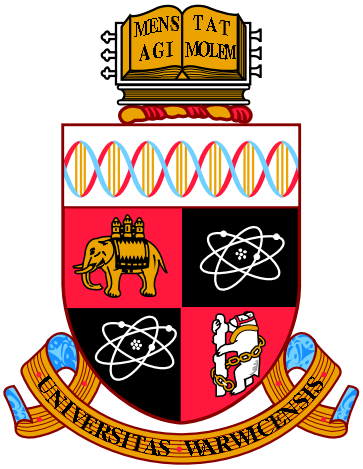


On the equivalence of 3-adic Galois representations

by

Mattia Sanna

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Department of Mathematics

2020

Contents

Acknowledgments

Firstly, I would like to thank my supervisor Professor John E. Cremona, for his constant guidance and support through these years. I am thankful for his continuous encouragement, the brilliant discussions we had, and all the time he dedicates to me. His passion and knowledge of mathematics is a great inspiration for me.

A special thank you goes to Professor David Loeffler and Dr Nuno Freitas for the enlightening discussions and suggestions. I am also grateful to the Number Theory group and PhD students at the University of Warwick for the stimulating environment.

I am and always be in debt with my parents Giuliana e Pietro. Nothing could be possible to achieve without their enormous sacrifices and support trough my entire life. No thanks will be enough for what they did and continue to do. I thank you also my brother Riccardo for showing me to always aim for greater things.

I am thankful to Max, Alessandro, Giovanni, Gian, il Lama, Cassa, Zampa, Alice, Chicco, Serena, Bruno, Ilaria, Andrea, Livia, Ferdinando, Marco, Matteo, Lorenzo, George, Edwin and Aurelio for all the scheduled sbratto-dinner and friendship. You guys made the life here fantastic.

My warm thanks to Gigio, Sabino, Carletto, Darietto, Isa, il Santa, Luciana, Cristina, Giuliano, Silvia, Ivo, Daniele, Silvia, Benedetta & Caiulo, Busquets, Marco, Roberta, Francesco, Antonietta Frapi, and Libera. Even if we are in different parts of the world, you always demonstrated your friendship, thank you so much, guys.

I want to thanks my oldest friends, the *Boars*: Frankie, Jazzo, Moji, Gesoo, il Baghira-Socio. Your friendship is invaluable to me. We grow-up together and

probably made several stupid things together, but guys, I would do all over again.

Finally, my most enormous gratitude is for you, Cristiana. You are the bravest person I have ever met, and you are a constant inspiration for me. You are my idol, and your support, courage, and love gave me the happiness and strength to achieve all of this. Thank you for being in my life.

Declarations

The Preliminaries Chapter is expository recalling primary background material. No originality is claimed for this chapter. From Chapter 2 on, I declare that, unless otherwise indicated and to the best of my knowledge, the contents are the product of my own original research, under the guidance of my supervisor.

Abstract

Throughout this thesis, we develop theory and the algorithms that lead to an effective method to study the equivalence of two-dimensional 3-adic Galois representations attached to number fields. In order to reach our goal we need three steps: recognising the determinant characters, determining the residual or mod3 representations, and finally proving that the representations agree modulo 3^k for any positive integer k. We are able to achieve this using only a finite amount of information coming from the representations.

We start with a method that allows us to recognise any one-dimensional Galois representation of any number field K that is unramified outside a given finite set S of primes of K. Afterwards, we extend the methods developed by Argaez-Garcia and Cremona to determine 2-dimensional *black box* Galois representations of K, unramified outside a given finite set S, whose image lies in $\mathrm{GL}_2(\mathbb{F}_3)$. If such representations are irreducible, we can also prove if they are equivalent over $\mathrm{GL}_2(\mathbb{F}_3)$. Moreover, due to recent results in modularity lifting, these two methods have an impact on solving modularity problems.

Furthermore, starting from two 2-dimensional 3-adic Galois representations of K unramified outside the same S, which we proved by the previous results to have the same determinant character and equivalent residual representations, we are able to prove whether they are equivalent over $\mathrm{GL}_2(\mathbb{Z}_3)$ by checking their traces at finitely many places.

Finally, since we are able to achieve each step by just computing characteristic polynomials of Frobenius elements of $\mathscr{G}_K$, the absolute Galois group of K, at a suitable and computable finite set of primes of K, all our theoretical result are

actually effective. That is, we can, and we did, implement them as algorithms that return a precise answer in a finite (and reasonable) amount of time. An application of the algorithms developed is to prove modularity of elliptic curves. We address this studying Galois representations attached to Bianchi modular forms and elliptic curves defined over imaginary quadratic fields of class number one.

Introduction

Galois representations have a crucial role in modern number theory. Hence it is important to be able to characterise them and prove isomorphism between them. As well as global results establishing categorical equivalence of the objects related to them, the understanding of specific Galois representations may give valuable insight to develop new theories. For this reason, methods that provide information on Galois modules and answer the isomorphism question are of interest. One of the strongest results in this direction is the Faltings-Serre-Livné method [31], [42] for two-dimensional Galois representations that take values in a finite extension of $\mathbb{Q}_2$. Several number theorists have translated these theoretical results into a deterministic and implementable algorithm, for example, the work of Dieulefait, Guerberoff and Pacetti [21], where they implemented the method under the condition that one of the representations comes from an elliptic curve defined over an imaginary quadratic field. Recently Schembri in [38] with the support of his implementation of the Livné method was able to prove that the geometric objects attached to some Bianchi modular forms are abelian varieties with quaternionic multiplication. A significant breakthrough is the recent works of Argáez-Garcia [4], Argáez-Garcia and Cremona [5] about 2-dimensional Galois representations with values in $\mathbb{Q}_2$, in which they developed the theory and the algorithms that lead to full implementation of the Faltings-Serre method for such representations with residually absolutely irreducible representations.

In general, the philosophy behind the original Faltings-Serre method is to retrieve information on two given Galois representations from a finite number of known traces and determinants to check whether they are isomorphic. Because Galois representations naturally arise in several dimensions, and with values in some extension of $\mathbb{Q}_\ell$, we would like to have an effective Faltings-Serre that works in such generality. The theoretical existence of such method for general n-dimensional representations with values in $\mathbb{Z}_\ell$ was achieved in 2019 by Brumer, Pacetti, Poor, Tornaría, Voight, and Yuen [8] and they provided an effective method for representations with values

in $\mathrm{GSp}_4(\mathbb{Q}_2)$. The effective result was used to present examples of paramodular abelian surfaces. Furthermore, the astonishing results obtained in modularity lifting [1], later refined by Allen, Khare, and Thorne in [2] to be applied to 2-dimensional $\mathbb{F}_p$-representations with p a small rational prime, moves the focus to the study of residual representations. Indeed, under certain precise hypotheses, they prove that having an isomorphism between residual representations of two Galois representations with values in $\mathrm{GL}_n(\bar{\mathbb{Q}}_\ell)$, with one representation not known to come from an automorphic form, is enough to assert the existence of an automorphic form with attached Galois representation globally isomorphic to the "unknown-modular" one. It is important to remark that this last modularity lifting theorem requires much weaker hypotheses when ℓ is odd, and therefore it may be used in much more general situations then when $\ell = 2$. Finally, most of the representations we are interested in form a compatible-system of representations allowing us to pick our favourite prime ℓ, work with representations that take values in $\overline{\mathbb{Q}}_\ell$, and if we are able to prove that some isomorphism holds in this case, then it holds also for all primes. Thus, having a 3-adic version of the Faltings-Serre method, we will be able to study much more easily compatible systems of $\mathrm{GL}_2(\mathbb{Q}_\ell)$-valued Galois representations if we are able to understand in turn the associated 2-adic and 3-adic representations. In particular, in case we want to prove modularity (for example of an elliptic curve defined over a number field) the mod 3 modularity lifting offers more possibilities to be applied then the mod 2 equivalent.

Highly motivated by all these developments, in this thesis, we study the following problem:

Problem. *Let K be a number field and S a finite set of primes of K. Fix an algebraic closure $\overline{K}$ of K and let $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Let $\rho_1, \rho_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}(V)$ be two 3-adic Galois representations $\mathscr{G}_K$ such that we only know:*

i) $\dim_{\mathbb{Q}_3} V = 2$*;*

ii) ρ_1, ρ_2 *are both unramified outside* S*;*

iii) the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ *for each* $\mathfrak{p} \notin S$*.*

Then is it possible to prove with an effective method that ρ_1 and ρ_2 are equivalent?

We have a positive answer that leads to a method which we may refer as a 3-adic Faltings-Serre method. Throughout the chapters of this work we will develop all the theory necessary to prove it and make it an effective algorithm.

The work is divided into the following contents.

Chapter 1 focusses on preliminaries, recalling basic notions on group representations and Galois representations. No originality is claimed in the discussion occurring in this chapter.

In Chapter 2 we study one-dimensional Galois representations taking values in $\mathcal{O}_L^\times$, where $\mathcal{O}_L^\times$ is the ring of integers of a finite degree local field $L/\mathbb{Q}_\ell$. In particular we are interested in recognising characters $\chi : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$ that are unramified outside a finite set S of primes of K from a finite number of known values. To achieve the goal we will introduce for any $n \geq 2$ a *n-basis* that is a finite set $T_n(S)$ of primes of K disjoint from S. In particular, the definition $T_n(S)$ only depends on K, S and not on the particular representation we are studying. The main result of the chapter is the following theorem:

Theorem (Theorem 2.0.5)**.** *Let K be a number field and let S be a finite set of primes of K. Let ℓ be a prime number, let $L/\mathbb{Q}_\ell$ be a finite extension of degree d with ring of integers $\mathcal{O}_L$ and residue field $\mathbb{F}_q$, where $q = \ell^f$ for some positive integer f. Let $p_1, \ldots, p_h$ be the prime dividing $q-1$ and consider*

$$T(S) = T_{q-1}(S) \cup T_\ell(S) := \bigcup_{i=1}^{h} T_{p_i}(S) \cup T_\ell(S).$$

Assume we have a continuous character $\chi : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$ unramified outside S that satisfies $\chi(\mathrm{Frob}_\mathfrak{p}) = 1$ for all $\mathfrak{p} \in T(S)$. Then χ is trivial.

A straightforward corollary is that if two characters, both unramified outside S, agree on $T(S)$ then they are the same.

In Chapter 3 and Chapter 4 we will present a careful study of two dimensional mod 3 Galois representations. In general a 2-dimensional Galois representation over $\mathbb{F}_\ell$ is a continuous homomorphism $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}(V)$ with V a 2-dimensional vector space over $\mathbb{F}_\ell$ with ℓ a rational prime. They naturally arise as the reduction mod ℓ of continuous 2-dimensional ℓ-adic Galois representations $\rho : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$ attached to algebraic varieties or automorphic forms. Indeed, due to the topological properties of $\mathscr{G}_K$ and $\mathrm{GL}_2(\mathbb{Q}_\ell)$ and the fact that ρ is continuous there exists always a (full) stable lattice of $\mathbb{Q}_\ell^2$ for ρ (this is true in more generality see Prop. 1.3.5). Thus, if we have more than one stable lattice the mod ℓ representation $\bar{\rho}$ depends on a choice of stable lattice (though the semisimplification of $\bar{\rho}$ and its irreducibility is

independent if the choice). Moreover, the knowledge of the mod ℓ representations is often the first approach in trying to answer the isomorphism question between ℓ-adic representations. Here, we extend the methods developed in [5, §3-§5] to study two dimensional Galois representations over $\mathbb{F}_3$, when they are presented as *black box*. To be specific, a Galois representation ρ is presented as a black box when we know the number field K, the finite set of prime S of K in which the representation is unramified, and the only information about $\bar{\rho}$ comes from the characteristic polynomials of $\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ for a finite number of chosen primes $\mathfrak{p}$ of K not in S. With the access to exactly this information, we are able to determine the following:

i) the determinant character of $\bar{\rho}$;

ii) whether $\bar{\rho}$ is irreducible;

iii) the image of $\bar{\rho}$ and the fixed field of $\ker(\bar{\rho})$ when $\bar{\rho}$ is irreducible;

iv) whether ρ has more than 2 stable non-homothetic lattices, when $\bar{\rho}$ is reducible;

v) whether two irreducible Galois representations with values in $\mathrm{GL}_2(\mathbb{F}_3)$ are equivalent.

Throughout the sections of Chapter 3 and Chapter 4 we present the methods that lead to these results. In Section 3.2 and Section 3.3 we design a test to determine the irreducibility of $\bar{\rho}$ by studying the attached projective representation, that is the representation obtained projecting $\bar{\rho}$ in $\mathrm{PGL}_2(\mathbb{F}_3)$. In Section 3.4 we develop a method to compute the image and the splitting field of an irreducible projective representation. This information together with that coming from the black box presentation leads to a criterion for determining the image and the splitting field of $\bar{\rho}$ when irreducible, as explained in explained in Section 3.5.

In Chapter 4 we focus our attention on reducible residual representations $\bar{\rho}$, seen as the projective reduction of 2-dimensional 3-adic Galois representations ρ. In these sections, we seek information about the stable sublattices of ρ. Indeed, we have at least two stable sublattices and we present an algorithm to check whether we have exactly two of them, in other terms (in the terminology of [5]) we are able to determine if the isogeny class of the representation has width two or more. In particular, when the width is two we can compute the splitting field of the projective representation $\tilde{\rho}$ associated to which lattice we are considering. It is important to remark that we are able to achieve each goal with the information coming from the characteristic polynomial of $\tilde{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ for primes $\mathfrak{p}$ in a suitable set T, usually referred as the test set, that depends only on K and S.

We can summarise the results of these two chapters in the following theorem:

Theorem. *Let K be a number field and S a finite set of primes of K. There exist finite sets of primes T_0, Σ_0, Σ_1, disjoint from S, that depends only on K and S, such that for any 2-dimensional $\mathbb{F}_3$-Galois representation $\bar{\rho}$ which is unramified outside S*

i) the irreducibility of $\bar{\rho}$ and its splitting field are completely determined by the value of the characteristic polynomials of $\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p} \in T_0$;

ii) if $\bar{\rho}$ is irreducible and $\bar{\rho}' : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ is another Galois representation unramified outside S then $\bar{\rho} \sim \bar{\rho}'$ if and only if the characteristic polynomials of $\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}}), \bar{\rho}'(\mathrm{Frob}_{\mathfrak{p}})$ agree for all $\mathfrak{p} \in \Sigma_0$;

iii) if $\rho : \mathscr{G}_K \to \mathrm{GL}_2(\mathbb{Q}_3)$ is such that $\bar{\rho}$ is reducible then we can determine whether there are exactly 2 stable sublattices of $\mathbb{Q}_3^2$ under the action of ρ by the value of the characteristic polynomials $\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p} \in \Sigma_1$.

Chapter 5 contains the proof of the following theorem[1]:

Theorem (Theorem 5.2.1)**.** *Let ρ_1, ρ_2 be two 3-adic Galois representations unramified outside a set of primes S of $\mathcal{O}_K$ satisfying*

i) $\det(\rho_1) = \det(\rho_2)$;

ii) $\rho_1(\sigma) \equiv \rho_2(\sigma) \bmod 3^k$, *for an integer $k \geq 1$ and for all $\sigma \in \mathscr{G}_K$;*

iii) the common $\bmod 3$ *representation $\bar{\rho}$ is irreducible.*

Let $\tilde{\rho} : \mathscr{G}_K \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ be the projective representation associated to $\bar{\rho}$, and let L be the fixed field of $\ker(\tilde{\rho})$. *Suppose that one of the following holds:*

a) the common projective representation $\tilde{\rho} : \mathscr{G}_K \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ is such that

$$\tilde{\rho}(\mathscr{G}_K) \in \left\{S_4, A_4, D_4, V_4^-, V_4^+\right\};$$

b $\tilde{\rho}(\mathscr{G}_K) \simeq C_4$ and K does not admit any Galois extension M unramified outside S and containing L such that $Gal(M/L) \simeq C_3^2$;

c) $\tilde{\rho}(\mathscr{G}_K) \simeq C_2^+$ and K does not admit any S_3 extension unramified outside S with L as quadratic sub-extension.

[1] For the notation of V_4^-, V_4^+, C_2^+ see § 3.1.

Then there exists a finite set of primes $\Sigma \subset MaxSpec(\mathcal{O}_K) \setminus S$*, that we call the* obstruction set of primes*, such that*

$$\rho_1 \sim \rho_2 \iff \mathrm{Tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_\mathfrak{p})) \qquad \forall \mathfrak{p} \in \Sigma.$$

The proof is subdivided into three main sections. Starting with the first three hypotheses of the theorem, in Section 5.1 we present how the obstruction to lifting the equivalence from modulo 3^k to modulo 3^{k+1} arises from Galois cohomology, and define a test function that allows us to identify the trivial cohomology class in a certain $H^1(\mathcal{G}_K, \cdot)$. As in the previous chapter, our test function computes traces of $\mathrm{Frob}_\mathfrak{p}$ for certain primes $\mathfrak{p}$ of K not in S. Moreover, this first part is presented for a generic rational prime ℓ. Since in the previous chapter we have developed a method to identify mod 3 representations, from section 5.2 on we restrict to the case $\ell = 3$. Here, we show how our test function can be used to prove that a certain cohomology class is trivial, and we prove also that we need to test only a finite number of primes $\mathfrak{p}$ of K. We call the set of such primes the obstruction set. In § 5.3.1 and § 5.3.2 we present two methods to compute the obstruction set one based on class field theory and one that we called the *sextic field method* just as the original Faltings-Serre method is sometimes called the method of *quartic fields*.

In Chapter 6 we present applications of our methods. One of them is to use the sextic field method to prove modularity of elliptic curves defined over imaginary quadratic fields of class number one. This was done proving isomorphisms between the Galois representations attached to such curves and the ones attached to weight two Bianchi cuspidal newforms with trivial Nebentypus. We start the chapter with a brief introduction on weight 2 Bianchi newforms and just recall the major results on the existence and property of the attached Galois representations. Then we give two highly detailed examples of how the sextic field method performs, and in section 6.1 we present tables of elliptic curves that we proved to be modular. We carried out the computation with our implementation of the algorithm in Sage [46]. The elliptic curves data and the values of the $a_\mathfrak{p}$ attached to Bianchi modular forms for primes $\mathfrak{p}$ with norm ≤ 100 come from the LMFDB page [32]. For primes with larger norm the $a_\mathfrak{p}$ were provided by Prof. John Cremona using his implementation of the modular symbols method [15], [17]. We summarise the result of our application in the following theorem

Theorem. *Let* E *be an elliptic curve defined over* $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$*, or* $\mathbb{Q}(\sqrt{-3})$*, with conductor norm less than* 1000 *and irreducible* mod 3

representation. Then E is modular modulo 3, and if the $\bmod 3$ *representation is absolutely irreducible than E is modular.*

Finally, in the last section, we discuss how our method is connected with the very recent results in modularity lifting due to Allen, Khare, and Thorne [2]. The implementation of their modularity lifting theorems together with the sextic fields method extends the result of the previous theorem for E defined over $\mathbb{Q}(\sqrt{-1})$

Theorem. *All the elliptic curves in the LMFDB database defined over* $\mathbb{Q}(\sqrt{-1})$ *with irreducible* $\bmod 3$ *representation are modular modulo 3. If the* $\bmod 3$ *representation is absolutely irreducible, they are modular.*

Chapter 1

Preliminaries

We recall some background material. In order to avoid too much detail we do not provide many proofs in the first section, the reader may refer to [23], [40], [41], [26, Chapter 2] and the first chapter of [12]. We do not claim any originality in the contents of this chapter.

1.1 Notation

Throughout this work we write:

- $\mathbb{Q}$ for the field of rational numbers.
- $\mathbb{Z}$ for the ring of integers.
- ℓ, p for primes in $\mathbb{Z}$.
- $\mathbb{Q}_\ell$ for the completion of $\mathbb{Q}$ with respect to the ℓ-adic norm.
- $\mathbb{Z}_\ell$ for the ring of ℓ-adic integers.
- $\mathbb{F}_q$ for the finite field with q elements.
- K for a *number field*.
- $\mathcal{O}_K$ for *the ring of integers* of K.
- $\mathrm{MaxSpec}(\mathcal{O}_K)$ for the set of nonzero prime ideals of the ring $\mathcal{O}_K$.
- S for a *finite* subset of $\mathrm{MaxSpec}(\mathcal{O}_K)$.
- $\mathfrak{p}$ for a prime ideal of $\mathcal{O}_K$, we may refer to it as a *prime of* K.

- $K(S,p)$ for the *p-Selmer group* of the number field K, whose definition is $K(S,p) := \{\alpha \in K^\times/(K^p)^\times \mid \mathrm{ord}_\mathfrak{p}(\alpha) \equiv 0 \pmod p,\ \forall\, \mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S\}$.
- $\overline{K}$ for a chosen algebraic closure of K.
- $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ for the *absolute Galois group* of K.
- GL_n for the general linear group of dimension n.
- PGL_n for the projective linear group of dimension n.
- ρ for a Galois representation of $\mathscr{G}_K$ with values in $\mathrm{GL}_n(\mathbb{Q}_\ell)$ or $\mathrm{GL}_n(\mathbb{Z}_\ell)$. In the latter case we may refer to ρ as *integral Galois representation.*
- $\bar\rho$ for a Galois representation of $\mathscr{G}_K$ with values in $\mathrm{GL}_n(\mathbb{F}_\ell)$. We may refer to $\bar\rho$ as the *residual* or mod ℓ *representation.*
- $\tilde\rho$ for a Galois representation of $\mathscr{G}_K$ with values in $\mathrm{PGL}_n(\mathbb{F}_\ell)$. We may refer to $\tilde\rho$ as *projective representation.*

1.2 Group Representations

Let G be a group, F a field, V a finite dimensional F-vector space endowed with a linear action of G, i.e. there exists a group homomorphism $\rho : G \longrightarrow \mathrm{GL}(V)$.

Definition 1.2.1. We call the pair (V,ρ) an *F-linear representation* of G.

If F and V are well understood we will use ρ to identify the representation (V,ρ). If W is a vector sub-space of V invariant under the action of G, explicitly

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

we call the restriction $\rho_{|_W}$ a *sub-representation* of ρ. In particular, we say that ρ is *irreducible* if does not admit any nontrivial sub-representation, and we call ρ *semi-simple* if can be written as a direct sum of irreducible sub-representations. Now, let (V,ρ) be a representation and $\overline{F}$ an algebraic closure of F. Then we can consider the representation $(V \otimes_F \overline{F}, \rho)$ via $\rho : G \to \mathrm{GL}(V) \hookrightarrow \mathrm{GL}(V) \otimes_F \overline{F}$. We say that (V,ρ) is *absolutely irreducible* if $(V \otimes_F \overline{F}, \rho)$ is irreducible.

Definition 1.2.2. Consider two representations $(V_1,\rho_1), (V_2,\rho_2)$. A *homomorphism of representations* is an F-linear map $f : V_1 \longrightarrow V_2$ such that

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

If f is invertible we say that ρ_1 is isomorphic to ρ_2, in symbols $\rho_1 \simeq \rho_2$.

Every representation ρ admits a *Jordan-Hölder composition series*, that is a decreasing filtration

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n = 0$$

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 $\mathrm{JH}(\rho)$ 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 $\mathrm{JH}(\rho)$ does not depend on the choice of a Jordan-Hölder composition series for ρ. Therefore we can define an equivalence relation on the set of representations.

Definition 1.2.3. Let ρ_1, ρ_2 be two representations of a group G. We say they are equivalent, and write $\rho_1 \sim \rho_2$, if $\mathrm{JH}(\rho_1) = \mathrm{JH}(\rho_2)$.

In the next theorem, we present the relation between isomorphic representations and equivalent representations.

Theorem 1.2.4. *Let ρ_1 and ρ_2 be F-linear representations of a group G. Then*

i) If $\rho_1 \simeq \rho_2$ then $\rho_1 \sim \rho_2$.

ii) If ρ_1, ρ_2 are semisimple, then $\rho_1 \simeq \rho_2$ if and only if $\rho_1 \sim \rho_2$, i.e. a semisimple representation is determined up to isomorphism by the multiplicities of its simple constituents.

iii) For every representation ρ, there exists a unique (up to isomorphism) semisimple representation ρ^{ss} such that $\rho \sim \rho^{ss}$. Explicitly, if

$$JH(\rho) = \{(W_1, m_1), \ldots, (W_n, m_n)\}$$

then ρ^{ss} is given by the action of G on $W_1^{m_1} \oplus \cdots \oplus W_n^{m_n}$

The isomorphism class of the semisimple representation ρ^{ss} is called the *semisimplification* of ρ. We deduce from (ii) and (iii) above that

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

Every element $g \in G$ is mapped by ρ to a linear map $\rho(g) \in \mathrm{GL}(V)$ and we can compute the trace $\mathrm{tr}(\rho(g)) \in F$. We define $\mathrm{tr}\rho$ to be the following composition

$$\mathrm{tr}\rho : G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{\mathrm{tr}} F$$

The Brauer-Nesbitt theorem [26, Corollary 2.8, p. 38] shows that traces determine whether two representations are equivalent.

Theorem 1.2.5 (Brauer-Nesbitt)**.** *Let ρ_1 and ρ_2 be two F-linear representations of a group G, and assume that one of them is absolutely irreducible. Then*

$$\rho_1 \sim \rho_2 \Longleftrightarrow \mathrm{tr}\rho_1 = \mathrm{tr}\rho_2.$$

Now, the trace map does not distinguish a representation from its semisimplification since it is additive on short exact sequences whether they are split or not. Under the assumption of the theorem, we deduce that

$$\rho_1 \sim \rho_2 \Longleftrightarrow \rho_1^{ss} \simeq \rho_2^{ss} \Longleftrightarrow \mathrm{tr}\rho_1 = \mathrm{tr}\rho_2.$$

We end this section noting that G, F and V may be endowed with a topology compatible with their algebraic structures. Therefore, we may require that the group homomorphism $\rho : G \longrightarrow \mathrm{GL}(V)$ be continuous with respect to these topologies. Indeed we could always equip everything with the discrete topology if needed. For this reason, we will assume that all the representations in this thesis are continuous. Also, if we choose a basis of V over F then we have the isomorphism $\mathrm{GL}(V) \simeq \mathrm{GL}_n(F)$, where $n = \dim_F(V)$. In particular, ρ determines a matrix representation $G \longrightarrow \mathrm{GL}_n(F)$, well defined up to conjugation within $\mathrm{GL}_n(F)$.

1.3 Galois Representations

Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. For a fixed algebraic closure $\overline{K}$ of K, the group $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ is called the *absolute Galois group* of K. In particular, we have the following identification

$$\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K) = \varprojlim_{L/K} \mathrm{Gal}(L/K)$$

where L runs over all finite Galois subextensions of $\overline{K}/K$. Hence, $\mathscr{G}_K$ is a profinite group, so it is a topological group where the topology is the *Krull topology*. With respect to this topology, $\mathscr{G}_K$ is Hausdorff, compact and totally disconnected.

Let L/K be a finite Galois extension, and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal. Then from general theory (ref. [33]) we know $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_k^e$, i.e. the ideal generated by $\mathfrak{p}$ in $\mathcal{O}_L$ can be expressed uniquely as a product of prime ideals $\mathfrak{P}_i \subset \mathcal{O}_L$. Moreover, if we fix $\mathfrak{p}$ then the Galois group acts transitively on the $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$. The stabilizer of a such ideal is called the *decomposition group* at $\mathfrak{P}/\mathfrak{p}$, i.e.

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

Now, the ring of integers of a number field is a *Dedekind domain*, so each nonzero prime ideal is also maximal. Therefore, the quotient $\mathcal{O}_K/\mathfrak{p}$ is actually a field, which we will denote $k_\mathfrak{p}$. Moreover, let $p \in \mathbb{Z}$ a prime such that $p\mathcal{O}_K \subset \mathfrak{p}$, then $k_\mathfrak{p}$ is a finite field with $|k_\mathfrak{p}| = p^f$ for some positive integer f. Let $k_\mathfrak{P}$ be the field $\mathcal{O}_L/\mathfrak{P}$. Then we have a short exact sequence

$$1 \longrightarrow I(\mathfrak{P}/\mathfrak{p}) \longrightarrow D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p}) \longrightarrow 1,$$

which defines the *inertia group* $I(\mathfrak{P}/\mathfrak{p})$ as

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

Now, $\mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})$ is the Galois group of an extension of finite fields; hence it is generated by the automorphism

$$x \mapsto x^{|k_\mathfrak{p}|},$$

denoted by $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$, and called *Frobenius automorphism*. Hence, if $I(\mathfrak{P}/\mathfrak{p}) = 1$ then we may think of $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ as an element of $\mathrm{Gal}(L/K)$ which generates $D(\mathfrak{P}/\mathfrak{p})$. A natural question is how the decomposition group and the inertia group change when we change the prime above $\mathfrak{p}$. Given one prime $\mathfrak{P}$ we get all the primes above $\mathfrak{p}$ just acting by the Galois group of L/K. In particular, we have the following relations

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

In particular, we say that the extension L/K is *unramified* at $\mathfrak{p}$ if the inertia subgroup is trivial, and in this case we obtain:

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

We denote by $\mathrm{Frob}_\mathfrak{p}$ the conjugacy class in $\mathrm{Gal}(L/K)$ of the Frobenius,

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

Theorem 1.3.1 (Weak Chebotarev)**.** *[41, Corollary 2, p.I-8]. Let L/K be a not necessarily finite Galois extension unramified outside the finite set S of primes of $\mathcal{O}_K$. Then, the union of the Frobenius conjugacy classes of the primes $\mathfrak{p} \notin S$ is*

dense in $\mathrm{Gal}(L/K)$.

We can now state the definition and some basic properties of a Galois representation.

Definition 1.3.2. Let L/K be a Galois extension with Galois group $\mathscr{G} = \mathrm{Gal}(L/K)$. Let F be a topological field and V a finite dimensional F-vector space endowed with the product topology. We call an *F-linear Galois representation* (or simply *Galois representation* when F is understood) a pair (V, ρ) with

$$\rho : \mathscr{G} \longrightarrow \mathrm{GL}(V)$$

a continuous group homomorphism (with respect to the Krull topology on $\mathscr{G}$).

Let ℓ be a rational prime and consider $F = \mathbb{Q}_\ell$, the completion of $\mathbb{Q}$ with respect to the ℓ-adic topology.

Definition 1.3.3. Let V a finite dimensional $\mathbb{Q}_\ell$-vector space endowed with a continuous linear action ρ of $\mathrm{Gal}(L/K)$. We call the couple (V, ρ) an *ℓ-adic representation* of the Galois group $\mathrm{Gal}(L/K)$.

As in the previous section, when V, F are clear, we refer to the representation as ρ.

Definition 1.3.4. Let V be a finite dimensional $\mathbb{Q}_\ell$-vector space. Then a $\mathbb{Z}_\ell$-lattice Λ in V is a $\mathbb{Z}_\ell$-submodule of V spanned by $\mathbb{Q}_\ell$ linearly independent vectors. If the vectors are a basis of V over $\mathbb{Q}_\ell$ then we call Λ a *full* $\mathbb{Z}_\ell$-lattice.

Since any Galois group $\mathrm{Gal}(L/K)$ is compact with respect to the Krull topology, and since we are considering continuous representations, we have the following crucial proposition.

Proposition 1.3.5. *Let (V, ρ) be an ℓ-adic Galois representation of a Galois group $\mathscr{G}$. Then, ρ stabilizes a full $\mathbb{Z}_\ell$-lattice of V.*

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

Corollary 1.3.6. *If we choose a basis of V over $\mathbb{Q}_\ell$ which is a $\mathbb{Z}_\ell$-basis of a full lattice Λ under ρ, we have $\rho : G \longrightarrow \mathrm{GL}_n(\mathbb{Z}_\ell)$ (not only $\mathrm{GL}_n(\mathbb{Q}_\ell)$).*

Remark 1.3.7. If we take any local field F, with λ the maximal ideal of $\mathcal{O}_F$, then a F-valued representation is called λ-adic. Moreover, for any such representation, we have the same result as in the proposition. This is because $\mathscr{G}$ is compact and ρ is continuous, hence $\rho(\mathscr{G})$ is contained in a maximal compact subgroup of $\mathrm{GL}_n(F)$ (after fixing a basis for V over F). Since any such maximal subgroup is conjugate to $\mathrm{GL}_n(\mathcal{O}_F)$ we are done. This means we can always regard any λ-adic representation as an $\mathcal{O}_F$-valued matrix representation. Furthermore, if two representations are conjugate over $\mathcal{O}_F$ then they are conjugate modulo λ^α for all α. However, if ρ_1 and ρ_2 are conjugate over F, it does not imply that they are conjugate over $\mathcal{O}_F$. Indeed, let C_2 be the cyclic group of order 2, and $F = \mathbb{Q}_2$. Consider the following representations

$$\begin{aligned} \rho_1 : C_2 &\longrightarrow \mathrm{GL}_2(\mathbb{Q}_2) \\ \sigma &\mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \rho_2 : C_2 &\longrightarrow \mathrm{GL}_2(\mathbb{Q}_2) \\ \sigma &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Since the characteristic polynomials of σ are the same, the representations ρ_1, ρ_2 are conjugate over K. However, if ρ_1, ρ_2 were conjugate over $\mathcal{O}_K = \mathbb{Z}_2$, then they would be conjugate mod 2, i.e. over $\mathbb{F}_2$. But, this is impossible since $\bar{\rho}_2(\sigma) = \mathrm{Id} \neq \bar{\rho}_1(\sigma)$.

Definition 1.3.8. Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K and $I_\mathfrak{p}$ the inertia subgroup of $\mathfrak{p}$ up to conjugacy. We say that a representation ρ is unramified at $\mathfrak{p}$ if $\rho(I_\mathfrak{p}) = 1$.

Let L/K be a Galois extension of number fields. Let S be a finite set of primes of K, and let I_S be the closed normal subgroup of $\mathrm{Gal}(L/K)$ generated by all the inertia subgroups $I(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{p} \notin S$. Consider the quotient

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

by the Galois correspondence there exists a field L_S such that $K \subset L_S \subset L$ and

$\mathrm{Gal}(L/L_S) = I_S$. In particular, L_S is the maximal intermediate extension which is unramified outside S. In general, for any topological group H, the continuous homomorphisms $\rho : \mathrm{Gal}(L/K) \longrightarrow H$ that are unramified outside S are exactly those factor through $\mathrm{Gal}(L_S/K)$.

Proposition 1.3.9. *Let ρ_1, ρ_2 be two F-linear Galois representations of $\mathrm{Gal}(L/K)$ unramified outside S. Assume that at least one of the representation is absolutely irreducible. Then*

$$\rho_1 \sim \rho_2 \Longleftrightarrow \mathrm{tr}\rho_1(\mathrm{Frob}_\mathfrak{p}) = \mathrm{tr}\rho_2(\mathrm{Frob}_\mathfrak{p}) \text{ for all } \mathfrak{p} \notin S.$$

Proof. By the previous section, we know that the equivalence class of an absolutely irreducible continuous representation $\rho : \mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}(V)$ unramified outside S is determined by its trace. In particular, we may view the trace map as a continuous function on $\mathrm{Gal}(L_S/K)$, which therefore is itself determined by its restriction to a dense subset. □

1.4 The n-Selmer Group of a Number Field

Let K be a number field and S a finite set of primes of K. It will be important later to use the following group:

Definition 1.4.1. Let $n \geq 2$ be an integer. We define the *n-Selmer group* of the number field K at S as

$$K(S,n) := \left\{\alpha \in K^\times/(K^n)^\times \mid \mathrm{ord}_\mathfrak{p}(\alpha) \equiv 0 \bmod n,\ \forall\, \mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S\right\}.$$

An important result is:

Proposition 1.4.2. *$K(S,n)$ is a finite group.*

Proof. Consider the *ring of the S-integers* of K

$$\mathcal{O}_{K,S} = \{\alpha \in K \mid \mathrm{ord}_\mathfrak{p}(\alpha) \geq 0,\ \forall\, \mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S\}.$$

Since the class number of K is finite, we can add a finite number of elements to S so that $\mathcal{O}_{K,S}$ is a principal ideal domain.
We have a natural map

$$f : \mathcal{O}_{K,S}^\times \longrightarrow K(S,n)$$

and we claim it is surjective. To see this, let $a \in K^\times$ be a representative of an element of $K(S,n)$. Since the prime ideals of $\mathcal{O}_{K,S}$ are $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$, then

the ideal $a\mathcal{O}_{K,S}$ is the n-th power of an ideal of $\mathcal{O}_{K,S}$. Furthermore, we assumed $\mathcal{O}_{K,S}$ is a PID, therefore there is a $b \in K^\times$ such that $a\mathcal{O}_{K,S} = b^n\mathcal{O}_{K,S}$. Thus, there exists a $u \in \mathcal{O}_{K,S}^\times$ such that $a = ub^n$. Since a and u represents the same class in $K(S,n)$ then $\mathcal{O}_{K,S}^\times$ surjects onto $K(S,n)$.
Finally, the Dirichlet's S-unit theorem [29, Chapter V, § 1] assert that $\mathcal{O}_{K,S}^\times$ is finitely generated, hence $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n$ is finite. Since $(\mathcal{O}_{K,S}^\times)^n \subseteq \ker(f)$ (it is actually an equality), then $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n$ surjects onto $K(S,n)$. Therefore $K(S,n)$ is finite. □

If we assume that our number field K contains the n-th roots of unity ζ_n there is an important connection between abelian extensions of K of exponent n unramified outside S and the elements of $K(S,n)$.

Proposition 1.4.3. *The maximal abelian extension L/K of exponent n unramified outside S is finite and is of the form*

$$L = \prod_{\alpha \in G} K(\sqrt[n]{\alpha})$$

for a set of representatives $G \subset K^\times$ of a suitable subgroup of $K(S,n)$.

Proof. By the main theorem of Kummer theory [11, Chapter III, § 2] we know that the maximal abelian extension K'/K of exponent n is given by adjoining the nth roots of elements of K, i.e. $K' = \prod_{\alpha \in K^\times/(K^n)^\times} K(\sqrt[n]{\alpha})$. Consider $S' = S \cup \{\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S \mid \mathrm{ord}_\mathfrak{p}(n) > 0\}$, then $K(S',n) \subseteq K(S,n)$ is a subgroup and finite by the previous proposition. Now, for each $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)\setminus S'$ the extension of local fields $K_\mathfrak{p}(\sqrt[n]{\alpha})/K_\mathfrak{p}$ is unramified if and only if

$$\mathrm{ord}_\mathfrak{p}(\alpha) \equiv 0 \mod n.$$

Therefore, the compositum of all $K(\sqrt[n]{\alpha})$'s where each α represents a different class of $K(S',n)$, is the maximal subextension of K' unramified outside S. Hence, $L = \prod_{\alpha \in G} K(\sqrt[n]{\alpha})$ with G a set of representatives of $K(S',n)$, and since the latter is finite L is finite. □

Remark 1.4.4. If we drop the assumption $\zeta_n \in K$, the finiteness part of the previous statement still holds, since the proposition holds for $K(\zeta_n)$ and $K(\zeta_n)/K$ is finite. On the other hand, to identify the structure of L and the equivalent finite set of elements $\alpha_i \in K^\times$ such that $L = K(\alpha_1, \ldots, \alpha_n)$ we need *class field theory.*

By the previous proposition and the Shafarevich's theorem [37, Theorem 9.5.1, p. 476] we have the following

Theorem 1.4.5. *Let K be a number field. Given a finite solvable group G, there exist only finitely many Galois extensions F/K unramified outside S such that $Gal(F/K) \simeq G$.*

Chapter 2

One dimensional ℓ-adic Galois Representation

Let K be a number field, $\mathcal{O}_K$ its ring of integers, S a finite set of primes of K, and ℓ a rational prime. In view of [13], Prop. 3.3.22, we can construct a modulus $\mathfrak{m}_S$, which is a product of primes $\mathfrak{p}$ in S with exponent at most 1 unless $\mathfrak{p}$ lies above ℓ, such that the *ray class field* $K(\mathfrak{m}_S)$ associated to $\mathfrak{m}_S$ contains all the abelian extensions of K of exponent ℓ unramified outside S. Let L be the composite of all such extensions, then

$$G = \mathrm{Gal}(L/K) \simeq Cl(\mathfrak{m}_S)/Cl(\mathfrak{m}_S)^\ell$$

where $Cl(\mathfrak{m}_S)$ is the *ray class group* attached to $\mathfrak{m}_S$, and the (reverse) isomorphism is given by the Artin map. Since $Cl(\mathfrak{m}_S)$ is a finite abelian group, we can consider $V = Cl(\mathfrak{m}_S)/Cl(\mathfrak{m}_S)^\ell$, hence also G, as a finite dimensional $\mathbb{F}_\ell$-vector space. Therefore, we can fix a basis $\mathcal{B}^V_{\mathbb{F}_\ell} := \{[\mathfrak{p}_i]\}_{i=1}^t$ for some $\mathfrak{p}_i \in \mathrm{MaxSpec}\mathcal{O}_K \setminus S$.
The following definition generalises Def. 3.1 of [5], which is the case $\ell = 2$.

Definition 2.0.1. Let ℓ be a rational prime. A set $T_\ell(S)$ of primes $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)\setminus S$ is called an *ℓ-basis*, if the set $\{[\mathfrak{p}] \mid \mathfrak{p} \in T_\ell(S)\}$ forms a basis for the vector space $V = Cl(\mathfrak{m}_S)/Cl(\mathfrak{m}_S)^\ell$ over $\mathbb{F}_\ell$.

Remark 2.0.2. By the isomorphism given by the Artin map we have that for any ℓ-basis $T_\ell(S)$, the set $\{\,\mathrm{Frob}_\mathfrak{p} \in G \mid \mathfrak{p} \in T_\ell(S)\}$ is a basis for G over $\mathbb{F}_\ell$. The dual basis $\{\chi_i\}_{i=1}^t$ is formed of additive characters $\chi_i : \mathscr{G}_K \longrightarrow \mathbb{F}_\ell$ whose restriction to $\mathscr{G}_L$, the absolute Galois group of L, is trivial. This implies that every additive character

$\chi : \mathscr{G}_K \longrightarrow \mathbb{F}_\ell$ unramified outside S can be uniquely written as

$$\chi = \sum_{i=1}^{t} x_i \chi_i,$$

with $x_1, \ldots, x_t \in \mathbb{F}_\ell$.

The following lemma is crucial.

Lemma 2.0.3. *Let $\ell \in \mathbb{Q}$ be a prime, and $T_\ell(S)$ an ℓ-basis for K. Let $\chi : \mathscr{G}_K \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$ be an additive character unramified outside S, such that $\chi(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_\ell(S)$. Then $\chi = 0$.*

Proof. We prove this by induction on n. For $n = 1$ it is true by definition of $T_\ell(S)$. Let assume it is true for $n-1$. Since $\mathbb{Z}/\ell^n\mathbb{Z}$ as an additive group is cyclic we have the projection homomorphism onto the quotient

$$\pi : \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow \mathbb{Z}/\ell\mathbb{Z}.$$

When we consider $\bar{\chi} = \chi \circ \pi$ we have an additive character from $\bar{\chi} : \mathscr{G}_K \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$ that satisfies $\bar{\chi}(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_\ell(S)$ hence is trivial by definition of $T_\ell(S)$ and the remark. Thus $\mathrm{Im}(\chi) \subseteq \ker(\pi) \simeq \mathbb{Z}/\ell^{n-1}\mathbb{Z}$, that is we can actually consider $\chi : \mathscr{G}_K \longrightarrow \mathbb{Z}/\ell^{n-1}\mathbb{Z}$ and by inductive hypothesis we conclude since $\chi(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_\ell(S)$. □

Proposition 2.0.4. *Let $\chi : \mathscr{G}_K \longrightarrow \mathbb{Z}_\ell^\times$ be a continuous ℓ-adic character unramified outside S. Assume for $k \geq 1$ that*

i) $\chi(\sigma) \equiv 1 \pmod{\ell^k}$ *for all* $\sigma \in \mathscr{G}_K$*;*

ii) $\chi(\mathrm{Frob}_\mathfrak{p}) \equiv 1 \pmod{\ell^{k+1}}$ *for all* $\mathfrak{p} \in T_\ell(S)$.

Then $\chi(\sigma) \equiv 1 \pmod{\ell^{k+1}}$ *for all* $\sigma \in \mathscr{G}_K$

Proof. Assume that there exists $\sigma \in \mathscr{G}_K$ such that $\chi(\sigma) \not\equiv 1 \pmod{\ell^{k+1}}$. Then we have

$$\chi(\sigma) = 1 + \ell^k \alpha(\sigma)$$

with $\alpha(\sigma) \in \mathbb{Z}_\ell$. However, $\alpha(\cdot) \pmod{\ell}$ is an additive character which is trivial on $T_\ell(S)$. Therefore, by the lemma it is the trivial character, which implies $\chi(\sigma) \equiv 1 \pmod{\ell^{k+1}}$ for all $\sigma \in \mathscr{G}_K$. □

The next theorem extends to a generic finite extension $L/\mathbb{Q}_\ell$ for an odd rational prime ℓ the results for $\ell = 2$ and $L = \mathbb{Q}_2$ in [5, § 3].

Theorem 2.0.5. *Let $\ell \in \mathbb{Q}$ be a prime, let $L/\mathbb{Q}_\ell$ be a finite extension field of degree d with ring of integers $\mathcal{O}_L$ and residue field $\mathbb{F}_q$, where $q = \ell^f$ for some positive integer f. Let $p_1, \ldots, p_h$ be the primes dividing $q-1$, and set*

$$T(S) = T_{q-1}(S) \cup T_\ell(S) := \bigcup_{i=1}^{h} T_{p_i}(S) \cup T_\ell(S).$$

Let $\chi : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$ be a continuous character unramified outside S that satisfies $\chi(\mathrm{Frob}_\mathfrak{p}) = 1$ for all $\mathfrak{p} \in T(S)$. Then χ is trivial.

Proof. The structure theorem of $\mathcal{O}_L$ [36][Prop. 5.7, pag. 140] provides the following isomorphism (both topologically and algebraically)

$$\mathcal{O}_L^\times \simeq \frac{\mathbb{Z}}{(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{\ell^a\mathbb{Z}} \oplus \mathbb{Z}_\ell^d$$

where the right hand side is endowed with the additive structure. Therefore, we have the induced additive homomorphism

$$\begin{aligned} \chi_{\mathrm{add}} : \mathscr{G}_K &\longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/\ell^a\mathbb{Z} \oplus \mathbb{Z}_\ell^d \\ \sigma &\mapsto \chi_{\mathrm{add}}(\sigma) = (\chi_{q-1}(\sigma), \chi_{\ell^a}(\sigma), \chi_1(\sigma), \ldots, \chi_d(\sigma)) \end{aligned}$$

where each component of χ_{add} is an additive character.
Let $\mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{F}_q^\times \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_h\mathbb{Z}$ be the primary decomposition of the cyclic group $\mathbb{F}_q^\times$, where q_i is a power of a prime p_i for all i. Hence we have

$$\chi_{q-1} = \left(\chi_{p_1^{t_1}}, \ldots, \chi_{p_h^{t_h}}\right)$$

where $\chi_{p_i^{t_i}}$ is an additive character for all $i = 1, \ldots, h$. By our assumption, we have that $\chi_{p_i^{t_i}}(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T(S)$ and for all i. In particular, $\chi_{p_i^{t_i}}(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_{p_i}(S)$ and by Lemma 2.0.3 we have $\chi_{p_i^{t_i}} = 0$. Hence χ_{q-1} is the trivial character. With the same exact argument we can conclude that χ_{ℓ^a} is also trivial.

Now consider the additive characters $(\chi_1, \ldots, \chi_d)$. For each χ_j and each positive integer $k \geq 1$ we have the mod ℓ^k additive character $\bar{\chi}_{j,k} : \mathscr{G}_K \longrightarrow \mathbb{Z}_\ell/\ell^k\mathbb{Z}_\ell \simeq \mathbb{Z}/\ell^k\mathbb{Z}$. Since by hypothesis we have that $\bar{\chi}_{j,k}(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_\ell(S)$, by Lemma 2.0.3 we have that $\bar{\chi}_{j,k}$ for all j and all $k \geq 1$. This means that each χ_j is trivial and therefore χ_{add} is trivial since all its components are. We have then that $\chi : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$ is trivial as wanted. □

Corollary 2.0.6. *Let $\chi_1, \chi_2 : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$ be two continuous characters unramified outside S such that $\chi_1(\mathrm{Frob}_\mathfrak{p}) = \chi_2(\mathrm{Frob}_\mathfrak{p})$ for all $\mathfrak{p} \in T(S)$, where $T(S)$ is defined as in Theorem 2.0.5. Then $\chi_1 = \chi_2$.*

Proof. It is enough to apply the previous theorem to the character

$$\chi = \chi_1 \chi_2^{-1} : \mathscr{G}_K \longrightarrow \mathcal{O}_L^\times$$

to get $\chi = 1$ and therefore $\chi_1 = \chi_2$. □

Remark 2.0.7. With Corollary 2.0.6 we have the first step in establishing whether two given ℓ-adic Galois representations ρ_1, ρ_2 unramified outside the same set S and with computable traces and determinants are equal. Indeed, we can apply it to determine whether $\det(\rho_1) = \det(\rho_2)$. Moreover, we can use it to recognise a given continuous ℓ-adic character χ unramified outside S, for example, if it is a power of the cyclotomic character. It is important to note that we can only determine whether χ is equal to some candidate character (for example a power of a cyclotomic character).

Chapter 3

Irreducible 2-Dimensional $\mathbb{F}_3$-Galois Representations

Let K be a number field with ring of integers $\mathcal{O}_K$ and $S \subset \mathrm{MaxSpec}(\mathcal{O}_K)$ a finite set of primes of K. Let $\mathscr{G}_K$ be the absolute Galois group of K, and V a 2-dimensional $\mathbb{F}_3$-vector space on which $\mathscr{G}_K$ acts. If we fix a basis of V over $\mathbb{F}_3$ we can consider the Galois representation $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3) \simeq \mathrm{GL}(V)$. We can take the quotient $\mathrm{GL}_2(\mathbb{F}_3)/\mathbb{F}_3^\times = \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$, and composing with the projection $\pi : \mathrm{GL}_2(\mathbb{F}_3) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ we obtain the *projective representation* $\tilde{\rho} = \pi \circ \bar{\rho}$

$$\mathscr{G}_K \xrightarrow{\bar{\rho}} \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\pi} \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4.$$

The aim of this chapter is to recover information on $\bar{\rho}$ and $\tilde{\rho}$, assuming that the only information we have concerning $\bar{\rho}$ is

i) that $\bar{\rho}$ is unramified outside S;

ii) the characteristic polynomial of $\bar{\rho}(\mathrm{Frob}_\mathfrak{p})$ for a finite set of primes $\mathfrak{p} \notin S$.

We may refer to this way of presenting a representation as a *black box* representation.

3.1 Subgroups of S_4

Firstly, we want to study the irreducibility of $\bar{\rho}$ and its possible image. We first to define what it means for $\tilde{\rho}$ to be irreducible.

Definition 3.1.1. The projective representation $\tilde{\rho}$ is *reducible* if $\tilde{\rho}(\mathscr{G}_K)$ is contained in a *Borel subgroup* of $\mathrm{PGL}_2(\mathbb{F}_3)$. Otherwise the representation is called *irreducible*.

Remark 3.1.2. Note that with a suitable choice of basis of V over $\mathbb{F}_3$ then the previous definition is equivalent to saying that $\tilde{\rho}$ is *reducible* if $\bar{\rho}(\mathscr{G}_K)$ is contained in the subgroup of upper triangular matrices of $\mathrm{GL}_2(\mathbb{F}_3)$.

The next proposition follows directly from the definition.

Proposition 3.1.3. *The representation $\bar{\rho}$ is irreducible if and only if $\tilde{\rho}$ is irreducible.*

In view of the isomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ we may view the projective representation as a permutation representation on the four points of $\mathbb{P}^1(\mathbb{F}_3)$. By the previous proposition we can say that $\tilde{\rho}$ is irreducible if no point is fixed by the action of $\tilde{\rho}(\mathscr{G}_K)$. For each $g \in \mathscr{G}_K$ we have $\det(\bar{\rho}(g)) = \pm 1$ and $\mathrm{tr}(\bar{\rho}(g)) = 0$ or ± 1. Unfortunately, using only the information given by the trace and the determinant of $\bar{\rho}(g) \in \mathrm{GL}_2(\mathbb{F}_3)$ we cannot distinguish the identity matrix and the matrices of order 3 since they have the same characteristic polynomial $(x-1)^2$. However, this will not be a problem. The information about elements of $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ is shown in the table below.

det	tr	characteristic polynomial	cycle structure
1	0	x^2+1	2^2
1	± 1	$x^2 \mp x + 1 = (x \pm 1)^2$	1^4 or $1 \cdot 3$
-1	0	$x^2 - 1 = (x+1)(x-1)$	$1^2 \cdot 2$
-1	± 1	$x^2 \pm x - 1$	4

Table 3.1: Relation between the pairing of traces and determinant of elements of $\mathrm{GL}_2(\mathbb{F}_3)$ and elements of $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$.

Now, the 4-cycles and the products of two disjoint transpositions do not fix any points. The conjugacy classes of subgroups of S_4 that contain at least one of these elements are the *transitive* ones together with two other subgroups that we call V_4^- and C_2^+:

i) the normal subgroup $A_4 = \langle (1,2,3), (1,2)(3,4) \rangle$

ii) the normal subgroup $V_4^+ = \langle (1,2)(3,4), (1,4)(2,3) \rangle$:

iii) V_4^-, they are all conjugate to $\langle (1,2), (3,4) \rangle$

iv) D_4, a representatives of the class is $\langle (1,2,3,4), (1,3) \rangle$;

v) C_4, they are all conjugate to $\langle (1,2,3,4) \rangle$;

vi) $S_4 = \langle (1,2,3,4), (1,2) \rangle$;

vii) C_2^+, a representative is $\langle (1,2)(3,4) \rangle$.

Here, for subgroups $H \subset S_4$ isomorphic to C_2 or V_4 as abstract groups, there are two conjugacy classes. One is contained in A_4 and one not. We denote these with a superscript $+$ or $-$ respectively.
Therefore we see that

Proposition 3.1.4. *The linear representation $\bar{\rho}$ is irreducible if and only if the image of $\tilde{\rho}$ in S_4 is $S_4, A_4, V_4^{\pm}, D_4, C_4$, or C_2^+. Moreover, $\bar{\rho}$ is absolutely irreducible if and only if $\tilde{\rho}(\mathscr{G}_K) \in \{S_4, A_4, V_4^{\pm}, D_4\}$.*

Proof. The first statement follows from the easy computation of how each subgroup of S_4 acts on the 4 points of $\mathbb{P}^1(\mathbb{F}_3)$. The second one is a straightforward application of [19, Theorem 3.43, p. 54].

□

3.2 Irreducible projective representations and their splitting fields

Let $\tilde{\rho}$ be an irreducible projective representation taking values in $\mathrm{PGL}_2(\mathbb{F}_3)$, then in Proposition 3.1.4 we have established the possible image of $\tilde{\rho}$ in S_4, under the isomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$. The aim of this section is to show that the fixed field of $\ker(\tilde{\rho})$ is the splitting field of a suitable degree 4 polynomial with coefficients in the number field K.

Now, S_4, and hence its subgroups, is a solvable group, hence by Theorem 1.4.5 we have finitely many non-isomorphic Galois extensions of K unramified outside S with Galois group isomorphic to S_4 or any of the subgroups listed in Proposition 3.1.4. Let $\mathcal{A} = \{E_1, \ldots, E_t\}$ be the set of such extensions. Since each $E \in \mathcal{A}$ is the splitting field of infinitely many polynomials $f(x) \in K[x]$, we fix, for each $E \in \mathcal{A}$, a polynomial $f_E(x) \in \mathcal{O}_K[x]$ such that

i) $f_E(x)$ is monic;

ii) $\deg(f_E) = 4$;

iii) E is the splitting field of $f_E(x)$;

iv) f_E is irreducible unless $[E : K] = 2$, when we require f to have no roots in K.

We denote by $\mathcal{F}$ the set of these polynomials. Moreover, let $\mathcal{G}(f)$ be the Galois group of $f \in \mathcal{F}$ represented as a permutation group in S_4 on the roots of f. Then $\mathcal{G}(f) \in \left\{S_4, A_4, D_4, V_4^+, C_4, C_2^+\right\}$.

Consider an extension E/K such that $\mathrm{Gal}(E/K) = C_2$, hence $E = K(\sqrt{\alpha})$ for some $\alpha \in K^\times/(K^\times)^2$. In order to see C_2 inside S_4 we choose to represent E as the splitting field of the polynomial

$$f(x) = (x^2 - \alpha)(x^2 - 4\alpha)$$

with $\alpha \in \mathcal{O}_K$, which is a monic polynomial of degree 4. It will be convenient later to use such polynomials for quadratic extensions of K, rather then $g(x) = (x^2-\alpha)^2$, because $\mathrm{disc}(f) \neq 0$.
Now, let $\tilde{\rho}$ be a projective Galois representation with image conjugate to V_4^- in S_4. Then, the fixed field of $\ker(\tilde{\rho})$ is a Galois extension E/K with Galois group isomorphic to V_4. Even though V_4^- is not conjugate to V_4^+ in S_4, we can always find a monic irreducible quartic polynomial $f \in \mathcal{O}_K[x]$ such that E is the splitting field of f. Indeed, any V_4 extension of K is of the form $E = K(\sqrt{\alpha}, \sqrt{\beta})$ with $\alpha, \beta \in K^\times/(K^\times)^2$ $(\alpha, \beta \in \mathcal{O}_K)$ multiplicatively independent. In particular, E is the splitting field of

$$f(x) = x^4 - 2(\alpha + \beta)x^2 + (\alpha - \beta)^2$$

that is a monic irreducible polynomial of degree 4 over K with $\mathrm{disc}(f) \equiv 1$ modulo squares of K and $\mathrm{Gal}(f) \simeq V_4^+$. Note also that since V_4^- contains two transpositions then $\det(\tilde{\rho})$ cannot be the trivial character. Hence, it determines a nontrivial quadratic extension $K(\sqrt{\beta})$ for some $\beta \in K^\times/(K^\times)^2$. Thus, E is also the splitting field of a polynomial of the form of $f(x)$ for some $\alpha \in K^\times/(K^\times)^2$ multiplicatively independent from β. The polynomial $g(x) = (x^2 - \alpha)(x^2 - \beta)$ has $\mathrm{disc}(g) \equiv \alpha\beta$ modulo squares and $\mathrm{Gal}(g) \simeq V_4^-$. However, we will need to use irreducible polynomials later in order to determine the splitting behaviour of the primes of K in E.

Let $\Delta_i \in \mathcal{O}_K$ be the discriminant of f_{E_i}. Then the primes $\mathfrak{p}$ of K that divide the ideal $(\Delta_i) \subset \mathcal{O}_K$ may include some $\mathfrak{p} \notin S$. We set $S(\mathcal{F}) = S \cup \{\, \mathfrak{p} \,:\, \mathfrak{p} | \Delta_i \text{ for some } i \,\}$.

Definition 3.2.1. For each $G \in \left\{S_4, A_4, V_4^+, D_4, C_4, C_2^+\right\}$, we define the following subset of $\mathcal{F}$:

$$\mathcal{F}_G := \{f \in \mathcal{F} \mid \mathcal{G}(f) = G\}\,.$$

The discriminant of f has a fundamental role for our applications. First of all, we recall the following general result

Proposition 3.2.2. [20, Proposition 14.33-34, p. 610-611] *Let K be a field with $char(K) \neq 2$ and let $f \in K[x]$ be a separable polynomial of degree n. Then the following are equivalent*

1*) the Galois group $\mathcal{G}(f)$ of f is contained in A_n;*

2*) $disc(f)$ is a square in K;*

3*) A_n fixes the square root of $disc(f)$.*

From the proposition we deduce

Corollary 3.2.3. *Let K and $f \in K[x]$ be as in the previous proposition. Consider the Galois group $\mathcal{G}(f) \subset S_n$ as permutation group of the n roots of f. Then $K\left(\sqrt{disc(f)}\right)$ (possibly $= K$) is the fixed field of $\mathcal{G}(f) \cap A_n$.*

Thus, for each $f \in \mathcal{F}$ we have that $\sqrt{\mathrm{disc}(f)}$ defines a possibly trivial extension of K. Hence, by Proposition 1.4.3 we have $\mathrm{disc}(f) \equiv \Delta \bmod (K^\times)^2$ for a unique $\Delta \in K(S,2)$.

Proposition 3.2.4. *The linear representation $\bar{\rho}$ is irreducible if and only if the fixed field of $\ker(\tilde{\rho})$ is exactly one of the splitting fields of the polynomials $f \in \mathcal{F}$. Moreover, there is a unique $\Delta \in K(S,2)$ such that $\det(\tilde{\rho})$ is the quadratic character associated to Δ and when $\tilde{\rho}(\mathscr{G}_K) \neq V_4^-$ we have $disc(f) = \Delta$ (up to squares). If $\tilde{\rho}(\mathscr{G}_K) = V_4^-$ then the splitting field of f contains $K(\sqrt{\Delta})$.*

Proof. The first part of the statement follows from Prop. 3.1.4 and the construction of $\mathcal{F}$. For the second part we start by noticing that $\det(\tilde{\rho}) \longrightarrow \{\pm 1\}$ cuts out a possibly trivial quadratic extension $K_{\det(\tilde{\rho})}/K$. From the proof of Proposition 1.4.3 we see that $K_{\det(\tilde{\rho})} = K(\sqrt{\Delta})$ for some $\Delta \in K(S,2)$.
If the determinant character is trivial, then we must have $\Delta = 1$ and $\tilde{\rho}(\mathscr{G}_K) \in \left\{A_4, V_4^+, C_2^+\right\}$. Therefore, if f is a candidate to represent $K_{\ker(\tilde{\rho})}$, the splitting field of $\tilde{\rho}$, it must have Galois group $\mathcal{G}(f) \in \left\{A_4, V_4^+, C_2^+\right\}$. Hence, $\mathrm{disc}(f)$ must be a square in K so that $\mathrm{disc}(f) = 1 = \Delta$ up to squares.

In the case $\det(\tilde{\rho})$ is nontrivial we have that $\Delta \in K(S,2)$ is nontrivial and $\tilde{\rho}(\mathscr{G}_K) \in \left\{S_4, D_4, C_4, V_4^-\right\}$. Hence, if f is a candidate to represent $K_{\ker(\tilde{\rho})}$ we have $\mathcal{G}(f) \in \left\{S_4, D_4, C_4, V_4^+\right\}$ and E_f, the splitting field of f, must contain $K(\sqrt{\Delta})$.

When $\mathcal{G}(f) \in \{S_4, C_4\}$, since both S_4 and C_4 have a unique normal subgroup of index 2, then $K(\sqrt{\text{disc}(f)})$ is the unique quadratic sub-extension of E_f. Hence $\text{disc}(f) = \Delta$ up to squares.
Assume $\mathcal{G}(f) = D_4$. In D_4 there are three normal subgroups of index 2. By Corollary 3.2.3 we have that $K(\sqrt{\text{disc}(f)})$ is the fixed field of $D_4 \cap A_4 = V_4^+$. On the other hand, $K_{\det(\tilde{\rho})} = K(\sqrt{\Delta})$ is the fixed field of the subgroup of $D_4 \subset \text{PGL}_2(\mathbb{F}_3)$ whose elements are matrices with trivial determinant. By Table 3.1, such a subgroup is V_4^+ (seen as a permutation group of the four points of $\mathbb{P}^1(\mathbb{F}_3)$). Therefore, if f is a candidate to represent $K_{\ker(\tilde{\rho})}$ it must satisfy $K(\sqrt{\Delta}) = K(\sqrt{\text{disc}(f)})$, hence $\text{disc}(f) = \Delta$ (up to squares). When $\tilde{\rho}(\mathscr{G}_K) = V_4^-$, by the choice we made on the polynomials $f \in \mathcal{F}$, we have that $\mathcal{G}(f) = V_4^+ \subset A_4$. By Proposition 3.2.2 we have $\text{disc}(f) = 1$ (up to squares), therefore we can not have $\text{disc}(f) = \Delta$ since $\det(\tilde{\rho})$ is nontrivial. However, if f represents a possible candidate for $K_{\ker(\tilde{\rho})}$ then its splitting field must contain the $K(\sqrt{\Delta}) = K_{\det(\tilde{\rho})}$ as claimed. □

This last proposition implies that we have an isomorphism of abstract groups $\phi : \tilde{\rho}(\mathscr{G}_K) \longrightarrow \mathcal{G}(f)$ where f is the degree 4 polynomial that represents $K_{\ker(\tilde{\rho})}$. For each prime $\mathfrak{p} \in \text{MaxSpec}(\mathcal{O}_K) \setminus S$ we have that $\text{Frob}_\mathfrak{p}$ acts permuting the 4 roots of f and permuting the 4 points of $\mathbb{P}^1(\mathbb{F}_3)$ via $\tilde{\rho}(\text{Frob}_\mathfrak{p})$. It is useful for later, and to avoid any confusion, to understand when the cycle structures of these two permutations agree.

Proposition 3.2.5. *The cycle structures of $\tilde{\rho}(\text{Frob}_\mathfrak{p})$ as permutation of the 4 points of $\mathbb{P}^1(\mathbb{F}_3)$ is the same of $\text{Frob}_\mathfrak{p}$ as permutation of the 4 roots of f for all $\mathfrak{p} \in \text{MaxSpec}(\mathcal{O}_K) \setminus S$ if and only if $\tilde{\rho}(\mathscr{G}_K) \in \{A_4, V_4^+, C_2^+, C_4, S_4, D_4\}$. When $\tilde{\rho}(\mathscr{G}_K) = V_4^-$ the statement holds only for $\mathfrak{p} \in \text{MaxSpec}(\mathcal{O}_K) \setminus S$ that split in $K_{\det(\tilde{\rho})}$.*

Proof. The cycle structure of an element $\gamma \in S_4$ is completely determined by its order when $\text{ord}(\gamma) \neq 2$. When instead $\text{ord}(\gamma) = 2$ then it may be either a 2^2-cycle or 2-cycle. Consider $\tilde{\rho}(\mathscr{G}_K) \in \{A_4, V_4^+, C_2^+, C_4\}$. Since these groups contain only the 2^2-cycles and ϕ preserves the order of elements, in this cases the cycle structure of $\text{Frob}_\mathfrak{p}$ as permutation of the roots of f is the same of $\tilde{\rho}(\text{Frob}_\mathfrak{p})$ as permutation of the points of $\mathbb{P}^1(\mathbb{F}_3)$.
Let $\tilde{\rho}(\mathscr{G}_K) = S_4$. This time we have both types of elements of order 2. Hence ϕ may map a 2-cycle of $\tilde{\rho}(\mathscr{G}_K)$ to a 2^2-cycle of $\mathcal{G}(f)$. However, the 2^2-cycles form a unique conjugacy class of size 3, while the 2-cycles are all in a conjugacy class of size 6. Moreover, conjugate elements of $\tilde{\rho}(\mathscr{G}_K)$ have conjugate images under ϕ. Hence if a 2-cycle is mapped into a 2^2-cycle, then the entire conjugacy class is mapped to the 2^2-cycle conjugacy class. Due to the different sizes involved and the fact

the ϕ is bijective, this can not happen. Therefore the cycle structure is preserved. Equivalently, it follows from the fact that all automorphisms of S_4 are inner.
Consider $\tilde{\rho}(\mathscr{G}_K) = D_4$. Up to conjugation, we may assume that $\mathcal{G}(f) = \tilde{\rho}(\mathscr{G}_K) = \langle (1,2,3,4), (1,3) \rangle$. We have then the following conjugacy classes

$$G_{2^2} = \{(1,2)(3,4), (1,4)(2,3)\}\,; \quad G_2 = \{(1,3), (2,4)\}\,; \quad Z(D_4) = \{(1,3)(2,4)\}\,.$$

Since, D_4 is generated also by the pair $(1,2,3,4), (1,2)(3,4)$ we have the (outer) automorphism of D_4 that send $(1,3) \mapsto (1,2)(3,4)$ and $(1,2,3,4)$ in itself. So the isomorphism $\phi : \tilde{\rho}(\mathscr{G}_K) \longrightarrow \mathcal{G}(f)$ may actually swap the two cycle structures. However, let $\mathfrak{p}$ a prime of K such that $\tilde{\rho}(\mathrm{Frob}_\mathfrak{p}) \in \tilde{\rho}(\mathscr{G}_K)$ is a 2^2-cycle. By Table 3.1 $\det(\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})) = 1$, forcing $\mathfrak{p}$ to be split in the quadratic extension $K_{\det(\tilde{\rho})}/K$. By Proposition 3.2.4 we have $K_{\det(\tilde{\rho})} = K(\sqrt{\mathrm{disc}(f)})$ and since $\mathfrak{p}$ splits in $K(\sqrt{\mathrm{disc}(f)})$ then the associated $\mathrm{Frob}_\mathfrak{p} \in \mathcal{G}(f)$ must be trivial when restricted to this field. Hence $\mathrm{Frob}_\mathfrak{p} \in V_4^+ \lhd \mathcal{G}(f)$, and since it has order 2 it is a 2^2-cycle.
Finally, take $\tilde{\rho}(\mathscr{G}_K) = V_4^-$. Since $\mathcal{G}(f)$ as permutation group is isomorphic to V_4^+ then we have infinitely many primes $\mathfrak{p}$ such that the cycle structure of $\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})$ and $\mathrm{Frob}_\mathfrak{p} \in \mathcal{G}(f)$ do not agree. But if we take a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ that splits in $K_{\det(\tilde{\rho})}$ and such that $\mathrm{Frob}_\mathfrak{p}$ is non trivial, then $\det(\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})) = 1$ and it is of order 2; that means that $\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})$ is a 2^2-cycle as wanted. □

It is useful for later to introduce the following sets.

Definition 3.2.6. Let Δ be a representative of a class in $K(S,2)$, and let G be a group such that $G \in \{S_4, A_4, V_4^+, D_4, C_4, C_2^+\}$, and E_f the splitting field of f. Then we define

$$\mathcal{F}_G(\Delta) := \left\{ f \in \mathcal{F}_G \mid \mathrm{disc}(f) \equiv \Delta \pmod{(K^\times)^2} \right\}. \tag{3.1}$$

$$\mathcal{F}_{V_4^-}(\Delta) := \begin{cases} \left\{ f \in \mathcal{F}_{V_4^+} \;\middle|\; \sqrt{\Delta} \in E_f \right\} & \text{if } \Delta \not\equiv 1 \pmod{(K^\times)^2}\,; \\ \emptyset & \text{otherwise.} \end{cases} \tag{3.2}$$

We also define

$$\mathcal{F}_\Delta := \bigcup_{G \in \{S_4, A_4, V_4^\pm, D_4, C_4, C_2^+\}} \mathcal{F}_G(\Delta).$$

Note that by (3.1) ,(3.2) the union is disjoint. Moreover, if $\Delta \equiv 1$ i.e. Δ is a square in K, then we define

$$\mathcal{F}^+ := \mathcal{F}_1 = \bigcup_{G \in \{A_4, V_4^+, C_2^+\}} \mathcal{F}_G.$$

Similarly we define the possibly proper subset of $\mathcal{F}_\Delta$

$$\mathcal{F}^- := \bigcup_{\substack{\Delta \in K(S,2) \\ \Delta \neq 1 \\ G \in \{S_4, D_4, V_4^-, C_4\}}} \mathcal{F}_G(\Delta).$$

Remark 3.2.7. We have that

$$\mathcal{F} = \bigcup_{\Delta \in K(S,2)} \mathcal{F}_\Delta;$$

however the union is not disjoint since each $f \in \mathcal{F}_{V_4^+}$ is in $\mathcal{F}_\Delta$ for all Δ such that $K(\sqrt{\Delta}) \subset E_f$. It is also extremely important for later to note that, by definition, all the field extensions determined by polynomials in $\mathcal{F}$ are distinct.

3.3 Irreducibility test for 2-dimensional $\mathbb{F}_3$-Galois representations

We keep the notation of the previous sections. Here, we want to present an effective method to test whether a black box Galois representation $\bar{\rho}$ is irreducible. By Prop 3.1.3 it is enough to prove that $\tilde{\rho}$ is irreducible. We start by determining the quadratic character $\det(\tilde{\rho})$ and the associated quadratic extension $K(\sqrt{\Delta})$ using the method developed in Chapter 2. Indeed, for each $\Delta \in K(S,2)$ let χ_Δ be the quadratic character that cuts out $K(\sqrt{\Delta})$. We can test the quadratic character $\det(\tilde{\rho})\chi_\Delta^{-1}$ over T_2, since we know $\det(\tilde{\rho})(\mathrm{Frob}_\mathfrak{p})$ for each $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$. But then, by Lemma 2.0.3, we are able to determine which $K(\sqrt{\Delta})$ is related to $\tilde{\rho}$. As a consequence, by Proposition 3.2.4 we can restrict the possible images and fixed fields just to the ones determined by $\mathcal{F}_\Delta$. Therefore if $\tilde{\rho}$ is irreducible we have the following tower of extensions

$$\begin{array}{c} K_{\ker(\tilde{\rho})} \simeq K_f \\ | \\ K(\sqrt{\Delta}) \\ | \\ K \end{array}$$

where $K_f \in \mathcal{A}_\Delta := \{E \in \mathcal{A} \,|\, f_E \in \mathcal{F}_\Delta\}$. Here, $K(\sqrt{\Delta})$ is the fixed field of $\det(\tilde{\rho})$.

Remark 3.3.1. Above we are allowing $\Delta = 1$. In this case χ_Δ is trivial and we are testing whether $\det(\tilde{\rho})$ is the trivial character or not. This means that if the

determinant character is trivial then we can restrict to testing only $\mathcal{F}_1 = \mathcal{F}^+$. The situation is even better if $\det(\tilde{\rho}) \neq 1$,as in this case we need to deal only with a, possibly proper, subset of $\mathcal{F}^-$.

Now, if we look at the cycle structure of the elements in S_4, A_4, V_4^+, D_4, C_4, C_2^+, we note that each of them contains at least one product of disjoint transpositions. Since in each of these groups, the set X of these elements is a union of conjugacy classes, we conclude by the Chebotarev density theorem that the set $\mathcal{P}$ of primes of K unramified in the respective extensions, and whose associated Frobenius conjugacy class lies in X has positive density. The densities are given in Table 3.2.

$\mathcal{G}(f)$	density of $\mathcal{P}$
S_4	1/8
A_4	1/4
V_4^+	3/4
D_4	3/8
C_4	1/4
C_2^+	1/2

Table 3.2: Densities of primes of K that satisfy condition (3.3)

Therefore, for each field extension E_i/K, with $E_i \in \mathcal{A}$, we can find a prime $\mathfrak{p}_i \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F})$ such that

$$f_i(x) \equiv g_{i_1} g_{i_2} \pmod{\mathfrak{p}_i} \tag{3.3}$$

with $g_{i_1}, g_{i_2} \in \mathcal{O}_K/\mathfrak{p}_i[x]$ irreducible quadratic polynomials over the field $\mathcal{O}_K/\mathfrak{p}_i$. Note that this is true even in the case C_2^+ by the earlier choice of f_i in this case.

Definition 3.3.2. Let $\mathfrak{p}$ be a prime of K not in S. Then the characteristic polynomial of $\bar{\rho}\,(\mathrm{Frob}_\mathfrak{p})$ is

$$F_\mathfrak{p}(x) = x^2 - \mathrm{tr}\,(\bar{\rho}(\mathrm{Frob}_\mathfrak{p}))\,x + \det\,(\bar{\rho}(\mathrm{Frob}_\mathfrak{p}))\,.$$

Theorem 3.3.3. *Let K be a number field, S a finite set of primes of K and let $\mathcal{G}_K$ be the absolute Galois group of K. Let $\bar{\rho} : \mathcal{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ be a Galois representation of $\mathcal{G}_K$ unramified outside S. Then there exists a finite and computable set of primes T of K that we call the* irreducibility test set *such that $\bar{\rho}$ is irreducible if and only if $F_\mathfrak{p}(x) = x^2 + 1$ for some $\mathfrak{p} \in T$.*
Moreover, let $\mathfrak{p}_f \in T$ be a test prime associated to a unique polynomial f. If only $F_{\mathfrak{p}_f}(x) = x^2 + 1$ then the fixed field of $\ker(\tilde{\rho})$ is E_f.

Proof. It is enough to prove that $\tilde{\rho}$ is irreducible. After the determinant test we presented at the beginning of the section, all the possible irreducible images and splitting fields for $\tilde{\rho}$ are represented by the monic degree 4 polynomials $f \in \mathcal{F}_\Delta$ (see Proposition 3.2.4). By Proposition 3.2.5 for each polynomial f we can find a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ such that condition (3.3) holds if and only if $\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})$ is a 2^2-cycle. The density of such primes when $\mathcal{G}(f) = V_4^+$ but $\det(\tilde{\rho})$ is not trivial is $1/4$ while for the remaining cases it coincides with the one reported in Table 3.2. Let T be the finite set of these primes. By hypothesis, we are able to compute the characteristic polynomial $F_\mathfrak{p}(x)$ for each $\mathfrak{p} \in T$. If $F_{\mathfrak{p}_f}(x) \neq x^2 + 1$ for some $\mathfrak{p}_f \in T$ then we can discard E_f from the set of possible fixed field of $\ker(\tilde{\rho})$. But then, if for all $\mathfrak{p} \in T$ we have $F_\mathfrak{p}(x) \neq x^2 + 1$ then the image of $\tilde{\rho}$ is none of the groups $S_4, A_4, V_4^\pm, D_4, C_4, C_2^+$, hence $\tilde{\rho}$ is reducible by Prop 3.1.4, and hence by Prop 3.1.3 $\bar{\rho}$ is also reducible. Furthermore, if $F_\mathfrak{p}(x) = x^2 + 1$ for at least one $\mathfrak{p} \in T$ then the projective representation is irreducible since the $\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})$ does not fix any point in $\mathbb{P}^1(\mathbb{F}_3)$. In particular, if $F_\mathfrak{p}(x) = x^2 + 1$ for exactly one $\mathfrak{p} \in T$ that is associated to a unique polynomial f then the field extension of K cut out by $\tilde{\rho}$ is the splitting field of f. In this last case we can also determine to which subgroup of S_4 the image of $\tilde{\rho}$ is conjugate. Indeed, this is completely obvious when $\mathcal{G}(f) \in \left\{S_4, A_4, D_4, C_4, C_2^+\right\}$. If $\mathcal{G}(f) \simeq V_4^+$ then the image of $\tilde{\rho}$ will be conjugate to V_4^+ if $\det(\tilde{\rho}) = 1$ and it will be conjugate to V_4^- otherwise. □

Remark 3.3.4. With the theory developed until now, when the condition in the theorem is satisfied by more than one prime or by a prime associated to more than one polynomial, we can only detect whether $\tilde{\rho}(\mathscr{G}_K)$ lies either in $\{A_4, V_4^+, C_2^+\}$ or $\{S_4, D_4, V_4^-, C_4\}$ and the possible splitting field is some E_f for $f \in \mathcal{F}_\Delta$.

3.4 How to distinguish irreducible projective representations

We retain the notation of the previous sections. We have seen that we can attach to a Galois representation $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ a projective representation $\tilde{\rho} : \mathscr{G}_K \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$. In particular, we have shown

i) If $\tilde{\rho}$ is irreducible and $\det(\tilde{\rho})$ is the trivial character then

$$\tilde{\rho}(\mathscr{G}_K) \in \left\{A_4, V_4^+, C_2^+\right\};$$

ii) If $\tilde{\rho}$ is irreducible and $\det(\tilde{\rho})$ is not the trivial character then

$$\tilde{\rho}(\mathscr{G}_K) \in \left\{S_4, D_4, V_4^-, C_4\right\},$$

and the fixed field of $\det(\tilde{\rho})$ is a known quadratic extension $K(\sqrt{\Delta})$.
The aim of this section is to present an exhaustive method that determines the image of $\tilde{\rho}$ and the exact field extension $E_i \in \mathcal{A}$ which is the fixed field of $\ker(\tilde{\rho})$. Before introducing the method, we need some further considerations.

For each prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F})$ and $f \in \mathcal{F}$ one of the following two cases holds:

a) either f has respectively 4 or 1 roots mod $\mathfrak{p}$ or f is irreducible mod $\mathfrak{p}$;

b) or f has two roots mod $\mathfrak{p}$ or splits as the product of two irreducible quadratics mod $\mathfrak{p}$.

Case *a*) happens when $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(f) \subseteq S_4$ has order respectively: 1, 3 or 4. Accordingly to Table 3.1 we should have

$$\mathrm{tr}\left(\bar{\rho}\left(\mathrm{Frob}_\mathfrak{p}\right)\right) = \pm 1.$$

While *b*) occurs when $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(f) \subseteq S_4$ has order 2. By Table 3.1 we should have

$$\mathrm{tr}\left(\bar{\rho}\left(\mathrm{Frob}_\mathfrak{p}\right)\right) = 0.$$

So, for each $f \in \mathcal{F}$ we can define the following function

$$\lambda_f : \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F}) \longrightarrow \mathbb{F}_2$$

such that

$$\lambda_f(\mathfrak{p}) := \begin{cases} 1 & \text{if case } a) \text{ occurs for } \mathfrak{p}, f \\ 0 & \text{if case } b) \text{ occurs for } \mathfrak{p}, f. \end{cases}$$

Now, if $\mathcal{F} := \{f_1, \ldots, f_t\}$ we can define the function

$$\mathrm{v} : \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F}) \longrightarrow \mathbb{F}_2^t$$

by

$$\mathrm{v}(\mathfrak{p}) = (\lambda_{f_1}(\mathfrak{p}), \ldots, \lambda_{f_t}(\mathfrak{p}))$$

Definition 3.4.1. Let $t = \#\mathcal{F}$, and $T_0 := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \subset \mathcal{O}_K \setminus S(\mathcal{F})$ be a set of primes such that the matrix

$$\begin{pmatrix} \mathrm{v}(\mathfrak{p}_1) & \cdots & \mathrm{v}(\mathfrak{p}_s) \end{pmatrix} = \begin{pmatrix} \lambda_{f_1}(\mathfrak{p}_1) & \cdots & \lambda_{f_1}(\mathfrak{p}_s) \\ \vdots & \ldots & \vdots \\ \lambda_{f_t}(\mathfrak{p}_1) & \cdots & \lambda_{f_t}(\mathfrak{p}_s) \end{pmatrix} \in \mathrm{M}_{t\times s}\left(\mathbb{F}_2\right) \tag{3.4}$$

has distinct rows. Note that the i-th row describes the behaviour of f_i modulo the primes of T_0, and we denote it with $\mathfrak{v}(f_i)$. We call T_0 the *distinguishing set* for $\mathcal{F}$.

Remark 3.4.2. Actually, we do not need to compute the function v and the set T_0 for all $\mathcal{F}$. Indeed, after we study the determinant character, and after we apply the irreducibility test, we deal with $\mathcal{F}_\Delta$.

We have to prove that such a set exists. However, to have a clearer exposition, we postpone the proof until after the presentation of how we may use such a set to determine the image of the irreducible projective representation $\tilde{\rho}$, and the field extension it cuts out.

In order to do this, we recall that for each $\mathfrak{p} \in \mathcal{O}_K \setminus S(\mathcal{F})$ we can compute $\mathrm{tr}\left(\tilde{\rho}(\mathrm{Frob}_\mathfrak{p})\right) \in \{\pm 1, 0\}$. In particular, we can construct the following vector

$$\mathfrak{v} := (\Lambda_1, \ldots, \Lambda_s)\,,$$

where, Λ_i is equal to 1 if $\mathrm{tr}\left(\tilde{\rho}(\mathrm{Frob}_{\mathfrak{p}_i})\right) = \pm 1$ and zero otherwise, and $\mathfrak{p}_i \in T_0$ for all i. Now, we know that $\tilde{\rho}(\mathscr{G}_K) = \mathrm{Gal}(f)$ for some $f \in \mathcal{F}$, hence there exists at least one row of the matrix in (3.4) that is equal to $\mathfrak{v}$. Since all the rows are distinct, there exist just one $1 \leq i \leq t$ such that

$$\mathfrak{v}(f_i) = \mathfrak{v}.$$

Therefore, we conclude that $\tilde{\rho}(\mathscr{G}_K) = \mathrm{Gal}(f_i)$, and the fixed field of $\ker(\tilde{\rho})$ is the splitting field E_i of f_i.

It remains to prove the following proposition.

Proposition 3.4.3. *A distinguishing set T_0 for $\mathcal{F}$, and for each $\mathcal{F}_\Delta$ exists.*

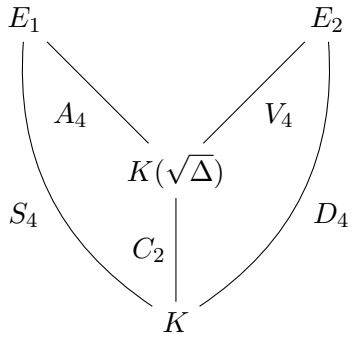
Proof. We have to show that given $f_1, f_2 \in \mathcal{F}$ we can find a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F})$ such that the factorization of the two polynomials modulo $\mathfrak{p}$ is different, i.e. $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$. This is equivalent to finding a prime $\mathfrak{p}$ of K for which f_1 has behaviour $\mathrm{mod}\,\mathfrak{p}$ as in a) and f_2 $\mathrm{mod}\,\mathfrak{p}$ behave as in b) or vice versa. This forces

the associated Frobenius (up to conjugacy) to have precise orders in the two Galois groups $\mathrm{Gal}(f_1), \mathrm{Gal}(f_2)$. In this way, we start with no primes and at each step we add a new prime $\mathfrak{p}$ such that $\mathfrak{v}(f_1) \neq \mathfrak{v}(f_2)$, increasing the number of columns by 1. It is not hard to see that the numbers of primes s needed is such that $\log_2(t) \leq s \leq t$.

Since before computing T_0 we can exclude one of $\mathcal{F}^+$ and $\mathcal{F}^-$ (see Remark 3.3.1), we treat the two cases separately.

We start with the case $\mathcal{F}^-$. Under this assumption, we have shown that we can actually restrict our attention to polynomials that lie in $\mathcal{F}_\Delta$ for some $\Delta \in K^\times/(K^\times)^2$ different from 1.
Therefore, let $f_1, f_2 \in \mathcal{F}_\Delta$. Their splitting fields E_1, E_2 intersect at least in the quadratic extension $K(\sqrt{\Delta})$. In each case we need to prove the existence of a prime $\mathfrak{p} \notin S(\mathcal{F}_\Delta)$ such that $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$. In fact we will show that the set of such primes has positive density in each case. We have the following cases:

Case 1) $(\mathrm{Gal}(f_1) = S_4, \mathrm{Gal}(f_2) = D_4)$. We have the following tower of extensions



Now, if we take the composite field E_1E_2 this is a Galois extension of K with Galois group

$$\mathrm{Gal}(E_1E_2/K) = S_4 \times_{C_2} D_4 := \left\{ (\sigma, \tau) \in S_4 \times D_4 \;\middle|\; \sigma_{|_{K(\sqrt{\Delta})}} = \tau_{|_{K(\sqrt{\Delta})}} \right\}$$

i.e. these are the pairs $(\sigma, \tau) \in S_4 \times D_4$ such that $\overline{\sigma} \in S_4/A_4 \simeq C_2$ is equal to $\overline{\tau} \in D_4/V_4 \simeq C_2$. By parity the 4-cycles and the 2-cycles of S_4 (resp. D_4) lie in the same coset of A_4 (resp. V_4). For simplicity we denote 4-cycles and 2-cycles by their cycle structure 4 and 2 respectively. Thus, the pair $(4, 2)$ lies in $\mathrm{Gal}(E_1E_2/K)$, and

since the set $X \subset S_4 \times_{C_2} D_4$ of these pairs is stable under conjugation, and

$$\frac{\#X}{\#\mathrm{Gal}(E_1E_2/K)} = \frac{1}{8},$$

then by Chebotarev there exist infinitely many primes $\mathfrak{p} \in \mathcal{O}_K \setminus S$ such that $\mathrm{Frob}_\mathfrak{p}$ is a 4-cycle in $\mathrm{Gal}(E_1/K)$ and $\mathrm{Frob}_\mathfrak{p}$ is a 2-cycle in $\mathrm{Gal}(E_2/K)$. In particular for a such a prime $\mathfrak{p}$ we have

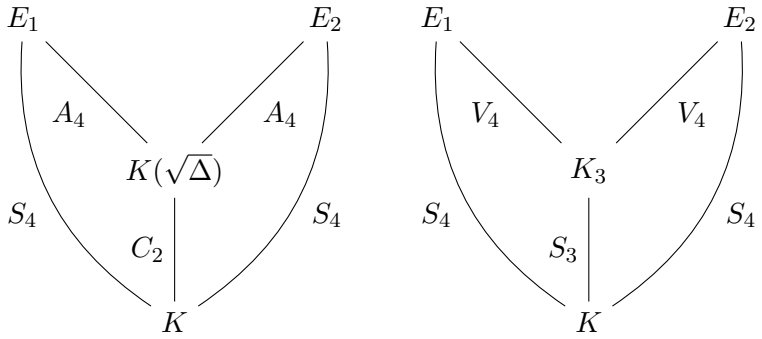
$$f_1 \text{ is irreducible mod } \mathfrak{p}, \tag{3.5}$$

$$f_2 \text{ is reducible mod } \mathfrak{p}. \tag{3.6}$$

We remark that the argument above is exactly the same, if we search for a prime $\mathfrak{p}$ such that the conditions (3.5) and (3.6) are swapped. Hence the density of primes $\mathfrak{p} \notin S(\mathcal{F}_\Delta)$ such that $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$ is 1/4.

Case 2) ($\mathbf{Gal}(f_1) = D_4, \mathbf{Gal}(f_2) = D_4$). This case is completely analogous to the previous one. Again, the density of the primes $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F}_\Delta)$ whose $\mathrm{Frob}_\mathfrak{p}$ is a 4-cycle in $\mathrm{Gal}(f_1)$ and a 2-cycle in $\mathrm{Gal}(f_2)$ is 1/8.

Case 3) ($\mathbf{Gal}(f_1) = S_4, \mathbf{Gal}(f_2) = S_4$). In this case the two extensions E_1, E_2 can intersect in $K(\sqrt{\Delta})$ or in an S_3 extension if the cubic resolvents g_1, g_2 of f_1 and f_2 respectively, have the same splitting field. Therefore we have the following possibilities



The first case is similar to the two we have seen before; for the second one, we have to look at the coset partition of S_4 by V_4. The 4-cycles and the 2-cycles are divided into three different cosets. In each coset there are two 4-cycles and two 2-cycles therefore not every combination $(4, 2)$ lies in $S_4 \times_{S_3} S_4 = \mathrm{Gal}(E_1E_2/K)$. It turns

out that we have

$$\#X := \#\{(4,2) \in S_4 \times_{S_3} S_4\} = 12.$$

Since X is closed under conjugation, by Chebotarev we have that the set $\mathcal{P}$ of the primes $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ such that conditions (3.5),(3.6) are satisfied, has density 1/8. Finally, if we swap the conditions of $f_1, f_2 \bmod \mathfrak{p}$, we obtain an additional set of primes of density 1/8 for which $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$.

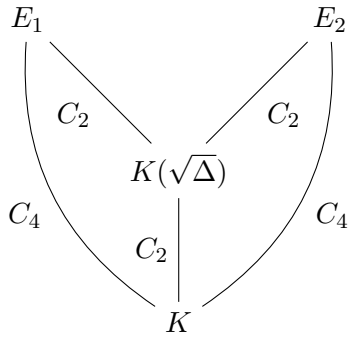
Case 4) $(\mathbf{Gal}(f_1) = C_4, \mathbf{Gal}(f_2) = S_4)$. It is clear that E_1, E_2 can intersect only in $K(\sqrt{\Delta})$. By parity, 4-cycles of C_4 have the same restriction to C_2 as 4-cycles and 2-cycles of S_4. Therefore, all the possible pairs $(4,2)$ lie in $C_4 \times_{C_2} S_4$. Hence, the density of the set

$$\mathcal{P} := \{\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S \mid \mathrm{Frob}_\mathfrak{p} = (4,2) \in \mathrm{Gal}(E_1E_2/K)\}$$

is 1/4. Note that this time we cannot swap the conditions since C_4 does not contain a 2-cycle.

Case 5) $(\mathbf{Gal}(f_1) = C_4, \mathbf{Gal}(f_2) = D_4)$. Similar to Case 4). The density is 1/4.

Case 6) $(\mathbf{Gal}(f_1) = C_4, \mathbf{Gal}(f_2) = C_4)$. We have the now familiar tower of extensions



where $\mathrm{Gal}(K(\sqrt{\Delta})) = C_4/C_2 \simeq C_2$ is given by the quotient of C_4 by the subgroup generated by the unique product of disjoint transpositions of $C_4 \subset S_4$. Thus, by parity we have that the 4-cycles have the same image in the quotient and the product of disjoint transpositions lies in the same coset as the identity. This means we cannot choose a prime $\mathfrak{p}$ of K whose associated conjugacy class of $\mathrm{Frob}_\mathfrak{p} \in X = \{(4,2) \in \mathrm{Gal}(E_1E_2/K)\}$. However, we can look for a prime

$\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ such that

$$f_1 \text{ is reducible, but has no roots mod } \mathfrak{p}, \tag{3.7}$$

$$f_2 \text{ has at least one root mod } \mathfrak{p}. \tag{3.8}$$

because if these conditions are satisfied then

$$\mathrm{Frob}_{\mathfrak{p}} \in X' = \left\{(2^2, 1) \in \mathrm{Gal}(E_1E_2/K)\right\}.$$

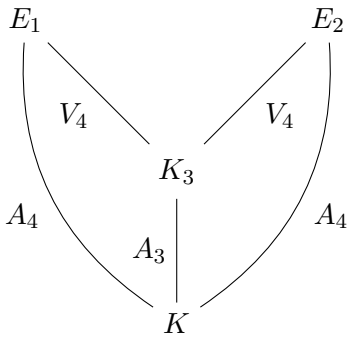
Since $\#X'/\#\mathrm{Gal}(E_1E_2/K) = 1/8$ we know that there are infinitely many primes that satisfy (3.7) and (3.8). By symmetry, we may swap the conditions on f_1, f_2; hence the density of primes $\mathfrak{p} \notin S(\mathcal{F}_\Delta)$ such that $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$ is 1/4.

Case 7) $\boldsymbol{\left(\mathrm{Gal}(f_1) = V_4^+, \mathrm{Gal}(f_2) = S_4\right).}$ Similar to case 4). The field $K(\sqrt{\Delta}) \subset E_{f_1}$ is fixed by a $C_2^+ = \langle v_1 \rangle$ for a 2^2 cycle $v_1 \in V_4^+$. Therefore, the other two 2^2-cycles have same nontrivial projection in $V_4/C_2^+ \simeq C_2$. By parity the same holds for the six 4-cycles of S_4. The density is then 1/4.

Case 8-9) $\boldsymbol{\left(\mathrm{Gal}(f_1) = V_4^+, \mathrm{Gal}(f_2) = D_4 \text{ or } \mathrm{Gal}(f_2) = C_4\right).}$ Similar to Case 7). The density is 1/4.

To address the case $\left(\mathrm{Gal}(f_1) = V_4^+, \mathrm{Gal}(f_2) = V_4^+\right)$ we study what happen more generally when $f_1, f_2 \in \mathcal{F}^+$. Under this assumption we have to distinguish A_4,V_4^+, C_2^+ extensions of K.

Case 10) $\boldsymbol{(\mathrm{Gal}(f_1) = A_4, \mathrm{Gal}(f_2) = A_4).}$ The only nontrivial normal subgroup of A_4 is V_4^+ and taking the quotient we have an intermediate extension with Galois group $C_3 \simeq A_3 \simeq A_4/V_4$. This implies that if the resolvents of f_1 and f_2 have the same splitting field we have the following



In $\mathrm{Gal}(E_1E_2/K) = A_4 \times_{A_3} A_4$ we have the pairs $(1, 2^2)$ and they form a set X closed under conjugation. This means we can find a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ such that

$$f_1 \text{ has at least one root mod } \mathfrak{p}, \tag{3.9}$$

$$f_2 \text{ has no roots mod } \mathfrak{p}. \tag{3.10}$$

and the density of such a primes is $\#X/\#(A_4 \times_{A_3} A_4) = 1/16$. By symmetry, the density of primes $\mathfrak{p} \notin S(\mathcal{F}_\Delta)$ such that $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$ is $1/8$. On the other hand, if the resolvents have different splitting fields then E_1 and E_2 intersect trivially. Therefore, $\mathrm{Gal}(E_1E_2/K) = A_4 \times A_4$ and we can take $X := \left\{(3, 2^2), (1, 2^2) \in \mathrm{Gal}(E_1E_2/K)\right\}$. Hence, the density of primes $\mathfrak{p} \notin S(\mathcal{F}_\Delta)$ such that conditions (3.9),(3.10) are satisfied is $3/16$. Switching the conditions, we obtain an additional set of primes of density $3/16$ for which $\lambda_{f_1}(\mathfrak{p}) \neq \lambda_{f_2}(\mathfrak{p})$.

Case 11) $\left(\mathbf{Gal}(\boldsymbol{f_1}) = \boldsymbol{V_4^+}, \mathbf{Gal}(\boldsymbol{f_2}) = \boldsymbol{V_4^+}\right)$**.** Clearly two distinct V_4 extensions can intersect in a quadratic field. When we quotient $V_4^+ \subset S_4$ by one of the C_2^+ then we have exactly one element $(1, 2^2) \in V_4^+ \times_{C_2^+} V_4^+$. Therefore, there are infinitely many primes $\mathfrak{p}$ of K such that conditions (3.9),(3.10) are satisfied. Their density is $1/8$.

Case 12) $\left(\mathbf{Gal}(\boldsymbol{f_1}) = \boldsymbol{A_4}, \mathbf{Gal}(\boldsymbol{f_2}) = \boldsymbol{V_4^+}\right)$**.** Since the unique nontrivial quotient of A_4 is isomorphic to A_3 while the quotients of V_4 are all isomorphic to C_2 we have that two such extensions do not intersect. In particular, $G = \mathrm{Gal}(E_1E_2/K) = A_4 \times V_4$. Therefore, the subset X of G defined by

$$X = \left\{(3, 2^2), (1, 2^2) \in G\right\}$$

can be used to distinguish f_1, f_2. The density of the primes $\mathfrak{p}$ of K such that conditions (3.9),(3.10) are satisfied is $9/16$.

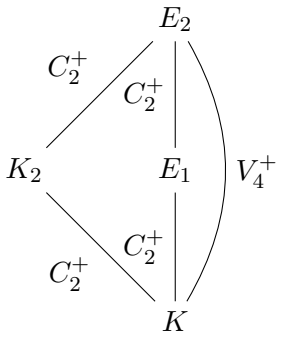
Case 13) $\left(\mathbf{Gal}(\boldsymbol{f_1}) = \boldsymbol{A_4}, \mathbf{Gal}(\boldsymbol{f_2}) = \boldsymbol{C_2^+}\right)$**.** Two such extensions intersect trivially, hence $G = \mathrm{Gal}(E_1E_2/K) = A_4 \times C_2^+$. We have the subset X of G defined by

$$X = \left\{(3, 2^2), (1, 2^2) \in G\right\},$$

can be used to distinguish f_1, f_2. The density of the primes $\mathfrak{p}$ of K such that conditions (3.9),(3.10) are satisfied is $3/4$.

Case 14) $\left(\mathbf{Gal}(f_1) = C_2^+, \mathbf{Gal}(f_2) = C_2^+\right)$**.** Clearly the two extensions do not intersect. With similar argument as cases 5), 6) we can find a prime $\mathfrak{p} \in \mathcal{O}_K \setminus S(\mathcal{F})$ such that $\text{Frob}_\mathfrak{p} = 1 \in \text{Gal}(f_1)$, and $\text{Frob}_\mathfrak{p} = 2^2 \in \text{Gal}(f_2)$. The density of such primes is 1/4. By symmetry, the total density is 1/2.

Case 15) $\left(\mathbf{Gal}(f_1) = C_2^+, \mathbf{Gal}(f_2) = V_4^+\right)$**.** This time we have the following tower of Galois extensions



We are searching for a prime $\mathfrak{p} \in \text{MaxSpec}(\mathcal{O}_K) \setminus S(\mathcal{F})$ such that the conditions (3.9),(3.10) are satisfied. This happens when $\mathfrak{p}$ splits completely in E_1 but not in E_2; that is, when both the following hold:

$$\text{Frob}_\mathfrak{p} \text{ is a product of two disjoint transpositions in } \text{Gal}(K_2/K);$$
$$\text{Frob}_\mathfrak{p} \text{ is trivial in } \text{Gal}(E_1/K).$$

Thus, we are in the same situation as in Case 7), and the density of these primes is 1/4.

□

3.5 Determining the irreducible mod 3 image

At this point we have completely determined the irreducible projective mod 3 representation $\tilde{\rho}$: the fixed field L/K of $\ker(\tilde{\rho})$, and a degree 4 polynomial $f \in K[x]$ that defines the extension. We have also determined, up to conjugacy, $\tilde{\rho}(\mathcal{G}_K)$ as subgroup of S_4. In this section we further determine the mod 3 representation $\bar{\rho}$: the fixed field M/K of $\ker(\bar{\rho})$.

3.5.1 The possible images

In this paragraph we determine the possible images an irreducible representation $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ may have.

Proposition 3.5.1. *We have* $[\ker(\tilde{\rho}) : \ker(\bar{\rho})] = 2$*, and hence* $[M : L] = 2$*.*

Proof. The fact that $[\ker(\tilde{\rho}) : \ker(\bar{\rho})] \leq 2$ is clear since $\mathbb{F}_3^\times$ has order 2 and

$$\mathscr{G}_K \xrightarrow{\bar{\rho}} \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\pi} \mathrm{PGL}_2(\mathbb{F}_3) = \mathrm{GL}_2(\mathbb{F}_3)/\mathbb{F}_3^\times.$$
$$\mathscr{G}_K \xrightarrow{\tilde{\rho}} \mathrm{PGL}_2(\mathbb{F}_3)$$

However, $-I$ is always in the image of $\bar{\rho}$, and the result follows. To see this, recall that under the isomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ each of these (conjugacy classes of) subgroups contains at least one product of two disjoint transpositions. Also, we have seen that such elements come from matrices $g \in \mathrm{GL}_2(\mathbb{F}_3)$ with characteristic polynomial x^2+1 (see discussion before table 3.1). By the Cayley-Hamilton theorem we get $g^2 = -\mathrm{Id}$ and the order of g is 4. Therefore, each of these groups lifts to $\bar{\rho}(\mathscr{G}_K) < \mathrm{GL}_2(\mathbb{F}_3)$ such that $\{\pm\mathrm{Id}\} \subset \bar{\rho}(\mathscr{G}_K)$ as claimed. □

Theorem 3.5.2. *Let K be a number field, and S a finite set of primes of K. Let $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ be continuous representation of the absolute Galois group $\mathscr{G}_K$ of K unramified outside S. Then $\bar{\rho}$ is irreducible if and only if its image lies in the following set*

$$\bar{\rho}(\mathscr{G}_K) \in \{\mathrm{GL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3), SD_{16}, Q_8, D_4, C_8, C_4\},$$

where SD_{16} is the semi dihedral group of order 16 and Q_8 is the quaternion group.

Proof. In view of Proposition 3.1.4, $\bar{\rho}$ is irreducible if and only if the projective image is one of the following groups $\{S_4, A_4, D_4, V_4^{\pm}, C_4, C_2^{+}\}$. Hence, it is enough to determine the preimage of these (conjugacy class of) groups in $\mathrm{GL}_2(\mathbb{F}_3)$.

It follows from Proposition 3.5.1 that the image of $\bar{\rho}$ is the complete preimage of $\tilde{\rho}$ in $\mathrm{GL}_2(\mathbb{F}_3)$. We consider each case in turn.

- $S_4 \leftrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ since $\bar{\rho}$ has size 48.
- $A_4 \leftrightarrow \mathrm{SL}_2(\mathbb{F}_3)$. A_4 contains all the 3 and 2^2-cycles plus the identity. We know also that they comes from matrices with determinant equal to one. Since $|\bar{\rho}(\mathscr{G}_K)| = 24$ then it must contains all such matrices. Alternatively, we can

argue that $\bar{\rho}$ is a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of index 2 and get the same result.

- $D_4 \leftrightarrow SD_{16}$. This is because $|\bar{\rho}(\mathscr{G}_K)| = 16$ and therefore it is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. We might conclude by the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ as presented for example in GroupNames [22]. Or we can proceed with a direct proof. Indeed, D_4 is generated by a 4-cycle $\tilde{g}$ and a 2-cycle $\tilde{h}$ such that $\tilde{h}\tilde{g}\tilde{h} = \tilde{g}^{-1}$. They come from $g, h \in \mathrm{GL}_2(\mathbb{F}_3)$ with characteristic polynomial $x^2 \mp x - 1$ and $x^2 - 1$ respectively. By Cayley-Hamilton we deduce that g has order 8 and $g^4 = -\mathrm{Id}$, while h has order 2. Finally by direct computation we can see that g, h generate $\bar{\rho}$ and satisfy $hgh = g^3$, that implies $\bar{\rho}(\mathscr{G}_K) \simeq SD_{16}$.

- $V_4^+ \leftrightarrow Q_8$. Indeed, $|\bar{\rho}(\mathscr{G}_K)| = 8$ and is generated by 3 elements α, β, γ such that it $\alpha^2 = \beta^2 = \gamma^2 = -\mathrm{Id}$. Or again we can say that is a normal subgroup of size 8 and conclude by the previous classification.

- $V_4^- \leftrightarrow D_4$. We have $|\bar{\rho}(\mathscr{G}_K)| = 4$. Now, V_4^- is generated by the product of two disjoint transpositions $\tilde{\alpha}, \tilde{\beta}$ and contains a 2^2-cycle $\tilde{\alpha}\tilde{\beta} = \tilde{\gamma}$. We know that their lifts to $\mathrm{GL}_2(\mathbb{F}_3)$ are matrices α, β of order 2 and γ of order 4. An easy computation shows that $\bar{\rho}(\mathscr{G}_K)$ is generated by α, γ and they satisfy $\alpha\gamma\alpha = \gamma^{-1}$. Therefore, $\bar{\rho}(\mathscr{G}_K) \simeq D_4$.

- $C_4 \leftrightarrow C_8$. From the previous discussion we have that $\bar{\rho}(\mathscr{G}_K)$ contains an element of order 8 and $|\bar{\rho}(\mathscr{G}_K)| = 8$, hence $\bar{\rho} \simeq C_8$.

- $C_2^+ \leftrightarrow C_4$. Indeed, C_2^+ is generated by a 2^2-cycle that correspond to a matrix of order 4 in $\mathrm{GL}_2(\mathbb{F}_3)$. Since the size of $\bar{\rho}(\mathscr{G}_K)$ is 4 then the result follows.

□

Remark 3.5.3. When we study Galois representations with value in $\mathrm{GL}_2(\mathbb{F}_p)$ it is usual to express their image in term of Cartan subgroups, normalisers of Cartan subgroups, Borel subgroups and exceptional subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. Consider $\bar{\rho}(\mathscr{G}_K) \simeq C_8$. This is a maximal abelian group in $\mathrm{GL}_2(\mathbb{F}_3)$. It contains $\pm\mathrm{Id}$ and 2 matrices whose characteristic polynomial is $x^2 + 1$ and 4 matrices with characteristic polynomials $x^2 \mp x - 1$. But then it is a set of commuting matrices that are separately diagonalisable over $\mathbb{F}_{3^2}$. This implies that all such matrices can be simultaneously diagonalised over $\mathbb{F}_{3^2}$. Thus C_8 is a *nonsplit Cartan* subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. A straightforward calculation shows that its normaliser in $\mathrm{GL}_2(\mathbb{F}_3)$ is the subgroup SD_{16}. Hence, SD_{16} is the *normaliser* of a Cartan subgroup.

Now, we have that $D_4, Q_8 \subset SD_{16}$. This can be deduced from the fact the D_4, Q_8 are the lifts of $V_4^-, V_4^+ \subset D_4$ respectively, and since SD_{16} is the lift of D_4 then the claim follows. Thus, we can say that D_4, Q_8 are in the normaliser of a nonsplit Cartan subgroup but not contained in the nonsplit Cartan. However, we can say more about the D_4 image. Indeed, it contains the following matrices $\pm\mathrm{Id}, g$ with g a matrix with characteristic polynomial x^2-1. It is easy to see that they form an abelian group H, and it is maximal in $\mathrm{GL}_2(\mathbb{F}_3)$. Since each element is diagonalisable over $\mathbb{F}_3$ then H is a *split Cartan subgroup*. Moreover, a straightforward computation shows that D_4 is its normaliser and $[D_4 : H] = 2$. Hence we can conclude that D_4 is the *normaliser of a split Cartan* subgroup. The subgroup $\bar{\rho}(\mathscr{G}_K) \simeq C_4$ contains $\pm\mathrm{Id}$ and 2 other matrices with characteristic polynomial x^2+1. Hence, C_4 is contained in a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Finally, the last two possibilities $\mathrm{GL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)$ are clearly not contained in any normaliser of Cartan subgroups or Borel subgroups. Their images in $\mathrm{PGL}_2(\mathbb{F}_3)$ are isomorphic to S_4 and A_4, so *exceptional* subgroups. We summarise this information in the next table. We use the labels introduced by Sutherland in [43]. We will use **Cn** for a nonsplit Cartan subgroup, **Nn** the Normaliser of a nonsplit Cartan subgroup, **Ns** the Normaliser of a split Cartan subgroup.

$\tilde{\rho}(\mathscr{G}_K)$	$\bar{\rho}(\mathscr{G}_K)$	Type of subgroup
S_4	$\mathrm{GL}_2(\mathbb{F}_3)$	exceptional
A_4	$\mathrm{SL}_2(\mathbb{F}_3)$	exceptional
V_4^+	Q_8	contained in a **Nn** but not in **Cn**
V_4^-	D_4	**Ns**
D_4	SD_{16}	**Nn**
C_4	C_8	**Cn**
C_2^+	C_4	contained in a **Cn**

3.5.2 A first method

In this paragraph we present a first method to determine the Galois extension M/K corresponding to the fixed field of $\bar{\rho}$. By Proposition 3.5.1 we know that $[M : L] = 2$; thus, by Kummer theory we have $M = L(\sqrt{\alpha})$ for α in the finite group

$$L(S_L, 2) := \left\{\alpha \in L^\times/(L^2)^\times \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 2,\ \forall\, \mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_L) \setminus S_L\right\}.$$

Moreover, since we need M/K Galois then α must be in $L(S_L, 2)^{\mathscr{G}_K}$, the fixed subgroup by the natural action of $\mathscr{G}_K$ on $L(S_L, 2)$. Now, $L(S_L, 2)^{\mathscr{G}_K}$ is a finite

dimensional vector space over $\mathbb{F}_2$ and its basis as vector space is in one-to-one correspondence with a 2-basis $T_2(L)$ for L. This is explicitly presented in [5, Chapter 3], where $T_2(L)$ is presented without the use of the class field theory. Finally, it is shown how to identify quadratic extensions unramified outside S. Indeed, if $\alpha_1, \ldots, \alpha_t$ is a basis for $L(S_L, 2)^{\mathscr{G}_K}$ as $\mathbb{F}_2$-vector space then $M = L(\sqrt{\alpha})$ where

$$\alpha = \prod_{i=1}^{t} \alpha_i^{[M|\mathfrak{P}_i]}$$

and $[M|\mathfrak{p}_i] = 0$ (resp. 1) if $\mathfrak{P}_i \in T_2(L)$ is split (resp. is inert) in M (cf. [5, § 3.1] for more details). Thus, we need to prove the following proposition

Proposition 3.5.4. *The extension M/L is uniquely determined by the finitely many characteristic polynomials of $\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ with $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P} \in T_2(L)$.*

Proof. Let $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$ be the prime that lies below a fixed $\mathfrak{P} \in T_2(L)$. Let $F_{\mathfrak{p}}, \bar{F}_{\mathfrak{p}}, \tilde{F}_{\mathfrak{p}}$ be the Frobenius elements associated to $\mathfrak{p}$ in $\mathscr{G}_K$, its projection onto the quotient $\mathrm{Gal}(M/K) \simeq \bar{\rho}(\mathscr{G}_K)$, and in $\mathrm{Gal}(L/K) \simeq \tilde{\rho}(\mathscr{G}_K)$ respectively. Therefore, $\mathrm{ord}(\bar{F}_{\mathfrak{p}})$, $\mathrm{ord}(\tilde{F}_{\mathfrak{p}})$ are equal to the order of the matrices $\bar{\rho}(F_{\mathfrak{p}}) \in \mathrm{GL}_2(\mathbb{F}_3)$, and $\tilde{\rho}(F_{\mathfrak{p}}) \in \mathrm{PGL}_2(\mathbb{F}_3)$ respectively (up to conjugacy). Furthermore, the splitting behaviour of $f \bmod \mathfrak{p}$ tell us the order of $\tilde{\rho}(F_{\mathfrak{p}}) \in \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$. Now, if $\tilde{\rho}(F_{\mathfrak{p}})$ has order 4 then it must be a 4-cycle. On the other hand, if it has order 2 we need to look at $\det(\tilde{\rho}(F_{\mathfrak{p}}))$ and if it is -1 (resp. 1) then $\tilde{\rho}(F_{\mathfrak{p}})$ is a 2-cycle (resp. 2^2-cycle). By the Cayley-Hamilton theorem if $\tilde{\rho}(F_{\mathfrak{p}})$ is a 2-cycle, 4-cycle or the product of two disjoint transpositions then its pre-image in $\mathrm{GL}_2(\mathbb{F}_3)$ can be only a matrix of order 2, 8 or 4 respectively. That is

$$\mathrm{ord}(\bar{F}_{\mathfrak{p}}) = \mathrm{ord}(\bar{\rho}(F_{\mathfrak{p}})) = \mathrm{ord}(\tilde{\rho}(F_{\mathfrak{p}})) = \mathrm{ord}(\tilde{F}_{\mathfrak{p}})$$

in the first case and

$$\mathrm{ord}(\bar{F}_{\mathfrak{p}}) = \mathrm{ord}(\bar{\rho}(F_{\mathfrak{p}})) = 2 \times \mathrm{ord}(\tilde{\rho}(F_{\mathfrak{p}})) = 2 \times \mathrm{ord}(\tilde{F}_{\mathfrak{p}})$$

in the last two. By the multiplicative property in towers of the inertia degree, we have that $\mathfrak{P}$ is split in the first case and inert in the others.
On the other hand, when $\tilde{\rho}(F_{\mathfrak{p}})$ is trivial we may have $\bar{\rho}(F_{\mathfrak{p}}) = \mathrm{Id}$ or $-\mathrm{Id}$. Similarly, when $\tilde{\rho}(F_{\mathfrak{p}})$ is of order 3 then $\bar{\rho}(F_{\mathfrak{p}})$ may be a matrix of order 3 or 6. However, by definition of black box representation we know the trace of $\bar{\rho}(F_{\mathfrak{p}})$ and accordingly with the value of $\mathrm{tr}(\bar{\rho}(F_{\mathfrak{p}}))$ we are able to distinguish between $\pm\mathrm{Id}$ or between a

matrix of order 3 and one of order 6. That is we know whether

$$\mathrm{ord}(\bar{F}_{\mathfrak{p}}) = \mathrm{ord}(\tilde{F}_{\mathfrak{p}}) \quad \text{or} \quad \mathrm{ord}(\bar{F}_{\mathfrak{p}}) = 2 \times \mathrm{ord}(\tilde{F}_{\mathfrak{p}});$$

and we the same reasoning as before, we are able to determine the splitting behaviour of $\mathfrak{P}$ in M. □

Thus, applying the proposition to $\mathfrak{P}_i$ for $\mathfrak{P}_i \in T_2(L)$ we are able to compute $[M|\mathfrak{P}_i]$, and hence identify α. Therefore, we have uniquely determined M as $L(\sqrt{\alpha})$.

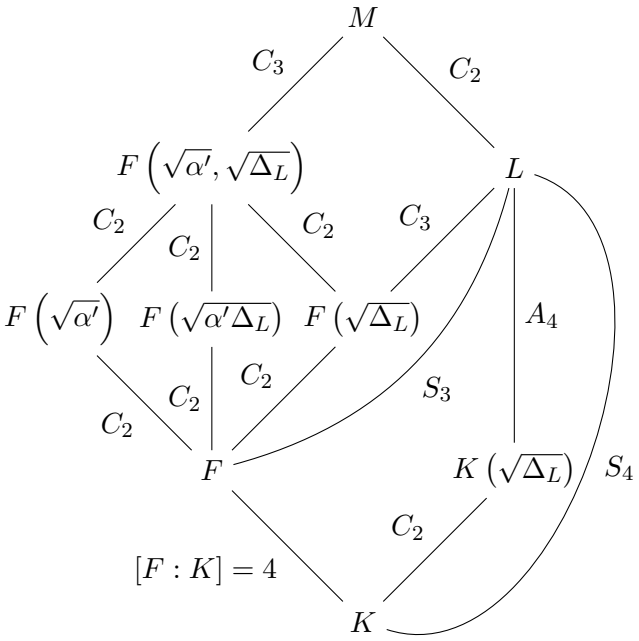
3.5.3 A refined method

While the approach presented in § 3.5.2 certainly give us an answer, it involves computation over a field extension L/K of degree 24 in the worst case. Computationally this might be a problem. For this reason, we prove the following theorem.

Theorem 3.5.5. *Let the projective image $\tilde{\rho}(\mathscr{G}_K)$ be one of the groups $\{S_4, A_4, D_4, V_4^{\pm}, C_4\}$, and let r be a root of f_L. Then the fixed field M/K of $\ker(\bar{\rho})$ is of the form $L(\sqrt{\alpha'})$, with α' in the intermediate extension $F = K(r) \subseteq L$. Such α' can be determined by the black-box data.*

Proof. The statement is trivial when $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^{\pm}$ or C_4 since $F = L$. We examine the remaining cases separately.

Case $\tilde{\rho}(\mathscr{G}_K) \simeq S_4$. We have that $\mathrm{Gal}(M/K) = \mathrm{GL}_2(\mathbb{F}_3)$, and F is the fixed field of a non-normal subgroup of order 12. By the classification of the subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$, as presented for example in GroupNames [22], we see that F is the fixed field of a D_6 subgroup. We have then the following tower of extensions



with $\mathrm{Gal}(M/F) = D_6$, $\mathrm{Gal}(M/K) = \mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{Gal}(F(\sqrt{\alpha'}, \sqrt{\Delta_L})/F) = V_4$. It is clear that $L \cap F(\sqrt{\alpha'}) = F$, i.e. $\alpha' \in L$ is not a square. Hence $M = L(\sqrt{\alpha'})$. This means that in order to find M/K it is enough to determine either α' or $\alpha'\Delta_L$. That is, we are just dealing with quadratic extensions of the degree 4 extension F/K, instead of the degree 24 extension L/K. The next step is to use the black box data over K to determine this pair of quadratic extensions.

Let $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_F) \setminus S_F$ be a prime that splits in $F(\sqrt{\Delta_L})$, and let $\mathfrak{Q}$ be a prime of L that lies above $\mathfrak{P}$. If $\mathfrak{Q}$ is split in M, then following the right path on the diagram of the extensions we have that the order of $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(M/F)$ is odd. Therefore, $\mathfrak{P}$ splits completely in $F(\sqrt{\alpha'}, \sqrt{\Delta_L})$ and hence in each sub-extension. With the same argument we have that when $\mathfrak{Q}$ is inert in M then $\overline{\mathrm{Frob}_{\mathfrak{P}}} \in \mathrm{Gal}(F(\sqrt{\alpha'}, \sqrt{\Delta_L})/F)$ is odd. Since $\mathfrak{P}$ split in $F(\sqrt{\Delta_L})$, that is Δ_L is a square mod $\mathfrak{P}$, then $\mathfrak{P}$ must be inert in both $F(\sqrt{\alpha'})$ and $F(\sqrt{\alpha'\Delta_L})$.
The previous proposition showed that the black box data tells us when a prime $\mathfrak{Q}$ of L is split or inert in M, hence the same data tell us whether $\mathfrak{P}$ is split or inert in the two quadratic sub-extensions. We proceed in the following way

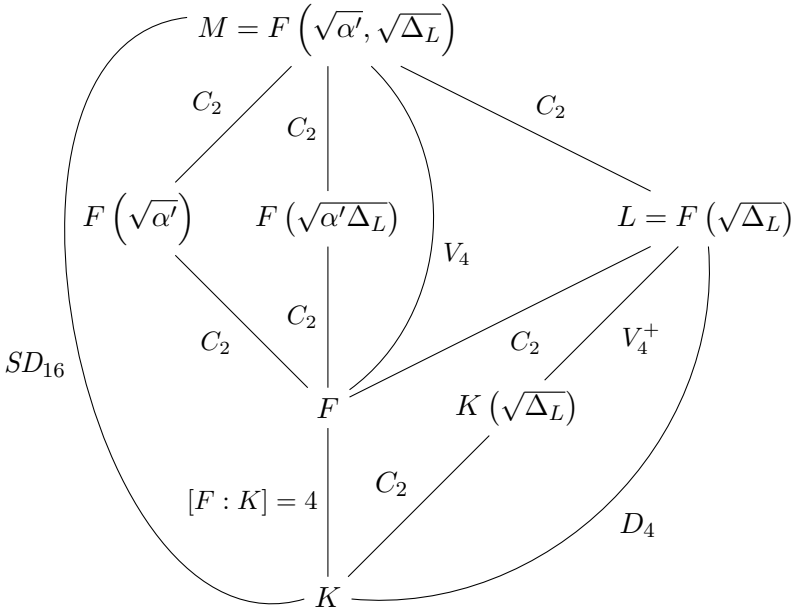
- compute a basis $\alpha_1, \ldots, \alpha_r$ for $F(S_F, 2)$;
- start with an empty set of primes $\mathscr{P}_F$, and with a $0 \times r - 1$ matrix A with values in $\mathbb{F}_2$;

- pick a prime $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_F) \setminus (\mathscr{P}_F \cup S_F)$ such that Δ_L is a square mod $\mathfrak{P}$, i.e. $[F(\sqrt{\alpha_1}) \mid \mathfrak{P}] = 0$, and compute the $\mathbb{F}_2^{r-1}$-vector

$$\mathrm{v} = ([F(\sqrt{\alpha_1}) \mid \mathfrak{P}], \ldots, [F(\sqrt{\alpha_{r-1}}) \mid \mathfrak{P}]);$$

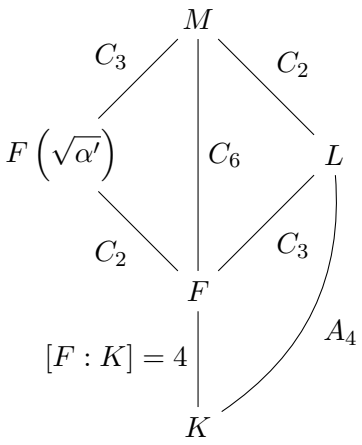
- if v is not in the row-span of A then add $\mathfrak{P}$ to $\mathscr{P}_F$ and add v as a new row of A;
- repeat the last two steps until $\mathrm{rank}(A) = r - 1$, the maximum rank possible.
- using the black box, compute the vector $b = ([M \mid \mathfrak{P}_1]', \ldots, [M \mid \mathfrak{P}_{r-1}]')$ where $[M \mid \mathfrak{P}_i]' = 0$ if $2 \nmid \mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}_i})$ and 1 otherwise;
- Set $x' = A^{-1}b$ and $x = (x', 0)$. Then, without loss of generality set $\alpha' = \prod_{i=1}^{r} \alpha_i^{x_i}$ and we are done.

Case $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$. By Theorem 3.5.2 we have $\bar{\rho}(\mathscr{G}_K) \simeq SD_{16}$. Hence, F is fixed by a subgroup $H < SD_{16}$ of size 4. We have two possibilities either $H \simeq C_4$ or $H \simeq V_4$. However, if F is fixed by a C_4 then it must contain the fixed field of Q_8. If we look at what happens projectively this means that F contains the fixed field of V_4^+ that is $K(\sqrt{\Delta_L})$, that is absurd. Therefore, F is fixed by a V_4 and we have the following lattice of fields:



Therefore, if pick primes $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S_F$ such that $\mathfrak{P}$ splits in L, then we can proceed with exactly the same argument as in the previous case and determine the pair $\alpha', \alpha'\Delta_L$ (up to squares). Hence, we can determine M either as $L(\sqrt{\alpha'})$ or $L(\sqrt{\alpha'\Delta_L})$.

Case $\tilde{\rho}(\mathscr{G}_K) \simeq A_4$. Since $\bar{\rho}(\mathscr{G}_K) \simeq \mathrm{SL}_2(\mathbb{F}_3)$, then F is the fixed field of a C_6. Hence we have the following lattice of fields:



From the diagram it is clear that a prime $\mathfrak{Q} \in \mathrm{MaxSpec}(\mathcal{O}_L) \setminus S_L$ splits or remains inert if and only if the prime $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_F)$ below $\mathfrak{Q}$ has the same behaviour in $F(\sqrt{\alpha'})$. That is $[M|\mathfrak{Q}] = [F(\sqrt{\alpha'})|\mathfrak{P}]$ for $\mathfrak{Q}|\mathfrak{P}$. And as shown in the previous proposition we can compute $[M|\mathfrak{Q}]$ from the black box data. Now, let $T_2(F) = \{\mathfrak{P}_i\}_{i=1}^r$ be a 2-basis for F, $\{\mathfrak{Q}_i \in \mathrm{MaxSpec}(\mathcal{O}_L) \mid \mathfrak{Q}_i|\mathfrak{P}_i\}$, and let $\alpha_1, \ldots, \alpha_r$ be a basis for $F(S_F, 2)$ over $\mathbb{F}_2$. Then we can determine α' (up to squares) as

$$\alpha' = \prod_{i=1}^{r} \alpha_i^{[M|\mathfrak{Q}_i]}.$$

□

Remark 3.5.6. In the S_4 and D_4 cases we have seen that when $\mathfrak{P}$ splits in $F(\sqrt{\Delta_L})$, the splitting behaviour of $\mathfrak{Q}$ in M implies the same behaviour of $\mathfrak{P}$ in $F(\sqrt{\alpha'})$ and $F(\sqrt{\alpha'\Delta_L})$. Under the assumption $\mathfrak{P}$ splits in $F(\sqrt{\Delta_L})$, the converse is also true. Indeed, if $\mathfrak{P}$ is inert in $F(\sqrt{\alpha'})$, then it must be inert also in $F(\sqrt{\alpha'\Delta_L})$ because of our assumption. Hence $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(M/F)$ has the order divisible by 2. Therefore, since $\mathfrak{P}$ splits in $F(\sqrt{\Delta_L})$ we must have $\mathfrak{Q}$ inert in M.
Now, let $\mathfrak{P}$ be split in $F(\sqrt{\alpha'})$, hence it must be split in $F(\sqrt{\alpha'\Delta_L})$. Then $\mathfrak{P}$ is totally split in $E = F(\sqrt{\alpha'}, \sqrt{\Delta_L})$. Therefore $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(M/F)$ has odd order.

We can then conclude that $\mathfrak{Q}$ splits in M as wanted.

3.6 Examples

We present some examples of two dimensional $\mathbb{F}_3$-Galois representations computed with the methods explained in the previous sections. The representations we will present come from the action of the Galois group $\mathscr{G}_K$, for K imaginary quadratic, on the group of the 3-torsion points of an elliptic curve E defined over K. We are aware that this is not the usual way to study the image of such representations since it can be recovered by the 3-torsion polynomial attached to E. We actually compared the information coming from our method and the 3-torsion polynomial to validate our implementation. On the other hand, we will see that the data provided by our method to study the residual representation we will be useful to address the isomorphism question between 3-adic Galois representations. All the elliptic curves considered are taken from the LMFDB database [32]. The code used to compute the examples is joint work with Professor John E. Cremona. The functions to list the field extensions we are interested in are mainly based on the theory developed in [16], [28], and [14]. These particular codes are available in the GitHub CremonaPacetti repository [18].

Now, it is a classic result that the determinant character of an ℓ-adic Galois representation attached to an elliptic curve E is the (ℓ-adic) cyclotomic character. Since we are interested in the mod 3 representation associated to E, then $\det(\bar{\rho}) : \mathscr{G}_K \longrightarrow \mathbb{F}_3^\times$ will be the trivial character if and only if -3 is a square in K. In particular, when $\det(\tilde{\rho})$ is non trivial the quadratic extension it cuts out is $K(\sqrt{-3})$.
We give seven examples, one for each of the possible groups $\tilde{\rho}(\mathscr{G}_K)$.

Example 1. Let E be the elliptic curve defined over $K = \mathbb{Q}(i)$, $i = \sqrt{-1}$, with Weierstrass equation:

$$E : y^2 + (i+1)xy = x^3 + (-i+1)x^2 + (37i-5)x + 88i + 53 \tag{3.11}$$

whose LMFDB label is 2.0.4.1-160.1-a1. First, we need the finite set S of primes of K, that contains the primes of bad reduction of E together with the primes above 3. We have then $S = \{(-i-2),\ (3),\ (i+1)\}$. Obviously -3 is not a square in K therefore the determinant character is non trivial. Hence, if $\tilde{\rho}$ is irreducible then the image is one among S_4, D_4, V_4^-, C_4. Thus, $\mathcal{F}_\Delta$ is the set of quartic polynomials whose splitting field E/K contains $K(\sqrt{-3})$ and is unramified outside S. There

are 102 candidates of such quartics of which 79 have Galois group isomorphic to S_4, 8 are D_4 extensions, 8 are C_4 and 7 are a V_4^-. The final step to determine the projective representation is to compute a distinguishing set of primes for $\mathcal{F}_\Delta$ (see 3.4.1 for the definition) and the test vector $\mathfrak{v} = (\mathrm{tr}(\tilde{\rho}(\mathrm{Frob}_\mathfrak{p}))^2)_{\mathfrak{p}\in T_0} \in \{0,1\}^{|T_0|}$ and see for which of the polynomials $f \in \mathcal{F}_\Delta$ we have $\mathfrak{v}(f) = \mathfrak{v}$. In this example T_0 and the test vector are

T_0	$(2i+5)$	$(i+6)$	$(-5i-4)$	$(-6i-5)$	$(4i+9)$
$\mathfrak{v}$	1	1	0	0	1
	$(10-3i)$	$(10+3i)$	$(-7-8i)$	$(10i-7)$	$(7i-10)$
	1	1	1	1	1
	$(-6i-11)$	$(13-2i)$	$(2i+13)$	$(7i-12)$	$(7i+12)$
	1	0	0	1	1
	$(2i+15)$				
	0				

and finally the fixed field L/K of $\ker(\tilde{\rho})$ is the splitting field of the polynomial

$$f_L = x^4 + (-12i+12)x^2 - 8ix - 24i + 24$$

whose Galois group is S_4. In particular, the mod 3 representation is irreducible and surjective.

We use first the method of § 3.5.2 in order to determine the splitting field of the full mod 3 representation. We need to compute the $T_2(L)$ set for L and then take the primes in K that are below them. In this case T_2 contains 35 primes of L while the number of primes of K below them is 12. To be precise we have

- 7 primes of T_2 are above (7);
- 4 are above (11)
- 4 are above $(2i+3)$;
- 7 are above $(-3i-2)$;
- 1 are above (19);
- 1 are above (23);
- 2 are above $(2i+5)$;
- 2 are above $(-2i+5)$;

- 2 are above $(i-6)$;
- 1 are above $(i+6)$;
- 2 are above $(-5i-4)$;
- 2 are above $(-8i+5)$;

with the following exponent vector $v = ([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)}$

$$(0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0)$$

that uniquely determines the splitting field of $\bar{\rho}$ as $M = L(\sqrt{\alpha})$ with

$$\alpha = \prod_{\mathfrak{P}\in T_2(L)} \alpha_{\mathfrak{P}}^{[M|\mathfrak{P}]}.$$

However, if instead we use Theorem 3.5.5, then we only need 6 primes of K, namely:

$$(2i+3), (-3i-2), (i+6), (i-6), (-6i-5), (5i+6).$$

We can also compare the α's given by the two methods. Let r be a root of f, and let $\gamma \in L$ be such that $L = F(\gamma)$, $F = K(r)$. Then the first method returns $\alpha \in L$ of the form

$$\begin{aligned}
\alpha =&((3559/54060i + 788/13515)r^3 + (-61/9010i + 943/13515)r^2 + \\
&+ (1028/13515i + 13309/13515)r - 39/106i + 163/106)\gamma^5 + \\
&+ ((36961/108120i + 701/36040)r^3 + (47/5406i + 30517/10812)r^2 + \\
&+ (-34477/27030i + 5093/9010)r - 13909/9010i + 194723/9010)\gamma^4 + \\
&+ ((107779/108120i - 542083/108120)r^3 + (16259/1590i + \\
&+ 14073/1060)r^2 + (-13327/5406i - 156107/5406)r + 29676/4505i + \\
&+ 310753/4505)\gamma^3 + ((-310509/36040i - 647087/36040)r^3 + \\
&+ (1146323/13515i + 6821/54060)r^2 + (8089/318i - 28603/318)r + \\
&+ 1320099/9010i + 155457/9010)\gamma^2 + ((-127222/2703i + \\
&- 71131/5406)r^3 + (50803/530i - 166963/1590)r^2 + (2513/27030i + \\
&- 1022537/9010)r + 1803913/9010i - 2509011/9010)\gamma + \\
&+ (-870137/27030i + 284641/18020)r^3 + (-165999/3604i - \\
&+ 1630381/10812)r^2 + (-197763/9010i - 499349/9010)r + \\
&- 461314/4505i - 1668592/4505
\end{aligned}$$

while the second one give us $\alpha' \in F = K(r)$:

$$\alpha' = \left(\frac{3}{53} - \frac{11i}{212}\right) r^3 + \left(\frac{13i}{212} - \frac{19}{212}\right) r^2 + \left(\frac{5}{53} - \frac{62i}{53}\right) r + \frac{83i}{53} - \frac{52}{53}.$$

And as expected $L(\sqrt{\alpha}) = L(\sqrt{\alpha'}) = M$.

Example 2. Let $\bar{\rho}$ be the mod 3 Galois representation attached to the elliptic curve $E : y^2 + xy + (i+1)y = x^3 + (-1)x^2 + (6i+3)x + (-11i+5)$ defined over $K = \mathbb{Q}(i)$. The LMFDB label of E is 2.0.4.1-325.1-a1. The set S of primes of K is $S = \{(-3i-2), (-i-2), (3)\}$ and since -3 is not a square in K we have that $\det(\bar{\rho})$ is nontrivial. Thus, if $\bar{\rho}$ is irreducible then the projective image is isomorphic to one among S_4, D_4, V_4^-, C_4. That is, the fixed field L/K of $\ker(\tilde{\rho})$ is the splitting field of a quartic polynomial f whose splitting field contains $K(\sqrt{-3})$, equivalently $f \in \mathcal{F}_\Delta$. We have 102 candidates of which 75 have Galois group isomorphic to S_4, 24 to D_4, 2 to C_4, and only 1 to V_4^-. The distinguishing set of primes and the test vector are given in the following table

T_0	$(-6i-5)$	$(31-8)$	$(-5i+8)$	$(i+10)$	$(1-10)$
$\mathfrak{v}$	0	1	1	1	1
	$(10-3i)$	$(3i+10)$	$(-8i-7)$	$(7i-10)$	$(6i-11)$
	1	1	1	1	0
	$(7i-12)$	$(2i+15)$			
	0	0			

We obtain that $\bar{\rho}$ is irreducible, $f_L = x^4 - 12i - 9$ is a quartic polynomial that defines L/K, and $\tilde{\rho}(\mathscr{G}_K) \simeq C_4$. Now, we want to determine the quadratic extension M/L such that M/K is Galois with $\mathrm{Gal}(M/K) \simeq \bar{\rho}(\mathscr{G}_K)$. The computation of the set $T_2(L)$ yields 10 of primes of L that are above the following primes of K:

$$[1](7),\ [4](11),\ [1](i+4),\ [1](19),\ [2](i-6),\ [1](3i-8)$$

where the numbers in $[\cdot]$ represent how many primes of $T_2(L)$ are above the prime of K. The corresponding vector $v = ([M|\mathfrak{P}])_{\mathfrak{P} \in T_2(L)}$ is

$$(1,1,1,1,1,1,1,1,1,0).$$

Example 3. Take $K = \mathbb{Q}\sqrt{-1} = \mathbb{Q}(i)$ as ground field and the elliptic curve $E : y^2 = x^3 + x^2 + (-132i+58)x + (-64i+568)$ over K. The LMFDB label for E

is 2.0.4.1-54080.6-a2. As in the previous case $\bar{\rho}$ is the mod 3 Galois representation attached to E. We have $S = \{(i+1), (3), (2i+3), (2i+1)\}$, and $\det(\bar{\rho})$ is non trivial due to -3 not being a square in K. As a consequence, we can restrict to the quartic polynomial $f \in \mathcal{F}_\Delta$. The number of possible extensions is 415, of which 336 are S_4 extensions, 48 are D_4, 16 are C_4, and 15 are V_4^-. In the table below we list the 19 primes of K that are in the distinguishing set with the corresponding test vector.

T_0	$(-3i+10)$	$(-6i-11)$	$(7i+12)$	$(13i-10)$	$(14-9i)$
$\mathfrak{v}$	1	0	1	0	1
	$(17-2i)$	$(-12-13i)$	$(16+9i)$	$(18-5i)$	$(8i+17)$
	0	0	0	1	0
	$(10i-17)$	$(10i+17)$	$(19-6i)$	$(19+6i)$	$(i-20)$
	0	0	0	1	0
	$(14i+15)$	$(7i-20)$	$(10i-19)$	$(20-13i)$	
	0	0	0	0	

With this information we have that $\bar{\rho}$ is irreducible and the image of the projective representation is a V_4^- extension L/K defined by the polynomial $f_L = x^4 + (-48i-48)x^2 + 2304i + 1728$. Next, the set $T_2(L)$ consists of 11 primes of L that lies above the following primes of K

$$[1](7),\ [2](11),\ [2](i-4),\ [2](23),\ [1](2i+5),\ [1](i+6),\ [1](4i+5),\ [1](43)$$

where $[\cdot]$ represent the number of primes of $T_2(L)$ above that prime of K. This leads to the exponent vector

$$([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)} = (1,1,1,0,0,1,1,0,1,0,0).$$

Example 4. Let $\bar{\rho}$ be the mod 3 Galois representation attached to the elliptic curve $E : y^2+(i+1)xy = x^3+ix^2+(238i-310)x+(-2522i+1574)$ defined over $K = \mathbb{Q}(i)$ with $i = \sqrt{-1}$. The LMFDB label for E is 2.0.4.1-27040.6-e2. The set S contains the following primes $\{(i+1), (3), (2i+3), (2i+1)\}$. The determinant character is not trivial as we have seen in Example 1 and 2, therefore we can restrict to $\mathcal{F}_\Delta$. Since the set of primes S of this example and the previous one are the same, and moreover the determinant character is not trivial, then the set $\mathcal{F}_\Delta$ is the same as

in the previous example. Thus we have 415 candidate quartics, of which 336 are S_4 extensions, 48 are D_4, 16 are C_4, and 15 are V_4^-. Furthermore, the distinguishing set of primes of K for $\mathcal{F}_\Delta$ is the same as in Example 3 but with the following test vector $\mathfrak{v}$:

T_0	$(-3i+10)$	$(-6i-11)$	$(7i+12)$	$(13i-10)$	$(14-9i)$
$\mathfrak{v}$	0	0	0	0	0
	$(17-2i)$	$(-12-13i)$	$(16+9i)$	$(18-5i)$	$(8i+17)$
	0	0	0	0	0
	$(10i-17)$	$(10i+17)$	$(19-6i)$	$(19+6i)$	$(i-20)$
	0	0	0	1	1
	$(14i+15)$	$(7i-20)$	$(10i-19)$	$(20-13i)$	
	0	1	0	1	

We have a correspondence with the polynomial $f_L = x^4 - 9x^2 + 6i + 9$ which has Galois group isomorphic to D_4. Thus, $\bar{\rho}$ is irreducible, the image of the projective representation is isomorphic to $D_4 \subset S_4$ and its splitting field L/K is the splitting field of f_L. The computation of the 2-basis $T_2(L)$ consists of 19 primes of L. The primes of K that are below them are

$$[3](7),\ [4](11),\ [3](i-4),\ [2](23),\ [2](2i+5),\ [1](-2i+5),$$
$$[1](31),\ [1](43),\ [1](-6i-5),\ [1](3i-8)$$

with the same notation as in the previous examples for $[\cdot]$. The exponent vector is

$$([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)} = (1,1,1,1,1,1,1,0,0,0,1,1,0,0,0,1,0,0,0).$$

Example 5. Let $K = \mathbb{Q}(a)$ with $a = (1+\sqrt{-3})/2$ be the ground field. Let $\bar{\rho}$ be the mod 3 Galois representation attached to the elliptic curve

$$E : y^2 + (a+1)xy + ay = x^3 + ax^2 + (1300a - 550)x + (-9800a - 7280)$$

defined over K. The LMFDB label of E is 2.0.3.1-124.1-a1. We want our extension be unramified outside the set of primes $S = \{(1-6a),\ (2),\ (1-2a)\}$, and since -3 is a square then the determinant character is trivial. This means we are able to restrict only to polynomial in $\mathcal{F}^+$ and in the case in which the projective representation is irreducible the possible images are A_4, V_4, C_2^+. We have 126 candidate quartics of which 76 have Galois group isomorphic to A_4, 35 to V_4^+, and 15 to C_2^+. We have

T_0	$(6a-5)$	$(3-7a)$	$(1-7a)$	$(9a-7)$	$(9a-8)$
$\mathfrak{v}$	1	1	0	1	1
	$(10a-3)$	$(3-11a)$	$(8-11a)$	$(11a-9)$	$(7-12a)$
	0	1	1	1	1
	$(7-13a)$	$(13a-3)$	$(4-15a)$	$(9-16a)$	$(15a-2)$
	1	1	0	1	1
	$(5-17a)$	$(19a-13)$	$(1-18a)$		
	1	0	0		

where T_0 is the distinguishing set of primes for $\mathcal{F}^+$ and $\mathfrak{v}$ is the test vector. We find a correspondence with the quartic polynomial $f_L = x^4 + (24a-30)x^2 - 8x - 216a + 21$ which has Galois group isomorphic to A_4. As a consequence we have that $\bar{\rho}$ is irreducible, $\tilde{\rho}(\mathscr{G}_K) \simeq A_4$ and the fixed field L/K of $\ker(\tilde{\rho})$ is the splitting field of f_L. In order to determine the splitting field of the residual mod 3 representation we compute $T_2(L)$. In this example we have 24 primes of L that lies above the following primes of K

$$[3](5),\ [6](1-3a),\ [4](3a-2),\ [3](11),\ [3](4a-3),\ [2](1-4a),\ [1](17),\ [2](83)$$

and the black box data yields the following exponent vector

$$([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)} = (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,1,0,0).$$

Example 6. Let K be as in the previous example. Let

$$E : y^2 + axy + ay = x^3 + (-a+1)x^2 + (-692a + 2824)x + (53672a - 12687)$$

be the elliptic curve defined over K, whose LMFDB label is 2.0.3.1-90601.1-c1. Let $\bar{\rho}$ be the residual mod 3 Galois representation attached to E. The determinant character is trivial and the set of primes is $S = \{(1-2a),\ (1-3a),\ (1-7a)\}$. We have 84 candidate quartics of which 80 are A_4 extensions of K, 1 is V_4^+ and 3 are C_2^+. The computation yields

T_0	$(1-6a)$	$(4-7a)$	$(7a-6)$	$(5-9a)$	$(4-9a)$
$\mathfrak{v}$	0	0	0	0	1
	$(9a-2)$	$(1-9a)$	$(9a-8)$	$(10a-7)$	$(10a-3)$
	0	0	1	0	0
	$(11a-2)$	$(12a-5)$	$(7-12a)$	$(7-13a)$	$(13a-10)$
	0	0	0	1	0
	$(5-14a)$	$(1-13a)$	$(13a-12)$	$(3-14a)$	$(11-14a)$
	0	0	0	0	1
	$(4-15a)$	$(19a-12)$			
	0	1			

that corresponds to the polynomial $f_L = x^4 + (-96a + 200)x^2 - 3200a + 2000$. Therefore, $\bar{\rho}$ is irreducible and $L = K_{\ker(\tilde{\rho})}/K$ is the splitting field of f_L. Moreover, the Galois group of f_L is isomorphic to $V_4^+ \subset S_4$, hence $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^+$. Next, we compute $T_2(L)$. It consists of 7 primes of L that are above the following primes of K

$$[1](11),\ [1](1-4a),\ [1](4a-3), [3](3-5a),\ [1](9a-8).$$

The black box data yields the exponent vector

$$([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)} = (1,1,1,1,1,1,1).$$

Example 7. Let E be the elliptic curve defined over $K = \mathbb{Q}((1+\sqrt{-3})/2) = \mathbb{Q}(a)$ with Weierstrass equation

$$E : y^2 + axy + (a+1)y = x^3 + (-a+1)x^2 + (-9a+63)x + (-407a-84).$$

The LMFDB label is 2.0.3.1-67500.1-b1. We have $S = \{(1-2a), (2), (5)\}$ and trivial determinant character. The are 138 candidate quartic fields of which 88 are A_4-extensions, 35 are V_4^+, and 15 are C_2^+. In this example we have 28 primes of K in T_0. In the table below we present them together with the test vector

T_0	$(6a-5)$	$(10a-7)$	$(10a-3)$	$(3-11a)$	$(8-11a)$
$\mathfrak{v}$	1	1	1	0	0
	$(11a-9)$	$(11a-2)$	$(12a-5)$	$(7-12a)$	$(7-13a)$
	0	0	1	1	0
	$(6-13a)$	$(13a-10)$	$(13a-3)$	$(5-14a)$	$(1-13a)$
	0	1	1	1	0
	$(11-14a)$	$(16a-7)$	$(9-16a)$	$(15a-13)$	$(6-17a)$
	0	0	0	1	0
	$(5-17a)$	$(10-19a)$	$(9-19a)$	$(19a-16)$	$(13-21a)$
	1	1	1	0	0
	$(3-20a)$	$(14-27a)$	$(28a-19)$		
	1	0	0		

which agree with the vector corresponding to the quartic polynomial $f_L = x^4 - 25x^2 + 100$. Since the Galois group of f_L is isomorphic to $C_2^+ \subset S_4$ we have that $\bar{\rho}$ is irreducible, $\tilde{\rho}(\mathscr{G}_K) \simeq C_2^+$, and $L_{\ker(\tilde{\rho})}/K$ is the splitting field of f_L. The 2-basis $T_2(L)$ consists of 6 primes of L that are above the following primes of K

$$[1](3a-2),\ [1](11),\ [1](1-4a),\ [1](17),\ [1](3-5a),\ [1](1-6a).$$

The test vector is $([M|\mathfrak{P}])_{\mathfrak{P}\in T_2(L)} = (1,0,1,1,1,0)$.

3.7 Proving Equivalence

In this section, we want to discuss how the theory and the methods defined so far lead to a method to prove whether two Galois representations $\bar{\rho}_1, \bar{\rho}_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ are equivalent. A key ingredient for this section is the Brauer-Nesbitt theorem (see Theorem 1.2.5).

In view of Proposition 3.1.4, we have that $\bar{\rho}_1 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ is absolutely irreducible if and only if

$$\bar{\rho}_1(\mathscr{G}_K) \in \{\mathrm{GL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3), SD_{16}, Q_8, D_4\}\,.$$

Thus, if we prove that $\bar{\rho}_1, \bar{\rho}_2$ have the same trace then the Brauer-Nesbitt theorem assert that $\bar{\rho}_1 \simeq \bar{\rho}_2$ (see Theorem 1.2.5). Obviously we want to prove the equivalence even when the image is only irreducible, that is $\bar{\rho}_i(\mathscr{G}_K) \in \{C_8, C_4\}$. This is possible and we have the following

Theorem 3.7.1. *Let K be a number field, S a finite set of primes of K and let $\bar{\rho}_1, \bar{\rho}_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ be two irreducible Galois representations unramified outside S. Then there exists a finite and computable set of primes Σ_0 of K disjoint from S such that*

$$\bar{\rho}_1 \sim \bar{\rho}_2 \iff \mathrm{tr}(\bar{\rho}_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\bar{\rho}_2(\mathrm{Frob}_{\mathfrak{p}})) \quad \forall\, \mathfrak{p} \in \Sigma_0.$$

Proof. With the theory developed in the previous chapter and section we are able to check whether $\bar{\rho}_1, \bar{\rho}_2$ have the same determinant character, are irreducible, and if irreducible whether they have the same splitting field. Indeed, by Corollary 2.0.6, Proposition 3.4.3, and Theorem 3.5.5, it is enough to check that the traces agree at all the primes $\mathfrak{p} \in T_2(K) \cup T_0 \cup T_2(F)$, here F/K is the extension presented in Theorem 3.5.5. If for one $\mathfrak{p}$ we have $\mathrm{tr}(\bar{\rho}_1(\mathrm{Frob}_{\mathfrak{p}})) \neq \mathrm{tr}(\bar{\rho}_2(\mathrm{Frob}_{\mathfrak{p}}))$ then we can conclude that $\bar{\rho}_1, \bar{\rho}_2$ are not equivalent. So we may assume from this point on that $\bar{\rho}_1, \bar{\rho}_2$ have the same determinant character and the same splitting field. It is fundamental to notice that since they have the same splitting field then

$$\mathrm{ord}(\bar{\rho}_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{ord}(\bar{\rho}_2(\mathrm{Frob}_{\mathfrak{p}})) \text{ for all primes } \mathfrak{p} \notin S.$$

Now, $\mathrm{GL}_2(\mathbb{F}_3)$ has the property that the elements different from $-I$ of order n with $n \neq 8$ are all conjugate. The elements of order 8 are instead split into two conjugacy classes of same size. Furthermore, if g_1, g_2 are two elements of order 8 lying in distinct conjugacy classes then $\mathrm{tr}(g_1) = 1 \neq -1 = \mathrm{tr}(g_2)$. Assume that $\bar{\rho}_i(\mathscr{G}_K) \in \{\mathrm{SL}_2(\mathbb{F}_3), Q_8, D_4\}$ then they are absolutely irreducible and they do not contain any elements of order 8. But then the traces agree at all primes not in S, and by Chebotarev and the fact that $\bar{\rho}_i$ $i = 1, 2$ are continuous we deduce $\mathrm{tr}(\bar{\rho}_1(\sigma)) = \mathrm{tr}(\bar{\rho}_2(\sigma))$ for all $\sigma \in \mathscr{G}_K$. Then, by the Brauer-Nesbitt theorem $\bar{\rho}_1 \sim \bar{\rho}_2$.

Assume now $\bar{\rho}_i(\mathscr{G}_K) \simeq G \in \{\mathrm{GL}_2(\mathbb{F}_3), SD_{16}\}$. This time we have elements of order 8 and in both groups are split into two conjugacy classes of same size. Since, $\bar{\rho}_1, \bar{\rho}_2$ have the same splitting field then they induce $\phi \in \mathrm{Aut}(G)$ such that:

$$\phi : \bar{\rho}_1(\mathscr{G}_K) \xrightarrow{\sim} \bar{\rho}_2(\mathscr{G}_K)$$

In particular, we have two very basic properties:

1) ϕ preserves the order of the elements, therefore the trace at the primes with order not 8 agree.

2) the conjugacy class of an element $g \in \bar{\rho}_1(\mathscr{G}_K)$ ϕ is mapped onto the conjugacy class of $\phi(g) \in \bar{\rho}_2(\mathscr{G}_K)$.

Then 1) and 2 imply that if $\mathrm{tr}(\bar{\rho}_1(\mathrm{Frob}_\mathfrak{p})) = \mathrm{tr}(\bar{\rho}_2(\mathrm{Frob}_\mathfrak{p}))$ for a single element $\mathrm{Frob}_\mathfrak{p}$ of order 8, then the trace at all elements of order 8 agree, and hence at all primes not in S, and we can conclude $\bar{\rho}_1 \sim \bar{\rho}_2$ in the same way as before.

We have just two cases left: $\{C_8, C_4\}$. In the C_4 case, we have that the image of $\bar{\rho}_1, \bar{\rho}_2$ is generated by a single element $\sigma \in \mathscr{G}_K$ of order 4. Without loss of generality, we may assume $\sigma = \mathrm{Frob}_\mathfrak{p}$ for a prime $\mathfrak{p} \notin S$. Since the elements of order 4 in $\mathrm{GL}_2(\mathbb{F}_3)$ are all conjugate, then we can conjugate the generator and therefore they are equivalent.

When $\bar{\rho}_i(\mathscr{G}_K) \simeq C_8$, again we may assume without loss of generality that the generator of both the images is $\mathrm{Frob}_\mathfrak{p}$ for the same prime $\mathfrak{p} \notin S$. From what we have said about the conjugacy classes of elements of order 8, we have that if the traces of the two representations agree at $\mathrm{Frob}_\mathfrak{p}$ then we can conjugate the generators and therefore the representations are equivalent. □

Remark 3.7.2. In the previous proof we can see that if $\bar{\rho}_1, \bar{\rho}_2$ have image in $\{\mathrm{SL}_2(\mathbb{F}_3), Q_8, C_4\}$ then having the same splitting field is enough to conclude that they are equivalent. On the other hand, in the other irreducible cases, we need to prove that they have the same splitting field, and they agree at one prime whose associated Frobenius has order 8. In all the cases we have tested there was always a prime of order 8 in the set T_0 used to prove the equivalence of splitting fields, so there was no need to search for other primes. Finally, if the representations are not equivalent, we are always able to provide a witness prime $\mathfrak{p} \notin S$ that certifies this result.

Chapter 4

Reducible 2-dimensional Galois representations over $\mathbb{F}_3$

In this chapter and the next one, we follow the ideas presented in [5, § 5] and extend them to the 3-adic case. In this section, we will use the terminology and basic results on the Bruhat-Tits trees, references are [6] and [4, Section 2.2].

Let $\rho : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_3)$ be a continuous Galois representation unramified outside a finite set of primes S. Let $\Lambda \subset \mathbb{Q}_3^2$ be a stable $\mathbb{Z}_3$-lattice under the action of ρ. Then after fixing a $\mathbb{Z}_3$-basis for Λ we can think ρ as an integral representation, that is $\rho : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_3)$. Let $\bar{\rho} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ be its residual mod3 representation, and let $\tilde{\rho} : \mathscr{G}_K \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ be its projective representation.. If we assume $\bar{\rho}$ reducible, then we have more than one stable lattice (up to homotheties) under the action of ρ. As presented in [4, Example 3, p. 13] determining the projective image and its splitting field is not a well-defined question since it might depend on which stable lattice we are considering to construct the integral representation. Hence, a possible first step for a better understanding of a projective reducible representation it might be knowing how many non-homothetic stable lattices we have.

The aim of the chapter is to present a method to determine whether there are exactly two non-homothetic lattices. We will see that if there are exactly two stable lattices (up to homotheties), we can determine the two projective images and their corresponding splitting fields. As in the previous chapters, we achieve this goal computing finitely many characteristic polynomials of the residual representation $\bar{\rho}$.

For the rest of the chapter we assume that $\bar{\rho}$ is reducible. By Remark 3.1.2 we can choose a $\mathbb{Z}_3$-basis for $\Lambda = \langle v, w \rangle$ such that for all $\sigma \in \mathscr{G}_K$ we have

$$\rho(\sigma) = \begin{pmatrix} \lambda_1(\sigma) + 3a(\sigma) & b(\sigma) \\ 3c(\sigma) & \lambda_2(\sigma) + 3d(\sigma) \end{pmatrix}$$

where $\lambda_1, \lambda_2 : \mathscr{G}_K \longrightarrow \{\pm 1\} \subset \mathbb{Z}_3^\times$ and $a, b, c, d : \mathscr{G}_K \longrightarrow \mathbb{Z}_3$ are functions. Note that the mod 3 reductions of λ_1, λ_2 are multiplicative characters. The action of $\rho(\sigma)$ on the basis vectors v, w is

$$v \mapsto \ (\lambda_1(\sigma) + 3a(\sigma))v + 3c(\sigma)w = A(\sigma)v + C(\sigma)w; \tag{4.1}$$

$$w \mapsto \quad b(\sigma)v \ + \ (\lambda_2(\sigma) + 3d)w = b(\sigma)v + D(\sigma)w. \tag{4.2}$$

Remark 4.0.1. If we conjugate ρ by the matrix $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ we obtain an equivalent integral representation with the roles of b and c swapped.

Since $\bar{\rho}$ is reducible we know there exists at least one stable sublattice Λ' of Λ under the action of ρ non-homothetic to Λ.

Now, we may change the basis for Λ and rescale it by a suitable power of 3 if needed and assume that Λ' is an index 3 sublattice of Λ [6, Proposition 1.3]. An important property is that such lattices are in one-to-one correspondence with one dimensional subspaces of $\mathbb{F}_3^2$ [6, Lemma 1.2]. Therefore we have exactly 4 (non homothetic) sublattices of Λ with index 3 and they are:

- $\Lambda_1 = \langle v, 3w \rangle = \{\alpha v + \beta w \mid \beta \equiv 0 \bmod 3\}$;
- $\Lambda_2 = \langle 3v, w \rangle = \{\alpha v + \beta w \mid \alpha \equiv 0 \bmod 3\}$;
- $\Lambda_3 = \langle v + w, 3w \rangle = \{\alpha v + \beta w \mid \alpha \equiv \beta \bmod 3\}$;
- $\Lambda_4 = \langle v - w, 3w \rangle = \{\alpha v + \beta w \mid \alpha \equiv -\beta \bmod 3\}$.

To see how ρ acts on Λ_i is enough to apply (4.1) and (4.2) to the basis of the lattice:

$$\begin{aligned}
\rho \cdot \Lambda_1 &= \{\alpha v + \beta w \mid \alpha = \alpha'(A + 3b),\ \beta = 3\beta'(c + D);\ \alpha', \beta' \in \mathbb{Z}_3\} \\
&\subseteq \{\alpha v + \beta w \mid \beta \equiv 0 \bmod 3\} = \Lambda_1; \\
\rho \cdot \Lambda_2 &= \{\alpha v + \beta w \mid \alpha = \alpha'(3A + b),\ \beta = \beta'(3C + D);\ \alpha', \beta' \in \mathbb{Z}_3\}; \\
\rho \cdot \Lambda_3 &= \{\alpha v + \beta w \mid \alpha = \alpha' A + (\alpha' + 3\beta')b,\ \beta = \alpha' C + (\alpha' + 3\beta')D;\ \alpha', \beta' \in \mathbb{Z}_3\}; \\
\rho \cdot \Lambda_4 &= \{\alpha v + \beta w \mid \alpha = \alpha' A + (3\beta' - \alpha')b,\ \beta = \alpha' C + (3\beta' - \alpha')D;\ \alpha', \beta' \in \mathbb{Z}_3\}.
\end{aligned}$$

By the properties that α, β must satisfy to have $\alpha v + \beta w \in \Lambda_i$ we deduce that:

- Λ_1 is stable under the action of ρ;

- Λ_2 is stable if and only if $b \equiv 0 \bmod 3$;

- Λ_3 is stable if and only if $b \equiv \lambda_2 - \lambda_1 \bmod 3$;

- Λ_4 is stable if and only if $b \equiv \lambda_1 - \lambda_2 \bmod 3$.

Hence if b does not satisfy the listed conditions then Λ_1 is the unique index 3 stable sublattice of Λ. This is not enough to conclude that Λ and Λ_1 are the only two stable lattices (up to homotheties) under the action of ρ because we may have a stable sublattice $\Lambda'' \subset \Lambda_1$ non homothetic to Λ and Λ_1. As before we may assume that Λ'' is an index 3 sublattice of Λ_1 and we have 4 index 3 sublattices:

- $\Lambda_5 = \langle v, 9w \rangle = \{\alpha v + \beta w \mid \beta \equiv 0 \bmod 9\}$;

- $\Lambda_6 = \langle v + 3w, 9w \rangle = \{\alpha v + \beta w \mid 3\alpha \equiv \beta \bmod 9\}$;

- $\Lambda_7 = \langle v - 3w, 9w \rangle = \{\alpha v + \beta w \mid 3\alpha \equiv -\beta \bmod 3\}$;

- $\Lambda_8 = \langle 3v, 3w \rangle = 3\Lambda$;

where we exclude Λ_8 since it is homothetic to Λ. Working exactly as before we can deduce the following:

- Λ_5 is stable if and only if $c \equiv 0 \bmod 3$;

- Λ_6 is stable if and only if $c \equiv \lambda_2 - \lambda_1 \bmod 3$;

- Λ_7 is stable if and only if $c \equiv \lambda_1 - \lambda_2 \bmod 3$.

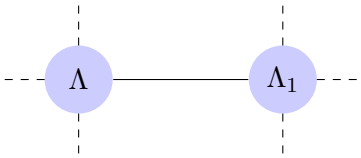
Thus, the behaviour of $b, c \bmod 3$ determine whether there are more than two non-homothetic stable lattices.

Definition 4.0.2. We say that ρ determines a **small isogeny class** if and only if there are exactly two stable lattices up to homothety. Otherwise, we say that ρ determines a **large isogeny class**.

Now, when $\det(\bar{\rho}) = 1$ then the conditions for $\Lambda_2, \Lambda_3, \Lambda_4$ are actually the same, so if one of them is stable then all of them are stable. In particular, $b \equiv 0 \bmod 3$ and therefore $\bar{\rho}(\mathscr{G}_K) \subset \{\pm I\}$. Under this determinant hypothesis the same holds for $\Lambda_5, \Lambda_6, \Lambda_7$, but this time we have $\overline{\rho_1}(\mathscr{G}_K) \subset \{\pm I\}$ with ρ_1 the equivalent representation

$$\rho_1 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \rho \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1}.$$

In this case, when the isogeny class is large, the associate Bruhat-Tits tree (see [4, § 2.2.1, p.8]) is of the form



If instead we have $\det(\bar{\rho}) = -1$ then each condition is distinct. Thus, we may have exactly one stable sublattice (up to homotheties) of index 3 of Λ other than Λ_1, and only one stable sublattice of index 3 of Λ_1 (up to homotheties). In this case when the isogeny class is large then the Bruhat-Tits tree is

In term of residual images we have

- $\bar{\rho}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ if and only if Λ_2 stable;
- $\bar{\rho}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\}$ if and only if Λ_3 stable;
- $\bar{\rho}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \right\}$ if and only if Λ_4 stable;
- $\overline{\rho_1}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ if and only if Λ_5 stable;
- $\overline{\rho_1}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \right\}$ if and only if Λ_6 stable;
- $\overline{\rho_1}(\mathscr{G}_K) \subseteq \left\{ \pm I, \pm \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\}$ if and only if Λ_7 stable.

So if the isogeny class is large, at least one of $\bar{\rho}(\mathscr{G}_K), \overline{\rho_1}(\mathscr{G}_K)$ contains as non trivial matrices only $\pm\gamma$ with characteristic polynomial of γ equal to $x^2 - 1$ (and it must contains at least one since the determinant character is non trivial). But then the image of the attached projective representation is a C_2 subgroup of $\mathrm{PGL}_2(\mathbb{F}_3)$.

In the next section we will present a method to distinguish the two isogeny classes knowing the values of a designed test function $t : \mathscr{G}_K \longrightarrow \mathbb{F}_3$ at a suitable finite set of Frobenius elements.

4.1 Identifying Small Isogeny Classes and Large Isogeny Classes

In Chapter 3 we have seen that the image of the projective representation is a subgroup of S_4. Moreover, in case the representation is reducible then, by the results of §3.3, we have

$$\tilde{\rho}(\mathscr{G}_K) \in \{S_3, C_3, C_2, C_1\},$$

or equivalently, $\tilde{\rho}(\mathscr{G}_K)$ is a subgroup of S_3. If we look the determinant character we have

i) $\tilde{\rho}(\mathscr{G}_K) \in \{C_3, C_1\}$, if $\det(\tilde{\rho})$ is trivial,

ii) $\tilde{\rho}(\mathscr{G}_K) \in \{S_3, C_2\}$, otherwise.

From the discussion of the previous section we have that in *i)* the isogeny class is large if and only if for some stable lattice the image of $\tilde{\rho}$ is C_1, while in *ii)* if and only if $\tilde{\rho}(\mathscr{G}_K) = C_2$ for some Λ stable under the action of ρ.

Now, in case *ii)* let $K_{\det(\bar{\rho})}$ be the non trivial quadratic extension that the determinant character cuts out, and let $\mathscr{G}_{\det} \subset \mathscr{G}_K$ its absolute Galois group. Assume that for one stable lattice $\tilde{\rho}$ has image S_3. When we restrict $\tilde{\rho}$ to $\mathscr{G}_{\det}$ then $\tilde{\rho}(\mathscr{G}_{\det}) \simeq C_3$. Similarly, if $\tilde{\rho}(\mathscr{G}_K) \simeq C_2$ then $\tilde{\rho}(\mathscr{G}_{\det}) \simeq C_1$. That is, if we restrict $\tilde{\rho}$ to $\mathscr{G}_{\det}$ we do not change the small/large isogeny class distinction. In particular, it is enough to develop a method just for case *i)* and apply it to $\tilde{\rho}_{|_{\mathscr{G}_{\det}}}$ when we are in case *ii)*.

In case *i)* we have

$$\rho(\sigma) = \begin{pmatrix} \lambda_1(\sigma) + 3a(\sigma) & b(\sigma) \\ 3c(\sigma) & \lambda_2(\sigma) + 3d(\sigma) \end{pmatrix}$$

with $\lambda_1(\sigma) = \lambda_2(\sigma) = \pm 1 \in \mathbb{Z}_3^{\times}$ for all $\sigma \in \mathscr{G}_K$, that is they are the same map λ. In particular, we can write $\rho(\sigma)$ in the following way

$$\rho(\sigma) = \lambda(\sigma) \begin{pmatrix} 1 + 3\tilde{a}(\sigma) & \tilde{b}(\sigma) \\ 3\tilde{c}(\sigma) & 1 + 3\tilde{d}(\sigma) \end{pmatrix}$$

with $\tilde{b} : \mathscr{G}_K \longrightarrow \mathbb{Z}_3$ such that $\sigma \mapsto \tilde{b}(\sigma) = \lambda^{-1}(\sigma) b(\sigma)$, and similarly $\tilde{a}, \tilde{d}, \tilde{c} : \mathscr{G}_K \longrightarrow \mathbb{F}_3$. This is crucial because now $\chi_{\tilde{b}}(\sigma) := \tilde{b}(\sigma) \bmod 3$ and $\chi_{\tilde{c}}(\sigma) := \tilde{c}(\sigma) \bmod 3$ are two cubic additive characters.

If we compute $\mathrm{tr}(\bar{\rho})$ we know the value of $\lambda(\sigma)$. Hence, when we evaluate the characteristic polynomial $F_\sigma(x) \in \mathbb{Z}_3[x]$ of $\rho(\sigma)$ for $x = \lambda(\sigma)$ we get

$$\begin{aligned} F_\sigma(\lambda(\sigma)) &= \det\left(\rho(\sigma) - \lambda(\sigma)\mathrm{Id}\right) \\ &= \lambda^2(\sigma)[9\tilde{a}(\sigma)\tilde{d}(\sigma) - 3\tilde{b}(\sigma)\tilde{c}(\sigma)] \\ &= 9\tilde{a}(\sigma)\tilde{d}(\sigma) - 3\tilde{b}(\sigma)\tilde{c}(\sigma) \end{aligned}$$

therefore we can define the following test function

$$t(\sigma) = -\frac{1}{3}F_\sigma(\lambda(\sigma)) \pmod 3 = \chi_{\tilde{b}}(\sigma)\chi_{\tilde{c}}(\sigma).$$

Now, let $T_3(S) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a 3-basis of K, $B = \{\mathrm{Frob}_{\mathfrak{p}_i}\}_{i=1}^t$ the associated basis, and $\{\chi_i\}_{i=1}^t$ the dual base of B (see Chapter 2). Therefore

$$\begin{aligned} \chi_{\tilde{b}} = \sum_{i=1}^t x_i\chi_i, \qquad \chi_{\tilde{c}} = \sum_{i=1}^t y_i\chi_i, \\ \chi_{\tilde{b}}(\mathrm{Frob}_{p_i}) = x_i, \quad \chi_{\tilde{c}}(\mathrm{Frob}_{p_i}) = y_i, \end{aligned}$$

with $\mathbf{x} := (x_1, \ldots, x_t), \mathbf{y} := (y_1, \ldots, y_t) \in \mathbb{F}_3^t$. Our aim is to prove whether one of $\mathbf{x}$ and $\mathbf{y}$ is the zero vector of $\mathbb{F}_3^t$. If we compute the test function on the basis elements we get:

$$t(\mathrm{Frob}_{\mathfrak{p}_i}) = x_i y_i.$$

Moreover, each χ in the dual basis cuts out a C_3-extension K_χ of K unramified outside S. For each prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ we have:

$$\chi(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} \pm 1 & \text{if } \mathfrak{p} \text{ is inert in } K_\chi \\ 0 & \text{if } \mathfrak{p} \text{ split in } K_\chi \text{ or } K_\chi/K \text{ is trivial,} \end{cases}$$

that means $\chi(\mathrm{Frob}_{\mathfrak{p}}) = 0$ if and only if $\overline{\mathrm{Frob}}_{\mathfrak{p}} \in \mathrm{Gal}(K_\chi/K)$ is trivial. Since each extension is different, by a standard Chebotarev argument, we can find for each $i \neq j$ a prime $\mathfrak{p}_{i,j}$ such that

$$\chi_i(\mathfrak{p}_{i,j}) = \chi_j(\mathfrak{p}_{i,j}) = 1, \quad \chi_r(\mathfrak{p}_{i,j}) = 0 \ \ \forall 1 \leq r \leq t,\ r \neq i, j.$$

Now, since $t(\mathrm{Frob}_{\mathfrak{p}_{i,j}}) = (x_i + x_j)(y_i + y_j)$ we have

$$t(\mathrm{Frob}_{\mathfrak{p}_{i,j}}) - t(\mathrm{Frob}_{\mathfrak{p}_i}) - t(\mathrm{Frob}_{\mathfrak{p}_j}) = x_i y_j + x_j y_i.$$

The next proposition shows that knowing these quantities for all $1 \leq i \leq j \leq t$ is enough to check whether $\mathbf{x}$ or $\mathbf{y}$ is the zero vector.

Proposition 4.1.1. *$x_i y_i = x_i y_j + x_j y_i = 0$ for all i, j if and only if at least one between $\mathbf{x}$ and $\mathbf{y}$ is equal to $\mathbf{0} \in \mathbb{F}_3^t$.*

Proof. Let $W = (w_{ij})$ be the symmetric matrix such that $w_{ij} = x_i y_j + x_j y_i$. Then the i-th row is of the form

$$\mathbf{w}_i = x_i \mathbf{y} + \mathbf{x} y_i.$$

In particular

$$\mathbf{w}_i = \begin{cases} \mathbf{0} & \text{if } (x_i, y_i) = (0,0) \\ \pm\mathbf{x} & \text{if } (x_i, y_i) = \pm(0,1) \\ \pm\mathbf{y} & \text{if } (x_i, y_i) = \pm(1,0) \\ \pm(\mathbf{x}+\mathbf{y}) & \text{if } (x_i, y_i) = \pm(1,1) \\ \pm(\mathbf{x}-\mathbf{y}) & \text{if } (x_i, y_i) = \pm(1,-1) \end{cases}$$

that easily imply

- $\mathrm{rk}(W) = 2$ if and only if $\mathbf{x} \neq \pm\mathbf{y}$ and both are different from the zero vector,
- $\mathrm{rk}(W) = 1$ if and only if $\mathbf{x} = \pm\mathbf{y} \neq \mathbf{0}$
- $\mathrm{rk}(W) = 0$ if and only if at least one between $\mathbf{x}$, $\mathbf{y}$ is equal to $\mathbf{0} \in \mathbb{F}_3^t$.

□

Thus, to check whether $\chi_{\tilde{b}}$ or $\chi_{\tilde{c}}$ is the trivial character we need to compute the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}}$ for

$$\binom{t+1}{2} = \frac{t(t+1)}{2}$$

primes $\mathfrak{p}$ of K. We denote this set by Σ_1. Note that Σ_1 depends only on K and S. From the previous proposition we have the following corollary

Corollary 4.1.2. *If $\mathrm{rk}(W) \in \{1,2\}$ we can identify, up to sign and up to swapping them, the vectors $\mathbf{x}, \mathbf{y}$. Therefore we know the characters $\chi_{\tilde{b}}, \chi_{\tilde{c}}$, again up to sign and order.*

The proof of the previous corollary is an easy case check which follows from the information given by prop. 4.1.1. However, a more general and elegant proof of the corollary and the cited proposition may be achieved by the theory of quadratic forms. The following argument is due to Prof. John Cremona.

Proposition 4.1.3. *Let* $\mathbf{x} = (x_1, \ldots, x_t), \mathbf{y} = (y_1, \ldots, y_t) \in \mathbb{F}_\ell^t$ *be two vectors of which we only know the quantities* $x_i y_i$ *and* $x_i y_j + x_j y_i$*. Then we can retrieve* $\mathbf{x}, \mathbf{y}$ *up to swapping them and scaling them by* c *and* c^{-1} *for some constant* $c \in \mathbb{F}_\ell^\times$*. Moreover, either* $\mathbf{x}$ *or* $\mathbf{y}$ *is equal to* $\mathbf{0} \in \mathbb{F}_\ell^t$ *if and only if* $x_i y_i = x_i y_j + x_j y_i = 0$ *for all* i, j*.*

Proof. Consider the polynomial ring $R = \mathbb{F}_\ell[U_1, \ldots, U_t],$, which is a unique factorisation domain. The unknown vector $\mathbf{x}$ defines a linear form $L_\mathbf{x} = x_1 U_1 + \cdots + x_t U_t$ which may be 0, and similarly for $\mathbf{y}$. The quadratic form $Q = L_\mathbf{x} L_\mathbf{y}$ has coefficients $x_i y_i$ and $x_i y_j + x_j y_i$ which are known, so we know Q. Since R is a domain then we have that $Q = 0$ if and only if either $L_\mathbf{x} = 0$ or $L_\mathbf{y} = 0$, that is if and only if either $\mathbf{x} = 0$ or $\mathbf{y} = 0$. On the other hand if Q is nonzero then we can factor Q. If Q has two distinct factors then we can retrieve $\mathbf{x}, \mathbf{y}$ up to swapping them and by scaling by c and c^{-1} for some constant $c \in \mathbb{F}_\ell^\times$. Note that $\mathbf{x}, \mathbf{y}$ are linearly independent in this case. Finally, if $Q = cL^2$ for some linear form L then we can take $L_\mathbf{x} = L$ and to obtain $\mathbf{x}$ and then $\mathbf{y} = c\mathbf{x}$. □

In particular, in the case of a small isogeny class determining $\mathbf{x}, \mathbf{y} \in \mathbb{F}_3^t$ is equivalent to determining the two cubic extensions of K that $\bar{\rho}$ cuts out.

Chapter 5

Comparing two irreducible representations

Let K be a number field with ring of integers $\mathcal{O}_K$ and $S \subset \mathrm{MaxSpec}(\mathcal{O}_K)$ a finite set of primes of K. Let $\mathscr{G}_K$ be the absolute Galois group of K. The aim of this chapter is to present an answer to the problem in the introduction:

Problem. *Let K be a number field and S a finite set of primes of K. Fix an algebraic closure $\overline{K}$ of K and let $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Let $\rho_1, \rho_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}(V)$ be two 3-adic Galois representations $\mathscr{G}_K$ such that we only know:*

i) $\dim_{\mathbb{Q}_3} V = 2$*;*

ii) ρ_1, ρ_2 *are both unramified outside S;*

iii) the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}}$ *for each* $\mathfrak{p} \notin S$.

Then is it possible to prove with an effective method that ρ_1 and ρ_2 are equivalent?

Under precise conditions on ρ_1, ρ_2 we have a positive answer, and hence a method, that we will present throughout the following sections. However, for the sake of completeness, we want to present the first part of the theory for a general prime ℓ, before specialising to the 3-adic case.

5.1 The obstruction function θ

In this section, we introduce well-known facts of Galois deformation theory that can be found at [25, Lecture 4] and no originality is claimed. We present the theory

in a more explicit way, to have a better and clearer introduction of the objects we need to study. We prefer to introduce the theory explicitly instead of the general cohomological setting, because we think that gives a deeper insight of the computational approach. A very similar presentation of the argument of this section, but in a general setting, can be found at [8, § 2.3].

Let $\rho_1, \rho_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$ be two ℓ-adic Galois representations unramified outside a finite set of primes $S \subset \mathrm{MaxSpec}(\mathcal{O}_K)$. We assume that for each $\mathfrak{p} \notin S$, the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ is known. We seek an answer to our problem which only requires this information for a finite set of primes $\mathfrak{p}$.
We fix bases for stable lattices to have two integral matrix representations. We assume that ρ_1, ρ_2 have the same determinant character and the same residual representation. The first condition may be checked using the algorithm of Chapter 2 and the second with the tools developed in Chapter 3. We are interested in finding conditions under which the two ℓ-adic representations are isomorphic, i.e. they are isomorphic mod ℓ^k for all $k \geq 1$. To achieve this by induction on k, suppose we already know that ρ_1 is isomorphic to $\rho_2 \bmod \ell^k$ for some $k \geq 1$, and try to extend the isomorphism to ℓ^{k+1}; initially $k = 1$.
Under these conditions we can write $\rho_1(\sigma) = \left(\mathrm{I} + \ell^k\theta(\sigma)\right)\rho_2(\sigma)$, where $\theta : \mathscr{G}_K \longrightarrow \mathrm{M}_2(\mathbb{Z}_\ell)$ is a function. Since, $\det(\rho_1) = \det(\rho_2)$ we have then

$$1 = \det(\mathrm{I} + \ell^k\theta(\sigma)) = 1 + \ell^k \mathrm{tr}\left(\theta(\sigma)\right) + \ell^{2k}\det\left(\theta(\sigma)\right)$$

and dividing by ℓ^k we get $\mathrm{tr}(\theta(\sigma)) \equiv 0 \bmod \ell^k$ for all $\sigma \in \mathscr{G}_K$.
We seek to obtain more information on the function θ. We denote the abelian additive subgroup of trace zero matrices in $\mathrm{M}_2(\mathbb{F}_\ell)$ with $\mathrm{M}_2^0(\mathbb{F}_\ell)$. It is important to notice that $\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $\mathrm{M}_2^0(\mathbb{F}_\ell)$ by conjugation. Therefore, $\mathscr{G}_K$ acts on $\mathrm{M}_2^0(\mathbb{F}_\ell)$ through the mod ℓ representation $\bar{\rho} = \bar{\rho}_1 = \bar{\rho}_2$. Hence we can form the semidirect product $\mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes \mathrm{GL}_2(\mathbb{F}_\ell)$. Consider the following map

$$\begin{aligned} \varphi : \mathscr{G}_K &\longrightarrow \mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes \mathrm{GL}_2(\mathbb{F}_\ell) \\ \sigma &\mapsto (\theta(\sigma) \bmod \ell,\ \bar{\rho}(\sigma)) \end{aligned} \tag{5.1}$$

It is not hard to prove that φ is actually a group homomorphism.

Proposition 5.1.1. *The function φ is a group homomorphism. In particular, the*

map

$$\begin{aligned}\overline{\theta} : \mathscr{G}_K &\longrightarrow \mathrm{M}_2^0(\mathbb{F}_\ell) \\ \sigma &\mapsto \theta(\sigma) \bmod \ell\end{aligned}$$

is a 1-cocycle of $\mathscr{G}_K$ *in* $\mathrm{M}_2^0(\mathbb{F}_\ell)$.

Proof. For $\sigma, \tau \in \mathscr{G}_K$ we have

$$\begin{aligned}\rho_1(\sigma) &= (1 + \ell^k \theta(\sigma))\rho_2(\sigma), \\ \rho_1(\tau) &= (1 + \ell^k \theta(\tau))\rho_2(\tau).\end{aligned}$$

Hence, since a representation is a group homomorphism, we have

$$\begin{aligned}(1 + \ell^k \theta(\sigma\tau))\rho_2(\sigma\tau) = \rho_1(\sigma\tau) =& \rho_1(\sigma)\rho_1(\tau) = \\ =& \rho_2(\sigma)\rho_2(\tau) + \ell^k \theta(\sigma)\rho_2(\sigma)\rho_2(\tau) + \\ &+ \ell^k \rho_2(\sigma)\theta(\tau)\rho_2(\tau) + \ell^{2k}\theta(\sigma)\rho_2(\sigma)\theta(\tau)\rho_2(\tau)\end{aligned}$$

therefore

$$\theta(\sigma\tau) = \theta(\sigma) + \theta(\tau)^{\rho_2(\sigma)} + \ell^k \theta(\sigma)\theta(\tau)^{\rho_2(\sigma)}$$

where x^y denotes the action by conjugation yxy^{-1}. Since $k \geq 1$ we deduce $\theta(\sigma\tau) \equiv \theta(\sigma) + \theta(\tau)^{\rho_2(\sigma)} \bmod \ell$, and thus

$$\begin{aligned}\varphi(\sigma\tau) &= \left(\theta(\sigma) + \theta(\tau)^{\bar{\rho}(\sigma)} \bmod \ell,\ \bar{\rho}(\sigma)\bar{\rho}(\tau)\right) \\ &= \left(\theta(\sigma) \bmod \ell,\ \bar{\rho}(\sigma)\right)\left(\theta(\tau) \bmod \ell,\ \bar{\rho}(\tau)\right) \\ &= \varphi(\sigma)\varphi(\tau),\end{aligned}$$

where the group law comes from the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathrm{M}_2^0(\mathbb{F}_\ell)$ by conjugation. □

A natural question is how $\bar{\theta}$ changes if we substitute ρ_1 with an equivalent representation mod ℓ^k.

Proposition 5.1.2. *If* $\ell \neq 2$ *then* $\bar{\theta}$ *represents a well defined cohomology class* $[\bar{\theta}] \in \mathrm{H}^1\left(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_\ell)\right)$.

Proof. Replace $\rho_1 \bmod \ell^k$ by an equivalent representation $U\rho_1 U^{-1}$, where $U = \left(\mathrm{I} + \ell^k M\right)$ for some $M \in \mathrm{M}_2(\mathbb{Z}_\ell)$. Note that since $U\rho_1 U^{-1} \equiv \rho_2 \bmod \ell^k$ then

$U\rho_1 U^{-1} = (\mathrm{I} + \ell^k\psi)\rho_2$ for some 1-cocycle ψ. In particular we have

$$U\rho_1 U^{-1} = (\mathrm{I} + \ell^k\psi)\rho_2 = U(\mathrm{I} + \ell^k\theta)\rho_2 U^{-1}$$

Since $U^{-1} \equiv \left(\mathrm{I} - \ell^k M\right) \bmod \ell^{k+1}$ we get

$$(1 + \ell^k\psi)\rho_2 \equiv \rho_2 + \ell^k M + \ell^k\theta\rho_2 - \ell^k\rho_2 M \qquad \bmod \ell^{k+1}$$

That implies

$$\bar{\psi} \equiv \bar{\theta} + M - \bar{\rho}M\bar{\rho}^{-1} \qquad \bmod \ell$$

as wanted. Moreover, if we assume $\ell \neq 2$ consider the trace zero matrix $M_0 = M - \frac{c}{2}\mathrm{I}$, where $c = \mathrm{tr}\,(M)$. Then we have

$$(\bar{\psi} - \bar{\theta})(\sigma) = M - \bar{\rho}M\bar{\rho}^{-1} = M_0 - \bar{\rho}M_0\bar{\rho}^{-1}.$$

Hence, the cohomology class of $\bar{\theta}$ is well defined in $\mathrm{H}^1\left(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_\ell)\right)$.

□

For more in the case $\ell = 2$, see [4, chapter 5].
The most critical property the function $\bar{\theta}$ satisfies is the following converse of the previous proposition

Proposition 5.1.3. *If $\bar{\theta}$ is a 1-coboundary for the action of $\mathscr{G}_K$ on $\mathrm{M}_2^0(\mathbb{F}_\ell)$, then there is a representation ρ_1' equivalent to ρ_1 such that $\rho_2(\sigma) \equiv \rho_1'(\sigma) \bmod \ell^{k+1}$.*

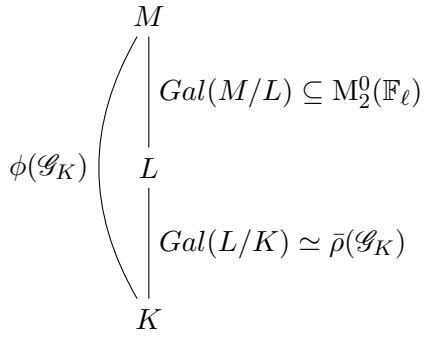
Proof. By the hypothesis we know there exists an $M \in \mathrm{M}_2^0(\mathbb{F}_\ell)$ such that $\bar{\theta} = \bar{\rho}M\bar{\rho}^{-1} - M$. Set $U = \mathrm{I} + \ell^k M$. Then the computation shows that $U\rho_1 U^{-1} \equiv \rho_2 \bmod \ell^{k+1}$. □

The following definition comes naturally from what we have seen.

Definition 5.1.4. We call the function θ the obstruction function and its class in $\mathrm{H}^1\left(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_\ell)\right)$ the obstruction class. It represents the obstruction of extending a congruence $\bmod \ell^k$ between ρ_1 and ρ_2 to one $\bmod \ell^{k+1}$ (after replacing one of the ρ_i by an equivalent representation).

Now, the group homomorphism $\varphi(\cdot) = (\bar{\theta}(\cdot), \bar{\rho}(\cdot))$ cuts out a Galois extension M/K with Galois group isomorphic to $\varphi(\mathscr{G}_K) \subseteq \mathrm{M}_2^0(\mathrm{F}_\ell) \rtimes \bar{\rho}(\mathscr{G}_K)$. Moreover, M

contains the Galois extension L/K cut out by $\bar{\rho}(\mathscr{G}_K)$, that is



If we have two such homomorphisms $\varphi_1 = (\bar{\theta}_1, \bar{\rho})$, $\varphi_2 = (\bar{\theta}_2, \bar{\rho})$ that are $\mathrm{M}_2^0(\mathbb{F}_\ell)$-conjugate, i.e. there exists an element $M \in \mathrm{M}_2^0(\mathbb{F}_\ell)$ such that

$$(M,1)(\varphi_1(\sigma))(M,1)^{-1} = \varphi_2(\sigma) \tag{5.2}$$

for all $\sigma \in \mathscr{G}_K$, then the fixed fields of their kernels are isomorphic. For if we expand (5.2) we see that

$$\begin{aligned}(M,1)(\varphi_1(\sigma))(M,1)^{-1} &= (M,1)(\varphi_1(\sigma))(-M,1)\\ &= (\bar{\theta}_1(\sigma) + M - \bar{\rho}(\sigma)M\bar{\rho}(\sigma)^{-1}, \bar{\rho}(\sigma))\\ &= (\bar{\theta}_2, \bar{\rho}(\sigma)),\end{aligned}$$

that is $\bar{\theta}_1 - \bar{\theta}_2$ is a 1-coboundary for the action of $\mathscr{G}_K$ on $\mathrm{M}_2^0(\mathbb{F}_\ell)$. We have established the following

Lemma 5.1.5. *There is a well defined map Ψ*

- *from cohomology classes $[\bar{\theta}] \in \mathrm{H}^1(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_\ell))$;*
- *to Galois extensions M/K containing L/K, where L is the splitting field of $\bar{\rho}$, with Galois group isomorphic to a subgroup H of*

$$\mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes \bar{\rho}(\mathscr{G}_K) = \mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes Gal(L/K),$$

  which surjects onto the second factor.

Proposition 5.1.6. *If $\ell = 3$ and $\bar{\rho}$ is irreducible then the map Ψ is injective.*

Proof. Let $\mathscr{G}_L$ be the absolute Galois group for L, it is a normal subgroup of $\mathscr{G}_K$ and acts trivially on $\mathrm{M}_2^0(\mathbb{F}_\ell)$. The inflation-restriction sequence then is

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), \mathrm{M}_2^0(\mathbb{F}_\ell)) \longrightarrow H^1(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_\ell)) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}(\mathscr{G}_L, \mathrm{M}_2^0(\mathbb{F}_\ell))^{\mathrm{Gal}(L/K)} \longrightarrow H^2(\mathrm{Gal}(L/K), \mathrm{M}_2^0(\mathbb{F}_\ell)).$$

To prove that Ψ is injective then we need to prove that $H^1(\mathrm{Gal}(L/K), \mathrm{M}_2^0(\mathbb{F}_\ell)) = 0$ for $\mathrm{Gal}(L/K) \in \left\{S_4, A_4, V_4^{\pm}, D_4, C_4, C_2^+\right\}$ (see Proposition 3.1.4). This is achieved easily by a case by case analysis and repeated use of the inflation-restriction sequence. □

Proposition 5.1.6 suggests a possible way to prove whether $[\bar{\theta}]$ is trivial. Indeed, given L/K assume we are able to list all possible extensions M/K as in the proposition. Assume also that we have a method to check whether or not M is *not* the right extension, i.e. whether or not $Gal(M/K) \simeq \varphi(\mathscr{G}_K)$, where φ is defined from ρ_1, ρ_2 and K as in § 5.1. For sure this list contains at least L. Then if we exclude all the possible $M \neq L$, we can conclude that $\varphi(\mathscr{G}_K) \simeq \bar{\rho}(\mathscr{G}_K)$. Hence, $[\bar{\theta}]$ is trivial and so $\rho_1 \simeq \rho_2$ by proposition 5.1.3.
Therefore, we need information about the possible images of $\varphi(\mathscr{G}_K)$ when the two black boxes are equivalent modulo ℓ^k but not modulo ℓ^{k+1}. A first result is the following proposition

Proposition 5.1.7. *Let ρ_1, ρ_2 be such that $\rho_1 \equiv \rho_2 \bmod \ell^k$. Then the group homomorphism $\varphi : \mathscr{G}_K \longrightarrow \mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes \tilde{\rho}(\mathscr{G}_K)$ cuts out a Galois extension M/K with $Gal(M/K)$ isomorphic to a subgroup $H \subseteq \mathrm{M}_2^0(\mathbb{F}_\ell) \rtimes Gal(L/K)$ that is an extension of $\bar{\rho}(\mathscr{G}_K)$ by a subspace W of $\mathrm{M}_2^0(\mathbb{F}_\ell)$ stable under the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Proof. Let $\varphi(\mathscr{G}_K) = H$, and $\pi : H \longrightarrow \bar{\rho}(\mathscr{G}_K)$ the projection. Note that π is surjective. Let $W := \ker(\pi)$, that is $W = \left\{ (\bar{\theta}(\sigma), \bar{\rho}(\sigma)) \mid \bar{\rho}(\sigma) = \mathrm{I},\ \sigma \in \mathscr{G}_K \right\}$. By abuse of notation we identify W with the subspace of $\mathrm{M}_2^0(\mathbb{F}_\ell)$ composed of the $\bar{\theta}(\sigma)$'s. Now, for all $S \in W$ and $g \in \bar{\rho}(\mathscr{G}_K)$ we have that (S, I), $(R, g) \in H$ for some $R \in V^0$. Hence

$$(R, g)(S, \mathrm{I})(R, g)^{-1} \in H,$$

and since $(R, g)^{-1} = (-g^{-1}Rg, g^{-1})$ we get

$$(R, g)(S, \mathrm{I})(R, g)^{-1} = (R + gSg^{-1}, g)(-g^{-1}Rg, g^{-1}) = (gSg^{-1}, \mathrm{I}).$$

Hence $gSg^{-1} \in W$ for all g in $\bar{\rho}(\mathscr{G}_K)$, which means that W is a stable subspace of $\mathrm{M}_2^0(\mathbb{F}_\ell)$. □

On the other hand, by condition *iii*) of our problem we can only compute traces and determinants of our Galois representations. Therefore, we need to find a correspondence between these quantities and the possible $\bar{\theta}$.

Definition 5.1.8. Assume $\rho_1 \equiv \rho_2 \bmod \ell^k$. We define the map

$$\Phi : \mathscr{G}_K \longrightarrow \mathbb{F}_\ell$$

by

$$\sigma \quad \mapsto \frac{\mathrm{tr}(\rho_1(\sigma)) - \mathrm{tr}(\rho_2(\sigma))}{\ell^k} \bmod \ell.$$

We call Φ the *comparison test function.*

Lemma 5.1.9. *Let $\rho_1 \equiv \rho_2 \bmod \ell^k$. Then the following hold:*

$$\Phi(\sigma) = \mathrm{tr}(\bar{\rho}(\sigma)\bar{\theta}(\sigma))$$

for all $\sigma \in \mathscr{G}_K$.

Proof. Simple computation. □

Remark 5.1.10. Clearly if $\rho_1 \simeq \rho_2$ then Φ is the trivial map. On the other hand, when we compute Φ we start with the computation of the ℓ-adic value $\mathrm{tr}(\rho_1(\sigma)) - \mathrm{tr}(\rho_2(\sigma))$ (which we assume to be known exactly–in the application we have in mind, the traces are rational integers whose value is known). Therefore, what we really require is that the two traces agree exactly for each σ, otherwise we can conclude that $\rho_1 \not\sim \rho_2$.

Now, given $\rho_1 \equiv \rho_2 \bmod \ell^k$, we seek a finite set Σ of primes $\mathfrak{p} \notin S$ such that if $\Phi(\mathrm{Frob}_\mathfrak{p}) = 0$ for the primes in this set then $[\bar{\theta}] = 0$, so that by Proposition 5.1.3, after replacing one of the ρ_i by an equivalent representation, we have $\rho_1 \equiv \rho_2$ modulo ℓ^{k+1}.

In the next section we will present a method showing that, under the assumption $\ell = 3$, the combined information coming from the comparison test function with the possible M/K of Proposition 5.1.6 will lead to this result. Moreover, we will see that the finite set Σ is independent of k, depending only on S.

5.2 A 3-adic Faltings-Serre method

We now fix $\ell = 3$. The aim of this section is to prove the following

Theorem 5.2.1. *Let ρ_1, ρ_2 be two 3-adic 2-dimensional black box Galois representations unramified outside a set of primes S of $\mathcal{O}_K$ satisfying*

i) $\det(\rho_1) = \det(\rho_2)$*;*

ii) $\rho_1(\sigma) \equiv \rho_2(\sigma) \bmod 3^k$*, for an integer $k \geq 1$ and for all $\sigma \in \mathscr{G}_K$;*

iii) the common $\bmod 3$ *representation $\bar{\rho}$ is irreducible.*

Let L be the fixed field of $\ker(\tilde{\rho})$*. Suppose that one of the following holds:*

a) the common projective representation $\tilde{\rho} : \mathscr{G}_K \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ is such that

$$\tilde{\rho}(\mathscr{G}_K) \in \left\{S_4, A_4, D_4, V_4^-, V_4^+\right\};$$

b) $\tilde{\rho}(\mathscr{G}_K) \simeq C_4$ and K does not admit any Galois extension M unramified outside S and containing L such that $Gal(M/L) \simeq C_3^2$;

c) $\tilde{\rho}(\mathscr{G}_K) \simeq C_2^+$ and K does not admit any S_3 extension unramified outside S with L as quadratic sub-extension.

Then there exists a finite set of primes $\Sigma \subset MaxSpec(\mathcal{O}_K) \setminus S$, that we call the obstruction set of primes*, such that*

$$\rho_1 \sim \rho_2 \Longleftrightarrow \Phi_{|_\Sigma} = 0.$$

The proof of this theorem will take up the rest of this section.

From the previous chapter we know that if $\bar{\rho}$ is irreducible then $\tilde{\rho}(\mathscr{G}_K) \in \left\{S_4, A_4, D_4, C_4, V_4^-, V_4^+, C_2^+\right\}$. However, at the end of the section it will be clear why the theorem does not always apply to the cases C_4, and C_2^+.

For the reader's convenience we recall how the elements of $\mathrm{GL}_2(\mathbb{F}_3)$ are mapped into S_4.

$g \in \mathrm{GL}_2(\mathbb{F}_3)$	order of $\tilde{g} \in \mathrm{PGL}_2(\mathbb{F}_3)$	cycle structure in S_4
$\mathrm{tr}(g) = 0, \det(g) = 1$	2	2^2
$\mathrm{tr}(g) = 0, \det(g) = -1$	2	$1^2 \cdot 2$
$\mathrm{tr}(g) = \pm 1, \det(g) = 1$	1 or 3	1^4 or $1 \cdot 3$
$\mathrm{tr}(g) = \pm 1, \det(g) = -1$	4	4

The additive abelian group $M_2^0(\mathbb{F}_3)$ is a 3-dimensional vector space over $\mathbb{F}_3$. From the previous table we see that the elements of $\mathrm{PGL}_2\mathbb{F}_3$ that have order 2 lie in $M_2^0(\mathbb{F}_3)$.

For the sake of simplicity, we denote the $\mathbb{F}_3$-vector space $M_2^0(\mathbb{F}_3)$ by V^0. Finally, since $\{\pm \mathrm{I}\}$ acts trivially on this vector space, the action of $\mathscr{G}_K$ on V^0 by $\bar{\rho}$ descends to $\tilde{\rho}$ acting via $\mathrm{PGL}_2(\mathbb{F}_3)$.

Proposition 5.1.6 asserts that we need to know the possible images of the homomorphism $\varphi : \mathscr{G}_K \longrightarrow \mathrm{V}^0 \rtimes \tilde{\rho}(\mathscr{G}_K)$ when the two black boxes are equivalent modulo 3^k but not necessarily modulo 3^{k+1}. Hence, the first step is to understand the action of $\tilde{\rho}(\mathscr{G}_K) \subseteq \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ on V^0.

Proposition 5.2.2. *The subgroups* $\left\{S_4, A_4, D_4, C_4, V_4^-, V_4^+, C_2^+\right\}$ *of* $S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ *act on* $V^0 \simeq \mathrm{M}_2^0(\mathbb{F}_3)$ *in the following way:*

1) *S_4 (resp. A_4) acts irreducibly on V^0;*

2) *as D_4-module (resp. C_4-module) $V^0 \cong W_1 \oplus W_2$, where W_1 and W_2 are simple submodules of dimension 1 and 2 respectively;*

3) *as $V_4^{\pm}$-module (resp. C_2^+-module) V^0 decomposes as the direct sum of three 1-dimensional submodules $V^0 \cong W_1 \oplus W_2 \oplus W_3$.*

Proof. Let $w_1, w_2, w_3 \in \mathrm{GL}_2(\mathbb{F}_3)$ be matrices with characteristic polynomial x^2+1 whose images $\bar{w}_1, \bar{w}_2, \bar{w}_3$ in $\mathrm{PGL}_2(\mathbb{F}_3)$ correspond to the three 2^2-cycles. Then, w_1, w_2, w_3 are a basis for V^0. Note that for all $i \neq j$ we have

$$w_i w_j w_i^{-1} = -w_j. \qquad (*)$$

We analyse each case separately.

$\boldsymbol{\tilde{\rho}(\mathscr{G}_K) \simeq V_4^+}$**.** Since $V_4^+ := \{\mathrm{I}, \bar{w}_1, \bar{w}_2, \bar{w}_3\}$, by $(*)$ we see that $W_i = \langle w_i \rangle$ is stable for $i = 1, 2, 3$ and that the action of V_4^+ on each is nontrivial.

$\boldsymbol{\tilde{\rho}(\mathscr{G}_K) \simeq C_2^+}$**.** We know that $C_2^+ := \{\mathrm{I}, \bar{w}_1\}$ (up to conjugation). From the previous case we get that $W_j = \langle w_j \rangle$ are the three one dimensional stable subspaces of V_0, but this time C_2^+ acts trivially on W_1 and nontrivially on the others.

$\boldsymbol{\tilde{\rho}(\mathscr{G}_K) \simeq A_4}$**.** We have $V_4^+ \lhd A_4$. By the study of the V_4^+ case we deduce that if V_0 decomposes as a sum of nontrivial A_4 modules, then at least one of the factors must be $W_i = \langle w_i \rangle_{\mathbb{F}_3}$. Thus, doing the conjugation in A_4 we must have $\bar{g}\bar{w}_i\bar{g}^{-1} = \bar{w}_i$ for any 3-cycle $\bar{g}$. That is $\bar{w}_i \in Z(A_4)$. But $Z(A_4)$ is trivial, hence this can not happen and V_0 is an irreducible A_4-module.

$\boldsymbol{\tilde{\rho}(\mathscr{G}_K) \simeq C_4}$**.** The nontrivial elements of C_4 are two 4-cycles $\bar{g}, \bar{h}$ and $\bar{g}^2 = \bar{h}^2 = \bar{w}_i$, for some i. Without loss of generality we can assume $i = 1$. Since C_4 is abelian, $W_1 = \langle \bar{w}_1 \rangle_{\mathbb{F}_3}$ is a stable one dimensional subspace. Moreover, the lifting of C_4 in

$\mathrm{GL}_2(\mathbb{F}_3)$ is C_8 (see Theorem 3.5.2), which is an abelian group. Since both the lifts of $\pm w_1$ of $\bar{w}_1$ are in C_8 then the action of C_4 on W_1 is trivial. Now, the subspace $\langle w_2, w_3\rangle_{\mathbb{F}_3}$ is stable under the action of C_4, since $\bar{w}_2, \bar{w}_3 \in V_4^+$ which is normal in S_4. In order to prove that is actually irreducible we look at the action of $\bar{g}, \bar{h}, \bar{w}_1$ on w_2, w_3

$$\bar{g} w_2 \bar{g}^{-1} = w_3, \qquad \bar{g} w_3 \bar{g}^{-1} = -w_2 \tag{5.3}$$

$$\bar{h} w_2 \bar{h}^{-1} = -w_3, \quad \bar{h} w_3 \bar{h}^{-1} = w_2 \tag{5.4}$$

$$\bar{w}_1 w_2 \bar{w}_1^{-1} = -w_2, \quad \bar{w}_1 w_3 \bar{w}_1^{-1} = -w_3 \tag{5.5}$$

which implies that none of the one dimensional subspaces of $\langle w_2, w_3\rangle_{\mathbb{F}_3}$ is stable under the action of C_4, and therefore it is irreducible.

$\tilde{\rho}(\mathscr{G}_K) \simeq D_4$. Since $C_4 \subset D_4$ then as D_4-module V^0 must be irreducible or must be the sum of a two dimensional submodule with a one dimensional one. By basic group theory we have that $Z(D_4) = \langle \bar{w}_i \rangle$. Without loss of generality we may assume $i = 1$. But then $W_1 = \langle w_1 \rangle_{\mathbb{F}_3}$ is stable under the action of D_4, therefore $V^0 = W_1 \oplus W_2$ with W_2 a two dimensional submodule. Moreover, from the previous case we get $W_2 = \langle w_2, w_3 \rangle_{\mathbb{F}_3}$.

$\tilde{\rho}(\mathscr{G}_K) \simeq S_4$. The result for A_4 implies that V^0 is also an irreducible S_4-module.

$\tilde{\rho}(\mathscr{G}_K) \simeq V_4^-$. We have that $V_4^- := \{\mathrm{I}, \bar{w}_1, \bar{\alpha}, \bar{\beta}\}$ (up to conjugation) where $\bar{\alpha}, \bar{\beta}$ are elements of $\mathrm{PGL}_2(\mathbb{F}_3)$ corresponding to 2-cycles of S_4 and such that $\bar{\alpha}\bar{\beta} = \bar{w}_1$. We have seen that $\alpha, \beta \in V_0$, in particular α, β, w_1 form a basis. Now, V_4^- is abelian, therefore each conjugacy class consists only of one element. Hence, the three one-dimensional stable subspaces of V^0 under the action of V_4^- are $W_\alpha = \langle \alpha \rangle$, $W_\beta = \langle \beta \rangle$ and $W_1 = \langle w_1 \rangle$. An easy calculation shows that when $\bar{g} \in V_4^-$ is different from the generator of the stable subspace we are considering, it acts as $-\mathrm{Id}$. Therefore, the action of V_4^- on W_α, W_β, W_1 is not trivial. □

The last proposition, together with Proposition 5.1.7, leads to the following result.

Corollary 5.2.3. *Let ρ_1, ρ_2 be such that $\rho_1 \simeq \rho_2 \bmod 3^k$ but $\rho_1 \not\simeq \rho_2 \bmod 3^{k+1}$. Then $\varphi(\mathscr{G}_K) \subseteq V^0 \rtimes \tilde{\rho}(\mathscr{G}_K)$ is one of the following groups. Here the W_i are the simple submodules from Proposition 5.2.2.*

a) $V^0 \rtimes S_4$ (resp. $V^0 \rtimes A_4$) if $\tilde{\rho}(\mathscr{G}_K) \simeq S_4$ (resp. $\tilde{\rho}(\mathscr{G}_K) \simeq A_4$);

b) $W \rtimes \tilde{\rho}(\mathscr{G}_K)$ where $W \in \{W_1, W_2, V^0\}$ if $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$ or C_4;

c) $W \rtimes \tilde{\rho}(\mathscr{G}_K)$ *where* $W \in \{W_1, W_2, W_3, V^0\}$ *or* $W \simeq W_i \oplus W_j$ *with* $i \neq j$, $i, j \in \{1,2,3\}$ *if* $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^{\pm}$ *or* C_2^+.

Proof. Case *a*) is clear. Cases *b*) and *c*) follow for example from the complete classification of subgroups for the possible $\varphi(\mathscr{G}_K)$ presented in [22]. □

Remark 5.2.4. It will be important later to note how the action of $V_4^{\pm}$ and C_2^+ on their stable submodules is reflected in terms of Galois groups. In the proof of Proposition 5.2.2 we have that $V_4^{\pm}$ acts non trivially on each of the stable subspaces W_1, W_2, W_3. In particular, each element of $V_4^{\pm}$ acts with eigenvalues $1, -1, -1$ (in some order). Then by the corollary, when $W = W_j$ we have $\varphi(\mathscr{G}_K) \simeq C_3 \rtimes V_4 \simeq D_6$. On the other hand, C_2^+ acts trivially on one WV_i and non trivially on the others. Then, as abstract group we have that when $W = W_j$ either $\varphi(\mathscr{G}_K) \simeq C_3 \times C_2 = C_6$ or $\varphi(\mathscr{G}_K) \simeq C_3 \rtimes C_2 = S_3$.

Now, we want to use the test function Φ to prove whether ρ_1 and ρ_2 are equivalent mod ℓ^{k+1}. To do this, we find by direct computation a relation between Φ and the group homomorphism φ.

Proposition 5.2.5. *Let* $\varphi(\sigma) = (\bar{\theta}(\sigma), \tilde{\rho}(\sigma))$ *for a* $\sigma \in \mathscr{G}_K$, *and consider* $\bar{\rho}(\sigma) \in \mathrm{GL}_2(\mathbb{F}_3)$. *Then* $\Phi(\sigma) = 0$ *if and only if the order of* $(\bar{\theta}(\sigma), \bar{\rho}(\sigma))$ *in* $V^0 \rtimes \mathrm{PGL}_2(\mathbb{F}_3)$ *is* ≤ 4.

Proof. By examination of all 27×24 cases, we found that $(\bar{\theta}(\sigma), \bar{\rho}(\sigma)) \in V^0 \rtimes \mathrm{PGL}_2(\mathbb{F}_3)$ has order ≤ 4 if and only if $\mathrm{tr}(\bar{\rho}(\sigma)\bar{\theta}(\sigma)) = 0$. □

Proposition 5.2.6. *For all the possible values of* $\varphi(\mathscr{G}_K)$ *in Corollary 5.2.3 the only ones for which there exists no elements of order* > 4 *are* $W_2 \rtimes C_4$ *and* $W_i \rtimes C_2^+$ *whenever* C_2^+ *does not act trivially on* W_i.

Proof. Consider $G \simeq W_2 \rtimes C_4$. Since our action is faithful, we have $G \simeq C_3^2 \rtimes_1 C_4$ and does not admit any element with order greater than 4. On the other hand, if $G \simeq W \rtimes C_4$ with either $W = V^0$ or $W = W_1 = \langle w_1 \rangle$ (up to conjugation), then we can consider the pair $(w_1, \bar{w_1}) \in G$. An easy computation shows that $(w_1, \bar{w_1})$ has order 6 in G.
Assume $G \simeq W_i \rtimes C_2^+$ where C_2^+ acts nontrivially on W_i. But then $G \simeq C_3 \rtimes C_2 \simeq S_3$ and therefore we do not have elements of order greater than 3. However, if C_2^+ acts trivially on W_i then $G \simeq C_3 \times C_2 \simeq C_6$ and we have an element of order 6.
In the remaining cases, we have always at least one element of order 6. This is because S_4, A_4, V_4^+, D_4 contain all the 2^2-cycles. Indeed, let $\tilde{\rho}(\mathscr{G}_K)$ be isomorphic to one of these groups. Let $\sigma_1, \sigma_2, \sigma_3 \in \mathscr{G}_K$ be any three elements such that

$\tilde{\rho}(\sigma_1), \tilde{\rho}(\sigma_2), \tilde{\rho}(\sigma_3) \in \tilde{\rho}(\mathscr{G}_K) \subseteq \mathrm{PGL}_2(\mathbb{F}_3)$ are three distinct matrices of order 2 with determinant 1. They exist because they are mapped onto the three different 2^2-cycles under the isomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$. When we compute $\mathrm{tr}(\bar{\rho}(\sigma_i)S)$ with S running through all the elements of $\mathrm{M}_2^0(\mathbb{F}_3)$, and for each $i = 1, 2, 3$, we notice that

$$\mathrm{tr}(\bar{\rho}(\sigma_1)S) = \mathrm{tr}(\bar{\rho}(\sigma_2)S) = \mathrm{tr}(\bar{\rho}(\sigma_3)S) = 0$$

if and only if S is the zero matrix. Therefore, for any $S \in \mathrm{M}_2^0(\mathbb{F}_3)$ different from the zero matrix we have $\mathrm{tr}(\bar{\rho}(\sigma_i)S) \neq 0$ for at least one $i = 1, 2, 3$. By Proposition 5.2.5, the pair $(S, \tilde{\rho}(\sigma_i))$ has order 6 as wanted. Finally, from Corollary 5.2.3 and Remark 5.2.4 we have that $C_3 \rtimes V_4^- \simeq D_6 \subseteq G$. Hence, by the structure of D_6, we have that G has elements of order 6 as needed. □

Overview of the method. Proposition 5.2.5 and Proposition 5.2.6 are the core of our method, and unfortunately show also its limitation. First we will show how the method works. From what we have proved in § 3.4 we know the image of $\tilde{\rho}$, and we have completely determined the fixed field L/K of $\ker(\tilde{\rho})$. Thus, we know if we are in case *a*),*b*) or *c*) of Corollary 5.2.3. Let $G \leq V^0 \rtimes \tilde{\rho}(\mathscr{G}_K)$ be one of the possible images of φ, and assume that there exists an element $g \in G$ with order greater than 4. The group $V^0 \rtimes \mathrm{PGL}_2(\mathbb{F}_3)$ is a finite solvable group, hence also so is G. Moreover, the fixed field of $\ker(\varphi)$, is a Galois extension M/K unramified outside S with Galois group $\mathrm{Gal}(M/K)$ isomorphic to G. Therefore, we have finitely many (non-isomorphic) possibilities for the field M. Let $\{M_i\}_{i=1}^t$ be the list of all non-isomorphic such extensions. By a Chebotarev argument for each M_i/K there are infinitely many primes $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$ such that the order of $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(M_i/K) \simeq G$ is greater than 4. Let $\Sigma = \{\mathfrak{p}_i\}_{i=1}^t \subset \mathrm{MaxSpec}(\mathcal{O}_K)$ be a set of these primes, one for each field M_i. If $\Phi(\mathrm{Frob}_{\mathfrak{p}_i}) \neq 0$ for some i then we can conclude that $\rho_1 \not\simeq \rho_2$ since their traces do not agree modulo 3^{k+1}. On the other hand if $\Phi(\mathrm{Frob}_{\mathfrak{p}_i}) = 0$ for all i, then none of the M_i is the fixed field by $\ker(\varphi)$, that means $\varphi(\mathscr{G}_K) \not\simeq G$. But then, if we can repeat this process for all the possible G in our case we can conclude that the cohomology class $[\bar{\theta}] \in \mathrm{H}^1(\mathscr{G}_K, V^0)$ is trivial and therefore we can extend the equivalence of ρ_1, ρ_2 modulo 3^{k+1}.

Hence, in order to use our test function Φ to prove the equivalence of the two representations, we need that for each possible G in cases *a*)-*c*) there exists at least one $g \in G$ with order greater than 4. Unfortunately, Proposition 5.2.6 shows that this does not happen for all possible cases of Corollary 5.2.3.

We have now completed the proof of Theorem 5.2.

Further Ideas

We want to conclude this section with an observation about the cases in which the theorem does not apply. The following comments come from stimulating conversations with Prof. John Cremona and Dr Nuno Freitas. We will define a test function Φ', such that, if we were able to prove specific properties of Φ', then our method could be extended to the cases excluded in Theorem 5.2.

We have seen that if $\tilde{\rho}(\mathscr{G}_K) \simeq C_2^+$ then it acts reducibly on V_0, and the three one-dimensional stable subspaces are generated by the three matrices $w_1, w_2, w_3 \in \mathrm{GL}_2(\mathbb{F}_3)$ having $\det(w_i) = 1$ and $\mathrm{tr}(w_i) = 0$. In exactly one case the method applies since for some j we have $W_j \rtimes C_2^+ \simeq C_6$. However, we see that $\det(\bar{g}w) = 1$ for all $\bar{g} \in \tilde{\rho}(\mathscr{G}_K)$ and all nontrivial $w \in W_i$, $i = 1, 2, 3$.

Now, consider $\tilde{\rho}(\mathscr{G}_K) \simeq C_4$. Let W_1 be the stable one dimensional subspace of V^0. We have seen that C_4 acts trivially on W_1 hence

$$W_1 \rtimes \tilde{\rho}(\mathscr{G}_K) \simeq C_3 \times C_4 \simeq C_{12},$$

and we can apply the method because clearly C_{12} contains elements of order greater then 4. On the other hand, consider $W_2 = \langle w_i, w_j \rangle$, the stable 2-dimensional subspace of V^0 under the action of C_4. An easy calculation shows that any nontrivial element $w \in W_2$ satisfies $\det(w) \neq 0$. But then again $\det(\bar{g}w) \neq 0$ for all $\bar{g} \in \tilde{\rho}(\mathscr{G}_K)$ and all nontrivial $w \in W_2$.

Let k be the greatest positive integer such that ρ_1 is isomorphic to $\rho_2 \bmod 3^k$. Then we have the following

$$\Phi'(\sigma) = \frac{\det\left(\rho_1(\sigma) - \rho_2(\sigma)\right)}{\ell^{2k}} \equiv \det(\bar{\theta}(\sigma)\bar{\rho}(\sigma)) = \det(\bar{\theta}(\sigma)\tilde{\rho}(\sigma)) \mod 3.$$

Proposition 5.2.7. *Let ρ_1, ρ_2 be two Galois representations of $\mathscr{G}_K$ unramified outside a finite set of primes $S \subset MaxSpec(\mathcal{O}_K)$. Assume that $\rho_1 \equiv \rho_2 \mod 3^k$ for some integer $k \geq 1$. Let $\tilde{\rho}$ be the common projective representation. Assume that $\tilde{\rho}(\mathscr{G}_K) \in \left\{C_4, C_2^+\right\}$ and let $W \rtimes \tilde{\rho}(\mathscr{G}_K)$ be isomorphic to either $C_3^2 \rtimes C_4$ or S_3 respectively. If one of the following holds:*

a) $\Phi'(\sigma) = 0$ for all $\sigma \in \mathscr{G}_K$;

b) $\Phi'(\sigma) = 0$ for some $\sigma \in \mathscr{G}_K$ such that $\bar{\theta}(\sigma) \neq 0$;

then $\rho_1 \simeq \rho_2$.

Proof. We have seen that under such hypotheses then $\det(\bar{\theta}(\sigma)\tilde{\rho}(\sigma))$ must be nonzero for all $\sigma \in \mathscr{G}_K$ such that $\bar{\theta}(\sigma) \neq 0$. Therefore, if either condition a) or condition b)

is satisfied then we can exclude all the S_3-extensions and the $C_3^2 \rtimes C_4$ extensions unramified outside S containing the splitting field of $\ker(\tilde{\rho})$. This implies that $[\bar{\theta}] \in H^1(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_3))$ is trivial, and hence by prop. 5.1.3 we can conclude that $\rho_1 \simeq \rho_2$. □

If we were able to verify condition *a*) and *b*) of this last proposition we would be able to extend Theorem 5.2.1 to all the possible images of the irreducible mod 3 representation. Unfortunately at the moment, we have not developed a method to verify them.

5.3 How to list the extensions and build the test set Σ

In this section, we would like to present two methods for listing all the possible extensions cited at the end of the previous section, and how to find the primes to test. The first method is based on class field theory and will use a construction method similar to the one developed in § 2. The second one will recall the philosophy behind the well-known *quartic-field* method [42], showing that it is possible to prove whether two 3-adic black box representation are equivalent just by identifying the splitting field of a degree 6 polynomial. We refer to this method as the *sextic-field* method.

Corollary 5.2.3 implies that when $\tilde{\rho}(\mathscr{G}_K) \simeq S_4$ or A_4, we need to list all Galois extensions of K with Galois group isomorphic to $V^0 \rtimes S_4$ or $V^0 \rtimes A_4$. As abstract groups, these are solvable groups of order 648 and 324 respectively. With the help of the SmallGroup function implemented in GAP [24] we were able to check that there is a unique isomorphism class of groups of order 648, labelled $[648, 703]$ there, such that if G lies in this class, then it has the same number of elements of any fixed order as $V^0 \rtimes S_4$. Furthermore, a conjugacy class of transitive subgroups of S_9, labelled[1] 9T30 in LMFDB [32], lies in this class. Hence, $V^0 \rtimes S_4 \in 9T30$. In the same way, we have $V^0 \rtimes A_4 \in 9T25$, where 9T25 is the LMFDB label of a conjugacy class of transitive subgroups of order 324 in S_9. Moreover, both actions are faithful. We have more cases to analyse when $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$ or V_4^+. First assume that the projective image is D_4, then

$$\varphi(\mathscr{G}_K) \in \left\{V_1 \rtimes D_4, V_2 \rtimes D_4, V^0 \rtimes D_4\right\}.$$

With our code in Sage we are able to specify the action of D_4 on V_1, V_2 and we find

[1] The notation was firstly introduced by Butler and McKay in their paper *The transitive groups of degree up to 11*

that

- D_4 acts on $V_1 \simeq C_3$ via $D_4/C_4 \simeq C_2$;
- D_4 acts faithfully on $V_2 \simeq C_3^2$.

Accordingly to the classification in the GroupNames [22] website we have $V_1 \rtimes D_4 \simeq D_{12}$, $V_2 \rtimes D_4 \simeq S_3 \wr C_2$ and $V^0 \rtimes D_4 \simeq C_3^2 \rtimes D_{12} \simeq C_3 \rtimes (S_3 \wr C_2)$. The LMFDB labels are respectively 12T12, 6T13 and 12T118, that means they are transitive subgroups of S_{12} or S_6.
Now, we have already seen in Remark 5.2.4 that $V_4^{\pm}$ acts non trivially on the three one-dimensional stable subspaces. In particular, we have seen that $V_4^{\pm}$ acts on V_i via $V_4^{\pm}/C_2 \simeq C_2$. Because of this, the action of $V_4^{\pm}$ on $V_i \oplus V_j$ for $i \neq j$ is faithful. As abstract groups then we have

- $V_i \rtimes V_4^{\pm} \simeq D_6$ whose LMFDB label is 6T3;
- $(V_i \oplus V_j) \rtimes V_4^{\pm} \simeq C_3^2 \rtimes V_4 \simeq S_3^2$ whose LMFDB label is 6T9;
- $V^0 \rtimes V_4^{\pm} \simeq C_3^2 \rtimes D_6$ where the action of D_6 on C_3^2 is via $D_6/C_3 \simeq V_4$. The LMFDB label is 12T71.

We summarise these results in the following proposition. The densities may be obtained from the LMFDB pages or the GroupName pages for each group. Indeed, for each one of them, they list (among other information) the conjugacy classes, their sizes and order of their elements.

Proposition 5.3.1. *Assume $\rho_1 \equiv \rho_2 \bmod 3^k$ but $\rho_1 \not\equiv \rho_2$ modulo 3^{k+1}. Then the fixed field of $\ker(\varphi)$ is the splitting field of an irreducible polynomial $f(x) \in K[x]$ of the following degrees*

- $\deg(f) = 9$ *if* $\tilde{\rho}(\mathscr{G}_K) \simeq S_4$ *or* A_4*;*
- $\deg(f) = 6$ *or* $\deg(f) = 12$ *if* $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$ *or* $V_4^{\pm}$.

The density of primes whose Frobenius has order greater than 4 in each extension is

		$order_{\mathfrak{p}} = 6$	$order_{\mathfrak{p}} = 9$	$order_{\mathfrak{p}} = 12$
9T30	$C_3^3 \rtimes S_4$	1/4	2/9	1/6
9T25	$C_3^3 \rtimes A_4$	1/6	4/9	0
12T12	$C_3 \rtimes D_4 \simeq D_{12}$	1/12	0	1/6
6T13	$C_3^2 \rtimes D_4 \simeq S_3 \wr C_2$	1/3	0	0
12T118	$C_3^3 \rtimes D_4 \simeq C_3 \rtimes (S_3 \wr C_2)$	5/12	0	1/6
6T3	$C_3 \rtimes V_4 \simeq D_6$	1/6	0	0
6T9	$C_3^2 \rtimes V_4 \simeq S_3^2$	1/3	0	0
12T71	$C_3^3 \rtimes V_4 \simeq C_3^2 \rtimes D_6$	1/2	0	0

Firstly, if we can write down all such polynomials then we can list all these extensions unramified outside S. Secondly, the factorisation of f modulo a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ tell us the order of $\mathrm{Frob}_{\mathfrak{p}}$.
However, writing down these polynomials is not an easy task so we have developed two alternative methods. Both the proposed methods list all the Galois extensions M/K with Galois group isomorphic to $W \rtimes \tilde{\rho}(\mathscr{G}_K) \subseteq \mathrm{M}_2^0(\mathbb{F}_3) \rtimes \tilde{\rho}(\mathscr{G}_K)$ that contain L, the field cut out by $\ker(\tilde{\rho})$, and such that $\mathrm{Gal}(M/K) \simeq W$. Finally, they will provide an explicit finite set $\Sigma \subset \mathrm{MaxSpec}(\mathcal{O}_K)$ disjoint from S to test via the comparison test function Φ (cf. Definition 5.1.8) whether $[\bar{\theta}] \in H^1(\mathscr{G}_K, \mathrm{M}_2^0(\mathbb{F}_3))$ is the trivial cohomology class.

5.3.1 The class field theory method

Let L/K be the fixed field of $\ker(\tilde{\rho})$. With the same construction as presented in Chapter 2, we can compute E/L the compositum of all C_3 extensions of L unramified outside S_L, the lifting of our set S to $\mathrm{MaxSpec}(\mathcal{O}_L)$. As we know, the Galois group $\mathrm{Gal}(E/L) \simeq Cl(\mathfrak{m}_{S_L})/Cl(\mathfrak{m}_{S_L})^3$ has the structure of a finite dimensional $\mathbb{F}_3$-vector space V. We have an action of $\mathrm{Gal}(L/K) \simeq \tilde{\rho}(\mathscr{G}_K)$ on V and the stable subspaces W corresponds to Galois extensions M/K with $\mathrm{Gal}(M/K) \simeq W \rtimes \tilde{\rho}(\mathscr{G}_K)$ unramified outside S. Obviously we are interested in W of dimension up to 3.
Fix such a stable subspace W, of dimension r. Let $\{w_i\}_{i=1}^r$, $r \leq 3$ be a basis of W and consider the dual basis $\{\chi_i\}_{i=1}^r$. That is,

$$\chi_i : \mathrm{Gal}(M/L) \simeq W \longrightarrow \mathbb{F}_3$$

is an additive character such that

$$\chi_i(w_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, these characters cut out non-isomorphic intermediate C_3 extension $L \subset W_i \subset W$. Take $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_L) \setminus S_L$, then

$$\chi_i(\mathrm{Frob}_{\mathfrak{P}}) = \begin{cases} \pm 1 & \text{if } \mathfrak{P} \text{ is inert in } W_i, \\ 0 & \text{if } \mathfrak{P} \text{ splits in } W_i. \end{cases}$$

Now, let $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$ be the prime that lies under $\mathfrak{P}$. Let $\mathrm{Frob}_{\mathfrak{p}}$ be the corresponding Frobenius automorphism in $\mathrm{Gal}(M/K)$, and $\overline{\mathrm{Frob}}_{\mathfrak{p}}$ be its projection in $\mathrm{Gal}(L/K)$. Recall that by the theory developed in Chapter 3 we know the irreducible quartic polynomial $f(x) \in \mathcal{O}_K[x]$ whose splitting field is L/K. Since $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) \times \mathrm{ord}(\overline{\mathrm{Frob}}_{\mathfrak{p}})$, we can determine whether $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p}}) > 4$ by the splitting behaviour of $f \bmod \mathfrak{p}$ and the value of $\chi_i(\mathrm{Frob}_{\mathfrak{P}})$. Indeed, If $\chi_i(\mathrm{Frob}_{\mathfrak{P}}) \neq 0$ for some i, then by multiplicativity in towers of the inertia degree, we obtain $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p}}) = 3 \times \mathrm{ord}(\overline{\mathrm{Frob}}_{\mathfrak{p}})$. Since $\mathrm{ord}(\overline{\mathrm{Frob}}_{\mathfrak{p}}) \in \mathrm{Gal}(L/K)$ can be determined by how f splits modulo $\mathfrak{p}$ we can explicitly compute $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p}})$. Thus we can determine whether to add $\mathfrak{p}$ to the obstruction set Σ.

We can summarise the class field method in the following way:

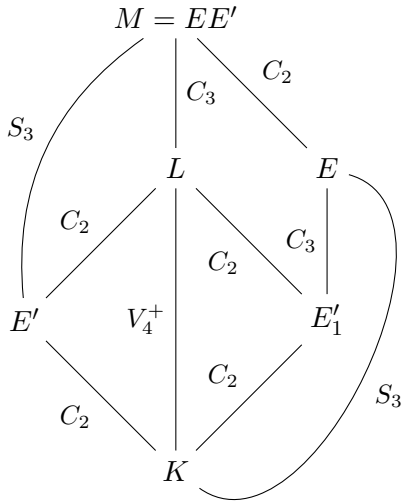
- With class field theory we compute $\mathrm{Gal}(E/L) = Cl(\mathfrak{m}_{S_L})/Cl(\mathfrak{m}_{S_L})^3$, E the compositum of all C_3 extensions of L unramified outside S_L, and the action of $\tilde{\rho}(\mathscr{G}_K) \simeq \mathrm{Gal}(L/K)$ on it;
- following Proposition 5.1.7, we consider each irreducible subspace W with $r = \dim(W) \in \{1, 2, 3\}$ in turn. Each W determines a Galois extension M of K unramified outside S with $\mathrm{Gal}(M/K) \simeq W \rtimes \mathrm{Gal}(L/K)$;
- for each W we list the r characters χ_i. Note that we did not construct the extension M/K explicitly. In order to compute the χ_i, we use a 3-basis for L as presented in the preliminaries, § 2;
- for each W we are able to compute a prime $\mathfrak{P} \in \mathrm{MaxSpec}(\mathcal{O}_L) \setminus S_L$, such that if $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ then the order of $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(M/K)$ is greater than 4;
- we add $\mathfrak{p}$ to the obstruction set Σ.

5.3.2 The sextic-fields method

Now, let ρ_1, ρ_2 be two 3-adic Galois representations that satisfy conditions $i)$ - $iii)$ of Theorem 5.2.1. Our goal is to present a second method that allows us to compute an obstruction set Σ and hence determine whether the two representations are equivalent.

We divide the discussion in cases according to the possible images of $\tilde{\rho}(\mathscr{G}_K)$ of the theorem. Let L/K be the fixed field of $\ker(\tilde{\rho})$, i.e. $\mathrm{Gal}(L/K) \simeq \tilde{\rho}(\mathscr{G}_K)$.

Case $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^{\pm}$. In order to determine whether ρ_1, ρ_2 are equivalent we have seen that it is enough to exclude all the possible Galois extensions M/K unramified outside S with $\mathrm{Gal}(M/K) \simeq C_3 \rtimes V_4 \simeq D_6$, containing L with $\mathrm{Gal}(M/L) \simeq C_3$. Moreover, as D_6 is a transitive subgroup of S_6, we can identify M as the splitting field of a degree 6 polynomial with coefficients in K. Since, $D_6 \simeq C_2 \times S_3$ we can list all these extensions by taking an S_3-extensions E/K and a C_2-extension E'/K such that $E \cap E' = K$, and setting $M = EE'$. The field extensions lattice is



By Kummer theory all the quadratic extensions E'/K unramified outside S are of the form $K(\sqrt{\alpha})$ for $\alpha \in K(S,2)$ (see § 3.5). To list all the S_3 extensions of K unramified outside S we refer to [28, § 4.3]. In particular, E is determined as the splitting field of a degree 3 polynomial $g(x) \in K[x]$. Let $\Delta_g \in K$ be the discriminant of g. Since we want $E \cap E' = K$ is enough to take only one α from each coset of $\langle \Delta_g \rangle$ in $K(S,2)$, that is $\alpha\Delta_g$ is not a square in K.
The next step is to use the comparison test function Φ over a suitable obstruction

set Σ to exclude these extensions. Hence, for each extension EE'/K we seek a prime $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$ such that $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(EE'/K)$ has order strictly greater then 4. But then any $\mathfrak{p}$ such that f is irreducible mod $\mathfrak{p}$, and α is not a square mod $\mathfrak{p}$ satisfies $\mathrm{ord}(\mathrm{Frob}_\mathfrak{p}) = 6$, and we can add it to the obstruction set Σ.

For the remaining cases, we need the following lemma. It is joint work with Professor John Cremona and extends Theorem 5.5.1 in [4].

Lemma 5.3.2. *Let $\rho_1, \rho_2 : G \longrightarrow \mathrm{GL}_d(\mathbb{Z}_\ell)$ be two representations of a group G. Let $\bar{\rho}_1, \bar{\rho}_2$ be the associated* mod ℓ *representations. Assume that G has a* normal *subgroup H of* index n *such that*

i) $\rho_1|_H \sim \rho_1|_H$, and both are absolutely irreducible.

Then $\rho_2(g) = \chi(g)\rho_1(g)$ for all g in G and for a multiplicative character $\chi : G \longrightarrow \mathbb{Z}_\ell^\times$.
Furthermore, if one of the following holds

ii) n is coprime to $2(\ell - 1)$;

iii) n is coprime to d, and $\det(\rho_1) = \det(\rho_2)$;

iv) n is coprime to d, and $\bar{\rho}_1 \sim \bar{\rho}_2$;

v) H is maximal, $\bar{\rho}_1 \sim \bar{\rho}_2$ and $\exists\, \gamma \in G \setminus H$ such that $\mathrm{tr}\rho_1(\gamma) \not\equiv 0 \bmod \ell$.

Then $\rho_1 \sim \rho_2$.

Proof. From condition *i*) we can replace ρ_2 by a conjugate and hence assume $\rho_1|_H = \rho_2|_H$. Let $g \in G$. Since $gHg^{-1} = H$ for all $h \in H$ we have

$$\rho_1(ghg^{-1}) = \rho_2(ghg^{-1}) \Longrightarrow \rho_1(h) = \rho_1(g)^{-1}\rho_2(g)\rho_2(h)\rho_2(g)^{-1}\rho_1(g).$$

But we know that $\rho_1(h) = \rho_2(h)$, hence $\rho_1(g)^{-1}\rho_2(g)$ commutes with $\rho_1(h)$ for all $h \in H$. Since $\rho_i|_H$ is absolutely irreducible, by Schur's lemma we have that $\rho_1(g)^{-1}\rho_2(g)$ is a scalar, say $\rho_2(g) = a_g\rho_1(g)$ with $a_g \in \mathbb{Z}_\ell^\times$. (Note: not just in $\mathbb{Q}_\ell^\times$ since taking determinants shows that $a_g^d \in \mathbb{Z}_\ell^\times$, so $a_g \in \mathbb{Z}_\ell^\times$.) Therefore, we have the following multiplicative character

$$\begin{aligned} \chi : G &\longrightarrow \mathbb{Z}_\ell^\times \\ g &\mapsto a_g \end{aligned}$$

such that $\chi|_H = 1$ and $\rho_2(g) = \chi(g)\rho_1(g)$. Indeed, let $g_1, g_2 \in G$ then

$$a_{g_1g_2} = \rho_1(g_1g_2)^{-1}\rho_2(g_1g_2) = \rho_1(g_2)^{-1}\left(\rho_1(g_1)^{-1}\rho_2(g_1)\right)\rho_2(g_2) = a_{g_1}a_{g_2}$$

Note also that since $g^n \in H$, then $\chi(g)^n = 1$ for all $g \in G$. Hence $\chi(g) \in \mathbb{Z}_\ell^\times$ is an n-th root of unity.

We will now show that $\rho_1 = \rho_2$ if at least one of the condition ii)-v) holds.

Condition ii) implies that χ is the trivial character since the roots of unity in $\mathbb{Z}_\ell^\times$ all have order dividing $\ell - 1$ (or dividing 2 if $\ell = 2$).

If condition iii) holds then taking determinants we have $\chi(g)^d = 1$ for all $g \in G$ and since $(d, n) = 1$ then we can conclude $\chi(g) = 1$ for all $g \in G$.

From iv) it follows that $\chi(g)^n \equiv 1 \bmod \ell$ and $\chi(g)^d \equiv 1 \bmod \ell$. Since n, d are coprime we have $\chi(g) \equiv 1 \bmod \ell$ for all $g \in G$. Then we can conclude that χ is the trivial character since the only root of unity in $\mathbb{Z}_\ell^\times$ congruent to one modulo ℓ is 1.

Finally, from v) we have that $\mathrm{tr}\rho_1(g) \equiv \mathrm{tr}\rho_2(g) \bmod \ell$ for all $g \in G$. On the other hand, for all $g \in G$ we know that $\mathrm{tr}\rho_2(g) = \chi(g)\mathrm{tr}\rho_1(g)$. Hence $(\chi(g) - 1)\mathrm{tr}\rho_1(g) \equiv 0 \bmod \ell$. This implies that either $\mathrm{tr}\rho_1(g) \equiv 0 \bmod \ell$ or $\chi(g) \equiv 1 \bmod \ell$. Since $\mathrm{tr}(\gamma) \not\equiv 0 \bmod \ell$ we have that $\chi(\gamma) \equiv 1 \bmod \ell$ and we can then conclude that $\chi(\gamma) = 1$. However, this would implies that $H < \ker(\chi)$ is a strict inclusion; by maximality of H, we have $\ker(\chi) = G$, that is χ is the trivial character.

Hence $\rho_1(g) = \rho_2(g)$ for all $g \in G$ as claimed.

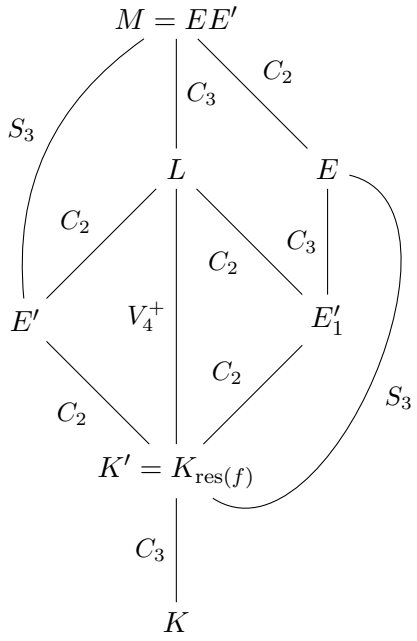
□

Remark 5.3.3. Assume that H satisfies only condition i). Then we have that ρ_1 and ρ_2 differ by a multiplicative character with values in $\mathbb{Z}_\ell^\times$. Hence, we can use an ℓ-linearly independent set of primes (see definition 2.0.1) to determine χ and therefore whether they are equivalent.

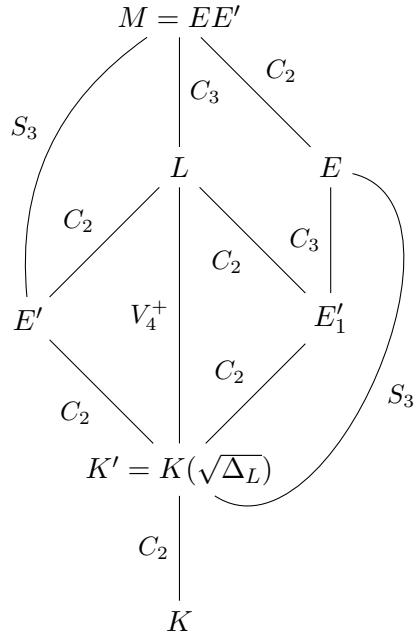
Even though we have stated the theorem in such generality we are mainly interested in its application when $d = 2, \ell = 3$.

Case $\tilde{\rho}(\mathscr{G}_K) \simeq A_4$. With the theory introduced in § 3.4 we have determined the fixed field L/K of $\ker(\tilde{\rho})$ as the splitting field of a degree 4 polynomial $f_L \in K[x]$. Let K'/K be the splitting field of the resolvent cubic of f_L. We have $\mathrm{Gal}(K'/K) = C_3$ and $\mathrm{Gal}(L/K') = V_4^+$. Since the absolute Galois group $\mathscr{G}_{K'}$ of K' is a normal subgroup of $\mathscr{G}_K$ of index 3, then condition ii) of the lemma is satisfied. Moreover, from Theorem 3.5.2 we have $\bar{\rho}(\mathscr{G}_K) \simeq Q_8$, absolutely irreducible, so $\rho_i|_{\mathscr{G}_{K'}}$ is also absolutely irreducible. From the lemma then we have $\rho_1 \sim \rho_2$ if and only if $\rho_1|_{\mathscr{G}_{K'}} \sim$

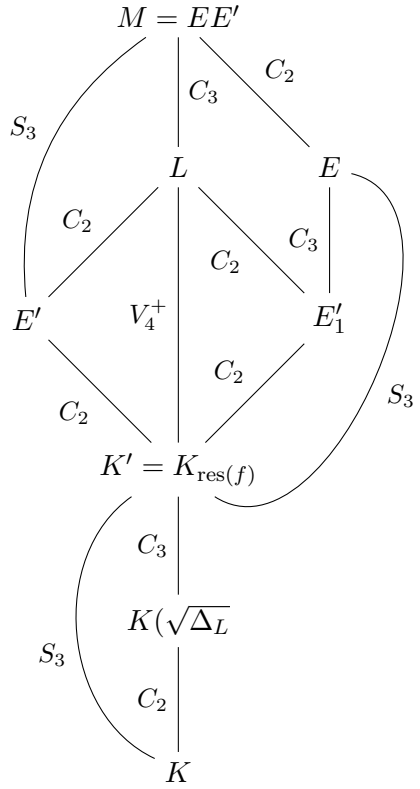
$\rho_2|_{\mathscr{G}_{K'}}$. Therefore, in order to study the restrictions of ρ_i to $\mathscr{G}_{K'}$ we can repeat exactly the same arguments as in the case $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^+$. The field extension lattice is as follows.



Case $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$. Let $f_L \in K[x]$ be the degree four polynomial that defines the extension L/K cut out by $\tilde{\rho}$. Let $K' = K(\sqrt{\Delta_L})$ where $\Delta_L \in K$ is the discriminant of f_L. Then, $\mathrm{Gal}(K'/K) = C_2$ and $\mathrm{Gal}(L/K') = V_4^+$. Therefore, $\mathscr{G}_{K'} \lhd \mathscr{G}_K$ has index 2, hence it is normal and maximal. Since $\tilde{\rho}(\mathscr{G}_K) \simeq D_4$ and $\tilde{\rho}(\mathscr{G}_{K'}) \simeq V_4^+$, we have elements $\sigma \in \mathscr{G}_K \setminus \mathscr{G}_{K'}$ such that $\tilde{\rho}(\sigma)$ corresponds to a 4-cycle. As we have seen, we have $\mathrm{tr}\bar{\rho}(\sigma) \not\equiv 0 \bmod 3$. Hence, $\mathscr{G}_{K'}$ satisfies condition v). Since $\rho_i|_{\mathscr{G}_{K'}}$ is absolutely irreducible by the same argument the previous case, by the lemma we have $\rho_1 \sim \rho_2$ if and only if $\rho_1|_{\mathscr{G}_{K'}} \sim \rho_2|_{\mathscr{G}_{K'}}$. So we may restrict again to the V_4^+ case. The field extension lattice is now as follows.



Case $\tilde{\rho}(\mathscr{G}_K) \simeq S_4$. Let $L/K, f_L$, and Δ_L be as in the previous cases. Consider $F = K(\sqrt{\Delta_L})$. Since $\mathrm{Gal}(F/K) = C_2, \mathrm{Gal}(L/F) = A_4, \tilde{\rho}(\mathscr{G}_K) \simeq S_4$, and $\tilde{\rho}(\mathscr{G}_F) \simeq A_4$, we can conclude that $\mathscr{G}_F$ is a maximal normal subgroup of $\mathscr{G}_K$. Note that $\rho_i|_{\mathscr{G}_F}$ is absolutely irreducible. Moreover, there exist $\sigma \in \mathscr{G}_K \setminus \mathscr{G}_F$ such that $\tilde{\rho}(\sigma)$ is a 4-cycle and therefore $\mathrm{tr}\tilde{\rho}(\sigma) \neq 0$. Thus, $\mathscr{G}_F$ satisfies condition v) of the Lemma 5.3.2. Hence, by the lemma, it is enough to prove the equivalence over $\mathscr{G}_F$. Since we are now in the case where the projective representation as image isomorphic to A_4, we have seen that we can restrict again to the absolute Galois group $\mathscr{G}_{K'}$, where K'/F is an intermediate C_3-extension of F contained in L. Note that, $\mathrm{Gal}(L/K') \simeq V_4^+$ and K' is the splitting field of the resolvent cubic of f_L. The corresponding lattice is as follows.



Remark 5.3.4. It is important to notice that when we list the D_6 extensions of K' ($K' = K$ when $\tilde{\rho}(\mathscr{G}_K) \simeq V_4^{\pm}$) we do not need all the possible D_6-extensions M/K' unramified outside the finite set $S_{K'}$. Indeed, we need exactly the extensions M/K' that contain L. Now, since $D_6 \simeq S_3 \times C_2$, a D_6-extension is the compositum of an S_3-extension E/K' with a disjoint quadratic extension E'/K'. On the other hand, since $M = EE'$ must contain L/K' with $\mathrm{Gal}(L/K') \simeq V_4^+$, then both E', E have non trivial intersection with L. Let $E_1 = K'(\sqrt{\Delta_1}), E_2 = K'(\sqrt{\Delta_2})$, and $E_3 = K'(\sqrt{\Delta_1\Delta_2} = \sqrt{\Delta_3})$ be the three quadratic extensions contained in L. Therefore, the candidates for $M = E'E$ are the compositum of one of the E_i with the splitting field of a cubic polynomial $g(x) \in K'[x]$ whose discriminant is equal to Δ_j with $i \neq j$.

Now, in order to exclude the D_6 extensions of F, and hence prove that $\rho_1|_{\mathscr{G}_F} \sim \rho_2|_{\mathscr{G}_F}$, we need to compute $\Phi|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$ where $\mathfrak{P} \in \Sigma_F \subset \mathrm{MaxSpec}(\mathcal{O}_F) \setminus S_F$. However, we are able to compute Φ only from the black box data over K. By Remark 5.1.10 we carry on with the method if and only if the traces $\mathrm{tr}\rho_1|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$,

$\mathrm{tr}\rho_2|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$ are equal. The next lemma establishes equivalence between the equality $\mathrm{tr}\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\rho_2(\mathrm{Frob}_{\mathfrak{p}})$ and the previous one, where $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$ is such that $\mathfrak{P}|\mathfrak{p}$. This result was suggested by Professor John Cremona.

Lemma 5.3.5. *Let $\rho_1, \rho_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be two Galois representations. Let F/K be a finite Galois extension with absolute Galois group $\mathscr{G}_F$. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P} \in$ MaxSpec$(\mathcal{O}_F)$ such that $\mathfrak{P}|\mathfrak{p}$. Assume that the following hold:*

1) *$\mathfrak{p}$ is unramified in F/K and both ρ_i are unramified at $\mathfrak{p}$;*

2) *$\det\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \det\rho_2(\mathrm{Frob}_{\mathfrak{p}})$, and $\mathrm{tr}\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\rho_2(\mathrm{Frob}_{\mathfrak{p}})$.*

Then $\mathrm{tr}\rho_1|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}}) = \mathrm{tr}\rho_2|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$.

Proof. Let $f = [\mathcal{O}_F/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ be the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$. Then we have $\mathrm{Frob}_{\mathfrak{P}} = (\mathrm{Frob}_{\mathfrak{p}}|_F)^f \in \mathscr{G}_F$. Now, let α_i, β_i be the eigenvalues of $\rho_i(\mathrm{Frob}_{\mathfrak{p}})$, $i = 1, 2$. Then α_i^f, β_i^f are the eigenvalues of $\rho_i|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$. Hence, $\mathrm{tr}\rho_i|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}}) = \alpha_i^f + \beta_i^f$ is a symmetric polynomial in α_i, β_i. In particular, it is a polynomial in the elementary symmetric polynomials in $\alpha_i + \beta_i = \mathrm{tr}\rho_i(\mathrm{Frob}_{\mathfrak{p}})$ and $\alpha_i\beta_i = \det\rho_i(\mathrm{Frob}_{\mathfrak{p}})$. Therefore, by condition 2) the statement holds. □

This implies that when we want to know whether $\Phi|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}})$ is zero, it is enough to compute $\Phi(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{P}|\mathfrak{p}$. If the latter is zero, then by the lemma $\Phi|_{\mathscr{G}_F}(\mathrm{Frob}_{\mathfrak{P}}) = 0$. If $\Phi(\mathrm{Frob}_{\mathfrak{p}}) \neq 0$ then we can conclude that $\rho_1 \not\sim \rho_2$ having different traces at $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$.

Summary of the sextic-fields method

The following steps summarise the sextic-field method:

- We compute the possibly trivial field extensions F/K, $K \subseteq F \subsetneq L$, such that $\tilde{\rho}(\mathscr{G}_F) \simeq V_4$. Depending on the image $\tilde{\rho}(\mathscr{G}_K)$ it is determined either as the splitting field of the resolvent cubic of f_L, or $F = K(\sqrt{\Delta_L})$, or is the trivial extension.

- We list all the D_6 extensions M/F that contain L as a compositum $M = EE'$, where E/F is the splitting field of a cubic polynomial $g \in F[x]$ disjoint from the quadratic extension E'/F.

- For each pair we take a prime $\mathfrak{P}_M \in \mathrm{MaxSpec}(\mathcal{O}_F) \setminus S_F$ such that $\mathfrak{P}_M$ is inert in E' and g is irreducible mod $\mathfrak{P}$. We add $\mathfrak{P}_M$ to the obstruction set Σ_F.

- for each $\mathfrak{P}_M \in \Sigma_F$ we compute $\Phi(\mathrm{Frob}_\mathfrak{p})$ for $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K)$ such that $\mathfrak{P}_M | \mathfrak{p}$.
- If $\Phi(\mathrm{Frob}_\mathfrak{p}) \neq 0$ then the two representations are not equivalent. Otherwise, we exclude M from the candidates.

In particular, the equivalence of $\rho_1, \rho_2 : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_3)$ can be determined by studying the splitting fields of degree 6 polynomials.

A note on the implementation. The sextic field method requires listing all the D_6-extensions of a given number field that are unramified outside a fixed set of primes and contain known intermediate extensions. Additionally, we need to compute for each one of these extensions a prime ideal with specific behaviour. We have implemented this, and found that the time the algorithm needed to run even in the easiest examples was too great. Therefore we needed to change how to deal with the extensions. We can proceed in the following way. Let L/K be the fixed field of the projective representation and let K'/K be the intermediate field extension such that $\tilde{\rho}(\mathscr{G}_F) \simeq V_4^+ = \mathrm{Gal}(L/K')$. Let E_1, E_2 be two quadratic extensions of K' contained in L. In order to list the D_6 extensions we are interested in we need to compute all the C_3-extensions of E_1 unramified outside S_1, the lifting of S to E_1, and to check which ones are Galois over K' in order to have an appropriate S_3-extension E' of K'. Prof. Cremona had already implemented this following the theory developed by Koutsianas [28]. However, it requires much computation since we need to deal with each extension individually. But our goal is only to find primes of K' with a specific behaviour in E_2 and the C_3-extension E'/E_2; to be specific, we want a prime of K' that is inert in E_2 and both its lifts to E_1 are inert in the E'. Therefore it is possible to consider all primes that have the right behaviour in more than one specific E'. The set we are looking for is then exactly $T_3(E_1)$, as defined in Chapter 2. What we are more precisely claiming is the following:

Claim. *Let E'/E_1 be a non trivial Galois extension with $Gal(E'/E_1) \simeq C_3$ unramified outside S_1, the lift of S to E_1. Then there exists a prime $\mathfrak{p} \in T_3(E_1)$ such that $\mathfrak{p}$ is inert in E'.*

Indeed, let M/E_1 be the Galois extension with Galois group $\mathrm{Gal}(M/E_1)$ isomorphic to $Cl(\mathfrak{m}_{S_1})/Cl(\mathfrak{m}_{S_1})^3$ determined by class field theory. Let $T_3(E_1)$ be a 3-linearly independent set of primes for E_1, i.e. the set $\{\mathrm{Frob}_\mathfrak{p} \,|\mathfrak{p} \in T_3(E_1)\}$ is an $\mathbb{F}_3$-basis for $\mathrm{Gal}(M/E_1)$. Consider now the dual basis $\{\chi_\mathfrak{p}\}$, where each $\chi_\mathfrak{p} : \mathrm{Gal}(M/E_1) \longrightarrow \mathbb{F}_3$ is an additive character. Note that elements of the dual space of $\mathrm{Gal}(M/E_1)$ are

in one to one correspondence with the C_3-extensions of E_1 unramified outside S_1. Moreover, let χ be an element of the dual space and let E_χ be the relative extension; if $\mathfrak{p}$ is a prime of E_1 we have that $\chi(\mathrm{Frob}_\mathfrak{p}) = 0$ if and only if $\mathfrak{p}$ is split in E_χ. But now if E'/E is a C_3-extension unramified outside S_1, possibly trivial, such that for all $\mathfrak{p} \in T_3(E_1)$ we have that $\mathfrak{p}$ is split in E', then the associate character χ' is trivial on $\{\mathrm{Frob}_\mathfrak{p} \,|\mathfrak{p} \in T_3(E_1)\}$ and by definition of $T_3(E_1)$ we have that χ' is trivial. As a consequence, E' must be the trivial extension and the claim follows. The improvement is then the following: if $Cl(\mathfrak{m}_{S_1})/Cl(\mathfrak{m}_{S_1})^3$ has dimension t over $\mathbb{F}_3$ then before the claim we needed to check $3^t - 1$ extensions, after the claim the number of tests is reduced to only t. Certainly t primes may be more than we need, since not all the cubic extension of E_1 are Galois over K' but the number of operations requested to find them is considerably less than test $3^t - 1$ extensions.

Furthermore, everything becomes simpler if E_1 contains the 3-rd roots of unity. If we enlarge S to contains the primes above 3 then by Kummer theory we may use the 3-Selmer group $E_1(S_1, 3)$ of E_1 (see § 1.4) instead of $Cl(\mathfrak{m}_{S_1})/Cl(\mathfrak{m}_{S_1})^3$. If $\mathfrak{p} \in T_3(E_1)$ and $N(\mathfrak{p})$ is the absolute norm of $\mathfrak{p}$, then we have the followings characters

$$\begin{aligned} \chi_\mathfrak{p} : E_1(S_1, 3) &\longrightarrow \mu_3 \\ a \quad &\mapsto \quad a^{(N(\mathfrak{p})-1)/3} \mod \mathfrak{p} \end{aligned}$$

Fix the unique isomorphism $\psi : \mu_3 \to \mathbb{F}_3$ such that $\omega \mapsto 1$. Then a basis for the dual space of $E_1(S_1, 3)$ is given by the additive characters $\alpha_\mathfrak{p} := \psi \circ \chi_\mathfrak{p}$. Therefore, to compute the set $T_3(E_1)$, we can use Algorithm 1 developed in [5], § 3 pag. 9, with the $\alpha_\mathfrak{p}$ defined above plus the condition that all $\mathfrak{p} \in T_3(E_1)$ must be inert in E_2. Moreover, when the representation has cyclotomic determinant, then the condition about the roots of unity in E_1 is automatically satisfied. Since the representations we have tested all have cyclotomic determinant, we have implemented only this explicit case instead of the full class field theory method.

We want to remark that even though the sextic field method and the class field theory method are from a theoretical point of view completely different, the actual implementation we use in practice combines features from both of them.

Finally, it is extremely important to remark that in both the methods we have presented, the obstruction set Σ does not depend on k, the integer such that $\rho_1 \equiv \rho_2 \mod 3^k$. Indeed, if $\Phi(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in \Sigma$ we can conclude that $\rho_1 \equiv \rho_2$ modulo 3^{k+1} after adjusting ρ_1 as in proposition 5.1.2. Hence, since Σ does not depend on k, we have proved this equivalence for any k and therefore $\rho_1 \sim \rho_2$ as 3-adic Galois representations.

Chapter 6

Applications

In this chapter, we apply the sextic field method to prove whether two given black box Galois representations are isomorphic. Of particular interest is establishing modularity of elliptic curves. We address this problem in the case of elliptic curves E defined over an imaginary quadratic field of class number one. The modularity of E then corresponds to proving an isomorphism between the Galois representation attached to E and the Galois representation attached to a weight 2 Bianchi newform F with trivial Nebentypus. Since such Galois representations form a compatible system, then having an isomorphism of the 3-adic Galois representations is enough to have an isomorphism of the ℓ-adic representations for all primes ℓ.

We start recalling what a weight 2 Bianchi new form is and why we can consider Galois representations attached to them. For this introduction we mainly follow [15, Chapter 2-3] and [39, § 5, § 8].

Let $\mathbb{H} = \{(x, y) \in \mathbb{C} \times \mathbb{R} | y > 0\}$ be hyperbolic 3-space. We have an action of $\mathrm{PSL}_2(\mathbb{C})$ on $z = (x, y) \in \mathbb{H}$ via the formula

$$\gamma \cdot z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x, y) = \left(\frac{(ax+b)\overline{(cx+d)} + a\bar{c}y^2}{|cx+d|^2 + |c|^2 y^2}, \frac{y}{|cx+d|^2 + |c|^2 y^2} \right)$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{C})$ and $\bar{*}$ is complex conjugation. If K is an imaginary quadratic field then its ring of integer $\mathcal{O}_K$ is a discrete subring of $\mathbb{C}$ and $\mathrm{PSL}_2(\mathcal{O}_K)$ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$. The group $\mathrm{PSL}_2(\mathcal{O}_K)$ is called the *Bianchi group associated to* K. Note that it acts properly discontinuously on $\mathbb{H}$. Furthermore, for

a nonzero ideal $\mathfrak{N}$ of $\mathcal{O}_K$, the *principal subgroup of level* $\mathfrak{N}$ is

$$\Gamma(\mathfrak{N}) = \{\gamma \in \mathrm{PSL}_2(\mathcal{O}_K) | \gamma \equiv \pm 1 \mod \mathfrak{N}\},$$

and a subgroup Γ of $\mathrm{PSL}_2(\mathcal{O}_K)$ is called a *congruence subgroup* if it contains a principal subgroup. Of particular interest are the congruence subgroups

$$\Gamma_0(\mathfrak{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_K) | c \equiv 0 \mod \mathfrak{N} \right\}.$$

For a given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{C})$ and $z = (x, y) \in \mathbb{H}$ we introduce the *multiplier system*

$$J(\gamma, z) = \begin{pmatrix} cx + d & -cy \\ \bar{c}y & \overline{cx + d} \end{pmatrix}.$$

Given a function $F : \mathbb{H} \longrightarrow \mathbb{C}^{k+1}$ and $\gamma \in \mathrm{PSL}_2(\mathbb{C})$, we define the *slash operator*

$$(F|_k \gamma)(z) = \mathrm{Sym}^k(J(\gamma, z)^{-1}) F(\gamma \cdot z)$$

where Sym^k is the symmetric k-th power of the standard representation of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathbb{C}^2$. It is more explicit when $k = 2$. In this case we have $F : \mathbb{H} \longrightarrow \mathbb{C}^3$ and the slash operator is

$$(F|_k \gamma)(z) = \frac{1}{|r|^2 + |s|^2} \begin{pmatrix} \bar{r}^2 & 2\bar{r}s & s^2 \\ -\bar{r}\bar{s} & |r|^2 - |s|^2 & rs \\ \bar{s}^2 & -2r\bar{s} & r^2 \end{pmatrix} F(\gamma \cdot z)$$

where $r = cx + d$ and $s = cy$.

Let $\beta_1 = -\dfrac{dx}{y}$, $\beta_2 = \dfrac{dy}{y}$, $\beta_3 = \dfrac{d\bar{x}}{y}$ be a basis of differential 1-form on $\mathbb{H}$. A differential form ω is *harmonic* id $\Delta\omega = 0$ where $\Delta = d \circ \delta + \delta \circ d$ is the usual Laplacian with d being the exterior derivative and δ the codifferential operator. Then $\mathrm{PSL}_2(\mathbb{C})$ acts on the space of differential 1-form as

$$\gamma \cdot {}^t(\beta_1, \beta_2, \beta_3)_{(z)} = \mathrm{Sym}^2(J(\gamma, z)) {}^t(\beta_1, \beta_2, \beta_3)_{(z)}$$

Definition 6.0.1. A weight 2 cuspidal Bianchi modular form for a congruence subgroup $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ is a real analytic function $F = (F_1, F_2, F_3) : \mathbb{H} \longrightarrow \mathbb{C}^3$ with the following properties

1) $F_1\beta_1 + F_2\beta_2 + F_3\beta_3$ is a harmonic differential 1-form on $\mathbb{H}$ that is Γ-invariant;

2) $F|\gamma = F$ for all $\gamma \in \Gamma$;

3) $\int_{\mathbb{C}\setminus\mathcal{O}_K}(F|\gamma)(x,y)dx = 0$ for every $\gamma \in \mathrm{PSL}_2(\mathcal{O}_K)$.

Here, condition 1) replaces the holomorphicity condition for classical modular forms, since $\mathbb{H}$ has no complex structure. Condition 3) is equivalent to saying that the constant coefficient of the Fourier-Bessel expansion of $F|\gamma$ is equal to zero for every $\gamma \in \mathrm{PSL}_2(\mathcal{O}_K)$ (for a detailed explanation see [39, § 5, p. 14]). The congruence subgroup Γ is called the *level* of F, but when $\Gamma = \Gamma_0(\mathfrak{N})$ it is common to say that F is a form of level $\mathfrak{N}$. The weight 2 cuspidal forms of level Γ forms a finite-dimensional vector space $\mathcal{S}_2(\Gamma)$ and it is endowed with an action of the *Hecke algebra* $\mathbb{T}$.
Consider two ideal $\mathfrak{M}, \mathfrak{N}$ of $\mathcal{O}_K$ such that $\mathfrak{M}|\mathfrak{N}$ then we have the inclusion of $\mathcal{S}_2(\Gamma_0(\mathfrak{M}))$ in $\mathcal{S}_2(\Gamma_0(\mathfrak{N}))$. Then, given a level $\Gamma_0(\mathfrak{N})$ and $F \in \mathcal{S}_2(\Gamma_0(\mathfrak{N}))$ we call F an *oldform* if it comes from a lower level $\mathfrak{M}|\mathfrak{N}$ and $N_{\mathbb{Q}}^K(\mathfrak{M}) < N_{\mathbb{Q}}^K(\mathfrak{N})$. Furthermore, $\mathcal{S}_2(\Gamma)$ admits an inner product analogous to the Petersson inner product for classical modular forms. The *newspace* $\mathcal{S}_2(\Gamma_0(\mathfrak{N}))^{\mathrm{new}}$ at level $\Gamma_0(\mathfrak{N})$ is the orthogonal complement in $\mathcal{S}_2(\Gamma_0(\mathfrak{N}))$, with respect to the inner product, of all the oldforms. The action of the Hecke algebra on $\mathcal{S}_2(\Gamma_0(\mathfrak{N}))$ preserves the newspace and acts semisimply on it.

Definition 6.0.2. A weight 2 Bianchi newform F of level $\Gamma_0(\mathfrak{N})$ (usually abbreviated to level $\mathfrak{N}$) is a Bianchi cusp form lying in the newspace $\mathcal{S}_2(\Gamma_0(\mathfrak{N}))^{\mathrm{new}}$ which is also a normalised eigenform for the Hecke Algebra $\mathbb{T}$.

The existence of a Galois representation attached to such Bianchi modular forms is established in [7] [35] (even though their result holds for more general automorphic forms). In particular, combining these results together with the theory developed in [47] and [34] we know that a Galois representation ρ_f associated to a weight 2 Bianchi newform F satisfies the following:

i) ρ_F is unramified at all primes of K that do not divide the level of F;

ii) if F has trivial nebentypus the determinant character $\det(\rho_F)$ is the cyclotomic character;

iii) for each prime $\mathfrak{p} \nmid \ell$ of K that does not divide the level of F we have

$$\mathrm{tr}(\rho_F(\mathrm{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}(F) \in \mathbb{Z}.$$

Finally, the Galois representations we are considering are rational, i.e. for each prime $\mathfrak{p}$ of K the coefficients of the characteristic polynomial of $\rho_F(\mathrm{Frob}_{\mathfrak{p}})$ are rational.

But then Lemma 3.1 in [27] and Theorem 2 in [10] imply that ρ_F takes values in $\mathrm{GL}_2(\mathbb{Q}_\ell)$.

To carry out the computation, we have implemented the sextic field method in Sage [46]. We use previous code written by Professor John Cremona to list all the possible S_3-extensions of a number field K unramified outside a finite set S of primes of K. The code is based on the theory developed in [28] and it can be find at the following repository [18]. Moreover, if the ground field is imaginary quadratic of class number one, we used the C++ code written by prof. John Cremona to compute the $a_{\mathfrak{p}}(F)$ of a weight 2 Bianchi newform F. The theory is developed in [15] and the code is available at the following repository [17].

Firstly, we prove that the Galois representations studied in § 3.6 with absolutely irreducible mod 3 image are isomorphic to the Galois representations attached to weight 2 Bianchi newforms.

Example 1. Let F be the Bianchi newform over $K = \mathbb{Q}(\sqrt{-1})$ of weight 2, level $(-12i - 4)$, and trivial character with LMFDB label 2.0.4.1-160.1-a. The set of bad primes is then $S = \{(-i-2), (3), (i+1)\}$. Consider the elliptic curve $E : y^2 + (i+1)xy = x^3 + (-i+1)x^2 + (37i-5)x + 88i + 53$ that we have analysed in example 1 in § 3.11. Then, the Galois representations ρ_F and ρ_E have the same determinant character and since they have the same set of bad primes we do not need to compute again the distinguishing set T_0. With the code of Prof. Cremona we can verify that the two representations agree on T_0, i.e. $\mathrm{tr}\rho_F(\mathrm{Frob}_{\mathfrak{p}}) \equiv \mathrm{tr}\rho_E(\mathrm{Frob}_{\mathfrak{p}}) \bmod 3$ for all $\mathfrak{p} \in T_0$. This implies that ρ_F, ρ_E have isomorphic projective representations. Moreover, since they have the same projective splitting field L/K we do not need to compute the $T_2(L)$ to determine the full mod 3 representation attached to ρ_F. The computation then yields $\mathrm{tr}\rho_F(\mathrm{Frob}_{\mathfrak{p}}) \equiv \mathrm{tr}\rho_E(\mathrm{Frob}_{\mathfrak{p}}) \bmod 3$ for all $\mathfrak{p} \in T_2(L)$, that implies $\bar{\rho}_F \simeq \bar{\rho}_E$. Since the projective image is then isomorphic to S_4 we can then apply the sextic field method in order to prove whether they are isomorphic. The obstruction set Σ has the following primes

$$\Sigma = \{(9-4i), (i-6), (12i+13), (2i+15), (-6i-5)\}.$$

With Prof. Cremona's code, we can check that the traces of the two representations agree on Σ and conclude that $\rho_F \sim \rho_E$. In particular, we deduce that the elliptic curve E is modular, and F is the associated automorphic form.

Example 2. In this example we compare the output of the sextic fields method with the 2-adic Faltings-Serre-Livné method. The 2-adic data and implementation

come from [21, example 6.3]. Here, $K = \mathbb{Q}(a)$ with $a = \sqrt{-31}$ and is the ground field. We want to apply the sextic field method to the 3-adic Galois representation attached to the elliptic curve E/K:

$$E : y^2 = x^3 + (-1)x^2 + (-1/2a + 5/2)x + (-3).$$

The set of bad primes is $S = \{(2, 1/2a - 1/2), (2, 1/2a + 1/2), (3)\}$. The output of the full 3-adic code is a set of primes of K formed by the set of primes Σ_0 introduced in theorem 3.7.1 and the obstruction set Σ. In this case the set $\Sigma \cup \Sigma_0$ of primes of K lies above the following primes of $\mathbb{Q}$:

$$7, 19, 31, 67, 97, 101, 103, 109, 113, 173, 227, 233, 255.$$

On the other hand, as reported in the paper [21] the 2-adic output contains primes that are above the following rational primes:

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 89, 109, 127,$$
$$131, 149, 173, 193, 227, 283, 293, 349, 379, 431, 521, 577, 607, 653, 839, 857,$$
$$1031, 1063, 1117, 1303, 1451, 1493, 1619, 1741, 2003, 2153, 2333, 2707, 2767,$$
$$2963, 3119, 3373, 3767.$$

The big difference here is due to the fact that while the mod 3 representation is absolutely irreducible, having projective image isomorphic to S_4, the mod 2 representation is only irreducible and therefore require a full application of the Livné method which requires several more primes. However, after conversations with Prof. Ariel Pacetti recent developments in both computer software and theory (for example the already cited [35]) would allows us to reduce significantly the number of primes required by the 2-adic method.

6.1 Examples of modularity

In the following table we have tested the sextic field method on isogeny classes of elliptic curves defined in turn over $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-3})$ with conductor norm up to 1000.
In the table, the column $\mathfrak{N}$ present the prime decomposition of the level in $\mathcal{O}_K$, it will correspond both to the conductor of the isogeny class and the level of a Bianchi modular form. If $p \in \mathbb{Z}$ splits in $\mathcal{O}_K$ then we denote the two primes above p as

$\mathfrak{p}_p, \overline{\mathfrak{p}}_p$. The choice is arbitrary but consistent throughout all the computation. The entry $N(\mathfrak{N})$ is the norm of the level. The E label is a link to the LMFDB page of the isogeny class, while the Bianchi form label is a link to the LMFDB page of the Bianchi modular form (BMF) with isomorphic Galois representation. The only exception is when the projective image is isomorphic to C_4, in those cases the isomorphism is proved only mod 3. The last two columns report the total number of primes of K that we need to establish the isomorphism and the biggest prime number p lying below them.

Table 6.1: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-1})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^5\mathfrak{p}_5$	160	2.0.4.1-160.1-a	S_4	160.1-a	23	313
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_5$	160	2.0.4.1-160.2-a	S_4	160.2-a	23	313
$\mathfrak{p}_2\mathfrak{p}_{97}$	194	2.0.4.1-194.1-b	S_4	194.1-b	27	241
$\mathfrak{p}_2\overline{\mathfrak{p}}_{97}$	194	2.0.4.1-194.2-b	S_4	194.2-b	27	241
$\mathfrak{p}_{233}$	233	2.0.4.1-233.1-a	S_4	233.1-a	16	181
$\overline{\mathfrak{p}}_{233}$	233	2.0.4.1-233.2-a	S_4	233.2-a	16	181
$\mathfrak{p}_{257}$	257	2.0.4.1-257.1-a	S_4	257.1-a	17	229
$\overline{\mathfrak{p}}_{257}$	257	2.0.4.1-257.2-a	S_4	257.2-a	18	229
$\mathfrak{p}_2^4\mathfrak{p}_{17}$	272	2.0.4.1-272.1-a	S_4	272.1-a	23	277
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{17}$	272	2.0.4.1-272.2-a	S_4	272.2-a	23	277
$\mathfrak{p}_{277}$	277	2.0.4.1-277.1-a	S_4	277.1-a	17	97
$\overline{\mathfrak{p}}_{277}$	277	2.0.4.1-277.2-a	S_4	277.2-a	16	97
$\mathfrak{p}_2\mathfrak{p}_{157}$	314	2.0.4.1-314.1-a	S_4	314.1-a	21	397
$\mathfrak{p}_2\overline{\mathfrak{p}}_{157}$	314	2.0.4.1-314.2-a	S_4	314.2-a	21	397
$\mathfrak{p}_5^2\mathfrak{p}_{13}$	325	2.0.4.1-325.1-a	C_4	325.1-a	20	241
$\overline{\mathfrak{p}}_5^2\overline{\mathfrak{p}}_{13}$	325	2.0.4.1-325.6-a	C_4	325.6-a	20	241
$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{41}$	410	2.0.4.1-410.1-a	S_4	410.1-a	32	421
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_{41}$	410	2.0.4.1-410.2-a	S_4	410.2-a	32	397
$\mathfrak{p}_2\overline{\mathfrak{p}}_5\mathfrak{p}_{41}$	410	2.0.4.1-410.3-a	S_4	410.3-a	32	397
$\mathfrak{p}_2\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{41}$	410	2.0.4.1-410.4-a	S_4	410.4-a	32	421
$\mathfrak{p}_5^2\mathfrak{p}_{17}$	425	2.0.4.1-425.1-a	S_4	425.1-a	25	421
$\overline{\mathfrak{p}}_5^2\overline{\mathfrak{p}}_{17}$	425	2.0.4.1-425.6-a	S_4	425.6-a	25	421
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2$	450	2.0.4.1-450.1-a	S_4	450.1-a	24	277
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_5^2$	450	2.0.4.1-450.3-a	S_4	450.3-a	23	277

Table 6.1: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-1})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_5\overline{\mathfrak{p}}_{101}$	505	2.0.4.1-505.2-a	S_4	505.2-a	25	409
$\overline{\mathfrak{p}}_5\mathfrak{p}_{101}$	505	2.0.4.1-505.3-a	S_4	505.3-a	24	409
$\mathfrak{p}_{509}$	509	2.0.4.1-509.1-a	S_4	509.1-a	17	241
$\overline{\mathfrak{p}}_{509}$	509	2.0.4.1-509.2-a	S_4	509.2-a	17	241
$\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{13}$	520	2.0.4.1-520.1-a	S_4	520.1-a	33	409
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{13}$	520	2.0.4.1-520.4-a	S_4	520.4-a	32	409
$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{41}$	533	2.0.4.1-533.2-a	S_4	533.2-a	24	457
$\overline{\mathfrak{p}}_{13}\mathfrak{p}_{41}$	533	2.0.4.1-533.3-a	S_4	533.3-a	24	457
$\mathfrak{p}_2\mathfrak{p}_{269}$	538	2.0.4.1-538.1-a	S_4	538.1-a	23	241
$\mathfrak{p}_2\mathfrak{p}_{269}$	538	2.0.4.1-538.1-b	S_4	538.1-b	25	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_{269}$	538	2.0.4.1-538.2-a	S_4	538.2-a	23	241
$\mathfrak{p}_2\overline{\mathfrak{p}}_{269}$	538	2.0.4.1-538.2-b	S_4	538.2-b	26	277
$\mathfrak{p}_5\mathfrak{p}_{113}$	565	2.0.4.1-565.1-a	S_4	565.1-a	25	173
$\mathfrak{p}_5\overline{\mathfrak{p}}_{113}$	565	2.0.4.1-565.2-a	S_4	565.2-a	27	433
$\overline{\mathfrak{p}}_5\mathfrak{p}_{113}$	565	2.0.4.1-565.3-a	S_4	565.3-a	26	433
$\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{113}$	565	2.0.4.1-565.4-a	S_4	565.4-a	25	173
$\mathfrak{p}_3\mathfrak{p}_5\overline{\mathfrak{p}}_{13}$	585	2.0.4.1-585.2-a	S_4	585.2-a	23	193
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{13}$	585	2.0.4.1-585.3-a	S_4	585.3-a	23	193
$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_{17}$	612	2.0.4.1-612.1-a	S_4	612.1-a	23	241
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_{17}$	612	2.0.4.1-612.2-a	S_4	612.2-a	24	241
$\mathfrak{p}_2^7\mathfrak{p}_5$	640	2.0.4.1-640.1-a	S_4	640.1-a	23	241
$\mathfrak{p}_2^7\overline{\mathfrak{p}}_5$	640	2.0.4.1-640.2-a	S_4	640.2-a	23	241
$\mathfrak{p}_2^4\mathfrak{p}_{41}$	656	2.0.4.1-656.1-a	S_4	656.1-a	20	277
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{41}$	656	2.0.4.1-656.2-a	S_4	656.2-a	20	277
$\mathfrak{p}_3\mathfrak{p}_{73}$	657	2.0.4.1-657.1-a	S_4	657.1-a	20	277
$\mathfrak{p}_3\overline{\mathfrak{p}}_{73}$	657	2.0.4.1-657.2-a	S_4	657.2-a	19	277
$\mathfrak{p}_2\mathfrak{p}_{337}$	674	2.0.4.1-674.1-a	S_4	674.1-a	24	241
$\mathfrak{p}_2\overline{\mathfrak{p}}_{337}$	674	2.0.4.1-674.2-a	S_4	674.2-a	25	241
$\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{17}$	680	2.0.4.1-680.1-a	S_4	680.1-a	31	373
$\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{17}$	680	2.0.4.1-680.1-b	S_4	680.1-b	31	373
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{17}$	680	2.0.4.1-680.4-a	S_4	680.4-a	32	373
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{17}$	680	2.0.4.1-680.4-b	S_4	680.4-b	32	373
$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_5$	720	2.0.4.1-720.1-a	S_4	720.1-a	24	277

Table 6.1: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-1})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^4\mathfrak{p}_3\overline{\mathfrak{p}}_5$	720	2.0.4.1-720.2-a	S_4	720.2-a	23	277
$\mathfrak{p}_5^2\mathfrak{p}_{29}$	725	2.0.4.1-725.1-a	S_4	725.1-a	24	229
$\mathfrak{p}_5^2\overline{\mathfrak{p}}_{29}$	725	2.0.4.1-725.2-a	S_4	725.2-a	28	373
$\mathfrak{p}_5^2\overline{\mathfrak{p}}_{29}$	725	2.0.4.1-725.2-b	S_4	725.2-b	28	373
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\mathfrak{p}_{29}$	725	2.0.4.1-725.3-a	S_4	725.3-a	32	373
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{29}$	725	2.0.4.1-725.4-a	S_4	725.4-a	33	373
$\overline{\mathfrak{p}}_5^2\mathfrak{p}_{29}$	725	2.0.4.1-725.5-a	S_4	725.5-a	28	373
$\overline{\mathfrak{p}}_5^2\mathfrak{p}_{29}$	725	2.0.4.1-725.5-b	S_4	725.5-b	28	373
$\overline{\mathfrak{p}}_5^2\overline{\mathfrak{p}}_{29}$	725	2.0.4.1-725.6-a	S_4	725.6-a	24	229
$\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_{37}$	740	2.0.4.1-740.1-a	S_4	740.1-a	30	601
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	740	2.0.4.1-740.4-a	S_4	740.4-a	30	601
$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{17}$	765	2.0.4.1-765.1-a	S_4	765.1-a	25	229
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{17}$	765	2.0.4.1-765.4-a	S_4	765.4-a	25	229
$\mathfrak{p}_2^2\mathfrak{p}_{193}$	772	2.0.4.1-772.1-a	S_4	772.1-a	28	229
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_{193}$	772	2.0.4.1-772.2-a	S_4	772.2-a	28	229
$\mathfrak{p}_5\mathfrak{p}_{157}$	785	2.0.4.1-785.1-a	S_4	785.1-a	25	313
$\mathfrak{p}_5\mathfrak{p}_{157}$	785	2.0.4.1-785.1-b	S_4	785.1-b	25	313
$\mathfrak{p}_5\overline{\mathfrak{p}}_{157}$	785	2.0.4.1-785.2-a	S_4	785.2-a	29	313
$\overline{\mathfrak{p}}_5\mathfrak{p}_{157}$	785	2.0.4.1-785.3-a	S_4	785.3-a	29	313
$\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{157}$	785	2.0.4.1-785.4-a	S_4	785.4-a	25	313
$\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{157}$	785	2.0.4.1-785.4-b	S_4	785.4-b	25	313
$\mathfrak{p}_2^5\mathfrak{p}_5^2$	800	2.0.4.1-800.1-a	S_4	800.1-a	23	313
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_5^2$	800	2.0.4.1-800.3-a	S_4	800.3-a	23	313
$\mathfrak{p}_{29}^2$	841	2.0.4.1-841.1-a	S_4	841.1-a	17	277
$\overline{\mathfrak{p}}_{29}^2$	841	2.0.4.1-841.3-a	S_4	841.3-a	17	277
$\mathfrak{p}_2^4\mathfrak{p}_{53}$	848	2.0.4.1-848.1-a	S_4	848.1-a	23	137
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{53}$	848	2.0.4.1-848.2-a	S_4	848.2-a	23	137
$\mathfrak{p}_{853}$	853	2.0.4.1-853.1-a	S_4	853.1-a	20	337
$\overline{\mathfrak{p}}_{853}$	853	2.0.4.1-853.2-a	S_4	853.2-a	19	337
$\mathfrak{p}_2\mathfrak{p}_{433}$	866	2.0.4.1-866.1-a	S_4	866.1-a	22	229
$\mathfrak{p}_2\overline{\mathfrak{p}}_{433}$	866	2.0.4.1-866.2-a	S_4	866.2-a	22	229
$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_5^2$	900	2.0.4.1-900.1-a	S_4	900.1-a	24	277
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_5^2$	900	2.0.4.1-900.3-a	S_4	900.3-a	23	277

Table 6.1: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-1})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^3\mathfrak{p}_{113}$	904	2.0.4.1-904.1-a	S_4	904.1-a	23	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{113}$	904	2.0.4.1-904.2-a	S_4	904.2-a	24	313
$\mathfrak{p}_5^2\overline{\mathfrak{p}}_{37}$	925	2.0.4.1-925.2-a	S_4	925.2-a	26	193
$\mathfrak{p}_5^2\overline{\mathfrak{p}}_{37}$	925	2.0.4.1-925.2-b	S_4	925.2-b	26	193
$\mathfrak{p}_5^2\overline{\mathfrak{p}}_{37}$	925	2.0.4.1-925.2-c	C_4	925.2-c	21	181
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\mathfrak{p}_{37}$	925	2.0.4.1-925.3-a	S_4	925.3-a	37	397
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	925	2.0.4.1-925.4-a	S_4	925.4-a	37	397
$\overline{\mathfrak{p}}_5^2\mathfrak{p}_{37}$	925	2.0.4.1-925.5-a	S_4	925.5-a	26	193
$\overline{\mathfrak{p}}_5^2\mathfrak{p}_{37}$	925	2.0.4.1-925.5-b	S_4	925.5-b	26	193
$\overline{\mathfrak{p}}_5^2\mathfrak{p}_{37}$	925	2.0.4.1-925.5-c	C_4	925.5-c	21	181
$\mathfrak{p}_2\mathfrak{p}_{13}\mathfrak{p}_{37}$	962	2.0.4.1-962.1-b	S_4	962.1-b	34	349
$\mathfrak{p}_2\mathfrak{p}_{13}\overline{\mathfrak{p}}_{37}$	962	2.0.4.1-962.2-a	S_4	962.2-a	35	409
$\mathfrak{p}_2\overline{\mathfrak{p}}_{13}\mathfrak{p}_{37}$	962	2.0.4.1-962.3-a	S_4	962.3-a	35	409
$\mathfrak{p}_2\overline{\mathfrak{p}}_{13}\overline{\mathfrak{p}}_{37}$	962	2.0.4.1-962.4-b	S_4	962.4-b	34	349
$\mathfrak{p}_5\mathfrak{p}_{193}$	965	2.0.4.1-965.1-a	S_4	965.1-a	25	337
$\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{193}$	965	2.0.4.1-965.4-a	S_4	965.4-a	25	337
$\mathfrak{p}_5\mathfrak{p}_{197}$	985	2.0.4.1-985.1-a	S_4	985.1-a	25	313
$\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{197}$	985	2.0.4.1-985.4-a	S_4	985.4-a	25	313
$\mathfrak{p}_2\mathfrak{p}_{17}\overline{\mathfrak{p}}_{29}$	986	2.0.4.1-986.2-a	S_4	986.2-a	31	353
$\mathfrak{p}_2\overline{\mathfrak{p}}_{17}\mathfrak{p}_{29}$	986	2.0.4.1-986.3-a	S_4	986.3-a	31	353

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_{47}$	47	2.0.11.1-47.1-a	S_4	47.1-a	24	577
$\overline{\mathfrak{p}}_{47}$	47	2.0.11.1-47.2-a	S_4	47.2-a	24	577
$\mathfrak{p}_{89}$	89	2.0.11.1-89.1-a	S_4	89.1-a	24	229
$\overline{\mathfrak{p}}_{89}$	89	2.0.11.1-89.2-a	S_4	89.2-a	25	229
$\mathfrak{p}_3^2\mathfrak{p}_{11}$	99	2.0.11.1-99.1-a	S_4	99.1-a	26	577
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	99	2.0.11.1-99.3-a	S_4	99.3-a	26	577
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	165	2.0.11.1-165.2-a	S_4	165.2-a	33	251
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{11}$	165	2.0.11.1-165.3-a	S_4	165.3-a	33	251

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\overline{\mathfrak{p}}_{59}$	177	2.0.11.1-177.2-a	S_4	177.2-a	26	163
$\overline{\mathfrak{p}}_3\mathfrak{p}_{59}$	177	2.0.11.1-177.3-a	S_4	177.3-a	26	163
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5$	180	2.0.11.1-180.3-a	S_4	180.3-a	33	379
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5$	180	2.0.11.1-180.4-a	S_4	180.4-a	33	379
$\mathfrak{p}_3^2\mathfrak{p}_{23}$	207	2.0.11.1-207.1-a	S_4	207.1-a	23	643
$\mathfrak{p}_3^2\mathfrak{p}_{23}$	207	2.0.11.1-207.1-b	S_4	207.1-b	22	181
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{23}$	207	2.0.11.1-207.6-a	S_4	207.6-a	22	643
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{23}$	207	2.0.11.1-207.6-b	S_4	207.6-b	22	181
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5\overline{\mathfrak{p}}_5$	225	2.0.11.1-225.5-b	S_4	225.5-b	30	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5\overline{\mathfrak{p}}_5$	225	2.0.11.1-225.5-c	S_4	225.5-c	30	331
$\mathfrak{p}_3^4\overline{\mathfrak{p}}_3$	243	2.0.11.1-243.2-a	S_4	243.2-a	17	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^4$	243	2.0.11.1-243.5-a	S_4	243.5-a	17	199
$\mathfrak{p}_5\mathfrak{p}_7$	245	2.0.11.1-245.1-a	S_4	245.1-a	36	421
$\overline{\mathfrak{p}}_5\mathfrak{p}_7$	245	2.0.11.1-245.2-a	S_4	245.2-a	36	421
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{23}$	276	2.0.11.1-276.1-a	S_4	276.1-a	34	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{23}$	276	2.0.11.1-276.4-a	S_4	276.4-a	34	433
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_5^2$	300	2.0.11.1-300.3-a	S_4	300.3-a	33	379
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_5^2$	300	2.0.11.1-300.3-b	S_4	300.3-b	33	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_5^2$	300	2.0.11.1-300.4-a	S_4	300.4-a	33	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_5^2$	300	2.0.11.1-300.4-b	S_4	300.4-b	33	379
$\mathfrak{p}_2\mathfrak{p}_3^3\overline{\mathfrak{p}}_3$	324	2.0.11.1-324.2-a	S_4	324.2-a	27	199
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^3$	324	2.0.11.1-324.4-a	S_4	324.4-a	27	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{37}$	333	2.0.11.1-333.3-a	S_4	333.3-a	23	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{37}$	333	2.0.11.1-333.4-a	S_4	333.4-a	24	331
$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$	345	2.0.11.1-345.1-a	S_4	345.1-a	34	421
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{23}$	345	2.0.11.1-345.8-a	S_4	345.8-a	34	421
$\mathfrak{p}_3^2\mathfrak{p}_{47}$	423	2.0.11.1-423.1-a	S_4	423.1-a	24	577
$\mathfrak{p}_3^2\mathfrak{p}_{47}$	423	2.0.11.1-423.1-b	S_4	423.1-b	22	313
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{47}$	423	2.0.11.1-423.3-a	S_4	423.3-a	25	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{47}$	423	2.0.11.1-423.4-a	S_4	423.4-a	25	199
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{47}$	423	2.0.11.1-423.6-a	S_4	423.6-a	24	577
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{47}$	423	2.0.11.1-423.6-b	S_4	423.6-b	22	313
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{31}$	465	2.0.11.1-465.4-a	S_4	465.4-a	36	631

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{31}$	465	2.0.11.1-465.4-b	S_4	465.4-b	36	631
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{31}$	465	2.0.11.1-465.5-a	S_4	465.5-a	36	631
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{31}$	465	2.0.11.1-465.5-b	S_4	465.5-b	36	631
$\mathfrak{p}_5\overline{\mathfrak{p}}_{97}$	485	2.0.11.1-485.2-a	S_4	485.2-a	30	317
$\mathfrak{p}_5\overline{\mathfrak{p}}_{97}$	485	2.0.11.1-485.2-b	S_4	485.2-b	36	367
$\overline{\mathfrak{p}}_5\mathfrak{p}_{97}$	485	2.0.11.1-485.3-a	S_4	485.3-a	35	367
$\overline{\mathfrak{p}}_5\mathfrak{p}_{97}$	485	2.0.11.1-485.3-b	S_4	485.3-b	30	317
$\mathfrak{p}_3^2\mathfrak{p}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.1-a	S_4	495.1-a	30	251
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.3-a	S_4	495.3-a	31	487
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.3-b	S_4	495.3-b	33	251
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.4-a	S_4	495.4-a	31	487
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.4-b	S_4	495.4-b	33	251
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	495	2.0.11.1-495.6-a	S_4	495.6-a	29	251
$\mathfrak{p}_2\mathfrak{p}_5^2\overline{\mathfrak{p}}_5$	500	2.0.11.1-500.2-a	S_4	500.2-a	40	709
$\mathfrak{p}_2\mathfrak{p}_5^2\overline{\mathfrak{p}}_5$	500	2.0.11.1-500.2-b	S_4	500.2-b	40	709
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_5^2$	500	2.0.11.1-500.3-a	S_4	500.3-a	39	709
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_5^2$	500	2.0.11.1-500.3-b	S_4	500.3-b	39	709
$\mathfrak{p}_3\mathfrak{p}_{179}$	537	2.0.11.1-537.1-a	S_4	537.1-a	26	163
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{179}$	537	2.0.11.1-537.4-a	S_4	537.4-a	26	163
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_5$	540	2.0.11.1-540.3-a	S_4	540.3-a	32	421
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_5$	540	2.0.11.1-540.6-a	S_4	540.6-a	31	421
$\mathfrak{p}_2\mathfrak{p}_3^3\overline{\mathfrak{p}}_5$	540	2.0.11.1-540.2-b	S_4	540.2-b	31	421
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^3\mathfrak{p}_5$	540	2.0.11.1-540.7-b	S_4	540.7-b	32	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{37}$	555	2.0.11.1-555.3-a	S_4	555.3-a	32	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	555	2.0.11.1-555.4-a	S_4	555.4-a	34	463
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	555	2.0.11.1-555.4-b	S_4	555.4-b	36	463
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{37}$	555	2.0.11.1-555.5-a	S_4	555.5-a	34	463
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{37}$	555	2.0.11.1-555.5-b	S_4	555.5-b	36	463
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\overline{\mathfrak{p}}_{37}$	555	2.0.11.1-555.6-a	S_4	555.6-a	32	421
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3$	576	2.0.11.1-576.2-b	S_4	576.2-b	26	199
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3$	576	2.0.11.1-576.2-c	S_4	576.2-c	26	199
$\mathfrak{p}_{11}\mathfrak{p}_{53}$	583	2.0.11.1-583.1-a	S_4	583.1-a	36	463
$\mathfrak{p}_{11}\overline{\mathfrak{p}}_{53}$	583	2.0.11.1-583.2-a	S_4	583.2-a	36	463

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{67}$	603	2.0.11.1-603.3-a	S_4	603.3-a	25	181
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{67}$	603	2.0.11.1-603.3-b	S_4	603.3-b	25	181
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{67}$	603	2.0.11.1-603.3-c	S_4	603.3-c	25	179
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{67}$	603	2.0.11.1-603.4-a	S_4	603.4-a	25	179
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{67}$	603	2.0.11.1-603.4-b	S_4	603.4-b	24	181
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{67}$	603	2.0.11.1-603.4-c	S_4	603.4-c	24	181
$\mathfrak{p}_{617}$	617	2.0.11.1-617.1-a	S_4	617.1-a	24	229
$\overline{\mathfrak{p}}_{617}$	617	2.0.11.1-617.2-a	S_4	617.2-a	24	229
$\mathfrak{p}_{619}$	619	2.0.11.1-619.1-a	S_4	619.1-a	24	661
$\overline{\mathfrak{p}}_{619}$	619	2.0.11.1-619.2-a	S_4	619.2-a	24	661
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_{31}$	620	2.0.11.1-620.2-a	S_4	620.2-a	43	1093
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_{31}$	620	2.0.11.1-620.2-c	S_4	620.2-c	44	1093
$\mathfrak{p}_2\overline{\mathfrak{p}}_5\mathfrak{p}_{31}$	620	2.0.11.1-620.3-b	S_4	620.3-b	43	1093
$\mathfrak{p}_2\overline{\mathfrak{p}}_5\mathfrak{p}_{31}$	620	2.0.11.1-620.3-c	S_4	620.3-c	44	1093
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{23}$	621	2.0.11.1-621.4-a	S_4	621.4-a	22	181
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{23}$	621	2.0.11.1-621.4-b	S_4	621.4-b	22	643
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{23}$	621	2.0.11.1-621.5-a	S_4	621.5-a	22	181
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{23}$	621	2.0.11.1-621.5-b	S_4	621.5-b	23	643
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{11}$	660	2.0.11.1-660.1-a	S_4	660.1-a	45	883
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	660	2.0.11.1-660.2-a	S_4	660.2-a	45	883
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{11}$	660	2.0.11.1-660.3-a	S_4	660.3-a	45	883
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{11}$	660	2.0.11.1-660.4-a	S_4	660.4-a	45	883
$\mathfrak{p}_2^3\mathfrak{p}_{11}$	704	2.0.11.1-704.1-b	S_4	704.1-b	37	433
$\mathfrak{p}_2^3\mathfrak{p}_{11}$	704	2.0.11.1-704.1-c	S_4	704.1-c	37	433
$\mathfrak{p}_3\mathfrak{p}_5\overline{\mathfrak{p}}_{47}$	705	2.0.11.1-705.2-a	S_4	705.2-a	35	433
$\mathfrak{p}_3\mathfrak{p}_5\overline{\mathfrak{p}}_{47}$	705	2.0.11.1-705.2-b	S_4	705.2-b	35	577
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{47}$	705	2.0.11.1-705.7-a	S_4	705.7-a	35	433
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\mathfrak{p}_{47}$	705	2.0.11.1-705.7-b	S_4	705.7-b	35	577
$\mathfrak{p}_2\mathfrak{p}_{179}$	716	2.0.11.1-716.1-a	S_4	716.1-a	38	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_{179}$	716	2.0.11.1-716.2-a	S_4	716.2-a	38	433
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5$	720	2.0.11.1-720.3-a	S_4	720.3-a	33	379
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5$	720	2.0.11.1-720.4-a	S_4	720.4-a	33	379
$\mathfrak{p}_2^2\mathfrak{p}_3^2\overline{\mathfrak{p}}_5$	720	2.0.11.1-720.2-a	S_4	720.2-a	31	421

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_5$	720	2.0.11.1-720.5-a	S_4	720.5-a	32	421
$\mathfrak{p}_3^5\overline{\mathfrak{p}}_3$	729	2.0.11.1-729.2-a	S_4	729.2-a	17	199
$\mathfrak{p}_3^5\overline{\mathfrak{p}}_3$	729	2.0.11.1-729.2-b	S_4	729.2-b	17	199
$\mathfrak{p}_3^4\overline{\mathfrak{p}}_3^2$	729	2.0.11.1-729.3-a	S_4	729.3-a	17	199
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^4$	729	2.0.11.1-729.5-a	S_4	729.5-a	17	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^5$	729	2.0.11.1-729.6-a	S_4	729.6-a	17	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^5$	729	2.0.11.1-729.6-b	S_4	729.6-b	17	199
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_7$	735	2.0.11.1-735.2-a	S_4	735.2-a	36	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\mathfrak{p}_7$	735	2.0.11.1-735.2-b	S_4	735.2-b	35	421
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_7$	735	2.0.11.1-735.3-a	S_4	735.3-a	36	421
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_7$	735	2.0.11.1-735.3-b	S_4	735.3-b	35	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_{251}$	753	2.0.11.1-753.2-b	S_4	753.2-b	26	163
$\overline{\mathfrak{p}}_3\mathfrak{p}_{251}$	753	2.0.11.1-753.3-b	S_4	753.3-b	26	163
$\mathfrak{p}_5^2\mathfrak{p}_{31}$	775	2.0.11.1-775.1-c	S_4	775.1-c	33	463
$\mathfrak{p}_5^2\mathfrak{p}_{31}$	775	2.0.11.1-775.1-d	S_4	775.1-d	33	463
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\mathfrak{p}_{31}$	775	2.0.11.1-775.3-a	S_4	775.3-a	41	757
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{31}$	775	2.0.11.1-775.4-a	S_4	775.4-a	41	757
$\overline{\mathfrak{p}}_5^2\overline{\mathfrak{p}}_{31}$	775	2.0.11.1-775.6-a	S_4	775.6-a	33	463
$\overline{\mathfrak{p}}_5^2\overline{\mathfrak{p}}_{31}$	775	2.0.11.1-775.6-d	S_4	775.6-d	33	463
$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{53}$	795	2.0.11.1-795.1-a	S_4	795.1-a	33	421
$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{53}$	795	2.0.11.1-795.1-b	S_4	795.1-b	31	421
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{53}$	795	2.0.11.1-795.8-a	S_4	795.8-a	33	421
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{53}$	795	2.0.11.1-795.8-b	S_4	795.8-b	31	421
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{89}$	801	2.0.11.1-801.2-a	S_4	801.2-a	25	229
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{89}$	801	2.0.11.1-801.5-a	S_4	801.5-a	25	229
$\mathfrak{p}_3^2\mathfrak{p}_{89}$	801	2.0.11.1-801.1-a	S_4	801.1-a	24	229
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{89}$	801	2.0.11.1-801.6-a	S_4	801.6-a	24	229
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{67}$	804	2.0.11.1-804.2-a	S_4	804.2-a	34	487
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_{67}$	804	2.0.11.1-804.3-a	S_4	804.3-a	34	487
$\mathfrak{p}_3\overline{\mathfrak{p}}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.3-a	S_4	825.3-a	33	251
$\mathfrak{p}_3\overline{\mathfrak{p}}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.3-b	S_4	825.3-b	33	251
$\mathfrak{p}_3\overline{\mathfrak{p}}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.3-c	S_4	825.3-c	33	251
$\overline{\mathfrak{p}}_3\mathfrak{p}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.4-a	S_4	825.4-a	33	251

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\overline{\mathfrak{p}}_3\mathfrak{p}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.4-b	S_4	825.4-b	33	251
$\overline{\mathfrak{p}}_3\mathfrak{p}_5^2\mathfrak{p}_{11}$	825	2.0.11.1-825.4-c	S_4	825.4-c	33	251
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{31}$	837	2.0.11.1-837.3-a	S_4	837.3-a	26	421
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{31}$	837	2.0.11.1-837.3-b	S_4	837.3-b	27	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{31}$	837	2.0.11.1-837.3-c	S_4	837.3-c	25	379
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{31}$	837	2.0.11.1-837.5-a	S_4	837.5-a	26	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{31}$	837	2.0.11.1-837.5-b	S_4	837.5-b	27	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{31}$	837	2.0.11.1-837.5-c	S_4	837.5-c	26	421
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.4-a	S_4	837.4-a	25	421
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.4-b	S_4	837.4-b	27	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.4-c	S_4	837.4-c	25	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.6-a	S_4	837.6-a	25	421
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.6-b	S_4	837.6-b	27	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{31}$	837	2.0.11.1-837.6-c	S_4	837.6-c	24	379
$\mathfrak{p}_{863}$	863	2.0.11.1-863.1-a	S_4	863.1-a	22	379
$\overline{\mathfrak{p}}_{863}$	863	2.0.11.1-863.2-a	S_4	863.2-a	22	379
$\mathfrak{p}_3\mathfrak{p}_{17}$	867	2.0.11.1-867.1-a	S_4	867.1-a	27	229
$\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	867	2.0.11.1-867.2-a	S_4	867.2-a	27	229
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{97}$	873	2.0.11.1-873.3-a	S_4	873.3-a	27	577
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{97}$	873	2.0.11.1-873.4-a	S_4	873.4-a	27	577
$\mathfrak{p}_3\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{59}$	885	2.0.11.1-885.4-a	S_4	885.4-a	32	367
$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_{59}$	885	2.0.11.1-885.5-a	S_4	885.5-a	31	367
$\mathfrak{p}_3^4\mathfrak{p}_{11}$	891	2.0.11.1-891.1-a	S_4	891.1-a	26	577
$\overline{\mathfrak{p}}_3^4\mathfrak{p}_{11}$	891	2.0.11.1-891.5-a	S_4	891.5-a	26	577
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	891	2.0.11.1-891.2-a	S_4	891.2-a	26	577
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	891	2.0.11.1-891.2-b	S_4	891.2-b	28	433
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	891	2.0.11.1-891.3-e	S_4	891.3-e	26	577
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	891	2.0.11.1-891.3-f	S_4	891.3-f	26	577
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^3\mathfrak{p}_{11}$	891	2.0.11.1-891.4-a	S_4	891.4-a	26	577
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^3\mathfrak{p}_{11}$	891	2.0.11.1-891.4-b	S_4	891.4-b	28	433
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5^2$	900	2.0.11.1-900.4-a	S_4	900.4-a	33	379
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5^2$	900	2.0.11.1-900.6-a	S_4	900.6-a	33	379
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_5^2$	900	2.0.11.1-900.3-a	S_4	900.3-a	31	421

Table 6.2: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-11})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_5^2$	900	2.0.11.1-900.3-b	S_4	900.3-b	31	421
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_5^2$	900	2.0.11.1-900.7-a	S_4	900.7-a	32	421
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_5^2$	900	2.0.11.1-900.7-b	S_4	900.7-b	32	421
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\mathfrak{p}_{37}$	925	2.0.11.1-925.3-a	S_4	925.3-a	46	1087
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\mathfrak{p}_{37}$	925	2.0.11.1-925.3-b	S_4	925.3-b	44	1087
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	925	2.0.11.1-925.4-a	S_4	925.4-a	46	1087
$\mathfrak{p}_5\overline{\mathfrak{p}}_5\overline{\mathfrak{p}}_{37}$	925	2.0.11.1-925.4-b	S_4	925.4-b	44	1087
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{103}$	927	2.0.11.1-927.3-a	S_4	927.3-a	28	229
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{103}$	927	2.0.11.1-927.4-a	S_4	927.4-a	29	229
$\mathfrak{p}_3\mathfrak{p}_{311}$	933	2.0.11.1-933.1-a	S_4	933.1-a	25	727
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{311}$	933	2.0.11.1-933.4-a	S_4	933.4-a	24	727
$\mathfrak{p}_3\mathfrak{p}_{313}$	939	2.0.11.1-939.1-a	S_4	939.1-a	29	661
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{313}$	939	2.0.11.1-939.4-a	S_4	939.4-a	29	661
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5$	960	2.0.11.1-960.1-b	S_4	960.1-b	30	313
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5$	960	2.0.11.1-960.1-c	S_4	960.1-c	32	313
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5$	960	2.0.11.1-960.1-d	S_4	960.1-d	33	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5$	960	2.0.11.1-960.4-a	S_4	960.4-a	33	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5$	960	2.0.11.1-960.4-c	S_4	960.4-c	30	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_5$	960	2.0.11.1-960.4-f	S_4	960.4-f	33	313
$\mathfrak{p}_{971}$	971	2.0.11.1-971.1-a	S_4	971.1-a	25	199
$\overline{\mathfrak{p}}_{971}$	971	2.0.11.1-971.2-a	S_4	971.2-a	25	199
$\mathfrak{p}_2\mathfrak{p}_3^3\overline{\mathfrak{p}}_3^2$	972	2.0.11.1-972.3-a	S_4	972.3-a	27	199
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^3$	972	2.0.11.1-972.4-a	S_4	972.4-a	27	199

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\mathfrak{p}_{17}$	51	2.0.8.1-51.1-a	S_4	51.1-a	25	307
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	51	2.0.8.1-51.4-a	S_4	51.4-a	25	307
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	99	2.0.8.1-99.3-a	S_4	99.3-a	22	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	99	2.0.8.1-99.4-a	S_4	99.4-a	22	331
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{19}$	114	2.0.8.1-114.1-a	S_4	114.1-a	31	307

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{19}$	114	2.0.8.1-114.4-a	S_4	114.4-a	31	307
$\mathfrak{p}_2^2\mathfrak{p}_{41}$	164	2.0.8.1-164.1-a	S_4	164.1-a	32	379
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_{41}$	164	2.0.8.1-164.2-a	S_4	164.2-a	32	379
$\mathfrak{p}_2\mathfrak{p}_{97}$	194	2.0.8.1-194.1-a	S_4	194.1-a	36	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_{97}$	194	2.0.8.1-194.2-a	S_4	194.2-a	36	457
$\mathfrak{p}_3\overline{\mathfrak{p}}_{73}$	219	2.0.8.1-219.2-a	S_4	219.2-a	24	313
$\overline{\mathfrak{p}}_3\mathfrak{p}_{73}$	219	2.0.8.1-219.3-a	S_4	219.3-a	24	313
$\mathfrak{p}_3^2\mathfrak{p}_5$	225	2.0.8.1-225.1-a	S_4	225.1-a	22	409
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_5$	225	2.0.8.1-225.3-a	S_4	225.3-a	22	409
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{41}$	246	2.0.8.1-246.2-a	S_4	246.2-a	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_{41}$	246	2.0.8.1-246.3-a	S_4	246.3-a	32	379
$\mathfrak{p}_3\mathfrak{p}_{83}$	249	2.0.8.1-249.1-a	S_4	249.1-a	20	409
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{83}$	249	2.0.8.1-249.4-a	S_4	249.4-a	21	409
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{43}$	258	2.0.8.1-258.1-a	S_4	258.1-a	32	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{43}$	258	2.0.8.1-258.4-a	S_4	258.4-a	33	337
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_{11}$	264	2.0.8.1-264.1-a	S_4	264.1-a	29	283
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	264	2.0.8.1-264.4-a	S_4	264.4-a	29	283
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	297	2.0.8.1-297.3-a	S_4	297.3-a	22	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	297	2.0.8.1-297.6-a	S_4	297.6-a	22	331
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_{11}$	297	2.0.8.1-297.2-b	S_4	297.2-b	22	331
$\overline{\mathfrak{p}}_3^3\mathfrak{p}_{11}$	297	2.0.8.1-297.7-b	S_4	297.7-b	22	331
$\mathfrak{p}_{17}\mathfrak{p}_{19}$	323	2.0.8.1-323.1-a	S_4	323.1-a	33	547
$\mathfrak{p}_{17}\mathfrak{p}_{19}$	323	2.0.8.1-323.1-b	S_4	323.1-b	33	547
$\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	323	2.0.8.1-323.4-a	S_4	323.4-a	32	547
$\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	323	2.0.8.1-323.4-b	S_4	323.4-b	32	547
$\mathfrak{p}_2^2\mathfrak{p}_{83}$	332	2.0.8.1-332.1-a	S_4	332.1-a	36	433
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_{83}$	332	2.0.8.1-332.2-a	S_4	332.2-a	36	433
$\mathfrak{p}_{337}$	337	2.0.8.1-337.1-a	S_4	337.1-a	25	283
$\overline{\mathfrak{p}}_{337}$	337	2.0.8.1-337.2-a	S_4	337.2-a	24	283
$\mathfrak{p}_3\mathfrak{p}_{113}$	339	2.0.8.1-339.1-a	S_4	339.1-a	25	283
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{113}$	339	2.0.8.1-339.4-a	S_4	339.4-a	25	283
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{59}$	354	2.0.8.1-354.1-a	S_4	354.1-a	31	547
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{59}$	354	2.0.8.1-354.4-a	S_4	354.4-a	30	547

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\overline{\mathfrak{p}}_{11}^2$	363	2.0.8.1-363.3-a	S_4	363.3-a	22	331
$\overline{\mathfrak{p}}_3\mathfrak{p}_{11}^2$	363	2.0.8.1-363.4-a	S_4	363.4-a	22	331
$\mathfrak{p}_3\mathfrak{p}_{11}^2$	363	2.0.8.1-363.1-a	S_4	363.1-a	21	283
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}^2$	363	2.0.8.1-363.6-a	S_4	363.6-a	21	283
$\mathfrak{p}_3^2\mathfrak{p}_{41}$	369	2.0.8.1-369.1-a	S_4	369.1-a	25	307
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{41}$	369	2.0.8.1-369.2-a	S_4	369.2-a	26	307
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{41}$	369	2.0.8.1-369.2-b	S_4	369.2-b	25	307
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{41}$	369	2.0.8.1-369.2-c	S_4	369.2-c	25	307
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{41}$	369	2.0.8.1-369.5-a	S_4	369.5-a	26	307
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{41}$	369	2.0.8.1-369.5-b	S_4	369.5-b	25	307
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{41}$	369	2.0.8.1-369.5-c	S_4	369.5-c	25	307
$\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{41}$	369	2.0.8.1-369.6-a	S_4	369.6-a	25	307
$\mathfrak{p}_2^7\mathfrak{p}_3$	384	2.0.8.1-384.1-a	S_4	384.1-a	22	211
$\mathfrak{p}_2^7\mathfrak{p}_3$	384	2.0.8.1-384.1-b	S_4	384.1-b	22	211
$\mathfrak{p}_2^7\overline{\mathfrak{p}}_3$	384	2.0.8.1-384.2-a	S_4	384.2-a	22	211
$\mathfrak{p}_2^7\overline{\mathfrak{p}}_3$	384	2.0.8.1-384.2-b	S_4	384.2-b	22	211
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{43}$	387	2.0.8.1-387.2-a	S_4	387.2-a	25	433
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{43}$	387	2.0.8.1-387.5-a	S_4	387.5-a	25	433
$\mathfrak{p}_2^2\mathfrak{p}_3^2\overline{\mathfrak{p}}_{11}$	396	2.0.8.1-396.2-a	S_4	396.2-a	29	379
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	396	2.0.8.1-396.5-a	S_4	396.5-a	30	379
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_{17}$	408	2.0.8.1-408.2-a	S_4	408.2-a	29	251
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	408	2.0.8.1-408.3-a	S_4	408.3-a	29	251
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	459	2.0.8.1-459.4-a	S_4	459.4-a	25	307
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{17}$	459	2.0.8.1-459.5-a	S_4	459.5-a	25	307
$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_{41}$	492	2.0.8.1-492.1-a	S_4	492.1-a	31	379
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{41}$	492	2.0.8.1-492.4-a	S_4	492.4-a	33	379
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{83}$	498	2.0.8.1-498.1-a	S_4	498.1-a	35	433
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{83}$	498	2.0.8.1-498.1-c	S_4	498.1-c	35	457
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{83}$	498	2.0.8.1-498.1-d	S_4	498.1-d	35	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{83}$	498	2.0.8.1-498.4-b	S_4	498.4-b	35	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{83}$	498	2.0.8.1-498.4-c	S_4	498.4-c	35	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{83}$	498	2.0.8.1-498.4-d	S_4	498.4-d	35	457
$\mathfrak{p}_2\mathfrak{p}_{251}$	502	2.0.8.1-502.1-a	S_4	502.1-a	35	353

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_{251}$	502	2.0.8.1-502.2-a	S_4	502.2-a	35	353
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{19}$	513	2.0.8.1-513.3-a	S_4	513.3-a	22	313
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{19}$	513	2.0.8.1-513.5-a	S_4	513.5-a	22	313
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{19}$	513	2.0.8.1-513.4-a	S_4	513.4-a	21	313
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{19}$	513	2.0.8.1-513.6-a	S_4	513.6-a	21	313
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_{43}$	516	2.0.8.1-516.2-a	S_4	516.2-a	32	499
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3\mathfrak{p}_{43}$	516	2.0.8.1-516.3-a	S_4	516.3-a	33	499
$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{11}$	528	2.0.8.1-528.1-a	S_4	528.1-a	29	283
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	528	2.0.8.1-528.4-a	S_4	528.4-a	29	283
$\mathfrak{p}_2^3\mathfrak{p}_{67}$	536	2.0.8.1-536.1-a	S_4	536.1-a	29	307
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{67}$	536	2.0.8.1-536.2-a	S_4	536.2-a	29	307
$\mathfrak{p}_3\overline{\mathfrak{p}}_{11}\mathfrak{p}_{17}$	561	2.0.8.1-561.3-a	S_4	561.3-a	35	433
$\mathfrak{p}_3\overline{\mathfrak{p}}_{11}\mathfrak{p}_{17}$	561	2.0.8.1-561.3-b	S_4	561.3-b	37	433
$\overline{\mathfrak{p}}_3\mathfrak{p}_{11}\overline{\mathfrak{p}}_{17}$	561	2.0.8.1-561.6-a	S_4	561.6-a	35	433
$\overline{\mathfrak{p}}_3\mathfrak{p}_{11}\overline{\mathfrak{p}}_{17}$	561	2.0.8.1-561.6-b	S_4	561.6-b	37	433
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{97}$	582	2.0.8.1-582.2-a	S_4	582.2-a	38	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_{97}$	582	2.0.8.1-582.3-a	S_4	582.3-a	37	457
$\mathfrak{p}_2\mathfrak{p}_3^3\overline{\mathfrak{p}}_{11}$	594	2.0.8.1-594.2-a	S_4	594.2-a	29	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^3\mathfrak{p}_{11}$	594	2.0.8.1-594.7-a	S_4	594.7-a	30	379
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	594	2.0.8.1-594.3-a	S_4	594.3-a	30	379
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	594	2.0.8.1-594.6-a	S_4	594.6-a	29	379
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{67}$	603	2.0.8.1-603.2-a	S_4	603.2-a	29	337
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{67}$	603	2.0.8.1-603.3-a	S_4	603.3-a	28	313
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{67}$	603	2.0.8.1-603.4-a	S_4	603.4-a	28	313
$\overline{\mathfrak{p}}_3^2\mathfrak{p}_{67}$	603	2.0.8.1-603.5-a	S_4	603.5-a	28	337
$\mathfrak{p}_2^2\mathfrak{p}_3^2\overline{\mathfrak{p}}_{17}$	612	2.0.8.1-612.2-b	S_4	612.2-b	30	457
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{17}$	612	2.0.8.1-612.5-b	S_4	612.5-b	31	457
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	612	2.0.8.1-612.3-a	S_4	612.3-a	31	571
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	612	2.0.8.1-612.4-a	S_4	612.4-a	31	571
$\mathfrak{p}_3\overline{\mathfrak{p}}_{11}\mathfrak{p}_{19}$	627	2.0.8.1-627.3-a	S_4	627.3-a	31	331
$\overline{\mathfrak{p}}_3\mathfrak{p}_{11}\overline{\mathfrak{p}}_{19}$	627	2.0.8.1-627.6-a	S_4	627.6-a	31	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_{211}$	633	2.0.8.1-633.2-a	S_4	633.2-a	23	211
$\overline{\mathfrak{p}}_3\mathfrak{p}_{211}$	633	2.0.8.1-633.3-a	S_4	633.3-a	23	211

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_{641}$	641	2.0.8.1-641.1-a	S_4	641.1-a	23	211
$\overline{\mathfrak{p}}_{641}$	641	2.0.8.1-641.2-a	S_4	641.2-a	23	211
$\mathfrak{p}_2\mathfrak{p}_{17}\mathfrak{p}_{19}$	646	2.0.8.1-646.1-a	S_4	646.1-a	44	691
$\mathfrak{p}_2\mathfrak{p}_{17}\mathfrak{p}_{19}$	646	2.0.8.1-646.1-b	S_4	646.1-b	44	691
$\mathfrak{p}_2\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	646	2.0.8.1-646.4-a	S_4	646.4-a	43	691
$\mathfrak{p}_2\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	646	2.0.8.1-646.4-b	S_4	646.4-b	44	691
$\mathfrak{p}_2^4\mathfrak{p}_{41}$	656	2.0.8.1-656.1-a	S_4	656.1-a	32	379
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{41}$	656	2.0.8.1-656.2-a	S_4	656.2-a	32	379
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{73}$	657	2.0.8.1-657.3-a	S_4	657.3-a	24	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{73}$	657	2.0.8.1-657.4-a	S_4	657.4-a	24	331
$\mathfrak{p}_3^3\mathfrak{p}_5$	675	2.0.8.1-675.1-a	S_4	675.1-a	22	409
$\overline{\mathfrak{p}}_3^3\mathfrak{p}_5$	675	2.0.8.1-675.4-a	S_4	675.4-a	22	409
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_5$	675	2.0.8.1-675.2-a	S_4	675.2-a	22	409
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_5$	675	2.0.8.1-675.3-a	S_4	675.3-a	22	409
$\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_{19}$	684	2.0.8.1-684.1-a	S_4	684.1-a	31	307
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{19}$	684	2.0.8.1-684.6-a	S_4	684.6-a	31	307
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{19}$	684	2.0.8.1-684.3-a	S_4	684.3-a	32	307
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{19}$	684	2.0.8.1-684.4-a	S_4	684.4-a	32	307
$\mathfrak{p}_3\overline{\mathfrak{p}}_{233}$	699	2.0.8.1-699.2-a	S_4	699.2-a	27	499
$\overline{\mathfrak{p}}_3\mathfrak{p}_{233}$	699	2.0.8.1-699.3-a	S_4	699.3-a	27	499
$\mathfrak{p}_3\mathfrak{p}_{241}$	723	2.0.8.1-723.1-a	S_4	723.1-a	27	307
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{241}$	723	2.0.8.1-723.4-a	S_4	723.4-a	26	307
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{11}^2$	726	2.0.8.1-726.3-a	S_4	726.3-a	29	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_{11}^2$	726	2.0.8.1-726.4-a	S_4	726.4-a	30	379
$\mathfrak{p}_{11}\mathfrak{p}_{67}$	737	2.0.8.1-737.1-b	S_4	737.1-b	36	409
$\mathfrak{p}_{11}\overline{\mathfrak{p}}_{67}$	737	2.0.8.1-737.2-a	S_4	737.2-a	36	577
$\overline{\mathfrak{p}}_{11}\mathfrak{p}_{67}$	737	2.0.8.1-737.3-a	S_4	737.3-a	36	577
$\overline{\mathfrak{p}}_{11}\overline{\mathfrak{p}}_{67}$	737	2.0.8.1-737.4-b	S_4	737.4-b	36	409
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_{41}$	738	2.0.8.1-738.2-b	S_4	738.2-b	32	379
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_{41}$	738	2.0.8.1-738.2-c	S_4	738.2-c	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{41}$	738	2.0.8.1-738.5-b	S_4	738.5-b	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{41}$	738	2.0.8.1-738.5-c	S_4	738.5-c	32	379
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{83}$	747	2.0.8.1-747.3-a	S_4	747.3-a	20	409

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{83}$	747	2.0.8.1-747.4-a	S_4	747.4-a	21	409
$\mathfrak{p}_3\mathfrak{p}_{257}$	771	2.0.8.1-771.1-a	S_4	771.1-a	25	283
$\mathfrak{p}_3\mathfrak{p}_{257}$	771	2.0.8.1-771.1-b	S_4	771.1-b	24	139
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{257}$	771	2.0.8.1-771.4-a	S_4	771.4-a	24	139
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{257}$	771	2.0.8.1-771.4-b	S_4	771.4-b	25	283
$\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_{11}$	792	2.0.8.1-792.1-a	S_4	792.1-a	28	313
$\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_{11}$	792	2.0.8.1-792.1-b	S_4	792.1-b	28	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	792	2.0.8.1-792.6-a	S_4	792.6-a	28	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	792	2.0.8.1-792.6-b	S_4	792.6-b	28	313
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	792	2.0.8.1-792.3-a	S_4	792.3-a	29	283
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	792	2.0.8.1-792.3-b	S_4	792.3-b	30	283
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	792	2.0.8.1-792.3-c	S_4	792.3-c	30	523
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	792	2.0.8.1-792.4-a	S_4	792.4-a	29	283
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	792	2.0.8.1-792.4-b	S_4	792.4-b	29	523
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{11}$	792	2.0.8.1-792.4-c	S_4	792.4-c	29	283
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{89}$	801	2.0.8.1-801.3-a	S_4	801.3-a	27	283
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{89}$	801	2.0.8.1-801.4-a	S_4	801.4-a	27	283
$\mathfrak{p}_2^4\mathfrak{p}_3\overline{\mathfrak{p}}_{17}$	816	2.0.8.1-816.2-a	S_4	816.2-a	29	251
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	816	2.0.8.1-816.3-a	S_4	816.3-a	29	251
$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{17}$	816	2.0.8.1-816.1-a	S_4	816.1-a	30	307
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	816	2.0.8.1-816.4-a	S_4	816.4-a	30	307
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{139}$	834	2.0.8.1-834.1-a	S_4	834.1-a	35	409
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{139}$	834	2.0.8.1-834.4-a	S_4	834.4-a	35	409
$\mathfrak{p}_2^5\mathfrak{p}_3^3$	864	2.0.8.1-864.1-a	D_4	864.1-a	25	433
$\mathfrak{p}_2^5\mathfrak{p}_3^3$	864	2.0.8.1-864.1-b	D_4	864.1-b	25	433
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_3^3$	864	2.0.8.1-864.4-a	D_4	864.4-a	25	433
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_3^3$	864	2.0.8.1-864.4-b	D_4	864.4-b	25	433
$\mathfrak{p}_3\mathfrak{p}_{17}^2$	867	2.0.8.1-867.1-a	S_4	867.1-a	25	307
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}^2$	867	2.0.8.1-867.6-a	S_4	867.6-a	25	307
$\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.1-a	S_4	882.1-a	37	571
$\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.1-b	S_4	882.1-b	37	571
$\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.1-c	S_4	882.1-c	37	571
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.3-a	S_4	882.3-a	37	571

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.3-b	S_4	882.3-b	37	571
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\mathfrak{p}_7$	882	2.0.8.1-882.3-c	S_4	882.3-c	37	571
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_3\mathfrak{p}_{11}$	891	2.0.8.1-891.3-a	S_4	891.3-a	22	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	891	2.0.8.1-891.5-a	S_4	891.5-a	22	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\mathfrak{p}_{11}$	891	2.0.8.1-891.5-c	S_4	891.5-c	22	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	891	2.0.8.1-891.6-a	S_4	891.6-a	22	331
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{11}$	891	2.0.8.1-891.6-c	S_4	891.6-c	22	331
$\mathfrak{p}_3\overline{\mathfrak{p}}_3^3\overline{\mathfrak{p}}_{11}$	891	2.0.8.1-891.8-a	S_4	891.8-a	22	331
$\mathfrak{p}_3^4\overline{\mathfrak{p}}_{11}$	891	2.0.8.1-891.2-a	S_4	891.2-a	22	331
$\overline{\mathfrak{p}}_3^4\mathfrak{p}_{11}$	891	2.0.8.1-891.9-a	S_4	891.9-a	22	331
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5$	900	2.0.8.1-900.2-a	S_4	900.2-a	35	499
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_5$	900	2.0.8.1-900.2-b	S_4	900.2-b	35	499
$\mathfrak{p}_2^3\mathfrak{p}_{113}$	904	2.0.8.1-904.1-a	S_4	904.1-a	35	499
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{113}$	904	2.0.8.1-904.2-a	S_4	904.2-a	35	499
$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{19}$	912	2.0.8.1-912.1-a	S_4	912.1-a	31	307
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{19}$	912	2.0.8.1-912.4-a	S_4	912.4-a	31	307
$\mathfrak{p}_2\mathfrak{p}_3^3\overline{\mathfrak{p}}_{17}$	918	2.0.8.1-918.2-a	S_4	918.2-a	30	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_3^3\mathfrak{p}_{17}$	918	2.0.8.1-918.7-a	S_4	918.7-a	31	457
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	918	2.0.8.1-918.3-a	S_4	918.3-a	31	457
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\mathfrak{p}_{17}$	918	2.0.8.1-918.3-c	S_4	918.3-c	31	331
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{17}$	918	2.0.8.1-918.5-a	S_4	918.5-a	31	331
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\mathfrak{p}_{17}$	918	2.0.8.1-918.5-b	S_4	918.5-b	31	457
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	918	2.0.8.1-918.4-a	S_4	918.4-a	31	331
$\mathfrak{p}_2\mathfrak{p}_3^2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}$	918	2.0.8.1-918.4-b	S_4	918.4-b	30	457
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{17}$	918	2.0.8.1-918.6-a	S_4	918.6-a	30	457
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{17}$	918	2.0.8.1-918.6-c	S_4	918.6-c	31	331
$\mathfrak{p}_{929}$	929	2.0.8.1-929.1-a	S_4	929.1-a	24	499
$\overline{\mathfrak{p}}_{929}$	929	2.0.8.1-929.2-a	S_4	929.2-a	25	499
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\mathfrak{p}_{107}$	963	2.0.8.1-963.3-a	S_4	963.3-a	22	457
$\mathfrak{p}_3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{107}$	963	2.0.8.1-963.4-a	S_4	963.4-a	22	457
$\mathfrak{p}_2^3\mathfrak{p}_{11}^2$	968	2.0.8.1-968.1-a	S_4	968.1-a	28	313
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{11}^2$	968	2.0.8.1-968.3-a	S_4	968.3-a	28	313
$\mathfrak{p}_3\mathfrak{p}_{17}\mathfrak{p}_{19}$	969	2.0.8.1-969.1-a	S_4	969.1-a	32	347

Table 6.3: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-2})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\mathfrak{p}_{17}\mathfrak{p}_{19}$	969	2.0.8.1-969.1-b	S_4	969.1-b	31	409
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	969	2.0.8.1-969.8-a	S_4	969.8-a	32	347
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{17}\overline{\mathfrak{p}}_{19}$	969	2.0.8.1-969.8-b	S_4	969.8-b	31	409
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{163}$	978	2.0.8.1-978.1-c	S_4	978.1-c	32	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{163}$	978	2.0.8.1-978.4-c	S_4	978.4-c	32	433
$\mathfrak{p}_{11}\overline{\mathfrak{p}}_{89}$	979	2.0.8.1-979.2-a	S_4	979.2-a	34	409
$\overline{\mathfrak{p}}_{11}\mathfrak{p}_{89}$	979	2.0.8.1-979.3-a	S_4	979.3-a	34	409
$\mathfrak{p}_2\mathfrak{p}_{491}$	982	2.0.8.1-982.1-a	S_4	982.1-a	34	433
$\mathfrak{p}_2\mathfrak{p}_{491}$	982	2.0.8.1-982.1-b	S_4	982.1-b	33	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_{491}$	982	2.0.8.1-982.2-a	S_4	982.2-a	33	433
$\mathfrak{p}_2\overline{\mathfrak{p}}_{491}$	982	2.0.8.1-982.2-b	S_4	982.2-b	34	433
$\mathfrak{p}_2^3\mathfrak{p}_3\overline{\mathfrak{p}}_{41}$	984	2.0.8.1-984.2-a	S_4	984.2-a	31	379
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\mathfrak{p}_{41}$	984	2.0.8.1-984.3-a	S_4	984.3-a	30	379
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_{41}$	984	2.0.8.1-984.1-a	S_4	984.1-a	31	571
$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_{41}$	984	2.0.8.1-984.1-b	S_4	984.1-b	29	379
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{41}$	984	2.0.8.1-984.4-a	S_4	984.4-a	33	571
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{41}$	984	2.0.8.1-984.4-b	S_4	984.4-b	30	379
$\mathfrak{p}_3\mathfrak{p}_{331}$	993	2.0.8.1-993.1-a	S_4	993.1-a	23	211
$\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_{331}$	993	2.0.8.1-993.4-a	S_4	993.4-a	24	211

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_{23}$	46	2.0.7.1-46.2-a	S_4	46.2-a	22	373
$\overline{\mathfrak{p}}_2\mathfrak{p}_{23}$	46	2.0.7.1-46.3-a	S_4	46.3-a	22	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_{43}$	86	2.0.7.1-86.2-a	S_4	86.2-a	27	331
$\overline{\mathfrak{p}}_2\mathfrak{p}_{43}$	86	2.0.7.1-86.3-a	S_4	86.3-a	27	331
$\mathfrak{p}_2^3\mathfrak{p}_{11}$	88	2.0.7.1-88.1-a	S_4	88.1-a	25	331
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{11}$	88	2.0.7.1-88.2-a	S_4	88.2-a	23	421
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_{11}$	88	2.0.7.1-88.7-a	S_4	88.7-a	23	421
$\overline{\mathfrak{p}}_2^3\overline{\mathfrak{p}}_{11}$	88	2.0.7.1-88.8-a	S_4	88.8-a	24	331
$\mathfrak{p}_2\mathfrak{p}_{79}$	158	2.0.7.1-158.1-a	S_4	158.1-a	23	163

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{79}$	158	2.0.7.1-158.4-a	S_4	158.4-a	24	163
$\mathfrak{p}_2^3\mathfrak{p}_5$	200	2.0.7.1-200.1-a	S_4	200.1-a	26	337
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_5$	200	2.0.7.1-200.4-a	S_4	200.4-a	26	337
$\mathfrak{p}_2^5\mathfrak{p}_7$	224	2.0.7.1-224.1-a	S_4	224.1-a	23	421
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\mathfrak{p}_7$	224	2.0.7.1-224.2-a	S_4	224.2-a	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_7$	224	2.0.7.1-224.5-a	S_4	224.5-a	32	379
$\overline{\mathfrak{p}}_2^5\mathfrak{p}_7$	224	2.0.7.1-224.6-a	S_4	224.6-a	22	421
$\mathfrak{p}_2\mathfrak{p}_{11}^2$	242	2.0.7.1-242.1-a	S_4	242.1-a	26	331
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{11}^2$	242	2.0.7.1-242.6-a	S_4	242.6-a	26	331
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_2^3$	256	2.0.7.1-256.4-a	S_4	256.4-a	22	457
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2^5$	256	2.0.7.1-256.6-a	S_4	256.6-a	21	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{67}$	268	2.0.7.1-268.3-b	S_4	268.3-b	33	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{67}$	268	2.0.7.1-268.4-b	S_4	268.4-b	33	337
$\mathfrak{p}_2^5\mathfrak{p}_3$	288	2.0.7.1-288.1-a	S_4	288.1-a	16	499
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\mathfrak{p}_3$	288	2.0.7.1-288.2-a	S_4	288.2-a	21	179
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_3$	288	2.0.7.1-288.5-a	S_4	288.5-a	21	179
$\overline{\mathfrak{p}}_2^5\mathfrak{p}_3$	288	2.0.7.1-288.6-a	S_4	288.6-a	16	499
$\mathfrak{p}_2\mathfrak{p}_{151}$	302	2.0.7.1-302.1-a	S_4	302.1-a	26	457
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{151}$	302	2.0.7.1-302.4-a	S_4	302.4-a	25	457
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_{79}$	316	2.0.7.1-316.2-a	S_4	316.2-a	24	211
$\overline{\mathfrak{p}}_2^2\mathfrak{p}_{79}$	316	2.0.7.1-316.5-a	S_4	316.5-a	24	211
$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{23}$	322	2.0.7.1-322.1-a	S_4	322.1-a	35	547
$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{23}$	322	2.0.7.1-322.1-b	S_4	322.1-b	35	547
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{23}$	322	2.0.7.1-322.4-a	S_4	322.4-a	35	547
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{23}$	322	2.0.7.1-322.4-b	S_4	322.4-b	35	547
$\mathfrak{p}_2\mathfrak{p}_{163}$	326	2.0.7.1-326.1-a	S_4	326.1-a	25	331
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{163}$	326	2.0.7.1-326.4-a	S_4	326.4-a	25	331
$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7$	350	2.0.7.1-350.1-a	S_4	350.1-a	38	463
$\overline{\mathfrak{p}}_2\mathfrak{p}_5\mathfrak{p}_7$	350	2.0.7.1-350.2-a	S_4	350.2-a	38	463
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{11}$	352	2.0.7.1-352.4-a	S_4	352.4-a	30	233
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_{11}$	352	2.0.7.1-352.9-a	S_4	352.9-a	30	233
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{23}$	368	2.0.7.1-368.4-a	S_4	368.4-a	34	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\mathfrak{p}_{23}$	368	2.0.7.1-368.7-a	S_4	368.7-a	34	337

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{11}$	396	2.0.7.1-396.3-b	S_4	396.3-b	32	499
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{11}$	396	2.0.7.1-396.4-b	S_4	396.4-b	32	499
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{23}$	414	2.0.7.1-414.2-a	S_4	414.2-a	22	373
$\overline{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{23}$	414	2.0.7.1-414.3-a	S_4	414.3-a	21	373
$\mathfrak{p}_2\mathfrak{p}_{211}$	422	2.0.7.1-422.1-a	S_4	422.1-a	27	337
$\mathfrak{p}_2\mathfrak{p}_{211}$	422	2.0.7.1-422.1-b	S_4	422.1-b	27	337
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{211}$	422	2.0.7.1-422.4-a	S_4	422.4-a	27	337
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{211}$	422	2.0.7.1-422.4-b	S_4	422.4-b	27	337
$\mathfrak{p}_2^3\mathfrak{p}_{53}$	424	2.0.7.1-424.1-a	S_4	424.1-a	23	193
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{53}$	424	2.0.7.1-424.2-a	S_4	424.2-a	21	163
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{53}$	424	2.0.7.1-424.2-b	S_4	424.2-b	22	277
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_{53}$	424	2.0.7.1-424.7-a	S_4	424.7-a	21	163
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_{53}$	424	2.0.7.1-424.7-b	S_4	424.7-b	22	277
$\overline{\mathfrak{p}}_2^3\overline{\mathfrak{p}}_{53}$	424	2.0.7.1-424.8-a	S_4	424.8-a	23	193
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{107}$	428	2.0.7.1-428.3-a	S_4	428.3-a	33	499
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{107}$	428	2.0.7.1-428.4-a	S_4	428.4-a	34	499
$\mathfrak{p}_2^6\mathfrak{p}_7$	448	2.0.7.1-448.1-a	S_4	448.1-a	23	421
$\overline{\mathfrak{p}}_2^6\mathfrak{p}_7$	448	2.0.7.1-448.7-a	S_4	448.7-a	22	421
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{29}$	464	2.0.7.1-464.2-a	S_4	464.2-a	23	457
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{29}$	464	2.0.7.1-464.2-b	S_4	464.2-b	24	277
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{29}$	464	2.0.7.1-464.4-a	S_4	464.4-a	33	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\mathfrak{p}_{29}$	464	2.0.7.1-464.7-a	S_4	464.7-a	33	277
$\overline{\mathfrak{p}}_2^4\mathfrak{p}_{29}$	464	2.0.7.1-464.9-a	S_4	464.9-a	24	457
$\overline{\mathfrak{p}}_2^4\mathfrak{p}_{29}$	464	2.0.7.1-464.9-b	S_4	464.9-b	25	277
$\mathfrak{p}_2\mathfrak{p}_{233}$	466	2.0.7.1-466.1-a	S_4	466.1-a	25	331
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{233}$	466	2.0.7.1-466.4-a	S_4	466.4-a	25	331
$\mathfrak{p}_{11}\mathfrak{p}_{43}$	473	2.0.7.1-473.1-a	S_4	473.1-a	28	571
$\overline{\mathfrak{p}}_{11}\overline{\mathfrak{p}}_{43}$	473	2.0.7.1-473.4-a	S_4	473.4-a	28	571
$\mathfrak{p}_2\mathfrak{p}_{239}$	478	2.0.7.1-478.1-a	S_4	478.1-a	25	331
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{239}$	478	2.0.7.1-478.4-a	S_4	478.4-a	24	331
$\mathfrak{p}_2\mathfrak{p}_{11}\mathfrak{p}_{23}$	506	2.0.7.1-506.1-a	S_4	506.1-a	35	373
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{11}\overline{\mathfrak{p}}_{23}$	506	2.0.7.1-506.8-a	S_4	506.8-a	35	373
$\mathfrak{p}_2^7\overline{\mathfrak{p}}_2^2$	512	2.0.7.1-512.3-a	S_4	512.3-a	22	179

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^7\overline{\mathfrak{p}}_2^2$	512	2.0.7.1-512.3-b	S_4	512.3-b	22	179
$\mathfrak{p}_2^6\overline{\mathfrak{p}}_2^3$	512	2.0.7.1-512.4-a	S_4	512.4-a	22	457
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_2^4$	512	2.0.7.1-512.5-a	S_4	512.5-a	22	457
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2^5$	512	2.0.7.1-512.6-a	S_4	512.6-a	21	457
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2^6$	512	2.0.7.1-512.7-a	S_4	512.7-a	21	457
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2^7$	512	2.0.7.1-512.8-a	S_4	512.8-a	21	179
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2^7$	512	2.0.7.1-512.8-b	S_4	512.8-b	21	179
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{29}$	522	2.0.7.1-522.1-a	S_4	522.1-a	24	457
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{29}$	522	2.0.7.1-522.1-b	S_4	522.1-b	24	193
$\overline{\mathfrak{p}}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{29}$	522	2.0.7.1-522.4-a	S_4	522.4-a	25	193
$\overline{\mathfrak{p}}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{29}$	522	2.0.7.1-522.4-b	S_4	522.4-b	24	457
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2\mathfrak{p}_{67}$	536	2.0.7.1-536.3-a	S_4	536.3-a	33	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^2\overline{\mathfrak{p}}_{67}$	536	2.0.7.1-536.6-a	S_4	536.6-a	33	337
$\mathfrak{p}_7^2\mathfrak{p}_{11}$	539	2.0.7.1-539.1-a	S_4	539.1-a	25	193
$\mathfrak{p}_7^2\overline{\mathfrak{p}}_{11}$	539	2.0.7.1-539.2-a	S_4	539.2-a	25	193
$\mathfrak{p}_5\mathfrak{p}_{23}$	575	2.0.7.1-575.1-a	S_4	575.1-a	29	379
$\mathfrak{p}_5\overline{\mathfrak{p}}_{23}$	575	2.0.7.1-575.2-a	S_4	575.2-a	29	379
$\mathfrak{p}_2^6\mathfrak{p}_3$	576	2.0.7.1-576.1-a	S_4	576.1-a	16	499
$\overline{\mathfrak{p}}_2^6\mathfrak{p}_3$	576	2.0.7.1-576.7-a	S_4	576.7-a	16	499
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{37}$	592	2.0.7.1-592.2-a	S_4	592.2-a	23	277
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\mathfrak{p}_{37}$	592	2.0.7.1-592.3-a	S_4	592.3-a	36	463
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\overline{\mathfrak{p}}_{37}$	592	2.0.7.1-592.8-a	S_4	592.8-a	35	463
$\overline{\mathfrak{p}}_2^4\mathfrak{p}_{37}$	592	2.0.7.1-592.9-a	S_4	592.9-a	23	277
$\mathfrak{p}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{43}$	602	2.0.7.1-602.2-b	S_4	602.2-b	37	499
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\mathfrak{p}_{43}$	602	2.0.7.1-602.3-a	S_4	602.3-a	37	499
$\mathfrak{p}_3\mathfrak{p}_{67}$	603	2.0.7.1-603.1-a	S_4	603.1-a	20	127
$\mathfrak{p}_3\overline{\mathfrak{p}}_{67}$	603	2.0.7.1-603.2-a	S_4	603.2-a	19	127
$\mathfrak{p}_2^3\mathfrak{p}_7\mathfrak{p}_{11}$	616	2.0.7.1-616.1-a	S_4	616.1-a	35	379
$\mathfrak{p}_2^3\mathfrak{p}_7\mathfrak{p}_{11}$	616	2.0.7.1-616.1-b	S_4	616.1-b	35	379
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_7\overline{\mathfrak{p}}_{11}$	616	2.0.7.1-616.8-a	S_4	616.8-a	35	379
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_7\overline{\mathfrak{p}}_{11}$	616	2.0.7.1-616.8-b	S_4	616.8-b	35	379
$\mathfrak{p}_{617}$	617	2.0.7.1-617.1-a	S_4	617.1-a	20	331
$\overline{\mathfrak{p}}_{617}$	617	2.0.7.1-617.2-a	S_4	617.2-a	20	331

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\mathfrak{p}_{11}\mathfrak{p}_{29}$	638	2.0.7.1-638.1-a	S_4	638.1-a	35	541
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{11}\overline{\mathfrak{p}}_{29}$	638	2.0.7.1-638.8-a	S_4	638.8-a	35	541
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_7\mathfrak{p}_{23}$	644	2.0.7.1-644.3-a	S_4	644.3-a	42	613
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{23}$	644	2.0.7.1-644.4-a	S_4	644.4-a	42	613
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{163}$	652	2.0.7.1-652.3-a	S_4	652.3-a	37	463
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{163}$	652	2.0.7.1-652.4-a	S_4	652.4-a	37	463
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{37}$	666	2.0.7.1-666.2-a	S_4	666.2-a	24	463
$\overline{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{37}$	666	2.0.7.1-666.3-a	S_4	666.3-a	24	463
$\mathfrak{p}_{23}\mathfrak{p}_{29}$	667	2.0.7.1-667.1-a	S_4	667.1-a	22	163
$\overline{\mathfrak{p}}_{23}\overline{\mathfrak{p}}_{29}$	667	2.0.7.1-667.4-a	S_4	667.4-a	22	163
$\mathfrak{p}_2^4\mathfrak{p}_{43}$	688	2.0.7.1-688.1-a	S_4	688.1-a	24	277
$\overline{\mathfrak{p}}_2^4\overline{\mathfrak{p}}_{43}$	688	2.0.7.1-688.10-a	S_4	688.10-a	24	277
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{43}$	688	2.0.7.1-688.4-a	S_4	688.4-a	31	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\mathfrak{p}_{43}$	688	2.0.7.1-688.7-a	S_4	688.7-a	32	373
$\mathfrak{p}_2\mathfrak{p}_{347}$	694	2.0.7.1-694.1-a	S_4	694.1-a	25	331
$\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{347}$	694	2.0.7.1-694.4-a	S_4	694.4-a	25	331
$\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_7$	700	2.0.7.1-700.1-a	S_4	700.1-a	38	463
$\overline{\mathfrak{p}}_2^2\mathfrak{p}_5\mathfrak{p}_7$	700	2.0.7.1-700.3-a	S_4	700.3-a	38	463
$\mathfrak{p}_2^6\mathfrak{p}_{11}$	704	2.0.7.1-704.1-a	S_4	704.1-a	25	331
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2^4\overline{\mathfrak{p}}_{11}$	704	2.0.7.1-704.10-a	S_4	704.10-a	30	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^5\mathfrak{p}_{11}$	704	2.0.7.1-704.11-a	S_4	704.11-a	31	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^5\overline{\mathfrak{p}}_{11}$	704	2.0.7.1-704.12-a	S_4	704.12-a	31	337
$\overline{\mathfrak{p}}_2^6\mathfrak{p}_{11}$	704	2.0.7.1-704.13-a	S_4	704.13-a	23	421
$\overline{\mathfrak{p}}_2^6\overline{\mathfrak{p}}_{11}$	704	2.0.7.1-704.14-a	S_4	704.14-a	24	331
$\mathfrak{p}_2^6\overline{\mathfrak{p}}_{11}$	704	2.0.7.1-704.2-a	S_4	704.2-a	23	421
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_2\mathfrak{p}_{11}$	704	2.0.7.1-704.3-a	S_4	704.3-a	31	337
$\mathfrak{p}_2^5\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{11}$	704	2.0.7.1-704.4-a	S_4	704.4-a	32	337
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2^2\mathfrak{p}_{11}$	704	2.0.7.1-704.5-a	S_4	704.5-a	30	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_{359}$	718	2.0.7.1-718.2-a	S_4	718.2-a	24	457
$\overline{\mathfrak{p}}_2\mathfrak{p}_{359}$	718	2.0.7.1-718.3-a	S_4	718.3-a	24	457
$\mathfrak{p}_2^5\mathfrak{p}_{23}$	736	2.0.7.1-736.1-a	S_4	736.1-a	25	193
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\overline{\mathfrak{p}}_{23}$	736	2.0.7.1-736.10-a	S_4	736.10-a	34	337
$\overline{\mathfrak{p}}_2^5\overline{\mathfrak{p}}_{23}$	736	2.0.7.1-736.12-a	S_4	736.12-a	25	193

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\mathfrak{p}_{23}$	736	2.0.7.1-736.3-a	S_4	736.3-a	32	337
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{23}$	736	2.0.7.1-736.4-a	S_4	736.4-a	34	337
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2^2\overline{\mathfrak{p}}_{23}$	736	2.0.7.1-736.6-a	S_4	736.6-a	33	337
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2^3\mathfrak{p}_{23}$	736	2.0.7.1-736.7-a	S_4	736.7-a	32	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_{23}$	736	2.0.7.1-736.9-a	S_4	736.9-a	32	337
$\mathfrak{p}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{53}$	742	2.0.7.1-742.2-a	S_4	742.2-a	36	373
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\mathfrak{p}_{53}$	742	2.0.7.1-742.3-a	S_4	742.3-a	36	373
$\mathfrak{p}_7\mathfrak{p}_{107}$	749	2.0.7.1-749.1-a	S_4	749.1-a	27	277
$\mathfrak{p}_7\overline{\mathfrak{p}}_{107}$	749	2.0.7.1-749.2-a	S_4	749.2-a	26	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{191}$	764	2.0.7.1-764.3-a	S_4	764.3-a	34	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{191}$	764	2.0.7.1-764.3-b	S_4	764.3-b	34	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{191}$	764	2.0.7.1-764.4-a	S_4	764.4-a	34	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{191}$	764	2.0.7.1-764.4-b	S_4	764.4-b	34	457
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{43}$	774	2.0.7.1-774.1-a	S_4	774.1-a	23	499
$\overline{\mathfrak{p}}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{43}$	774	2.0.7.1-774.4-a	S_4	774.4-a	23	499
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\mathfrak{p}_7^2$	784	2.0.7.1-784.2-a	S_4	784.2-a	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\mathfrak{p}_7^2$	784	2.0.7.1-784.4-a	S_4	784.4-a	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{197}$	788	2.0.7.1-788.3-a	S_4	788.3-a	29	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_{197}$	788	2.0.7.1-788.3-b	S_4	788.3-b	32	421
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{197}$	788	2.0.7.1-788.4-a	S_4	788.4-a	29	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{197}$	788	2.0.7.1-788.4-b	S_4	788.4-b	31	421
$\mathfrak{p}_2^5\mathfrak{p}_5$	800	2.0.7.1-800.1-a	S_4	800.1-a	28	277
$\overline{\mathfrak{p}}_2^5\mathfrak{p}_5$	800	2.0.7.1-800.6-a	S_4	800.6-a	27	277
$\mathfrak{p}_2\overline{\mathfrak{p}}_{401}$	802	2.0.7.1-802.2-a	S_4	802.2-a	24	193
$\overline{\mathfrak{p}}_2\mathfrak{p}_{401}$	802	2.0.7.1-802.3-a	S_4	802.3-a	24	193
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_7\mathfrak{p}_{29}$	812	2.0.7.1-812.3-a	S_4	812.3-a	38	701
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{29}$	812	2.0.7.1-812.4-a	S_4	812.4-a	39	701
$\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}}_{23}$	828	2.0.7.1-828.2-a	S_4	828.2-a	22	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{23}$	828	2.0.7.1-828.3-a	S_4	828.3-a	33	457
$\mathfrak{p}_2\overline{\mathfrak{p}}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{23}$	828	2.0.7.1-828.4-a	S_4	828.4-a	36	457
$\overline{\mathfrak{p}}_2^2\mathfrak{p}_3\mathfrak{p}_{23}$	828	2.0.7.1-828.5-a	S_4	828.5-a	21	373
$\mathfrak{p}_7\mathfrak{p}_{11}^2$	847	2.0.7.1-847.1-a	S_4	847.1-a	25	193
$\mathfrak{p}_7\overline{\mathfrak{p}}_{11}^2$	847	2.0.7.1-847.3-a	S_4	847.3-a	25	193

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{53}$	848	2.0.7.1-848.2-a	S_4	848.2-a	23	211
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_{53}$	848	2.0.7.1-848.2-b	S_4	848.2-b	23	211
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2\mathfrak{p}_{53}$	848	2.0.7.1-848.3-a	S_4	848.3-a	32	331
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^3\overline{\mathfrak{p}}_{53}$	848	2.0.7.1-848.8-a	S_4	848.8-a	32	331
$\overline{\mathfrak{p}}_2^4\mathfrak{p}_{53}$	848	2.0.7.1-848.9-a	S_4	848.9-a	24	211
$\overline{\mathfrak{p}}_2^4\mathfrak{p}_{53}$	848	2.0.7.1-848.9-b	S_4	848.9-b	24	211
$\mathfrak{p}_2^2\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{107}$	856	2.0.7.1-856.4-b	S_4	856.4-b	34	499
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^2\mathfrak{p}_{107}$	856	2.0.7.1-856.5-b	S_4	856.5-b	33	499
$\mathfrak{p}_2^6\overline{\mathfrak{p}}_2\mathfrak{p}_7$	896	2.0.7.1-896.2-a	S_4	896.2-a	32	379
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2^3\mathfrak{p}_7$	896	2.0.7.1-896.4-a	S_4	896.4-a	32	379
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_2^4\mathfrak{p}_7$	896	2.0.7.1-896.5-a	S_4	896.5-a	32	379
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^6\mathfrak{p}_7$	896	2.0.7.1-896.7-a	S_4	896.7-a	32	379
$\mathfrak{p}_2^5\mathfrak{p}_{29}$	928	2.0.7.1-928.1-a	S_4	928.1-a	24	373
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\overline{\mathfrak{p}}_{29}$	928	2.0.7.1-928.10-a	S_4	928.10-a	33	337
$\overline{\mathfrak{p}}_2^5\overline{\mathfrak{p}}_{29}$	928	2.0.7.1-928.12-a	S_4	928.12-a	24	373
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\mathfrak{p}_{29}$	928	2.0.7.1-928.3-a	S_4	928.3-a	33	337
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{29}$	928	2.0.7.1-928.4-a	S_4	928.4-a	32	487
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{29}$	928	2.0.7.1-928.4-b	S_4	928.4-b	32	487
$\mathfrak{p}_2^4\overline{\mathfrak{p}}_2\overline{\mathfrak{p}}_{29}$	928	2.0.7.1-928.4-c	S_4	928.4-c	33	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_{29}$	928	2.0.7.1-928.9-a	S_4	928.9-a	32	487
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_{29}$	928	2.0.7.1-928.9-b	S_4	928.9-b	32	487
$\mathfrak{p}_2\overline{\mathfrak{p}}_2^4\mathfrak{p}_{29}$	928	2.0.7.1-928.9-c	S_4	928.9-c	33	337
$\mathfrak{p}_2\overline{\mathfrak{p}}_{11}\overline{\mathfrak{p}}_{43}$	946	2.0.7.1-946.4-a	S_4	946.4-a	34	613
$\overline{\mathfrak{p}}_2\mathfrak{p}_{11}\mathfrak{p}_{43}$	946	2.0.7.1-946.5-a	S_4	946.5-a	34	613
$\mathfrak{p}_7\mathfrak{p}_{137}$	959	2.0.7.1-959.1-a	S_4	959.1-a	25	463
$\mathfrak{p}_7\overline{\mathfrak{p}}_{137}$	959	2.0.7.1-959.2-a	S_4	959.2-a	25	463
$\overline{\mathfrak{p}}_2^3\mathfrak{p}_{11}\overline{\mathfrak{p}}_{11}$	968	2.0.7.1-968.11-a	S_4	968.11-a	32	331
$\mathfrak{p}_2^3\mathfrak{p}_{11}\overline{\mathfrak{p}}_{11}$	968	2.0.7.1-968.2-a	S_4	968.2-a	31	331
$\mathfrak{p}_2\overline{\mathfrak{p}}_{491}$	982	2.0.7.1-982.2-a	S_4	982.2-a	25	211
$\overline{\mathfrak{p}}_2\mathfrak{p}_{491}$	982	2.0.7.1-982.3-a	S_4	982.3-a	26	211
$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{71}$	994	2.0.7.1-994.1-a	S_4	994.1-a	35	373
$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{71}$	994	2.0.7.1-994.1-b	S_4	994.1-b	35	373
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{71}$	994	2.0.7.1-994.4-a	S_4	994.4-a	34	373

Table 6.4: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-7})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\overline{\mathfrak{p}}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{71}$	994	2.0.7.1-994.4-b	S_4	994.4-b	34	373

Table 6.5: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-3})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\mathfrak{p}_{31}$	124	2.0.3.1-124.1-a	A_4	124.1-a	35	271
$\mathfrak{p}_2\overline{\mathfrak{p}}_{31}$	124	2.0.3.1-124.2-a	A_4	124.2-a	35	271
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{19}$	228	2.0.3.1-228.1-a	A_4	228.1-a	35	373
$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_{19}$	228	2.0.3.1-228.2-a	A_4	228.2-a	35	373
$\mathfrak{p}_{241}$	241	2.0.3.1-241.1-a	A_4	241.1-a	19	79
$\overline{\mathfrak{p}}_{241}$	241	2.0.3.1-241.2-a	A_4	241.2-a	19	79
$\mathfrak{p}_3\mathfrak{p}_7\mathfrak{p}_{13}$	273	2.0.3.1-273.1-a	A_4	273.1-a	30	271
$\mathfrak{p}_3\overline{\mathfrak{p}}_7\overline{\mathfrak{p}}_{13}$	273	2.0.3.1-273.4-a	A_4	273.4-a	30	271
$\mathfrak{p}_{283}$	283	2.0.3.1-283.1-a	A_4	283.1-a	23	211
$\overline{\mathfrak{p}}_{283}$	283	2.0.3.1-283.2-a	A_4	283.2-a	23	211
$\mathfrak{p}_{379}$	379	2.0.3.1-379.1-a	A_4	379.1-a	24	163
$\overline{\mathfrak{p}}_{379}$	379	2.0.3.1-379.2-a	A_4	379.2-a	24	163
$\mathfrak{p}_3\mathfrak{p}_7\overline{\mathfrak{p}}_{19}$	399	2.0.3.1-399.2-a	A_4	399.2-a	32	211
$\mathfrak{p}_3\overline{\mathfrak{p}}_7\mathfrak{p}_{19}$	399	2.0.3.1-399.3-a	A_4	399.3-a	32	211
$\mathfrak{p}_2\mathfrak{p}_{103}$	412	2.0.3.1-412.1-a	A_4	412.1-a	33	439
$\mathfrak{p}_2\overline{\mathfrak{p}}_{103}$	412	2.0.3.1-412.2-a	A_4	412.2-a	33	439
$\mathfrak{p}_3\mathfrak{p}_{139}$	417	2.0.3.1-417.1-a	A_4	417.1-a	23	157
$\mathfrak{p}_3\overline{\mathfrak{p}}_{139}$	417	2.0.3.1-417.2-a	A_4	417.2-a	23	157
$\mathfrak{p}_5\mathfrak{p}_{19}$	475	2.0.3.1-475.1-a	A_4	475.1-a	32	607
$\mathfrak{p}_5\overline{\mathfrak{p}}_{19}$	475	2.0.3.1-475.2-a	A_4	475.2-a	32	607
$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{37}$	481	2.0.3.1-481.2-a	A_4	481.2-a	35	283
$\overline{\mathfrak{p}}_{13}\mathfrak{p}_{37}$	481	2.0.3.1-481.3-a	A_4	481.3-a	35	283
$\mathfrak{p}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{19}$	532	2.0.3.1-532.2-a	A_4	532.2-a	50	727
$\mathfrak{p}_2\overline{\mathfrak{p}}_7\mathfrak{p}_{19}$	532	2.0.3.1-532.3-a	A_4	532.3-a	50	727
$\mathfrak{p}_7\overline{\mathfrak{p}}_{79}$	553	2.0.3.1-553.2-a	A_4	553.2-a	34	433
$\overline{\mathfrak{p}}_7\mathfrak{p}_{79}$	553	2.0.3.1-553.3-a	A_4	553.3-a	34	433
$\mathfrak{p}_3\mathfrak{p}_{193}$	579	2.0.3.1-579.1-a	A_4	579.1-a	22	151

Table 6.5: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-3})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_3\mathfrak{p}_{193}$	579	2.0.3.1-579.1-b	A_4	579.1-b	22	151
$\mathfrak{p}_3\overline{\mathfrak{p}}_{193}$	579	2.0.3.1-579.2-a	A_4	579.2-a	22	151
$\mathfrak{p}_3\overline{\mathfrak{p}}_{193}$	579	2.0.3.1-579.2-b	A_4	579.2-b	22	151
$\mathfrak{p}_3^2\mathfrak{p}_{67}$	603	2.0.3.1-603.1-a	A_4	603.1-a	21	163
$\mathfrak{p}_3^2\overline{\mathfrak{p}}_{67}$	603	2.0.3.1-603.2-a	A_4	603.2-a	21	163
$\mathfrak{p}_3\mathfrak{p}_7\overline{\mathfrak{p}}_{31}$	651	2.0.3.1-651.2-a	A_4	651.2-a	34	271
$\mathfrak{p}_3\overline{\mathfrak{p}}_7\mathfrak{p}_{31}$	651	2.0.3.1-651.3-a	A_4	651.3-a	34	271
$\mathfrak{p}_{673}$	673	2.0.3.1-673.1-a	A_4	673.1-a	21	157
$\overline{\mathfrak{p}}_{673}$	673	2.0.3.1-673.2-a	A_4	673.2-a	21	157
$\mathfrak{p}_7\mathfrak{p}_{97}$	679	2.0.3.1-679.1-a	A_4	679.1-a	35	331
$\mathfrak{p}_7\overline{\mathfrak{p}}_{97}$	679	2.0.3.1-679.2-a	A_4	679.2-a	32	331
$\overline{\mathfrak{p}}_7\mathfrak{p}_{97}$	679	2.0.3.1-679.3-a	A_4	679.3-a	32	331
$\overline{\mathfrak{p}}_7\overline{\mathfrak{p}}_{97}$	679	2.0.3.1-679.4-a	A_4	679.4-a	35	331
$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7$	700	2.0.3.1-700.1-a	A_4	700.1-a	53	661
$\mathfrak{p}_2\mathfrak{p}_5\overline{\mathfrak{p}}_7$	700	2.0.3.1-700.2-a	A_4	700.2-a	53	661
$\mathfrak{p}_7\overline{\mathfrak{p}}_{103}$	721	2.0.3.1-721.2-a	A_4	721.2-a	32	271
$\overline{\mathfrak{p}}_7\mathfrak{p}_{103}$	721	2.0.3.1-721.3-a	A_4	721.3-a	32	271
$\mathfrak{p}_3\mathfrak{p}_{241}$	723	2.0.3.1-723.1-a	A_4	723.1-a	20	139
$\mathfrak{p}_3\overline{\mathfrak{p}}_{241}$	723	2.0.3.1-723.2-a	A_4	723.2-a	20	139
$\mathfrak{p}_3\mathfrak{p}_{13}\mathfrak{p}_{19}$	741	2.0.3.1-741.1-a	A_4	741.1-a	36	367
$\mathfrak{p}_3\overline{\mathfrak{p}}_{13}\overline{\mathfrak{p}}_{19}$	741	2.0.3.1-741.4-a	A_4	741.4-a	36	367
$\mathfrak{p}_{13}\mathfrak{p}_{61}$	793	2.0.3.1-793.1-a	A_4	793.1-a	31	331
$\overline{\mathfrak{p}}_{13}\overline{\mathfrak{p}}_{61}$	793	2.0.3.1-793.4-a	A_4	793.4-a	32	331
$\mathfrak{p}_2^3\mathfrak{p}_{13}$	832	2.0.3.1-832.1-a	A_4	832.1-a	28	307
$\mathfrak{p}_2^3\mathfrak{p}_{13}$	832	2.0.3.1-832.1-b	A_4	832.1-b	29	307
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{13}$	832	2.0.3.1-832.2-a	A_4	832.2-a	28	307
$\mathfrak{p}_2^3\overline{\mathfrak{p}}_{13}$	832	2.0.3.1-832.2-b	A_4	832.2-b	29	307
$\mathfrak{p}_3^3\mathfrak{p}_{31}$	837	2.0.3.1-837.1-a	A_4	837.1-a	21	223
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_{31}$	837	2.0.3.1-837.2-a	A_4	837.2-a	21	223
$\mathfrak{p}_{853}$	853	2.0.3.1-853.1-a	A_4	853.1-a	21	139
$\overline{\mathfrak{p}}_{853}$	853	2.0.3.1-853.2-a	A_4	853.2-a	21	139
$\mathfrak{p}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{31}$	868	2.0.3.1-868.2-a	A_4	868.2-a	52	661
$\mathfrak{p}_2\mathfrak{p}_7\overline{\mathfrak{p}}_{31}$	868	2.0.3.1-868.2-c	A_4	868.2-c	52	661

Table 6.5: Sextic field method on elliptic curves E defined over $\mathbb{Q}(\sqrt{-3})$ with $N_E \leq 1000$

$\mathfrak{N}$	$N(\mathfrak{N})$	E label	$\tilde{\rho}(\mathscr{G}_K)$	BMF	♯ primes	max p
$\mathfrak{p}_2\overline{\mathfrak{p}}_7\mathfrak{p}_{31}$	868	2.0.3.1-868.3-a	A_4	868.3-a	50	661
$\mathfrak{p}_2\overline{\mathfrak{p}}_7\mathfrak{p}_{31}$	868	2.0.3.1-868.3-c	A_4	868.3-c	50	661
$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{67}$	871	2.0.3.1-871.2-a	A_4	871.2-a	35	229
$\overline{\mathfrak{p}}_{13}\mathfrak{p}_{67}$	871	2.0.3.1-871.3-a	A_4	871.3-a	35	229
$\mathfrak{p}_3\mathfrak{p}_7\mathfrak{p}_{43}$	903	2.0.3.1-903.1-a	A_4	903.1-a	34	277
$\mathfrak{p}_3\overline{\mathfrak{p}}_7\overline{\mathfrak{p}}_{43}$	903	2.0.3.1-903.4-a	A_4	903.4-a	34	277
$\mathfrak{p}_7^2\overline{\mathfrak{p}}_{19}$	931	2.0.3.1-931.2-a	A_4	931.2-a	32	211
$\overline{\mathfrak{p}}_7^2\mathfrak{p}_{19}$	931	2.0.3.1-931.5-a	A_4	931.5-a	32	211
$\mathfrak{p}_3\mathfrak{p}_{313}$	939	2.0.3.1-939.1-a	A_4	939.1-a	20	157
$\mathfrak{p}_3\overline{\mathfrak{p}}_{313}$	939	2.0.3.1-939.2-a	A_4	939.2-a	20	157
$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{73}$	949	2.0.3.1-949.2-a	A_4	949.2-a	38	373
$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{73}$	949	2.0.3.1-949.2-b	A_4	949.2-b	37	373
$\overline{\mathfrak{p}}_{13}\mathfrak{p}_{73}$	949	2.0.3.1-949.3-a	A_4	949.3-a	38	373
$\overline{\mathfrak{p}}_{13}\mathfrak{p}_{73}$	949	2.0.3.1-949.3-b	A_4	949.3-b	37	373
$\mathfrak{p}_3^3\mathfrak{p}_{37}$	999	2.0.3.1-999.1-a	A_4	999.1-a	17	163
$\mathfrak{p}_3^3\overline{\mathfrak{p}}_{37}$	999	2.0.3.1-999.2-a	A_4	999.2-a	17	163

Here we have reported a small sample of our calculations. Indeed, we have proved modularity of all the absolutely irreducible isogeny classes of non-CM elliptic curves defined over $\mathbb{Q}(\sqrt{-1})$ that are neither $\mathbb{Q}$-curves nor non-base change curves. Moreover, we have proved conditional modularity for the irreducible but not absolutely irreducible cases. We can summarise the tables in the following theorem

Theorem 6.1.1. *Let E be an elliptic curve defined over $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-3})$, with conductor norm less than 1000 and irreducible mod 3 representation. Then E is modular modulo 3, and if the residual representation is absolutely irreducible than E is modular.*

At the moment of writing, we also have the same result for all the isogeny classes of elliptic curves defined over $\mathbb{Q}(\sqrt{-1})$, and almost all the isogeny classes over $\mathbb{Q}(\sqrt{-11})$ with the same properties as before. We are doing it using both our method and the very recent results in modularity lifting as we will present in the next session.

6.2 Modularity lifting

As we have seen in the last set of examples, one of the applications of our 3-adic Faltings-Serre method is to prove that a given elliptic curve E is modular and identify the correct automorphic form related to E. The check is in two steps:

1) Determine the residual representation, i.e. to identify its determinant character, irreducibility, image, splitting field and if it is possible to apply Theorem 3.7.1 to prove residual isomorphism with a candidate representation.

2) If the conditions of Theorem 5.2.1 are satisfied, then prove whether the candidate representation is isomorphic to the representation attached to E.

Thanks to some very recent developments in the modularity lifting theory presented in [1] and [2], under certain hypotheses, step 1 is by itself enough to conclude that our elliptic curve is modular. Indeed, the following is a special case of [[2], Theorem 8.1, p. 69] that can be deduced from the discussion of § 9 of the same paper.

Theorem (Allen, Khare, Thorne, 2019)**.** *Let E be a non CM elliptic curve defined over a CM number field K, and let $\rho_{E,3} : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_3)$ be the attached 3-adic Galois representation. Assume the followings hold*

1) *$\bar{\rho}_{E,3}$ is decomposed generic and $\bar{\rho}_{E,3}|_{\mathscr{G}_{K(\zeta_3)}}$ is absolutely irreducible.*

2) *At any place $v \mid 3$, E_{K_v} is ordinary.*

3) *There exists an isomorphism $\iota : \bar{\mathbb{Q}}_3 \simeq \mathbb{C}$ and a cuspidal, regular algebraic automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$ such that $\overline{\rho_{\iota,\pi}} \simeq \bar{\rho}_{E,3}$.*

Then E is modular: there is a cuspidal, regular algebraic automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_K)$ such that $\rho_{E,3} \simeq \rho_\Pi$.

For sake of completeness we recall the definition of decomposed generic from [1, Definition 4.3.1, p. 54]:

Definition. Let k be a finite field of characteristic p.

(1) Let $\ell \neq p$ be a prime, and let $L/\mathbb{Q}_\ell$ be a finite extension. We say that a continuous representation $\bar{\rho} : \mathscr{G}_L \longrightarrow \mathrm{GL}_n(k)$ is generic if it is unramified and the eigenvalues $\alpha_1, \ldots, \alpha_n \in \bar{k}$ (with multiplicity) of $\bar{\rho}(\mathrm{Frob}_L)$ satisfy $\alpha_i/\alpha_j \notin \{1, |\mathcal{O}_L/\mathrm{m}_L|\}$ for all $i \neq j$.

(2) Let L be a number field, and let $\bar{\rho} : \mathscr{G}_L \longrightarrow \mathrm{GL}_n(k)$ be a continuous representation. We say that a prime $\ell \neq p$ is *decomposed generic* for $\bar{\rho}$ if ℓ splits completely in L and for all places $v|\ell$ of L, $\bar{\rho}|_{\mathscr{G}_{L_v}}$ is generic.

(3) Let L be a number field, and let $\bar{\rho} : \mathscr{G}_L \longrightarrow \mathrm{GL}_n(k)$ be a continuous representation. We say that $\bar{\rho}$ is *decomposed generic* if there exists a prime $\ell \neq p$ which is decomposed generic for $\bar{\rho}$.

However, we have the following

Proposition 6.2.1. *when $K/\mathbb{Q}$ is Galois and $\bar{\rho}|_{\mathscr{G}_{K(\zeta_3)}}$ is absolutely irreducible, then $\bar{\rho}$ is decomposed generic.*

Proof. By the hypothesis we must have $\bar{\rho}$ absolutely irreducible. Thus, by the results of Chapter 3, we know that $\bar{\rho}(\mathscr{G}_K)$ contains a conjugacy class X of elements with characteristic polynomial $x^2 + 1$. But then, for each $\gamma \in X$ the ratio of the two eigenvalues of γ is equal to -1. Since $K/\mathbb{Q}$ is Galois then by Chebotarev we have infinitely many prime numbers $\ell \neq 3$ that split completely in K and such that for all places $v|\ell$ we have $\bar{\rho}(\mathrm{Frob}_v) \in X$, i.e. ℓ is decomposed generic. □

When $\bar{\rho}$ has cyclotomic determinant then we can easily verify the condition on $\bar{\rho}|_{\mathscr{G}_{K(\zeta_3)}}$. This is because we have $K(\zeta_3) = K_{\det(\bar{\rho})}$. Hence, the image of $\bar{\rho}|_{\mathscr{G}_{K(\zeta_3)}}$ is given by $\bar{\rho}(\mathscr{G}_K) \cap \mathrm{SL}_2(\mathbb{F}_3)$ (see Proposition 3.2.4 and Theorem 3.5.2). By Proposition 3.1.4, having $\bar{\rho}|_{\mathscr{G}_{K(\zeta_3)}}$ absolutely irreducible is equivalent to $\tilde{\rho}|_{\mathscr{G}_{K(\zeta_3)}}(\mathscr{G}_K) = \tilde{\rho}(\mathscr{G}_K) \cap A_4 \in \left\{A_4, V_4^+\right\}$. Note that when $\bar{\rho}(\mathscr{G}_K) = D_4$ then we can not apply the modularity lifting since $\tilde{\rho}(\mathscr{G}_K) \cap A_4 = C_2^+$. On the other hand, when this condition is satisfied then automatically we can apply Theorem 3.7.1 to a given a set of candidates π in order to prove the residual isomorphism. Obviously, the crucial part is to have a method to compute the traces of $\overline{\rho_{\iota,\pi}}$.

In the specific case in which K is an imaginary quadratic field then $\overline{\rho_{\iota,\pi}}$ is the Galois representation attached to a Bianchi modular form defined over K. In this case by [15], [48], [9], [30], [3] it would be possible to compute the traces of $\overline{\rho_{\iota,\pi}}$ at the primes of Σ_0 and prove whether the residual isomorphism holds. If the answer is positive, and E satisfies the reduction condition, then we can conclude that E is modular. Now, Let $\mathcal{N} \subset \mathcal{O}_K$ be the conductor of E; then the candidates are the finite set of Bianchi newforms at level $\mathcal{N}$ with trivial character and integer Hecke eigenvalues $a_{\mathfrak{p}}$. Thus, if among the candidate Bianchi modular forms only one is proved to be residual isomorphic to $\rho_{E,3}$ then we will have also proved which is the modular object related to E.

With the modularity lifting theorem, we can determine modularity more efficiently when applicable. In particular, we have used the sextic field method together with the modularity lifting theorem to prove modularity for isogeny classes contained in the LMFDB database of non-CM elliptic curves with absolutely irreducible image defined over $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-11})$, that are also non $\mathbb{Q}$-curves and not base change. We do not include all the tables here because of their length. For $K = \mathbb{Q}(\sqrt{-1})$ we have analysed all the 38828 classes of which 34314 have projective image isomorphic to S_4, 44 have image D_4, 114 are C_4, and 4 are V_4^-. For the S_4, D_4, V_4^- cases we computed the associated Bianchi modular forms, while for the C_4 cases the isomorphism holds only mod 3.
For $K = \mathbb{Q}(\sqrt{-11})$ we have analysed 25731 classes out of the 29287 in the database, and we had 22210 classes with surjective residual mod 3 representation and we computed the associated Bianchi modular forms; 88 had residual image isomorphic to SD_{16} hence absolutely irreducible and therefore proved to be modular. Finally, only 6 of them had mod 3 image isomorphic to D_4 and we proved these to be modular with the sextic field method applied in the last step. The remaining 3427 are reducible, but it is possible to prove whether they are modular by applying the 2-adic version of the Faltings-Serre-Livné method to the 2-adic Galois representation. Unfortunately, we did not do this last computation. However, we plan to apply the modularity lifting and the sextic fields method to all the non-CM isogeny classes of elliptic curves defined over an imaginary quadratic field with class number 1 for all 5 of them.

Finally, we present an example to show how our method links to the modularity lifting theorem.

Example. Let E be the elliptic curve defined over $\mathbb{Q}(\sqrt{-11})$ with Weierstrass equation

$$y^2 + (a+1)\,xy + (a+1)\,y = x^3 + x^2 + (-65a + 789)\,x + 464a - 897$$

and LMFDB label 2.0.11.1-9900.5-c2. The LMFDB page of E provides all the data we need: E has conductor

$$\mathfrak{N} = (30 - 60a) = (2)(-a)(a-1)(-a-1)(a-2)(-2a+1) = \mathfrak{p}_2\mathfrak{p}_3\bar{\mathfrak{p}}_3\mathfrak{p}_5\bar{\mathfrak{p}}_5\mathfrak{p}_{11},$$

norm $N(\mathfrak{N}) = 9900$ and nonsplit multiplicative reduction at all primes above 3. The ramification set $S = \{\mathfrak{p}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3, \mathfrak{p}_5, \bar{\mathfrak{p}}_5, \mathfrak{p}_{11}\}$ consists of 6 primes, hence we expect a rather large set of possible extensions. Indeed, we have a total of 5563 candidate

quartics. With the method developed in Chapter 3, we find that the set of primes Σ_0 to determine the mod 3 representation and possible mod 3 isomorphism, consists of 43 primes with norm ≤ 2137. The running time of our implementation was roughly 1 hour (3998.17 s). The computation returns that $\bar{\rho}_{E,3}(\mathscr{G}_K)$ is surjective (obviously determining the image could also be done easily looking at the 3-torsion polynomial). Thus $\bar{\rho}_{E,3}|_{\zeta_3}(\mathscr{G}_K) = \mathrm{GL}_2(\mathbb{F}_3) \cap \mathrm{SL}_2(\mathbb{F}_3) = \mathrm{SL}_2(\mathbb{F}_3)$. By Proposition 3.1.4 we deduce that $\bar{\rho}_{E,3}|_{\zeta_3}$ is absolutely irreducible, and by Proposition 6.2.1 we have that $\bar{\rho}_{E,3}$ is decomposed generic.

Next we start looking at the possible "modular" candidates among the one dimensional weight 2 Bianchi newform F of level $\mathfrak{N}$ and trivial character defined over $\mathbb{Q}(\sqrt{11})$. The work of Cremona [15] completely classifies them and they are reported in the LMFDB page of Bianchi modular forms of level $(30-60a)$ over $\mathbb{Q}(\sqrt{-11})$. By Theorem 3.7.1, to prove $\bar{\rho}_{E,3} \simeq \bar{\rho}_{F,3}$ we need to check that $a_{\mathfrak{p}}(E) \equiv a_{\mathfrak{p}}(F) \bmod 3$ for all $\mathfrak{p} \in \Sigma_0$. To compute the left hand side we use the Sage library for elliptic curves over finite fields [45], which uses the Pari library [44] for point-counting. For each candidate F we computed the right hand side via [17]. It turns out there is only one candidate F that satisfies this condition, and it is the Bianchi form with LMFDB label 2.0.11.1-9900.5-c. Therefore all the conditions of Theorem 6.2 are satisfied. Hence we can conclude that E is modular. Moreover, we have only one candidate that satisfies the residual isomorphism, so we actually have that $\rho_{E,3} \simeq \rho_{F,3}$ (and hence $\rho_{E,\ell} \simeq \rho_{F,\ell}$ for all primes ℓ since they form a compatible system).

Remark 6.2.2. Now, Σ_0 depends only on S (see Chapter 3). Thus, we can use it to check whether any E defined over $\mathbb{Q}(\sqrt{-11})$ with conductor $(-60a+30)$ satisfies the conditions of Theorem 6.2. We have 13 isogeny classes, and proceeding exactly as in the example we have that each curve E has surjective mod 3 representation, is ordinary, and has residual representation isomorphic to exactly one Bianchi form of the same level. Therefore, they are all modular. However, we can go further. Since we are in a Galois extension, then we can conjugate Σ_0 by the non trivial element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-11})/\mathbb{Q})$. Then, the resulting set Σ_0' can be used for the isogeny classes of conductor $\sigma(\mathfrak{N})$ without any additional computation. This is handful when our implementation is used to analyse representations coming from large databases.

Conclusion

By the results proved in this thesis we have been able to develop and to implement an effective 3-adic Faltings-Serre method for Galois representations $\rho : \mathscr{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_3)$ unramified outside a finite set S of primes of a generic number field K. To apply the method, we place two conditions. The first one is to know the finite set of ramified primes S. The second one is to effectively compute the characteristic polynomials of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ for a suitable finite set of $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O}_K) \setminus S$. We can, for example, apply the method on a number field K with mixed signature with the possibility of providing examples of a modular elliptic curve defined over K. However, at the moment it has not yet been proved that the candidate automorphic forms on such fields have an attached Galois representation. Thus, we can only prove a *conditional* modularity. That is, if such automorphic form f admits a Galois representation ρ_f such that

- it has cyclotomic determinant,
- it is unramified outside the level of f,
- it takes values in $\mathrm{GL}_2(\mathbb{Q}_3)$,
- the characteristic polynomial at $\mathrm{Frob}_{\mathfrak{p}}$ for $\mathfrak{p} \notin S$ is given by the Hecke polynomial of f at $\mathfrak{p}$,
- the Hecke polynomial of f at any given $\mathfrak{p} \notin S$ is computable.

Then we can determine whether $\rho_F \simeq \rho_E$.

The most important feature of the output of the algorithm, namely the test set T of primes of K where two absolutely irreducible representations must agree in order to be isomorphic (up to semisimplification), depends only on K and S. Therefore, the method is most efficient when applied to elliptic curves in an extensive database, since we can use the same test set T for any pair of Galois representations unramified outside the same S. Furthermore, due to the relation with the most recent developments in modularity lifting, we can prove modularity for non-CM

elliptic curves over CM fields even more efficiently and also open up the possibility of proving modularity for more general algebraic varieties whose attached residual representation takes values in $\mathrm{GL}_2(\mathbb{F}_3)$ or can be split into blocks of this form.

Finally, even though we can not apply the sextic field method to all the possible irreducible mod 3 images, we hope to be able to extend our method to cover the remaining cases.

Bibliography

[1] Patrick B. Allen, Frank Calegari, Ana Caraiani, Toby Gee, David Helm, Bao V. Le Hung, James Newton, Peter Scholze, Richard Taylor, and Jack A. Thorne. Potential automorphy over CM fields. (2018). https://arxiv.org/abs/1812.09999, Preprint.

[2] Patrick B. Allen, Chandrashekhar Khare, and Jack A. Thorne. Modularity of $\mathrm{GL}_2(\mathbb{F}_p)$-representations over CM fields. (2019). https://arxiv.org/abs/1910.12986,Preprint.

[3] Maria Teresa Aranés. *Modular symbols over number fields.* PhD thesis, University of Warwick, (2010). http://wrap.warwick.ac.uk/35128/.

[4] Alejandro Argaez-Garcia. *Computational aspects of Galois representations.* PhD thesis, University of Warwick, (2016). http://wrap.warwick.ac.uk/80937/.

[5] Alejandro Argaez-Garcia and John Cremona. Black box Galois representations. *Journal of Algebra*, **512**:526–565, (2018).

[6] Joël Bellaïche. Ribet's lemma,generalizations, and pseudocharacters, (2009). Two lectures at the Clay Mathematical Institute Summer School, Honolulu, Hawaii. Available at http://people.brandeis.edu/~jbellaic/RibetHawaii3.pdf.

[7] Tobias Berger and Gergely Harcos. ℓ-adic representations associated to modular forms over imaginary quadratic fields. *International Mathematics Research Notices*, 01 (2007).

[8] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen. On the paramodularity of typical abelian surfaces. *Algebra and Number Theory*, **13**(5):1145–1195, (2019).

[9] Jeremy S. Bygott. *Modular forms and modular symbols over imaginary quadratic fields*. PhD thesis, University of Exeter, (1998). https://ore.exeter.ac.uk/repository/handle/10871/8322.

[10] Henri Carayol. Formes modulaires et représentations Galoisiennes à valeurs dans un anneau local complet. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume **165** of *Contemp. Math.*, pages 213–237. Amer. Math. Soc., Providence, RI, (1994).

[11] J. W. S. Cassels and A. Fröhlich. *Algebraic Number Theory*. London Mathematical Society, 2nd ed. edition, (2010). Proceedings of an Instructional Conference Organized by the London Mathematical Society (a Nato Advanced Study Institute) With the Support of the International Mathematical Union.

[12] Gabriel Chenevêrt. *Exponential sums, hypersurfaces with many symmetries and Galois representations*. PhD thesis, Mc Gill University, (2008).

[13] Henri Cohen. *Advanced topics in computational number theory*, volume **193** of *Graduate Texts in Mathematics*. Springer-Verlag, New York, (2000).

[14] Henri Cohen, Francisco Diaz, and Michel Olivier. Constructing complete tables of quartic fields using kummer theory. *Math. Comput.*, 72:941–951, 04 (2003).

[15] John Cremona. *Modular Symbols*. PhD thesis, University of Oxford, (1981). http://homepages.warwick.ac.uk/staff/J.E.Cremona/theses/JCthesis-scan.pdf.

[16] John Cremona. Classical invariants and 2-descent on elliptic curves. *Journal of Symbolic Computation*, 31(1):71 – 87, (2001).

[17] John Cremona. Bianchi-progs. https://github.com/JohnCremona/bianchi-progs, (2019).

[18] John Cremona. CremonaPacetti. https://github.com/JohnCremona/CremonaPacetti, (2019).

[19] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, (1981). With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[20] Richard M. Foote David S. Dummit. *Abstract algebra*. Wiley, 3rd ed edition, (2004).

[21] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Mathematics of Computation*, **79**, (2008).

[22] Tim Dokchitser. *GroupNames-small finite groups, their names, properties and character tables.* https://people.maths.bris.ac.uk/~matyd/GroupNames/index.html.

[23] W. Fulton and J. Harris. *Representation Theory: A First Course*. Graduate Texts in Mathematics. Springer New York, (1991).

[24] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.1*, (2019).

[25] Fernando Q. Gouvêa. Deformations of Galois representations. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 233–406. Amer. Math. Soc., Providence, RI, (2001). Appendix 1 by Mark Dickinson, Appendix 2 by Tom Weston and Appendix 3 by Matthew Emerton.

[26] Haruzo Hida. *Modular Forms and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, (2000).

[27] Andrew Jones. Modular elliptic curves over the field of twelfth roots of unity. *LMS Journal of Computation and Mathematics*, **19**(1):155–174, (2016).

[28] Angelos Koutsianas. *Application of the S-unit Equations to the Arithmetic of Elliptic Curves.* PhD thesis, University of Warwick, (2016). http://wrap.warwick.ac.uk/86760/.

[29] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1st ed. edition, (1986). Softcover reprint ofthe hardcover 1st edition.

[30] Mark Peter Lingham. *Modular forms and elliptic curves over imaginary quadratic fields*. PhD thesis, University of Nottingham, (2005). http://eprints.nottingham.ac.uk/10138/.

[31] Ron Livné. Cubic exponential sums and Galois representations. *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume **67** of Contemp. Math.:247–261, (1987).

[32] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, (2013). [Online; accessed 16 September 2013].

[33] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, (1977). Universitext.

[34] Toshitsune Miyake. On automorphic forms on GL_2 and Hecke operators. *Annals of Mathematics*, **94**(1):174–189, (1971).

[35] Chung Pang Mok. Galois representations attached to automorphic forms on GL_2 over CM fields. *Compositio Mathematica*, **150**(4):523–567, Mar (2014).

[36] Jürgen Neukirch. *Algebraic number theory*, volume **322** of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, (1999). Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[37] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume **323** of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2nd ed. edition, (2008).

[38] Ciaran Schembri. Examples of genuine QM abelian surfaces which are modular. *Research in Number Theory*, **5**(1):11, Jan (2019).

[39] Mehmet Haluk Şengün. Arithmetic aspects of bianchi groups. In *Computations with Modular Forms*, pages 279–315. Springer International Publishing, (2014).

[40] Jean-Pierre Serre. *Linear representations of finite groups*, volume **42** of *Graduate text in Mathematics*. Springer-Verlag, New York, (1977). Translated from the second French edition by Leonard L. Scott.

[41] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 2nd ed. edition, (1989). With the collaboration of Willem Kuyk and John Labute.

[42] Jean-Pierre Serre. Resumé des cours au Collège de France 1984-1985. *Oeuvres - Collected Papers*, volume **IV**, (2000).

[43] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, **4**:4, 79, (2016).

[44] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.11.2`, 2019. available from http://pari.math.u-bordeaux.fr/.

[45] The Sage Developers. Sagemath 9.1 Reference Manual: Elliptic curves over finite fields). https://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/ell_finite_field.html.

[46] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.9)*, (2019). `https://www.sagemath.org`.

[47] André Weil. *Dirichlet Series and Automorphic Forms*, volume **189** of *Lecture Note in Mathematics*. Springer Berlin Heidelberg, (1971).

[48] Elise Whitley. *Modular Forms and Elliptic Curves over Imaginary Quadratic Fields*. PhD thesis, University of Exeter, (1990). https://ore.exeter.ac.uk/repository/handle/10871/8427.