Computational aspects of Galois representations

by

Alejandro Argáez García

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Warwick Mathematical Institute

June 2016

Contents

Acknowledgements. **iii**

Abstract. **iv**

Declaration. **v**

Notation. **vi**

1 Introduction. **1**

2 Background. **3**

2.1 Galois and Number theory. 3

2.2 Lattices in $\mathbb{Q}_\ell^2$ and the Bruhat-Tits Tree. 6

2.2.1 Bruhat-Tits Tree. 8

2.3 Representation theory. 9

2.3.1 Galois representations. 10

2.3.2 Integral Galois representations. 12

2.4 Livné 16

3 Preliminaries. **18**

3.1 Obtaining information from a 2-adic Galois representation. 18

3.2 Classification of Galois extensions L/K with group C_1, C_2, C_3 or S_3. 19

3.2.1 Distinguishing the irreducible cases from the reducible cases. 20

3.2.2 Linearly independent sets of primes 23

3.3 1-dimensional Galois representations. 24

4 Black Box Galois representations. **26**

4.1 Determining the residual image. 27

4.2 Reducible Residual Representation. 29

4.2.1 Small Isogeny Class. 30

4.2.2 Determining the Small Isogeny Class. 32

4.3 Large Isogeny Class of width at least 2. 41

4.3.1 Bruhat-Tits tree of width at least 2: Large Isogeny class. 43

4.3.2 The test. . . . 46
4.3.3 Δ_{det} trivial. . . . 47
4.3.4 Δ_{det} non-trivial. . . . 54
4.4 Isogenous Galois representations modulo 2^{k+1}. . . . 59

5 Comparing two Black Box Galois representations. 63
5.1 Proving congruence modulo 2^{k+1}. . . . 64
5.1.1 The four possible images. . . . 66
5.2 The cohomology class $[\mu]$ in $\tilde{H}_1(G_K, V_0)$. . . . 68
5.3 Proving $[\mu] = 0$. . . . 70
5.4 Case S_3: proving $[\mu] = 0$. . . . 70
5.4.1 $[\mu_1] = 0$. . . . 71
5.4.2 $[\mu_2] = 0$. . . . 73
5.5 Case C_3: proving $[\mu] = 0$. . . . 79
5.6 Cases C_2 and C_1: proving $[\mu] = 0$. . . . 81

Bibliography 82

Acknowledgements.

I would like to thank my supervisor Professor John Edward Cremona for his help, support, advice, friendship and guidance throughout my Ph.D. years and the years before. Also, I am thankful to the University of Warwick and the Warwick Mathematical Institute for sponsoring my the three years of the Ph.D., via the "Vice chancellor international scholarship", without this funding I would have never been able to realize my dream of studying a Ph.D.

Also, I would like to thank my examiners Professor Samir Siksek and Dr. Christian Wuthrich for their corrections, comments and expertise.

Many thanks to the Number Theory group and the administrative team at the Warwick Mathematical Institute and particularly to Carole Fisher.

I would like to add a special thanks to Professor Kirti Joshi and Professor Javier Diaz-Vargas for their help and friendship during my Undergrad's and Master's studies.

A big thanks to my friends, my current and former postgraduate colleagues, and my brothers and sisters in arms: Florian, Aggelos, Vandita, Samuele, Stephanos, Italo, Rosemberg, Alejandra, Rodolfo, Felipe, Buli, Beto, Javier, Edwin, Jaime, Clark, Marin, Giannis and more for all their support and friendship over the years.

Finally I would like to thank my family for everything. My parents Carlos Argaez Carillo and Nelly Garcia Diaz, thank you for encouraging me to always pursue my dreams, for all your advices and specially for being with me in the darkest times of my life. To my sisters and brother; Nelly, Josefina and Carlos for all their advice and continuing support. And at last but not at least, to my nephews and niece; Ernesto, Carlos y Josefina, I promise you that I will be always there for you.

Abstract.

This thesis contains a series of studies about 2-adic integral Galois representations unramified outside a finite set of primes. There are two main focuses of research: the study of 2-adic integral Galois representations and the study on how to compare two 2-adic integral Galois representations.

Firstly, when studying a representation, we develop methods to determine whether the residual image is reducible or irreducible: in the irreducible case the residual image is completely determined. On the other hand, when the residual image is reducible we are able to make a choice of a stable lattice to completely determine the residual image. Lastly, from the choice of lattice, we are able to extend our methods to determine whether the representation is trivial modulo 2^{k+1} assuming that is trivial modulo 2^k.

Secondly, when comparing two 2-adic integral Galois representations, we are able to determine whether the representations are isogenous that is, after conjugation if necessary, their residual representations are the same. In some cases, this process follows the approach given in [11] by Ron Livné.

Finally, the idea behind these studies was the notion of what we call a “Black Box representation”, i.e., a system that will provide the characteristic polynomial of the representation for any prime not in the set of primes.

Declaration.

All the work presented in this thesis is the result of three and a half years of joint work with my supervisor Professor John Edward Cremona. Several results were proven by him(which are clearly referenced), Section is 4.2 is based on unpublished notes by him and the original ideas were also introduced by him. Also the motivation of Chapter 5 was given by the article [8].

Except as noted above, I declare that, to my best of knowledge, the material contained in this thesis is original and my own work except where otherwise indicated, cited or commonly known.

The material in this thesis is submitted to the University of Warwick for the degree of Doctor of Philosophy, and has not been submitted to any other university or for any other degree.

Notation

- K is a number field.
- L is a finite extension of K.
- S is a finite set of primes of K including the primes above 2.
- $G_K = \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group.
- $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is an ℓ-adic continuous Galois representation unramified outside S.
- $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is a mod-ℓ Galois representation unramified outside S.

Chapter 1

Introduction.

In Number theory, one of the most relevant topics is *Galois representations*; in particular Galois representations attached to elliptic curves and modular forms. These representations are a lively subject of research and have been widely studied by famous mathematicians like Jean-Pierre Serre, Gerd Faltings, Barry Mazur, John Tate and others. In fact, the famous proof of *Fermat's last theorem* given by Andrew Wiles involves Galois representations attached to modular forms and semistable elliptic curves over $\mathbb{Q}$. This capability of attaching representations to different mathematical objects gives rise to two of the most sought objectives in Number theory; the first one is to be able to extract all major information of an object by its attached representation, and the second one is to determine whether two, a priori different, objects are the "same" by proving that their respective attached representations are the same.

Roughly speaking, for given number field K, a *Galois representation unramified outside a set of primes S* is a continuous homomorphism from the absolute Galois group of K to the general linear group of a vector space V over a field F, satisfying that ρ factors though $\mathrm{Gal}(K_S/K)$ where K_S is the maximal extension of K unramified outside S. Depending on what F is, we can divide the Galois representations in three types, for ℓ prime we say ρ is

1. an *Artin Galois representation* if $F = \mathbb{C}$,
2. an *ℓ-adic Galois representation* if $F = \mathbb{Q}_\ell$,
3. a *mod-ℓ Galois representation* if $F = \mathbb{F}_\ell$.

Moreover we say that ρ is an *ℓ-adic integral Galois representation unramified outside S* when, by finding a suitable Galois stable lattice in $\mathbb{Q}_\ell^n$, we obtain a $\mathbb{Z}_\ell$-basis for V and so an integral matrix representation $\rho\colon G_K \to \mathrm{GL}_n(\mathbb{Z}_\ell)$. Once a suitable lattice has been found, we can then obtain the *residual representation* $\overline{\rho}\colon G_K \to \mathrm{GL}_n(\mathbb{F}_\ell)$. From now on, we will work with representations with $\ell = n = 2$.

We introduce the notion of a "Black Box representation" related to ρ, which is a system that provides the (quadratic) characteristic polynomial of the representation for any prime $\mathfrak{p}$ in K not in S, and we compute a *quadratically independent set of primes T_2 with respect to S.*

Now consider a representation ρ for which we would like to obtain as much information as possible. To do so, we start by computing a quadratically independent set of primes T_2, a set of monic cubic polynomials defining all possible S_3 and C_3 extensions of K unramified outside S, and the "Black Box representation". Then with only these we are able to determine whether the image of $\overline{\rho}$ is irreducible(image S_3 or C_3) or reducible(image C_2 or C_1). When the image is irreducible, its splitting field is that of a single monic cubic polynomial and by calculating its discriminant we can distinguish between the S_3 and the C_3 cases. When the image is reducible, we develop methods, based on determining the width of the *stable Bruhat-Tits tree* related to ρ, to determine if there is a choice of lattice to distinguish between the C_2 and the C_1 cases. Moreover, by improving these methods we are able to determine whether ρ is trivial modulo 2^{k+1} assuming that it is trivial modulo 2^k.

On the other hand, when working with two, a priori, different representations ρ_1 and ρ_2 we would like to determine if these are the same. To do this, we start by checking that $\det(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \det(\rho_2(\mathrm{Frob}_\mathfrak{p})) \pmod 2$ for all $\mathfrak{p}$ in K. Then we compute a quadratically independent set of primes T_2 and prove that their residual images $\overline{\rho}_1$ and $\overline{\rho}_2$ are the same. This process then continues with an inductive argument, we assume that $\rho_1 = \rho_2 \pmod{2^k}$ and we want to prove that they are equal modulo 2^{k+1}. By doing this assumption an "obstruction" arises when lifting from 2^k to 2^{k+1}. We are able to eliminate this obstruction by obtaining a finite set of primes on K and checking, depending on the residual image, only the trace condition $\mathrm{tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_\mathfrak{p}))$ or the trace condition and the determinant condition $\det(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \det(\rho_2(\mathrm{Frob}_\mathfrak{p}))$. We found this set of primes combining developed theory in the thesis and the Faltings-Serre-Livné method given in [11].

Finally, a side product of the developed of methods and algorithms in this thesis are some computational programs, which are not included in here, written in Sage [7] which determine whether the residual image of ρ is irreducible or reducible. When the image is reducible the programs determine whether there is a choice lattice for ρ such that the residual image is C_1 or C_2. Furthermore, when the residual image is S_3 the programs are able to determine a set of primes to determine the trace condition for two different Galois representations.

Chapter 2

Background.

This chapter encapsulates the basic, and not so basic, mathematical theory needed to understand the contents of this thesis.

1. Section 2.1. In this section we summarize well-known facts about Number theory and Galois theory.

2. Section 2.2. In this section we introduce the definition of a lattice and some of its important properties. Then we continue with the definition of the *Bruhat-Tits tree*; we will see that the usage of lattices will help us to define integral representations in Section 2.3. From these constructions, in Chapter 4, we will be able to use these trees to classify the representations they are attached to.

3. Section 2.3. In this section we give the definition of, what is going to be for us, a Galois representation. We will also explore how to construct an *integral Galois representation* using what was seen in Section 2.2.

4. Section 2.4. Lastly we present results that are stated and proven the article [11] by Ron Livné; instead of just referring to the article, we present without proofs, the results needed in chapters 4 and 5.

2.1 Galois and Number theory.

This section is based on [2].

Let K be a number field. Let L/K be a finite extension and consider the ideal $\mathfrak{p}\mathcal{O}_L$ where $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$. Then we have that

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

where $\mathfrak{P}_j$ are distinct prime ideals of $\mathcal{O}_L$, $g = g(\mathfrak{p})$ is a positive integer and e_j are positive integers. We call e_j the *ramification index* for $\mathfrak{P}_j/\mathfrak{p}$, denoted $e_j = e(\mathfrak{P}_j/\mathfrak{p})$.

If L/K is a Galois extension, then the Galois group permutes the $\mathfrak{P}_j$ transitively, so that $e_1 = \cdots = e_g = e$.

It is well-known that $\mathcal{O}_L$ is Dedekind domain, so every non-zero prime ideal is maximal. Thus the quotients $\mathcal{O}_L/\mathfrak{P}_j$ and $\mathcal{O}_K/\mathfrak{p}$ are fields, called *residue fields.* They are finite fields of characteristic p, with p a rational prime, where $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We may view $\mathcal{O}_K/\mathfrak{p}$ as a subfield of $\mathcal{O}_L/\mathfrak{P}_j$. The *residue field degree* is

$$f(\mathfrak{P}_j/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}_j : \mathcal{O}_K/\mathfrak{p}] \,.$$

If L/K is Galois then $f(\mathfrak{P}_1/\mathfrak{p}) = \cdots = f(\mathfrak{P}_g/\mathfrak{p}) = f$. In general we have that

$$\sum_{j=1}^{g} e(\mathfrak{P}_j/\mathfrak{p}) f(\mathfrak{P}_j/\mathfrak{p}) = [L : K]. \tag{2.1}$$

When L/K is a Galois extension, then (2.1) becomes $efg = [L : K]$. Moreover, when L/K is an extension of number fields, we say that the prime $\mathfrak{p}$ is

1. *unramified* in L/K if $e(\mathfrak{P}_j/\mathfrak{p}) = 1$ for all j,
2. *remains inert* in L/K if $\mathfrak{p}\mathcal{O}_L$ is a prime in $\mathcal{O}_L$, and
3. *splits completely* in L/K if $g = [L : K]$.

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ and let $\mathfrak{P}$ be a prime in $\mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$. Define the *(relative) norm* of $\mathfrak{P}$ as

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}.$$

Furthermore, we can extend the notion of $N_{L/K}$ to any fractional ideals of K by multiplicativity, i.e.,

$$N_{L/K}(\mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_t^{a_t}) = N_{L/K}(\mathfrak{P}_1)^{a_1} \cdots N_{L/K}(\mathfrak{P}_t)^{a_t}.$$

Thus the norm of a fractional ideal in L is a fractional ideal in K. Note that if L/K is Galois, then for $\mathfrak{U}$ ideal we have that

$$N_{L/K}(\mathfrak{U})\mathcal{O}_L = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{U}).$$

If $\alpha \in K$ then $N_{L/K}(\alpha\mathcal{O}_L) = N_{L/K}(\alpha)\mathcal{O}_K$, where the norm on the right is the usual element norm. Also if $F \subseteq L \subseteq K$ then $N_{K/F} = N_{L/F} \circ N_{K/L}$.

Given a Galois extension of number fields L/K with Galois group G, a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, we define the *decomposition group* of $\mathfrak{P}$ as

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

Observe that $Z(\mathfrak{P}/\mathfrak{p})$ acts on the finite field $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ fixing the subfield $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, so there is a natural homomorphism of groups

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}). \tag{2.2}$$

From Algebraic Number theory we have the following theorem.

Theorem 2.1.1 (Theorem 1.2,[2])**.** *Let L/K be a Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_K$.*

(*a*) *G acts transitively on the set of primes ideals $\mathfrak{P}$ of $\mathcal{O}_L$ that divide $\mathfrak{p}\mathcal{O}_K$, hence*

$$[G : Z(\mathfrak{P}/\mathfrak{p})] = \#\{\textit{primes } \mathfrak{P} \textit{ of } \mathcal{O}_L : \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L\}.$$

Also, if $\mathfrak{P}$ and $\mathfrak{P}'$ are prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}\mathcal{O}_L$ then, $Z(\mathfrak{P}/\mathfrak{p})$ and $Z(\mathfrak{P}'/\mathfrak{p})$ are G-conjugate.

(*b*) *$N(\mathfrak{p}) = \#\mathbb{F}_{\mathfrak{p}}$, $N(\mathfrak{P}) = \#\mathbb{F}_{\mathfrak{P}}$ and $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic, generated by the Frobenius automorphism $\varphi_{\mathfrak{p}} \colon x \mapsto x^{N(\mathfrak{p})}$.*

(*c*) *The homomorphism (2.2) is surjective. Its kernel is called the* inertia group, *denoted $I(\mathfrak{P}/\mathfrak{p})$. Note that $[Z(\mathfrak{P}/\mathfrak{p}) : I(\mathfrak{P}/\mathfrak{p})] = f$ and $I(\mathfrak{P}/\mathfrak{p})$ has order e.*

We can observe that when an unramified prime $\mathfrak{p}$ is chosen, we obtain that its inertia group is trivial. Thus we see that the homomorphism (2.2) becomes an isomorphism and we get

$$Z(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}). \tag{2.3}$$

The Galois group for the residue fields is generated by the Frobenius automorphism $\varphi_{\mathfrak{p}}$, hence there is a unique element $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$ that corresponds to $\varphi_{\mathfrak{p}}$ under the natural isomorphism (2.3). We have that $Z(\mathfrak{P}/\mathfrak{p}) = \langle\sigma\rangle$. This element is called *Frobenius element* at $\mathfrak{P}/\mathfrak{p}$ and is denoted by $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$. Moreover we have that for any $\sigma \in G_K$

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

so the Frobenius elements of the primes lying above $\mathfrak{p}$ form a conjugacy class in $\mathrm{Gal}(L/K)$. We will abuse notation and write $\mathrm{Frob}_{\mathfrak{p}}$ instead of $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$.

Proposition 2.1.2 (Proposition 1.4,[2])**.** *Let L/K be a Galois extension of number fields, $\mathfrak{p}$ a non-zero prime of $\mathcal{O}_K$ that is unramified in L/K and $\mathfrak{P}$ a prime of $\mathcal{O}_L$*

with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Then the Frobenius at $\mathfrak{P}/\mathfrak{p}$ is the unique element $\sigma \in \mathrm{Gal}(L/K)$ that satisfies $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ for every $\alpha \in \mathcal{O}_L$.

Moreover, by Čebotarev's density theorem we have the following.

Lemma 2.1.3 (Corollary 2, page I-8, [14])**.** *Let L/K be a Galois extension which is unramified outside a finite set of primes S. Then the Frobenius elements of the unramified primes are dense in $\mathrm{Gal}(L/K)$.*

Consider the absolute Galois group of K. In Section 2.3, when we define what a Galois representation unramified outside S is, we will see that the image of this representation is given by a Galois extension L/K with $\mathrm{Gal}(L/K) < G_K$. Thus any $\mathrm{Frob}_\mathfrak{p}$ taken from G_K will be lying in $\mathrm{Gal}(L/K)$. In this way, by Lemma 2.1.3, each $\sigma \in \mathrm{Gal}(L/K)$ has the form $\sigma = \mathrm{Frob}_\mathfrak{p}$ for (infinitely many) primes $\mathfrak{p}$ of K unramified in L/K.

Lastly, let K be a number field and let S be a set of primes containing the primes above 2 of K. We define the group $K(S, 2)$, which is a subgroup of $K^*/(K^*)^2$, as

$$K(S,2) := \{a \in K^*/(K^*)^2 : \mathrm{ord}_\mathfrak{p}(a) \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \in K \text{ with } \mathfrak{p} \notin S\}. \tag{2.4}$$

This group is finite. Moreover, there is a finite number of extensions $K(\sqrt{a})/K$ given by $a \in K(S, 2)$ which are unramified outside S (see pages 213-214 in [17]).

Remark 2.1.4. *Observe that after this section we will say that a prime is 'in K', but it will be understood that the prime is a prime ideal of $\mathcal{O}_K$.*

2.2 Lattices in $\mathbb{Q}_\ell^2$ and the Bruhat-Tits Tree.

This section is based on the notes [1].

The theory of lattices and trees is vast, rich and they are defined in general over d-dimensional vector spaces. We start this section with the general definition of lattice and at some point we are going to focus explicitly in the 2-dimensional vector space $\mathbb{Q}_\ell^2$ over $\mathbb{Q}_\ell$.

Let A be a discrete valuation domain and K its field of fractions. Also, let V be a vector space over K of dimension d. Since $A \subset K$, V has a structure of A-module.

Proposition 2.2.1. *Let Λ be an A-submodule of V. The following statements are equivalent:*

(*a*) *Λ is a finite A-module and $K\Lambda = V$.*

(*b*) *Λ is a finite A-module. The natural map*

$$\begin{aligned} \Lambda \otimes_A K &\to V \\ v \otimes x &\mapsto xv \end{aligned} \tag{2.5}$$

is an isomorphism.

(*c*) *Λ is a free A-module of rank d.*

Any Λ satisfying Proposition 2.2.1 it is called a *lattice* of V.

Lemma 2.2.2. *Let Λ be a lattice. If $\Lambda' \subset \Lambda$ and Λ'' is a A-module such that $\Lambda' \subset \Lambda'' \subset \Lambda$ then Λ'' is also a lattice. If Λ and Λ' are lattices then $\Lambda + \Lambda'$ is a lattice. More generally, if $\{\Lambda_i\}$ is a non-empty family of sublattices of a lattice Λ then $\sum_i \Lambda_i$ is a lattice.*

Definition 2.2.3. *Two lattices Λ and Λ' are* homothetic *if there exists $\lambda \in K^*$ such that $\Lambda = \lambda\Lambda'$.*

From now on, let $K = \mathbb{Q}_\ell$, $A = \mathbb{Z}_\ell$ and $V = \mathbb{Q}_\ell^2$ as a $\mathbb{Z}_\ell$-modulo. Then we re-define Λ in V as follows.

Definition 2.2.4. *A subset $\Lambda \subseteq \mathbb{Q}_\ell^2$ is a* lattice *if there exist two independent vectors $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Q}_\ell^2$ such that*

$$\Lambda = \mathbb{Z}_\ell \,\mathbf{v}_1 + \mathbb{Z}_\ell \,\mathbf{v}_2 = \{x \,\mathbf{v}_1 + y \,\mathbf{v}_2 \,| x, y \in \mathbb{Z}_\ell\}.$$

Some well-known examples of lattices in $\mathbb{Q}_\ell^2$ are

$$\Lambda_0 = \mathbb{Z}_\ell(1,0) + \mathbb{Z}_\ell(0,1) = \mathbb{Z}_\ell^2$$

and

$$\Lambda_{a,b} = \mathbb{Z}_\ell(\ell^a, 0) + \mathbb{Z}_\ell(0, \ell^b) \qquad \text{with } a, b \in \mathbb{Z}.$$

Let's fix a lattice $\Lambda = \mathbb{Z}_\ell \,\mathbf{v}_1 + \mathbb{Z}_\ell \,\mathbf{v}_2$. We would like to characterize all the lattices Λ' such that $\ell\Lambda \subseteq \Lambda' \subseteq \Lambda$. To do this define

$$\begin{aligned} \phi\colon \Lambda &\to \mathbb{F}_\ell^2 \\ x \,\mathbf{v}_1 + y \,\mathbf{v}_2 &\mapsto (\overline{x}, \overline{y}), \end{aligned}$$

where $\overline{x} \equiv x \pmod{\ell}$ is the reduction map $\mathbb{Z}_\ell \to \mathbb{F}_\ell \cong \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell \cong \mathbb{Z}/\ell\mathbb{Z}$. We can see that $\ker(\phi) = \ell\Lambda$ and then we have $\Lambda/\ell\Lambda \cong \mathbb{F}_\ell^2$. Hence for any Λ' such that $\ell\Lambda \subseteq \Lambda' \subseteq \Lambda$, the quotient $\Lambda'/\ell\Lambda$ is a subspace of $\mathbb{F}_\ell^2$.

Observe that the quotient $\Lambda'/\ell\Lambda$ can be fully characterized. First we can see that its extreme cases are the following,

$$\Lambda'/\ell\Lambda = \begin{cases} 0 & \text{iff } \; \Lambda' = \ell\Lambda \\ \mathbb{F}_\ell^2 & \text{iff } \; \Lambda' = \Lambda. \end{cases}$$

The rest of the cases are when $\Lambda'/\ell\Lambda$ is isomorphic to a one dimensional subspace of $\mathbb{F}_\ell^2$.

Definition 2.2.5. *A sublattice Λ' of a lattice Λ is* cocyclic *if the quotient Λ/Λ' is cyclic.*

Lemma 2.2.6. *Let Λ be a lattice. Then there are exactly $\ell + 1$ sublattices of Λ such that $[\Lambda : \Lambda']$ is equal to ℓ.*

2.2.1 Bruhat-Tits Tree.

Let X be the set of lattices of $\mathbb{Q}_\ell^2$ up to homothethies. For a lattice Λ, we denote $[\Lambda] \in X$ as its *equivalence class* up to homotheties.

Definition 2.2.7. *Two points x and x' in X are* neighbours *if there are distinct lattices Λ, Λ' with $x = [\Lambda]$ and $x' = [\Lambda']$ such that $\ell\Lambda \subset \Lambda' \subset \Lambda$.*

There is a natural bijection between the set of neighbours in X and the set of proper non-trivial subspaces of $\Lambda/\ell\Lambda$.

Lemma 2.2.8. *Let $x = [\Lambda]$ be a point in X. There exists a natural bijection between the set of neighbours of x and the set of proper non-trivial $\mathbb{F}_\ell$-subspaces of the $\mathbb{F}_\ell$ vector space $\Lambda/\ell\Lambda$.*

This bijection is defined as follows: if x' is a neighbour of x then the lattice Λ' satisfying that $\ell\Lambda \subset \Lambda' \subset \Lambda$ is unique for Λ being fixed. Moreover, the relation "x and x' are neighbours" is symmetric. Thus the set with these notions of neighbourhood is an *undirected graph*, and all notions of graph theory apply [16].

Definition 2.2.9. *The* Bruhat-Tits tree *is the graph satisfying that*

(*a*) *its vertex set is X,*

(*b*) *there is an edge between two vertices x and x' of X if and only if x and x' are neighbours.*

By abuse of notation we will use X to denote this graph.

Proposition 2.2.10. *The graph X is simply connected, i.e., for any $x, x' \in X$ such that $x \neq x'$, there is exactly one path from x to x'.*

Definition 2.2.11. *A graph that is simply connected is called a* tree*.*

Observe that our graph X is simply connected which implies that is connected and thus is a tree [16]. Since we are working with 2-adic representations, the tree attached to the image of a representation is called the *Bruhat-Tits tree.*

A *path* from x to x' in X is a sequence $x = x_0, x_1, ..., x_n = x'$ of points in X such that for all $i = 0, .., n-1$, x_i is a neighbour of x_{i+1} and $x_i \neq x_j$ for all $0 \leq i \neq j \leq n$. The integer $n \geq 0$ is the *length* of the path, and the *distance*, denoted $d(x, x')$, between x and x' is the minimal length of a path from x to x' (if any).

If $d(x, x') = n$, then we can choose points $x = [\Lambda]$ and $x' = [\Lambda']$ such that $\ell^n \Lambda \subset \Lambda' \subset \Lambda$. Once Λ is fixed, Λ' is unique, and Λ/Λ' and $\Lambda/\ell^n\Lambda$ are isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$, i.e., both quotients are cyclic of order ℓ^n.

2.3 Representation theory.

This section is based on [15].

Let V be a vector space over the field K and let $\mathrm{GL}(V)$ be the group of automorphisms of V. An element a of $\mathrm{GL}(V)$ is, by definition, a linear mapping of V into V which has an inverse a^{-1} and is linear. When V has a finite basis $\{e_i\}_{i=1}^n$ of n elements, each linear map $a\colon V \to V$ is defined by a square matrix (a_{ij}) of order n. The coefficients $a_{ij} \in K$, they are obtained by expressing the images $a(e_j)$ in terms of the basis (e_i):

$$a(e_j) = \sum_i a_{ij} e_i.$$

Saying that a is an isomorphism is equivalent to say that the determinant of a, $\det(a) = \det(a_{ij})$, is not zero. The group $\mathrm{GL}(V)$ is thus identifiable with the group of *invertible square matrices of order n.*

Now, suppose that G is a finite group with identity element 1 and with composition $(s, t) \mapsto st$.

Definition 2.3.1. *A linear representation of G in V is a homomorphism ρ from the group G into the group* $\mathrm{GL}(V)$.

In other words, we associate to each element $s \in G$ an element $\rho(s)$ of $\mathrm{GL}(V)$ in such a way that we have the equality

$$\rho(st) = \rho(s) \cdot \rho(t) \qquad \text{for } s, t \in G.$$

Observe that the previous formula implies that:

$$\rho(1) = 1, \qquad \rho(s^{-1}) = \rho(s)^{-1}.$$

When ρ is given, we say that V is a *representation space* of G (or even simply, by abuse of language, a *representation* of G).

Moreover, suppose that V is n-dimensional: we say also that n is the degree of the representation under consideration. Let $\{e_i\}_{i=1}^n$ be a basis of V and let $\mathbf{R}_s$ be the matrix of $\rho(s)$ with respect to this basis. We have

$$\det(\mathbf{R}_s) \neq 0, \qquad \mathbf{R}_{st} = \mathbf{R}_s \cdot \mathbf{R}_t \quad \text{if } s, t \in G.$$

If we denote by $r_{ik}(s)$ the coefficients of the matrix $\mathbf{R}_s$, the second formula becomes

$$r_{ik}(st) = \sum_j r_{ij}(s) \cdot r_{jk}(t).$$

Conversely, given invertible matrices $\mathbf{R}_s = (r_{ij}(s))$ satisfying the previous identities, there is a corresponding linear representation ρ of G in V; this is what it means to give a representation "in matrix form".

Definition 2.3.2. *Let ρ_1 and ρ_2 be two representations of the same group G in vector spaces V_1 and V_2. These representations are said to be* similar *or* isomorphic *if there exists a linear isomorphism $\tau\colon V_1 \to V_2$ which "transforms" ρ_1 into ρ_2, that is, which satisfies the identity*

$$\tau \circ \rho_1(s) = \rho_2(s) \circ \tau, \qquad \textit{for all } s \in G.$$

When ρ_1 and ρ_2 are given in matrix form $\mathbf{R}_s$ and $\mathbf{R}'_s$ respectively, this means that there exists an invertible matrix $\mathbf{T}$ such that

$$\mathbf{T} \cdot \mathbf{R}_s = \mathbf{R}'_s \cdot \mathbf{T}, \qquad \text{for all } s \in G.$$

which is also written $\mathbf{R}'_s = \mathbf{T} \cdot \mathbf{R}_s \cdot \mathbf{T}^{-1}$. We can *identify* two such representations by having each $x \in V_1$ correspond to the element $\tau(x) \in V_2$. In particular, ρ_1 and ρ_2 have the same degree.

Definition 2.3.3. *Let $\rho\colon G \to \mathrm{GL}(V)$ be a linear representation and let W be a vector subspace of V. We say W is* stable *or* invariant *under the action of G when $x \in W$ implies $\rho(s)x \in W$ for all $s \in G$.*

2.3.1 Galois representations.

This section is based on [9].

We say a representation is a *Galois representation* when the group G is actually a Galois group. Let K be a number field, let L/K be a finite Galois extension and consider the following diagram.

$$\begin{tikzcd} \overline{K} \arrow[d, dash, "\mathrm{Gal}(\overline{K}/L)"] \\ L \arrow[d, dash, "\mathrm{Gal}(L/K)"] \\ K \arrow[uu, dash, bend left, "G_K"] \end{tikzcd}$$

Definition 2.3.4. *A continuous ℓ-adic Galois representation over K is a continuous homomorphism $\rho\colon G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$.*

This representation is sometimes referred as a *rational ℓ-adic representation.* Let ρ be an ℓ-adic representation and let L be the extension of K corresponding to $H = \ker(\rho)$, i.e., $\mathrm{Gal}(\overline{K}/L) = \ker(\rho)$. Then we have that

$$\rho(G_K) \cong \frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Gal}(\overline{K}/L)} \cong \mathrm{Gal}(L/K).$$

We can see in the following diagram that

$$\begin{tikzcd}
G_K \arrow[r, "\rho"] & \mathrm{GL}_2(\mathbb{Q}_\ell) \\
& \mathrm{Gal}(L/K) \arrow[ul, hook] \arrow[u]
\end{tikzcd}$$

In this way, as was mentioned at the end of Section 2.1, the image of ρ is given by a Galois extension L/K with Galois group $\mathrm{Gal}(L/K)$.

Example 1. *Let ζ_{ℓ^n} be a primitive ℓ^n-root of unity in $\overline{K}$ with $(\zeta_{\ell^n})^\ell = \zeta_{\ell^{n-1}}$. For $g \in G_K$ define a sequence of integers $0 \leq a_i < \ell$ by*

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

*Then we define the ℓ-*adic cyclotomic character *χ_{cyc} by*

$$\chi_{cyc}(g) = a_1 + a_2\ell + \cdots + a_n\ell^{n-1} + \cdots \in \mathbb{Z}_\ell^*.$$

Note that the value $\chi_{cyc} \pmod{\ell^n}$ simply says what g does to the ℓ^n-roots of 1. It is easy to check that the ℓ-adic cyclotomic character is multiplicative and hence gives a 1-dimensional representation

$$\chi_{cyc} \colon G_K \to \mathbb{Z}_\ell^* \subset \mathrm{GL}_1(\mathbb{Q}_\ell).$$

Taking $F_n = K(\zeta_{\ell^n})$ we have that $\mathrm{Gal}(\overline{K}/F_n) \to id \pmod{\ell^n}$ so χ_{cyc} is continuous.

Example 2. *Let E/K be an elliptic curve and, for each $n \geq 1$, let P_n and Q_n be a basis for $E[\ell^n]$ with $\ell P_n = P_{n-1}$ and $\ell Q_n = Q_{n-1}$. For $g \in G_K$ define $0 \leq$*

$a_i, b_i, c_i, d_i < \ell$ by

$$\begin{aligned}
g(P_1) &= a_1P_1 + c_1Q_1\\
g(Q_1) &= b_1P_1 + d_1Q_1\\
&\vdots\\
g(P_n) &= (a_1 + \cdots + a_n\ell^{n-1})P_n + (c_1 + \cdots + c_n\ell^{n-1})Q_n\\
g(Q_n) &= (b_1 + \cdots + b_n\ell^{n-1})P_n + (d_1 + \cdots + d_n\ell^{n-1})Q_n.
\end{aligned}$$

Then we have that

$$\rho(g) = \begin{pmatrix} a_1 + \cdots + a_n\ell^{n-1} + \cdots & b_1 + \cdots + b_n\ell^{n-1} + \cdots \\ c_1 + \cdots + c_n\ell^{n-1} + \cdots & d_1 + \cdots + d_n\ell^{n-1} + \cdots \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$$

is the representation on the ℓ-adic Tate module of E.

Now, let $\mathfrak{p}$ be a prime in K and $\mathfrak{P}$ be a prime in L such that $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Abusing notation we write the inertia group of $\mathfrak{P}/\mathfrak{p}$ as $I_\mathfrak{p}$(see Theorem 2.1.1).

Definition 2.3.5. *A representation ρ is* unramified at $\mathfrak{p}$ *if $\rho(I_\mathfrak{p}) = \{1\}$.*

We can characterize the unramified Galois representations by the following proposition.

Proposition 2.3.6 (p.I-7,[14])**.** *Let K be a number field, ρ be an ℓ-adic representation and L/K be a finite Galois extension with Galois group G. If L is the extension of K corresponding to $H = \ker(\rho)$, then ρ is unramified at $\mathfrak{p}$ if and only if $\mathfrak{p}$ is unramified in L/K.*

2.3.2 Integral Galois representations.

Let ρ be an ℓ-adic representation of G_K and let Λ be a lattice of $\mathbb{Q}_\ell^2$.

Definition 2.3.7. *A lattice Λ is G_K-*stable *(with respect to ρ) if $\rho(G_K)(\Lambda) \subseteq \Lambda$. This property only depends on the homothety class $[\Lambda]$ of Λ.*

Proposition 2.3.8 ([14])**.** *Every ℓ-adic representation ρ has at least one stable lattice.*

Given a rational Galois representation ρ, a stable lattice Λ and using a $\mathbb{Z}_\ell$-basis for Λ as a basis for V we obtain an integral matrix representation $\rho_\Lambda \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. This such representation ρ_Λ is called an *integral ℓ-adic Galois representation*. We will be interested in the collection of these, for fixed ρ and varying stable lattice Λ.

Definition 2.3.9. *Let ρ be rational Galois representation. The* isogeny class *of ρ is the set of pairs (Λ, ρ_Λ) where Λ is a stable lattice and ρ_Λ the induced map from G_K to $\mathrm{Aut}(\Lambda)$, modulo the equivalence relation which identifies homothetic lattices.*

Essentially the isogeny class of a Galois representation, for a fixed lattice Λ, is the "family" of representations given by all the homotetic lattices to Λ.

We would like to introduce the notion on how to compare two different integral Galois representations; this is due to the fact that for two different integral Galois representations coming from two different stable lattices, we may not have that they are equivalent as integral representations and in particular their images may not be the same or even conjugate. Nevertheless it is possible to compare them by their images in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The following definition expresses this idea.

Definition 2.3.10. *Two integral representations $\rho_j \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ are* isogenous *if there exists $\mathbf{U} \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ such that $\rho_2(\sigma) = \mathbf{U}\,\rho_1(\sigma)\,\mathbf{U}^{-1}$ for all $\sigma \in G_K$.*

Now that we have introduced the definition of an integral representation, we are able to talk about its *residual representation.*

Definition 2.3.11. *Let $\rho \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ be an integral representation. The* residual representation *associated to ρ is the map $\overline{\rho} \colon G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ obtained by composing ρ with the reduction modulo ℓ, as is described in the following diagram*

$$\begin{tikzcd}
G_K \arrow[r, "\rho"] \arrow[rd, "\overline{\rho}"'] & \mathrm{GL}_2(\mathbb{Z}_\ell) \arrow[d, "\text{mod } \ell"] \\
 & \mathrm{GL}_2(\mathbb{F}_\ell)
\end{tikzcd}$$

If ρ is any representation and Λ a stable lattice for ρ, then the associated residual representation $\overline{\rho}_\Lambda$ is the induced representation on $\Lambda/\ell\Lambda \cong \mathbb{F}_\ell^2$. Moreover, by the Brauer-Nesbitt theorem [6], the semisimplification of the residual representation does not depend on the choice of lattice.

On the other hand, for isogenous Galois representations their residual representation do not need to be isomorphic. Indeed, for a given rational Galois representation ρ with more than one stable lattice, say $\{\Lambda_i\}$, we will have more than one residual representation, $\overline{\rho}_{\Lambda_i}$, and these are not necessarily isomorphic.

Example 3. *Let E_1 and E_2 be elliptic curves defined over K with a K-rational 2-isogeny from $E_1 \to E_2$. As we saw in Example 2, for each curve we obtain an integral representation into $\mathrm{GL}_2(\mathbb{Z}_2)$ by letting G_K act on the 2-adic Tate module of each curve. Their residual representations have images which are either of order 1 (if $E_j(K)[2]$ has order 4) or 2 (if $E_j(K)[2]$ has order 2). Both can occur in the same isogeny class. In fact there must be a curve in the class with non-trivial residual image by the result known as* Ribet's wrench *[12].*

We can see this behaviour in Example 4. If we take the elliptic curves

$$E_{15.a1}\colon y^2+xy+y=x^3+x^2-2160x-39540$$
$$E_{15.a2}\colon y^2+xy+y=x^3+x^2-135x-660$$

representing the isogenies given in vertices ① and ② will get that $\overline{\rho}_{E_{15.a1}}(G_{\mathbb{Q}})\cong C_2$ *and* $\overline{\rho}_{E_{15.a2}}(G_{\mathbb{Q}})\cong C_1$.

We will mainly be interested in irreducible representations, such as those attached to elliptic curves. For these, the number of stable lattices is finite (up to homothety). The following result must be well-known, but since we could not find a reference, Professor Cremona provided the proof.

Proposition 2.3.12. *The number of stable lattices (up to homothety) is finite if and only if ρ is irreducible.*

Proof. If ρ is reducible, let Λ be a stable lattice and $\langle w\rangle$ a stable line for some $w\in V$. We may scale w by a power of ℓ so that $w\in\Lambda$ but $\ell^{-1}w\notin\Lambda$, and then there exists $v\in\Lambda$ such that $\Lambda=\langle v,w\rangle$. Set $\Lambda_n=\langle \ell^n v,w\rangle$ for $n\geq 0$. Then every Λ_n is stable and no two are homothetic. Notice that the stable line $\langle w\rangle$ is the limit of the Λ_n as $n\to\infty$.

Conversely suppose that there are infinitely many pairwise non-homothetic stable lattices. These determine infinitely many stable vertices in the Bruhat-Tits tree. Note that if $[\Lambda_1]$, $[\Lambda_2]$ are both stable and distance d apart, then all of the $d-1$ lattices between them are also stable. To see this, we may represent the classes $[\Lambda_j]$ by lattices Λ_j such that $\Lambda_1\supset\Lambda_2$ and Λ_1/Λ_2 is cyclic of order ℓ^d. Now G_K acts on Λ_1/Λ_2 and leaves every subgroup invariant, since (being cyclic) it has only one subgroup of each order ℓ^k for $0\leq k\leq d$. These subgroups have the form Λ/Λ_2 where $\Lambda_1\supseteq\Lambda\supseteq\Lambda_2$, and the class of Λ is a vertex between $[\Lambda_1]$ and $[\Lambda_2]$, which is therefore stable.

Now any infinite subtree of the Bruhat-Tits tree is unbounded and contains an infinite half line, so there is an infinite sequence of stable lattices Λ_n for $n\geq 0$ such that $\Lambda_n\supset\Lambda_{n+1}$ with index ℓ and Λ_0/Λ_n is cyclic of order ℓ^n for all n. The intersection $\Lambda_\infty=\bigcap_{n\geq 0}\Lambda_n$ is a stable $\mathbb{Z}_\ell$-module of rank at most 1 (since it has infinite index in Λ_0), and to complete the proof we show that it has rank exactly 1 (a line).

Let $\Lambda_0=\langle v,w\rangle$. Each Λ_n is determined by an element $(c_n:d_n)\in\mathbb{P}^1(\mathbb{Z}/\ell^n\mathbb{Z})$ such that

$$\Lambda_n=\{xv+yw\mid x,y\in\mathbb{Z}_\ell, c_nx+d_ny\equiv 0\pmod{\ell}\}.$$

Without loss of generality, $(c_1:d_1)=(1:0)$ and $\Lambda_1=\langle \ell v,w\rangle$. Since $\Lambda_{n+1}\subset\Lambda_n$ we have $(c_{n+1}:d_{n+1})\equiv(c_n:d_n)\pmod{\ell^n}$ and in particular $c_n\in\mathbb{Z}_\ell^*$, so again without loss of generality we may take $c_n=1$ and then $d_{n+1}\equiv d_n\pmod{\ell^n}$ for all n. This implies that $d=\lim_n d_n$ exists in $\mathbb{Z}_\ell$ (in fact in $\ell\mathbb{Z}_\ell$). Hence $\Lambda_\infty=\{xv+yw\mid x=-dy\}=\langle w-dv\rangle$, which is a stable line as required. □

Proposition 2.3.13. *Let ρ be an integral representation. The number of stable lattices (up to homothety) is* 1 *if and only if the residual representation $\overline{\rho}$ is irreducible.*

Proof. This lemma is Exercise 1.4 in [14]. This proof is due to Professor Cremona.

Let Λ be any stable lattice and let $\overline{\rho} = \overline{\rho}_\Lambda$ be the induced representation on $\Lambda/\ell\Lambda$. Suppose that there is another stable lattice Λ', not homothetic to Λ. Without loss of generality, we may take Λ' to have homothety class adjacent to that of Λ in the Bruhat-Tits tree, and hence (replacing Λ' by a homothetic lattice if necessary) be contained in Λ with index ℓ. Now G_K leaves stable the line $\Lambda'/\ell\Lambda$ in $\Lambda/\ell\Lambda$, so $\overline{\rho}$ is reducible.

Conversely, if $\overline{\rho}$ is reducible, then it leaves stable a line in $\Lambda/\ell\Lambda$ which must have the form $\Lambda'/\ell\Lambda$ where Λ' has index ℓ in Λ and is G_K-stable, so the class of Λ' is stable and distinct from that of Λ. □

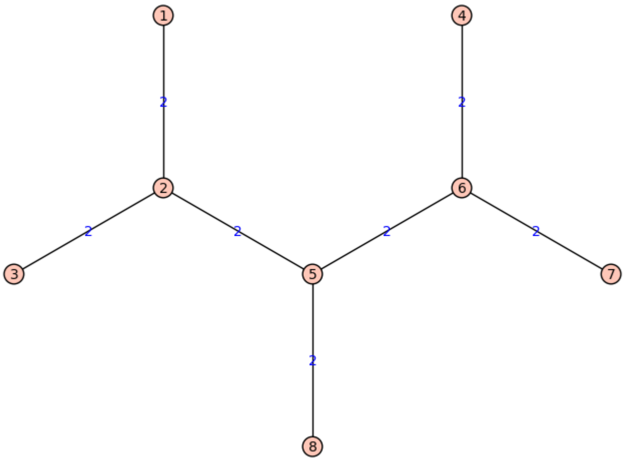
Definition 2.3.14. *The* stable Bruhat-Tits tree *with respect to a representation ρ is the subgraph of the Bruhat-Tits tree whose nodes are stable lattices with all edges between them.*

Remark 2.3.15. *If x and x' are stable all vertices in the unique path between between them are also stable, hence the stable Bruhat-Tits tree is indeed a tree. In what follows we will refer to the stable Bruhat-Tits tree as the* isogeny graph *of ρ.*

The preceding propositions say that the isogeny graph of a representation ρ is finite if and only if ρ is irreducible, and is a singleton if and only if the residual representation $\overline{\rho}$ (with respect to any stable lattice) is irreducible.

Example 4.

1. *There are eight* 2*-isogeny classes for the elliptic curves with conductor 15.*



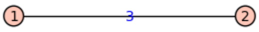
Each point (vertex) is a family of isomorphic elliptic curves over $\mathbb{Q}$ and each edge (path) is a 2*-isogeny between elliptic curves. We can observe that the maximum length between points is* 4*.*

2. *In Example 3 we have that all the representations attached to the elliptic curves representing each vertex are reducible.*

3. *For the isogeny class* 44a *we have*

$$E_{44.a1}\colon y^2 = x^3 + x^2 - 77x - 289$$
$$E_{44.a2}\colon y^2 = x^3 + x^2 + 3x - 1$$

the representations attached to those elliptic curves are irreducible and its Bruhat-Tits tree looks like



4. *For isogeny class* 254a *we have that*

$$E_{245.a1}\colon y^2 + y = x^3 - 7x + 12$$

the representations attached to these elliptic curves are irreducible and its Bruhat-Tits tree looks like

2.4 Livné

In this section are stated a definition, a proposition and a theorem from the article [11] by Ron Livné. These results are "heavy machinery" when talking about proving that two Galois representations are isomorphic. Since the proofs are beyond this thesis objectives, the reader can refer to the article to read the proofs.

Definition 2.4.1. *A subset T of a (finite dimensional) vector space V is non-quadratic (respectively non-cubic) if every homogeneous polynomial of degree $d = 2$ (respectively $d = 3$) on V which vanishes on T vanishes on V.*

Proposition 2.4.2 (4.2, [11])**.** *Let V be a vector space over $\mathbb{F}_2$. Then a function $f\colon V \to \mathbb{F}_2$ is represented by a homogeneous polynomial of degree d if and only if $\sum_{I\subset\{0,1,2,\ldots,d\}} f(\sum_{i\in I} v_i) = 0$ for any subset $\{v_i\}_{i=0}^{d} \subset V$ and $f(0) = 0$.*

The process of identifying non-quadratics and non-cubics sets, due to the proposition presented above, is straightforward.

Before finishing this section, it is important to remark that the following theorem is one of the "heaviest tools" that modern mathematicians have to prove that two Galois representations are isogenous. A modern reference in which this tool has been used is given in the article [8], where the motivation for Chapter 5 came from.

Theorem 2.4.3 (4.3 Theorem, [11])**.** *Let K be a global field, S a finite set of primes of K and E a finite extension of $\mathbb{Q}_2$. Denote the maximal ideal in the ring of integers of E by $\mathfrak{p}$ and the compositum of all quadratic extensions of K unramified outside S by K_S. Suppose ρ_1 and $\rho_2\colon G_K \to \mathrm{GL}_2(E)$ are two continuous representations, from G_K to $\mathrm{GL}_2(E)$, unramified outside S satisfying*

1. $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \equiv 0 \pmod{\mathfrak{p}}$ *and* $\det\rho_1 \equiv \det\rho_2 \pmod{\mathfrak{p}}$.

2. *There exists a set T of primes of K, disjoint from S, for which*

   i. *The image of the set* $\{\mathrm{Frob}_t\}_{t\in T}$ *in (the* $\mathbb{Z}/2\mathbb{Z}$*-vector space)* $\mathrm{Gal}(K_S/K)$ *is non-cubic.*

   ii. $\operatorname{tr}\rho_1(\mathrm{Frob}_t) = \operatorname{tr}\rho_2(\mathrm{Frob}_t)$ *and* $\det\rho_1(\mathrm{Frob}_t) = \det\rho_2(\mathrm{Frob}_t)$ *for all $t \in T$.*

Then ρ_1 and ρ_2 have isomorphic semisimplifications.

Chapter 3

Preliminaries.

Let K be a number field and let S be a finite set of primes of K. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be an integral continuous Galois representation unramified outside S and $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_2)$ its residual representation. This chapter concerns the following:

1. Section 3.1. In this section we introduce the definition of a *Black Box representation*; a system that provides the trace and the determinant of a 2-adic (integral) Galois representation.

2. Section 3.2. In this section we will see the full classification of the Galois extension, L/K, cut out by $\overline{\rho}$.

3. Section 3.3. Lastly, we state and prove a theorem which determines, for a finite set of primes, whether two 1-dimensional Galois representations, i.e., two multiplicative characters unramified outside S, are the same.

3.1 Obtaining information from a 2-adic Galois representation.

Let K be a number field and S be a finite set of primes of K. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be an integral Galois representation unramified outside S. The two pieces of information about the representation ρ that will be assumed to be known are

(a) the determinant of ρ, i.e., $\det(\rho(\sigma))$, and

(b) the trace of ρ, i.e., $\mathrm{tr}(\rho(\sigma))$,

for $\sigma \in G_K$, which will be specified (up to conjugacy) as a Frobenius, $\mathrm{Frob}_\mathfrak{p}$, attached to an unramified prime $\mathfrak{p} \notin S$, i.e., $\sigma = \mathrm{Frob}_\mathfrak{p} \in G_K$ (see sections 2.1 and 2.1).

Observe that the previous information can be summarized as follows, for any $\sigma \in G_K$, the characteristic polynomial of $\rho(\sigma)$ given by

$$\begin{aligned} F_\sigma(t) &= \det(\rho(\sigma) - t \times \mathbf{I}) \\ &= t^2 - \mathrm{tr}(\rho(\sigma))t + \det(\rho(\sigma)), \end{aligned} \tag{3.1}$$

is a monic quadratic polynomial in $\mathbb{Z}_2[t]$ whose coefficients are the trace and determinant of $\rho(\sigma)$.

Moreover, when the Frobenius is specified, $\sigma = \mathrm{Frob}_\mathfrak{p}$, for any prime $\mathfrak{p} \notin S$, we can also write (3.1) as

$$F_\mathfrak{p}(t) = F_{\mathrm{Frob}_\mathfrak{p}}(t).$$

Note that the determinant and trace of ρ are independent of the choice of ρ within its isogeny class. This is relevant when the residual representation $\overline{\rho}$ is reducible since otherwise, by Proposition 2.3.13, the isogeny class only contains one element.

Definition 3.1.1. *A* Black Box Galois representation *is a system given for K and S which provides the quadratic polynomial $F_\mathfrak{p}(t)$ in $\mathbb{Z}_2[t]$ for any given prime $\mathfrak{p}$ not in S.*

Since $F_\sigma(t) \in \mathbb{Z}_2[t]$, for each natural number k, if $F_\mathfrak{p}(1) \equiv 0 \pmod{2^k}$ for any unramified prime $\mathfrak{p} \notin S$, then we can define the *test function*

$$t_k(\mathfrak{p}) := \frac{1}{2^k}(1 - \mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) + \det(\rho(\mathrm{Frob}_\mathfrak{p}))) \pmod{2}. \tag{3.2}$$

Other useful quantities which will be used in the next chapters are

$$v(\mathfrak{p}) = \mathrm{ord}_2(F_\mathfrak{p}(1)) \tag{3.3}$$

a non-negative integer and

$$v_1(\mathfrak{p}) = \mathrm{ord}_2(\det(\rho(\mathrm{Frob}_\mathfrak{p})) - 1) \tag{3.4}$$

a positive integer. Note that $t_k(\mathfrak{p})$ is defined when $v(\mathfrak{p}) \geq k$ and its values tell us whether or not $v(\mathfrak{p}) \geq k + 1$.

3.2 Classification of Galois extensions L/K with group C_1, C_2, C_3 or S_3.

Let K be a number field and S be a finite set of primes of K. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be an integral Galois representation unramified outside S and let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_2)$ be its residual Galois representation, which is also unramified outside S. In this section we will see the classification of all possible images of the representation and their related Galois extensions.

To start with this classification, let's take $G = \overline{\rho}(G_K)$. Since $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to S_3, G will be either isomorphic to C_1, C_2, C_3 or S_3. Let L be the splitting field of $\overline{\rho}$ with cubic polynomial $f(x) \in K[x]$, that is, L is the fixed field of $\ker(\rho)$. Then $\mathrm{Gal}(L/K) \cong G$ and $[L : K] \leq 6$. Recall from Section 2.3.2 that the residual image is only well-defined once we have specified a stable lattice Λ.

We have two cases to analyse, depending on whether $\overline{\rho}$ is irreducible or reducible.

(i) When $\overline{\rho}$ is irreducible, i.e., the image is either C_3 or S_3: the lattice Λ is unique up to homothety and the isomorphism class of the image is well-defined. Therefore we will know exactly in which case we are. We define the discriminant[I] of L as $\Delta = \mathrm{disc}(f)$. Observe that the image is C_3 if and only if $\Delta \in (K^*)^2$.

(ii) When $\overline{\rho}$ is reducible, i.e., the image is either C_1 or C_2: the residual image and splitting field depend (in general) on the stable lattice Λ. In this case, at the beginning we will treat these two cases as one but in Section 4.2 we will explain how to distinguish between the cases C_1 and C_2. When the image is C_2 the fixed field is $K(\sqrt{\Delta})$ with $\Delta \in (K^*)/(K^*)^2$ and when the image is C_1 take $\Delta = 1$.

The set of Galois extensions L/K with $\mathrm{Gal}(L/K) \cong G$, unramified outside S, is finite. Moreover there is an algorithm to find them. In Section 4.1 we will see how to determine the splitting field.

3.2.1 Distinguishing the irreducible cases from the reducible cases.

As above let S be a finite set of primes of the number field K. The set of Galois extensions L of K unramified outside S and with $\mathrm{Gal}(L/K)$ isomorphic to either C_3 or S_3 is finite (see [3]). An algorithm for finding this finite set may be found in [10]. We denote by F a set of monic cubic polynomials in $\mathcal{O}_K[x]$ satisfying the following:

each extension L/K, unramified outside S and Galois with $\mathrm{Gal}(L/K) \cong C_3$ *or* S_3 *is the splitting field of f for a unique $f \in F$.*

(3.5)

We would like to find a way to characterize these fields by examining their splitting behaviour of primes $\mathfrak{p}$ of K not in S. To do this, we start with the following definition.

Definition 3.2.1. *For a given monic cubic polynomial $f \in \mathcal{O}_K[x]$ and for a prime $\mathfrak{p} \notin S$ of K define*

$$\lambda(f, \mathfrak{p}) = \begin{cases} 1 & \textit{if } f \textit{ is irreducible mod } \mathfrak{p} \\ 0 & \textit{else.} \end{cases}$$

[I] Here and throughout we only ever define discriminants modulo squares, i.e., as elements of $K^*/(K^*)^2$.

Lemma 3.2.2. *Let f be an irreducible monic cubic polynomial in $\mathcal{O}_K[x]$ with splitting field L. Then for $\mathfrak{p} \not| \Delta_f$*

$$\lambda(f,\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathrm{Frob}_{\mathfrak{p}} \text{ has order } 3 \text{ in } \mathrm{Gal}(L/K) \\ 0 & \text{if } \mathrm{Frob}_{\mathfrak{p}} \text{ has order } 1 \text{ or } 2 \text{ in } \mathrm{Gal}(L/K). \end{cases}$$

Proof. Straightforward. □

Definition 3.2.3. *Let K and S be as before. Let F be a set of cubic polynomials satisfying (3.5). An ordered set of primes $T_0 = \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$ of K is a* distinguishing set *for (F, S) if*

(1) $T_0 \cap S = \emptyset$,

(2) $\mathrm{ord}_{\mathfrak{p}}(\mathrm{disc}(f)) = 0$ *for all* $\mathfrak{p} \in T_0$ *and* $f \in F$,

(3) *the vectors* $(\lambda(f,\mathfrak{p}_i), ..., \lambda(f,\mathfrak{p}_t)) \in \mathbb{F}_2^t$ *for* $f \in F$ *are distinct and non-zero.*

As notation we will write $\mathbf{v}(f, T_0) := (\lambda(f,\mathfrak{p}_i), ..., \lambda(f,\mathfrak{p}_t))$ when $T_0 = \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$.

Remark 3.2.4. *For fixed S and a set F of cubics satisfying (3.5) we will set a distinguishing set of primes for (F, S) once and for all and denote it by T_0.*

Lemma 3.2.5. *A distinguishing set of primes for (F, S) does exist.*

Proof. Let $F = \{f_i\}_{i=1}^n$. Set $f_0 = x^3$ so that $\lambda(f_0,\mathfrak{p}) = 0$ for all $\mathfrak{p}$. It is enough to show that for all $0 \le j < i \le n$ there exists a prime $\mathfrak{p}$ not in S such that $\lambda(f_i,\mathfrak{p}) \ne \lambda(f_j,\mathfrak{p})$. For $i \ge 1$ let L_i be the splitting field of f_i. We divide into three cases:

Case 1. When $j = 0$ so that $\lambda(f_j, T_0) = 0$ for all $\mathfrak{p}$, we analyse the frequency for a single $\lambda(f_i,\mathfrak{p}) = 1$; by the Čebotarev density theorem when $\mathrm{Gal}(L_i/K) \cong S_3$ it is $\dfrac{1}{3}$ and when $\mathrm{Gal}(L_i/K) \cong C_3$ it is $\dfrac{2}{3}$.

Case 2. When $i, j \ge 1$ and $\mathrm{disc}(L_i) \not\equiv \mathrm{disc}(L_j) \pmod{(K^*)^2}$ then L_i and L_j are disjoint. There are three possibilities for the Galois group of their composition and, in every case, the frequency(density) of the primes we need is:

$$2\left(\frac{1}{3} \times \frac{2}{3}\right) = \frac{4}{9} \text{ when } \mathrm{Gal}(L_iL_j) \text{ is } S_3 \times S_3,$$

$$\frac{1}{3} \times \frac{1}{3} + \frac{2}{3} \times \frac{2}{3} = \frac{5}{9} \text{ when } \mathrm{Gal}(L_iL_j) \text{ is } S_3 \times C_3,$$

$$\frac{1}{3} \times \frac{1}{3} + \frac{2}{3} \times \frac{2}{3} = \frac{5}{9} \text{ when } \mathrm{Gal}(L_iL_j) \text{ is } C_3 \times S_3.$$

Case 3. When $i, j \ge 1$ and $\mathrm{disc}(L_i) \equiv \mathrm{disc}(L_j) \pmod{(K^*)^2}$ then again we have two possibilities, both Galois groups are either isomorphic to C_3 or S_3. When both are isomorphic to C_3 we have

$$2\left(\frac{1}{3}\times\frac{2}{3}\right)=\frac{4}{9}.$$

On the other hand, when both fields have Galois groups isomorphic to S_3. In this case we have the following diagram

$$\begin{tikzcd}
 & L_iL_j & \\
L_i \arrow[ur, "3"] & & L_j \arrow[ul, "3"'] \\
 & K(\sqrt{\Delta}) \arrow[uu, "9"] \arrow[ul, "3"] \arrow[ur, "3"'] & \\
 & K \arrow[u, "2"] &
\end{tikzcd}$$

where $L_iL_j \cong C_2 \rtimes C_3 \times C_3$ and the density(frequency) of the primes is

$$2\left(\frac{1}{2}\left(\frac{2}{3}\times\frac{1}{3}\right)\right)=\frac{2}{9}.$$

□

The number t of elements in T_0 depends on the number n of C_3 and S_3 extensions of K unramified outside S, so it is not difficult to see that $t \leq n$ and $n \leq 2^t$, thus $\lceil \log_2(n) \rceil \leq t \leq n$.

We will use a distinguishing set T_0 in Section 4.1 below to determining the residual image of a Galois representation.

Algorithm 1: This function finds the finite set of monic cubic polynomials $\{f_i\}_{i=1}^n$ in $\mathcal{O}_K[x]$ defining all possible C_3 or S_3 extensions $\{L_i\}_{i=1}^n$ of K unramified outside S.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
Output: A finite set list of irreducible monic cubics $f_1, ..., f_n \in \mathcal{O}_K$ such that
         every Galois extension of $K$ with Galois group $C_3$ or $S_3$ unramified
         outside $S$ is the splitting field of one of the $f_i$.
By Class Field Theory or Kummer Theory return: $\{f_i\}_{i=1}^n$.
```

For a full description of the Kummer Theory method see [10].

Algorithm 2: This function finds a finite set T_0 of primes of K satisfying Definition 3.2.3.

```
Input : A number field $K$.
        A finite set $S$ of primes of $K$.
Output: A finite set $T_0$ of primes of $K$ satisfying Definition 3.2.3.
Use Algorithm 1 to compute the polynomials $\{f_i\}_{i=1}^n$;
Let $t_0$ be a reducible polynomial;
Define an empty set $T_0 = \{\}$;
while $\#\{\mathbf{v}_i(f_i, T_0) \mid 0 \leq i \leq n\} < n+1$ do
    find $i \neq j$ such that $\mathbf{v}_i(f_i, T_0) = \mathbf{v}_j(f_j, T_0)$;
    find a prime $\mathfrak{p} \notin S \cup T_0$ such that $\lambda(f_i, \mathfrak{p}) \neq \lambda(f_j, \mathfrak{p})$;
    set $T_0 := T_0 \cup \{\mathfrak{p}\}$;
Return: $T_0$.
```

3.2.2 Linearly independent sets of primes

For K and S as before, consider all quadratic extensions L/K having Galois group $G \cong C_2$. Then we have that there is a finite number of these extensions and they look like $L = K(\sqrt{\Delta})$ for $\Delta \in K(S,2) \leq K^*/(K^*)^2$, where $K(S,2)$ is given by (2.4).

In fact $K(S,2)$ is finite of cardinality 2^r with $r \geq 1$. We can see that the multiplicative group $K(S,2)$ is a finite-dimensional vector space over $\mathbb{F}_2$ of dimension $r = \dim_{\mathbb{F}_2}(K(S,2))$.

Let $\{\Delta_i\}_{i=1}^r$ be a basis for $K(S,2)$. We have an isomorphism

$$\begin{aligned} \mathbb{F}_2^r &\xrightarrow{\sim} K(S,2) \\ \mathbf{x} &\mapsto \prod_{i=1}^r \Delta_i^{x_i}, \end{aligned} \tag{3.6}$$

where $\mathbf{x} = (x_i)_{i=1}^r$. Each prime $\mathfrak{p} \notin S$ determines a linear map

$$\alpha_{\mathfrak{p}} \colon K(S,2) \to \mathbb{F}_2 \tag{3.7}$$

defined as

$$\begin{aligned} \alpha_{\mathfrak{p}}(\Delta) &= [\Delta \mid \mathfrak{p}] \\ &= \begin{cases} 0 \pmod 2 & \text{if } \mathfrak{p} \text{ splits in } K(\sqrt{\Delta}) \text{ or } \Delta = 1 \\ 1 \pmod 2 & \text{if } \mathfrak{p} \text{ is inert in } K(\sqrt{\Delta}). \end{cases} \end{aligned}$$

Moreover, for $I \subseteq \{1, ..., r\}$, $\mathfrak{p}_I$ denotes a prime such that

$$[\Delta_i \mid \mathfrak{p}_I] = 1 \Leftrightarrow i \in I. \tag{3.8}$$

In this way, if $I = \{i\}$ we write $\mathfrak{p}_i = \mathfrak{p}_{\{i\}}$ and if $I = \{i, j\}$ we write $\mathfrak{p}_{ij} = \mathfrak{p}_{\{i,j\}}$.

Lemma 3.2.6. *For each $I \subseteq \{1, ..., r\}$ a prime $\mathfrak{p}_I \notin S$ exists.*

Proof. By the Čebotarev's density theorem the set of primes satisfying (3.8) has density $1/2^r$. □

Now we define a set of primes which may be used (see next section) to distinguish two characters unramified outside S.

Definition 3.2.7. *A set T_1 of primes $\mathfrak{p}$ of K where $\mathfrak{p} \notin S$, is* linearly independent with respect to S *if the linear functions $\{\alpha_{\mathfrak{p}} \mid \mathfrak{p} \in T_1\}$ form a basis for the dual space of $K(S, 2)$.*

Remark 3.2.8. *By Lemma 3.2.6 such a set exists, for example $\{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$. We fix once and for all a linearly independent set of primes and denote it by T_1 where $\#T_1 = r$.*

By (3.8) we get that

$$\alpha_{\mathfrak{p}_I}(\Delta) = \sum_{i \in I} \alpha_{\mathfrak{p}_i}(\Delta). \tag{3.9}$$

Algorithm 3: This function determines a finite set T_1 of primes of K satisfying Definition 3.2.7.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
Output: A linearly independent set $T_1$ of primes of $K$.
Compute a basis $\{\Delta_i\}_{i=1}^r$ for $K(S, 2)$;
$T_1 := \{\}$;
$A :=$ a $0 \times r$ matrix over $\mathbb{F}_2$;
while rank($A$) $< r$ do
    Take $\mathfrak{p} \notin S \cup T_1$;
    Set $\mathbf{v} = ([\Delta_1|\mathfrak{p}], ..., [\Delta_r|\mathfrak{p}])$;
    if $\mathbf{v}$ is not in the row-space of $A$ then
        $A := A + \mathbf{v}$;      # i.e., adjoin $\mathbf{v}$ as a new row of $A$
        $T_1 := T_1 \cup \{\mathfrak{p}\}$.
Return: $T_1$.
```

3.3 1-dimensional Galois representations.

Let ρ_1 and ρ_2 be two 2-adic Galois representations unramified outside S. The objective of this section is to prove that for a given finite set T_1 of linearly independent primes, if $\det(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \det(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ for all $\mathfrak{p} \in T_1$ then $\det(\rho_1(\sigma)) = \det(\rho_2(\sigma))$ for all $\sigma \in G_K$.

Let just recall that $\det(\rho_i)\colon G_K \to \mathrm{GL}_1(\mathbb{Z}_2) \cong \mathbb{Z}_2^*$ is a 1-dimensional Galois representation which is indeed a character. In this way we can formulate the following proposition.

Lemma 3.3.1. *Let $\chi\colon G_K \to \mathbb{F}_2$ be an additive quadratic character unramified outside S. If $\chi(\mathrm{Frob}_{\mathfrak{p}}) = 0$ for all $\mathfrak{p}$ in T_1 then $\chi = 0$.*

Proof. Suppose that $\chi \neq 0$, then the fixed field of $\ker(\chi)$ is a quadratic extension $K(\sqrt{\Delta})$ for some non-trivial Δ in $K(S, 2)$. Since $\chi(\mathrm{Frob}_{\mathfrak{p}}) = 0$ for all $\mathfrak{p}$ in T_1 we have that $[\Delta|\mathfrak{p}] = 0$. By Definition 3.2.7 we get that $\Delta = 1$. □

We end the chapter by stating the main theorem of the section that will allow us to prove that two 1-dimensional Galois representations are the same.

Theorem 3.3.2. *Let $\chi_i\colon G_K \to \mathbb{Z}_2^*$ for $i = 1, 2$ be two continuous characters both unramified outside a finite set of primes S and let T_1 be a linearly independent set of primes. If $\chi_1(\mathrm{Frob}_{\mathfrak{p}}) = \chi_2(\mathrm{Frob}_{\mathfrak{p}})$ for all $\mathfrak{p} \in T_1$, then $\chi_1(\sigma) = \chi_2(\sigma)$ for all $\sigma \in G_K$.*

Proof. Let $\chi_1\chi_2^{-1}\colon G_K \to \mathbb{Z}_2^*$ be a character denoted by χ. Suppose that $\chi \neq 1$. Let $k \geq 1$ be the greatest integer such that $\chi(\sigma) \equiv 1 \pmod{2^k}$. Note that $\chi(\sigma) \equiv 1 \pmod{2}$ for all $\sigma \in G_K$ so k does exist. Consider

$$\chi(\sigma) \equiv 1 + 2^k\alpha(\sigma) \pmod{2^{k+1}}$$

where $\sigma \mapsto \alpha(\sigma)$ is a non-trivial (additive) quadratic character $G_K \to \mathbb{F}_2$. However, $\alpha(\mathrm{Frob}_{\mathfrak{p}}) \equiv 0 \pmod{2}$ for all $\mathfrak{p} \in T_1$, so by Lemma 3.3.1 we have that $\alpha = 0$, which contradicts the minimality of k. □

Chapter 4

Black Box Galois representations.

Let K be a number field and let S be a finite set of primes of K. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a 2-adic integral Galois representation unramified outside S and let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_2)$ be its residual representation. Let L be the Galois extension of K cut out by $\overline{\rho}$. Assume we are able to compute $\det(\rho(\mathrm{Frob}_\mathfrak{p}))$ and $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p}))$ for primes $\mathfrak{p}$ in K. By only using the determinant and the trace of ρ at $\mathrm{Frob}_\mathfrak{p}$ for a finite set of primes $\mathfrak{p}$, depending only on S, we will be able to determine much information about $\mathfrak{p}$ in the following sections.

1. Section 4.1. In this section we develop techniques and algorithms which determine whether the residual Galois representation $\overline{\rho}$ is reducible or irreducible. When $\overline{\rho}$ is irreducible, its image is completely determined and it will be possible to determine the splitting field L of $\overline{\rho}$, which is given by a monic cubic polynomial in $\mathcal{O}_K$. When $\overline{\rho}$ is reducible, we proceed to the next section.

2. Section 4.2. In this section we develop techniques and algorithms, assuming that $\overline{\rho}$ is reducible, which determine whether there is a choice of a stable lattice, for ρ, such that the image of $\overline{\rho}$ is C_1. This is done by computing the width of the stable Bruhat-Tits tree related to ρ. It will be seen that when the width of the tree is one, for all stable lattices, the image of $\overline{\rho}$ is C_2, i.e., there is no choice of stable lattice for which the image is C_1, and the splitting field L is one of two quadratic extensions. On the other hand, when the width of the tree is at least 2, there exists a stable lattice such that the image of $\overline{\rho}$ is C_1 and we proceed to the next section.

3. Section 4.3. In this section we extend and generalize the techniques and algorithms proven in Section 4.2. Using these generalizations it will be possible for us to determine completely the representation ρ modulo 2^{k+1} under the assumption that it is trivial modulo 2^k. Moreover, in some cases, it will be possible to

determine the width, the edges and nodes of the stable Bruhat-Tits tree related to ρ. Particularly, when $k = 1$, it will be seen in examples 6 and 7 how these techniques are applied to determine the triviality of the representation ρ modulo 2^2, determine whether the width of the stable Bruhat-Tits tree is exactly 2, 3 or at least 4 and obtain its respective edges and nodes.

4. Section 4.4. In this section we state and prove a theorem that will provide an easy criterion to determine whether, for a given Galois representation which is trivial modulo 2^k and satisfies certain conditions, there exists an isogenous representation, to the given one, that is trivial modulo 2^{k+1}. As a corollary we obtain a criterion based on a finite of primes (depending only on S) for ρ to have trivial semisimplification.

4.1 Determining the residual image.

Let K be a number field and S be a set of primes of K. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a Galois representation unramified outside S and let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_2)$ be its residual representation. We would like to determine the image of the residual representation.

To do this, using Algorithm 1, we find a set of monic cubic polynomials $\{f_i\}_{i=1}^n$ in $\mathcal{O}_K[x]$ defining all possible C_3 or S_3 extensions $\{L_i\}_{i=1}^n$ of K unramified outside S. We also set f_0 as a reducible monic cubic polynomial in $\mathcal{O}_K[x]$, say $f_0 = x^3$.

We start the algorithm to determine the residual image with the following lemma.

Lemma 4.1.1. *Let $\{f_i\}_{i=1}^n$ be a set of monic cubic polynomials in $\mathcal{O}_K[x]$ defining all possible C_3 or S_3 extensions $\{L_i\}_{i=1}^n$ of K unramified outside S and f_0 be any reducible monic cubic polynomial in $\mathcal{O}_K[x]$. Then*

1. *If $[L : K] = 6$ or 3 then, for one i, we will have that $L = L_i$ and then*

$$\lambda(f_i, \mathfrak{p}) \equiv \mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) \pmod 2$$

for all $\mathfrak{p} \notin S$. Moreover, for infinitely many primes $\mathfrak{p}$ we will have that

$$\mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod 2.$$

2. *$[L : K] \leq 2$ if and only if*

$$\lambda(f_0, \mathfrak{p}) \equiv \mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 0 \pmod 2$$

for all $\mathfrak{p} \notin S$.

Proof. Suppose that $[L : K] = 6$ or 3. Then the image of $\overline{\rho}$ is C_3 or S_3 and $L = L_i$ is the splitting field of f_i, which is an irreducible polynomial and its discriminant may be a square or not, for some i, $1 \leq i \leq n$. Hence, by Lemma 3.2.2, for all $\mathfrak{p} \notin S$ we have that

$$\begin{aligned}\lambda(f_i, \mathfrak{p}) = 1 &\Leftrightarrow \text{Frob}_{\mathfrak{p}} \text{ has order 3 in } \text{Gal}(L_i/K)\\ &\Leftrightarrow \overline{\rho}(\text{Frob}_{\mathfrak{p}}) \text{ has order 3 in } \text{GL}_2(\mathbb{F}_2)\\ &\Leftrightarrow \text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \equiv 1 \pmod 2.\end{aligned}$$

On the other hand, if $[L : K] \leq 2$ then the image of $\overline{\rho}$ is C_1 or C_2 and we will have for all $\mathfrak{p} \notin S$ that $\lambda(f_0, \mathfrak{p}) = 0$ and $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \equiv 0 \pmod 2$ since Frob_p has order 1 or 2.

□

We can observe from the previous lemma that only one prime is needed to show that we are in the irreducible case and by checking the discriminant of the found polynomial, we can be certain that the residual image is exactly C_3 or S_3. On the other hand, to be completely certain of lying on the reducible cases there are needed, apparently, an infinite number of primes to prove it. Nevertheless, by the following lemma, we will see a criterion that will allow us to determine the residual image by using a finite set of primes.

Lemma 4.1.2. *Let K and S be as above then, for any set T_0 of primes satisfying Definition 3.2.3 the values of* $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}}))$ *modulo* 2 *for* $\mathfrak{p} \in T_0$ *determine the residual Galois representation up to semisimplification.*

Proof. Let $\{f_i\}_{i=1}^n$ be the polynomials generating the C_3 and S_3 extensions of K found using Algorithm 1, and let $T_0 = \{\mathfrak{p}_i\}_{i=1}^t$ be a set of primes satisfying Definition 3.2.3, such that the vectors

$$\mathbf{v}_i = (\lambda(f_i, \mathfrak{p}_1), ..., \lambda(f_i, \mathfrak{p}_t))$$

in $\mathbb{F}_2^t$ are distinct and non-zero by Lemma 3.2.5. Set $\mathbf{v}_0$ as a zero vector in $\mathbb{F}_2^t$. For this set of primes, take the vector

$$\mathbf{v} = (\text{tr}(\overline{\rho}(\text{Frob}_{\mathfrak{p}_1})), ..., \text{tr}(\overline{\rho}(\text{Frob}_{\mathfrak{p}_t})))$$

in $\mathbb{F}_2^t$. Therefore, by Lemma 4.1.1, we have that

$$\mathbf{v} = \mathbf{v}_i,\ 1 \leq i \leq n,\ \Leftrightarrow L = L_i \Leftrightarrow [L : K] = 6 \text{ or } 3$$

and

$$\mathbf{v} = \mathbf{v}_0 = \mathbf{0} \Leftrightarrow [L : K] \leq 2$$

where $\mathbf{v}$ must be equal exactly to one of the $\mathbf{v}_i$. □

As we saw in Definition 3.2.3, in general we will have that $\lceil \log_2(n) \rceil \leq t \leq n$.

Algorithm 4: This function determines the residual image of an integral 2-adic Galois representation.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
         A Black Box Galois representation $\rho$ unramified outside $S$.
Output: If the image is irreducible return: True, $f_i$ generating the $C_3$ or $S_3$
         splitting field.
         If the image is reducible return: False.
Use Algorithm 1 to compute $\{f_i\}_{i=1}^n$;
Use Algorithm 2 to compute $T_0$;
Set $\mathbf{v} = (\mathrm{tr}(\overline{\rho}(\mathrm{Frob}_{\mathfrak{p}_1})), ..., \mathrm{tr}(\overline{\rho}(\mathrm{Frob}_{\mathfrak{p}_t})))$ for $\mathfrak{p}_i \in T_0$;
for $i$=1...$n$ do
    if $\mathbf{v} = \mathbf{v}_i(f_i, T_0)$ then
        Return: True, $f_i$.
Return: False.
```

4.2 Reducible Residual Representation.

This section is based on unpublished notes by Professor John Cremona which include proofs but no examples. Some details, and all the examples, are original.

Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be an irreducible Galois representation unramified outside a set of primes S with reducible residual representation $\overline{\rho}$, i.e., $\overline{\rho}(G_K)$ is either C_1 or C_2. Then, by Section 2.3.2, ρ determines a finite class of isogenous integral representations. We next distinguish two different possibilities:

1. "Small isogeny class" or "width=1": exactly two stable lattices, with adjacent vertices in the Bruhat-Tits tree. Both residual representations have splitting fields which are quadratic over K, say $K(\sqrt{\Delta_j})$ for $j = 1, 2$ with $\Delta_j \in K(S, 2)$.

2. "Large isogeny class of width at least 2": more than two stable lattices. Now the stable subtree of the Bruhat-Tits tree has at least 4 vertices and at least one has degree exactly 3. In other words, the isogeny class contains at least 4 elements, and at least one has trivial residual representation. (See figure A1 at page 44.)

Our aim is to be able to distinguish between the "small isogeny class" and the "large isogeny class" by only using the Black Box.

4.2.1 Small Isogeny Class.

Let Λ_1 be a stable lattice under the action of ρ. Since $\overline{\rho}$ is reducible, there is an index 2 sublattice, Λ_2, which is also stable under ρ. Choosing the bases $\Lambda_1 = \langle v, w\rangle$ and $\Lambda_2 = \langle 2v, w\rangle$, we have that

$$\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod 2$$

for all $\sigma \in G_K$.

There are two ways in which the graph of adjacent stable lattices Λ_1—Λ_2 could be extended.

(1) If $c \equiv 0 \pmod 4$ for all $\sigma \in G_K$ then

$$\rho(\sigma) \equiv \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix} \pmod 4$$

and $\Lambda_3 = \langle 4v, w\rangle$ is also stable, extending the stable graph to Λ_1—Λ_2—Λ_3. Observe that the lattice $\Lambda_4 = \langle 2v + w, 2w\rangle$ is also stable and adjacent to Λ_2.

(2) If $b \equiv 0 \pmod 2$ for all $\sigma \in G_K$ then

$$\rho(\sigma) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

so $\overline{\rho}$ is trivial. Then $\Lambda_3' = \langle v, 2w\rangle$ is also stable and extends the graph to Λ_3'—Λ_1—Λ_2. Observe that the lattice $\Lambda_4' = \langle 2v, v + w\rangle$ is also stable and adjacent to Λ_1.

These two situations are not essentially different; by conjugating with the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ we interchange the roles of Λ_1 and Λ_2, and the two cases (1) and (2).

Thus, we obtain two additive quadratic characters of G_K

$$\chi_c \colon \sigma \mapsto \frac{c}{2} \pmod 2 \quad \text{and} \quad \chi_b \colon \sigma \mapsto b \pmod 2 \tag{4.1}$$

unramified outside S, which correspond to two extensions $K(\sqrt{\Delta_b})$, $K(\sqrt{\Delta_c})$ with $\Delta_b, \Delta_c \in K(S, 2)$, possibly equal or trivial.

The stable lattice graph can be extended if and only if at least one of these characters, and its related extension, is trivial: χ_c is trivial if and only if the two lattices Λ_3 and Λ_4, which are the two index 2 sublattices of Λ_2 not homothetic to Λ_1, are stable. Moreover, χ_b is trivial if and only if the two lattices Λ_3' and Λ_4', which are the two index 2 sublattices of Λ_1 other than Λ_2, are stable. This proves the following proposition.

Proposition 4.2.1. *The condition for the isogeny class to be small is therefore that the characters χ_b and χ_c are* both *non-trivial.*

Now consider all pairs $\{\Delta_1, \Delta_2\}$ with $\Delta_j \in K(S,2)$ both non-trivial, but possibly equal. We are looking for a condition which tests whether this pair is compatible with what we know about the representation ρ, with a view to excluding either all possible pairs, in which case the isogeny class is large, or excluding all but one pair, in which case the class is small and we know the pair attached to it.

The condition must involve only using the data we have access to, namely the trace and determinant of $\rho(\mathrm{Frob}_\mathfrak{p})$ for a finite set of primes $\mathfrak{p} \notin S$. Then for $\sigma \in G_K$ we have the test

$$t_1(\sigma) := \frac{1}{2}(F_\sigma(1)) \equiv \frac{1}{2}(1 - \mathrm{tr}(\rho(\sigma)) + \det(\rho(\sigma))) \pmod 2. \tag{4.2}$$

Take $\sigma = \mathrm{Frob}_\mathfrak{p}$ and set $t_1(\mathfrak{p}) = t_1(\mathrm{Frob}_\mathfrak{p})$ for $\mathfrak{p} \notin S$. Then the value of $t_1(\mathfrak{p})$ may be computed for each $\mathfrak{p}$, using the Black Box. Observe that in this case $\det(\rho(\sigma)) \equiv 1 \pmod 2$ for all $\sigma \in G_K$.

Proposition 4.2.2. *With notation as above,*

$$t_1(\sigma) = \chi_b(\sigma)\chi_c(\sigma)$$

Proof. We compute

$$t_1(\sigma) = \frac{1}{2}(1-(a+d)+(ad-bc)) = \frac{1}{2}((1-a)(1-d)-bc) \equiv \frac{1}{2}bc \equiv \chi_b(\sigma)\chi_c(\sigma) \pmod 2,$$

using $a \equiv d \equiv 1 \pmod 2$. □

Observe that the previous proposition also proves that the t_1 is well-defined.

Corollary 4.2.3. *For $j = 1, 2$, let Δ_j be a pair of non-trivial elements of $K(S,2)$ (possibly equal). Let $\mathfrak{p}$ be a prime which is inert in both extensions $K(\sqrt{\Delta_j})$. If $t(\mathfrak{p}) = 0$ then $\{\Delta_1, \Delta_2\} \neq \{\Delta_b, \Delta_c\}$.*

Proof. If $\{\Delta_1, \Delta_2\} = \{\Delta_b, \Delta_c\}$ and $\sigma = \mathrm{Frob}_\mathfrak{p}$, then $\chi_b(\sigma) = \chi_c(\sigma) = 1$. Hence $t_1(\sigma) = 1$ by Proposition 4.2.2. □

4.2.2 Determining the Small Isogeny Class.

Let $V = K(S, 2)$ be given by Definition 2.4. Let $\{\Delta_i\}_{i=1}^r$ be a basis for $K(S, 2)$ and take $\Delta_b, \Delta_c \in K(S, 2)$ such that $\Delta_b = \prod_{i=1}^r \Delta_i^{x_i}$, $\Delta_c = \prod_{i=1}^r \Delta_i^{y_i}$ with $\mathbf{x} = (x_i)$ and $\mathbf{y} = (y_i)$ vectors in $\mathbb{F}_2^r$ given by the isomorphism (3.6). Determining the vectors $\mathbf{x}$ and $\mathbf{y}$ is equivalent to determining Δ_b and Δ_c, which then tell us whether the width of the graph is 1 or at least 2.

Let T_1 be a linearly independent set of primes chosen Remark 3.2.8 so that $T_1 = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$ where the $\alpha_{\mathfrak{p}_i}$ are a dual basis for $K(S, 2)$ with respect to the Δ_j, then for each i, by (3.9) we have:

$$\begin{array}{rclcrcl} \alpha_{\mathfrak{p}_i}(\Delta_b) & = & [\Delta_b \mid \mathfrak{p}_i] & \qquad & \alpha_{\mathfrak{p}_i}(\Delta_c) & = & [\Delta_c \mid \mathfrak{p}_i] \\ & = & \chi_b(\mathfrak{p}_i) & & & = & \chi_c(\mathfrak{p}_i) \\ & = & x_i & & & = & y_i \end{array} \tag{4.3}$$

Hence, by Proposition 4.2.2, we have that

$$\begin{aligned} t_1(\mathfrak{p}_i) &= \chi_b(\mathfrak{p}_i)\chi_c(\mathfrak{p}_i) \\ &= x_i y_i \\ &= v_i, \end{aligned} \tag{4.4}$$

where

$$\begin{aligned} \mathbf{v} &= (v_1, ..., v_r) \\ &= (x_1 y_1, ..., x_r y_r) \in \mathbb{F}_2^r. \end{aligned} \tag{4.5}$$

This shows that there is an intrinsic relation between the primes in T_1 and the discriminants Δ_b and Δ_c. In fact we can define

$$\begin{aligned} \psi \colon V \times V \times V^* &\to \mathbb{F}_2 \\ (\Delta, \Delta', \alpha) &\mapsto \alpha(\Delta)\alpha(\Delta') \end{aligned} \tag{4.6}$$

When we fix α, the map ψ becomes a symmetric bilinear function on $V \times V$

$$\begin{aligned} \psi_\alpha \colon V \times V &\to \mathbb{F}_2 \\ (\Delta, \Delta') &\mapsto \alpha(\Delta)\alpha(\Delta') \end{aligned} \tag{4.7}$$

i.e., an element of the space we denoted $\mathrm{Sym}^2(V)^*$ which has dimension $r(r+1)/2$ and basis the functions $x_i y_i$ and $x_i y_j + x_j y_i$ for $i \neq j$.

Definition 4.2.4. *A set T_2 of primes of K not in S is* quadratically independent with respect to S *if $\{\psi_{\alpha_\mathfrak{p}} \mid \mathfrak{p} \in T_2\}$ is a basis for* $\mathrm{Sym}^2(V)^*$.

Remark 4.2.5. *If we fix instead* (Δ, Δ') *in* (4.6) *we obtain a quadratic function*

$$\begin{aligned} \psi_{(\Delta,\Delta')} \colon V^* &\to \mathbb{F}_2 \\ \alpha &\mapsto \alpha(\Delta)\alpha(\Delta'). \end{aligned}$$

Then, one can show that the $\alpha_{\mathfrak{p}}$ *in a quadratically independent set of primes form a* non-quadratic *subset of* V^* *in the sense of Livné given by Definition 2.4.1.*

Observe that the following proposition gives the sufficient conditions to determine if our isogeny graph has width 1 or at least 2.

Proposition 4.2.6.

1. $x_iy_i = x_iy_j + x_jy_i = 0$ *for all* i, j *if and only if either* $\mathbf{x} = \mathbf{0}$ *or* $\mathbf{y} = \mathbf{0}$*,*
2. *if* $\mathbf{x} \neq \mathbf{0}$ *and* $\mathbf{y} \neq \mathbf{0}$ *then* $\mathbf{x}$ *and* $\mathbf{y}$ *are uniquely determined by the values* x_iy_i *and* $x_iy_j + x_jy_i$ *for all* i, j*.*

Proof. Let $\mathbf{v} = (v_i)$ be a vector in V defined by (4.5) and let $\mathbf{W}$ be the skew-symmetric matrix over $\mathbb{F}_2$ defined by $w_{ij} = x_iy_j + x_jy_i$. Then the i-th row of $\mathbf{W}$ is given by

$$\mathbf{w}_i = (w_{ij})_j = y_i\,\mathbf{x} + x_i\,\mathbf{y} \in \{\mathbf{0}, \mathbf{x}, \mathbf{y}, \mathbf{x}+\mathbf{y}\}$$

and we have that

$$\mathbf{w}_i = \begin{cases} \mathbf{0} & \text{if } (x_i, y_i) = (0,0), \\ \mathbf{x} & \text{if } (x_i, y_i) = (0,1), \\ \mathbf{y} & \text{if } (x_i, y_i) = (1,0), \\ \mathbf{x}+\mathbf{y} & \text{if } (x_i, y_i) = (1,1). \end{cases} \tag{4.8}$$

The proof follows from the following observations:

(a) if $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$ then $\mathbf{v} = \mathbf{0}$ and $\mathbf{W} = \mathbf{0}$,

(b) if $\mathbf{x} = \mathbf{y} \neq \mathbf{0}$ then $\mathbf{v} = \mathbf{x} = \mathbf{y} \neq \mathbf{0}$ and $\mathbf{W} = \mathbf{0}$,

(c) if $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$ then $\mathbf{W} \neq \mathbf{0}$. Moreover,

- $i)$ if $\mathbf{v} \neq \mathbf{0}$ then the rows of $\mathbf{W}$ for which $v_i = 1$ are $\mathbf{x}+\mathbf{y}$ and the remaining rows are either $\mathbf{x}$ or $\mathbf{y}$ or both,
- $ii)$ if $\mathbf{v} = \mathbf{0}$ then the non-zero rows of $\mathbf{W}$ are all $\mathbf{x}$ and $\mathbf{y}$.

□

The way we apply the previous proposition is the following: for each unordered pair $\{i, j\}$ with $i \neq j$, recall that let $\mathfrak{p}_{ij} \notin S$ denotes a prime inert in both $K(\sqrt{\Delta_i})$ and

$K(\sqrt{\Delta_j})$ but split in all $K(\sqrt{\Delta_k})$ for $1 \leq k \leq r$ with $k \notin \{i, j\}$. Then, for any Δ and by (3.9) we have that

$$\alpha_{\mathfrak{p}_{ij}}(\Delta) = \alpha_{\mathfrak{p}_i}(\Delta) + \alpha_{\mathfrak{p}_j}(\Delta)$$

from where we get that

$$\begin{aligned} \alpha_{\mathfrak{p}_{ij}}(\Delta_b) &= \chi_b(\mathfrak{p}_{ij}) & \qquad \alpha_{\mathfrak{p}_{ij}}(\Delta_c) &= \chi_c(\mathfrak{p}_{ij}) \\ &= x_i + x_j & &= y_i + y_j. \end{aligned}$$

Hence the values

$$\begin{aligned} t_1(\mathfrak{p}_{ij}) &= \chi_b(\mathfrak{p}_{ij})\chi_c(\mathfrak{p}_{ij}) \\ &= (x_i + x_j)(y_i + y_j) \end{aligned}$$

are used to compute

$$\begin{aligned} w_{ij} &= x_i y_j + y_i x_j \\ &= t_1(\mathfrak{p}_{ij}) - t_1(\mathfrak{p}_i) - t_1(\mathfrak{p}_j), \quad i \neq j \geq 1. \end{aligned} \tag{4.9}$$

From these we may determine, using Proposition 4.2.6, whether either

(a) $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$, then either Δ_b or Δ_c is trivial and the isogeny class is “large”, or

(b) $\mathbf{x}$ and $\mathbf{y}$ are both non-zero, then the unordered pair $\{\mathbf{x}, \mathbf{y}\}$ is uniquely determined, so the pair $\{\Delta_b, \Delta_c\}$ is then determined and the isogeny class is “small”.

In practice this process might not be efficient since we may need to test many primes $\mathfrak{p}$ before finding the set of primes of the form $\{\mathfrak{p}_{ij}\}$ and the resulting primes are likely to be large. Moreover, in applications it may be computationally expensive to compute the trace of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ for primes $\mathfrak{p}$ of large norm. For example, this is the case for a Galois representation attached to a Bianchi modular form.

Nevertheless, it is possible to improve the way of finding the “test” primes to thereby have an efficient set of primes for which, by computing (4.2) for each prime in the set, will be possible to recover $\{\mathbf{x}, \mathbf{y}\}$ or prove that at least one vector is the zero vector.

In order to do this, let $\mathfrak{p} \notin S$ be a prime, let $\Delta \in K(S, 2)$ and consider the subset $I \subseteq \{1, \ldots, r\}$ given by

$$I(\mathfrak{p}) = \{i : [\Delta_i \mid \mathfrak{p}] = 1\}. \tag{4.10}$$

In the notation of Chapter 3, $\mathfrak{p}_I$ denotes any prime such that $I(\mathfrak{p}_I) = I$. Then, as we saw in (3.9), we have that

$$\alpha_{\mathfrak{p}_I}(\Delta) = \sum_{i\in I} \alpha_{\mathfrak{p}_i}(\Delta),$$

moreover, we get that

$$\begin{array}{rclcrcl} \chi_b(\mathfrak{p}_I) & = & \sum_{i\in I} x_i & \quad & \chi_c(\mathfrak{p}_I) & = & \sum_{i\in I} y_i \\ & =: & x_I & & & =: & y_I \end{array}$$

say, and

$$t_1(\mathfrak{p}_I) = x_I y_I$$

where $x_I y_I$ is the sum of terms $x_i y_i$ and $x_i y_j + x_j y_i$ for $i \in I$ and $\{i, j\} \subseteq I$.

Now we loop through the primes $\mathfrak{p}$ not in S to construct a matrix $\mathbf{A}$ whose columns are indexed by the subsets of $\{1, 2, ..., r\}$ of size 1 and 2, i.e., the sets $\{i\}$ for $1 \le i \le r$ and $\{i, j\}$ for $1 \le i < j \le r$, initially with 0 rows and, a column vector $\mathbf{b}$, initially of size 0. For each prime $\mathfrak{p}$ we compute $I(\mathfrak{p})$ and set $\mathbf{v}(\mathfrak{p})$ in $\mathbb{F}_2^{\frac{r(r+1)}{2}}$ by

$$\mathbf{v}(\mathfrak{p}) = \begin{cases} 1 & \text{in position } i \text{ if } i \in I(\mathfrak{p}) \\ 1 & \text{in position } \{i,j\} \text{ if } \{i,j\} \subseteq I(\mathfrak{p}) \\ 0 & \text{else.} \end{cases} \tag{4.11}$$

We add $\mathbf{v}(\mathfrak{p})$ as a new row of $\mathbf{A}$ and $t_1(\mathfrak{p})$ as a new entry in $\mathbf{b}$, provided that this increases the rank of $\mathbf{A}$ and we stop when the rank of $\mathbf{A}$ is $r(r+1)/2$. We also construct the matrix $\mathbf{P}$ of size $r(r+1)/2$ whose rows and columns are indexed as the columns of $\mathbf{A}$ as follows: for the first r rows a 1 is added to the column whose index is $\{i\}$ and for the last $r(r-1)/2$ rows a 1 is added to the columns whose index is a subset of $\{i, j\}$.

Finally, the entries of $\mathbf{P}^{-1}\,\mathbf{A}\,\mathbf{b}$ give the values of $t_1(\mathfrak{p}_i), t_1(\mathfrak{p}_{ij})$ and, using (4.4), (4.9) and Proposition 4.2.6 we recover the vectors $\mathbf{x}$, $\mathbf{y}$ and Δ_b, Δ_c.

Conclusion.

Let T_2 be a quadratically independent set of primes and for each prime $\mathfrak{p}$ in T_2 apply the test function t_1 given by (4.2). Then we have either that

- $t_1(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_2$, then $t_1(\mathfrak{p}) = 0$ for all $\mathfrak{p}$ and by Proposition 4.2.6 we have that $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$, which implies that the isogeny class is “large”, or
- $t_1(\mathfrak{p}) = 1$ for at least one $\mathfrak{p} \in T_2$, then the isogeny class is “small”. Moreover using Proposition 4.2.6 we can recover $\mathbf{x}$, $\mathbf{y}$ and hence we obtain Δ_b and Δ_c.

Observe that a set T_2 of quadratically independent primes $\mathfrak{p}$ for which we need to evaluate $t_1(\mathfrak{p})$ depends only on the original finite set S of primes, so the set T_2 may be determined once and for all if several Black Boxes are to be considered with the same set S of primes.

Algorithms.

Algorithm 5: This function determines a quadratically independent set T_2 of primes of K.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
Output: A finite quadratically independent set $T_2$ of primes of $K$.
Compute a basis $\{\Delta_i\}_{i=1}^r$ for $K(S,2)$;
$T_2 := \{\}$;
$\mathbf{A} :=$ a $0 \times \frac{r(r+1)}{2}$ matrix over $\mathbb{F}_2$;
while $\mathbf{A}$ has $< r(r+1)/2$ rows do
    Take $\mathfrak{p} \notin S \cup T_2$;
    Compute $I(\mathfrak{p})$ given by (4.10);
    Compute $\mathbf{v}(\mathfrak{p})$ given by (4.11);
    Set $\mathbf{A}' := \mathbf{A} + \mathbf{v}(\mathfrak{p})$ # i.e., adjoin $\mathbf{v}(\mathfrak{p})$ as a new row of $\mathbf{A}$;
    if *If* rank($\mathbf{A}'$) >rank($\mathbf{A}$) then
        $\mathbf{A} := \mathbf{A}'$;
        $T_2 := T_2 \cup \{\mathfrak{p}\}$.
```

To simplify the exposition of the algorithm which follows, using such sets T_2, we will always assume that the set T_2 has a special form, where $\#I(\mathfrak{p}) = 1$ or 2 for all $\mathfrak{p} \in T_2$:

$$T_2 = \{\mathfrak{p}_i | 1 \leq i \leq r\} \cup \{\mathfrak{p}_{ij} | 1 \leq i < j \leq r\}, \tag{4.12}$$

where $I(\mathfrak{p}_i) = \{i\}$ and $I(\mathfrak{p}_{ij}) = \{i, j\}$. For completeness we provide a special version of Algorithm 5 whose output is such an indexed set.

Algorithm 6: This function determines a quadratically independent set T_2 of primes as in (4.12).

```
Input  : A number field $K$.
         A set $S$ of primes of $K$.
Output: An indexed quadratically independent set $T_2$ of primes as in (4.12).
Set a list $A := \{\}$; % singletons
Set a list $B := \{\}$; % doubletons
while $\#(A \cup B) < r(r+1)/2$ do
    Take $\mathfrak{p} \notin S \cup T_2$;
    Compute $I = I(\mathfrak{p})$ using (4.10);
    if $\#I = 1$ with $I = \{i\}$ then
        if $i \notin A$ then
            Set $\mathfrak{p}_i := \mathfrak{p}$;
            $A := A \cup \{i\}$;
            $T_2 := T_2 \cup \{\mathfrak{p}_i\}$.
    if $\#I = 2$ with $I = \{i, j\}$ and $i < j$ then
        if $(i, j) \notin B$ then
            Set $\mathfrak{p}_{ij} := \mathfrak{p}$;
            $B := B \cup \{(i, j)\}$;
            $T_2 := T_2 \cup \{\mathfrak{p}_{ij}\}$.
Return: $T_2$.
```

Finally we present the algorithm to determine whether, for a given 2-adic Galois representation ρ unramified outside S, the stable Bruhat-Tits tree of ρ has width 1 or at least 2.

Algorithm 7: This function determines whether the stable Bruhat-Tits tree of ρ has width exactly 1 or at least 2.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
         A Black Box Galois representation unramified outside $S$ whose
         residual image is reducible.
Output: If width =1 return: True, $\{\prod_{i=1}^{r} \Delta_i^{x_i}, \prod_{i=1}^{r} \Delta_i^{y_i}\}$.
         If width $\geq 2$ return: False.
Use Algorithm 6 to compute a quadratically independent set $T_2$;
Compute $\mathbf{b} = (t_1(\mathfrak{p}_1), ..., t_1(\mathfrak{p}_{\frac{r(r+1)}{2}}))$ for $\mathfrak{p}_i \in T_2$;
if $\mathbf{b} \neq \mathbf{0}$ then
    Compute $\mathbf{v} = (t_1(\mathfrak{p}_1), ..., t_1(\mathfrak{p}_r)) \in \mathbb{F}_2^r$;
    Compute $\mathbf{W} = (t_1(\mathfrak{p}_{ij}) - t_1(\mathfrak{p}_i) - t_1(\mathfrak{p}_j)) \in M_r(\mathbb{F}_2)$;
    if $\mathbf{W} = \mathbf{0}$ then
        Take $\mathbf{x} = \mathbf{y} = \mathbf{v}$.
    else
        if $\mathbf{v} = \mathbf{0}$ then
            Take $\mathbf{x}$ and $\mathbf{y}$ to be two distinct non-zero rows of $\mathbf{W}$.
        else
            Let $\mathbf{z}$ be a row $i$ of $\mathbf{W}$ such that $\mathbf{w}_i \neq \mathbf{0}$;
            Let $\mathbf{x}$ be any non-zero row of $\mathbf{W}$ distinct from $\mathbf{z}$;
            Let $\mathbf{y} = \mathbf{x} + \mathbf{z}$.
    Return: True, $\{\prod_{i=1}^{r} \Delta_i^{x_i}, \prod_{i=1}^{r} \Delta_i^{y_i}\}$.
else
    Return: False.
```

Example 5. *Let $K = \mathbb{Q}(a)$ with $a = \sqrt{-2}$ and let $S = \{a, a-1, a-3\}$ be the set of bad primes. Observe that for these K and S we have*

$$\begin{aligned} K(S,2) &= \langle a, -1+a, -3+a, -1 \rangle \\ &\cong (\mathbb{Z}/2\mathbb{Z})^4. \end{aligned}$$

Consider

$$K_1 = K(\sqrt{\Delta_1}) \qquad K_2 = K(\sqrt{\Delta_2}) \qquad K_3 = K(\sqrt{\Delta_3}) \qquad K_4 = K(\sqrt{\Delta_4})$$

where

$$\Delta_1 = a \qquad \Delta_2 = -1+a \qquad \Delta_3 = -3+a \qquad \Delta_4 = -1,$$

and take the set of primes

$$T_2 = \{37, 7, 23, -5+3a, 5, 13, -3-5a, 31, -11-3a, 1+3a\}.$$

We can see that T_2 *is a quadratically independent set of primes satisfying the special conditions of Algorithm 6, i.e., we have that*

	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
37	1	0	0	0	0	0	0	0	0	0
7	0	1	0	0	0	0	0	0	0	0
23	0	0	1	0	0	0	0	0	0	0
$-5+3a$	0	0	0	1	0	0	0	0	0	0
5	1	1	0	0	1	0	0	0	0	0
13	1	0	1	0	0	1	0	0	0	0
$-3-5a$	1	0	0	1	0	0	1	0	0	0
31	0	1	1	0	0	0	0	1	0	0
$-11-3a$	0	1	0	1	0	0	0	0	1	0
$1+3a$	0	0	1	1	0	0	0	0	0	1

Therefore we have found a correct set of primes to determine whether the isogeny class is "small" or "large". The Black Box that is considered here comes from the Galois representation of a Bianchi modular form[I] *of level* $2+17\sqrt{-2}$ *whose Hecke eigenvalues give the traces. In this way, applying the test (4.2) on* T_2 *we get that*

$$\mathbf{b} = \begin{pmatrix} t_1(37) \\ t_1(7) \\ t_1(23) \\ t_1(-5+3a) \\ t_1(5) \\ t_1(13) \\ t_1(-5-5a) \\ t_1(31) \\ t_1(-11-3a) \\ t_1(1+3a) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

According to Algorithm 7, since $\mathbf{b} \neq \mathbf{0}$*, we are in the "small isogeny class". This implies that the width of the related stable Bruhat-Tits tree is* 1*. Moreover, the vector* $\mathbf{v}$ *is* $\mathbf{0}$*, which implies that the vector* $\mathbf{x}$ *and* $\mathbf{y}$ *are given by the non-zero rows of the matrix* $\mathbf{W}$*.*

[I] The Bianchi modular form's label is "[528,32,4].a" and was taken from http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/iqfdata/data/nflist.2.1-10000 on March 2016.

To determine the vectors $\mathbf{x}$ *and* $\mathbf{y}$ *we construct the matrix* $\mathbf{W}$ *given by*

$$\begin{aligned}\mathbf{W} &= \begin{pmatrix} 0 & x_1y_2+x_2y_1 & x_1y_3+x_3y_1 & x_1y_4+x_4y_1 \\ x_1y_2+x_2y_1 & 0 & x_2y_3+x_3y_2 & x_2y_4+x_4y_2 \\ x_1y_3+x_3y_1 & x_2y_3+x_3y_2 & 0 & x_3y_4+x_4y_3 \\ x_1y_4+x_4y_1 & x_2y_4+x_4y_2 & x_3y_4+x_4y_3 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\end{aligned}$$

from where we can see, without loss of generality, that $\mathbf{x} = (0,1,1,0)$ *and* $\mathbf{y} = (1,0,0,0)$*. Thus, the discriminants related to these vectors are*

$$\begin{aligned}\Delta_b &= \Delta_1^0\Delta_2^1\Delta_3^1\Delta_4^0 \\ &= (-1+a)(-3+a) \\ &= 1-4a\end{aligned}$$

and

$$\begin{aligned}\Delta_c &= \Delta_1^1\Delta_2^0\Delta_3^0\Delta_4^0 \\ &= a.\end{aligned}$$

Furthermore, the quadratic fields are

$$K(\sqrt{1-4a}) \text{ and } K(\sqrt{a}).$$

We can match the data presented in the previous example to the 2*-isogeny class*[II] *of the elliptic curves of conductor* $N = 528a$ *over* $\mathbb{Q}(\sqrt{-2})$ *given by the Weierstrass equation* $y^2 + axy + ay = x^3 + (-1+8a)x + (2+12a)$*.*

Up to this point we have seen how to determine whether the width of the stable Bruhat-Tits tree is 1 ("small isogeny class", i.e., none of the residual images is C_1) or at least 2 ("large isogeny class", i.e., at least one residual image is C_1). So for the rest of the chapter we will study in more detail the "large isogeny class" case, i.e., without loss of generality we may always assume that representation is trivial modulo 2.

By the end of this chapter we will have developed techniques and algorithms to determine whether the representation is trivial modulo 2^{k+1} under the assumption that the representation is trivial modulo 2^k. Moreover we will be able to determine, for small k, the width, the edges and the nodes of the stable Bruhat-Tits tree related

[II] Taken from http://www.lmfdb.org/EllipticCurve/2.0.8.1/%5B528%2C32%2C4%5D/a/ on March 2016.

to the representation modulo 2^{k+1}. Particularly, we will see in examples 6 and 7, how this technique is applied to determine the triviality of the representation modulo 2^2 and also distinguish whether the width of the stable Bruhat-Tits tree is exactly 2, 3 or at least 4 and its respective edges.

4.3 Large Isogeny Class of width at least 2.

Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a continuous Galois representation unramified outside a set of primes S and let Λ be the lattice for which it is defined. We start this section with the following lemma.

Lemma 4.3.1. *Suppose that* $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ *for all* $\sigma \in G_K$ *and some positive integer* k. *Then*

1. $\det(\rho(\sigma)) \equiv 1 \pmod{2^k}$,
2. $v(\sigma) \geq 2k$.

Proof.

1. Straightforward.
2. Let $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$, so we have

$$\rho(\sigma) = \mathbf{I} + 2^k\mu(\sigma), \tag{4.13}$$

where

$$\mu(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \in M_2(\mathbb{Z}_2).$$

Thus we have

$$\begin{aligned} 1 - \mathrm{tr}(\rho(\sigma)) + \det(\rho(\sigma)) &= \det(\rho(\sigma) - \mathbf{I}) \\ &= 2^{2k}ad - 2^{2k}bc, \end{aligned} \tag{4.14}$$

which means that $F_\sigma(1)$ is divisible by 2^{2k} and that $v(\sigma) \geq 2k$ for all $\sigma \in G_k$.

□

Suppose that $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ for all $\sigma \in G_K$ and some positive integer k. Then

$$\begin{aligned} \det(\rho(\sigma)) &= 1 + 2^k(a+d) + 2^{2k}ad - 2^{2k}bc \\ &\equiv 1 + 2^k(a+d) \pmod{2^{k+1}} \\ &\equiv \begin{cases} 1 & \pmod{2^{k+1}} \quad \text{if } a+d \text{ is even} \\ 1+2^k & \pmod{2^{k+1}} \quad \text{if } a+d \text{ is odd.} \end{cases} \end{aligned} \tag{4.15}$$

Note that the map $\sigma \mapsto \mu(\sigma) \pmod 2$ is a group homomorphism from G_K to $M_2(\mathbb{F}_2)$. Composing the homomorphism with the four characters from

$$\begin{aligned} M_2(\mathbb{F}_2) &\to \mathbb{F}_2 \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto a, b, c, d \end{aligned}$$

we obtain four additive characters unramified outside S

$$\begin{aligned} &G_K \to \mathbb{F}_2 \\ &\quad \sigma \mapsto a(\sigma), b(\sigma), c(\sigma), d(\sigma) \pmod 2 \end{aligned}$$

which we denote by χ_a, χ_b, χ_c and χ_d. To each character there is associated a discriminant, named $\Delta_a, \Delta_b, \Delta_c, \Delta_d \in K(S, 2)$. Setting $\chi_{abcd} = \chi_a + \chi_b + \chi_c + \chi_d$, $\chi_{\det} = \chi_a + \chi_d$ and using (4.15) we see that

$$\begin{aligned} \chi_{\det}(\sigma) = 1 &\Leftrightarrow a + d \equiv 1 \pmod 2 \\ &\Leftrightarrow \det(\rho(\sigma)) \equiv 1 + 2^k \pmod {2^{k+1}} \end{aligned}$$

and

$$\begin{aligned} \chi_{\det}(\sigma) = 0 &\Leftrightarrow a + d \equiv 0 \pmod 2 \\ &\Leftrightarrow \det(\rho(\sigma)) \equiv 1 \pmod {2^{k+1}}, \end{aligned}$$

so therefore $\chi_{\det}$ is the quadratic character associated to (4.15). Observe we obtain naturally that

$$\Delta_{\det} = \Delta_a \Delta_d \tag{4.16}$$

is the discriminant of $\chi_{\det}$.

From now on we will always assume that the representation ρ is always trivial modulo 2^k and hence satisfies Lemma 4.3.1.

Remark 4.3.2. *Since we are working with integral Galois representations, we also can work with their isogenies. In fact, in sections 4.3.3 and 4.3.4, we may choose to do one of the following adjustments to the given matrix representation:*

(1) *replace $\rho(\sigma)$ by $\mathbf{U}\,\rho(\sigma)\,\mathbf{U}^{-1}$ with $\mathbf{U} \in \mathrm{GL}_2(\mathbb{Z}_2)$. This means that we are taking a new $\mathbb{Z}_2$-basis for the same stable lattice, replacing $\rho(\sigma)$ by a new representation isomorphic(over $\mathbb{Z}_2$) to it.*

(2) *replace $\rho(\sigma)$ by $\mathbf{U}\,\rho(\sigma)\,\mathbf{U}^{-1}$ with $\mathbf{U} \in \mathrm{GL}_2(\mathbb{Q}_2)$ and $\det(\mathbf{U}) = 2$, such that this conjugation give us new values that are still integral. This means that we are*

replacing our stable lattice Λ by one adjacent to it in the stable Bruhat-Tits tree, namely $\mathbf{U}(\Lambda)$, and replacing ρ by an isogenous(over $\mathbb{Q}_2$) representation to it.

4.3.1 Bruhat-Tits tree of width at least 2: Large Isogeny class.

Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a Galois representation unramified outside a set of primes S such that $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ for all $\sigma \in G_K$. When $k=1$, this means that we are in the "large isogeny class" case, i.e., the width of the stable Bruhat-Tits tree is at least 2.

We would like to determine the shape and the corresponding quadratic characters associated to the nodes of the stable Bruhat-Tits tree related to the representation ρ which has the matrix representation given by (4.13). To do this, we have to focus on the cocyclic sublattices(see Definition 2.2.5) Λ' of $\Lambda = \mathbb{Z}_2^2$ of index 2^{k+1} that are fixed by ρ, this is because these cocyclic sublattices correspond to paths of length $k+1$ in the tree starting at the vertex Λ. These cocyclic sublattices are given by

$$\Lambda' = \langle \mathbf{v} \rangle + 2^{k+1}\Lambda, \quad \mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}_2^2$$

where x, y are not both even. So Λ' is fixed by ρ if and only if for all $\sigma \in G_K$

$$\begin{aligned} \rho(\sigma)\Lambda' \equiv \Lambda' \pmod{2^{k+1}} &\Leftrightarrow \rho(\sigma)\,\mathbf{v} \equiv \lambda\,\mathbf{v} \pmod{2^{k+1}} \\ &\Leftrightarrow (\mathbf{I} + 2^k\mu(\sigma))\,\mathbf{v} \equiv \lambda\,\mathbf{v} \pmod{2^{k+1}} \\ &\quad\ \text{for some } \lambda \in \{1, 1+2^k\} \end{aligned}$$

from where we have the two following cases:

(a) if $\lambda = 1$ then

$$\begin{aligned} (\mathbf{I} + 2^k\mu(\sigma))\,\mathbf{v} \equiv \mathbf{v} \pmod{2^{k+1}} &\Rightarrow 2^k\mu(\sigma)\,\mathbf{v} \equiv \mathbf{0} \pmod{2^{k+1}} \\ &\Rightarrow \mu(\sigma)\,\mathbf{v} \equiv \mathbf{0} \pmod{2}, \end{aligned} \tag{4.17}$$

(b) if $\lambda = 1 + 2^k$ then

$$\begin{aligned} (\mathbf{I} + 2^k\mu(\sigma))\,\mathbf{v} \equiv (1+2^k)\,\mathbf{v} \pmod{2^{k+1}} &\Rightarrow 2^k(\mathbf{I} + \mu(\sigma))\,\mathbf{v} \equiv \mathbf{0} \pmod{2^{k+1}} \\ &\Rightarrow (\mathbf{I} + \mu(\sigma))\,\mathbf{v} \equiv \mathbf{0} \pmod{2}. \end{aligned} \tag{4.18}$$

Hence we can determine the condition for each possible lattice Λ' to be stable under ρ, which only depends on $\mathbf{v}$ modulo 2:

1. $\mathbf{v} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{2}$ and for one of these two cases (4.17) or (4.18) to hold is

equivalent to say that

$$c(\sigma) \equiv 0 \pmod 2, \quad \forall \sigma \in G_K,$$

2. $\mathbf{v} \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \pmod 2$ and for one of these two cases (4.17) or (4.18) to hold is equivalent to say that

$$b(\sigma) \equiv 0 \pmod 2, \quad \forall \sigma \in G_K,$$

3. $\mathbf{v} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod 2$ and

   (i) for (4.17) we have that

$$\rho(\sigma)\begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod 2 \Leftrightarrow \begin{pmatrix} a+b \\ c+d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod 2$$

   (ii) for (4.18) we have that

$$\rho(\sigma)\begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod 2 \Leftrightarrow \begin{pmatrix} a+b \\ c+d \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod 2.$$

   Hence, in order to either (4.17) or (4.18) to hold we must have

$$a+b+c+d \equiv 0 \pmod 2 \quad \forall \sigma \in G_K.$$

For example, when $k = 1$, the generic stable Bruhat-Tits tree of width at least 2 looks like

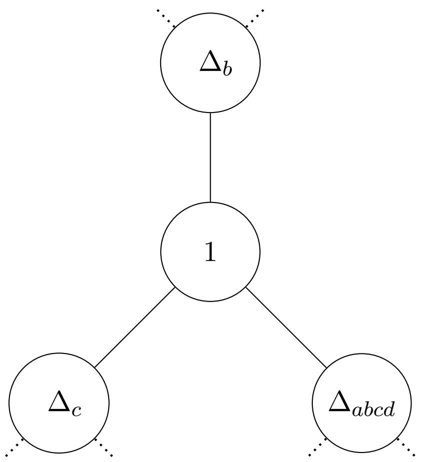


Figure A1: Tree of width at least 2.

where the quadratic characters and their quadratic extensions related to the four nodes of the tree are

1. $\chi_b \colon \sigma \mapsto b \pmod 2$ is the quadratic character associated to $K(\sqrt{\Delta_b})/K$,
2. $\chi_c \colon \sigma \mapsto c \pmod 2$ is the quadratic character associated to $K(\sqrt{\Delta_c})/K$,
3. $\chi_{\det} \colon \sigma \mapsto a + d \pmod 2$ is the character associated to $K(\sqrt{\Delta_{\det}})/K$,
4. $\chi_{abcd} \colon \sigma \mapsto a + b + c + d \pmod 2$ is the quadratic character associated to $K(\sqrt{\Delta_{abcd}})/K$.

Observe that the condition of the width being at least 3 is equivalent to have one of these sublattices itself having a stable sublattice of index 2. This occurs if and only if one (or more) of the characters $\chi_b, \chi_c, \chi_{abcd}$ is trivial.

Finally we ask ourselves, how can we determine the values of Δ_a, Δ_b, Δ_c, Δ_d and Δ_{abcd}? This question will be answered in the following sections.

Remark 4.3.3. *We can see how the conjugation by* $\mathbf{U}$*, for the matrices* $\mathbf{U}$ *given in Remark 4.3.2, swaps the characters* χ_a*,* χ_b*,* χ_c*,* χ_d*:*

(1) *when* $\mathbf{U} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ *then, by conjugation, we have that*

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\to \begin{pmatrix} b+d & (b+d)-(a+c) \\ -b & a-b \end{pmatrix} \\ &\to \begin{pmatrix} c+d & -c \\ (a+c)-(b+d) & a+c \end{pmatrix} \\ &\to \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \end{aligned}$$

where we can see how the triplet $(b, c, a+b+c+d)$ *gets* 3*-cycled as*

$$\begin{aligned} (b, c, a+b+c+d) &\to (a+b+c+d, b, c) \\ &\to (c, a+b+c+d, b) \\ &\to (b, c, a+b+c+d). \end{aligned}$$

(2) *when* $\mathbf{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$*, then by conjugation we have that*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

where we can see how the triplet $(b, c, a+b+c+d)$ *get* 2*-cycled as*

$$(b, c, a+b+c+d) \leftrightarrow (c, b, a+b+c+d)$$

In sections 4.3.3 and 4.3.4 we will see how this remark is important.

4.3.2 The test.

Let $\{\Delta_i\}_{i=1}^{r}$ be a fixed basis of $K(S, 2)$ and take

$$\Delta_b = \prod_{i=1}^{r} \Delta_i^{x_i}, \qquad \Delta_c = \prod_{i=1}^{r} \Delta_i^{y_i}, \qquad \Delta_{abcd} = \prod_{i=1}^{r} \Delta_i^{z_i},$$

$$\Delta_a = \prod_{i=1}^{r} \Delta_i^{u_i}, \qquad \Delta_d = \prod_{i=1}^{r} \Delta_i^{v_i},$$

where

$$\mathbf{x} = \{x_i\}_{i=1}^{r}, \mathbf{y} = \{y_i\}_{i=1}^{r}, \mathbf{z} = \{z_i\}_{i=1}^{r}, \mathbf{u} = \{u_i\}_{i=1}^{r}, \mathbf{v} = \{v_i\}_{i=1}^{r} \in \mathbb{F}_2^r.$$

Since we are assuming that ρ is trivial modulo 2^k, to determine the ρ modulo 2^{k+1}, it is enough to determine the four discriminants Δ_a, Δ_b, Δ_c and Δ_d. As a special case, when $k = 1$, we will be able to determine whether the stable Bruhat-Tits tree has width exactly 2, 3, or at least 4, given that it has width at least 2.

Now consider a quadratically independent set T_2 of primes. Then for the primes $\mathfrak{p} \in T_2$, due to (4.15), we get two test functions.

1. If $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod{2^{k+1}}$ then

   $$a + d \equiv 0 \pmod 2$$

   and in this situation we have that

   $$t_{2k}(\mathfrak{p}) := \frac{1}{2^{2k}}(1 - \mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) + \det(\rho(\mathrm{Frob}_{\mathfrak{p}}))) \equiv a + bc \pmod 2. \tag{4.19}$$

2. If $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 + 2^k \pmod{2^{k+1}}$ then

   $$a + d \equiv 1 \pmod 2$$

   and in this situation we have that

   $$t_{2k}(\mathfrak{p}) := \frac{1}{2^{2k}}(1 - \mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) + \det(\rho(\mathrm{Frob}_{\mathfrak{p}}))) \equiv bc \pmod 2. \tag{4.20}$$

Observe that we will be always able to distinguish between (4.19) and (4.20) because

$$\operatorname{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) = 2 + 2^k(a+d) \tag{4.21}$$

for any prime $\mathfrak{p} = \mathrm{Frob}_{\mathfrak{p}}$ in G_K.

4.3.3 $\Delta_{\det}$ trivial.

Suppose that $\Delta_{\det}$ is trivial. Since $\Delta_{\det} = \Delta_a\Delta_d$ this implies that $\Delta_a = \Delta_d$. Thus the vectors $\mathbf{u}$ and $\mathbf{v}$ are the same. Moreover,

$$\Delta_{abcd} = \Delta_b\Delta_c, \tag{4.22}$$

with $\mathbf{z} = \mathbf{x}+\mathbf{y}$. In this way,

$$\mathbf{x}+\mathbf{y}+\mathbf{z} = \mathbf{0}\,. \tag{4.23}$$

To determine the values of the discriminants take the primes $\mathfrak{p}_i, \mathfrak{p}_j, \mathfrak{p}_{ij} \in T_2$ then, by the test (4.19), we have that

$$\begin{aligned} t_{2k}(\mathfrak{p}_i) &= u_i + x_iy_i, \quad i \geq 1, \\ t_{2k}(\mathfrak{p}_j) &= u_j + x_jy_j, \quad j \geq 1, \\ t_{2k}(\mathfrak{p}_{ij}) &= u_i + u_j + (x_i+x_j)(y_i+y_j), \quad i,j \geq 1. \end{aligned} \tag{4.24}$$

Hence

$$\begin{aligned} w_{ij} &= x_iy_j + x_jy_i \\ &= t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_j) + t_{2k}(\mathfrak{p}_{ij}), \quad i,j \geq 1. \end{aligned} \tag{4.25}$$

We construct the matrix $\mathbf{W}$ with the entries w_{ij} given by (4.25). As before, the i-th row (and column) are given by $\mathbf{w}_i = (w_{ij})_j = y_i\,\mathbf{x} + x_i\,\mathbf{y} \in \{\mathbf{0}, \mathbf{x}, \mathbf{y}, \mathbf{z} = \mathbf{x}+\mathbf{y}\}$, thus

$$\mathbf{w}_i = \begin{cases} \mathbf{0} & \text{if } (x_i, y_i) = (0,0), \\ \mathbf{x} & \text{if } (x_i, y_i) = (0,1), \\ \mathbf{y} & \text{if } (x_i, y_i) = (1,0), \\ \mathbf{z} = \mathbf{x}+\mathbf{y} & \text{if } (x_i, y_i) = (1,1), \end{cases} \tag{4.26}$$

and two cases arise.

Case 1. The matrix $\mathbf{W}$ contains at least two (distinct) non-zero rows. We retrieve the values of $\mathbf{x}$ and $\mathbf{y}$ from the matrix $\mathbf{W}$ and by (4.23) we also obtain the value of

$\mathbf{z}$. Moreover, we obtain the values of $\mathbf{u} = \mathbf{v}$ by using

$$t_{2k}(\mathfrak{p}_i) = u_i + x_i y_i, \quad 1 \leq i \leq r \tag{4.27}$$

and the now known values of $\mathbf{x}$ and $\mathbf{y}$. Therefore we have computed the all the vectors $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and obtained $\Delta_a, \Delta_b, \Delta_c, \Delta_d$ and Δ_{abcd}.

Case 2. The matrix $\mathbf{W}$ is the zero matrix. In this case we have either that $\mathbf{x} = \mathbf{y}$ (which implies that $\mathbf{z} = \mathbf{0}$) or that $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$ and $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. In both cases, by remarks 4.3.2 and 4.3.3, we have complete symmetry between $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$, so we can safely assume that $\mathbf{y} = \mathbf{0}$ and thus $\mathbf{x} = \mathbf{z}$.

Observe that we do not know the values of $\mathbf{x}$ and $\mathbf{z}$ yet, but since $x_i y_i = 0$ for $1 \leq i \leq r$, we can retrieve the values of $\mathbf{u} = \mathbf{v}$ using (4.27).

Now, to obtain the discriminant Δ_b we need to go a step further and think on the test $t_{2k+1}(\mathfrak{p})$ for $\mathfrak{p} \in T_2$.

Recalling (4.13) we observe that, because $\mathbf{y} = \mathbf{0}$, the entry c is always even, i.e., $c = 2c_1$. This means that we can re-write (4.13) to obtain

$$\rho(\sigma) = \begin{pmatrix} 1 + 2^k a & 2^k b \\ 2^{k+1} c_1 & 1 + 2^k d \end{pmatrix} \tag{4.28}$$

then, for $\mathfrak{p} \in T_2$ we have that

$$F_{\mathfrak{p}}(1) = 2^{2k}(ad - 2bc_1). \tag{4.29}$$

By this stage we have obtained the vector $\mathbf{u} = \mathbf{v}$. Moreover, we know that $\Delta_a = \Delta_d$ and because of this, every time we take a prime $\mathfrak{p}$ we will know exactly in which of the two following cases we are:

1. Take $\mathfrak{p} \in T_2$ such that $a \equiv d \equiv 0 \pmod 2$. Then $a = 2a_1$ and $d = 2d_1$ so (4.29) becomes

$$\begin{aligned} F_{\mathfrak{p}}(1) &= 2^{2k}(ad - 2bc_1) \\ &= 2^{2k}(4a_1 d_1 - 2bc_1) \\ &= 2^{2k+1}(2a_1 d_1 - bc_1) \end{aligned}$$

   so

$$t_{2k+1}(\mathfrak{p}) := \frac{F_{\mathfrak{p}}(1)}{2^{2k+1}} \equiv bc_1 \pmod 2. \tag{4.30}$$

2. Take $\mathfrak{p} \in T_2$ such that $a \equiv d \equiv 1 \pmod 2$. By analysing (4.21) we obtain two cases.

(*i*) $a + d \equiv 0 \pmod 4$. Then $ad \equiv -1 \pmod 4$, so $ad = -1 + 4s_1$ and (4.29) becomes

$$\begin{aligned} F_{\mathfrak{p}}(1) &= 2^{2k}(ad - 2bc_1) \\ &= 2^{2k}(-1 + 4s_1 - 2bc_1) \\ &= -2^{2k} + 2^{2k+1}(2s - bc_1) \end{aligned}$$

so

$$t_{2k+1}(\mathfrak{p}) := \frac{F_{\mathfrak{p}}(1) + 2^{2k}}{2^{2k+1}} \equiv bc_1 \pmod 2. \tag{4.31}$$

(*ii*) $a+d \equiv 2 \pmod 4$. Then $ad \equiv 1 \pmod 4$, $ad = 1+4s_2$ and (4.29) becomes

$$\begin{aligned} F_{\mathfrak{p}}(1) &= 2^{2k}(ad - 2bc_1) \\ &= 2^{2k}(1 + 4s_2 - 2bc_1) \\ &= 2^{2k} + 2^{2k+1}(2s_2 - bc_1) \end{aligned}$$

so

$$t_{2k+1}(\mathfrak{p}) := \frac{F_{\mathfrak{p}}(1) - 2^{2k}}{2^{2k+1}} \equiv bc_1 \pmod 2. \tag{4.32}$$

It is not hard to see that $\sigma \mapsto c_1(\sigma) \pmod 2$ is again an additive quadratic character unramified outside S, hence has an associated discriminant Δ_{c_1}.

Let Δ_{c_1} be defined as

$$\Delta_{c_1} = \prod_{i=1}^{r} \Delta_i^{m_i}$$

with $\mathbf{m} = \{m_i\}_{i=1}^r \in \mathbb{F}_2^r$. Then just as we did it in Section 4.2.1 using the set of primes T_2 and the tests (4.30), (4.31) and (4.32) we are going to determine whether Δ_b or Δ_{c_1} is trivial.

We construct the matrix $\mathbf{W}$, as before, with entries

$$\begin{aligned} w_{ij} &= x_i m_j + x_j m_i \\ &= t_{2k+1}(\mathfrak{p}_i) + t_{2k+1}(\mathfrak{p}_j) + t_{2k+1}(\mathfrak{p}_{ij}), \quad i, j \geq 1 \end{aligned}$$

and, as before, the rows are given by $\mathbf{w}_i = (w_{ij})_j = m_i\,\mathbf{x} + x_i\,\mathbf{m} \in \{\mathbf{0}, \mathbf{x}, \mathbf{m}, \mathbf{x} + \mathbf{m}\}$ and we have that

$$\mathbf{w}_i = \begin{cases} \mathbf{0} & \text{if } (x_i, m_i) = (0,0), \\ \mathbf{x} & \text{if } (x_i, m_i) = (0,1), \\ \mathbf{m} & \text{if } (x_i, m_i) = (1,0), \\ \mathbf{x}+\mathbf{m} & \text{if } (x_i, m_i) = (1,1). \end{cases} \tag{4.33}$$

Furthermore, let $\mathbf{w}$ be the vector in $\mathbb{F}_2^r$ defined as $\mathbf{w} = (t_{2k+1}(\mathfrak{p}_1), ..., t_{2k+1}(\mathfrak{p}_r))$ where $t_{2k+1}(\mathfrak{p}_i) = x_i m_i$ are found using the tests given by (4.30), (4.31) and (4.32). In this way, we have two cases to consider:

(a) if $t_{2k+1}(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_2$ then, by Proposition 4.2.6, we have that $\mathbf{x} = \mathbf{0}$ or $\mathbf{m} = \mathbf{0}$,

(b) if $t_{2k+1}(\mathfrak{p}) = 1$ for at least one $\mathfrak{p} \in T_2$ then we analyse whether $\mathbf{W} = \mathbf{0}$. If $\mathbf{W} = \mathbf{0}$ then, by Proposition 4.2.6 we have that $\mathbf{x} = \mathbf{m} = \mathbf{w}$. If $\mathbf{W} \neq \mathbf{0}$ then, using Proposition 4.2.6, we can recover $\mathbf{x}$, $\mathbf{m}$ and hence obtain Δ_b and Δ_{c_1}.

Therefore we have computed all the vectors $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and obtained $\Delta_a, \Delta_b, \Delta_c, \Delta_d$ and Δ_{abcd}.

Finally we present the algorithms of the methods to determine ρ modulo 2^{k+1} assuming that Δ_{det} is trivial.

Algorithm 8: This function determines the vectors $\mathbf{x}$ and $\mathbf{m}$ given by the rows of the matrix $\mathbf{W}$ constructed using the test function $t_{2k+1}(\mathfrak{p})$.

```
Input  : A quadratically independent set $T_2$ of primes.
         A Black Box Galois representation $\rho$ unramified outside $S$ such that
         $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ and $\det(\rho(\sigma)) \equiv 1 \pmod{2^{k+1}}$.
Output: The vectors $\mathbf{x}$ and $\mathbf{m}$.
Let $\mathfrak{p} \in T_2$;
Take $\mathbf{m} \in \mathbb{F}_2^r$ and define the discriminant $\Delta_{c_1}$;
Construct the matrix $\mathbf{W} = (t_{2k+1}(\mathfrak{p}_{ij}) - t_{2k+1}(\mathfrak{p}_i) - t_{2k+1}(\mathfrak{p}_j)) \in M_r(\mathbb{F}_2)$ using
  (4.30), (4.31), (4.32) and satisfying (4.33);
Construct $\mathbf{w} = (t_{2k+1}(\mathfrak{p}_1), ..., t_{2k+1}(\mathfrak{p}_r))$ for $\mathfrak{p}_i \in T_2$ using (4.30), (4.31), (4.32);
if $\mathbf{W} = \mathbf{0}$ then
    Take $\mathbf{x} = \mathbf{m} = \mathbf{w}$.
else
    if $\mathbf{w} = \mathbf{0}$ then
        Take $\mathbf{x}$ and $\mathbf{y}$ to be two distinct non-zero rows of $\mathbf{W}$.
    else
        The $i$-th row of $\mathbf{W}$ such that $\mathbf{w}_i \neq \mathbf{0}$ is $\mathbf{z}$;
        Take $\mathbf{x}$ to be any non-zero row of $\mathbf{W}$ distinct from the $i$-th row;
        Thus $\mathbf{m} = \mathbf{z} + \mathbf{x}$.
Return: $\{\mathbf{x}, \mathbf{m}\}$.
```

Algorithm 9: This function determines the representation $\rho(\sigma)$ modulo 2^{k+1} assuming that $\rho(\sigma)$ is trivial modulo 2^k and $\det(\rho(\sigma))$ is 1 modulo 2^{k+1} for all $\sigma \in G_K$.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
         A Black Box Galois representation unramified outside $S$ which is
         trivial modulo $2^k$ and its determinant is 1 modulo $2^{k+1}$.
Output: $\{\Delta_a, \Delta_b, \Delta_c, \Delta_d, \Delta_{abcd}\}$.
Use Algorithm 6 to compute a set $T_2$;
Construct $\mathbf{W} = (t_{2k}(\mathfrak{p}_{ij}) - t_{2k}(\mathfrak{p}_i) - t_{2k}(\mathfrak{p}_j)) \in M_r(\mathbb{F}_2)$ using (4.19) and
  satisfying (4.26) ;
if $\mathbf{W}$ has at least two distinct non-zero rows then
    Retrieve the vectors $\mathbf{x}$, $\mathbf{y}$ from the matrix $\mathbf{W}$ and take $\mathbf{z} = \mathbf{x} + \mathbf{y}$;
    Retrieve the vectors $\mathbf{u} = \mathbf{v}$ using (4.27).
else
    Assume $\mathbf{y} = \mathbf{0}$ and retrieve the vectors $\mathbf{u} = \mathbf{v}$ using (4.27);
    Call Algorithm 8.
return: $\{\Delta_a, \Delta_b, \Delta_c, \Delta_d, \Delta_{abcd}\}$.
```

Example 6. *Let $K = \mathbb{Q}(i)$ be our base field and assume*[III] *that over this field* $\det(\rho(\sigma)) \equiv 1 \pmod{2^2}$ *for all $\sigma \in G_K$. Let $S = \{1+i, 1+2i, 11+6i\}$ be the set of bad primes. Then we have that*

$$\begin{aligned} K(S,2) &= \langle 1+i, 1+2i, 11+6i, i\rangle \\ &\cong (\mathbb{Z}/2\mathbb{Z})^4. \end{aligned}$$

Consider

$$K_1 = K(\sqrt{\Delta_1}) \qquad K_2 = K(\sqrt{\Delta_2}) \qquad K_3 = K(\sqrt{\Delta_3}) \qquad K_4 = K(\sqrt{\Delta_4})$$

where

$$\Delta_1 = 1+i \qquad \Delta_2 = 1+2i \qquad \Delta_3 = 11+6i \qquad \Delta_4 = i.$$

Take the set of primes,

$$T_2 = \{11, 4+5i, 79, 5+2i, 3, 59, 6+i, 7, 2+i, 2+3i\},$$

and, as was done in Example 5, we construct the matrix $\mathbf{A}$

$$\begin{array}{r|cccccccccc}
 & \{1\} & \{2\} & \{3\} & \{4\} & \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\
\hline
11 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4+5i & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
79 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
5+2i & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
59 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
6+i & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
7 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
2+i & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
2+3i & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}.$$

which satisfies the special conditions of Algorithm 6. So we have found a quadratically independent set T_2 of primes. The Black Box considered here comes from the Galois representation of a Bianchi modular form[IV] *of level $56+2i$ whose Hecke eigenvalues give the traces. In this way, applying the test (4.2) on the set T_2 we can see that*

[III] We actually can verify if this assumption holds: since $\det(\rho(\sigma)) \equiv 1 \pmod 2$ for all $\sigma \in G_K$ and $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod{2^2}$ for all $\mathfrak{p} \in T_1 = \{11, 4+5i, 79, 5+2i\}$ by Proposition 4.4.1 then $\det(\rho(\sigma)) \equiv 1 \pmod{2^2}$ for all $\sigma \in G_K$.

[IV] The Bianchi modular form's label is "[3140,56,2].c" and was taken from `http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/iqfdata/data/nflist.1.1-10000` on March 2016.

$$\mathbf{b} = \begin{pmatrix} t_1(11) \\ t_1(4+5i) \\ t_1(79) \\ t_1(5+2i) \\ t_1(3) \\ t_1(59) \\ t_1(6+i) \\ t_1(7) \\ t_1(2+i) \\ t_1(2+3i) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

the width of the isogeny class is at least 2 *and thus we are in a "large isogeny class". To determine whether the width of the isogeny class is actually* 2*, we need to apply the tests* (4.19) *and* (4.20) *with* $k = 1$ *on the previously found set of primes* T_2*. As a result we get that*

$$\mathbf{b} = \begin{pmatrix} t_2(11) \\ t_2(4+5i) \\ t_2(79) \\ t_2(5+2i) \\ t_2(3) \\ t_2(59) \\ t_2(6+i) \\ t_2(7) \\ t_2(2+i) \\ t_2(2+3i) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

indeed, we are in a "large isogeny class" of width exactly 2*. Now, according to Algorithm 9, we find the vectors* $\mathbf{x}$ *and* $\mathbf{y}$ *by constructing the matrix* $\mathbf{W}$*, given by*

$$\mathbf{W} = \begin{pmatrix} 0 & x_1y_2+x_2y_1 & x_1y_3+x_3y_1 & x_1y_4+x_4y_1 \\ x_1y_2+x_2y_1 & 0 & x_2y_3+x_3y_2 & x_2y_4+x_4y_2 \\ x_1y_3+x_3y_1 & x_2y_3+x_3y_2 & 0 & x_3y_4+x_4y_3 \\ x_1y_4+x_4y_1 & x_2y_4+x_4y_2 & x_3y_4+x_4y_3 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Without loss of generality, take $\mathbf{x} = (0,0,1,1)$*,* $\mathbf{y} = (0,1,0,1)$ *and* $\mathbf{z} = \mathbf{x}+\mathbf{y} = (0,1,1,0)$*. Moreover we get that* $\mathbf{u} = \mathbf{v} = (0,0,0,1)$*. Therefore*

$$\begin{aligned}\Delta_b &= \Delta_1^0\Delta_2^0\Delta_3^1\Delta_4^1\\ &= (11+6i)(i)\\ &= -6+11i,\end{aligned} \qquad \begin{aligned}\Delta_{abcd} &= \Delta_1^0\Delta_2^1\Delta_3^1\Delta_4^0\\ &= (11+6i)(1+2i)\\ &= -1+28i.\end{aligned}$$

$$\begin{aligned}\Delta_c &= \Delta_1^0\Delta_2^1\Delta_3^0\Delta_4^1\\ &= (1+2i)(i)\\ &= -2+i,\end{aligned} \qquad \begin{aligned}\Delta_a &= \Delta_d\\ &= \Delta_1^0\Delta_2^0\Delta_3^0\Delta_4^1\\ &= i.\end{aligned}$$

In this way, the quadratic fields are

$$K(\sqrt{-6+11i}), \quad K(\sqrt{-2+i}) \quad \textit{and} \quad K(\sqrt{-1+28i}).$$

We can match the data presented in the previous example to the 2-isogeny class[V] *of the elliptic curves of conductor $N = 3140c$ over $\mathbb{Q}(i)$ given by the Weierstrass equation $y^2+(1+i)xy = x^3-x^2+(18-48i)x+(-158+30i)$.*

4.3.4 Δ_{det} non-trivial.

Suppose that Δ_{det} is non-trivial. Choose a basis $\{\Delta_i\}_{i=1}^r$ of $K(S,2)$ such that $\Delta_1 = \Delta_{\text{det}}$. Since $\Delta_{\text{det}} = \Delta_a\Delta_d$, we get that

$$\begin{aligned}\Delta_{abcd} &= \Delta_1\Delta_b\Delta_c,\\ &= \Delta_1^{1+x_1+y_1}\prod_{i=2}^{r}\Delta_i^{x_i+y_i}\end{aligned} \tag{4.34}$$

where $\mathbf{z} = \mathbf{x}+\mathbf{y}+\mathbf{e}_1$ and $\mathbf{e}_1 = (1,0,...,0) \in \mathbb{F}_2^r$. In this way,

$$\mathbf{x}+\mathbf{y}+\mathbf{z} = \mathbf{e}_1\,. \tag{4.35}$$

To determine the values of the discriminants, take primes $\mathfrak{p}_i, \mathfrak{p}_j, \mathfrak{p}_{ij} \in T_2$ with $i \neq j \geq 2$, then by test (4.19) we have that

$$\begin{aligned} t_{2k}(\mathfrak{p}_i) &= u_i + x_iy_i, \quad i \geq 2, \qquad (4.36)\\ t_{2k}(\mathfrak{p}_j) &= u_j + x_jy_j, \quad j \geq 2,\\ t_{2k}(\mathfrak{p}_{ij}) &= u_i + u_j + (x_i+x_j)(y_i+y_j), \quad 2 \leq i \neq j \leq r.\end{aligned}$$

[V] Taken from http://www.lmfdb.org/EllipticCurve/2.0.4.1/%5B3140%2C56%2C2%5D/c/ on March 2016.

We want to find the vectors $\mathbf{u}$, $\mathbf{v}$, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ with $\mathbf{x}+\mathbf{y}+\mathbf{z}=\mathbf{e}_1$ and $\mathbf{u}+\mathbf{v}=\mathbf{e}_1$. We define shortened versions of these vectors by dropping the first coordinate of them and naming them as $\mathbf{u}'$, $\mathbf{v}'$, $\mathbf{x}'$, $\mathbf{y}'$ and $\mathbf{z}'$ where we can see that $\mathbf{u}'=\mathbf{v}'$ and $\mathbf{x}'+\mathbf{y}'+\mathbf{z}'=\mathbf{0}$.

Observe that the test functions given in (4.36) are exactly the same as those given in (4.24), except that the indices now start from 2, not from 1. So using exactly the methods of Section 4.3.3 and the values $t_{2k}(\mathfrak{p}_i)$ and $t_{2k}(\mathfrak{p}_{ij})$ for $i \neq j \geq 2$ we can determine all of these shortened vectors.

It remains to use the test functions $t_{2k}(\mathfrak{p}_1)$ and $t_{2k}(\mathfrak{p}_{1i})$, for $2 \leq i \leq r$, to determine the first coordinates u_1, $v_1 = 1+u_1$, x_1, y_1 and z_1 with $x_1+y_1+z_1=1$. Before that we note the following symmetries:

(1) $\mathbf{u}'$ and $\mathbf{v}'$, and hence $\mathbf{u}$ and $\mathbf{v}$, are interchangeable (by a suitable conjugation) so at the end we can arbitrarily set $u_1 = 1$ and $v_1 = 0$;

(2) the symmetries between $\mathbf{x}'$, $\mathbf{y}'$ and $\mathbf{z}'$ depend on:

   (a) if $\mathbf{x}'$, $\mathbf{y}'$ and $\mathbf{z}'$ are all non-zero, and hence also distinct, then we can permute them how we like;

   (b) if $\mathbf{x}'=\mathbf{y}'=\mathbf{z}'=\mathbf{0}$ then again we can permute $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ how we like;

   (c) otherwise we have one of them is $\mathbf{0}$ and the others equal and non-zero, and we have chosen it so that $\mathbf{y}'=\mathbf{0}$ and $\mathbf{x}'=\mathbf{z}'$, so we can still swap $\mathbf{x}$ and $\mathbf{z}$ if we like.

Now, since $u_1v_1 = 0$ we have that $t_{2k}(\mathfrak{p}_1) = x_1y_1$. Thus, if $x_1y_1 = 1$ then we will have that $x_1 = y_1 = z_1 = 1$, so we put a 1 in front of $\mathbf{x}'$, $\mathbf{y}'$, $\mathbf{z}'$ to get $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ and we are done. Otherwise we have that $x_1y_1 = 0$ and we need to determine whether $(x_1, y_1, z_1) = (1, 0, 0)$, $(0, 1, 0)$ or $(0, 0, 1)$. We can compute $t_{2k}(\mathfrak{p}_{1i}) = (u_1+u_i)(v_1+v_i)+(x_1+x_i)(y_1+y_i) = (x_1+x_i)(y_1+y_i)$ for $i \geq 2$ and hence, since we know the rest already, we get the values $y_1x_i + x_1y_i$ for $i \geq 2$. The vector of these, say $\mathbf{q} = (t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_{1i}) + u_i)_{i=2}^{r}$ in $\mathbb{F}_2^{r-1}$, is thus $y_1\,\mathbf{x}' + x_1\,\mathbf{y}'$.

In (2)a, $\mathbf{x}'$ and $\mathbf{y}'$ are linearly independent so we get x_1 and y_1 uniquely. In (2)b, we have complete symmetry and set $\mathbf{x}=\mathbf{y}=\mathbf{0}$ and $\mathbf{z}=\mathbf{e}_1$. In (2)c, since $\mathbf{y}'=\mathbf{0}$ we have $\mathbf{q} = y_1\,\mathbf{x}'$ and $\mathbf{x}'$ is not zero, so if $\mathbf{q} \neq \mathbf{0}$ then $y_1 = 1$ and $x_1 = z_1 = 0$. On the other hand, if $\mathbf{q} = \mathbf{0}$ then $y_1 = 0$ and we can set $x_1 = 0$, $z_1 = 1$ (or vice versa, it does not matter since $\mathbf{x}' = \mathbf{z}'$).

Therefore we have computed the all the vectors $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and obtained Δ_a, Δ_b, Δ_c, Δ_d and Δ_{abcd}.

Remark 4.3.4. *Observe that the values of $\Delta_a, \Delta_b, \Delta_c, \Delta_d$ and Δ_{abcd} depend on which node of the Bruhat-Tits tree we stand on. For example, in Example 4 if we stand on the node ②, we get that $\Delta_b = \Delta_c = 5$ and $\Delta_{abcd} = -5$. On the other hand, if we stand on the node ⑥ we get $\Delta_b = \Delta_c = 15$ and $\Delta_{abcd} = -15$.*

Conclusion

Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z})$ be a Galois representation unramified outside S such that $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ for all $\sigma \in G_K$. Then by sections 4.3.3 and 4.3.4 we can determine ρ modulo 2^{k+1} only by finding and testing, with our test $t_{2k}(\mathfrak{p})$, a quadratically independent set T_2 of primes. Particularly when $k = 1$ and the width of the stable Bruhat-Tits tree is at least 2, we are able to determine whether the width is 2, 3 or at least 4 using the same set T_2 of primes that was found to distinguish the "small isogeny class" case and the "large isogeny class" case!

Finally we present the algorithm related to this section.

Algorithm 10: This function determines the representation $\rho(\sigma)$ modulo 2^{k+1} assuming that $\rho(\sigma)$ is trivial 2^k and $\det(\rho(\sigma)) \not\equiv 1 \pmod{2^{k+1}}$ for some $\sigma \in G_K$.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
         A Black Box Galois representation unramified outside $S$ which is
         trivial modulo $2^k$ and its determinant lies in $\{1, 1+2^k\}$ modulo $2^{k+1}$.
Output: $\{\Delta_a, \Delta_b, \Delta_c, \Delta_d, \Delta_{abcd}\}$.
Compute a basis of $K(S,2)$ such that $\Delta_1 = \Delta_{\text{det}}$;
Use Algorithm 6 to compute a set $T_2$;
Construct $\mathbf{W}' = (t_{2k}(\mathfrak{p}_{ij}) - t_{2k}(\mathfrak{p}_i) - t_{2k}(\mathfrak{p}_j)) \in M_{r-1}(\mathbb{F}_2)$ using (4.36) and
  satisfying (4.26) for $i \neq j \geq 2$;
Use algorithms 8 and 9 to determine the shortened vectors $\mathbf{x}'$, $\mathbf{y}'$, $\mathbf{z}'$, $\mathbf{u}'$, $\mathbf{v}'$;
Set $u_1 = 1$ and $v_1 = 0$;
if $x_1 y_1 = 1$ then
    $x_1 = y_1 = z_1 = 0$.
else
    Compute $\mathbf{q} = (t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_{1i}) + u_i)_{i=2}^{r}$ for $\mathfrak{p}_i, \mathfrak{p}_{1i} \in T_2$ and $2 \leq i \leq r$;
    if $\mathbf{q} \neq \mathbf{0}$ then
        if $\mathbf{x}' \neq \mathbf{y}' \neq \mathbf{0}$ then
            $x_1 = 0$, $y_1 = 1$ and $z_1 = 0$.
        else
            $\mathbf{y}' = \mathbf{0}$, $\mathbf{x}' = \mathbf{z}' \neq \mathbf{0}$, so $x_1 = z_1 = 0$ and $y_1 = 1$.
    else
        $x_1 = y_1 = 0$ and $z_1 = 1$.
return: $\{\Delta_a, \Delta_b, \Delta_c, \Delta_d, \Delta_{abcd}\}$.
```

Example 7. *Let $K = \mathbb{Q}$ and let $S = \{2, 3, 7\}$ be our set of bad primes. Observe that for these K and S we have*

$$K(S,2) = \langle -1, 2, 3, 7 \rangle \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

Consider

$$K_1 = \mathbb{Q}(\sqrt{-1}) \qquad K_2 = \mathbb{Q}(\sqrt{2}) \qquad K_3 = \mathbb{Q}(\sqrt{3}) \qquad K_4 = \mathbb{Q}(\sqrt{7})$$

and take the set

$$T_2 = \{47, 37, 113, 73, 59, 31, 23, 29, 13, 17\}.$$

As was done in examples 5 and 6, we construct the matrix $\mathbf{A}$

	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
47	1	0	0	0	0	0	0	0	0	0
37	0	1	0	0	0	0	0	0	0	0
113	0	0	1	0	0	0	0	0	0	0
73	0	0	0	1	0	0	0	0	0	0
59	1	1	0	0	1	0	0	0	0	0
31	1	0	1	0	0	1	0	0	0	0
23	1	0	0	1	0	0	1	0	0	0
29	0	1	1	0	0	0	0	1	0	0
13	0	1	0	1	0	0	0	0	1	0
17	0	0	1	1	0	0	0	0	0	1

which satisfies the special conditions of Algorithm 6. Thus we have found a quadratically independent set T_2 *of primes. The Black Box considered here is the modular form*[VI] $f = 168.2.1a$ *so there is an associated Galois representation* ρ *unramified outside* $\{2,3,7\}$ *such that for* $p \notin \{2,3,7\}$ *we have*

$$\det(\rho(\mathrm{Frob}_p)) = p$$
$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = a_p,$$

the p*-th Hecke eigenvalue of* f*. In this way, applying the test (4.2) on set* T_2 *we get that*

[VI] Taken from http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/168/2/1/a/) on March 2016

$$\mathbf{b} = \begin{pmatrix} t_1(47) \\ t_1(37) \\ t_1(113) \\ t_1(73) \\ t_1(59) \\ t_1(31) \\ t_1(23) \\ t_1(29) \\ t_1(13) \\ t_1(17) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

the isogeny class is "large" of width at least 2*. Now, since the determinant is* ± 1 *modulo* 2^2*, applying the tests* (4.19) *and* (4.20) *for* $k = 1$ *on the set* T_2 *will give us that*

$$\mathbf{b} = \begin{pmatrix} t_2(47) \\ t_2(37) \\ t_2(113) \\ t_2(73) \\ t_2(59) \\ t_2(31) \\ t_2(23) \\ t_2(29) \\ t_2(13) \\ t_2(17) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

the width of the "large isogeny class" is exactly 2*. According to Algorithm 10, we need to construct the matrix* $\mathbf{W}'$ *with entries*

$$w_{23} = w_{32} = t_2(37) + t_2(113) + t_2(29) = 0,$$

$$w_{24} = w_{42} = t_2(37) + t_2(73) + t_2(13) = 0,$$

$$w_{34} = w_{43} = t_2(113) + t_2(73) + t_2(17) = 1.$$

Thus the matrix $\mathbf{W}'$ *looks like*

$$\mathbf{W}' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Since the second row is different from the third row, w.l.o.g., set $\mathbf{x}' = (0, 0, 1)$ *and* $\mathbf{y}' = (0, 1, 0)$*. Moreover, because* $x_1 y_1 = 0$*, we have that* $\mathbf{u}' = \mathbf{v}' = \mathbf{0}$ *and, from these,* $\mathbf{q} = (0, 0, 1)$*. Thus* $x_1 = 0$*,* $y_1 = 1$ *and* $z_1 = 0$*. In this way* $\mathbf{x} = (0, 0, 0, 1)$*,*

$\mathbf{y} = (1,0,1,0)$, $\mathbf{z} = (0,0,1,1)$ *and the discriminants related to these vectors are* $\Delta_b = 7, \Delta_c = -3$ *and* $\Delta_{abcd} = 21$.

Finally, the quadratic fields are

$$K(\sqrt{7}), \quad K(\sqrt{-3}) \quad \textit{and} \quad K(\sqrt{21}).$$

Note that the data presented in the previous example matches the 2*-isogeny class*[VII] *of the elliptic curves of conductor* $N = 168$ *over* $\mathbb{Q}$ *given by the Weierstrass equation* $y^2 = x^3 - x^2 - 4032x + 99900$.

4.4 Isogenous Galois representations modulo 2^{k+1}.

We finish the chapter by stating and proving a theorem that will provide us an easy criterion to determine whether, for a given Galois representation which is trivial modulo 2^k and satisfies certain conditions, there exists an isogenous representation, to the given one, that is trivial modulo 2^{k+1}.

Proposition 4.4.1. *Let* $\chi\colon G_K \to \mathbb{Z}_2^*$ *be a continuous character unramified outside a set of primes* S. *If*

1. $\chi(\sigma) \equiv 1 \pmod{2^{k-1}}$ *for all* $\sigma \in G_K$,
2. $\chi(\mathrm{Frob}_{\mathfrak{p}}) \equiv 1 \pmod{2^k}$ *for all* $\mathfrak{p} \in T_1$,

then $\chi(\sigma) \equiv 1 \pmod{2^k}$ *for all* $\sigma \in G_K$.

Proof. Let $\chi\colon G_K \to \mathbb{Z}_2^*$ be a continuous character unramified outside a set of primes S. Suppose that for all $\mathfrak{p} \in T_1$ with $\sigma = \mathrm{Frob}_{\mathfrak{p}}$ we have that $\chi(\sigma) \equiv 1 \pmod{2^k}$ but there exists at least one $\sigma \in G_K$ such that $\chi(\sigma) \not\equiv 1 \pmod{2^k}$. This means that $\chi(\sigma) \equiv 1 + 2^{k-1}\alpha(\sigma) \pmod{2^k}$ where $\alpha(\sigma) \in \mathbb{Z}_2$.

We observe that $\alpha(\sigma) \equiv 0 \pmod 2$ for all $\mathfrak{p} \in T_1$. This implies that the quadratic extension $K(\sqrt{\Delta})$ related to α modulo 2 (which is an additive quadratic character) is trivial by Lemma 3.3.1, i.e., $\Delta = 1$. Hence $\alpha(\sigma) \equiv 0 \pmod 2$ for all $\sigma \in G_K$. Therefore $\chi(\sigma) \equiv 1 \pmod{2^k}$ for all $\sigma \in G_K$. □

Lemma 4.4.2. *Let* G *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}_2)$ *such that for some* $k \geq 1$, *every* g *in* G *has the form*

$$g = \mathbf{I} + 2^k \begin{pmatrix} 2a & b \\ 2c & 2d \end{pmatrix}$$

with a, b, c, d *in* $\mathbb{Z}_2$ *and* bc *even, i.e., for each* g, *either* b *is even or* c *is even. Then in fact either* b *is even for all* g *in* G, *or* c *is even for all* g *in* G. *In the first case*

$$g \equiv \mathbf{I} \pmod{2^{k+1}} \textit{ for all } g \textit{ in } G.$$

[VII] Taken from http://www.lmfdb.org/EllipticCurve/Q/168/a/ on March 2016.

In the second case

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \equiv \mathbf{I} \pmod{2^{k+1}} \text{ for all } g \text{ in } G.$$

Proof. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ such that its elements satisfy the conditions given above; g_b is such that b is even and g_c is such that c is even. Observe that the elements, g_b and g_c, i.e., the two types of elements in G_K for which either b or c is even, make two subgroups of G. But G cannot be the union of two proper subgroups! Therefore G is a subgroup such that either, for all its elements, b or c is even. □

Theorem 4.4.3. *Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a Galois representation unramified outside S such that*

$$\rho(\sigma) \equiv \mathbf{I} \pmod{2^k} \text{ for all } \sigma \in G_K$$

and suppose that for a linearly independent set T_1 and a quadratically independent set T_2 we have that

1. $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod{2^{k+1}}$ *for all* $\mathfrak{p} \in T_1$,
2. $v(\mathfrak{p}) \geq 2k+2$ *for all* $\mathfrak{p} \in T_2$.

Then there exists an isogenous representation ρ' such that $\rho'(\sigma) \equiv \mathbf{I} \pmod{2^{k+1}}$ for all $\sigma \in G_K$.

The proof of the theorem follows an inductive step.

Proof. Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a Galois representation unramified outside a set of primes S such that $\rho(\sigma) \equiv \mathbf{I} \pmod{2^k}$ for all $\sigma \in G_K$. Suppose that $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod{2^{k+1}}$ for all $\mathfrak{p} \in T_1$. Then Proposition 4.4.1 implies that $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) \equiv 1 \pmod{2^{k+1}}$ for all $\mathrm{Frob}_{\mathfrak{p}} = \sigma \in G_K$.

To prove that ρ is congruent to the identity modulo 2^{k+1}, we have to prove that the entries a, b, c, d of (4.13) are divisible by 2. To do this, assume that $v(\mathfrak{p}) > 2k$ for all $\mathfrak{p} \in T_2$. Thus $a \equiv d \pmod 2$ and $a + bc \equiv 0 \pmod 2$ for all $\mathfrak{p} \in T_2$. By Section 4.3.3, at least one of the characters χ_b, χ_c or χ_{abcd} is 0. W.l.o.g., suppose that $\chi_c = 0$, i.e., $c \equiv 0 \pmod 2$. This implies that $a \equiv d \equiv 0 \pmod 2$.

Notice that until this point we do not know if χ_b is trivial or not. Therefore (4.13) looks like

$$\rho(\sigma) = \begin{pmatrix} 1 + 2^{k+1}a_1 & 2^k b \\ 2^{k+1}c_1 & 1 + 2^{k+1}d_1 \end{pmatrix}.$$

Applying the determinant to the matrix presented above, we get that

$$\det(\rho(\sigma)) = (1 + 2^{k+1}a_1)(1 + 2^{k+1}d_1) - 2^{2k+1}bc_1$$

and

$$\begin{aligned} 1 - \operatorname{tr}(\rho(\sigma)) + \det(\rho(\sigma)) &= 2^{2k+2}a_1d_1 - 2^{2k+1}bc_1 \\ &\equiv 2^{2k+1}bc_1 \pmod{2^{2k+2}}. \end{aligned}$$

Hence, we are now allow to use the test (4.20), e.g.,

$$t_{2k+1}(\sigma) := \frac{1}{2^{2k+1}}(1 - \operatorname{tr}(\rho(\sigma)) + \det(\rho(\sigma))) \equiv bc_1 \pmod 2.$$

Now, since by hypothesis for all $\mathfrak{p} \in T_2$ we get that $v(\mathfrak{p}) > 2k + 1$ then $bc_1 \equiv 0 \pmod 2$ for all $\mathfrak{p} \in T_2$. Then, by Lemma 4.4.2, we always get that $b \equiv 0 \pmod 2$ or $c_1 \equiv 0 \pmod 2$ for all $\mathfrak{p} \in T_2$. Thus, again by Lemma 4.4.2, we get whether the same representation ρ or an isogenous representation ρ' both being congruent to the identity modulo 2^{k+1}:

$$\rho(\sigma) = \begin{pmatrix} 1 + 2^{k+1}a_1 & 2^{k+1}b_1 \\ 2^{k+1}c_1 & 1 + 2^{k+1}d_1 \end{pmatrix}$$

or

$$\rho(\sigma) = \begin{pmatrix} 1 + 2^{k+1}a_1 & 2^{k}b \\ 2^{k+2}c_2 & 1 + 2^{k+1}d_1 \end{pmatrix} \xleftrightarrow{\text{isogenous}} \begin{pmatrix} 1 + 2^{k+1}a_1 & 2^{k+1}b \\ 2^{k+1}c_2 & 1 + 2^{k+1}d_1 \end{pmatrix} = \rho'(\sigma)$$

and therefore we are done. □

Now we present the algorithm based on the previous theorem.

Algorithm 11: This function determines whether exists a representation $\rho'(\sigma)$ congruent to the identity modulo 2^{k+1} given a representation $\rho(\sigma)$, which is isogenous to ρ', congruent to the identity modulo 2^k for all $\sigma \in G_K$.

Input : A number field K.
A finite set S of primes of K.
A Black Box Galois representation unramified outside S which is trivial modulo 2^k.

Output: Return: True if there exists such representation.
Else return: False.

```
Use Algorithm 3 to compute $T_1$;
Use Algorithm 6 to compute $T_2$;
if $v_1(\mathfrak{p}) > k$ for all $\mathfrak{p} \in T_1$ then
    if $v(\mathfrak{p}) > 2k+1$ for all $\mathfrak{p} \in T_2$ then
        return: True.
    else
        return: False.
else
    return: False.
```

In summary, given that ρ is trivial modulo 2^k, if $v_1(\mathfrak{p}) > k$ for all $\mathfrak{p}$ in T_1 and $v(\mathfrak{p}) > 2k+1$ for all $\mathfrak{p} \in T_2$ then there exists ρ' which is trivial modulo 2^{k+1}.

We end the chapter with the following corollary.

Corollary 4.4.4. *Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a continuous Galois representation unramified outside S such that $\overline{\rho}$ is trivial. If*

(a) $\det(\rho(\mathrm{Frob}_{\mathfrak{p}})) = 1$ *for all* $\mathfrak{p} \in T_1$, *and*

(b) $\mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) = 2$ *for all* $\mathfrak{p} \in T_2$

then ρ is reducible with trivial semisimplification.

Chapter 5

Comparing two Black Box Galois representations.

Let K be a number field and let S be a finite set of primes of K. Let $\rho_j\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be two integral continuous Galois representations unramified outside S and consider their Black Boxes as in Chapter 4. We will be referring to the Black Boxes as ρ_1 and ρ_2 for each representation. Throughout the chapter the following results will be described.

1. Section 5.1. In this section we develop the theory to determine, in subsequent sections, whether two Black Boxes are isogenous. The strategy follows an inductive argument; by proving that the Black Boxes have the same residual image and are isogenous modulo 2^k, an obstruction arises when lifting the isogeny modulo 2^k to one modulo 2^{k+1}. Then we prove that the obstruction is represented by a cocycle μ whose class is a well-defined element of a very special cohomology group. We proceed to the next section.

2. Section 5.2. In this section we give a thorough and full description of the cohomology group named $\tilde{H}_1(G_K, V_0)$. This description relies on the residual image of the Black Boxes. Moreover, this will allow us to see the class $[\mu]$ as the sum of classes in simpler cohomology groups. We proceed to the next section.

3. Section 5.3. In this section we give and prove sufficient conditions to determine whether the class $[\mu]$ is zero when $\overline{\rho}$ is surjective. The process starts by dividing the class $[\mu]$ as the sum of two classes $[\mu_1]$ and $[\mu_2]$ as was seen in the previous section. Then we find finite sets of primes satisfying certain conditions to establish that each class is zero by comparing traces at these primes. In this way, by checking a finite number of primes, the obstruction to the lifting vanishes and the isogeny is proved. Currently our methods, as developed here, only succeed in eliminating the obstruction when the residual representations are surjective, though some of the results could apply in the other cases.

The motivation of the chapter came from what was proven in [8] by professors Luis Dieulefait, Lucio Guerberoff and Ariel Pacetti. The main goal of this chapter was to create an alternative improved method for the Faltings-Serre-Livné method given in Livné's article [11]; one of the aimed improvements was to find a set of smaller set of primes, compared to the one found by Faltings-Serre-Livné, for which to test if the representations are the same. In the end, Livné's results ended up being used and unfortunately the main goal was only partially achieved.

5.1 Proving congruence modulo 2^{k+1}.

Let ρ_1 and ρ_2 be two Black Box Galois representations unramified outside S. We would like to prove that these two representations are isogenous. We start this process by checking first, using Theorem 3.3.2, whether $\det(\rho_1) = \det(\rho_2)$, which is a necessary condition for them to be isogenous. Thus, from now on we assume that $\det(\rho_1) = \det(\rho_2)$. Furthermore, using the methods of Chapter 4 we determine the residual image representations $\overline{\rho}_1$ and $\overline{\rho}_2$. If these (or their semisimplification) differ, then certainly ρ_1 and ρ_2 are not isogenous. Hence we may assume that $\overline{\rho}(\sigma) \equiv \rho_1(\sigma) \equiv \rho_2(\sigma) \pmod 2$.

Now, by an inductive argument, suppose that ρ_1 and ρ_2 are isogenous modulo 2^k but not necessarily modulo 2^{k+1}. We can assume, after replacing ρ_1 by a conjugate if necessary, that $\rho_1(\sigma) \equiv \rho_2(\sigma) \pmod{2^k}$ for some $k \geq 1$. This defines a possible non-constant map

$$\begin{aligned} \varphi\colon G_K &\to \mathbb{F}_2 \\ \sigma &\mapsto \frac{\operatorname{tr}(\rho_1(\sigma)) - \operatorname{tr}(\rho_2(\sigma))}{2^k} \pmod 2. \end{aligned} \tag{5.1}$$

Also, for every given $\sigma \in G_K$ there is a matrix $\mu(\sigma) \in \mathrm{M}_2(\mathbb{Z}_2)$ such that

$$\rho_1(\sigma) = (\mathbf{I} + 2^k \mu(\sigma))\rho_2(\sigma). \tag{5.2}$$

Since $\det(\rho_1) = \det(\rho_2)$ we have that $1 = \det(\mathbf{I} + 2^k \mu(\sigma))$, which implies that $\operatorname{tr}(\mu(\sigma)) \equiv 0 \pmod 2$. In this way, we get an induced map

$$\begin{aligned} \overline{\mu}\colon G_K &\to V_0 \\ \sigma &\mapsto \mu(\sigma) \pmod 2 \end{aligned} \tag{5.3}$$

where $V = M_2(\mathbb{F}_2)$, $V_0 = \{\mathbf{A} \in M_2(\mathbb{F}_2) : \operatorname{tr}(\mathbf{A}) = 0\}$ and satisfying

$$\overline{\mu}(\sigma_1\sigma_2) \equiv \overline{\mu}(\sigma_1) + \overline{\rho}(\sigma_1)\overline{\mu}(\sigma_2)\overline{\rho}(\sigma_1)^{-1} \pmod 2. \tag{5.4}$$

Substituting (5.2) in (5.1) we get

$$\varphi(\sigma) = \operatorname{tr}(\overline{\mu}(\sigma)\overline{\rho}(\sigma)). \tag{5.5}$$

Since we are only interested in $\overline{\mu}$, the reduction of μ modulo 2, to simplify notation we will write μ for $\overline{\mu}$ from now on.

The map μ depends on the choice of conjugation, as we will see later. It will turn out that μ determines a well-defined cohomology class which represents the obstruction of extending the isogeny modulo 2^k to module 2^{k+1}.

Observe that, by (5.4), μ is actually a cocycle with values in the G_K-module V_0 where the G_K-action on V_0 is given by

$$\sigma\colon\ \mathbf{A} \mapsto \overline{\rho}(\sigma)\,\mathbf{A}\,\overline{\rho}(\sigma)^{-1}, \qquad \mathbf{A} \in V_0 \tag{5.6}$$

denoted by ${}^{\sigma}\mathbf{A}$, where $\overline{\rho}(\sigma) \in \overline{\rho}(G_K)$. However the class of μ in $H^1(G_K, V_0)$ is not well-defined as we now discuss.

Take $V_0 = V_1 \oplus V_2$ as G_K-modules with $\dim V_j = j$ for $j = 1, 2$ where

$$\begin{aligned} V_1 &= \langle \mathbf{I} \rangle \\ &= \{\mathbf{0}, \mathbf{I}\} \\ &= \left\{\mathbf{A} \in V_0 : \operatorname{tr}(\mathbf{A}\,\mathbf{T}) = 0 \text{ for all } \mathbf{T} \in \mathrm{GL}_2(\mathbb{F}_2) \text{ with } \mathbf{T}^2 = \mathbf{I}\right\} \end{aligned}$$

and

$$\begin{aligned} V_2 &= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \\ &= \left\{ \mathbf{0}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \\ &= \{\mathbf{0}\} \cup \{\mathbf{A} : \mathbf{A}^2 = \mathbf{I}\} \\ &= \{\mathbf{A} \in V_0 : \operatorname{tr}(\mathbf{A}\,\mathbf{R}) = \mathbf{0} \text{ for all } \mathbf{R} \in \mathrm{GL}_2(\mathbb{F}_2) \text{ such that } \mathbf{R}^3 = \mathbf{I}\}. \end{aligned}$$

Observe that V_1 and V_2 are G_K-invariant. Indeed, by direct calculations, when (5.6) acts on matrices $A \in V_j$ we get ${}^{\sigma}A \in V_j$ for $j = 1, 2$.

We have constructed a cocycle $\mu \in Z^1(G_K, V_0) \subseteq Z^1(G_K, V)$. Moreover, we have that

$$H^1(G_K, V_0) = H^1(G_K, V_1) \oplus H^1(G_K, V_2). \tag{5.7}$$

A natural related question is, do we have a well-defined cohomology class in either $H^1(G_K, V_0)$ or in $H^1(G_K, V)$?

Lemma 5.1.1. *The class of μ in $H^1(G_K, V)$ is well-defined, but its class in $H^1(G_K, V_0)$*

may not be.

Proof. Let ρ_1 and ρ_2 be two representations satisfying (5.2). Replace ρ_2 by a conjugate $\mathbf{U}\,\rho_2\,\mathbf{U}^{-1}$ where $\mathbf{U} \equiv \mathbf{I} \pmod{2^k}$ is of the form $\mathbf{U} = \mathbf{I} + 2^k\,\mathbf{B}$ with $\mathbf{B} \in V$, then

$$\begin{aligned} \rho_1(\sigma) &= (\mathbf{I} + 2^k\mu(\sigma))\rho_2(\sigma) \\ &= (\mathbf{I} + 2^k\mu'(\sigma))\,\mathbf{U}\,\rho_2(\sigma)\,\mathbf{U}^{-1} \end{aligned}$$

with $\mu'(\sigma) \in V_0$ as before. We compute

$$\begin{aligned} (\mathbf{I} + 2^k\mu(\sigma))\rho_2(\sigma) &\equiv (\mathbf{I} + 2^k\mu'(\sigma))\,\mathbf{U}\,\rho_2(\sigma)\,\mathbf{U}^{-1} && \pmod{2^{k+1}} \\ &\equiv (\mathbf{I} + 2^k\mu'(\sigma))(\mathbf{I} + 2^k\,\mathbf{B})\rho_2(\sigma)(\mathbf{I} - 2^k\,\mathbf{B}) && \pmod{2^{k+1}} \\ \rho_2(\sigma) + 2^k\mu(\sigma)\rho_2(\sigma) &\equiv \rho_2(\sigma) + 2^k(\mu'(\sigma)\rho_2(\sigma) + \mathbf{B}\,\rho_2(\sigma) - \rho_2(\sigma)\,\mathbf{B}) && \pmod{2^{k+1}} \\ \mu(\sigma)\overline{\rho}(\sigma) &\equiv (\mu'(\sigma) + \mathbf{B})\overline{\rho}(\sigma) + \overline{\rho}(\sigma)\,\mathbf{B} && \pmod{2} \\ \mu(\sigma) &\equiv \mu'(\sigma) + \mathbf{B} + \overline{\rho}(\sigma)\,\mathbf{B}\,\overline{\rho}(\sigma)^{-1} && \pmod{2} \\ \mu(\sigma) - \mu'(\sigma) &\equiv {}^{\sigma}\,\mathbf{B} - \mathbf{B} && \pmod{2} \end{aligned}$$

We can see that the cocycle $\mu(\sigma)$ and the coboundary $\mu(\sigma) - \mu'(\sigma) = {}^{\sigma}\,\mathbf{B} - \mathbf{B}$ take values in V_0, but $\mathbf{B}$ itself is in V and not necessarily in V_0.

Therefore μ is indeed well-defined in $H^1(G_K, V)$ and is not necessarily well-defined in $H^1(G_K, V_0)$. □

In the following section we will see that, for $H^1(G_K, V_0)$, there is a zero or one-dimensional subspace W of $H^1(G_K, V)$ such that μ defines a well-defined element in the quotient $\dfrac{H^1(G_K, V_0)}{W} \subseteq H^1(G_K, V)$.

Moreover, the proof of Lemma 5.1.1 shows that if the class of μ is trivial, there exists a conjugate $\rho_2' = \mathbf{U}\,\rho_2\,\mathbf{U}^{-1}$ such that $\rho_1 \equiv \rho_2' \pmod{2^{k+1}}$ (see Proposition 5.3.1 below).

5.1.1 The four possible images.

Since the action of G_K on V preserves trace, we have the following short exact sequence of G_K-modules

$$\begin{tikzcd} 0 \arrow[r] & V_0 \arrow[r, hook] & V \arrow[r, "\text{trace}"] & \mathbb{F}_2 \arrow[r] & 0. \end{tikzcd}$$

By standard cohomology theory we have

$$\begin{tikzcd} 0 \arrow[r] & H^0(G_K, V_0) \arrow[r, "\delta"'] & H^0(G_K, V) \arrow[r] & H^0(G_K, \mathbb{F}_2) \arrow[dlll, rounded corners] \\ H^1(G_K, V_0) \arrow[r] & H^1(G_K, V) \arrow[r] & H^1(G_K, \mathbb{F}_2) \arrow[r] & \cdots \end{tikzcd} \tag{5.8}$$

We can observe that the behaviour of the connecting homomorphism δ depends on the four possible images of the residual representation, i.e., on $\overline{\rho}(G_K)$ being isomorphic to one group of the following list

$$\overline{\rho}(G_K) \cong \begin{cases} C_1 \\ C_2 \\ C_3 \\ S_3 \end{cases} \tag{5.9}$$

Without loss of generality, when the image of $\overline{\rho}$ is isomorphic to C_2 or C_3, choose $\mathbf{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\mathbf{R} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ respectively, so in this way we will have $C_2 \cong \langle \mathbf{T} \rangle$ or $C_3 \cong \langle \mathbf{R} \rangle$.

Now, observe that $H^0(G_K, V)$ and $H^0(G_K, V_0)$, according to (5.9), will look like

$$H^0(G_K, V) = \begin{cases} V & \text{if} \quad \overline{\rho}(G_K) \cong C_1 \\ \langle \mathbf{I}, \mathbf{T} \rangle & \text{if} \quad \overline{\rho}(G_K) \cong C_2 \\ \langle \mathbf{I}, \mathbf{R} \rangle & \text{if} \quad \overline{\rho}(G_K) \cong C_3 \\ V_1 & \text{if} \quad \overline{\rho}(G_K) \cong S_3 \end{cases} \tag{5.10}$$

and

$$H^0(G_K, V_0) = \begin{cases} V_0 & \text{if} \quad \overline{\rho}(G_K) \cong C_1 \\ \langle \mathbf{I}, \mathbf{T} \rangle & \text{if} \quad \overline{\rho}(G_K) \cong C_2 \\ V_1 & \text{if} \quad \overline{\rho}(G_K) \cong C_3 \\ V_1 & \text{if} \quad \overline{\rho}(G_K) \cong S_3 \end{cases} \tag{5.11}$$

For example, when the image of $\overline{\rho}$ is $C_3 \cong \langle \mathbf{R} \rangle$, the only elements $\mathbf{A}$ in V satisfying the condition ${}^{\sigma}\,\mathbf{A} = \mathbf{A}$ are those in $\{\mathbf{0}, \mathbf{I}, \mathbf{R}, \mathbf{R}^2\}$. Thus $H^0(G_K, V) = \langle \mathbf{I}, \mathbf{R} \rangle$. Observe that $\mathbf{R}^2 = \mathbf{R} + \mathbf{I}$.

So, for each case in (5.10) and (5.11), the long exact sequence (5.8) becomes

$$\begin{tikzcd}
C_1\colon & 0 \arrow[r] & V_0 \arrow[r] & V \arrow[r, two heads] & \mathbb{F}_2 \arrow[r, "0"] & H^1(G_K, V_0) \arrow[r, hook, "\phi"] & H^1(G_K, V) \\
C_2\colon & 0 \arrow[r] & \langle \mathbf{I}, \mathbf{T} \rangle \arrow[r] & \langle \mathbf{I}, \mathbf{T} \rangle \arrow[r, "0"] & \mathbb{F}_2 \arrow[r, hook, "\delta"] & H^1(G_K, V_0) \arrow[r, "\phi"] & H^1(G_K, V) \\
C_3\colon & 0 \arrow[r] & V_1 \arrow[r] & \langle \mathbf{I}, \mathbf{R} \rangle \arrow[r, two heads] & \mathbb{F}_2 \arrow[r, "0"] & H^1(G_K, V_0) \arrow[r, hook, "\phi"] & H^1(G_K, V) \\
S_3\colon & 0 \arrow[r] & V_1 \arrow[r] & V_1 \arrow[r, "0"] & \mathbb{F}_2 \arrow[r, hook, "\delta"] & H^1(G_K, V_0) \arrow[r, "\phi"] & H^1(G_K, V)
\end{tikzcd} \tag{5.12}$$

In this way the map

$$\phi \colon H^1(G_K, V_0) \to H^1(G_K, V) \tag{5.13}$$

is injective if and only if $\overline{\rho}(G_K)$ is C_1 or C_3.

To compute the value of the connecting homomorphism δ on $1 \in \mathbb{F}_2$, in the C_2 and S_3 cases, take $\mathbf{R} \in V \backslash V_0$ and define

$$w(\sigma) = {}^{\sigma}\mathbf{R} - \mathbf{R} \tag{5.14}$$

a cocycle representing $\delta(1) \in H^1(G_K, V_0)$. By construction w is in $B^1(G_K, V)$, giving us that $[w] = 0$ in $H^1(G_K, V)$.

Now, again by construction, the image of $\mathbb{F}_2$ in $H^1(G_K, V_0)$ is always generated by the class $[w]$ where, as was saw in (5.12), it is the trivial class in the cases C_1 and C_3. Therefore, for all four possible images, we have an injective map

$$\tilde{H}_1(G_K, V_0) := \frac{H^1(G_K, V_0)}{\langle [w] \rangle} \hookrightarrow H^1(G_K, V) \tag{5.15}$$

and our cocycle μ given by (5.3) determines a well-defined class $[\mu]$ in $\tilde{H}_1(G_K, V_0)$.

5.2 The cohomology class $[\mu]$ in $\tilde{H}_1(G_K, V_0)$.

So far we have shown that the obstruction when lifting an isogeny modulo 2^k between ρ_1 and ρ_2 to an isogeny modulo 2^{k+1} is represented by a cocycle μ whose class is a well-defined element of $\tilde{H}_1(G_K, V_0)$. Now we proceed to give a full description and properties of this cohomology class. We start by proving the following lemma.

Lemma 5.2.1. *The class $[w]$ is contained in $H^1(G_K, V_1)$.*

Proof. Let $[w]$ be the class represented by (5.14). We can observe that $w(\sigma)$ is always in V_1. Let $\overline{\rho}(\sigma)$ be in $\overline{\rho}(G_K)$ then

(a) if $\overline{\rho}(\sigma) \in \{\mathbf{I}, \mathbf{R}, \mathbf{R}^2\}$, then ${}^{\sigma}\mathbf{R} = \mathbf{R}$ and hence ${}^{\sigma}\mathbf{R} - \mathbf{R} = 0$,

(b) if $\overline{\rho}(\sigma) \notin \{\mathbf{I}, \mathbf{R}, \mathbf{R}^2\}$, then ${}^{\sigma}\mathbf{R} = \mathbf{R} + \mathbf{I}$ and hence ${}^{\sigma}\mathbf{R} - \mathbf{R} = \mathbf{I}$.

□

By the previous lemma this defines

$$\tilde{H}_1(G_K, V_1) := \frac{H^1(G_K, V_1)}{\langle [w] \rangle}. \tag{5.16}$$

Then, combining (5.15) and (5.16), we get that

$$\tilde{H}_1(G_K, V_0) \cong \tilde{H}_1(G_K, V_1) \oplus H^1(G_K, V_2),$$

which translates into the following lemma.

Lemma 5.2.2.

$$\frac{H^1(G_K, V_0)}{\langle [w] \rangle} \cong \frac{H^1(G_K, V_1)}{\langle [w] \rangle} \oplus H^1(G_K, V_2)$$

In this way, by the previous lemma, we have that

$$[\mu] = [\mu_1] + [\mu_2].$$

Also, it is not difficult to see that, the action of G_K on V_1 is trivial: by direct calculations, for $\mathbf{A}$ in V_1, we have that ${}^{\sigma}\mathbf{A} = \mathbf{A}$.

Observe that by standard Galois cohomology theory (see $[[4], pp.103-106]$) we have

$$H^1(G_K, V_1) \cong \mathrm{Hom}(G_K, \mathbb{F}_2) \cong \frac{K^*}{(K^*)^2}. \tag{5.17}$$

The following lemma shows that under this isomorphism, the class $[w]$ corresponds to a $\Delta \in K^*$.

Lemma 5.2.3.

1. *Under (5.17), the class $[w] \in H^1(G_K, V_1)$ maps to the class of $\Delta \in \frac{K^*}{(K^*)^2}$. Hence*

$$\begin{aligned}\frac{H^1(G_K, V_1)}{\langle [w] \rangle} &\cong \frac{\mathrm{Hom}(G_K, \mathbb{F}_2)}{\langle \Delta \rangle} \\ &\cong \frac{K^*}{\langle (K^*)^2, \Delta \rangle}.\end{aligned}$$

2. *In particular, when the image of $\overline{\rho}(G_K)$ is either C_3 or C_1, we have*

$$\tilde{H}_1(G_K, V_1) = H^1(G_K, V_1).$$

Proof.

1. We need to show for $\sigma \in G_K$ that $\sigma(\sqrt{\Delta}) = \sqrt{\Delta} \Leftrightarrow w(\sigma) = 0$. But $w(\sigma) = {}^{\sigma}\mathbf{R} - \mathbf{R}$, so $w(\sigma) = 0 \Leftrightarrow \sigma \in C_3$, while $\sigma(\sqrt{\Delta}) = \sqrt{\Delta} \Leftrightarrow \sigma \in C_3$ by Galois theory.

2. In these cases we have that $\Delta \in (K^*)^2$ and so $[w]$ is trivial.

□

5.3 Proving $[\mu] = 0$.

Our objective from here until the end of the chapter is to find sufficient conditions which imply that $[\mu] = 0$. The reason of this objective is given in the following result.

Proposition 5.3.1. *If the class $[\mu]$ in $\tilde{H}_1(G_K, V_0)$ is zero, then ρ_1 and ρ_2 are conjugate modulo 2^{k+1}.*

Proof. Suppose $[\mu] = 0$, then there exists $\mathbf{B}$ in V such that $\mu(\sigma) = {}^{\sigma}\mathbf{B} - \mathbf{B}$. Let $\mathbf{U} \equiv \mathbf{I} + 2^k\mathbf{B} \pmod{2^{k+1}}$ and $\mathbf{U}^{-1} \equiv \mathbf{I} - 2^k\mathbf{B} \pmod{2^{k+1}}$ be matrices in $\mathrm{GL}_2(\mathbb{Z}_2)$, and recall from (5.2) that $\rho_2(\sigma) = (\mathbf{I} + 2^k\mu(\sigma))\rho_1(\sigma)$. So,

$$\begin{aligned}
\rho_2(\sigma) &\equiv (\mathbf{I} + 2^k({}^{\sigma}\mathbf{B} - \mathbf{B}))\rho_1(\sigma) && \pmod{2^{k+1}}\\
&\equiv (\mathbf{I} + 2^k(\overline{\rho}(\sigma)\,\mathbf{B}\,\overline{\rho}(\sigma)^{-1} - \mathbf{B})\rho_1(\sigma) && \pmod{2^{k+1}}\\
&\equiv \rho_1(\sigma) + 2^k(\overline{\rho}(\sigma)\,\mathbf{B} - \mathbf{B}\,\overline{\rho}(\sigma)) && \pmod{2^{k+1}}
\end{aligned}$$

then

$$\begin{aligned}
\mathbf{U}\,\rho_1(\sigma)\,\mathbf{U}^{-1} &\equiv (\mathbf{I} + 2^k\mathbf{B})\rho_1(\sigma)(\mathbf{I} - 2^k\mathbf{B}) && \pmod{2^{k+1}}\\
&\equiv \rho_1(\sigma) + 2^k(\mathbf{B}\,\overline{\rho}(\sigma) - \overline{\rho}(\sigma)\,\mathbf{B}) && \pmod{2^{k+1}}\\
&\equiv \rho_2(\sigma) && \pmod{2^{k+1}}
\end{aligned}$$

therefore

$$\rho_2(\sigma) \equiv \mathbf{U}\,\rho_1(\sigma)\,\mathbf{U}^{-1} \pmod{2^{k+1}}$$

which proves the proposition. □

We aim to prove $[\mu] = 0$ by proving separately that $[\mu_1] = 0$ and $[\mu_2] = 0$. We will proceed by diving the cases as in the possible four images that the residual representation $\overline{\rho}$ can have, S_3, C_3, C_2 and C_1.

5.4 Case S_3: proving $[\mu] = 0$.

We start this section by assuming that the residual representation $\overline{\rho}$ has image S_3. This mean that there is a cubic monic irreducible polynomial $f(x) \in K[x]$ which defines the S_3 extension L/K where its discriminant is not a square.

5.4.1 $[\mu_1] = 0$.

Now suppose that $[\mu_1] \neq 0$. Then, by Lemma 5.2.3, there exists $\alpha \in K^*/\left\langle (K^*)^2, \Delta \right\rangle$ such that $[\mu_1]$ corresponds to the extension $K(\sqrt{\alpha})/K$ as follows: define

$$\mu_1^* \colon G_K \mapsto \{\pm 1\}$$
$$\mu_1^*(\sigma) = \begin{cases} 1 & \text{if } \sigma(\sqrt{\alpha}) = \sqrt{\alpha} \\ -1 & \text{if } \sigma(\sqrt{\alpha}) = -\sqrt{\alpha}. \end{cases}$$

In this correspondence, for $\sigma = \mathrm{Frob}_{\mathfrak{p}}$, we have that

$$\mu_1(\sigma) = \mathbf{0} \Leftrightarrow \mathfrak{p} \text{ splits in } K(\sqrt{\alpha}) \Leftrightarrow \mu_1^*(\sigma) = 1 \tag{5.18}$$
$$\mu_1(\sigma) = \mathbf{I} \Leftrightarrow \mathfrak{p} \text{ is inert in } K(\sqrt{\alpha}) \Leftrightarrow \mu_1^*(\sigma) = -1.$$

Since the class $[\mu]$ is unramified outside the finite set of primes S we have that $\alpha \in K(S,2)/\left\langle \Delta \right\rangle$. Hence there are only finitely many possibilities for α and hence for $[\mu_1]$.

Lemma 5.4.1. *If $\alpha \neq 1$ then $K(\sqrt{\alpha}) \nsubseteq L$.*

Proof. The only quadratic subfield of L is $K(\sqrt{\Delta})$. □

Now we relate the value of $\mu_1(\sigma)$ to the map φ defined earlier by (5.1) which will lead us to a congruence of traces modulo 2^{k+1}.

Proposition 5.4.2. *Let $\sigma \in G_K$,*

(a) if $\overline{\rho}(\sigma)$ has order 3, then

$$\mu_1(\sigma) = \mathbf{0} \Leftrightarrow \varphi(\sigma) = 0,$$

(b) if $\overline{\rho}(\sigma)$ has order 2, then

$$\mu_2(\sigma) = \mathbf{0} \Leftrightarrow \varphi(\sigma) = 0.$$

Observe that if $\overline{\rho}(\sigma)$ has order 1 then, by (5.5), $\varphi(\sigma) = 0$.

Proof.

(a) Replacing σ by σ^{-1} if necessary, we can assume that $\overline{\rho}(\sigma) = \mathbf{R} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$\begin{aligned} \mu_1(\sigma) = \mathbf{0} &\Leftrightarrow \mu(\sigma) = \mu_2(\sigma) \\ &\Leftrightarrow \mu(\sigma) \in V_2 \\ &\Leftrightarrow \operatorname{tr}(\mu(\sigma)\,\mathbf{R}) = 0 \\ &\Leftrightarrow \operatorname{tr}(\mu(\sigma)\overline{\rho}(\sigma)) = 0 \\ &\Leftrightarrow \operatorname{tr}(\rho_1(\sigma)) \equiv \operatorname{tr}(\rho_2(\sigma)) \pmod{2^{k+1}} \\ &\Leftrightarrow \varphi(\sigma) = 0. \end{aligned}$$

(b) This proof follows the same logic that the proof of part (a).

□

Now for σ in G_K such that $\overline{\rho}(\sigma)$ has order 3, which exists in the S_3 and C_3 cases, we have that

$$\begin{aligned} \mu_1(\sigma) = \mathbf{0} &\Leftrightarrow \operatorname{tr}(\rho_1(\sigma)) \equiv \operatorname{tr}(\rho_2(\sigma)) \pmod{2^{k+1}} \\ \mu_1(\sigma) = \mathbf{I} &\Leftrightarrow \operatorname{tr}(\rho_1(\sigma)) \not\equiv \operatorname{tr}(\rho_2(\sigma)) \pmod{2^{k+1}}. \end{aligned} \tag{5.19}$$

In order to reach a contradiction, for each of the finitely many possible non-trivial values of α, we will show the existence of a prime $\mathfrak{p}$ of K not in S such that $\overline{\rho}(\mathrm{Frob}_{\mathfrak{p}})$ has order 3 and $\mu_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathbf{I}$. For such a prime $\mathfrak{p}$ if we are able to show that $\varphi(\mathrm{Frob}_{\mathfrak{p}}) = 0$, for example, by checking that $\operatorname{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \operatorname{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$, then this proves that the class $[\mu_1]$ is not represented by α.

Theorem 5.4.3. *Suppose that the residual image $\overline{\rho}(G_K)$ is isomorphic to either C_3 or S_3 with residual splitting field L defined by the irreducible cubic polynomial $f(x) \in K[x]$. For each of the finitely many non-trivial elements α of $K(S,2)/\langle\Delta\rangle$, let $\mathfrak{p}_\alpha$ be a prime of K with $\mathfrak{p}_\alpha \notin S$ satisfying*

- (a) *$f(x)$ is irreducible modulo $\mathfrak{p}_\alpha$,*
- (b) *$x^2 - \alpha$ is irreducible modulo $\mathfrak{p}_\alpha$.*

If $\operatorname{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}_\alpha})) = \operatorname{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}_\alpha}))$ *for all α, then $[\mu_1] = 0$.*

Proof. By contradiction, suppose that the class $[\mu_1]$ is not trivial. Let α be the representative of the class, $\mathfrak{p}_\alpha$ be the prime satisfying (a) and (b), and take $\sigma_{\alpha_{\mathfrak{p}}} = \mathrm{Frob}_{\mathfrak{p}_\alpha}$. Then we have that $\overline{\rho}(\mathfrak{p}_\alpha)$ has order 3 and $\mu_1(\mathfrak{p}_\alpha) = \mathbf{I}$. By Proposition 5.4.2 these imply that $\phi(\mathfrak{p}_\alpha) \neq 0$, which contradicts the equality of the traces of $\rho_j(\sigma)$ stated before. □

Remark 5.4.4. *Infinitely many such primes $\mathfrak{p}_\alpha$ exist since, by Lemma 5.4.1, the extensions of L and $K(\sqrt{\alpha})$ are disjoint.*

5.4.2 $[\mu_2] = 0$.

Now that we have shown how to establish that $[\mu_1] = 0$ we would like to find conditions to prove that the class $[\mu_2]$ is equal to zero. To do this, we start by observing that $[\mu_1] = 0$ implies that

$$\begin{aligned} [\mu] &= [\mu_1] + [\mu_2] \\ &= [\mu_2] \in H^1(G_K, V_2). \end{aligned} \tag{5.20}$$

By standard cohomology theory(see [13] or [8]), consider the semidirect product

$$\begin{aligned} V_2 \rtimes \overline{\rho}(G_K) &\cong (C_2 \times C_2) \rtimes S_3 \\ &\cong S_4 \end{aligned} \tag{5.21}$$

with operation law

$$(A, B)(C, D) = (A + BCB^{-1}, BD)$$

which give us a homomorphism

$$\begin{aligned} \phi \colon G_K &\to V_2 \rtimes \overline{\rho}(G_K) \\ \sigma &\mapsto (\mu_2(\sigma), \overline{\rho}(\sigma)). \end{aligned}$$

Defining

$$\begin{aligned} \tau \colon V_2 \rtimes \overline{\rho}(G_K) &\to \mathbb{F}_2 \\ (A, B) &\mapsto \operatorname{tr}(AB) \pmod 2, \end{aligned}$$

we get a diagram

$$\begin{tikzcd} G_K \arrow[r, "\varphi"] \arrow[dr, "\phi"'] & \mathbb{F}_2 \\ & V_2 \rtimes \overline{\rho}(G_K) \arrow[u, "\tau"'] \end{tikzcd}$$

that commutes. Then by (5.20) we have that

$$\begin{aligned} \varphi(\sigma) &= (\tau \circ \phi)(\sigma) \\ &= \operatorname{tr}(\mu(\sigma)\overline{\rho}(\sigma)) \\ &= \operatorname{tr}(\mu_2(\sigma)\overline{\rho}(\sigma)). \end{aligned}$$

In [5] it is shown how the non-trivial classes in $H^1(G_K, V_2)$ correspond to S_4 extensions of K with cubic resolvent L. So, suppose that $[\mu_2] \neq 0$. Then, there is an extension of K, named M, with Galois group S_4, given by a quartic polynomial g whose cubic resolvent is f, satisfying

$$\begin{tikzcd}
& M & & \\
& & L \arrow[ul, "4"'] & \\
F \arrow[uur, "6"] & & & \\
& L_1 \arrow[uur, "2"] & L_2 \arrow[uu, "2"] & L_3 \arrow[uul, "2"'] \\
& K \arrow[uul, "4"] \arrow[u, "3"] \arrow[ur, "3"] \arrow[urr, "3"'] & &
\end{tikzcd} \tag{5.22}$$

where L_i is given by adjoining one root of $f(x)$ to K, L is the splitting field of $f(x)$ and F is given by adjoining one root of $g(x)$ to K. Also there exist conjugates $\alpha_i \in L_i^*$, with $i \in \{1, 2, 3\}$, such that

$$M = L(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_3}),$$

where $N_{L_i/K}(\alpha_i) = \alpha_1\alpha_2\alpha_3 \in (K^*)^2$. Without loss of generality, set $i = 1$ and consider

$$H := \ker\left(\frac{L_1^*}{(L_1^*)^2} \xrightarrow{N} \frac{K^*}{(K^*)^2}\right) \tag{5.23}$$

where $N = N_{L_1/K}$ is the norm map. Then we have the following proposition.

Proposition 5.4.5. *There is a bijection between*

(1) *$H^1(G_K, V_2)$,*

(2) *S_4 extensions M/K containing L allowing $M = L$ as a degenerative case when $\alpha = 1$, and*

(3) *H.*

Proof. This proposition is implicit in [5] and we fill the details in here.
(1) $\Rightarrow$ (2). Let $[\xi] \in H^1(G_K, V_2)$ and consider the restriction of ξ to $G_L = \mathrm{Gal}(\overline{K}/L)$,

i.e.,

$$\begin{aligned}\phi\colon H^1(G_K, V_2) &\to H^1(G_L, V_2)\\ [\xi] &\mapsto \xi|_{G_L}.\end{aligned}$$

Recall that the action of G_K on V_2 is via its quotient $\mathrm{Gal}(L/K)$ which acts on V_2 by permuting its non-trivial elements. When we restrict to G_L this action, by definition, is trivial on V_2 where we get that

$$\begin{aligned}H^1(G_L, V_2) &= \hom(G_L, V_2)\\ &= \hom(G_L, C_2 \times C_2)\end{aligned}$$

and when $[\xi] \neq 0$ we have that

$$\xi|_{G_L} \colon G_L \to V_2$$

is in fact surjective ([5]). Denoting the fixed field of $\ker(\xi|_{G_L})$ by M, we get that if $[\xi] \neq 0$ then M is a V_2 extension of L, which is Galois over K and $[M : L] = 4$. The extension M of L can be written as

$$M = L(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_3})$$

where $\alpha_1 \in L_1$ is a cubic extension over K, with α_2 and α_3 being conjugates of α_1 and

$$N_{L_1/K}(\alpha_1) = \alpha_1\alpha_2\alpha_3 \in (K^*)^2.$$

Moreover

$$\begin{aligned}\mathrm{Gal}(M/K) &\cong V_2 \rtimes \mathrm{Gal}(L/K)\\ &\cong S_4\end{aligned} \tag{5.24}$$

is the splitting field of a quartic polynomial g.

(2) ⇒ (1). On the other way around, let L_1 be a cubic extension of K obtained by adjoining a root of f to K. Taking $\alpha_1 \in L_1$ such that $\alpha_1 \in H$ define

$$M = L(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_3}),$$

which is biquadratic over L, Galois over K and corresponds to the splitting field of a quartic g. For each $\sigma \in G_K$ we have that $\alpha_i^\sigma = \sigma(\alpha_i) = \alpha_{\overline{\sigma}(i)}$ means the permutations of α_i, where $\overline{\sigma} \in S_3$. Fix one $\sqrt{\cdot}$ of each α_i arbitrary with the condition that $\sqrt{\alpha_1}\sqrt{\alpha_2}\sqrt{\alpha_3} = C$ where $N_{L_1/K}(\alpha_1) = C^2$ and $C \in K^*$. Now, we can define characters

$$\varepsilon_i \colon G_K \to \{\pm 1\}$$

such that

$$(\sqrt{\alpha_i})^{\sigma} = \varepsilon_i(\sigma)\sqrt{\alpha_{\overline{\sigma}(i)}} \tag{5.25}$$

with $\varepsilon_1(\sigma)\varepsilon_2(\sigma)\varepsilon_3(\sigma) = 1$. Then the triplet

$$(\varepsilon_1(\sigma), \varepsilon_2(\sigma), \varepsilon_3(\sigma)) \in \{(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)\}$$

defines a map

$$\begin{aligned} \xi \colon G_K &\to \{(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)\} \\ \sigma &\mapsto (\varepsilon_1(\sigma), \varepsilon_2(\sigma), \varepsilon_3(\sigma)) \end{aligned}$$

from where we can see that

$$\{(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)\} \cong V_2. \tag{5.26}$$

Moreover, S_3 acts on (5.26) by permuting their coordinates, and a short calculation show that the isomorphism is an isomorphism of S_3-modules. Now, observe the following:

(1) ξ is a cocycle: first observe that our superscripts denotes a left action on $\sqrt{\alpha_i}$, so we will have that $(\sqrt{\alpha_i})^{\sigma_1\sigma_2}$ means $(\sqrt{\alpha_i}^{\sigma_2})^{\sigma_1}$. In this we have that

$$\begin{aligned} \varepsilon_i(\sigma_2)\varepsilon_{\sigma_2(i)}(\sigma_1) &= \frac{(\sqrt{\alpha_i})^{\sigma_2}}{\sqrt{\alpha_i}} \cdot \frac{(\sqrt{\alpha_{\sigma_2(i)}})^{\sigma_1}}{\sqrt{\alpha_{\sigma_2(i)}}} \\ &= \frac{(\sqrt{\alpha_{\sigma_2(i)}})^{\sigma_1}}{\sqrt{\alpha_i}} \\ &= \frac{(\sqrt{\alpha_i}^{\sigma_2})^{\sigma_1}}{\sqrt{\alpha_i}} \\ &= \varepsilon_i(\sigma_1\sigma_2). \end{aligned}$$

Therefore

$$\begin{aligned} \xi(\sigma_1\sigma_2) &= (\varepsilon_1(\sigma_1\sigma_2), \varepsilon_2(\sigma_1\sigma_2), \varepsilon_3(\sigma_1\sigma_2)) \\ &= (\varepsilon_1(\sigma_2)\varepsilon_{\sigma_2(1)}(\sigma_1), \varepsilon_2(\sigma_2)\varepsilon_{\sigma_2(2)}(\sigma_1), \varepsilon_3(\sigma_2)\varepsilon_{\sigma_2(3)}(\sigma_1)) \\ &= \xi(\sigma_2)\xi(\sigma_1)^{\sigma_2}. \end{aligned}$$

(2) Changing the choices of $\sqrt{\alpha_i}$ changes the cocycle ξ by a coboundary: let $t_i\sqrt{\alpha_i}$ with $t_i = \pm 1$ and $t_1t_2t_3 = 1$ be another choice and take $\mathbf{t} = (t_1, t_2, t_3)$. Then we

have that

$$\frac{(t_i\sqrt{\alpha_i})^\sigma}{t_i\sqrt{\alpha_i}} = \frac{t_i^\sigma(\sqrt{\alpha_i})^\sigma}{t_i\sqrt{\alpha_i}}$$
$$= \frac{t_i}{t_i^\sigma}\varepsilon_i(\sigma), \quad \text{since } \frac{t_i^\sigma}{t_i} = \frac{t_i}{t_i^\sigma}.$$

In this way, changing $\sqrt{\alpha_i}$ to $t_i\sqrt{\alpha_i}$ will change ξ into a new one, ξ', such that $\xi'(\sigma) = \xi(\sigma)\mathbf{t}(\mathbf{t}^\sigma)^{-1}$.

(3) Changing α_i to $\alpha_i\beta_i^2$ ($\beta_i \in L_1^*$) does not change ξ at all: this is due to the fact that we are working modulo squares.

Finally as an exercise in Galois theory we can prove that (2) ⇔ (3).

□

In our case, we have representations that are unramified outside S, so we can add this condition to have a bijection between

(1) classes $[\xi] \in H^1(G_K, V_2)$ which are unramified outside S,

(2) the S_4 extensions M/K unramified outside S containing L allowing $M = L$ as a degenerative case when $\alpha = 1$, and

(3) the $\alpha \in H(S)$ such that $L_1(\sqrt{\alpha})/L$ is unramified outside S, where

$$H(S) := \ker(L_1(S,2) \xrightarrow{N} K(S,2)).$$

In the following proposition we show how to construct a quartic polynomial whose splitting field is S_4, given by an element $\alpha \in H(S)$.

Proposition 5.4.6. *Let α be an element in $H(S)$. Then α has characteristic polynomial $x^3 - Ax^2 + Bx - C^2 \in K[x]$ and the quartic (up to translation and scaling) related to a class in $H^1(G_K, V_2)$ is given by*

$$g(x) = x^4 - 2Ax^2 + 8Cx + A^2 - 4B.$$

Proof. This proposition is implicit in [5].

Let $\alpha \in H(S)$. Then its minimal polynomial is given by

$$(x-\alpha)(x-\alpha')(x-\alpha'') = x^3 - (\alpha+\alpha'+\alpha'')x^2 + (\alpha\alpha'+\alpha\alpha''+\alpha'\alpha'')x - \alpha\alpha'\alpha''$$
$$= x^3 - Ax^2 + Bx - C^2$$

where $A = \alpha+\alpha'+\alpha'', B = \alpha\alpha'+\alpha\alpha''+\alpha'\alpha'', C = \alpha\alpha'\alpha'' \in K^*$. (Since that is the minimal polynomial for α we have that A, B, C^2 belong to K and C belongs to K^* since $N(\alpha)$ is a square.)

A suitable quartic g looks like

$$g(x) = x^4 + cx^2 + dx + e.$$

Choosing $a = 1$ and $b = 0$ from the equation (3.3) in [5]. Using the equations in page 73 of [5] we get that:

$$\begin{aligned} A &= 3b^2 - 8ac \\ &= -8c \end{aligned}$$

then

$$c = -\frac{A}{8}.$$

Also

$$\begin{aligned} C &= b^3 + 8a^2d - 4abc \\ &= 8d \end{aligned}$$

then

$$d = \frac{C}{8}.$$

Moreover

$$\begin{aligned} B &= 3b^2 - 16ab^2c + 16a^2c^2 + 16a^2bd - 64a^3e \\ &= 16c^2 - 64e \end{aligned}$$

then

$$\begin{aligned} e &= \frac{16c^2 - B}{64} \\ &= \frac{c^2}{4} - \frac{B}{64} \\ &= \frac{A^2 - 4B}{256}. \end{aligned}$$

Therefore, after scaling by $4x$, the quartic g becomes

$$g(x) = x^4 - 2Ax^2 + 8Cx + A^2 - 4B.$$

□

Thus, by Proposition 5.4.5 and Proposition 3.2 (1) in [5] we have

$$\begin{aligned} [\xi] = 0 &\Leftrightarrow g(x) \text{ has a root in } K \\ [\xi] \neq 0 &\Leftrightarrow g(x) \text{ is irreducible.} \end{aligned}$$

Let's go back to analyse (5.24). In S_4 there are 24 elements and we can relate these elements into the elements of $V_2 \rtimes \overline{\rho}(G_K)$. Since $[\mu_2] \neq 0$ we have that $\mu_2(\sigma) \neq \mathbf{0}$ for σ in G_K. Then

$$\mu_2(\sigma) \in \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \tag{5.27}$$

and by direct calculations

$$\begin{gathered} \operatorname{tr}(\mu_2(\sigma)\overline{\rho}(\sigma)) = 1 \Leftrightarrow (\mu_2(\sigma), \overline{\rho}(\sigma)) \text{ lies in} \\ \left\{ \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right), \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right), \left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right), \right. \\ \left. \left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right), \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right), \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right) \right\}. \end{gathered} \tag{5.28}$$

These calculations show that these six elements have order 4 and correspond to the six 4-cycles of S_4. We only have $\varphi(\sigma) \neq 0$ for the 4-cycles.

In order to get a contradiction, using Proposition 5.4.6, we need to find a finite set of quartics g whose splitting fields gives all S_4 extensions of K containing L. For each quartic g, find a prime $\mathfrak{p}_g$ such that g is irreducible modulo $\mathfrak{p}_g$. Then check that the traces agree on the Frobenius of all these $\mathfrak{p}_g$.

Theorem 5.4.7. *Suppose that the image of the residual representation $\overline{\rho}$ is isomorphic to S_3. For each of the finitely many quartics g found by Proposition 5.4.6, let $\mathfrak{p}_g \notin S$ be a prime of K such that g is irreducible modulo $\mathfrak{p}_g$. If $\operatorname{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}_g})) = \operatorname{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}_g}))$, then $[\mu_2]$ is not represented by g.*

Proof. By contradiction, suppose that the class $[\mu_2]$ is not trivial. Let ξ be the representative of the class, g be the quartic found using Proposition 5.4.6, $\mathfrak{p}_g$ be the prime such that g is irreducible modulo $\mathfrak{p}_g$ and take $\sigma_\xi = \mathrm{Frob}_{\mathfrak{p}}$. Thus σ_ξ corresponds to a 4-cycle as in (5.28). This implies that $\phi(\sigma_\xi) \neq 0$, which contradicts the equality of the traces of $\rho_j(\sigma)$ stated before. □

5.5 Case C_3: proving $[\mu] = 0$.

Assume that the residual representation $\overline{\rho}$ has image C_3. This mean that there is a cubic monic irreducible polynomial $f(x) \in K[x]$ which defines the C_3 extension L/K

of $\overline{\rho}$, where its discriminant is a square (Section 3.2.1).

To obtain the a of primes $\mathfrak{p}$ not in S for which we need to test $\mathrm{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ to determine whether $[\mu_1] = 0$, we just need to apply Theorem 5.4.3; the reason is simple, as we saw before in Section 5.4.1, the theorem is valid for both S_3 and C_3 cases.

On the other hand, to find a set to determine whether $[\mu_2] = 0$, first we have to take a $\mathfrak{p} \notin S$ such that $\mu_2(\mathrm{Frob}_{\mathfrak{p}}) \neq \mathbf{0}$. Then the tuple $(\mu_2(\mathrm{Frob}_{\mathfrak{p}}), \overline{\rho}(\mathrm{Frob}_{\mathfrak{p}}))$ would correspond to a 4-cycle in $V_2 \rtimes \overline{\rho}(G_K)$. Thus we determine that the class of μ_2 is trivial by checking the trace condition as in theorems 5.4.3 and 5.4.7.

Unfortunately this cannot happen in this case: since $\overline{\rho}(G_K) \cong C_3$ we have that (5.21) becomes

$$\begin{aligned} V_2 \rtimes \overline{\rho}(G_K) &\cong (C_2 \times C_2) \rtimes C_3 \\ &\cong A_4 \end{aligned} \tag{5.29}$$

which does not contains any 4-cycles. Instead we "translate" our problem by using the following theorem:

Theorem 5.5.1. *Let $\rho_1, \rho_2 \colon G \to \mathrm{GL}_d(\mathbb{Z}_p)$ be two representations of a group G. Assume that G has a normal subgroup H such that*

(a) H has finite index n in G, where n is coprime to $2(p-1)$,

(b) $\rho_1|_H \sim \rho_2|_H$, and both are absolutely irreducible.

Then $\rho_1 \sim \rho_2$.

Proof. This proof is due to Professor Cremona.

From *(b)* we can replace ρ_2 by a conjugate and hence assume that $\rho_1|_H = \rho_2|_H$. Now we will show that $\rho_1 = \rho_2$.

Let $g \in G$. Since $gHg^{-1} = H$, for all $h \in H$ we have

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

Since $\rho_1(h) = \rho_2(h)$, this implies that $\rho_1(g)^{-1}\rho_2(g)$ commutes with $\rho_1(h)$ for all $h \in H$. Since $\rho_1|_H$ is absolutely irreducible, this implies that $\rho_1(g)^{-1}\rho_2(g)$ is a scalar, say $\rho_2(g) = a\rho_1(g)$ with $a \in \mathbb{Z}_p^*$. (Note: not just in $\mathbb{Q}_p^*$ since taking determinants shows that $a^d \in \mathbb{Z}_p^*$, so $a \in \mathbb{Z}_p^*$.) Finally, since $g^n \in H$, it follows that $a^n = 1$, and condition *(a)* implies that $a = 1$ since the roots of unity in $\mathbb{Z}_p^*$ all have order dividing $p-1$ (or dividing 2 when $p = 2$). Hence $\rho_1(g) = \rho_2(g)$ for all $g \in G$ as claimed.

□

Applying this with $p = d = 2$, $n = 3$ give the following corollary:

Corollary 5.5.2. *Let $\rho_1, \rho_2 \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be two Galois representations such that $\overline{\rho}_1 = \overline{\rho}_2$ and that the common splitting field L of $\overline{\rho}_1, \overline{\rho}_2$ is cyclic of order 3. If $\rho_1|_{G_L} \sim \rho_2|_{G_L}$ then $\rho_1 \sim \rho_2$.*

First observe that

$$\begin{tikzcd}
\overline{K} \arrow[d, dash, "\} G_L"] \\
L \arrow[d, dash, "C_3 \{"'] \\
K
\end{tikzcd}$$

where $G_L = \mathrm{Gal}(\overline{K}/L)$. Then by Theorem 5.5.1 we can reduce from $\overline{K}/K$ to $\overline{K}/L$. Instead of considering the whole G_K we can just consider the following diagram

$$\begin{tikzcd}
\rho_i \colon G_K \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_2) \\
G_L \arrow[u, hook] \arrow[ur] &
\end{tikzcd}$$

and then we will have that

$$\rho_i \colon G_L \to \mathrm{GL}_2(\mathbb{Z}_2)$$

where $\overline{\rho}(\mathrm{Gal}(\overline{K}/L)) \cong C_1$. Now we may apply Livné's method: construct a non-cubic set of primes T not containing any prime in $S_L = \{\mathfrak{p}$ primes of L above a primes in $S\}$. We know that $\det(\rho_1(\sigma)) = \det(\rho_2(\sigma)) \pmod 2$ for all $\sigma \in G_K$ and since $\overline{\rho}(\sigma) \equiv \mathbf{I} \pmod 2$ we have that $\mathrm{tr}(\overline{\rho}(\sigma)) \equiv 0 \pmod 2$ for all $\sigma \in G_K$. Take K_S as the compositum of all quadratic extension of K. If we have that $\{\mathrm{Frob}_{\mathfrak{p}} |_{\mathrm{Gal}(K_S/K)}\}_{\mathfrak{p} \in T}$ is non-cubic and that for all $\mathfrak{p} \in T$ we have that $\mathrm{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ and $\det(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \det(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ then, by Theorem 2.4.3, $\rho_1|_{G_L}$ and $\rho_2|_{G_L}$ isogenous up to semisimplification. Therefore, by Corollary 5.5.2, ρ_1 and ρ_2 are isogenous.

5.6 Cases C_2 and C_1: proving $[\mu] = 0$.

In this last case, we assume that the residual image of $\overline{\rho}$ is C_1 or C_2. To determine whether ρ_1 and ρ_2 are isogenous, we apply Livné's method: construct a non-cubic set of primes T not containing any prime in S. We know that $\det(\rho_1(\sigma)) = \det(\rho_2(\sigma)) \pmod 2$ for all $\sigma \in G_K$ and since $\overline{\rho}(\sigma) \equiv \mathbf{I} \pmod 2$ we have that $\mathrm{tr}(\overline{\rho}(\sigma)) \equiv 0 \pmod 2$ for all $\sigma \in G_K$. Take K_S as the compositum of all quadratic extension of K. If we have that $\{\mathrm{Frob}_{\mathfrak{p}} |_{\mathrm{Gal}(K_S/K)}\}_{\mathfrak{p} \in T}$ is non-cubic and that for all $\mathfrak{p} \in T$ we have that $\mathrm{tr}(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ and $\det(\rho_1(\mathrm{Frob}_{\mathfrak{p}})) = \det(\rho_2(\mathrm{Frob}_{\mathfrak{p}}))$ therefore, by Theorem 2.4.3, we have that ρ_1 and ρ_2 isogenous up to semisimplification.

Conclusion.

Using the methods of Chapter 4 we can check that $\rho_1 = \rho_2 \pmod 2$ up to isogeny. Moreover we can precisely determine their residual image. Unfortunately, if their residual image is not S_3 only a few ideas could have been applied to "eliminate" the obstruction that arises when lifting from modulo 2^k to modulo 2^{k+1}. So we ended up relying on Livné's non-cubic sets of primes and Theorem 2.4.3 to prove that ρ_1 and ρ_2 are isogenous up to semisimplification.

Bibliography

[1] Joël Bellaïche. Ribet's lemma, generalizations, and pseudocharacters. *Two lectures at the Clay Mathematical Institute Summer School, Honolulu, Hawaii*, 2009. 2.2

[2] Nancy Childress. *Class field theory*. Universitext. Springer, New York, 2009. 2.1, 2.1.1, 2.1.2

[3] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. 3.2.1

[4] Silverman J.H. Stevens G. Cornell, G., editor. *Modular forms and Fermat' last theorem*. Springer-Verlag, New York, 1997. 5.2

[5] J. E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.*, 31(1-2):71–87, 2001. Computational algebra and number theory (Milwaukee, WI, 1996). 5.4.2, 5.4.2, 5.4.2

[6] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original. 2.3.2

[7] The Sage Developers. *Sage Mathematics Software (Version 7.0.0)*, 2016. `http://www.sagemath.org`. 1

[8] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.*, 79(270):1145–1170, 2010. (document), 2.4, 5, 5.4.2

[9] V. Dokchitser and S. Anni. l-Adic Representations and their Associated Invariants. *ArXiv e-prints*, October 2014. 2.3.1

[10] Aggelos Koutsianas. Applications of S-unit Equations to the Arithmetic of Elliptic Curves. *PhD Thesis, University of Warwick*, 2016. 3.2.1, 1

[11] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp.*

Math., pages 247–261. Amer. Math. Soc., Providence, RI, 1987. (document), 1, 4, 2.4, 2.4.2, 2.4.3, 5

[12] Barry Mazur. How can we construct abelian Galois extensions of basic number fields? *Bull. Amer. Math. Soc. (N.S.)*, 48(2):155–209, 2011. 3

[13] Matthias Schütt. On the modularity of three Calabi-Yau threefolds with bad reduction at 11. *Canad. Math. Bull.*, 49(2):296–312, 2006. 5.4.2

[14] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968. 2.1.3, 2.3.6, 2.3.8, 2.3.2

[15] Jean-Pierre Serre. *Linear representations of finite groups.* Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. 2.3

[16] Jean-Pierre Serre. *Trees.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation. 2.2.1, 2.2.1

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009. 2.1