2019

Comparison of Three Dimensional Selfdual Representations by Faltings-Serre Method

Lian Duan

COMPARISON OF THREE DIMENSIONAL SELFDUAL REPRESENTATIONS BY FALTINGS-SERRE METHOD

A Dissertation Presented

by

LIAN DUAN

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

September 2019

Department of Mathematics and Statistics

COMPARISON OF THREE DIMENSIONAL SELFDUAL REPRESENTATIONS BY FALTINGS-SERRE METHOD

A Dissertation Presented

by

LIAN DUAN

Approved as to style and content by:

Siman Wong, Chair

David A. Mix Barrington, Member

Paul Gunnells, Member

Tom Weston, Member

Nathaniel Whitaker, Department Chair
Department of Mathematics and Statistics

DEDICATION

In memory of my grandfather, Qiao Lu

ACKNOWLEDGMENTS

Of many people to whom I would like to thank, first and foremost is my advisor, Professor Siman Wong. Throughout the past six years, as a graduate student I have been learning a lot from him, not only about mathematics itself but also about being a young mathematician. Without his infinitely patient guidance and encouragement, I can hardly imagine how to finish my Ph.D. project.

I am also very grateful to Professor Paul Gunnells, Professor Tom Weston and Professor David A. Mix Barrington for serving on my dissertation committee; and to Professor Paul Hacking and Professor Farshid Hajir for conversation and suggestions in algebraic geometry, representation theory and pro-p groups.

Also, I want to give my thanks to the Department of Mathematics and Statistics. Without the support from our department I have no chance to learn the realize my dream of learning the fantastic mathematics. Especially I should thank Professor Hans Johnston and Daniel Nichols for their support on the computational resource and coding technique.

I can hardly omit the warm help from my friends, including but not limited to: Dr. Zhijie Dong, Dr. Mei Duanmu, Dr. Jinchao Feng, Professor Dongchun Han, Tangxin Jin, Dr. Huy Le, Dr. Vy Nguyen, Professor Yuan Ren, Dr. Jie Wang, Dr. Meizhe Wang, Dr. Wanting Xie, Dr. Xueying Yu, Dr. Haitian Yue and Dr. Bo Zhao.

Finally but specially, I owe sincere thanks to my lover, Han Guo. She is the person who knows me best, who gave me the hand at the toughest moment in my life and who loves me all the time. I truly could not have asked for a better gift from the God in my life. I also want to thank the support from my family.

ABSTRACT

COMPARISON OF THREE DIMENSIONAL SELFDUAL REPRESENTATIONS BY FALTINGS-SERRE METHOD

SEPTEMBER 2019

LIAN DUAN

B.Sc., SICHUAN UNIVERSITY

M.Sc., SICHUAN UNIVERSITY

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Siman Wong

In this thesis, we prove that, a selfdual 3-dimensional Galois representation constructed by van Geemen and Top in [34] is isomorphic to a quadratic twist of the symmetric square of the Tate module of an elliptic curve. This is an application of our refinement of the Faltings-Serre method to 3-dimensional Galois representations with ground field not equal to $\mathbb{Q}$. The proof makes use of the Faltings-Serre method, ℓ-adic Lie algebra, and Burnside groups.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

INTRODUCTION

Since the Galois representations do not only reveal the information of the mysterious Galois group, but also play important role in the Langlands program, the study of Galois representations is one of the central objects in number theory and arithmeticians geometry. In this thesis, we concern the Galois representations studied by van Geemen and Top in [34]. Let K be a number field with ring of algebraic integers $\mathcal{O}_K$ and absolute Galois group G_K. For each pair $(a, s) \in K^2$ with $a \neq \pm 1$ and $s \neq 0$, consider the following elliptic surface parameterized by t

$$y^2 = x(x^2 + 2(s^2(a+1) + at^2)x + t^4)$$

and take $\mathcal{S}_{a,s}$ to be its projective closure. van Geemen and Top [34, § 2.4] consider a degree 4 cover of $\mathcal{S}_{a,s}$, denoted by $\mathcal{A}_{a,s}$. They then construct a selfdual 3-dimensional G_K representation $(V_\ell)_{a,s}$ by taking a subquotient of the transcendental part of the second étale cohomology of $\mathcal{A}_{a,s}$ [34, §5.1]. Based on experimental data, they conjecture that for every such pair (a, s), the representation $(V_\ell)_{a,s}$ is related to the symmetric square of the Tate module of an elliptic curve E defined over K or one of its quadratic extensions [34, §5.4]. Specifically, they conjecture that

$$s\delta(N_{K/\mathbb{Q}}(\mathfrak{p}))tr(F_\mathfrak{p}|(V_\ell)_{a,s}) = tr(F_\mathfrak{p}|Sym^2(T_E)), \tag{0.0.1}$$

where $Sym^2(T_E)$ is the symmetric square of the Tate module of E, $N_{K/\mathbb{Q}}$ is the norm, tr is the trace, $F_\mathfrak{p}$ is the Frobenius class corresponding to the prime ideal $\mathfrak{p}$ of the algebraic integer ring of K, and δ is a Dirichlet character.

Now let $K = \mathbb{Q}(\sqrt{-3})$, and let E be the elliptic curve defined by

$$Y^2 = X^3 + (\sqrt{-1} - 1)X^2 + \left(-\frac{\sqrt{-1}}{4} + \frac{\sqrt{-3}}{8} - \frac{1}{8}\right)X.$$

Take $V_\ell = (V_\ell)_{\sqrt{-3},0,1}$, and write $\theta_a(*) = \left(\frac{a}{*}\right)$ for the Kronecker symbol corresponding to the integer a. In this thesis we will prove the following theorem.

Theorem 0.0.1. *We have*

$$\theta_{-2} \otimes V_\ell \simeq Sym^2(T_E).$$

In particular, equation (0.0.1) *is true for all* $\mathfrak{p}$ *not dividing* 2.

Remark 0.0.1. Note that the elliptic curve E is not defined over K. But it is a K-curve (cf. section 5.1), and thus its Tate module can be descended to a G_K-representation.

Let K be a number field, and let M_λ be a finite extension of the ℓ-adic field $\mathbb{Q}_\ell$. Let $\rho_1, \rho_2 : G_K \to \mathrm{GL}_n(M_\lambda)$ be Galois representations unramified outside a finite set of primes. In the proof of the Mordell Conjecture, Faltings shows that we can test if ρ_1, ρ_2 are equivalent up to semisimplification by performing a finite calculation [13]. Serre [29] turns this into an effective tool, and Livné [21, thm. 4.3] improves this specifically for the case $n = 2$. Many researchers (including but not limited to Boston [3], Hulek, Kloosterman, Schütt [20], Schoen [27], Socrates, Whitehouse [31], Dieulefait, Guerberoff, Pacetti [11]) have successfully applied the Faltings-Serre method to study the modularity over $\mathbb{Q}$ or some imaginary quadratic fields. However, due to the limits of current hardware, there was no known application of the Faltings-Serre method when $n > 2$ and $K \neq \mathbb{Q}$.

In his work [14], Grenié finds an explicit bound of the norm of prime ideals such that the equivalence between ρ_1 and ρ_2 can be verified as long as they have the same traces for all Frobenius of unramified prime ideals with norm under this bound.

However, a direct application of Grenié's work to the setups of Theorem 0.0.1 leads to a bound that is too large to be verified.

In this work, we refine Grenié's criterion for 3-dimensional selfdual Galois representations in two aspects. First, for general selfdual representations, by studying the rank of the Lie algebras of their images we reduce the number of prime ideals that needed to be checked in Grenié's result (see Theorem 0.0.2). Second, suppose K is quadratic, and suppose $\mathrm{Gal}(K^{ur}_{2,\infty}(2)/K)$ is generated by two elements, where $K^{ur}_{2,\infty}(2)$ is the maximal pro-2 extension of K unramified outside 2 and ∞. We improve the bound (Theorem 0.0.3, Theorem 5.3.2) further by studying the structure of the Burnside group $B(2,4)$ (Example 3.0.3). As an application, we verify Theorem 0.0.1 with the improved bound from Theorem 0.0.3. In the following Table 1, we compare Grenié's criterion, our first improvement (Theorem 0.0.2) and our second improvement (Theorem 0.0.3) in the case of Theorem 0.0.1. In this table, we list the sizes of the sets T of prime ideals that are needed to check to prove Theorem 0.0.1, if the Extended Riemann Hypothesis (ERH) is assumed to find T, and the total time we spend to verify Theorem 0.0.1.

Methods	size of T	assume ERH	running time
By Grenié's criterion only[a]	cannot construct[a]		unknown
By first improvement only[a]			
By Grenié's criterion and structure of $\mathrm{Gal}(K^{ur}_{2,\infty}(2)/K)$[b]	$\#(T) \geq 7 \times 10^9$	yes	$>$ one year[c]
By first improvement and structure of $\mathrm{Gal}(K^{ur}_{2,\infty}(2)/K)$[b]			
Second improvement (Theorem 0.0.3)	$\#(T) \leq 75$	no	$\approx$ two weeks[d]

Table 1. Comparison of different methods

[a] In these cases, then the field K_3 (see below) is too large to be constructed by computers.
[b] Details can be found in section 5.2.
[c] This is an estimation, in fact we did not finish 10% of the process after two months.
[d] We spent about two weeks finding T. Once T is found, it takes less than one day to verify Theorem 0.0.1.

To state the first refinement, we introduce the following concept and notations. A matrix in $\mathrm{GL}_n(\mathbb{Z}_\ell)$ is *congruent trivial* if its characteristic polynomial is congruent to $(t-1)^n \pmod{\ell}$. We say a G_K-representation is *congruent trivial* if every element in the image is congruent trivial. Take S to be a finite set of prime places (S may include the Archmedian places). For a pair of ℓ-adic G_K-representations (ρ_1, ρ_2), let $K_0 = K$, then let K_1 to be the Galois extension of K_0 such that K_1 is unramified outside S and $\mathrm{Gal}(K_1/K_0)$ is isomorphic to the image of the $\mod \ell$ residue representation of $\rho_1 \oplus \rho_2$. Then for each $i \geq 1$, let K_{i+1} be the maximal abelian extension over K_i unramified outside S and $\mathrm{Gal}(K_{i+1}/K_i)$ is an elementary ℓ-group. Let $\epsilon = 1$ if $\ell = 2$ or 0 otherwise, then let $K_S = K_{5+3\epsilon}$. Take T to be a finite set of prime ideals in $\mathcal{O}_K$ such that $\mathfrak{p} \nmid 2$ and every element of $\mathrm{Gal}(K_S/K)$ corresponds to at least one Frobenius $F_\mathfrak{p}$ with $\mathfrak{p} \in T$ (i.e. T is a covering set of $\mathrm{Gal}(K_S/K)$, see Definition 2.1.2). For an ℓ-adic Galois representation φ, its mth Tate twist $\varphi \otimes \mu_\ell^{\otimes m}$ is denoted by $\varphi(m)$, where μ_ℓ is the cyclotomic representation. Denote by φ^* the dual representation of φ.

Theorem 0.0.2. *With notations as above, suppose that $\rho_1, \rho_2 : G_K \to GL_3(\mathbb{Z}_\ell)$ both satisfy $\rho_i^* \simeq \rho_i(2m)$ for some integer m and suppose that both $\rho_i(-m)$ are congruent trivial. Moreover, suppose T is disjoint with the ramified ideals with respect to $\rho_1 \oplus \rho_2$. Then ρ_1 and ρ_2 are equivalent up to semisimplification if*

$$tr(\rho_1(F_\mathfrak{p})) = tr(\rho_2(F_\mathfrak{p}))$$

for all $\mathfrak{p} \in T$.

Remark 0.0.2. As a comparison, using Grenié's criterion we have to take K_S to be $K_{8+3\epsilon}$. While with our criterion, either $K_S = K_{5+3\epsilon}$. For the purpose of Theorem 0.0.1, our criterion reduces the degree of K_S by a factor of at least 2^9.

Theorem 0.0.2 is not enough to prove Theorem 0.0.1 since it takes more than a month to construct a degree 2^7 extension using PARI/Magma while K_2 has degree 2^8.

In order to prove Theorem 0.0.1, we reduce the size of the set T further in Theorem 0.0.2 by making use of the fact that $\mathrm{Gal}(K_{2,\infty}^{ur}(2)/K)$ is a free pro-2 group with two generators [19, Theorem 2] and studying the Burnside group $B(2,4)$.

Theorem 0.0.3. *Let $K = \mathbb{Q}(\sqrt{n})$ with $n = -1, -2, -p$ or $-2p$ where $p = \pm 3 \ (mod\ 8)$. Assume ρ_i $(i = 1, 2)$ are congruent trivial and unramified outside 2 and ∞. Then there exists a set T which only depends on K and consists of at most 75 prime ideals of $\mathcal{O}_K$ not lying above 2. With this T, we have that ρ_1 and ρ_2 are equivalent if and only if*

$$tr(\rho_1(F_{\mathfrak{p}})) = tr(\rho_2(F_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$. In particular, when $K = \mathbb{Q}(\sqrt{-2})$, the set T is given by Table 5.2. When $K = \mathbb{Q}(\sqrt{-3})$, T is given by Table 5.3.

Remark 0.0.3. Theorem 0.0.3 is effective in the sense that all elements in the finite set T can be listed by Theorem 5.3.2.

Remark 0.0.4. Theorem 0.0.3 and hence Theorem 5.3.2 also work for non-selfdual representations except that when comparing non-selfdual representations, one needs to check

$$char(\rho_1(F_{\mathfrak{p}})) = char(\rho_2(F_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$. Here *char* stands for the characteristic polynomial.

One can see that Theorem 0.0.1 immediately follows once we verify that the two representations V_ℓ and $Sym^2(T_E)$ are both congruent trivial.

Here is an outline of this thesis. In chapters 1, 2 and 3 we review the background of Galois representations, Faltings-Serre method and pro-p groups respectively. In particular, we will review powerful pro-p groups, and recall a theorem that will help us to find a powerful subgroup in every pro-p group.

We prove our first improvement in chapter 4. Given a 3-dimensional selfdual representation ρ, in order to find a bound of the rank of its image, we study the Lie

algebras of its image. We show that its Lie algebra has dimension at most 3. Hence the image of ρ has rank at most 3. Hence Theorem 0.0.2 follows as a consequence.

In chapter 5, we prove Theorem 0.0.1. First we descend the Tate module of the elliptic curve E in Theorem 0.0.1 as a G_K-representation by a result of Ribet. Also we give a formula to compute the trace of the symmetric square of the descended representation. Then to compare the two sides of (0.0.1), we try to find a covering set T by Theorem 0.0.2. Then to speed up this process, we prove Theorem 5.3.2 and successfully cut off the size of T so that the whole process can be completed in two weeks hence Theorem 0.0.1 is verified.

Notations

In this thesis, unless mentioned specifically, we will assume the followings.

- $\mathbb{Q}$ is the rational field, with integer ring $\mathbb{Z}$ and ℓ, p represent prime integers of $\mathbb{Z}$.

- K, L represent number fields or infinitely Galois extensions of $\mathbb{Q}$, with algebraic integer ring $\mathcal{O}_K, \mathcal{O}_L$ respectively. Prime ideals are usually written as $\mathfrak{p}$ or $\mathfrak{P}$. Their corresponding Frobenius class are denoted by $F_\mathfrak{p}$ or $\mathfrak{P}$ respectively.

- Given a number field K and a finite set S of prime places of K, K_S^{ur} is the maximal Galois extension of K which is unramified outside S.

- $\mathbb{Q}_\ell$ is the local field with ring of integer $\mathbb{Z}_\ell$. M_λ is either a finite extension of $\mathbb{Q}_\ell$ or the algebraic closure $\overline{\mathbb{Q}}_\ell$, with $\mathcal{O}_{M_\lambda}$ (or $\mathcal{O}$ is there is no confusion) its integer ring.

- If F'/F is an Galois extension of either local or global field, we denote by $\mathrm{Gal}(F'/F)$ the corresponding Galois group. In particular, $G_F = \mathrm{Gal}(\overline{F}/F)$ is the absolute Galois group of F.

- $K_S^{ur}(p)$ is the maximal pro-p extension of K unramified outside S. In particular, $K_{2,\infty}^{ur}(2)$ is the maximal pro-2 extension of K unramified outside 2 and ∞.
- ρ, φ represent Galois representations.
- $\mathcal{G}$ represents a Lie group with its Lie algebra $\mathfrak{g}$.
- E, $\tilde{E}$ are elliptic curves defined over number fields. Their Tate module are written as $T_\ell(E)$ and $T_\ell\tilde{E}$ respectively. Without danger of confusion we will simply write T_ℓ.
- T stands for a covering set (Definition 2.1.2).

CHAPTER 1

BACKGROUND OF GALOIS REPRESENTATIONS

This chapter aims to establish notation and to provide background on ℓ-adic Galois representations. Nothing except (1.5.1) in this chapter is new.

In sections 1.1 to 1.3 we review the basic properties of linear representations, Galois groups and ℓ-adic Galois representations respectively. After that, in sections 1.4 and 1.5, we focus on the selfdual representations come from the symmetric square of Tate module of elliptic curves and the one studied by van Geemen and Top. Some properties of these selfdual representations are stated for later use. Readable reference for this chapter are [7], [30] and [23].

1.1 Linear representations and semisimple equivalence

We review basic facts about linear representations in this section. Let G be a (finite or infinite) group, let A be a commutative ring and take V to be a free A-module. Denote by $\mathrm{Aut}_A(V)$ the automorphism group of V as an A-module. A group homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}_A(V)$$

is called a *A-valued linear representation of G* (sometimes we simply say *G-representation* or even *representation* if there is no danger of confusion). In this case, V is called a *representation space of G*. To emphasis the linearity with respect to A, in this thesis

we prefer to consider ρ a group homomorphism from G to the general linear group of V, i.e.

$$\rho : G \longrightarrow \mathrm{GL}(V). \tag{1.1.1}$$

In particular, if V is of finite rank n, then we also write

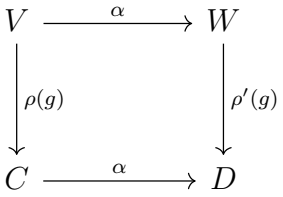
$$\rho : G \longrightarrow \mathrm{GL}_n(A) \tag{1.1.2}$$

to indicate that ρ is an n-dimensional linear representation. Note that when we have one such ρ, it means that G can act on V via ρ, i.e. any element $g \in G$ can be considered as an action on V be sending $v \in V$ to $g(v) := \rho(g)(v)$. Conversely, suppose V admits an action of G, then this group action induces an linear representation ρ by taking $\rho(g)(v) = g(v)$.

In the above definition and notations, we usually require that G, A and V are endowed with a topology compatible with their algebraic structure. In this case, we will require ρ to be continuous.

Remark 1.1.1. In fact, (5.1.2) and (1.1.2) are not totally equivalent to each other. This is because the former is intrinsic while latter requires a choice of A-basis of V. Hence it may happen that different ρ in the sense of (1.1.2) refer the same representation in the sense (5.1.2). To settle this issue, we need to tell when two representations are isomorphic.

To simplify our argument, from now on, we will only consider F-representations, where F is a field. Given two representation spaces V and W of G, we say that their induced representations ρ and ρ' are *isomorphic* and write $\rho \simeq \rho'$ if there is an F-vector space isomorphism $\alpha : V \to W$ such that the following diagram is commutative for all $g \in G$.



Two isomorphic representations can be considered "the same". Another equivalence relationship on the category of representations is the *semisimple equivalnet* relationship. To define this, recall that a *simple* representation is one which has no nontrivial subrepresentation. A *semisimple* representation is one which can be written as a direct sum of simple subrepresentations, or equivalently, if every proper subrepresentation of it has complement as a subrepresentation. When V has finite rank, every $\rho : G \to \mathrm{GL}(V)$ admits a *Jordan-Hölder* series

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

such that every V_i/V_{i+1} $(i = 0, \cdots m-1)$ is simple. Let $JH(\rho)$ be the set of isomorphism classes of these quotients with multiplicities. The following lemma is well-known.

Lemma 1.1.1. *The set $JH(\rho)$ does not depend on the choice of a Jordan-Hölder series of ρ.*

With this lemma, we can see the following is well-defined.

Definition 1.1.1. Two representations ρ and ρ' are *semisimple equivalent* (or simply *equivalent*) if $JH(\rho) = JH(\rho')$. In this case, we write $\rho \sim \rho'$.

It follows immediately that two isomorphic representations are equivalent, and the converse it true if both representations are semisimple. In particular, given a finite dimensional representation ρ, suppose $JH(\rho) = \{W_1, \cdots, W_m\}$, then it is easy to see that $\rho \sim W_1 \oplus \cdots \oplus W_m$. In fact, $W_1 \oplus \cdots \oplus W_m$ is the unique (up to

isomorphism) semisimple representation which is equivalent to ρ, hence we say that it is the *semisimplification* of ρ.

In practice, to determine whether two representations are equivalent, we need to use the character theory. Recall that given a representation $\rho : G \to \mathrm{GL}(V)$, its character is the following composition

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

According to the Jacobian density theorem [17, chap. 4, § 3], we have

Proposition 1.1.2. *If F has characteristic 0, then two F-valued representations ρ, ρ' are equivalent if and only their characters are the same, i.e.*

$$\rho \sim \rho' \Leftrightarrow tr\rho = tr\rho'.$$

1.2 Galois theory

In this section, we recall the basic facts about Galois theory of number fields. Let K be a number field, i.e. a finite extension of $\mathbb{Q}$. Take L/K to be a finite extension. Recall that the *Galois group* of L/K, written by $\mathrm{Gal}(L/K)$ is defined to be the group of field automorphisms of L which fix K. This group is a finite group and admits the discrete topology.

A field extension L/K is called *Galois* if it is both separable and normal. If L/K is Galois, according to the famous Galois correspondence, we have the following bijection between sets

$$\left\{ \begin{array}{c} \text{Intermediate Galois} \\ \text{extension } L/M/K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Normal subgroup} \\ N_M \text{ of } \mathrm{Gal}(L/K) \end{array} \right\}.$$

Moreover, with respect to this correspondence, we have $\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/N_M$.

We also consider the infinite case. If L/K is an infinite Galois extension, then the corresponding Galois group $\mathrm{Gal}(L/K)$ is defined to be the inverse limit with profinite topology

$$\mathrm{Gal}(L/K) = \varprojlim_{L'/K} \mathrm{Gal}(L'/K)$$

where L' runs over all finite intermediate Galois extension of L/K. In particular, we denote by $G_K := \mathrm{Gal}(\overline{K}/K)$ the *absolute Galois group* of K. The above Galois correspondence is still true as long as we are restricted to closed normal subgroups.

1.3 ℓ-adic Galois representations

With the definitions and notations from sections 1.1 and 1.2, we can talk about ℓ-adic Galois representations in this section. Let M_λ be an extension of local field $\mathbb{Q}_\ell$, an (n-dimensional) ℓ-adic (or λ-adic) Galois representation of $\mathrm{Gal}(L/K)$ is a continuous group homomorphism

$$\rho : \mathrm{Gal}(L/K) \to GL_n(M_\lambda).$$

Since $\mathrm{Gal}(L/K)$ is a compact group, we can assume that their images are in $GL_n(\mathcal{O}_\lambda)$ ([10, Prop. 9.3.5] or [28, Remark 1, p. I-1]), where $\mathcal{O}_\lambda$ is the ring of integers of M_λ.

Fix a number field K, and let $\mathfrak{p}$ be one of the prime ideals of its algebraic integer ring $\mathcal{O}_K$. Then we have corresponding local field $K_\mathfrak{p}$ and the corresponding residue field $k_\mathfrak{p}$. The kernel of the natural quotient $G_{K_\mathfrak{p}} \to G_{k_\mathfrak{p}}$ is the inertia group at $\mathfrak{p}$, and denoted by $I_\mathfrak{p}$, and we denote by $F_\mathfrak{p}$ the preimage of the Frobenius of $G_{k_\mathfrak{p}}$. Take ρ to be a $\mathrm{Gal}(L/K)$-representation. It is called *unramified* at $\mathfrak{p}$ if $I_\mathfrak{p}$ is in the kernel of ρ. Moreover, when ρ is unramified at $\mathfrak{p}$, it makes sense to consider $\rho(F_\mathfrak{p})$ as an element in $GL_n(M_\lambda)$. Let S be a set consisting of finite prime ideals (which may include the infinite primes). We denote by K_S^{ur} the maximal Galois extension above K which is unramified outside S. Thus if ρ is unramified outside S then it factors through $\mathrm{Gal}(K_S^{ur}/K)$.

Example 1.3.1. For any prime integer ℓ, the absolute Galois group G_K permutes the t^{th} roots of unity $\mu_t(\overline{K})$ in the algebraic closure $\overline{K}$. In particular, take $t = \ell, \ell^2, \cdots, \ell^r$ respectively, we get a compatible system with respect to G_K-action

$$\mu_{\ell^\infty}(\overline{K}) := \varprojlim_r \mu_{\ell^r}(\overline{K}) \simeq \varprojlim_r \mathbb{Z}/\ell^r\mathbb{Z} = \mathbb{Z}_\ell.$$

Hence it induces an ℓ-adic *cyclotomic character* of G_K. We will write this character to be χ_ℓ. It is easy to see that χ_ℓ is unramified away from ℓ, and

$$\chi_\ell(F_\mathfrak{p}) = N_{K/\mathbb{Q}}(\mathfrak{p})$$

as long as $\mathfrak{p} \nmid \ell$.

Proposition 1.3.2. *Let $\rho_i : G \to GL_n(M_\lambda)$ $(i = 1, 2)$ be two ℓ-adic Galois representations. Then $\rho_1 \sim \rho_2$ if and only if*

$$tr(\rho_1(g)) = tr(\rho_2(g))$$

for all $g \in G$.

Proof. This follows from Proposition 4.3.9. □

Given an F-valued G-representation space V with corresponding representation ρ, its *(algebraic) dual space* V^* is defined to be the linear space of all linear functionals $f : V \to F$. The dual space V^* is also a G-representation as long as we consider G acts on F trivially. The *dual representation* ρ^* induced by V^* is defined to be

$$\rho^*(g)(f) := f \circ \rho(g^{-1}).$$

In particular, fix a basis of V $\rho^*(g)$ can be computed by $(\rho(g)^T)^{-1}$, i.e. the transverse inverse of $\rho(g)$.

Definition 1.3.1. Let m be an integer. For an ℓ-adic representation ρ,

$$\rho(m) := \rho \otimes \chi_\ell^m$$

is called the m^{th} *Tate twist* of ρ.

Definition 1.3.2. A G_K-representation ρ is called *selfdual* if ρ^* is isomorphic to $\rho(2m)$ for some integer number m. In particular, if $m = 0$ i.e. $\rho \simeq \rho^*$, then we say that ρ is *strictly selfdual*.

Remark 1.3.1. Indeed, the conception of selfdual representation is more general. However, in this thesis we only focus on the selfdual representations in the sense of the above definition.

In the rest of this chapter, we focus on two kinds of selfdual representations related to Theorem 0.0.1.

1.4 Symmetric square of Tate module of elliptic curves

In this section, we recall the basic knowledge of elliptic curves, and explain that the symmetric square of the Tate module of an elliptic curve is a selfdual Galois representation. The main reference of this section is Silverman's book [30].

An elliptic curve E over a number field K is a genus one smooth projective curve with a K-point O. Every such curve can be described by its affine Weierstrass form

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with O the infinity point.

Every elliptic curve is an abelian variety of dimension 1. Precisely, there is an abelian group $E(\overline{K})$ consisting of the $\overline{K}$-points of E. The identity element in this

group is O, and the sum of two points $P, Q \in E$ is the unique point $R \in E$ such that $R - O$ is equal to $P + Q - 2O$ in the Picard group of E ([30, III, Lemma 3.3]). The geometric description of the group law can be found at [30, III.2]. In particular, for every m, the m-torsion subgroup $E[m]$ of $E(\overline{K})$ is isomorphic to $\mathbb{Z}/m \oplus \mathbb{Z}/m$ ([30, III, Corollary 6.4]). Since the addition law is defined over the ground field K ([30, III, 2.3]), G_K permutes $E[m]$ for every m. Moreover, suppose $m_2 = m_1 t$, then group homomorphism $[t] : E[m_2] \to E[m_1], P \mapsto [t]P := P + P + \cdots + P$ (t times) is compatible with G_K action.

Definition 1.4.1. Let E be an elliptic curve and let $\ell \in \mathbb{Z}$ be a prime integer. The ℓ-adic *Tate module* of E is the group

$$T_\ell(E) := \varprojlim_r E[\ell^r].$$

Proposition 1.4.1. *[30, III, Proposition 7.1] For a number field K and an E defined over K,*

$$T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Proposition 1.4.2. *[30, VII, Theorem 7.1] As G_K-module, the Tate module $T_\ell(E)$ is unramified at all places $\mathfrak{p}$ such that*

1. *E has good reduction at $\mathfrak{p}$.*
2. *$\mathfrak{p} \nmid \ell$.*

Proposition 1.4.3. *[30, V, Theorem 2.3.1] Let φ be the ℓ-adic Galois representation induced by $T_\ell(E) \otimes \mathbb{Q}_\ell$. Suppose φ is unramified at $\mathfrak{p}$, we have*

(a). $tr\varphi(F_\mathfrak{p}) = \alpha + \beta \in \mathbb{Q}$ with $\alpha, \beta \in \overline{\mathbb{Q}}$ independent of ℓ.

(b). Both of α and β have absolute value $\sqrt{q}$ with $q = N_{K/\mathbb{Q}}(\mathfrak{p})$, and $\alpha\beta = q$.

(c). Let $N(\varphi)$ be the composition $G_K \to \mathrm{GL}(T_\ell(E)) \otimes \mathbb{Q}_\ell \xrightarrow{norm} \mathbb{Z}_\ell$, then $N(\rho) = \chi_\ell$. Where χ_ℓ is the ℓ-adic cyclotomic character of G_K (Example 1.3.1).

With the above propositions one can see that $tr(F_\mathfrak{p}^{-1}) = \alpha/q + \beta/q$. Let ρ be the symmetric square of φ. A simple calculation shows that

$$tr(\rho(F_\mathfrak{p})) = tr(\varphi(F_\mathfrak{p}))^2 - q = (\alpha+\beta)^2 - q$$

and

$$tr(\rho(F_\mathfrak{p}^{-1})) = (\alpha/q + \beta/q)^2 - 1/q.$$

Thus, $tr(\rho^*(2)(F_\mathfrak{p})) = tr(\rho^*(F_\mathfrak{p}))q^2 = ((\alpha/q+\beta/q)^2 - 1/q)q^2 = tr(\rho(F_\mathfrak{p}))$ for all unramified $\mathfrak{p}$. Then by the Chebotarev density theorem we know that ρ is selfdual up to semisimplification.

For later use, we cite the Serre's open image theorem.

Proposition 1.4.4. *[28, §2.2 Theorem at page IV-12] Let E be an elliptic curve defined over a number field K, and let $\varphi : G_K \to GL_2(\mathbb{Q}_\ell)$ be the Galois representation induced by the Tate module of E. If E has no complex multiplication, then $img(\varphi)$ has finite index in $GL_2(\mathbb{Z}_\ell)$.*

Corollary 1.4.4.1. *Let V be the representation space of $Sym^2(\varphi)$. Then $V \otimes \mathbb{Q}_\ell$ is generated by any nonzero vector as a $\mathbb{Q}_\ell[G_K]$-module. In particular, V is an irreducible G_K-representation.*

Proof. This follows from Proposition 1.4.4 and direct calculation. □

1.5 The selfdual representation of van Geemen and Top

In this section, we roughly describe the ℓ-adic Galois representations induced by the Étale cohomology of algebraic varieties and state without attempt of proof some

of its properties. In particular, we will focus on the example studied by van Geemen and Top. Main reference of this section are [23] and [22].

Let X be a smooth algebraic variety defined over a field F. As well as the category X_{zar} of Zariski open sets of X, we can consider the categor X_{et} of étale open sets of X. The category $\mathcal{S}h(X_{et})$ of étale sheaves has enough injectives. For any sheaf $\mathcal{F}$, the functor

$$\mathcal{F} \mapsto \Gamma(X_{et}, \mathcal{F}) : \quad \mathcal{S}h(X_{et}) \to Ab$$

is left exact, hence we can define the corresponding sheaf cohomology $H^r_{et}(X, -)$, as its right derived functor [22, § 9]. In particular, when $\mathcal{F} = \mathbb{Z}/m$, we have the corresponding étale cohomology $H^r_{et}(X, \mathbb{Z}/m)$ for every r. And each of them admits the action from the Galois group G_K ([22, § 19]). Moreover, when $m_2 = m_1 t$, we have that the natural map $H^r_{et}(X, \mathbb{Z}/m_2) \xrightarrow{t} H^r_{et}(X, \mathbb{Z}/m_1)$ is compatible with G_K-action. Hence we can define

$$H^r_{et}(X, \mathbb{Z}_\ell) := \varprojlim_r H^r_{et}(X, \mathbb{Z}/\ell^r)$$

as the inverse limit, and $H^r_{et}(X, \mathbb{Q}_\ell) := H^r_{et}(X, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell$.

Now suppose X is defined over $\mathcal{O}_K$, and for every prime ideal $\mathfrak{p}$, we denote by $X_\mathfrak{p}$ the corresponding reduction. This reduced variety is defined over the residue field $\mathbb{F}_q$ with $q = N_{K/\mathbb{Q}}(\mathfrak{p})$. Let $|X_\mathfrak{p}(\mathbb{F}_{q^n})|$ be the number of $\mathbb{F}_{q^n}$-points of $X_\mathfrak{p}$. Recall that the *Hasse-Weil zeta function* of X at $\mathfrak{p}$ is defined to be

$$Z(X_\mathfrak{p}/\mathbb{F}_q; T) := \exp\left(\sum_{n=1}^{\infty} |X_\mathfrak{p}(\mathbb{F}_q)| \frac{T^n}{n}\right).$$

Proposition 1.5.1 (Weil conjecture)**.** *Suppose both X and $X_\mathfrak{p}$ are smooth of dimension d and let $\mathfrak{p} \nmid \ell$, then*

$$Z(X_\mathfrak{p}/\mathbb{F}_q; T) = \frac{P_1(T) P_3(T) \cdots P_{2d-1}(T)}{P_0(T) P_2(T) \cdots P_{2d}(T)}.$$

where each $P_r(T) = \det(1 - F_q T | H^r_{et}(X, \mathbb{Q}_\ell))$ *is the characteristic polynomial of the Frobenius element* $F_q \in G_K$ *with repect to the Galois representation induced by the étale cohomology.*

In their paper [34, § 2], for each $\mathcal{S}_{a,s}$, van Geemen and Top construct a degree 4 branched covering surface $\mathcal{A}_{a,s}$, i.e. there is a degree 4 automorphism σ of $\mathcal{A}_{a,s}$ such that $\mathcal{A}_{a,s}/\langle\sigma\rangle = \mathcal{S}_{a,s}$. They consider a subquotient of the transcendental part of the second étale cohomology of $\mathcal{A}_{a,s}$, and find that it is a Galois representation which admits an action induced by σ. Then the representation space $(V_\ell)_{a,s}$ is defined to be one of the eigenspaces of σ. They show that when $a \neq \pm 1$ and $s \neq 0$, the corresponding G_K-representation on $(V_\ell)_{a,s}$ is 3-dimensional and (possibly up to semisimplification) selfdual [34, Prop. 5.2]. In that case, they show that [34, Prop. 3.1 and Thm. 3.5]

$$tr(F_\mathfrak{p} | (V_\ell)_{a,s}) = \#(\mathcal{S}_{a,s})_\infty(\mathbb{F}_q) + \sum_{\tau \in \mathbb{F}_q, \tau^2+16 \in \mathbb{F}_q^{*2}} \left(\frac{u_\tau^2 + 4}{q}\right) \#(\mathcal{S}_{a,s})_{r+s\tau/4}(\mathbb{F}_q)$$

where $\mathbb{F}_q$ is the residue field corresponding to finite prime ideal $\mathfrak{p}$ and u_τ denotes a root in $\mathbb{F}_q$ of $X^2 - \tau X - 4 = 0$ and $(\mathcal{S}_{a,s})_t$ is the fiber over t.

Specifically, when $(a, s) = (\sqrt{-3}, 0, 1)$, the surface is

$$\mathcal{S} : Y^2 = X(X^2 + 2(\sqrt{-3} + 1 + \sqrt{-3}t^2)X + t^4).$$

When $\ell = 2$, V_ℓ is defined over $\mathbb{Z}_2(\sqrt{-1})$. But its semisimplification is in fact a $GL_3(\mathbb{Z}_2)$ representation according to the following proposition and the fact that its characteristic polynomial of $F_\mathfrak{p}$ with prime $\mathfrak{p}$ above 31 has three distinct roots in $\mathbb{Z}_2$.

Proposition 1.5.2. *Let* G *be a group, and* E *a field of characteristic* 0. *Let* $\phi : G \to GL_n(\overline{E})$ *be a semisimple representation defined over* $\overline{E}$. *let* $\phi \simeq \phi_1 \oplus \cdots \phi_r$ *be an irreducible decomposition of* ϕ. *Assume that the following conditions are satisfied:*

1. *ϕ is defined over a finite extension of E.*

2. *$tr(\phi) \in E$ for every $g \in G$.*

3. *There is an elemetn $g_0 \in G$ such that the characteristic polynomial of $\phi(g_0)$ has n distinct roots in E.*

Then each ϕ_i is defined over E. In particular, ϕ is defined over E.

Proof. See [9, Prop. 7], [16, Lem. 2.1] or the proof of [8, Prop. 3.2.5]. □

Fix $\mathfrak{p} \nmid 2$, V_ℓ is unramified at $\mathfrak{p}$, and we claim that the characteristic polynomial of $F_\mathfrak{p}$ with respect to V_ℓ satisfies

$$t^3 + t^2 + t + 1 = (t-1)^3 \ \ (mod\ 2). \tag{1.5.1}$$

To see this, note that V_ℓ is a selfdual representation, so we only need to compute its trace of $F_\mathfrak{p}$. Making use of the above formula for trace, and the symmetry of S with respect to the involution $t \mapsto -t$, and also reviewing the details of the construction of V_ℓ [34, §.2], we can compute $\#\mathcal{S}_t(\mathbb{F}_q)$ $(mod\ 4)$ as t runs through $\mathbb{P}^1_{\mathbb{F}_q}$. In fact, we have the following:

(a) When $t = 0$, if $\sqrt{3} + \sqrt{-1} \in \mathbb{F}_q$, then $\mathcal{S}_0$ contributes q points; otherwise it contributes $q + 2$ points.

(b) When $t = \infty$, we have $\#\mathcal{S}_\infty(\mathbb{F}_q) = 0$ $(mod\ 4)$.

(c) When $t = \pm\frac{1+\sqrt{-3}}{2}$, if $\sqrt{-1} \in \mathbb{F}_q$, then $\mathcal{S}_t$ contributes q points; otherwise it contributes $q + 2$ points.

(d) When $t = \pm i$, if $\sqrt{-1} \in \mathbb{F}_q$, then $\mathcal{S}_t$ gives q points; otherwise it contributes $q+2$ points.

By all above, we obtain

$$tr(F_{\mathfrak{p}}|V_\ell) = \begin{cases} 1(\ mod\ 4) & \text{if } p \equiv 7, 13\ (mod\ 24) \\ 3(\ mod\ 4) & \text{if } p \equiv 1, 5, 11, 17, 19, 23\ (mod\ 24) \end{cases}$$

and our claim follows immediately.

CHAPTER 2

FALTINGS-SERRE METHOD

In this chapter, we review the Faltings-Serre method. Some useful references are [7, chap. 5, §. 5.2, 5.4] and [21]. We will basically follow [7]. Recall that to compare two characteristic 0 representations of a finite group, we basically compare their characters, i.e. if the traces of the two representations match for every element of the finite group, then the two representations are isomorphic. Note that this process is effective in the sense that it finishes and always returns the result after finitely many steps. This is because the group is finite. When the group G is infinite, according to Proposition 4.3.9 we can still tell whether two characteristic 0 G-representations ρ_1, ρ_2 are equivalent by the comparison of their characters. However, in general this process will not be effective. Hence finding an effective algorithm to compare such ρ_1 and ρ_2 is very useful in computational number theory. Faltings [13] first shows that there exists a finite-step process for ℓ-adic representations of Galois groups which are unramified outside finitely many primes. His method is turned to be an effective algorithm by Serre [29]. Their methods is usually call the *Faltings-Serre method*.

In section 2.1 we recall the basic idea of Faltings-Serre and review the definitions of deviation group and covering set which play important roles in the proof of Falthings-Serre method. Then in section 2.2, we focus on congruent trivial 3-dimensional representations and deduce more explicit conditions to apply the Faltings-Serre method. This conditions will be used in our proof of Theorem 0.0.1.

2.1 The deviation group and covering set

Let S be a finite set of prime places of number field K. Assume that $\rho_i : G_K \to GL_n(M_\lambda)$ $(i = 1, 2)$ are unramified outside S. Since G_K is compact, we can assume that their image are in $\mathrm{GL}_n(\mathcal{O}_\lambda)$ ([10, Prop. 9.3.5] or [28, Remark 1, p. I-1]). Take $\rho = \rho_1 \oplus \rho_2$, and consider it as an $\mathcal{O}_\lambda$-algebra homomorphism

$$\rho : \mathcal{O}_\lambda[G_K] \to M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda).$$

Let N be its image and consider the composition

$$\delta : G_K \to N^\times \to (N/\lambda N)^\times.$$

Definition 2.1.1. The image $\delta(G_K)$ is called the *deviation group* of the pair (ρ_1, ρ_2).

Remark 2.1.1.

1. $\delta(G_K)$ a finite group. To see this, just notice that N is a free $\mathcal{O}_\lambda$-lattice with finite rank.

2. In general $\delta(G_K)$ is not a subgroup of $\mathrm{GL}_n(k) \oplus \mathrm{GL}_n(k)$ since in general $\lambda N \neq N \cap \lambda[M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)]$ [7, Proposition 5.2.2 and its remark].

The following proposition improves Proposition 1.3.2.

Proposition 2.1.1. *[7, Prop. 5.2.3] Let Σ be a subset of G_K surjecting onto $\delta(G_K)$. Then*

$$\rho_1 \sim \rho_2 \Leftrightarrow tr\rho_1|_\Sigma = tr\rho_2|_\Sigma.$$

Proof. For the convenience of readers, we state the sketch of the proof. It is easy to see that the only nontrivial part is the $(\Leftarrow)$ statement. To see this, suppose ρ_1 is not equivalent to ρ_2, then we can find the least positive integer a such that

$$tr\rho_1 \neq tr\rho_2 \pmod{\lambda^a}.$$

Let $\phi : tr\rho_1 - tr\rho_2$, which can be considered as an $\mathcal{O}_\lambda$-linear map from $\mathcal{O}_\lambda[G_K]$ to $\mathcal{O}_\lambda$. Then our assumption implies that

$$\phi \equiv 0 \pmod{\lambda^b} \text{ for all } b < a \tag{2.1.1}$$

$$\phi(g) \neq 0 \pmod{\lambda^a} \text{ for some } g \in G_K. \tag{2.1.2}$$

Hence we see that the image of ϕ is contained in $\lambda^{a-1}\mathcal{O}_\lambda$. Thus the following $\mathcal{O}_\lambda$-linear map

$$\frac{\phi}{\lambda^{a-1}} : \mathcal{O}_\lambda[G_K] \to \mathcal{O}_\lambda,$$

(which is well-defined according to (2.1.1)) induces another linear map over the residue field $\mathbb{F}_\lambda := \mathcal{O}_\lambda/\lambda$:

$$\tilde{\phi} : \mathbb{F}_\lambda[G_K] \to \mathbb{F}_\lambda.$$

Notice that $\tilde{\phi}$ is nontrivial due to (2.1.2), hence we can find $g \in G_K$ such that $tr\rho_1(g) \neq tr\rho_2(g)$. Take $t := \rho(g) \pmod{\lambda N}$ to be an element in the deviation group $\delta(G_K)$, we can see that for every preimage g' of t via ρ, we have

$$tr\rho_1(g') \neq tr\rho_2(g').$$

Since Σ surjects onto $\delta(G_K)$, we can see that for at least one element in Σ, ρ_1 and ρ_2 have different traces, and this ends the proof.

□

Definition 2.1.2. Fix a number field K, let U be a finite set, and $\Psi : G_K \to U$ be a map of sets. A finite set T of prime ideals of $\mathcal{O}_K$ is called a *covering set* of U (with respect to Ψ) if every element of U is in the image $\Psi(F_\mathfrak{p})$ for at least one $\mathfrak{p} \in T$.

In particular, if L is a finite Galois extension of K, T is called a *covering set of* $\mathrm{Gal}(L/K)$ if it is a covering set of $\Psi : G_K \to U$ with $U = \mathrm{Gal}(L/K)$ and with Ψ to be the natural quotient map $G_K \to \mathrm{Gal}(L/K)$.

Remark 2.1.2. Using this definition, we can restate Proposition 2.1.1 as follows:

$$\rho_1 \sim \rho_2 \text{ if and only if } tr\rho_1(F_\mathfrak{p}) = tr\rho_2(F_\mathfrak{p}) \text{ for all } \mathfrak{p} \in T$$

where T is a covering set of $\delta(G_K)$.

In particular, if ρ_1 and ρ_2 can be descended to $\mathrm{Gal}(L/K)$-representations, with L/K a finite Galois extension, then T can be chosen as any covering set of $\mathrm{Gal}(L/K)$.

2.2 Congruent trivial 3-dimensional ℓ-adic representations

For the rest of this chapter, to simplify our arguments, we will always assume that $n = 3$, and $M_\lambda = \mathbb{Q}_\ell$ and we assume the following *congruent trivial* condition for ρ_i $(i = 1, 2)$:

$$\{\text{the characteristic polynomial of } \rho_i(g)\} \equiv (t-1)^3 \ (\mathrm{mod}\ell) \text{ for all } g \in G_K. \quad (2.2.1)$$

Proposition 2.2.1. *Under the assumption* (2.2.1)*, $\delta(G_K)$ is an ℓ-group.*

Proof. In fact, we have a filtration of the image of ρ:

$$img(\rho(G_K)) =: G_0 > G_1 > G_2 > \cdots > G_m > \cdots$$

where G_i for $i \geq 1$ is the kernel of $img(\rho(G))$ $(mod\ \lambda^i)$. Since for every $i \geq 1$, the quotient G_i/G_{i+1} is isomorphic to a subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^{18}$, hence G_1 is pro-ℓ. Now consider G_0/G_1 as a subgroup of $GL_3(k) \oplus GL_3(k)$. When $\ell \geq 3$, let $t \in G_1/G_0$ we have

$$t^\ell - 1 = (t-1)^\ell = (t-1)^3 \times (t-1)^{\ell-3} = 0$$

which means every element in G_1/G_0 has order ℓ. When $\ell = 2$, by listing all possible characteristic polynomials of elements in $GL_3(\mathbb{F}_2)$ we can show the same result. $\square$

Definition 2.2.1. With G_K, ρ_1, ρ_2 as above, define Ξ to be the subset of elements $g \in G_K$ for which the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ coincide (or, equivalently, $tr_1(g^i) = tr_2(g^i)$ for $i = 1, 2, 3$).

By Proposition 2.1.1 (and Remark 2.1.2), we know that if Ξ surjects onto $\delta(G_K)$, then $\rho_1 \sim \rho_2$. Thus showing that $\rho_1 \sim \rho_2$ is reduced to finding at least one subset of Ξ which is a covering set of $\delta(G_K)$.

Proposition 2.2.2. *If $g \in \Xi$, then $\delta(g)^\ell = 1$ ($\delta(g)^4 = 1$ when $\ell = 2$) in $\delta(G_K)$.*

Proof. Recall that $g \in \Xi$ means that $\rho_1(g)$ and $\rho_2(g)$ have the same characteristic polynomial. Denoteing this common polynomial by $t^3 + a_2t^2 + a_1t + a_0$. If $\ell > 2$, we know that

$$(t-1)^{\ell-3}(t^3 + a_2t^2 + a_1t + a_0) = (t-1)^{\ell-3}(t-1)^3 = (t-1)^\ell = t^\ell - 1 \ (\mathrm{mod}\ell).$$

Thus one can see that $\rho(g)^\ell - 1 \in \lambda(M)$, which implies that $\delta(g)^\ell = 1$ in $\delta(G_K)$. By similar argument we could show that we get the corresponding result for the case $\ell = 2$. □

Definition 2.2.2. Given a group G, denote by $G[\ell]$ (resp. $G[4]$ if $\ell = 2$) the subset of elements of order dividing ℓ (resp. 4) in G, and let $G^\ell = \langle g^\ell | h \in G \rangle$ (resp. $G^4 = \langle g^4 | h \in G \rangle$) be the subgroup generated by the ℓth (resp. 4th) power of elements in G, and let $G_\ell = G/G^\ell$ (resp. $G_4 = G/G^4$).

Lemma 2.2.3. *Let H be a (pro) ℓ-group such that every element in H_ℓ (resp. H_4 when $\ell = 2$) has a lift to an element of $H[\ell]$ (resp. $H[4]$). Then $H = H_\ell$ (resp. $H = H_4$).*

Proof. [14, Lemma. 7] or [7, Lemma. 5.4.7]). □

Proposition 2.2.4. *If ρ_1 and ρ_2 be two representations satisfying the condition* (2.2.1). *Then the followings are equivalent:*

1. $\rho_1 \sim \rho_2$;

2. Ξ *is a covering set of* $(G_K)_\ell$ *(resp.* $(G_K)_4$*);*

3. Ξ *is a covering set of* $\rho(G_K)_\ell$ *(resp.* $\rho(G_K)_4$*).*

Proof. The only non-trivial part is (3) $\Rightarrow$ (1). To prove this implication, we first take $\ell > 2$, and consider the following commutative diagram

$$\begin{array}{ccc} G_K & \longrightarrow & (G_K)_\ell \\ \downarrow & & \downarrow \\ \delta(G_K) & \longrightarrow & \delta(G_K)_\ell \end{array}$$

Since Ξ covers $(G_K)_\ell$, it also covers $\delta(G_K)_\ell$. Every element $\bar{g}$ in $\delta(G_K)_\ell$ has a lifting to Ξ, denoted by g, and by Proposition 2.2.2, we know that $\delta(g) \in \delta(G_K)[\ell]$. Then the conclusion follows from the Lemma 2.2.3. By a similar argument we also show the result for case $\ell = 2$. □

CHAPTER 3

BACKGROUND OF (PRO)-p GROUPS

According to Proposition 2.2.4 we know that to compare two congruent trivial (condition 2.2.1) 3-dimensional $\mathbb{Q}_\ell$ representation ρ_1 and ρ_2, we are reduced to comparing their traces for an arbitrary covering set of $(G_K)_\ell$ (resp. $(G_K)_4$ if $\ell = 2$) or of $\rho(G_K)_\ell$ (resp. $\rho(G_K)_4$). In order to attack this problem, in this chapter, we collect the necessary background on (pro)-p groups which will be helpful later. In particular, the Theorem 3.0.4 is useful in both the proof of Grenié's criterion [14] and our Theorem 0.0.2. And in Example 3.0.3 we introduce the Burnside group, which will be used in the proof of Theorem 5.3.2. We adopt the definitions and notations in [12], especially its first three chapters.

Let p be a prime integer. A group is called a p-group if each element of this group has a power of p as its order. A pro-p group is a topological profinite p-group, or equivalently, it is a an inverse limit of a system of finite p-groups with respect to profinite topology. For the rest of this section, unless otherwise stated, all groups are assumed to be (pro)-p. For two elements g and h in group G, we denote $[g, h]$ to be the commutator of $ghg^{-1}h^{-1}$, and $[G, G] := \{[g, h]|g, h \in G\}$, and $G^p := \langle g^p|g \in G\rangle$ is the normal subgroup generated by the pth power of elements in G.

Definition 3.0.1. For a (pro)-p group G, the *Frattini subgroup* of G, denoted by $\Phi(G)$, is the intersection of all maximal proper subgroups of G.

Proposition 3.0.1. *[12, 0.9]*

1. $\Phi(G) = [G, G]G^p$.

2. *Let $X \subset G$ be a subset, and assume that $X\Phi(G)$ generates $G/\Phi(G)$. Then X generates G.*

3. *Let d be the minimal cardinality of any topological generating set for G. Then $G/\Phi(G) \simeq \mathbb{F}_p^d$, and we denote by $d(G)$ the number d.*

Definition 3.0.2. For a finite p-group G, we define the rank of G to be

$$rank(G) := \sup\{d(H)|H < G\}.$$

Definition 3.0.3. [12, 3.11] For a pro-p group G, we define the rank of G to be the common value of following r_i $(i = 1, 2, 3, 4)$:

$$r_1 = \sup\{d(H)|H \text{ is a closed subgroup of } G\}$$
$$r_2 = \sup\{d(H)|H \text{ is a closed subgroup of } G \text{ and } d(H) < \infty\}$$
$$r_3 = \sup\{d(H)|H \text{ is a open subgroup of } G\}$$
$$r_4 = \sup\{rank(G/N)|N \text{ is a open subgroup of } G\}$$

Definition 3.0.4. The *exponent* of a group (not necessary profinite) G is the least common multiple of order of elements in G.

Example 3.0.2. By definition of G^p, we know that G/G^p has exponent p. In fact, it is the largest quotient of G with this property, i.e. every other exponent p quotient of G has to factor through G/G^p.

Example 3.0.3. Given a free (and not a profinite) group F generated by d elements and n a positive integer, we denote by $B(d, n)$ the quotient F/F^n. It is called the *Burnside group*. For a fixed pair (d, n), the Burnside group is the universal group which is generated by d elements and has exponent n. For all d, the group $B(d, 2)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus d}$. However, when $n > 2$, not much is known about $B(d, n)$. In this article, we will use the groups structure of $B(2, 4)$ [32].

The definition of powerful (pro)-p groups and its properities will help us to find a subgroup of G^p (G^4 if $p = 2$) for a given G.

Definition 3.0.5. A (pro)-p group G is called *powerful* if G/G^p (or G/G^4 when $p = 2$) is abelian.

Corollary 3.0.3.1. *[12, 3.4] Let G be powerful and finitely generated, then every element of G^p is a pth power in G and G^p (resp. G^4) is open in G.*

Proof. This is an immediate consequence of Definition 3.0.5. □

The following theorem will help us in finding a powerful subgroup for a given G.

Theorem 3.0.4. *[12, 14] Let G be a finitely generated pro-p group of rank r, and define $\lambda(r)$ be the minimal integer such that $2^{\lambda(r)} \geq r$. Then G has a powerful open subgroup of index at most $p^{r\lambda(r)}$ if p is odd, and $2^{r+r\lambda(r)}$ if $p = 2$.*

Remark 3.0.1. In fact, the method of the proof is to construct a filtration of subgroups

$$G =: G_0 > G_1 > \cdots > G_{\lambda(r)+\epsilon} =: V$$

such that V is a powerful subgroup of G, where $\epsilon = 1$ when $\ell = 2$ and 0 otherwise.

CHAPTER 4

SELFDUAL LIE ALGEBRAS AND PROOF OF THEOREM 0.0.2

From the first four chapters, especially by Proposition 2.1.1, we know that to compare ρ_1 and ρ_2 that satisfy the condition (2.2.1), we need to find a covering set of G_ℓ (resp. G_4 is $\ell = 2$), where G is $(\rho_1 \oplus \rho_2)(G_K)$. Galois theory reduces this to finding the finite extension L that corresponds to the subgroup G^ℓ (resp. G^4). In principal, we can keep building Kummer ℓ extensions until we reach L. But this method is not effective unless there exists a numerical criterion to ensure that we can reach L in a certain number of steps. Such criterion can be deduced from Theorem 3.0.4 if we know the rank of $(\rho_1 \oplus \rho_2)(G_K)$.

The main result of this chapter is Theorem 4.1.4 which implies that the rank of $\rho(G_K)_\ell$ (resp. $\rho(G_K)_4$) is at most 6. Then by Theorem 3.0.4 we give a proof of Theorem 0.0.2. In section 4.1, we introduce selfdual ℓ-adic Lie algebras, and show that we are reduced to finding the maximal rank of selfdual Lie subalgebras of $\mathfrak{sl}_3(\overline{\mathbb{Q}}_\ell)$. Then in section 4.2, assuming Theorem 4.1.4, we give a proof to Theorem 0.0.2. The proof to Theorem 4.1.4 is in section 4.3.

4.1 Selfdual Lie algebras

Recall that for every subgroup $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z}_\ell)$ there is a Lie algebra $\mathfrak{g}$ attached to it. More specifically, we have the logarithm map

$$\log : 1 + \ell M_n(\mathbb{Z}_\ell) \longrightarrow M_n(\mathbb{Z}_\ell)$$
$$1 + y \longmapsto \sum_{m=1}^{\infty} \frac{(-y)^m}{m}.$$

According to [26, Lemma. 31.1], there exists an open neighborhood $\mathcal{U}$ of $1_{\mathcal{G}}$ in $\mathcal{G}$ such that the map log sends $\mathcal{U}$ onto an open neighborhood $\mathfrak{V}$ of 0 in $\mathfrak{g}$, and the exponential map $\exp(x) = \sum_{m=0}^{\infty} \frac{x^m}{m!}$ gives the local inverse to log.

Definition 4.1.1. For each integer $r \geq 0$, we define $\Gamma_r = \{y \in \mathrm{GL}_n(\mathbb{Z}_\ell) : y \in 1 + \ell^r M_n(\mathbb{Z}_\ell)\}$ for $r > 0$ and $\Gamma_0 = \mathrm{GL}_n(\mathbb{Z}_\ell)$. If $\mathcal{G}$ is a subgroup of $\mathrm{GL}_n(\mathbb{Z}_\ell)$, then we define $\Gamma_r(\mathcal{G}) = \Gamma_r \cap \mathcal{G}$.

Proposition 4.1.1. *For every $r \geq 2$, the* exp *and* log *maps induce the following group morphisms*

$$\log^{(r)} : \Gamma_r/\Gamma_{r+1} \longrightarrow \ell^r M_n(\mathbb{Z}_\ell)/\ell^{r+1} M_n(\mathbb{Z}_\ell)$$
$$1 + \ell^r x \longmapsto \ell^r x$$

$$\exp^{(r)} : \ell^r M_n(\mathbb{Z}_\ell)/\ell^{r+1} M_n(\mathbb{Z}_\ell) \longrightarrow \Gamma_r/\Gamma_{r+1}$$
$$\ell^r y \longmapsto 1 + \ell^r y$$

Proof. It follows from a straight forward calculation. □

Definition 4.1.2. For any subgroup $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z}_\ell)$, we define its *mod* ℓ^r rank to be the $\mathbb{F}_\ell$-dimension of its image of $\log^{(r)}$.

Proposition 4.1.2. *For every Lie subgroup $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z}_\ell)$, there exist an integer $r_0 = r_0(\mathcal{G})$ such that for all $r \geq r_0$, the mod ℓ^r ranks of $\mathcal{G}$ is a constant.*

Proof. We know that the $\mathbb{Z}_\ell$ rank of $\mathfrak{g} \cap (\ell^r M_n(\mathbb{Z}_\ell))/\mathfrak{g} \cap (\ell^{r+1} M_n(\mathbb{Z}_\ell))$ are equal to $\dim_{\mathbb{Q}_\ell} \mathfrak{g}$ for all $r \geq 0$. Thus the conclusion follows from Proposition 4.1.1 and the fact for sufficient large r, the restriction

$$\log : \Gamma_r(\mathcal{G}) \to \mathfrak{g} \cap \ell^r M_n(\mathbb{Z}_\ell)$$

is bijective. □

In the following, let $\epsilon = 1$ when $\ell = 2$ and 0 otherwise.

Proposition 4.1.3. *If $\mathcal{G}$ is the image of a G_K-representation in $GL_n(\mathbb{Z}_\ell)$, then*

$$rank(\Gamma_{1+\epsilon}(\mathcal{G})) \leq \dim_{\mathbb{Q}_\ell} \mathfrak{g}.$$

Proof. Without loss of generality, we can assume that $\mathcal{G} = \Gamma_{1+\epsilon}(\mathcal{G})$. Now consider a minimal set of topological group generators $\{a_1, \cdots, a_m\}$ of $\mathcal{G}$. We assume that r_i is the least number such that $a_i \in \Gamma_{r_i}(\mathcal{G})$, and that $r_1 \leq r_2 \leq \cdots \leq r_m$. Then $a_1^{\ell^{r_m - r_1}}, a_2^{\ell^{r_m - r_2}}, \cdots, a_m$ are all in $\Gamma_{r_m}(\mathcal{G})$. We claim that the image of $a_i^{\ell^{r_m - r_i}}$ in $\Gamma_{r_m}/\Gamma_{r_m+1}$ are $\mathbb{F}_\ell$-linearly independent. Before we prove our claim, note that if it is true, then for every $r \geq r_m$, the elements $a_1^{\ell^{r-r_1}}, a_2^{\ell^{r-r_2}}, \cdots, a_m^{\ell^{r-r_m}}$ are linearly independent in $\Gamma_r(\mathcal{G})/\Gamma_{r+1}$. This implies that $m \leq \dim_{\mathbb{Q}_\ell} \mathfrak{g}$ by the proof of Proposition 4.1.2 and by Proposition 3.0.1 (3), hence this proposition follows.

We will prove our claim by contradiction. Let i_0 be the first integer such that $a_1^{\ell^{r_m - r_1}}, a_2^{\ell^{r_m - r_2}}, \cdots, a_{i_0}^{\ell^{r_m - r_{i_0}}}$ are dependent in $\Gamma_{r_m}/\Gamma_{r_m+1}$, then it is easy to see that $a_1^{\ell^{r_{i_0} - r_1}}, a_2^{\ell^{r_{i_0} - r_2}}, \cdots, a_{i_0}$ are already linearly dependent in $\Gamma_{r_{i_0}}/\Gamma_{r_{i_0}+1}$. And by their linear dependence relation, we can find integers $s_i \in \{0, 1, \cdots \ell - 1\}$ for $i = 1, \cdots, i_0 - 1$ such that for all $r \geq 1$

$$a_{i_0}^{\ell^r} \equiv \left(\prod_{i=1}^{i_0 - 1} a_i^{s_i \ell^{r_{i_0} - r_i}} \right)^{\ell^r} \pmod{\Gamma_{r_{i_o} + r + 1}}. \tag{4.1.1}$$

Now we take $b_0 = a_{i_0}$ and $c_0 = \prod_{i=1}^{i_0-1} a_i^{s_i \ell^{r_{i_0}-r_i}}$. Let $b_1 = c_0^{-1} a_{i_0}$, then $b_1 \in \Gamma_{r_{i_0}+1}(\mathcal{G})$ and

$$b_1 \equiv a_{i_0}^{s\ell} b_1' \pmod{\Gamma_{r_{i_0}+2}}$$

where $s \in \{0, 1, \cdots, \ell - 1\}$ and b_1' is a product of a_i with $i \neq i_0$. Note that this can be done since $\Gamma_{j_1}/\Gamma_{j_1+1}$ is an abelian group (Proposition. 4.1.1). Then according to (4.1.1)

$$b_1 \equiv a_{i_0}^{s\ell} b_1' \equiv \left(\prod_{i=1}^{i_0-1} a_i^{s_i \ell^{r_{i_0}-r_i}} \right)^{s\ell} b_1' \pmod{\Gamma_{r_{i_0}+2}}.$$

If we let $c_1 = \left(\prod_{i=1}^{i_0-1} a_i^{s_i \ell^{r_{i_0}-r_i}} \right)^{s\ell} b_1'$, then

$$b_1 \equiv c_1 \pmod{\Gamma_{r_{i_0}+2}}.$$

By repeating the similar arguments as above, for each $k \geq 2$, we can construct b_k and c_k inductively such that $b_k = c_{k-1}^{-1} b_{k-1} \in \Gamma_{r_{i_0}+k}(\mathcal{G})$, c_k is a product of a_i with $i \neq i_0$ and $b_k \equiv c_k \ \ mod\ \Gamma_{r_{i_1}+k+1}$. As consequence, we have

$$\lim_{N \to \infty} \prod_{k=1}^{N} c_k = a_0$$

which means that a_{i_0} is topologically generated by all the rest of the generators. This contradicts the assumption that $\{a_1, \cdots, a_m\}$ is a minimal set of topological generators. □

Corollary 4.1.3.1. *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be the image of two G_K-representations φ_1 and φ_2, respectively. Assume their Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ have ranks r_1 and r_2, respectively. Then $\Gamma_{1+\epsilon}(img(\varphi_1 \oplus \varphi_2))$ has rank at most $r_1 + r_2$.*

Proof. This follows from the above proposition and the fact that $\Gamma_{1+\epsilon}(img(\varphi_1 \oplus \varphi_2))$ is a subgroup of $\Gamma_{1+\epsilon}(img(\varphi_1) \oplus img(\varphi_2))$. □

Now if we assume that $\mathcal{G}$ is the image of a strictly selfdual representation φ, then there exists an invertible matrix $P \in \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ such that $PgP^{-1} = (g^{-1})^t$ for every $g \in \mathcal{G}$. After taking derivative, we have a selfdual condition for Lie algebras

$$PxP^{-1} = -x^t \quad \text{for all } x \in \mathfrak{g}. \tag{4.1.2}$$

After base extension $\mathfrak{g} \otimes \overline{\mathbb{Q}}_\ell$, we get a Lie subalgebra of $\mathfrak{gl}_n(\overline{\mathbb{Q}}_\ell)$ which satisfies the same condition.

Definition 4.1.3. A Lie subalgebra of $\mathfrak{gl}_n(\overline{\mathbb{Q}}_\ell)$ which satisfies the condition (4.1.2) is called a *selfdual Lie algebra*.

Now we are ready to state the main result in this section. Its proof will be postponed until subsection 4.3.

Theorem 4.1.4. *If $\mathfrak{g}$ is a selfdual Lie subalgebra of $\mathfrak{sl}_3(\overline{\mathbb{Q}}_\ell)$, then one of the followings is true.*

(a) $\dim \mathfrak{g} = 1$.

(b) $\dim \mathfrak{g} = 2$ *and* $\mathfrak{g}$ *non-abelian.*

(c) $\mathfrak{g} \simeq \mathfrak{sl}_2(\overline{\mathbb{Q}}_\ell)$.

In particular, $\dim \mathfrak{g} \leq 3$.

Corollary 4.1.4.1. *If φ is a strictly selfdual representation to $\mathrm{GL}_3(\mathbb{Z}_\ell)$ with image $\mathcal{G}$, then $\Gamma_{1+\epsilon}(\mathcal{G})$ has rank at most 3.*

Proof. This follows immediately from the above theorem and Proposition 4.1.3. □

Now let ρ_1 and ρ_2 be two representations such that

1. they are both strictly selfdual, and

2. they both satisfy condition 2.2.1.

Recall that $\rho = \rho_1 \oplus \rho_2$ has image $\mathcal{G}$.

Corollary 4.1.4.2. *There is a filtration of subgroups*

$$\Gamma_{1+\epsilon}(\mathcal{G}) = G_1' > G_2' > \cdots > G_{4+\epsilon}' =: V$$

where G_i'/G_{i+1}' is an elementary Abelian ℓ-group of degree at most ℓ^6 and V is powerful. Moreover, $[\Gamma_{1+\epsilon}(\mathcal{G}) : V] \leq \ell^{18+6\epsilon}$.

Proof. By Corollary 4.1.4.1 and Corollary 4.1.3.1, we know that $\Gamma_{1+\epsilon}(\mathcal{G})$ has rank at most 6. Thus $\lambda(6) = 3$, and the filtration follows from Theorem 3.0.4 and its remark. □

Theorem 4.1.5. *Let $\mathcal{G}$ be as above, then there is a filtration of subgroups*

$$\mathcal{G} = G_0 > G_1 > G_2 > \cdots > G_4 = V > G_5 = V^\ell \qquad \text{if } \ell \neq 2$$

$$\mathcal{G} = G_0 > G_1 > G_2 > \cdots > G_6 = V > \cdots > G_8 = (V^2)^2 \qquad \text{if } \ell = 2$$

such that

1. *For every $i \geq 1+\epsilon$, the group G_i/G_{i+1} is an elementary ℓ-group of rank at most 6 and V is a powerful subgroup of $\mathcal{G}$.*

2. *Every element in V^ℓ (resp. $(V^2)^2$) is an ℓth (resp. 4th) power of some other element. Thus $\mathcal{G}/V^\ell$ (resp. $\mathcal{G}/(V^2)^2$) surjects onto $\mathcal{G}_\ell$ (resp. $\mathcal{G}_4$).*

3. *In particular, if $\ell = 2$ and G is pro-2, then G_0/G_1 is elementary of rank at most 4.*

Proof. If $\ell \neq 2$, we let $G_i = G_i'$ in Corollary 4.1.4.2 for $i > 0$, and if $\ell = 2$, we let $G_1 = \Gamma_1(\mathcal{G})$ and $G_i = G_{i-1}'$ for all $i > 1$. Then the first conclusion follows from Corollary 4.1.4.2. And Corollary 3.0.3.1 implies the second conclusion. To show the last statement, note that $GL_3(\mathbb{F}_2)$ has its strictly upper triangular subgroups as one of its 2-Sylow subgroups. Thus if ρ_i $(i = 1, 2)$ satisfies condition (2.2.1), its image in Γ_0/Γ_1 is isomorphic to one of the five possible cases:

$$\{1\}, \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{D}_4$$

where $\mathcal{C}_n$ is the cyclic group of degree n and $\mathcal{D}_4$ is the dihedral group of degree 8.

By the next lemma, we know that up to conjugation by an element in $GL_3(\frac{1}{2}\mathbb{Z}_2)$ that the residue image of $\rho_i(G_K)$ is isomorphic to one of the first three cases, hence the last statement follows. □

Lemma 4.1.6. *Let*

$$P = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{2} \\ 1 & 1 & 0 \end{pmatrix}$$

then

$$P \begin{pmatrix} 1+2a_{11} & 2a_{12} & 2a_{13} \\ 2a_{21} & 1+2a_{22} & 2a_{23} \\ 2a_{31} & 2a_{32} & 1+2a_{33} \end{pmatrix} P^{-1} \in \begin{pmatrix} 1 & 0 & a_{31} \\ 0 & 1 & a_{21}+a_{31} \\ 0 & 0 & 1 \end{pmatrix} + 2M_3(\mathbb{Z}_2)$$

$$P \begin{pmatrix} 1+2a_{11} & 1+2a_{12} & 2a_{13} \\ 2a_{21} & 1+2a_{22} & 2a_{23} \\ 2a_{31} & 2a_{32} & 1+2a_{33} \end{pmatrix} P^{-1} \in \begin{pmatrix} 1 & 0 & a_{31} \\ 0 & 1 & a_{21}+a_{31} \\ 0 & 0 & 1 \end{pmatrix} + 2M_3(\mathbb{Z}_2)$$

$$P \begin{pmatrix} 1+2a_{11} & 1+2a_{12} & 1+2a_{13} \\ 2a_{21} & 1+2a_{22} & 1+2a_{23} \\ 4a_{31} & 2a_{32} & 1+2a_{33} \end{pmatrix} P^{-1} \in \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a_{21} \\ 0 & 0 & 1 \end{pmatrix} + 2M_3(\mathbb{Z}_2)$$

Proof. Just a calculation. □

4.2 Proof of Theorem 0.0.2

Proof of Theorem 0.0.2. Now suppose we have two selfdual G_K-representations, ρ_1 and ρ_2, such that $\rho_i^*(2m) \simeq \rho_i$ $(i = 1, 2)$. Then we have

$$\rho_1 \simeq \rho_2 \Leftrightarrow \rho_1(-m) \simeq \rho_2(-m).$$

Thus to comparing ρ_1 with ρ_2, we are reduced to comparing $\rho_1(-m)$ with $\rho_2(-m)$. Since $(\rho_i(-m))^* = \rho_i^*(m) \simeq \rho_i(-m)$ is strictly selfdual and satisfies condition 2.2.1, we can use Theorem 4.1.5 to construct a filtration of subgroups of $\mathcal{G}$. On the other hand, if we build K_i as described above in Theorem 0.0.2, then we have $G_K > \mathrm{Gal}(\overline{K}/K_i) > G_i$ for all $i \geq 1$. Thus there are surjections

$$\mathrm{Gal}(K_S/K) \twoheadrightarrow \mathcal{G}/G_{5+3\epsilon} \twoheadrightarrow \mathcal{G}_\ell(\text{resp. } \mathcal{G}_4).$$

Now if T is a covering set of $\mathrm{Gal}(K_S/K)$, it is also a covering set of $\mathcal{G}_\ell$ (resp. $\mathcal{G}_4$), then Theorem 0.0.2 follows from Proposition 2.2.4 and Remark 2.1.2. □

4.3 Proof of Theorem 4.1.4

In this section, we classify all the selfdual Lie subalgebras of $\mathfrak{sl}_3(\overline{\mathbb{Q}}_\ell)$ up to conjugacy, and thus prove Theorem 4.1.4. Our arguments are based on detailed calculations. For people who want to skip the calculation details, we provides an outline of our discussion:

1. From Lemma 4.3.1 to Lemma 4.3.3, we list some basic observations.

2. After that, we prove that every 2-dimensional Lie subalgebra of $\mathfrak{sl}_3$ is non-abelian at Proposition 4.3.4, hence prove part (b) of Theorem 4.1.4.

3. At Propositions 4.3.5 we show that the selfdual Lie subalgebras of $\mathfrak{sl}_3$ have dimension at most 3, and all 3-dimension Lie subalgebras are isomorphic to $\mathfrak{sl}_2$

abstractly. This is the main result of this section since it finishes the proof and Theorem 4.1.4. In order to prove Proposition 4.3.5

(a) From Proposition 4.3.6 to Proposition 4.3.8, we discuss solvable case.

(b) At Proposition 4.3.9, we discuss non-solvable case.

Note that if $\mathfrak{g}$ is a selfdual Lie subalgebra of $\mathfrak{gl}_3(\overline{\mathbb{Q}}_\ell)$, then by condition (4.1.2)

$$tr(x) = tr(-x^t) = -tr(x) \Rightarrow tr(x) = 0 \text{ for all } x \in \mathfrak{g}$$

thus $\mathfrak{g}$ is a Lie subalgebras of $\mathfrak{sl}_3(\overline{\mathbb{Q}}_\ell)$. To simplify the notation, for the rest of this subsection, we simply write $\mathfrak{sl}_3$ for $\mathfrak{sl}_3(\overline{\mathbb{Q}}_\ell)$. Similarly, we write $\mathfrak{t}$ for $\mathfrak{t}(3, \overline{Q}_\ell)$, which is the Lie algebra consisting of upper triangular matrices, and $\mathfrak{n}$ for $\mathfrak{n}(3, \overline{\mathbb{Q}}_\ell)$, which is the subalgebra of $\mathfrak{sl}_3$ consisting of all strict upper triangular matrices. In this subsection we always assume $\mathfrak{g}$ to be selfdual. In addition, we assume that there is an invertible matrix $P = (p_{ij}) \in GL_3(\overline{\mathbb{Q}}_\ell)$ such that $Px + x^tP = 0$ for all $x \in \mathfrak{g}$. Also, we will use the following notation in [35]:

$$K_1 = \frac{1}{2}\begin{pmatrix} 1 & & \\ & -1 & \\ & & 0 \end{pmatrix}, K_2 = \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, K_3 = \frac{1}{2}\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & & \\ & 1 & \\ & & -2 \end{pmatrix},$$
$$P_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, P_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} R_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, R_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Before our dimensional arguments, we have some basic observations.

Lemma 4.3.1. *If there is a nonzero diagonal element* $\begin{pmatrix} a & & \\ & b & \\ & & -a-b \end{pmatrix}$ *in* $\mathfrak{g}$*, then exactly one of* a *or* b *or* $a+b$ *is* 0*. In particular,* $D \notin \mathfrak{g}$*.*

Proof. To show this, let A to be the given diagonal matrix. Then,

$$0 = PA + A^tP = \begin{pmatrix} 2ap_{11} & (a+b)p_{12} & -bp_{13} \\ (a+b)p_{21} & 2bp_{22} & -ap_{23} \\ -bp_{31} & -ap_{32} & -2(a+b)p_{33} \end{pmatrix},$$

which proves the lemma by the fact that P is invertible. □

With the same idea and similar calculations, we also have the following lemmas.

Lemma 4.3.2. *At most one of $K_2 - K_3$ and R_2 is in $\mathfrak{g}$.*

Lemma 4.3.3. *$\mathfrak{g} \cap \mathfrak{n}$ has dimension at most 1. In particular, at most one of $K_2 - K_3$ or P_1 or P_2 is in $\mathfrak{g}$.*

Remark 4.3.1. By symmetry, $\mathfrak{g} \cap \mathfrak{n}^t$ also has dimension ≤ 1 also.

Now we discuss dimension. If $\dim \mathfrak{g} = 1$, it is trivial, so we start from the 2-dimensional case and give a proof to part (b) of Theorem 4.1.4.

Proposition 4.3.4. *If $\mathfrak{g}$ is a 2-dimensional selfdual Lie subalgebra of $\mathfrak{sl}_3$, then $\mathfrak{g}$ is non-abelian.*

Proof. Suppose $\mathfrak{g}$ is abelian, and let $\{x, y\}$ be its basis. Without loss of generality, we assume that x is of its Jordan form.

If x is diagonalizable, by Lemma 4.3.1, we can write $x = \begin{pmatrix} 1 & & \\ & -1 & \\ & & 0 \end{pmatrix}$ up to scalar. Then y is not diagonal due for Lemma 4.3.1. However, since $[x, y] = 0$, y must be diagonal, which is impossible. Thus x is not diagonalizable.

Next suppose $x = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & -2a \end{pmatrix}$ with $a \neq 0$. Write $y = (y_{ij})_{1 \leq i,j \leq 3}$. Then $[x, y] = 0$ implies that $y_{13} = y_{21} = y_{23} = y_{31} = y_{32} = 0$, and $y_{22} = y_{11}$. Replacing y by $y - \frac{y_{11}}{a}x$ if necessary, we may assume that $y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. But then we see that $x - y$ is diagonal, a contradiction.

If $x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then $[x, y] = 0$ implies $y_{21} = y_{23} = y_{31} = 0$, and $y_{22} = y_{11}$. So we can assume $y = \begin{pmatrix} y_{11} & 0 & y_{13} \\ 0 & y_{11} & 0 \\ 0 & y_{32} & -2y_{11} \end{pmatrix}$. Note that if $y_{11} \neq 0$, we may assume that $y_{11} = 1$. Then taking $b = 0$ if $y_{13}y_{32} = 0$ and $-\frac{y_{13}y_{32}}{3}$ otherwise, one can verify that $y + bx$ is diagonalizable, contradiction. Now if $y_{11} = 0$, then $y = \begin{pmatrix} 0 & 0 & y_{13} \\ 0 & 0 & 0 \\ 0 & y_{32} & 0 \end{pmatrix}$, by Lemma 4.3.2 and Lemma 4.3.3, we have $y_{13}y_{32} \neq 0$. But then we cannot find an invertible matrix P satisfying condition 4.1.2.

Finally, if $x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, we can write $y = \begin{pmatrix} y_{11} & 0 & y_{13} \\ y_{21} & y_{22} & y_{23} \\ y_{31} & y_{32} & -y_{11}-y_{22} \end{pmatrix}$. Then $[x, y] = 0$ implies $y_{21} = y_{23} = y_{31} = y_{32} = 0$ and $y_{11} = y_{22} = y_{33} = 0$. So we have $y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$,

but then $x, y \in \mathfrak{g} \cap \mathfrak{n}$, contradict Lemma 4.3.3. This completes the proof that there is no 2-dimensional abelian selfdual Lie subalgebra of $\mathfrak{sl}_3$. □

Suppose the dimension of $\mathfrak{g}$ is at least 3. We will prove the following proposition which shows part (c) of Theorem 4.1.4 and finishes the proof of that theorem.

Proposition 4.3.5. *Every selfdual Lie subalgebra $\mathfrak{g}$ of $\mathfrak{sl}_3$ has dimension ≤ 3. And when $\dim \mathfrak{g} = 3$, $\mathfrak{g} \simeq \mathfrak{sl}_2$ as abstract Lie algebra.*

To prove Proposition 4.3.5, we will discuss the solvable and non-solvable cases separately (for the related background please see Appendix A.1 or [15]). And Proposition follows immediately from Proposition 4.3.8 and Proposition 4.3.9.

First, we discuss the solvable cases. Thanks to Lie's theorem (cf. Prop. A.1.1), we can assume that $\mathfrak{g}$ is a subalgebra of $\mathfrak{t}$.

Proposition 4.3.6. *If $\mathfrak{g}$ is selfdual and solvable, then $\dim \mathfrak{g} \leq 3$.*

Proof. Suppose not, we have $\dim \mathfrak{g} \geq 4$. But then by Lemma 4.3.1 $\mathfrak{g} \cap \mathfrak{n}$ has dimension at least 2, which contradicts Lemma 4.3.3. □

Proposition 4.3.7. *If $\mathfrak{g}$ is solvable, then $[\mathfrak{g}, \mathfrak{g}] = 0$ or $\dim[\mathfrak{g}, \mathfrak{g}] = 1$.*

Proof. This follows from the fact that $[\mathfrak{t}, \mathfrak{t}] \subset \mathfrak{n}$ and Lemma 4.3.3. □

Proposition 4.3.8. *If $\mathfrak{g}$ is a solvable and selfdual Lie subalgebra of $\mathfrak{sl}_3$ then $\dim \mathfrak{g} \leq 2$.*

Proof. Suppose not, we assume $\dim \mathfrak{g} = 3$. By Proposition 4.3.7, we have two possible situations. If $[\mathfrak{g}, \mathfrak{g}] = 0$, i.e. $\mathfrak{g}$ is Abelian, then according to Lemma 4.3.3, up to scalar there is a unique nonzero element v in $\mathfrak{g} \cap \mathfrak{n}$. Now let $\{v, u_1, u_2\}$ be a fixed basis of $\mathfrak{g}$

as a linear space. Write $v = \begin{pmatrix} 0 & v_{12} & v_{13} \\ 0 & 0 & v_{23} \\ 0 & 0 & 0 \end{pmatrix}$ and let $u = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & -u_{11}-u_{22} \end{pmatrix}$ be an arbitrary element in $\mathfrak{g} \setminus \langle v \rangle$, then

$$[u, v] = 0 \Rightarrow \begin{cases} u_{11}v_{12} = u_{22}v_{12} \\ 2u_{11}v_{13} + u_{12}v_{23} + u_{22}v_{13} = u_{23}v_{12} \\ u_{11}v_{23} = -2u_{22}v_{23}. \end{cases}$$

If either v_{12} or v_{23} is nonzero, we see that the entries on the main diagonal of u are not independent, and thus there is a nontrivial linear combination of u_1, u_2 lying in $\mathfrak{n}$, which implies that $\dim \mathfrak{g} \cap \mathfrak{n} = 2$, contradiction. So $v_{12} = v_{23} = 0$. But then $v_{13} \neq 0$, and with the same argument, we still have $\dim \mathfrak{g} \cap \mathfrak{n} = 2$. Hence $[\mathfrak{g}, \mathfrak{g}] = 0$ is impossible.

Now suppose $\mathfrak{g}$ is non-abelian. We can find linearly independent elements $x, y, v \in \mathfrak{g}$, such that $[\mathfrak{g}, \mathfrak{g}] = \langle v \rangle \subset \mathfrak{n}$. Moreover, we assume at least one of x and y is not commutative with v since otherwise the same arguments as above will imply contradiction. Without loss of generality we let $[v, x] = v$. Then if $[v, y] = bv$ and $[x, y] = cv$, then by replacing y by $y - bx - cv$, we can assume $[x, y] = [v, y] = 0$.

If $v^2 \neq 0$, then up to a conjugation by an upper triangular element, we assume that $v = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, then the conditions $[v, x] = v$ and $[v, y] = 0$ imply

$$x = \begin{pmatrix} -1 & x_{12} & x_{13} \\ 0 & 0 & x_{12} \\ 0 & 0 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 0 & y_{12} & y_{13} \\ 0 & 0 & y_{12} \\ 0 & 0 & 0 \end{pmatrix}.$$

But then $[x, y] = 0$ will force $y = 0$, contradiction.

Thus v^2 has to be 0. Up to scaling and conjugation by an upper triangular element, v is one of the following three matrices

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

We assume the first. Then by $[v, x] = v$ and $[v, y] = 0$, we get

$$x = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ 0 & x_{11}+1 & 0 \\ 0 & 0 & -2x_{11}-1 \end{pmatrix}, y = \begin{pmatrix} y_{11} & y_{12} & y_{13} \\ 0 & y_{11} & 0 \\ 0 & 0 & -2y_{11} \end{pmatrix}.$$

By Lemma 4.3.3, $y_{11} \neq 0$, replace y by $\frac{y}{y_{11}}$ and x by $x - \frac{x_{11}}{y_{11}}y$, we still have $[v, x] = v, [v, y] = [x, y] = 0$. Then we have

$$x = \begin{pmatrix} 0 & x_{12} & x_{13} \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, y = \begin{pmatrix} 1 & y_{12} & y_{13} \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

Then $[x, y] = 0$ will imply that $y_{13} = 3x_{13}$ and $y_{12} = 0$, so we have $y = \begin{pmatrix} 1 & 0 & 3x_{13} \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$. But a quick calculation tells us that in this case the invertible P does not exist. For the remaining two choices of v, similar arguments give us the same conclusion and finish the proof. □

Second, we talk about non-solvable case.

Proposition 4.3.9. *If $\mathfrak{g}$ is non-solvable and selfdual, then* $\dim \mathfrak{g} \leq 3$. *If* $\dim \mathfrak{g} = 3$, *then $\mathfrak{g} \simeq \mathfrak{sl}_2$.*

Proof. First, we show that $\mathfrak{g}$ has dimension at most 5. If not, then by linear combination, we can find a Lie subalgebra of $\mathfrak{g} \cap \mathfrak{t}$ which has dimension at least 3, but this contradicts Theorem 4.3.8.

If $\dim \mathfrak{g} \geq 4$, $\mathfrak{g}/Rad(\mathfrak{g})$ is semisimple and nontrivial. By Proposition A.1.2 we know the quotient has dimension 3 and is isomorphic to $\mathfrak{sl}_2$, and thus $\dim Rad(\mathfrak{g}) \geq 1$. If we fix s to be an arbitrary nonzero element in $Rad(\mathfrak{g})$, then the following linear map $u \mapsto [s, u]$ from $\mathfrak{g}$ to $Rad(\mathfrak{g})$ has nonzero kernel. Take $x \neq 0$ to be in that kernel, then s and x spans an abelian dimensional 2 selfdual Lie subalgebra of g. But this contradicts Proposition 4.3.4. Hence, we know that $Rad(\mathfrak{g}) = 0$ and thus $\mathfrak{g} \simeq \mathfrak{sl}_2$. □

CHAPTER 5

PROOF OF THEOREM 0.0.1

In this chapter, we prove our main theorem 0.0.1. To do this, in section 5.1 we show that the symmetric square of the Tate module of elliptic curve E in Theorem 0.0.1 can be descended as a $G_{\mathbb{Q}(\sqrt{-3})}$-representation and we give an explicit formula to compute its trace at Frobenius. Then in section 5.2, by Theorem 0.0.2 and the effective Chebotarev density theorem under the Extended RiemannHypothesis (ERH) in [1] we find a covering set T by bounding the norm of Frobenius. But that bound is too large for computers to verify Theorem 0.0.1. To find a better T, in section 5.3 we note that the Galois group $(G_{\mathbb{Q}(\sqrt{-3}),\{2,\infty\}})_4 \simeq B(2,4)$ (cf. example 3.0.3). By studying the conjugacy classes of $B(2,4)$, we prove Theorem 5.3.2, which is the main theorem of this chapter. As a consequence of this theorem, we finally find a set T consisting of no more than 75 Frobenius as a covering set for Theorem 0.0.1. With the final version of covering set T, we are able to finish the calculation in about two weeks.

Through out this chapter, we will fix the notation K to be the number field $\mathbb{Q}(\sqrt{-3})$, fix $\mathcal{S}$ and E to be the elliptic surfaces and the elliptic curve involved in Theorem 0.0.1. Also, let ρ_1 to be the representation V_ℓ in Theorem 0.0.1, and take ρ_2 to be the descended symmetric square of the Tate module $T_\ell(E)$, and ρ to be the direct sum $\rho_1 \oplus \rho_2$.

5.1 Descent of the symmetric square of Tate module

Recall that for a number field F, and one of its Galois extensions M/F, an elliptic curve defined over M is called an F-curve if it is isogenous to all its $\mathrm{Gal}(M/F)$ conjugates. Let ξ be a primitive 8th root of unity and let $b = \left(-\frac{\sqrt{-1}}{4} + \frac{\sqrt{-3}}{8} - \frac{1}{8}\right)$, one can check that the 2-isogeny

$$(x, y) \longmapsto \left(\frac{y^2}{2\xi^2 x^2}, \frac{y^2(b - x^2)}{2\sqrt{2}\xi^3 x^2}\right)$$

is a morphism from the elliptic curve E in Theorem 0.0.1 to its G_K-conjugate

$$\tilde{E} : Y^2 = X^3 + (-\sqrt{-1} - 1)X^2 + \left(\frac{\sqrt{-1}}{4} + \frac{\sqrt{-3}}{8} - \frac{1}{8}\right) X.$$

Hence E is a K-curve. Moreover, one can verify that E does not have complex multiplication. Ribet [25, §6,7] constructs the descent Tate module for every F-curve without complex multiplication. We apply Ribet's techniques to our case.

Suppose E' another elliptic curve and let $\mu : E' \to E$ be an isogeny with dual $\mu^\vee$. We write μ^{-1} to be $\frac{1}{\deg \mu}\mu^\vee \in Hom(E, E') \otimes \mathbb{Q}$. For every element $\sigma \in G_K$, we denote by E^σ the conjugation of E by σ, and fix an isogeny $\mu_\sigma : E^\sigma \to E$. Then the following map

$$\begin{aligned} c : G_K \times G_K &\longrightarrow \mathbb{Q} \\ (\sigma, \tau) &\mapsto \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} \end{aligned}$$

is a well-defined (recall that E does not have complex multiplication) 2-cocycle. By the following Proposition 5.1.1 we know that c is a 2-boundary, i.e. there exists $\alpha : G_K \to \overline{\mathbb{Q}}^*$, such that

$$c(\sigma, \tau) = \frac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)}.$$

Proposition 5.1.1. *[25, Thm. 6.3]* $H^2(G_K, \overline{\mathbb{Q}}^*) = 0$, *where* $\overline{\mathbb{Q}}^*$ *has the trivial* G_K*-action.*

Now we define a G_K-action ϕ on $\overline{\mathbb{Q}}_l \otimes T_E$ by

$$\phi(\sigma)(1 \otimes x) = \alpha^{-1}(\sigma) \otimes \mu_\sigma(x^\sigma).$$

It is a well-defined for $\phi(\sigma)\phi(\tau)\phi(\sigma\tau)^{-1} = c(\sigma,\tau)(\frac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)})^{-1} = 1$.

Every conjugation E^σ is either isomorphic to E or $\tilde{E}$ over K. Let $\mu : \tilde{E} \to E$ be a 2-isogeny and take

$$\mu_\sigma = \begin{cases} 1 \text{ if } \sigma \in G_{K(\sqrt{-1})} \\ \mu \text{ if } \sigma \notin G_{K(\sqrt{-1})}. \end{cases}$$

By calculation, we have

(1) If $\sigma, \tau \in G_{K(\sqrt{-1})}$, then $c(\sigma,\tau) = \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = 1 \circ 1 \circ 1 = 1$;

(2) If $\sigma \in G_{K(\sqrt{-1})}, \tau \notin G_{K(\sqrt{-1})}$, then $c(\sigma,\tau) = \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = 1 \circ \mu \circ \mu^{-1} = 1$;

(3) If $\sigma \notin G_{K(\sqrt{-1})}, \tau \in G_{K(\sqrt{-1})}$, then $c(\sigma,\tau) = \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = \mu \circ 1 \circ \mu^{-1} = 1$;

(4) If $\sigma, \tau \notin G_{K(\sqrt{-1})}$, then $c(\sigma,\tau) = \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = \mu \circ \mu^\sigma \circ 1 = \pm \deg(\mu) = \pm 2$.

Thus, let

$$\alpha(\sigma) = \begin{cases} 1 \text{ if } \sigma \in G_L \\ \sqrt{2} \text{ if } \sigma \notin G_L \end{cases}$$

then we can descend T_E as G_K-representation as following:

$$\phi : G_K \to End(T_E) \otimes \mathbb{Q}_\ell$$

$$\sigma \mapsto \begin{cases} x \mapsto x^\sigma & \text{if } \sigma \in G_{K(\sqrt{-1})} \\ x \mapsto \frac{\mu(x^\sigma)}{\sqrt{2}} & \text{if } \sigma \notin G_{K(\sqrt{-1})} \end{cases}.$$

Remark 5.1.1. The image of ϕ is in $GL_2(\frac{1}{\sqrt{2}}\mathbb{Z}_\ell)$. But since we only care about ρ_2 which is the symmetric square of ϕ, we know that the image of ρ_2 is still in $GL_3(\mathbb{Z}_\ell)$. By the same reason, ρ_2 will not change if we choose $\alpha(\sigma) = -\sqrt{2}$ for $\sigma \notin G_{K(\sqrt{-1})}$.

Now we need to compute the trace of $\rho_2 = Sym^2(\phi)$ for every Frobenius $F_\mathfrak{p}$ over K. If we denote by π the representation induced by T_E, it's easy to see that when $\mathfrak{p}$ splits in $K(\sqrt{-1})$, we have $tr(Sym^2(\phi)(F_\mathfrak{p})) = tr(Sym^2(\pi)(F_\mathfrak{p}))$. Now assume $\mathfrak{p}$ is inert in $K(\sqrt{-1})$, with $\mathfrak{P}$ lying above it. With a proper choice of the basis of $T_E \otimes \overline{\mathbb{Q}}_\ell$ such that $\phi(F_\mathfrak{p}) = \left(\begin{smallmatrix} a & * \\ 0 & b \end{smallmatrix}\right)$, we get

$$tr(Sym^2(\phi)(F_\mathfrak{p})) = a^2 + b^2 + ab = tr(\pi(F_\mathfrak{P})) + ab.$$

Since $(ab)^2 = \det(\pi(F_\mathfrak{P})) = N_{K/\mathbb{Q}}(\mathfrak{p})^2$, we know that $\det(\phi(F_\mathfrak{p})) = ab = \pm N_{K/\mathbb{Q}}(\mathfrak{p})$. To determine the sign, we use the idea in the proof of [30, chap. V, Prop. 2.3, Thm. 2.4]: if we consider the reduced curve of E on the residue field at $\mathfrak{p}$, then the determinant of $\sqrt{2}\phi(F_\mathfrak{p})$ can be explained as the degree of isogeny $\mu \circ F_\mathfrak{p}$, and hence it must be positive. As conclusion, we have

$$tr(Sym^2(\phi)(F_\mathfrak{p})) = \begin{cases} tr(\pi(F_\mathfrak{p}))^2 - N_{K/\mathbb{Q}}(\mathfrak{p}) \text{ when } \mathfrak{p} \text{ splits} \\ tr(\pi(F_\mathfrak{P})) + N_{K/\mathbb{Q}}(\mathfrak{p}) \text{ otherwise} \end{cases} \tag{5.1.1}$$

In particular, since $(0,0)$ is a 2-torsion point of E, we know that $tr(\pi(F_\mathfrak{P})) = 0 \pmod 2$ for all finite prime ideals $\mathfrak{P}$ in $K(\sqrt{-1})$. Hence we know that all mod2 characteristic polynomials of $Sym^2(\phi)$ are equal to

$$t^3 + t^2 + t + 1 = (t-1)^3 \pmod 2, \tag{5.1.2}$$

thus $\rho_2(-1)$ satisfies the condition (2.2.1).

5.2 Finding a covering set by Theorem 0.0.2

When $\ell = 2$, by (1.5.1) and (5.1.2) we know that $\rho_1(-1)$ and $\rho_2(-1)$ are congruent trivial (condition (2.2.1)). Moreover, since both $\mathcal{S}$ and E are smooth outside primes above 2. The Galois representations ρ_1 and ρ_2 are unramified outside of the finite set $S = \{2, \infty\}$. According to Theorem 0.0.2 we can find a covering set by the algorithm below:

1. Take $K_0 = K$, then for every $i \geq 0$, list all quadratic extensions L/K_i which satisfy the following conditions:

   (a) Unramified outside $S = \{2, \infty\}$;

   (b) For every prime place $\mathfrak{p}$ in K not dividing 2, and for every prime place $\mathfrak{P}$ in L above $\mathfrak{p}$, the corresponding local field extension has Galois group of exponent no greater than 4.

2. Take K_{i+1} to be the compost of all the L listed above. And build K_{i+2} inductively, until either

   (a) There is no such quadratic extension L/K_i satisfying the conditions in step (1), which means this K_i is the maximal exponent 4 pro-2 extension above K which is unramified outside S, or;

   (b) $i = 8$, which means $K_i = K_S$ in Theorem 0.0.2.

3. Denote by K_{max} the field which the above process ends up to, and use the effective Chebotarev density theorem to find a bound B of the absolute norm of Frobenius classes for the covering set of $\mathrm{Gal}(K_{max}/K)$. Then

$$T = \{F_{\mathfrak{p}} | N_{K/\mathbb{Q}}(\mathfrak{p}) \leq B\}$$

   is sufficient to be a covering set.

In our situation, we have $K_1 = \mathbb{Q}(\zeta_{24})$. Then K_2/K_1 has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 5}$. But now $[K_2 : \mathbb{Q}] = 2^8 = 256$, which means K_2 is very hard to be constructed via computers. To get more information without extending K_2, recall that $\mathrm{Gal}(K_{max}/K)$ is a quotient of $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4$ where $K^{ur}_{\infty,2}(2)$ is the maximal pro-2 extension above K and unramified outside $S = \{2, \infty\}$. Hence we are reduced to finding a covering set of $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4$. By [19, Thm. 2], and calculations with help of computers, we find that:

1. $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)$ is isomorphic to the free group generated by two elements, hence $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4 \simeq B(2,4)$ (cf. Example 3.0.3).

2. The natural quotient map $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4 \to \mathrm{Gal}(K_2/K)$ has kernel isomorphic to $(\mathbb{Z}/2)^{\oplus 5}$, so $K_{max} = K_3$, and $\mathrm{Gal}(K_3/K_2)$ is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^{\oplus 5}$.

3. Since K_3/K_2 is an abelian extension, by Conductor-Discriminant formula, we get $disc(K_3) \leq 2^{109568}3^{4096}$. Assume Extended Riemann Hypotheses and apply the the following Theorem 5.2.1 and its remark to find a covering set

$$T := \{\mathfrak{p} \in K | N_{K/\mathbb{Q}}(\mathfrak{p}) \leq 7.03 \times 10^9\}.$$

Theorem 5.2.1. *[1, Thm. 5.1] Let Δ be the discriminant of L/K and take $n = [L : K]$. If we assume the Extended Riemann Hypotheses, then*

$$B(L/K) \leq (4 \log \Delta + 2.5n + 5)^2.$$

Remark 5.2.1. In practice, instead of using the above inequality, one can write a code to find a sharper bound with the idea in [1, § 3,4]. This is what we did in our case.

5.3 Conjugacy classes in $B(2,4)$, proof of Theorem 0.0.3

The covering set $T = \{\mathfrak{p} | N_{K/\mathbb{Q}}(\mathfrak{p}) \leq 7.03 \times 10^9\}$ is sufficient large to verify Theorem 0.0.1 by Faltings-Serre method. But even with a Xeon-E3 CPUs, it would take years to finish calculations. In this subsection, we reduce the size of T. The main result of this subsection is Theorem 5.3.2. With this theorem we can find a new covering set consisting only 75 prime ideals without requiring Extended Riemann Hypotheses. Our method is based on the group structure of $B(2,4)$ and Galois theory. For this section, we loose our restriction from letting K and ρ_i $(i = 1, 2)$ by supposing they are as stated in Theorem 0.0.3. Hence taking $K = \mathbb{Q}(\sqrt{-3})$ and ρ_1 and ρ_2 to be the selfdual representations induced by V_ℓ and $Sym^2(T_E)$, we prove Theorem 0.0.1.

Recall that if we have a covering set of $\mathrm{Gal}(K^{ur}_{2,\infty}/K)$, then to verify Theorem 0.0.1, we need to compare the trace of ρ_1 and ρ_2 for every element in the covering set. But in fact if two elements x and y are conjugate in $\mathrm{Gal}(K^{ur}_{2,\infty})$, then $\rho_i(x)$ and $\rho_i(y)$ have the same trace $(i = 1, 2)$. Hence to verify Theorem 0.0.1, we only need to check if ρ_1 and ρ_2 share the same trace for every representative of conjugate classes in T. Therefore, a covering set of the conjugate classes of $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4 \simeq B(2,4)$ will be sufficient to verify Theorem 0.0.1.

So we are reduced to find a covering set (still denoted by T) of the (conjugate) classes in $B(2,4)$. If we denote by $C_1, \cdots, C_{88}$ the 88 classes in $B(2,4)$, then to find a covering set of those C_i's, we need to tell which class $F_\mathfrak{p}$ belongs to for every given prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. This is not easy since the isomorphism between $\mathrm{Gal}(K^{ur}_{2,\infty})$ and $B(2,4)$ is not explicit. However, suppose we can find 88 distinct Frobenius elements $F_{\mathfrak{p}_i}$ and show that they belong to distinct classes, then the set $\{\mathfrak{p}_i\}$ is a desired covering set.

In order to differentiate non-conjugate Frobenius elements, we note that if N is a normal subgroup of $B(2,4)$, then for each i either $C_i \subset N$ or $C_i \cap N = \emptyset$. Thus we can differentiate two classes C_i and C_j if there is a normal subgroup N which contains

one of the two classes and is disjoint with the other. Hence, if we can find a finite set $\mathcal{N}$ of normal subgroups of $B(2,4)$ such that every conjugate class has a unique "intersection intersection pattern" (Definition 5.3.1) with respect to elements in $\mathcal{N}$. Then $\mathcal{N}$ can be used to differentiate all the classes. On the other hand, since every Frobenius element $F_{\mathfrak{p}}$ represents a conjugate classes of elements in the Galois group, we can tell that $F_{\mathfrak{p}_1}$ and $F_{\mathfrak{p}_2}$ are not in the same conjugate class if one of them is in a normal subgroup N and another is not. Therefore, if we are able to find 88 F_p's so that they have distinct "intersection patterns" with respect to elements in $\mathcal{N}$ above, then these 88 $F_{\mathfrak{p}}$'s will provide a desired covering set. To realize this method in an effective way, we need the following notations and definitions.

Definition 5.3.1. For a group G, let $\mathcal{C} = \{C_1, \cdots, C_r\}$ be a set of (conjugate) classes and let $\mathcal{N} = \{N_1, \cdots, N_s\}$ be an ordered set consisting of normal subgroups of G. For each $1 \leq i \leq r$ and $1 \leq j \leq s$, take

$$\delta_{i,j} = \begin{cases} 1 & \text{if } C_i \subset N_j \\ 0 & \text{otherwise} \end{cases}.$$

Then for a fixed C_i, we define the vector $P(C_i, \mathcal{N}) = (\delta_{i,1}, \delta_{i,2}, \cdots, \delta_{i,s})$ the *pattern of* C_i *with respect to* $\mathcal{N}$. If there is no confusion, we will simply call it the *pattern of* C_i and write $P(C_i)$ for short.

Definition 5.3.2. Let F be a number field, denote by $\mathcal{L} = \{L_1, \cdots, L_s\}$ an ordered set of finite Galois extensions F. For a prime ideal $\mathfrak{p}$ in F, we define

$$\delta(\mathfrak{p}, L_j) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ is toltally split in } L_j \\ 0 & \text{otherwise} \end{cases}.$$

The vector $P(\mathfrak{p}, \mathcal{L}) = (\delta(\mathfrak{p}, L_1), \cdots, \delta(\mathfrak{p}, L_s))$ is defined to be the *pattern of* $\mathfrak{p}$ *with respect to* $\mathcal{L}$. When there is no confusion, we call it the *pattern* of $\mathfrak{p}$ and simply write $P(\mathfrak{p})$.

We can rephrase our method by the definitions above. We want to find an order set $\mathcal{N}$ of normal subgroups of $B(2,4) \simeq \mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4$ such that every class has a unique pattern with respect $\mathcal{N}$. Then by Galois theory, for every $N_j \in \mathcal{N}$, we denote by L_j/K the corresponding Galois intermediate extension of $K^{ur}_{2,\infty}/K$. Then take $\mathcal{L} = \{L_j\}$ to be the corresponding ordered set. Then we know that

$$F_{\mathfrak{p}} \in C_i \text{ if and only if } P(\mathfrak{p}, \mathcal{L}) = P(C_i, \mathcal{N}).$$

Hence if we want to find a desired covering set, we only need to factor the prime ideals of $\mathcal{O}_K$ one-by-one until we find 88 primes with distinct patterns. Based on this idea, we will state the main theorem of this section (Theorem 5.3.2) after some definitions and lemmas.

Definition 5.3.3. Let F be a number field, a Galois extension L/F is called an *exponent* 4 *extension* if its Galois group $\mathrm{Gal}(L/F)$ has exponent 4.

Lemma 5.3.1. *For every number field in Theorem 0.0.3, there are exact* 7 *quartic exponent* 4 *Galois extensions which are unramified outside* $\{2, \infty\}$*. In particular, among them there is exact one biquadratic extension.*

Proof. According to [19, Theorem 2] we know that for each K satisfying the condition in Theorem 0.0.3, its maximal pro-2 extension which is unramified outside $\{2, \infty\}$ (i.e. $K^{ur}_{\infty,2}(2)/K$) has a free pro-2 Galois group generated by 2 elements. Hence $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4 \simeq B(2,4)$. The Burnside group $B(2,4)$ has order 2^{12}. One can find by calculation that there are exact 7 order 2^{10} normal subgroups N of $B(2,4)$, and exact one of them satisfies $B(2,4)/N \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. This finishes the proof. □

Theorem 5.3.2. *Let K and ρ_1, ρ_2 be as in Theorem 0.0.3. Denote by L_i ($i = 1, \cdots, 7$) the* 7 *Galois quartic extensions of K which are unramified outside $\{2, \infty\}$, and let L_1 be the unique biquadratic extension of K. For each $1 \leq i \leq 7$, let $\mathcal{L}_1 =$*

$\{M_{i,s}\}$ be an ordered set of all exponent 4 Galois extensions of L_i such that $M_{i,s}/L_i$ is unramified outside $\{2,\infty\}$, and $[M_{i,s}:L_i] \leq 2^{r_i}$ with $r_i = 3$ if $i = 1$ and 2 otherwise. Then we have the followings.

1. *There are 63 prime ideals $\mathfrak{p}_h$ $(h = 1, \cdots, 63)$ of $\mathcal{O}_K$ satisfying the followings.*
   (a) *$\mathfrak{p}_h \nmid 2$ and $\mathfrak{p}_h$ is totally split in $\mathcal{O}_{L_1}$.*
   (b) *Let $U_1 = \{\mathfrak{P}_{h,j}\}$ consist of all prime ideals $\mathfrak{P}_{h,j}$ of $\mathcal{O}_{L_1}$ such that $\mathfrak{P}_{h,j}$ is lying above $\mathfrak{p}_h$. Then the set of patterns $\{P(\mathfrak{P}_{h,j}), \mathcal{L}_1\}$ has 204 elements.*
2. *For each $i \in \{2, \cdots, 7\}$, there are 2 prime ideals $\mathfrak{p}_h$ $(h = 1, 2)$ of $\mathcal{O}_K$ satisfying the followings.*
   (a) *$\mathfrak{p}_h \nmid 2$ and $\mathfrak{p}_h$ is totally split in $\mathcal{O}_{L_i}$.*
   (b) *Let $U_i = \{\mathfrak{P}_{h,j}\}$ consist of all prime ideals $\mathfrak{P}_{h,j}$ of $\mathcal{O}_{L_i}$ such that $\mathfrak{P}_{h,j}$ is lying above $\mathfrak{p}_h$. Then the set of patterns $\{P(\mathfrak{P}_{h,j}), \mathcal{L}_i\}$ has 8 elements.*

Let T be the collection of all the prime ideals of $\mathcal{O}_K$ stated in (1) and (2), then

$$\rho_1 \sim \rho_2 \quad \text{if and only if} \quad tr(\rho_1(F_\mathfrak{p})) = tr(\rho_2(F_\mathfrak{p})) \text{ for all } \mathfrak{p} \in T.$$

In particular, when $K = \mathbb{Q}(\sqrt{-2})$, the set T is given by Table 5.2. When $K = \mathbb{Q}\sqrt{-3}$, T is given by Table 5.3.

Remark 5.3.1. The above results do not change if we change the order of L_i in $\mathcal{L}$.

Proof of Theorem 5.3.2. Let $\mathcal{N} = \{N_1, \cdots, N_7\}$ be the ordered set consisting of all normal subgroups of order $\geq 2^{10}$ (i.e. those corresponding to Galois extensions over K and having absolute extension degree $\leq 2^3 = 8$). In particular we fix N_1 to be the unique group such that $B(2,4)/N_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. By calculating the patterns of every C_i with respect to $\mathcal{N}$, we partially differentiate them in to 7 subsets $TC_1, \cdots, TC_7$. In

Table 5.1 we list all the 7 subsets by writing down their classes the common pattern of the classes in each subset. The characteristic of the sets TC_i $(i = 0, \cdots 7)$ can be read from this table.

TC_i	classes in the set	Description of the pattern
TC_1	$C_1, \cdots, C_{64}$	$\delta_{i,1} = 1$
TC_2	$C_{65}, C_{71}, C_{84}, C_{85}$	$\delta_{i,j} = 1$ for exact one of $2 \leq j \leq 7$
TC_3	$C_{66}, C_{72}, C_{74}, C_{78}$	
TC_4	$C_{67}, C_{68}, C_{87}, C_{88}$	
TC_5	$C_{69}, C_{80}, C_{82}, C_{86}$	
TC_6	$C_{70}, C_{75}, C_{81}, C_{83}$	
TC_7	$C_{73}, C_{76}, C_{77}, C_{79}$	

Table 5.1. Classes of the same patterns with respect to $\mathcal{N} = \{N_1, \cdots, N_7\}$

Remark 5.3.2. (a) Theoretically, adding more normal subgroups of $B(2,4)$ to $\mathcal{N}$ will be helpful to refine Table 5.1. However in it is hard in practice since the normal subgroups we do not consider are corresponding to extension of degree $\geq 2^7 = 128$, which take too much time to construct. Hence we finally take our $\mathcal{N}$ to be as above.

(b) Changing the order of elements in $\mathcal{N}$ does not change the classification in Table 5.1.

Now in order to differentiate the classes in TC_1, we let $\mathcal{N}_1$ to be the ordered set of all normal subgroups of N_1 with order $\geq 2^7$. Then applying the same idea as above except with $\mathcal{N}$ replaced by $\mathcal{N}_1$, we find the followings by calculation.

1. A conjugate class of $B(2,4)$ may not still be a single conjugate class with respect to N_1. In fact, for each C_i for $i = 1, \cdots, 64$, we have $C_i = \bigsqcup C_{i,k}$ is a disjoint union of several conjugate classes of N_1. By calculation, there are totally 208 sub classes $\{C_{i,k}\}$ spitted from $C_1, \cdots, C_{64}$.

2. By computing all the patterns $P(C_{i,k}, \mathcal{N}_1)$, we find 204 distinct patterns. In particular, except that the sub classes from C_{63} have the same patterns with the sub classes from C_{64}, each other sub class has a unique pattern with respect to $\mathcal{N}_1$.

3. If $g \in C_{63}$, then $g^{-1} \in C_{64}$.

Therefore, to find a covering set of the set $\{C_i\}_{i=1,\cdots,64}$, we are reduced to finding a covering set of $\{C_{i,k}\}_{i=1,\cdots,64}$. For the later, take $\mathcal{L}_1$ to be the ordered set in Theorem 5.3.2, then we need to find 204 prime ideals of $\mathcal{O}_K$ which totally splits in L_1, and have distinct patterns with respect $\mathcal{L}_1$. Note that there is no need to differentiate C_{63} from C_{64} since by part (3) above, once we find an element in either one of the two classes, we automatically find an element in another. This proves part (1) of Theorem 5.3.2.

To differentiate the classes in each of TC_i $(i = 2, \cdots, 7)$, we let $\mathcal{N}_i$ be the ordered set of all normal subgroups of N_i with order $\geq 2^8$. Then the classes in each T_i will split into 16 sub classes of N_i. By computing their patterns with respect to $\mathcal{N}_i$, we have 8 distinct patterns. Moreover, if g is in a sub class C then g^{-1} is the sub class C' such that $C' \neq C$ but $P(C, \mathcal{N}_i) = P(C', \mathcal{N}_i)$. Hence to find a covering set to each of T_i $(i = 2, \cdots, 7)$, we take $\mathcal{L}_i$ to be the corresponding ordered set in Theorem 5.3.2, and then find 8 prime ideals of $\mathcal{O}_K$ which totally splits in L_i and have distinct patterns with respect to $\mathcal{L}_i$. This proves part (2) of Theorem 5.3.2.

Finally, if we denote by T_i $(i = 1, \cdots, 7)$, the covering TC_i, and take T to be the union of all T_i. Then T is sufficient large in the sense that every conjugate class has a representative in terms of an element in T or the inverse of an element in T. As conclusion, by Faltings-Serre method, to verify whether ρ_1 is equivalent to ρ_2, we only need to test if they have the same characteristic polynomial for every element in T. In particular, when $K = \mathbb{Q}(\sqrt{-2})$ and $K = \sqrt{-3}$, the corresponding sets T are given by Tables 5.2 and 5.3 respectively. This finishes the proof. $\square$

T_i	prime integers lying below $\mathfrak{p}$
T_1	439, 503, 607, 823, 1231, 1399, 1423, 3049, 3089 3449, 3823, 3967, 4057, 4177, 4201, 4217, 4409, 4937 5737, 6121, 6353, 6553, 7793, 9377, 9473, 9769, 11113 11969, 12241, 16433, 18593, 25409, 26993, 27809, 67217 67489, 68449, 126641, 132929, 268817, 392737
T_2 T_3 T_4 T_5 T_6 T_7	29,67,97,137,139,193,251,283

Table 5.2. The primes in T when $K = \mathbb{Q}(\sqrt{-2})$

T_i	prime integers lying below $\mathfrak{p}$
T_1	419, 461, 587, 617, 647, 653, 761, 911, 929, 983, 1439, 2273 2521, 3023, 3793, 3889, 4297, 4513, 4969, 5113, 6337, 6673 7393, 8161, 8329, 8353, 8641, 9049, 9337, 9721, 10369 10729, 11113, 11161, 12577, 13873, 14713, 15121, 15913 19777, 21193, 25537, 31393, 40177, 57697, 71233, 74353 87697, 98641, 100801, 104593, 115153, 234721
T_2 T_3 T_4 T_5 T_6 T_7	37,127,181,199,211,271,379,523,619,631

Table 5.3. The primes in T when $K = \mathbb{Q}(\sqrt{-3})$

Proof of Theorem 0.0.3. It immediately follows from Theorem 5.3.2. □

Proof of Theorem 0.0.1. First by (1.5.1) and (5.1.2) we know that $\rho_1(-1)$ and $\rho_2(-1)$ are congruent trivial. Then by running code on twelve CPUs, it takes about 15 days to finish the comparison. As result, we know that the two representations in Theorem 0.0.1 are equivalent. Then by the fact that E does not have complex multiplication and apply Serre's open image theorem (Theorem 1.4.4) and its Corollary 1.4.4.1 we

know that the two representations in Theorem 0.0.1 are both irreducible, thus they are isomorphic to each other. This finishes the proof of Theorem 0.0.1. □

CHAPTER 6

RELATED PROGRAMS

In this chapter, we state some future works.

6.1 Nonselfdual representaitons

As Remark 0.0.4 states, Theorem 0.0.3 and 5.3.2 also work for 3-dimensional non-selfdual representations. In fact, the non-selfdual representations are even more interesting. This is because in the spirit of Langlands program, they are expected to correspond to certain GL_3-type automorphic forms which are not induced from the GL_2-type ones.

In [33], van Geemen and Top give some evidence for the fact that the 3-dimensional non-selfdual representation induced by the the surface

$$S_a : t^2 = xy(x^2-1)(y^2-1)(x^2-y^2+axy)$$

with $a = 2$ ([33, § 3.2]) should relate to the GL_3-automorphic representaiton defined by a cuspidal cohomology class in $H^3(\Gamma_0(128), \mathbb{C})$ ([33, § 2]). Their claim is supported by the fact that the two representations coincide for primes $3 \leq p \leq 67$. However, limited by both the theoretic study of Faltings-Serre method and the computational source at that time, they did not end up with a proof to their claim. Recently, a work of Ito, Koshikawa and Mieda [16] completes the proof of van Geemen and Top's conjecture. And one of the main tool used in this work is the Falthings-Serre method based on Grenié's criterion.

However, as we explained in the introduction that Grenié's criterion is limited to $G_{\mathbb{Q}}$-representations. While when $a = \sqrt{-2}$ and $K = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{-2})$, Theorem 5.3.2 can still provide a relative small set of primes T which can be used to verify the equivalence between the G_K-representation induced by S_a and its conjectural correspondence. If we can find and verify such equivalence, then this can be an evidence for the Langlands program even for $K \neq \mathbb{Q}$.

6.2 Faltings-Serre methods for GSp_4-representations

The Langlands program predicts deep connections between geometry and automorphic forms. The modularity conjecture claims the connection is encoded in associated L-functions and Galois representations. In particular, it is known that for every elliptic curve E over $\mathbb{Q}$ and of conductor N, there is a cuspidal newform $f \in S_2(\Gamma_0(N))$ of weight 2 and level N such that

$$L(E, s) = L(f, s).$$

One of the generalizations of the modularity conjecture is made precise by Brumer and Kramer [4, Conjecture 1.1], here we follow the version in [5, Conjecture 1.1.1]

Conjecture 6.2.1 (Paramodular conjecture)**.** *Given an abelian surface A over $\mathbb{Q}$ of conductor N and with $\mathrm{End}(A) = \mathbb{Z}$, there exists a cuspidal, nonlift Siegel paramodular newform f of degree 2, weight 2 and level N such that*

$$L(A, s) = L(f, s, spin).$$

Moreover, f is unique up to (nonzero) scaling and depends only on the isogeny class of A; and if N is square free, then this association is bijective.

The paramodular conjecture is still open, while it is supported by extensive experimental and theoretical evidence, see [4, 24, 18, 2] for instance. In particular, Brumer, Voight, Poor, Tornaría, Voight and Yuen[5] show the following result.

Theorem 6.2.1. *[5, Theorem 1.2.1] Let X be the curve over $\mathbb{Q}$ defined by*

$$y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x;$$

let $A = Jac(X)$ be its Jacobian, a typical abelian surface over $\mathbb{Q}$ of conductor 277. Let f be the cuspidal, nonlift Siegel paramodular form of genus 2, weight 2, and conductor 277, unique up to scalar multiple. Then

$$L(A, s) = L(f, s, spin).$$

Their verification makes use of a generalization of the Faltings-Serre method [5, § 2]. Their algorithm relies on the absolutely irreduciblity of the representations ([5, Theorem 2.1.4], [6, Théorème 1]). Here we say an ℓ-adic Galois representation ρ is *absolutely irreducible* if its residue representation

$$\bar{\rho} : G_K \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Z}_\ell) \to GL_n(\mathbb{F}_\ell) \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$$

is irreducible.

However, there are still non-absolutely irreducible Galois representations. In particular, the algorithm used in [5] cannot be applied to the case when the residue representations are trivial. Hence a definite algorithm which can be applied to all kinds of GSp_4-representations will be useful in practice. As analogs to Theorem 0.0.2 and 0.0.3, we can try to refine the Faltings-Serre method in from both group algebra (i.e. Lie algebra) aspect and Galois extension aspect.

6.3 Potential Improvements and Generalizations of the Faltings-Serre Method

In our work, we improve the criterion of comparison of two Galois representations under the self-dual assumption. However, even the improved criterion is far from being useful in practice. So in this plan, we want to improve our criterion. Precisely,

Goal: *Improve the criterion with addition assumptions.*

In the following, we list some additional assumptions under which we can potentially improve the criterion.

- **Comparison of self-dual representations of the same type.** We say that two representations are of the same type if their irreducible subrepresentations, up to a permutation, are of the same dimensions. Then we can ask

  Question: *Can we improve the criterion for comparison of two self-dual representations that are of the same type?*

  The answer is yes, in fact we can show that up to a quadratic twist, every irreducible self-dual 3-dimensional representation is the symmetric square of a 2-dimensional representation. Thus to compare a pair of irreducible 3-dimensional self-dual ℓ-adic Galois representations, we are reduced to comparing the pair of 2-dimensional Galois representations which give rise to the original 3-dimensional representations. With the method that is used in our work, we can find a criterion, which only depends on the field where the traces are defined, the ramified primes, for comparing the two 2-dimensional ℓ-adic Galois representations. That criterion is potentially better compared with the one in our work.

  With the same idea we can find a potentially better criterion for the case when both of the selfdual representations can be factored as a direct sum of a 1-dimensional subrepresentation and a 2-dimensional subrepresentation, and

also for the case that the two representations are totally factored into three 1-dimensional subrepresentations. However, given two 3-dimensional selfdual representations, we do not know if they are of the same type. So our next question is

Question: *Is there an effective way to determine whether the semi-simplification of a given Galois representation is irreducible or not?*

Unfortunately, we do not have an answer to this question.

- **Comparison of Galois representations with irreducible reduced representations.** In Faltings-Serre method, the derivation group δ of two given ℓ-adic Galois representations ρ_1, ρ_2 is easy to define but hard to compute in the sense that its structure is not clear for a general pair of representations. This is particularly problematic when one of the representations is highly reducible, i.e. the images of reduced representations $\mod \ell^r$ are trivial for a large integer r. And that is the case in Theorem 0.0.1. However, if the reduced representations of the two representations are irreducible, we can get a better control over the structure of the derivation group, and hence a better bound for the Faltings-Serre method. To realize this, we need to study possible liftings of irreducible reduced representations up to conjugations of $GL_3(\mathbb{Z}_\ell)$, then study the derivation group of each pair of representatives from the classes.

6.4 Faltings-Serre methods related to other Burnside groups

In our work, we reduce the verification of Theorem 0.0.1 to find a covering set to $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)_4$ with $K = \mathbb{Q}(\sqrt{-3})$. In order to find a realizable covering set, we make use of the theorem of [19] which describes the group structure of $\mathrm{Gal}(K^{ur}_{\infty,2}(2)/K)$. As a similar question, we can ask if both Jossy's method can be used to $\mathrm{Gal}(K^{ur}_{\infty,p}(p)/K)$ for some odd prime integers p. If the answer is

positive, then a p-adic analog of Theorem 5.3.2 should exist and can be used to compare two ℓ-adic Galois represenations with $\ell = p$ and are unramified outside $\{p, \infty\}$.

APPENDIX

BACKGROUNDS OF LIE ALGEBRAS

This chapter is devoted to fill the backgrounds of Lie algebras that are needed in our paper.

A.1 Solvable Lie algebras

In this subsection, $\mathfrak{g}$ is a Lie algebra which is not necessary selfdual.

Definition A.1.1. Given a Lie algebra $\mathfrak{g}$, it is called solvable if the derived series: $\mathfrak{g}^{(0)} = \mathfrak{g}, \mathfrak{g}^{(n+1)} := [\mathfrak{g}^{(n)}, \mathfrak{g}^{(n)}]$ terminates; and it is called Nilpotent if the lower central seires: $\mathfrak{g}^0 = \mathfrak{g}, \mathfrak{g}^{n+1} := [\mathfrak{g}^n, \mathfrak{g}]$ terminates. The unique maximal solvable ideal of $\mathfrak{g}$ is denoted by $Rad(\mathfrak{g})$, and $\mathfrak{g}$ is called semisimple if $Rad(\mathfrak{g}) = 0$.

It is obvious that $\mathfrak{g}/Rad(\mathfrak{g})$ is always semisimple.

Definition A.1.2. Given a Lie algebra $\mathfrak{g}$, the Borel subalgebras of $\mathfrak{g}$ are defined to be the maximal solvable subalgebras of $\mathfrak{g}$.

Proposition A.1.1. *[15, §4.1, Cor. 4.1,Lie's Theorem] If $\mathfrak{g}$ is solvable, then with respect to a suitable basis, all elements in $\mathfrak{g}$ are upper triangular.*

Recall that every semisimple Lie algebra $\mathfrak{g}$ has its root system [15, chap. II to IV] such that $\mathfrak{g} = H \oplus \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha$, where H is a maximal toral subalgebra of $\mathfrak{g}$ (i.e. a subalgebra consisting of semisimple elements) and Φ is the set of roots, i.e., nonzero elements in the dual space H^* such that there exists $x \in \mathfrak{g}$, where $[h, x] = \alpha(h)x$ for all $h \in H$. Moreover, for each $\alpha \in \Phi$, we have a triple $(h_\alpha, x_\alpha, y_\alpha)$, where $x_\alpha \in \mathfrak{g}_\alpha, y_\alpha \in \mathfrak{g}_{-\alpha}, h_\alpha = [x_\alpha, y_\alpha] \in H$.

Proposition A.1.2. *If $\mathfrak{g}$ is semisimple Lie algebra of dimension ≤ 5, then $\mathfrak{g}$ is simple, and isomorphic to $\mathfrak{sl}_2$ as an abstract Lie algebra.*

Proof. In fact, if $\dim \mathfrak{g} \leq 5$, then the Φ has at most two elements since otherwise there are at least four roots, which implies $\dim H \geq 2$ and hence $\dim \mathfrak{g} \geq 6$, contradiction. On the other hand, $\dim \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha \geq 2$ (since otherwise $\mathfrak{g} = H$. But H is abelian [15, Lemma. 8.1], thus solvable, contradiction). Now the proposition follows from the fact that $\mathfrak{sl}_2$ is the only dimensional 3 semisimple Lie algebra up to isomorphism. $\square$

BIBLIOGRAPHY

[1] Bach, E., and Sorenson, J. Explicit bounds for primes in residue classes. *Math. Comp. 65* (1996), 1717–1735.

[2] Berger, Tobias, Dembélé, Lassina, Pacetti, Ariel, and Şengün, Mehmet Haluk. Theta lifts of Bianchi modular forms and applications to paramodularity. *J. Lond. Math. Soc. (2) 92*, 2 (2015), 353–370.

[3] Boston, N. A refinement of the faltings-serre method. In *Number theory (Paris, 1992–1993)*, vol. 215 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, 1995, pp. 61–68.

[4] Brumer, Armand, and Kramer, Kenneth. Paramodular abelian varieties of odd conductor. *Trans. Amer. Math. Soc. 366*, 5 (2014), 2463–2516.

[5] Brumer, Armand, Pacetti, Ariel, Poor, Cris, Tornaría, Gonzalo, Voight, John, and S. Yuen, David. On the paramodularity of typical abelian surfaces, aug 2018.

[6] Carayol, Henri. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, vol. 165 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 213–237.

[7] Chênevert, G. *Exponential sums, hypersurfaces with many symmetries and Galois represen- tations.* PhD thesis, McGill University, 2008.

[8] Chenevier, G., and Harris, M. Construction of automorphic galois representations, ii. *Camb. J. Math. 1*, 1 (2013), 53–73.

[9] Chin, C. Independence of ℓ in lafforgue's theorem. *Adv. Math. 180*, 1 (2003), 64–86.

[10] Diamond, F., and Shurman, J. *A First Course in Modular Forms*, vol. 228 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[11] Dieulefait, L., Guerberoff, L., and Pacetti, A. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp. 270*, 79 (2010), 1145–1170.

[12] Dixon, J. D., du Sautoy, M. P. F, Mann, A., and Segal, D. *Analytic Pro-p groups.* Cambridge University Press, Cambridge, 1999.

[13] Faltings, G. Endlichkeitssätze für abelsche varietätenüber zahlkörpern. *Invent. Math. 73*, 3 (1983), 349–366.

[14] Grenié, Loïc. Comparison of semi-simplifications of galois representations. *J. Algebra 316*, 2 (2007), 608–618.

[15] Humphreys, James E. *Introduction to Lie algebras and representation theory*, second ed., vol. 9. Springer-Verlag, Now York, 1978.

[16] Ito, T., Koshikawa, T., and Mieda, Y. Galois representations associated with a non-selfdual automorphic representation of gl(3), nov 2018.

[17] Jacobson, N. *Basic Algebra II*, second ed. W. H. Freeman and Company, New York, 1989.

[18] Johnson-Leung, Jennifer, and Roberts, Brooks. Siegel modular forms of degree two attached to Hilbert modular forms. *J. Number Theory 132*, 4 (2012), 543–564.

[19] Jossey, John. Galois 2-extensions unramified outside 2. *Journal of Number Theory 124*, 1 (2007), 42–56.

[20] Kloosterman, K. Hulek R., and Schütt, M. Modularity of calabi-yau varieties. In *Global Aspects of Complex Geometry*. Springer, 2006, pp. 271–309.

[21] Livné, R. Cubic exponential sums and galois representations. *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985) 67* (1987), 247–261.

[22] Milne, J. Lectures on etale cohomology, mar 2013.

[23] Milne, J. S. *Étale cohomology*. Princeton University Press, Princeton, N.J., 1980.

[24] Poor, Cris, and Yuen, David S. Paramodular cusp forms. *Math. Comp. 84*, 293 (2015), 1401–1438.

[25] Ribet, K. A. Abelian varieties over Q and modular forms. *Algebra and topology (Taejŏn) Korea Adv. Inst. Sci. Tech., Taejŏn, 1992* (1992), 53–79.

[26] Schneider, P. *p-Adic Lie Groups*, vol. Grundlehren Math. Wiss. 344. Springer, 2011.

[27] Schoen, C. Algebraic cycles on certain desingularized nodal hypersurfaces. *Math. Annals 270*, 1 (1985), 17–27.

[28] Serre, Jean-Pierre. *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.

[29] Serre, Jean-Pierre. *Résumé des cours au Collége de France 1984-1985, In Euvres*. Springer-Verlag, Berlin, 2000.

[30] Silverman, J. H. *The arithmetic of elliptic curves*, second ed., vol. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[31] Socrates, J., and Whitehouse, D. Unramified hilber modular forms, with examples relating to elliptic curves. *Pacific J. Math 219*, 2 (2005), 333–364.

[32] Tobin, J. J. *On Groups with Exponent 4*. Thesis, University of Manchester, 1954.

[33] van Geemen, Bert, and Top, Jaap. A non-selfdual automorphic representation of GL_3 and a Galois representation. *Invent. Math. 117*, 3 (1994), 391–401.

[34] van Geemen, Bert, and Top, Jaap. Selfdual and non-selfdual 3-dimensional Galois representations. *Compositio Math. 97*, 1-2 (1995), 51–70. Special issue in honour of Frans Oort.

[35] Winternitz, P. Subalgebras of lie algebras. example of $\mathfrak{sl}(3, r)$. *Symmetry in physics CRM Proc. Lecture Notes*, 34 (2004), 215–227.