \pmod 2.$$

To show that the determinant is 1 is easy: both residual representations have determinant the mod 2 cyclotomic character, which is just 1.

To show that the traces coincide and are even, however, is more difficult. To show that the elliptic curve has even trace, we observe that $E[2](\mathbb{Q}) \neq \emptyset$, since the point $P := [27/4 : -27/8 : 1] \in \mathbb{P}^1(\mathbb{Q})$ has order 2. One can check it with `Magma`. This implies that we can take P as one of the two elements of the basis of $E[2]$, hence any $\mathrm{Aut}(E[2]) \cong \mathrm{GL}_2(\mathbb{F}_2)$ has matrix in this basis of the form

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

Since the determinant is 1, then the matrix is of the form

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix},$$

with $c \in \mathbb{F}_2$. Thus $\overline{\rho}_{E,2}$ has traces $2 \equiv 0 \pmod 2$ as desired.

Now for the residual representation attached to the modular form, we have to use a different strategy, since we only know the characteristic polynomials at the Frobenius elements. Recall that the residual representation has image in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, i.e. it is one of the subgroups $\{1\}, C_2, C_3$ or S_3. If it has an element of order 3 (i.e. the image is C_3 or S_3) then the corresponding matrix in $\mathrm{GL}_2(\mathbb{F}_2)$ has trace 1 and therefore does not satisfy the hypothesis. Moreover, all elements of order 1 or 2 in $\mathrm{GL}_2(\mathbb{F}_2)$ are the identity or conjugations of the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

hence they have trace $0 \pmod 2$. So we need to see that the field fixed by the residual representation $\overline{\rho}_{f,2}$ does not have an element of order 3 in its Galois group. In order to do so, recall from Proposition 1.2.28 that $\overline{\rho}_{f,2}$ can ramify only at 2, 3 and 11. This allows us to search in the NFDB for a list of possible fields. It gives a long, but complete, list with 51 possible fields, in which the 2-torsion field of E is included. (No bound on the discriminant is required to have a complete result.)

Now to discard that the residual representation cuts out a field with Galois group C_3 or S_3, we must find, for each of the listed fields with degree ≥ 3, a prime p where Frob_p has order 3. Then, looking at $a_p(f)$ we see this number is even, so the trace of $\overline{rho}_{E,2}(\mathrm{Frob}_p)$ is $0 \pmod 2$, giving a contradiction. The code on Appendix A.3.1 finds such a prime p in all cases.

We now apply Theorem 3.1.10 with the following set of primes

$$T = \{5, 7, 13, 17, 19, 23, 29, 31, 37, 59, 67, 73, 83, 89, 167\}$$

whose corresponding Frobenius elements surject to the Galois group of $\mathbb{Q}_{2,S}/\mathbb{Q}$, the maximal polyquadratic extension of $\mathbb{Q}$ unramified outside $S = \{2, 3, 11\}$. We use the code provided in Appendix A.3.2 which verifies the equality of traces as desired. The output is

```
p = 5 || ap(f) =  -2 | ap(E) =  -2
p = 7 || ap(f) =  4 | ap(E) =  4
p = 13 || ap(f) =  -2 | ap(E) =  -2
p = 17 || ap(f) =  -2 | ap(E) =  -2
p = 19 || ap(f) =  0 | ap(E) =  0
p = 23 || ap(f) =  8 | ap(E) =  8
p = 29 || ap(f) =  -6 | ap(E) =  -6
p = 31 || ap(f) =  -8 | ap(E) =  -8
p = 37 || ap(f) =  6 | ap(E) =  6
p = 59 || ap(f) =  -4 | ap(E) =  -4
p = 67 || ap(f) =  -4 | ap(E) =  -4
p = 73 || ap(f) =  -14 | ap(E) =  -14
p = 83 || ap(f) =  12 | ap(E) =  12
p = 89 || ap(f) =  -6 | ap(E) =  -6
p = 167 || ap(f) =  0 | ap(E) =  0
```

Remark. It is possible to find a subset of T which also surjects onto $\mathrm{Gal}(\mathbb{Q}_{2,S}/\mathbb{Q})$ by finding only Frobenius elements that correspond to the conjugacy classes of the Galois group. The code in Appendix A.3.2 finds a Frobenius element for each one of the elements in $\mathrm{Gal}(\mathbb{Q}_{2,S}/\mathbb{Q})$ because this is a small example and the computation is inexpensive, but the Galois group gets exponentially larger with S.

Chapter 4

Conclusions and Future Work

In this thesis we have studied the problem of identifying when two ℓ-adic Galois representations

$$\rho_1, \rho_2 \colon \operatorname{Gal}_K \longrightarrow GL_n(\mathbb{Q}_\ell)$$

are equivalent, with special focus on the case $K = \mathbb{Q}$ and $n = 2$.

We have seen in detail the method that started all the theory of comparing Galois representations, as described by Serre in 1984, and also the algorithm for the reducible residual case, given by Livné in 1987. This thesis is aimed at master's or doctorate students who are trying to get into the theory of Galois representations. Our objective was to describe with full detail and give references to all of the results which are not standard in the curriculum of a Mathematics degree or master. We have put an extra effort to cite the results used in the arguments involving Algebraic Number Theory and Class Field Theory.

In Chapter 1, we have given a brief introduction to the necessary concepts from Algebraic Number Theory. Then we have introduced representations and Galois representations. Particularly, the Galois representations attached to elliptic curves and modular forms, the object of study in this thesis. In Chapter 2, we have seen the deviation group and the Faltings-Serre method and two applications of it in the case of elliptic curves over $\mathbb{Q}$. However, the method by Serre is only the first stepping stone into the world of comparing Galois representations.

We have also seen the Faltings-Serre-Livné method in Chapter 3, a variant that works when the image of the residual representations $\overline{\rho}_i$ is a 2-group and provides a computable criterion for deciding if two such representations are equivalent or not. This method was generalised by Gabriel Chênevert: he eliminated the hypothesis on the traces by augmenting the possible fields in the compositum similar to $K_{2,S}$ in Livné's case, but with more fields, not only quadratic extensions.

Moreover, trying to prove a theorem of Mestre (see Theorem 2.2.15) that we did not use in Chapter 2 requires of more advanced techniques, such as the cohomology of the Galois groups. These techniques are essential to someone who wants to do research in the area of Galois representations.

Finally, we have only seen applications of elliptic curves and modular forms over $\mathbb{Q}$. The more interesting examples (and the ones not considered trivial after the proof of the modularity theorem), are the ones that consider elliptic curves over a number field K or, more generally, abelian varieties over a number field K. Particularly, to prove the modularity of more abelian surfaces, such as [7], one should follow the line of work of John Cremona's PhD students, Alejandro Argàez [2] and Mattia Sanna [26], to extend their methods to the case of dimension 4, with a particular interest in the 2-adic case with reducible residual representations.

Appendix A

Code and functions

A.1 Code for the example of conductor 11

A.1.1 Check Ramification at 2

```
R<x> := PolynomialRing(Rationals());
possibleTildeK := [ x^4 - 2*x^3 - 4*x^2 - 6*x - 2, \
                    x^4 - 2*x^2 - 4*x - 1, \
                    x^4 - 2*x^3 - 3*x^2 + 2, \
                    x^4 - 44*x + 22, \
                    x^4 - 6*x^2 - 8*x - 25, \
                    x^4 - 8*x^2 - 16*x + 24 ];

E := EllipticCurve("11a3");
cInv := cInvariants(E);
f := x^3-27*cInv[1]*x-54*cInv[2];
K<a> := SplittingField(f);

fact2AtK := Factorization(2*MaximalOrder(K)); // we know that it ramifies in here
ramIdx := fact2AtK[1][2];
print "Factorization of 2 in K: ", fact2AtK;

for tildeK in possibleTildeK do
    tK<b> := SplittingField(tildeK);
    sbfLat := Subfields(tK, 6);
    for sbf in sbfLat do
        if IsIsomorphic(K,sbf[1]) then // Only if we have K as a subfield
            fact2AttK := Factorization(2*MaximalOrder(tK));
            ramIdxAttK := fact2AttK[1][2];
            print "Ramification index of 2 in tilde{K}/K = ", ramIdxAttK/ramIdx;
            break;
        end if;
    end for;
end for;
```

A.1.2 Check hypothesis for general N

```
N := 11;
print "N = 3 (mod 8)? ", N mod 8 eq 3;

R<x> := PolynomialRing(Rationals());

// Check the hypothesis on the class number of Q(sqrt(+-N));
print "h(Q(sqrt(-N))) =", ClassNumber(SplittingField(x^2+N));
print "h(Q(sqrt(N))) =", ClassNumber(SplittingField(x^2-N));

// Build the field lattice.
F<c>:=SplittingField(x^2+N);
RCF<r2> := AbsoluteField(NumberField(RayClassField(2*MaximalOrder(F))));
RCF<r2> := OptimizedRepresentation(RCF);
K<a> := Subfields(RCF,6)[1][1];
K<a> := OptimizedRepresentation(K);
M<b> := Subfields(K,3)[1][1];

// Check the hypothesis on the class number of M
print "h(M) =", ClassNumber(M);

// Check the hypothesis on the units of M
U,phi := UnitGroup(M);
print "Units of M";
[M!phi(U.i) : i in [1..Ngens(U)]];
minPoly := MinimalPolynomial(M!phi(U.2), Rationals());
print "Minimal polynomial for the fundamental unit:", minPoly;
// coerce into modulo N
coef := Coefficients(minPoly);
R<x> := PolynomialRing(Integers(N));
minPolyModN := 0*x;
for i in [1..#coef] do
    minPolyModN := minPolyModN + (Integers()!coef[i] mod Integers()!N)*x^(i-1);
end for;

print "Minimal polynomial mod N: ", minPolyModN;
fact := Factorization(minPolyModN);
print "Factorisation of minimal polynomial mod N:", fact;

residues := [Coefficients(f[1])[1] : f in fact];
print "List of tuples <root, IsQuadraticResidue>:", //
    [<r,LegendreSymbol(Integers()!r,N)> : r in residues];
```

A.2 Code for the example of conductor 5077

A.2.1 Find matrix order

```
QQ := Rationals();
R<x> := PolynomialRing(QQ);

redModP := function(f, p)
    Rp<y> := PolynomialRing(Integers(p));
    returnPoly := 0*y;
    coef := Coefficients(f);
    for i in [1..#coef] do
        returnPoly := returnPoly + (Integers()!coef[i] mod Integers()!p)*y^(i-1);
    end for;
    return returnPoly;
end function;

diagMatrix := function(charpoly)
    cpMod2 := redModP(charpoly,2);
    if not IsIrreducible(cpMod2) then
        print "The reduction mod 2 of the polynomial is not irreducible";
        return -1;
    end if;
    K,phi:=ext<GF(2)|cpMod2>;
    RK<z> := PolynomialRing(K);
    coef := [phi(c) : c in Coefficients(cpMod2)];
    retPol := 0*z;
    for i in [1..#coef] do
        retPol := retPol + coef[i]*z^(i-1);
    end for;
    roots := Roots(retPol);
    M := Matrix(2,2,[roots[1][1], 0, 0, roots[2][1]]);
    return M;
end function;

matOrder := function(M)
    prod := M;
    n := 1;
    Id := Matrix(2,2,[1,0,0,1]);
    while prod*M ne Id do
        prod := prod * M;
        n := n+1;
    end while;
    return n+1;
end function;

ff := Newform("G0N5077k2A"); // Gamma_0(N) of lvl 5077 & wt 2 & iso class A
p := 3;
apf := Coefficient(ff,p);
charpoly := x^2 - apf*x + p;
M := diagMatrix(charpoly);
```

```
matOrder(M);
```

A.2.2 Find quadratic extensions of K

```
/* Selmer group computations. */

QQ := Rationals();
PolsQ<x> := PolynomialRing(QQ);


/* 2-division field of the curve of conductor 5077. */

h := x^3 - 28*x + 50;
K := OptimizedRepresentation(SplittingField(h));
OK := Integers(K);
G, _, fromG := AutomorphismGroup(K);
G0 := [ fromG(g) : g in G  ];

/* Computing the full 2-Selmer group */


Prs := { s[1] : s in Factorisation(5077*OK) };
S2, toS2 := pSelmerGroup(2, Prs);
print "2-Selmer gruop allowing ramification at 5077 only has ", #S2, " elements";

/* Computing orbits. */

orbits := [ ];
S0 := Set(S2);

while(IsEmpty(S0) eq false) do
  s := Random(S0);
  orb := {@ toS2(phi(s@@toS2)) : phi in G0 @};
  Append(~orbits, orb);
  S0 := S0 diff orb;
  //H := sub<S2| orb>;
  //[#orb, #Invariants(H)];
end while;


/* Colecting S4 fields with correct ramification at 2. */

S4:=SymmetricGroup(4);
S4fields := [];
grdS4 := [];


print "There are ", #orbits, " of elemens in the 2-Selmer group";

orbitRank2 := [ s : s in orbits | #(sub<S2|s>) eq 4 ];
print "There are ", #orbitRank2, " orbits of rank 2.";
```

```
for s in orbitRank2 do
  s1 := s[1];
  L := AbsoluteField(ext<K|Polynomial([-s1@@toS2, 0, 1])>);
  OL := MaximalOrder(L : Ramification := [ 2, 5077 ]);
  _, OL := OptimizedRepresentation(OL);
  L := NumberField(OL);
  G, R, S := GaloisGroup(L);

  M := SplittingField(L);
  OM := MaximalOrder(M : Ramification := [ 2, 5077 ]);
  _, OM := OptimizedRepresentation(OM);
  M := NumberField(M);
  //Discriminant(OM)^(1/24);
  //Factorisation(Discriminant(OM));
  if Factorisation(2*OM)[1,2] eq 3 and IsIsomorphic(G, S4) then
   Append(~S4fields,DefiningPolynomial(M));
   Append(~grdS4,Discriminant(OM)^(1/24));
  end if;
end for;


print "There are ", #S4fields, " S4 fields to consider";

// sanity check
grdS4;
print "The three fields of root discriminant approx 113 belong to the set, as expected.";
```

A.2.3 Check the hypothesis on the traces

```
R<x> := PolynomialRing(Rationals());
K<a> := NumberField(x^6 - 2*x^5 - 163*x^4 - 284*x^3 + 2095*x^2 + //
                     6274*x + 4483);
possibleKTilde := [
    x^24 - 768*x^22 - 1044*x^21 + 207820*x^20 + 623960*x^19 - 16241308*x^18 -
        134490640*x^17 - 1199620624*x^16 + 6403989632*x^15 + 170496149024*x^14 +
        844907263648*x^13 + 9718281955056*x^12 + 10504707677504*x^11 +
        233726615121408*x^10 + 435373235946432*x^9 + 6632303935157952*x^8 +
        14462639076832256*x^7 + 75456769923825856*x^6 + 176765487641250304*x^5 +
        892265953333372672*x^4 + 3093979354576895488*x^3 +
        5735563640611065856*x^2 + 4848578612082150400*x + 2994197252275334144,
    x^24 + 4*x^23 + 344*x^22 + 1080*x^21 + 47393*x^20 + 185256*x^19 +
        18111384*x^18 + 169777454*x^17 + 2452136182*x^16 + 7745919636*x^15 +
        89352176896*x^14 + 676584855692*x^13 + 15134915674853*x^12 +
        132167280625752*x^11 + 1124854949679324*x^10 + 5915789283347506*x^9 +
        38408193987041206*x^8 + 165413107052078948*x^7 + 203694171277625524*x^6
        + 202552723280751218O*x^5 + 3217181714617109185*x^4 -
        22296957747934339616*x^3 + 4014651578422035762O*x^2 -
        32029840653811622586*x + 11796203027981615769,
    x^24 - 8*x^23 - 2*x^22 + 672*x^21 + 9321*x^20 - 258468*x^19 + 3859746*x^18 -
        58106896*x^17 + 743541567*x^16 - 7353174560*x^15 + 72342120578*x^14 -
        703986635908*x^13 + 6013059324607*x^12 - 43380528820464*x^11 +
        293650020729538*x^10 - 1907777596031764*x^9 + 10720003549794808*x^8 -
        46359869994967172*x^7 + 189164556190567356*x^6 - 771680088204856584*x^5
        + 2365119561410505664*x^4 - 5136262747153807584*x^3 +
        20667644673950506656*x^2 - 14175534002866179840*x +
        85365252617909589184,
    x^24 + 362*x^22 - 888*x^21 + 37205*x^20 - 212920*x^19 + 3168390*x^18 -
        25416556*x^17 + 143450887*x^16 - 671681992*x^15 + 1784818490*x^14 +
        25393019780*x^13 - 363601496305*x^12 + 3636405611644*x^11 -
        3272703778574*x^10 - 245336839380128*x^9 + 2721592161459780*x^8 -
        14745168147343628*x^7 + 45804471248662724*x^6 - 82505563999076880*x^5 +
        83640048162301808*x^4 + 545365373218400*x^3 - 257251747274755520*x^2 +
        151600036671104896*x + 710701106514873152,
    x^24 - 12*x^23 - 74*x^22 + 1268*x^21 + 521*x^20 - 44700*x^19 + 39450*x^18 +
        759704*x^17 - 899161*x^16 - 6931956*x^15 + 7391334*x^14 + 34259440*x^13
        - 26126405*x^12 - 88439984*x^11 + 38036334*x^10 + 110900964*x^9 -
        25235180*x^8 - 64163060*x^7 + 8311884*x^6 + 14870944*x^5 - 1031600*x^4 -
        795200*x^3 - 20096*x^2 + 3008*x + 64,
    x^24 - 12*x^23 + 78*x^22 - 340*x^21 + 1599*x^20 - 9028*x^19 + 37544*x^18 -
        74884*x^17 - 80657*x^16 + 871420*x^15 - 4150194*x^14 + 25893380*x^13 -
        115564199*x^12 + 196897892*x^11 + 609983388*x^10 - 4216898652*x^9 +
        9448977848*x^8 - 2624229984*x^7 - 37912012512*x^6 + 101919818384*x^5 -
        97261562848*x^4 - 81980901264*x^3 + 370117386688*x^2 - 458624922688*x +
        208312622192,
    x^24 + 6*x^23 + 203*x^22 + 1104*x^21 + 16975*x^20 + 82774*x^19 + 767877*x^18
        + 3287588*x^17 + 20702760*x^16 + 75868256*x^15 + 345575448*x^14 +
        1059356600*x^13 + 3618564372*x^12 + 9109880416*x^11 + 23788563360*x^10 +
        48229480736*x^9 + 96563687472*x^8 + 153614027680*x^7 + 232906571824*x^6
        + 279572330304*x^5 + 310295077184*x^4 + 260804775552*x^3 +
        192919551488*x^2 + 93122246784*x + 34601690048
];
E := EllipticCurve("5077a1");
M := ModularForms(5077,2);
ff := Newform(M, 1, 1);

for f in possibleKTilde do
    Ktilde<a> := NumberField(f);
    flag := true;
    index := 2;
    while flag do
        p := NthPrime(index);
        Frob := FrobeniusElement(Ktilde, p);
        if Order(Frob) eq 4 then
            apf := Coefficient(ff, p);
            apE := FrobeniusTraceDirect(E,p);
            if apf eq apE then
                flag := false;
            end if;
        end if;
        index := index+1;
    end while;
    print "p =", p, "||", "ap(f) = ", apf, "|", "ap(E) = ", apE;
end for;
```

A.2.4 Possible fields $\widetilde{K}/K$

$$\begin{aligned}
x^{24} - 768x^{22} - 1044x^{21} + 207820x^{20} + 623960x^{19} - 16241308x^{18} - 134490640x^{17} \\
-1199620624x^{16} + 6403989632x^{15} + 170496149024x^{14} + 844907263648x^{13} \\
+9718281955056x^{12} + 10504707677504x^{11} + 233726615121408x^{10} \\
+435373235946432x^{9} + 6632303935157952x^{8} + 14462639076832256x^{7} \\
+75456769923825856x^{6} + 176765487641250304x^{5} + 892265953333372672x^{4} \\
+3093979354576895488x^{3} + 5735563640611065856x^{2} \\
+4848578612082150400x + 2994197252275334144
\end{aligned}$$

$$\begin{aligned}
x^{24} + 4x^{23} + 344x^{22} + 1080x^{21} + 47393x^{20} + 185256x^{19} + 18111384x^{18} \\
+169777454x^{17} + 2452136182x^{16} + 7745919636x^{15} + 89352176896x^{14} \\
+676584855692x^{13} + 15134915674853x^{12} + 132167280625752x^{11} \\
+1124854949679324x^{10} + 5915789283347506x^{9} + 38408193987041206x^{8} \\
+165413107052078948x^{7} + 203694171277625524x^{6} + 2025527232807512180x^{5} \\
+3217181714617109185x^{4} - 2229695774793433961 6x^{3} \\
+40146515784220357620x^{2} - 32029840653811622586x \\
+11796203027981615769
\end{aligned}$$

$$\begin{aligned}
x^{24} - 8x^{23} - 2x^{22} + 672x^{21} + 9321x^{20} - 258468x^{19} + 3859746x^{18} - 58106896x^{17} \\
+743541567x^{16} - 7353174560x^{15} + 72342120578x^{14} - 703986635908x^{13} \\
+6013059324607x^{12} - 43380528820464x^{11} + 293650020729538x^{10} \\
-1907777596031764x^{9} + 10720003549794808x^{8} - 46359869994967172x^{7} \\
+189164556190567356x^{6} - 771680088204856584x^{5} + 2365119561410505664x^{4} \\
-5136262747153807584x^{3} + 2066764467395050665 6x^{2} \\
-14175534002866179840x + 85365252617909589184
\end{aligned}$$

$$\begin{aligned}
x^{24} + 362x^{22} - 888x^{21} + 37205x^{20} - 212920x^{19} + 3168390x^{18} - 25416556x^{17} \\
+143450887x^{16} - 671681992x^{15} + 1784818490x^{14} + 25393019780x^{13} \\
-363601496305x^{12} + 3636405611644x^{11} - 3272703778574x^{10} - 245336839380128x^{9} \\
+2721592161459780x^{8} - 14745168147343628x^{7} + 45804471248662724x^{6} \\
-82505563999076880x^{5} + 83640048162301808x^{4} + 545365373218400x^{3} \\
-25725174727475552 0x^{2} + 151600036671104896x + 710701106514873152
\end{aligned}$$

$$\begin{aligned}x^{24} - 12x^{23} - 74x^{22} + 1268x^{21} + 521x^{20} - 44700x^{19} + 39450x^{18} + 759704x^{17}\\ -899161x^{16} - 6931956x^{15} + 7391334x^{14} + 34259440x^{13} - 26126405x^{12}\\ -88439984x^{11} + 38036334x^{10} + 110900964x^{9} - 25235180x^{8} - 64163060x^{7}\\ +8311884x^{6} + 14870944x^{5} - 1031600x^{4} - 795200x^{3} - 20096x^{2} + 3008x + 64\end{aligned}$$

$$\begin{aligned}x^{24} - 12x^{23} + 78x^{22} - 340x^{21} + 1599x^{20} - 9028x^{19} + 37544x^{18} - 74884x^{17}\\ -80657x^{16} + 871420x^{15} - 4150194x^{14} + 25893380x^{13} - 115564199x^{12}\\ +196897892x^{11} + 609983388x^{10} - 4216898652x^{9} + 9448977848x^{8}\\ -2624229984x^{7} - 37912012512x^{6} + 101919818384x^{5} - 97261562848x^{4}\\ -81980901264x^{3} + 370117386688x^{2}\\ -458624922688x + 208312622192\end{aligned}$$

$$\begin{aligned}x^{24} + 6x^{23} + 203x^{22} + 1104x^{21} + 16975x^{20} + 82774x^{19} + 767877x^{18} + 3287588x^{17}\\ +20702760x^{16} + 75868256x^{15} + 345575448x^{14} + 1059356600x^{13}\\ +3618564372x^{12} + 9109880416x^{11} + 23788563360x^{10} + 48229480736x^{9}\\ +96563687472x^{8} + 153614027680x^{7} + 232906571824x^{6} + 279572330304x^{5}\\ +310295077184x^{4} + 260804775552x^{3} + 192919551488x^{2}\\ +93122246784x + 34601690048\end{aligned}$$

A.3 Code for the example of conductor 33

A.3.1 Find fixed field by modular residual representation

```
QQ := Rationals();
R<x> := PolynomialRing(QQ);

ff := Newform("G0N33k2A");

possibleFields := [ x^2 - x + 1, x^2 + 1, x^2 - 2, x^2 + 2, \
x^2 - x + 3, x^2 - 3, x^2 - 6, x^2 + 6, x^2 - x - 8, x^2 - 11, \
x^2 - 22, x^2 + 22, x^2 + 33, x^2 - 66, x^2 + 66, x^3 - 3*x - 1, \
x^3 - x^2 + x + 1, x^3 - 2, x^3 - 3, x^3 - 3*x - 4, \
x^3 - x^2 + 4*x + 2, x^3 + 3*x - 2, x^3 - 12, x^3 - 6, \
x^3 - 3*x - 10, x^3 - x^2 - 7*x + 13, x^3 + 6*x - 1, \
x^3 - 11, x^3 - 9*x - 6, x^3 + 6*x - 10, x^3 - 12*x - 28, \
x^3 + 6*x - 12, x^3 - 9*x - 3, x^3 - 22, x^3 - 9*x - 14, \
x^3 - 99, x^3 - 33, x^3 + 6*x - 32, x^3 + 33*x - 22, \
x^3 + 33*x - 176, x^3 - 33*x - 66, x^3 - 132, x^3 - 396, \
x^3 - 198, x^3 - 66, x^3 - 66*x - 176, x^3 + 18*x - 48, \
x^3 - 9*x - 30, x^3 - 27*x - 78, x^3 - 99*x - 330, \
x^3 - 99*x - 66];
```

```
for f in possibleFields do
    if Degree(f) eq 2 then continue; end if;
    print "---------";
    print "f(x) =", f;
    Kf<a> := SplittingField(f);

    n := 2;
    flag := false;
    while flag eq false do
        p := NthPrime(n);
        if p eq 2 or p eq 3 or p eq 11 then
            n := n+1;
            continue;
        end if;

        apf := Coefficient(ff,p);
        ordK := Order(FrobeniusElement(Kf,p));

        if ordK eq 3 and Integers()!apf mod 2 eq 0 then
            print "Frobenius has order 3 but the trace is even:", apf;
            flag := true;
        end if;
        n := n+1;
    end while;

end for;
```

A.3.2 Livné's theorem

```
R<x> := PolynomialRing(Rationals());

E := EllipticCurve("33a3");
ff := Newform("G0N33k2A");

S := {2,3,11};

Q23<ap> := NumberField(x^2-3);
Q211<ap> := NumberField(x^2-11);
Q22<a2> := CyclotomicField(8);
Q2S<a> := OptimizedRepresentation(CompositeFields(CompositeFields(Q23,Q211)[1],Q22)[1]);
G := GaloisGroup(Q2S);

elsG := {g : g in G};
elsG := elsG diff {Id(G)};

i := 1;
while not IsEmpty(elsG) do
    p := NthPrime(i);
    if p notin S then
        Frobp := FrobeniusElement(Q2S,p);
        if Frobp in elsG then
```

```
            apf := Coefficient(ff,p);
            apE := FrobeniusTraceDirect(E,p);
            if apf eq apE then
                elsG := elsG diff {Frobp};
                print "p =", p, "||", "ap(f) = ", apf, "|", "ap(E) = ", apE;
            end if;
        end if;
    end if;
    i := i+1;
end while;
```

Appendix B

Group isomorphisms from the quartic field method

B.1 Proof $GL_2(\mathbb{F}_2) \cong S_3$

We can represent S_3 as the permutations of a set of three elements $\{1, 2, 3\}$:

$$S_3 = \{\text{Id},\ (12),\ (13),\ (23),\ (123),\ (132)\}.$$

And $GL_2(\mathbb{F}_2)$ is the group of invertible 2×2 matrices with coefficients in $\mathbb{F}_2$, i.e. its the group of matrices with coefficients $\{0, 1\}$ and determinant 1.

$$GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Then the isomorphism is explicitly given by:

$$\begin{array}{rlrlrl}
\text{Id} \longleftrightarrow & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & (12) \longleftrightarrow & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & (13) \longleftrightarrow & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\
(23) \longleftrightarrow & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & (123) \longleftrightarrow & \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & (132) \longleftrightarrow & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}
\end{array}$$

B.2 Proof $M_2(\mathbb{F}_2) \cong \mathbb{F}_2^2 \oplus V_4$

Recall that $M_2(\mathbb{F}_2)$ is the additive group of 2×2 matrices with coefficients in $\mathbb{F}_2$. Particularly, its the set

$$M_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \{0, 1\} \right\}.$$

This set has cardinality $2^4 = 16$, since we have 2 choices (0 or 1) for 4 variables (a, b, c, d).

Then, we represent $\mathbb{F}_2^2$ as a subgroup of $M_2(\mathbb{F}_2)$, particularly,

$$\mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Similarly, we represent the Klein group V_4 as a subgroup of $M_2(\mathbb{F}_2)$ in the following manner:

$$V_4 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

Then, as an S_3 module under the action by conjugation of $GL_2(\mathbb{F}_2) \cong S_3$, we have

$$M_2(\mathbb{F}_2) \cong \mathbb{F}_2^2 \oplus V_4.$$

The explicit isomorphism is given by:

$$\begin{array}{ll}
\begin{pmatrix}0&0\\0&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&0\\0&0\end{pmatrix} \oplus \begin{pmatrix}0&0\\0&0\end{pmatrix} & \begin{pmatrix}0&0\\0&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&1\\1&1\end{pmatrix} \oplus \begin{pmatrix}0&1\\1&0\end{pmatrix} \\[1em]
\begin{pmatrix}0&0\\1&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&0\\0&1\end{pmatrix} \oplus \begin{pmatrix}1&0\\1&1\end{pmatrix} & \begin{pmatrix}0&0\\1&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&1\\1&0\end{pmatrix} \oplus \begin{pmatrix}1&1\\0&1\end{pmatrix} \\[1em]
\begin{pmatrix}0&1\\0&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&0\\0&1\end{pmatrix} \oplus \begin{pmatrix}1&1\\0&1\end{pmatrix} & \begin{pmatrix}0&1\\0&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&1\\1&0\end{pmatrix} \oplus \begin{pmatrix}1&0\\1&1\end{pmatrix} \\[1em]
\begin{pmatrix}0&1\\1&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&0\\0&0\end{pmatrix} \oplus \begin{pmatrix}0&1\\1&0\end{pmatrix} & \begin{pmatrix}0&1\\1&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&1\\1&1\end{pmatrix} \oplus \begin{pmatrix}0&0\\0&0\end{pmatrix} \\[1em]
\begin{pmatrix}1&0\\0&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&1\\1&0\end{pmatrix} \oplus \begin{pmatrix}0&1\\1&0\end{pmatrix} & \begin{pmatrix}1&0\\0&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&0\\0&1\end{pmatrix} \oplus \begin{pmatrix}0&0\\0&0\end{pmatrix} \\[1em]
\begin{pmatrix}1&0\\1&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&1\\1&1\end{pmatrix} \oplus \begin{pmatrix}1&1\\0&1\end{pmatrix} & \begin{pmatrix}1&0\\1&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&0\\0&0\end{pmatrix} \oplus \begin{pmatrix}1&0\\1&1\end{pmatrix} \\[1em]
\begin{pmatrix}1&1\\0&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&1\\1&1\end{pmatrix} \oplus \begin{pmatrix}1&0\\1&1\end{pmatrix} & \begin{pmatrix}1&1\\0&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}0&0\\0&0\end{pmatrix} \oplus \begin{pmatrix}1&1\\0&1\end{pmatrix} \\[1em]
\begin{pmatrix}1&1\\1&0\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&1\\1&0\end{pmatrix} \oplus \begin{pmatrix}0&0\\0&0\end{pmatrix} & \begin{pmatrix}1&1\\1&1\end{pmatrix} \longleftrightarrow \begin{pmatrix}1&0\\0&1\end{pmatrix} \oplus \begin{pmatrix}0&1\\1&0\end{pmatrix}
\end{array}$$

Bibliography

[1] M. K. Agrawal et al. "Elliptic Curves of Conductor 11". In: *Mathematics of Computation* 35.151 (1980), pp. 991–1002. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2006209.

[2] Alejandro Argáez-García and John Cremona. "Black Box Galois representations". In: *Journal of Algebra* 512 (2018), pp. 526 –565. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2018.05.017.

[3] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., 1969, pp. ix+128.

[4] Nigel Boston. "A refinement of the Faltings-Serre method". In: *Number theory (Paris, 1992–1993)*. Vol. 215. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1995, pp. 61–68. DOI: 10.1017/CBO9780511661990.004. URL: https://doi.org/10.1017/CBO9780511661990.004.

[5] Christophe Breuil et al. "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises". In: *J. Amer. Math. Soc.* 14.4 (2001), pp. 843–939. ISSN: 0894-0347. DOI: 10.1090/S0894-0347-01-00370-8. URL: https://doi.org/10.1090/S0894-0347-01-00370-8.

[6] Armand Brumer and Kenneth Kramer. "The rank of elliptic curves". In: *Duke Math. J.* 44.4 (Dec. 1977), pp. 715–743. DOI: 10.1215/S0012-7094-77-04431-3. URL: https://doi.org/10.1215/S0012-7094-77-04431-3.

[7] Armand Brumer et al. "On the paramodularity of typical abelian surfaces". In: *Algebra and Number Theory* 13.5 (2019), 1145–1195. ISSN: 1937-0652. DOI: 10.2140/ant.2019.13.1145. URL: http://dx.doi.org/10.2140/ant.2019.13.1145.

[8] Gabriel Chenevert. *Exponential sums, hypersurfaces with many symmetries and Galois representations*. Thesis (Ph.D.)–McGill University (Canada). ProQuest LLC, Ann Arbor, MI, 2008, p. 162. ISBN: 978-0494-53476-2. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:NR53476.

[9] Henri Cohen. *Advanced topics in computational number theory*. Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+578. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0. URL: https://doi.org/10.1007/978-1-4419-8489-0.

[10] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[11] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. "Proving modularity for a given elliptic curve over an imaginary quadratic field". In: *Math. Comp.* 79.270 (2010), pp. 1145–1170. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-09-02291-1. URL: https://doi.org/10.1090/S0025-5718-09-02291-1.

[12] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Invent. Math.* 73.3 (1983), pp. 349–366. ISSN: 0020-9910. DOI: 10.1007/BF01388432. URL: https://doi.org/10.1007/BF01388432.

[13] Walter L. Hill. "Formal groups and zeta-functions of elliptic curves". In: *Invent. Math.* 12 (1971), pp. 321–336. ISSN: 0020-9910. DOI: 10.1007/BF01403311. URL: https://doi.org/10.1007/BF01403311.

[14] Klaus Hulek, Remke Kloosterman, and Matthias Schütt. "Modularity of Calabi-Yau varieties". In: *Global aspects of complex geometry.* Springer, Berlin, 2006, pp. 271–309. DOI: 10.1007/3-540-35480-8_8. URL: https://doi.org/10.1007/3-540-35480-8_8.

[15] John W. Jones and David P. Roberts. "A database of number fields". In: *LMS Journal of Computation and Mathematics* 17.1 (2014), 595–618. DOI: 10.1112/S1461157014000424.

[16] Chandrashekhar Khare and Jean-Pierre Wintenberger. "Serre's modularity conjecture. I". In: *Invent. Math.* 178.3 (2009), pp. 485–504. ISSN: 0020-9910. DOI: 10.1007/s00222-009-0205-7. URL: https://doi.org/10.1007/s00222-009-0205-7.

[17] Chandrashekhar Khare and Jean-Pierre Wintenberger. "Serre's modularity conjecture. II". In: *Invent. Math.* 178.3 (2009), pp. 505–586. ISSN: 0020-9910. DOI: 10.1007/s00222-009-0206-6. URL: https://doi.org/10.1007/s00222-009-0206-6.

[18] Ron Livné. "Cubic exponential sums and Galois representations". In: *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985).* Vol. 67. Contemp. Math. Amer. Math. Soc., Providence, RI, 1987, pp. 247–261. DOI: 10.1090/conm/067/902596. URL: https://doi.org/10.1090/conm/067/902596.

[19] Jean-François Mestre. "Courbes de Weil de conducteur 5077". In: *C. R. Acad. Sci. Paris Sér. I Math.* 300.15 (1985), pp. 509–512. ISSN: 0249-6291.

[20] James S. Milne. *Algebraic Number Theory (v3.08).* Available at www.jmilne.org/math/. 2020.

[21] J.S. Milne. *Class Field Theory (v4.03).* Available at www.jmilne.org/math/. 2020.

[22] Hyunsuk Moon and Yuichiro Taguchi. "Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations". In: Extra Vol. Kazuya Kato's fiftieth birthday. 2003, pp. 641–654.

[23] Nicole Moser. "Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbf{Q}$". In: *Abh. Math. Sem. Univ. Hamburg* 48 (1979), pp. 54–75. ISSN: 0025-5858. DOI: 10.1007/BF02941290. URL: https://doi.org/10.1007/BF02941290.

[24] M. Ram Murty. "Congruences between modular forms". In: *Analytic number theory (Kyoto, 1996).* Vol. 247. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1997, pp. 309–320. DOI: 10.1017/CBO9780511666179.020. URL: https://doi.org/10.1017/CBO9780511666179.020.

[25] Jürgen Neukirch. *Algebraic number theory.* Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0. URL: https://doi.org/10.1007/978-3-662-03983-0.

[26] Mattia Sanna. "On the equivalence of 3-adic Galois representations". University of Warwick PhD thesis, unpublished as of 1st of September of 2020. 2020.

[27] Jean-Pierre Serre. *Correspondance Serre-Tate. Vol. II.* Vol. 14. Documents Mathématiques (Paris) [Mathematical Documents (Paris)]. Edited, and with notes and commentaries by Pierre Colmez and Jean-Pierre Serre. Société Mathématique de France, Paris, 2015, pp. 699–705. ISBN: 978-2-85629-803-9.

[28] Jean-Pierre Serre. *Local fields.* Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241. ISBN: 0-387-90424-7.

[29] Jean-Pierre Serre. *Oeuvres/Collected papers. IV. 1985–1998.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2013, pp. 27–33. ISBN: 978-3-642-39839-1.

[30] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Invent. Math.* 15.4 (1972), pp. 259–331. ISSN: 0020-9910. DOI: 10.1007/BF01405086. URL: https://doi.org/10.1007/BF01405086.

[31] Bennett Setzer. "Elliptic curves of prime conductor". In: *J. London Math. Soc. (2)* 10 (1975), pp. 367–378. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-10.3.367. URL: https://doi.org/10.1112/jlms/s2-10.3.367.

[32] Joseph H. Silverman. *The arithmetic of elliptic curves.* Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[33] Richard Taylor and Andrew Wiles. "Ring-theoretic properties of certain Hecke algebras". In: *Ann. of Math. (2)* 141.3 (1995), pp. 553–572. ISSN: 0003-486X. DOI: 10.2307/2118560. URL: https://doi.org/10.2307/2118560.

[34] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". In: *Ann. of Math. (2)* 141.3 (1995), pp. 443–551. ISSN: 0003-486X. DOI: 10.2307/2118559. URL: https://doi.org/10.2307/2118559.