Title
Automorphy Lifting Theorems

Author
Kalyanswamy, Sudesh

Publication Date
2017

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA

Los Angeles

Automorphy Lifting Theorems

A dissertation submitted in partial satisfaction

of the requirements for the degree

Doctor of Philosophy in Mathematics

by

Sudesh Kalyanswamy

2017

ABSTRACT OF THE DISSERTATION

Automorphy Lifting Theorems

by

Sudesh Kalyanswamy

Doctor of Philosophy in Mathematics

University of California, Los Angeles, 2017

Professor Chandrashekhar Khare, Chair

This dissertation focus on automorphy lifting theorems and related questions. There are two primary components.

The first deals with residually dihedral Galois representations. Namely, fix an odd prime p, and consider a continuous geometric representation $\rho : G_F \to \mathrm{GL}_n(\mathcal{O})$, where F is either a totally real field if $n = 2$, or a CM field if $n > 2$, and $\mathcal{O}$ is the integer ring of a finite extension of $\mathbb{Q}_p$. The goal is to prove the automorphy of representations whose residual representation $\bar{\rho}$ has the property that the restriction to $G_{F(\zeta_p)}$ is reducible, where ζ_p denotes a primitive p-th root of unity. This means the classical Taylor-Wiles hypothesis fails and classical patching techniques do not suffice to prove the automorphy of ρ. Building off the work of Thorne, we prove an automorphy theorem in the $n = 2$ case and apply the result to elliptic curves. The case $n > 2$ is examined briefly as well.

The second component deals with the generic unobstructedness of compatible systems of adjoint representations. Namely, given a compatible system of representations, one can consider the adjoints of the residual representations and determine whether the second Galois cohomology group with the adjoints as coefficients vanishes for infinitely many primes. Such a question relates to classical problems such as Leopoldt's conjecture. While theorems are hard to prove, we discuss heuristics and provide computational evidence.

The dissertation of Sudesh Kalyanswamy is approved.

Haruzo Hida

Don Blasius

Michael Gutperle

Chandrashekhar Khare, Committee Chair

University of California, Los Angeles

2017

To my parents and fiancé for

their constant love and support.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGMENTS

Firstly, I want to thank my advisor, Chandrashekhar Khare, whose guidance has been invaluable throughout my time in graduate school. He was helpful in not only suggesting the problems, but also guiding me and answering any questions I had. Without his help, this thesis could not exist. I would also like to thank the rest of my committee, Professors Haruzo Hida, Don Blasius, and Michael Gutperle, for taking the time to read and comment on this thesis.

There are, of course, so many other people to acknowledge, as the journey to get to this point was not a short one. I have wanted to be a mathematician since I was a little kid, and along the way my parents did everything in their power to provide me with the opportunities and resources to make that happen. I will always be eternally grateful to them for this and everything else they have done for me in life. I also need to give a shout out to my sister, who put up with so many of my math ramblings throughout the years. I want to thank my grandfather who showed me many math tricks when I was a kid, and who is probably very happy that they did not go to waste.

The path through graduate school is not an easy one to take, but having a good group of people around you makes it easier. There are not enough words to describe how much I am indebted to Josie Bailey, who is a constant source of love, support, and encouragement; she is always pushing me to be better. I also want to mention Zach Norwood, who was my office mate all five years, Katie Arterburn, Melissa Lynn, and Joe Hughes. All of them are incredible friends, though Zach slightly less so since he refuses to play tennis anymore. Thankfully Joe was always there for our weekly tennis.

Two professors that I have had deserve special credit. The first is Marty Lewinter at SUNY Purchase, who was my mentor throughout my high school years. He introduced me to mathematical research and opened my eyes to many interesting topics. The second is Ravi Ramakrishna at Cornell University. He taught me so many of the preliminary topics needed for modern number theory, was my undergraduate thesis advisor, and was (and still is) always there to talk math or life.

All my wonderful friends from Chappaqua deserve credit as well; they have been there for me since middle school, some even earlier. This includes Jared LaPorta, Ross Carstens, Ben Kleinman, Chris Gabriele, David Thomason, David Roher, and many others that I cannot include since I have gone on long enough already.

In terms of this dissertation, the final chapter is from a project I am currently working on with my advisor, Chandrashekhar Khare, as well as Gebhard Böckle and David Guiraud of the University of Heidelberg. Some of the programs used to generate the computer data in that chapter are slightly modified versions of the ones written by David Guiraud. I want to thank them for allowing me to join their team.

VITA

2011-2012	Attended University of Oxford
2012	B.A. (Mathematics with Honors), Cornell University.
2012-2017	Teaching Assistant, Department of Mathematics, University of California, Los Angeles
2015	Graduate Student Instructor, Department of Mathematics, University of California, Los Angeles

PUBLICATIONS

S. Karimi, M. Lewinter, S. Kalyanswamy, *On the Equitability of Multiply-connected Monolayered Cyclofusene*, Journal of Mathematical Chemistry, Vol. 41, No. 1, 2007

S. Karimi, M. Lewinter, S. Kalyanswamy, *Bilayered Cyclofusene*, Journal of Mathematical Chemistry, Vol. 43, No. 2, 2008

S. Kalyanswamy, *Remarks on Automorphy of Residually Dihedral Representations*, to appear in Mathematical Research Letters, available at https://arxiv.org/abs/1607.04750

CHAPTER 1

Introduction

1.1 Main Questions

The overarching theme of this dissertation will be automorphy lifting theorems. The questions addressed in this thesis are of the following flavors:

Question 1.1.1. Under what conditions will a geometric Galois representation be "the same" as a Galois representation arising from an automorphic representation of GL_n over some adele ring.

Question 1.1.2. Given a compatible system of Galois representations, in what situations will a specific deformation problem be "generically unobstructed" as the prime varies.

All the terms used above will be defined in due course. Questions similar to 1.1.1 have been a focus of number theorists since around the time of Wiles' proof of Fermat's Last Theorem. Indeed, as will be discussed in the next section, Wiles' proof relied on proving the Shimura-Taniyama-Weil conjecture for semistable elliptic curves, which asked when the representations arising from semistable elliptic curves are the same as those arising from modular forms. There has been extensive work on Question 1.1.1 in the case $n = 2$, but not as much has been done in the higher dimensional (i.e. $n > 2$) setting.

The second question, on the other hand, is not one that has been thoroughly examined. It will be discussed in Chapter 5.

1.2 Galois Representations, Fermat's Last Theorem, and Automorphy Lifting

Number theorists are interested in finding rational solutions to polynomial equations. This is done not by trying to necessarily find every solution, but by studying the "symmetries" in the solutions. There is a group which encodes the symmetries to all solutions to every polynomial equation with rational coefficients, called the absolute Galois group of $\mathbb{Q}$, which is denoted $G_{\mathbb{Q}}$. This group is too large and mysterious, so instead we study its representations, which are continuous homomorphisms $G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ for some ring A.

Writing down such maps is not much easier than studying $G_{\mathbb{Q}}$, so it would be nice to have some natural sources of representations. The story of Fermat's Last Theorem and automorphy lifting has two main characters, both geometric objects from which Galois representations naturally arise: elliptic curves and modular forms. These representations will be introduced in Chapter 2.

We briefly describe the ideas of the proof of Fermat's Last Theorem. Recall that the theorem asserts:

Theorem 1.2.1. For $n > 2$, the following holds:

$$\mathrm{FLT}(n) : a, b, c \in \mathbb{Z} \text{ and } a^n + b^n = c^n \implies abc = 0.$$

The case $n = 3$ was proved by Euler in the 18th century, and the case $n = 4$ is due to Fermat. It is relatively straightforward to see that it suffices to prove $\mathrm{FLT}(p)$ for odd primes p. Kummer made the biggest contributions towards a proof when he showed that $\mathrm{FLT}(p)$ is true if p does not divide the class number of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, where ζ_p is a primitive p-th root of unity. However, a proof eluded mathematicians until the end of the 20th century.

A big step towards a proof was made when Frey [15] connected the problem to elliptic curves. His insight was to take a nontrivial solution to $\mathrm{FLT}(p)$, say $a^p + b^p + c^p = 0$, where a, b, c are all coprime, and create the elliptic curve

$$E = E_{a,b,c} : y^2 = x(x - a^p)(x + b^p).$$

Assume $a \equiv -1 \bmod 4$ and $2|b$. Attached to this elliptic curve, for any prime number q, is a corresponding Galois representation, denoted $\rho_{E,q} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_q)$ and an associated residual representation $\bar{\rho}_{E,q} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$. This residual representation can be gotten geometrically using torsion points of E, and it can also be gotten by reducing $\rho_{E,q}$ modulo the ideal $q\mathbb{Z}_q$.

Frey and Serre studied the properties of the residual representation. More precisely, they showed:

Theorem 1.2.2. [35, Theorem 3.1] Let $q = p$. With the assumptions and notation as above, the representation $\bar{\rho}_{E,p}$ is:

- Absolutely irreducible,
- Odd,
- Unramified outside $2p$, flat at p, and semistable at 2.

To prove Fermat's Last Theorem, it would suffice to prove that no such representation exists. This statement was unknown at the time of Wiles' proof, though it is now known from the proven Serre's conjecture. However, without the power of Serre's conjecture, Wiles needed a different approach. The observation was that it is true if one restricts to Galois representations arising from separate geometric objects, namely modular forms (to be explained in Chapter 2). Representations which are isomorphic to a representation arising from modular forms is called modular. An elliptic curve is called modular if $\rho_{E,q}$ is modular for some (equivalently all) q. The next chapter will make this more precise.

Wiles [44] and Taylor-Wiles [45] showed that semistable elliptic curves over $\mathbb{Q}$ are modular. Namely, that the representations gotten from this class of elliptic curves can also be gotten from modular forms. This is where they proved an modularity (or automorphy) lifting theorem. Such a theorem has the following shape: If ρ is a representation and there is an associated "residual" representation $\bar{\rho}$, then the modularity of $\bar{\rho}$ implies the modularity of ρ. In practice, such a theorem is hard to prove without imposing some conditions on the representations ρ and $\bar{\rho}$.

A deep theorem of Langlands and Tunnell gives the modularity of $\bar{\rho}_{E,3}$ assuming $\bar{\rho}_{E,3}$ is irreducible. Under this assumption, the automorphy lifting theorem of Wiles and Taylor-Wiles gives the automorphy of E. Wiles used a clever trick and the automorphy lifting theorem to deal with the cases where this assumption did not hold. A theorem of Ribet then shows that a modular representation with the required properties could not exist. The details of Wiles' ingenious "3-5 switch" trick will be given near the end of Chapter 3.

Since the time of this proof, number theorists have tried to prove the automorphy of other representations, not just those arising from elliptic curves. In the two-dimensional setting, many representations are known to be automorphic. However, in the higher dimensional case, less is known, partially due to the unproven Ihara's lemma.

1.3 Basic Notation

We first will take the time to establish the notation and terminology used throughout this dissertation. The basics of algebraic number theory and Galois theory will be assumed.

If F is a field, we will let $\overline{F}$ denote a choice of algebraic closure of F. If F is a number field and v is a place of F, then we write F_v for the completion of F at v, and $\overline{F}_v$ will be a choice of algebraic closure (in the case of v an archimedean place, the algebraic closure of $F_v = \mathbb{R}$ is $\mathbb{C}$).

If p is a rational prime, then S_p will denote the places of F above p. The infinite places of F will be denoted S_∞. The p-adic valuation val_p on $\overline{\mathbb{Q}}_p$ is normalized so that $\mathrm{val}_p(p) = 1$. With these choices having been made, we define the absolute Galois groups

$$G_F = \mathrm{Gal}(\overline{F}/F), \quad G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v),$$

and $I_{F_v} \subset G_{F_v}$ will denote the inertia subgroup.

If v is a finite place of F, then we can fix embeddings $\overline{F} \hookrightarrow \overline{F}_v$ which extend the standard embeddings $F \hookrightarrow F_v$. These choices determine embeddings $G_{F_v} \hookrightarrow G_F$. We will use q_v to denote the size of the residue field of F at v.

If S is a finite set of places of F, then $F_S \subset \overline{F}$ will be the maximal extension of F

unramified outside S, with Galois group $G_{F,S} = \mathrm{Gal}(F_S/F)$, which is naturally a quotient of G_F. If $v \notin S$ is a finite place of F, then the composite map $G_{F_v} \hookrightarrow G_F \to G_{F,S}$ factors through the quotient G_{F_v}/I_{F_v}, and $\mathrm{Frob}_v \in G_{F,S}$ will be the image of a geometric Frobenius element. If F is a number field, then $\mathbb{A}_F$ will denote the adele ring of F, and $\mathbb{A}_F^\infty$ will denote the finite adeles.

1.4 Structure of Dissertation

In Chapter 2, much of the necessary background information will be introduced. This dissertation uses ideas from Galois cohomology and Galois deformation theory, and so this material is carefully introduced, though most of the proofs are omitted and references are given instead. The topics include Galois representations, Galois cohomology, Galois deformation theory, and automorphic representations, in varying amounts of detail. The end of the chapter contains a discussion of the two methods of modularity lifting used in Chapter 3.

The last three chapters contain the original work for the purposes of this dissertation. Chapter 3 contains the work done on automorphy lifting in the two dimensional setting. Building off the work of Thorne [41], we examine the automorphy of geometric Galois representations which are residually dihedral. We then apply the theorem to the setting of elliptic curves.

Chapter 4 details our quest to prove the analogue of the main theorem of Chapter 3 for higher dimensional representations. This is very much a work in progress, and we describe the future of the project at the end of the chapter.

Chapter 5 describes work done jointly with Chandrashekhar Khare, Gebhard Boeckle, and David Guiraud on questions such as Question 1.1.2. This is mainly a computational project, and we provide heuristics and computational evidence for a couple of questions. This is also a project with future work to be done, again detailed at the end of the chapter.

CHAPTER 2

Background Information

This chapter is designed to introduce the reader to the concepts necessary for this dissertation. Section 2.1 first introduces a few examples of Galois representations and then delves into a survey of the theory of local representations. In Section 2.2, all the important definitions and theorems of Galois cohomology are presented with an eye towards the Galois deformation theory of Section 2.3, which is arguably the most important section for understanding this dissertation. Section 2.4 gives the very basics of the theory of automorphic representations, just enough to understand the notation and terminology of the next chapter, and finally Section 2.5 describes the two methods of automorphy lifting that will be used in the next chapter. Knowledge of both algebraic number theory and class field theory will be assumed throughout the chapter.

2.1 Galois Representations

2.1.1 Examples of Galois Representations

Galois representations seem mysterious at first, which is why it is important to keep in mind the examples which appear repeatedly. When studying these representations, it is best to find "natural sources," and these usually come from studying a Galois action on some geometric object. The objects themselves (e.g. elliptic curves, modular forms, etc.) would take some time to introduce, so we instead direct the reader to a few sources for more information.

2.1.1.1 Cyclotomic Character

Let F be a number field. For an integer $m \geq 1$, let $\mu_m(\overline{F}^\times)$ denote the m-th roots of unity of $\overline{F}^\times$, i.e.

$$\mu_m(\overline{F}^\times) = \ker(\overline{F}^\times \xrightarrow{x \mapsto x^m} \overline{F}^\times).$$

Consider the projective limit

$$\mu_{p^\infty}(\overline{F}^\times) = \varprojlim_n \mu_{p^n}(\overline{F}^\times).$$

This is sometimes denoted $T_p(\overline{F}^\times)$, called the p-adic Tate module of $\overline{F}^\times$. Each $\mu_{p^n}(\overline{F}^\times)$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, the isomorphism sending a primitive p^n-th root of unity to 1. Choosing a compatible system of primitive p^n-th roots of unity $(\zeta_{p^n})_{n\geq 1}$ (compatible in the sense that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$) yields an isomorphism $\mu_{p^\infty}(\overline{F}^\times) \cong \mathbb{Z}_p$. The group G_F acts compatibly on all $\mu_{p^n}(\overline{F}^\times)$, and thus acts on $\mu_{p^\infty}(\overline{F}^\times)$. This gives rise to a representation

$$\epsilon_p : G_F \to \mathrm{Aut}(\mu_{p^\infty}(\overline{F}^\times)) \cong \mathbb{Z}_p^\times,$$

called the p-adic cyclotomic character of F. Note that for $\sigma \in G_F$, the element $\epsilon_p(\sigma)$ describes the action of σ on the p-power roots of unity of $\overline{F}^\times$.

Lemma 2.1.1. The representation ϵ_p is unramified outside S_p, and for a finite place $v \notin S_p$, we have $\epsilon_p(\mathrm{Frob}_v) = q_v^{-1}$.

We can also consider the reduction $\bar{\epsilon}_p$ of ϵ_p modulo p, which is a representation

$$\bar{\epsilon}_p : G_F \to \mathbb{F}_p^\times,$$

called the mod p cyclotomic character. This map can also be gotten by considering the action of G_F on $\mu_p(\overline{F}^\times)$.

Remark 2.1.2. (1) This construction works over any field F of characteristic zero, not just number fields.

(2) If the prime p is clear from context, it is dropped from the notation.

2.1.1.2 Elliptic Curves

One possible source for this section is [33, Chapter III.6-7]. Let E be an elliptic curve over a number field F, and let $m \geq 2$ be an integer. As an abelian group, the m-torsion $E[m]$ of the elliptic curve is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ([33, Corollary 6.4]). As in the previous section, we consider the p-adic Tate module, this time of E:

$$T_p(E) = \varprojlim_n E[p^n],$$

the inverse limit being taken with respect to the multiplication by p maps on E. As a $\mathbb{Z}_p$-module, the Tate module $T_p(E) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. The group G_F acts compatibly on each of the $E[p^n]$, and so we obtain a representation

$$\rho_{E,p} : G_F \to \mathrm{Aut}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

We can again reduce $\rho_{E,p}$ modulo the maximal ideal $p\mathbb{Z}_p \subset \mathbb{Z}_p$, and this yields a representation

$$\bar{\rho}_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{F}_p),$$

which is also gotten by considering the action of G_F on the p-torsion of E, i.e. on $E[p]$. The most important property of $\rho_{E,p}$ (for the purposes of this thesis) is the following:

Proposition 2.1.3. The determinant of $\rho_{E,p}$ is the p-adic cyclotomic character ϵ_p of F.

Proof. This comes from the Weil pairing. See, for example [32, Page 21]. □

2.1.1.3 Modular Forms

There are many good sources for modular forms, including [10] and [29]. Let f denote a newform of level N, weight $k \geq 2$, and character χ, i.e. f is a Hecke eigenform in $S_k(\Gamma_0(N), \chi)^{\mathrm{new}}$. Write

$$f = \sum_{n \geq 1} a_n(f) q^n$$

for the Fourier expansion of F, and note that $a_1(f) = 1$ since f is normalized by assumption. Let $K = \mathbb{Q}(\{a_n(f)\}_{n \geq 1})$ be the field gotten by adjoining the Fourier coefficients of f to $\mathbb{Q}$. A well known result is that K is, in fact, a number field. The following result due to Shimura for $k = 2$ and Deligne for $k \geq 2$:

Theorem 2.1.4. ([8]) Let $\mathfrak{p}$ be a prime of K lying above p. Then there exists a continuous representation

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{\mathfrak{p}})$$

such that:

(1) $\rho_{f,\mathfrak{p}}$ is unramified outside Np,

(2) The trace and determinant of $\rho_{f,\mathfrak{p}}(\mathrm{Frob}_l)$ for $l \nmid Np$ are $a_l(f)$ and $l^{k-1}\chi(l)$, respectively.

In fact, this representation $\rho_{f,\mathfrak{p}}$ is equivalent to a representation taking values in $\mathcal{O}_{K_{\mathfrak{p}}}$, the integer ring of the completion. Letting k denote the residue field, composing $\rho_{f,\mathfrak{p}}$ with the natural projection $\mathrm{GL}_2(\mathcal{O}_{K_{\mathfrak{p}}}) \to \mathrm{GL}_2(k)$ gives a representation

$$\bar{\rho}_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k).$$

It is actually better to consider the semi-simplification of this representation, and so it will simply be assumed that $\bar{\rho}_{f,\mathfrak{p}}$ refers to the semi-simplification.

Definition 2.1.5. (1) Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(L)$ be a representation, where $L/\mathbb{Q}_p$ is a finite extension. Then ρ is called *modular* if it is isomorphic over $\overline{\mathbb{Q}}_p$ to some $\rho_{f,\mathfrak{p}}$.

(2) If $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ is a continuous semi-simple representation with k a finite field of characteristic p, then $\bar{\rho}$ is *modular* if it is isomorphic over $\overline{\mathbb{F}}_p$ to some $\bar{\rho}_{f,\mathfrak{p}}$.

It is now known that all elliptic curves over $\mathbb{Q}$ are modular, which is to say that if $E/\mathbb{Q}$ is an elliptic curve, then some (equivalently all) $\rho_{E,p}$ is modular. This is a result due to many, and appropriate sources will be provided in the next chapter.

2.1.1.4 Adjoint Representations

Let F be a either a number field or a finite extension of $\mathbb{Q}_p$ for some prime p, and let $\rho : G_F \to \mathrm{GL}_n(K)$ be a representation, with K some field. The adjoint representation $\mathrm{ad}\,\rho$

is defined as follows. As a set, the module $\operatorname{ad}\rho$ is just the set of $n \times n$ matrices over K. It becomes a G_F-module via the action:

$$g \cdot A = \rho(g) A \rho(g)^{-1}.$$

Namely, G_F acts through conjugating by ρ. The set of trace zero matrices are invariant under the action, and hence is a G_F-submodule, denoted by $\operatorname{ad}^0 \rho \subset \operatorname{ad}\rho$. These two G_F-modules will be essential later on.

2.1.1.5 Tate Twists

Let F be any field of characteristic zero. Consider $T_p(\overline{F}^\times)$, the p-adic Tate module of $\overline{F}^\times$. From Section 2.1.1.1, there is an isomorphism $T_p(\overline{F}^\times) \cong \mathbb{Z}_p$, and that G_F acts on $T_p(\overline{F}^\times)$ via the p-adic cyclotomic character $\epsilon_p : G_F \to \mathbb{Z}_p^\times$. Write $\mathbb{Z}_p(1) = T_p(\overline{F}^\times)$, called the Tate twist of $\mathbb{Z}_p$. We also let $\mathbb{Q}_p(1) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$.

More generally, for $r \in \mathbb{Z}$, let

$$\mathbb{Z}_p(r) := \operatorname{Sym}^r_{\mathbb{Z}_p} \mathbb{Z}_p(1), \quad \mathbb{Z}_p(-r) := \operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(r), \mathbb{Z}_p).$$

As a set $\mathbb{Z}_p(r) = \mathbb{Z}_p(-r) = \mathbb{Z}_p$, but the action of G_F on $\mathbb{Z}_p(r)$ is

$$g \cdot m = \epsilon_p(g)^r m.$$

There are corresponding modules

$$\mathbb{Q}_p(r) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(r).$$

In fact, for any $\mathbb{Z}_p$-module T on which G_F acts, we can form the G_F-module

$$T(r) := T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(r).$$

2.1.2 Local Representations: $l \neq p$

Ultimately, the goal will be to study representations of G_F, where F is a number field. However, it is desirable to impose local behavior of these representations. Namely, if ρ is the representation in question, then we will be imposing conditions on the restrictions $\rho|_{G_{F_v}}$, where v is a finite place of F. Such representations can be studied independently of the global representation ρ, and there are many interesting properties. Both this section and the next section will examine these local representations.

For this section, let $K/\mathbb{Q}_p$ be a finite extension, and consider $G_K = \mathrm{Gal}(\overline{K}/K)$. The representations of interest are of the form

$$\rho : G_K \to \mathrm{GL}_n(L),$$

where $L/\mathbb{Q}_l$ is an algebraic extension with integer ring $\mathcal{O}_L$. Equivalently, one can examine finite dimensional L-vector spaces V with a continuous and linear action of G_K, which gives a map

$$\rho : G_K \to \mathrm{Aut}(V) \cong \mathrm{GL}_n(L),$$

the isomorphism coming after a basis for V is chosen. As it turns out, the cases $l \neq p$ (the l-adic case) and $l = p$ (the p-adic case) behave very differently, and so each is treated individually, the former being treated in this section and the latter in the next section. The main source for this section is [13], although [16] and [36] are good references.

Assume $l \neq p$.

Definition 2.1.6. An *l-adic representation* of G_K is a finite dimensional L vector space V, together with a continuous, linear action of G_K.

Remark 2.1.7. Every l-adic representation V of G_K has a G_K-stable lattice T, meaning the representation V has a free $\mathcal{O}_L$-module T of rank $\dim_L V$ which is stable under the action of G_K (here $\mathcal{O}_L$ is the integer ring of L). In matrix terms, this means that the representation

$$\rho : G_K \to \mathrm{Aut}(V) \cong \mathrm{GL}_n(L)$$

is conjugate to a representation $\rho' : G_K \to \mathrm{GL}_n(\mathcal{O}_L)$. Conversely, if T is a free $\mathcal{O}_L$-module of rank d with a continuous, linear action of G_K, then one can form an associated l-adic representation of dimension d over $\mathbb{Q}_l$ by considering

$$V = L \otimes_{\mathcal{O}_L} T.$$

Example 2.1.8. (1) Take $L = \mathbb{Q}_l$ and $T = \mathbb{Z}_l$. Then G_K acts on T via the cyclotomic character $\epsilon_l : G_K \to \mathbb{Z}_l^\times$ (section 2.1.1.1). By the above remark, this gives rise to a one-dimensional l-adic representation of G_K.

(2) Again let $L = \mathbb{Q}_l$. If E is an elliptic curve over K, then G_K acts on the l-adic Tate module $T_l(E)$ of E (section 2.1.1.2). This produces a two-dimensional l-adic representation of G_K.

There is useful terminology when discussing l-adic representations.

Definition 2.1.9. ([13, Definition 1.22]) Let V be an l-adic representation of G_K.

(1) The representation V is *unramified (or has good reduction)* if the inertia group I_K acts trivially on V.

(2) The representation V is *semi-stable* if the inertia group I_K acts unipotently (equivalently, if the semi-simplification of V has good reduction).

Remark 2.1.10. For any property X, the representation V is said to be potentially X if there is a finite extension K'/K such that the restricted representation $V|_{G_{K'}}$ has characteristic X. For example, V is potentially semi-stable if there is a finite extension K'/K such that $V|_{G_{K'}}$ is semi-stable.

While l-adic representations are the objects of interest, it turns out that the category of l-adic representations is equivalent to the category of a different sort of representation. We describe this other category, called Weil-Deligne representations.

Let $\mathcal{O}_K \subset K$ be the integer ring, $\mathfrak{m}_K \subset \mathcal{O}_K$ the maximal ideal, and $k = \mathcal{O}_K/\mathfrak{m}_K$ the residue field. We will let $\mathrm{Frob}_k \in G_k$ denote the geometric Frobenius element. There is a short exact sequence

$$1 \to I_K \to G_K \xrightarrow{\pi} G_k \to 1.$$

Definition 2.1.11. The Weil group W_K of K is defined to be

$$W_K = \{g \in G_K : \pi(g) = \mathrm{Frob}_k^n \text{ for some } n \in \mathbb{Z}\}.$$

Clearly $I_K \subset W_K$, and the topology on W_K is determined by declaring that I_K be an open subgroup with its usual topology. Let $\alpha : W_K \to \mathbb{Z}$ be the map $g \mapsto n$, where $\pi(g) = \mathrm{Frob}_k^n$. We can now define representations on W_K.

Definition 2.1.12 ([16, Definition 2.9], [13, p.16])**.** Let E be any field of characteristic zero.

(1) A representation of W_K over E is a representation over a finite dimensional E vector space V which is continuous when E is given the discrete topology. In other words, it is a homomorphism

$$\rho : W_K \to \mathrm{Aut}(V)$$

such that $\ker \rho \cap I_K \subset I_K$ is open.

(2) A *Weil-Deligne representation* of W_K over E is a pair (r, N), where $r : W_K \to \mathrm{Aut}(V)$ is a representation of W_K over E and $N \in \mathrm{End}(V)$ is an endomorphism such that, for $\sigma \in W_K$, we have

$$r(\sigma)Nr(\sigma)^{-1} = q^{-\alpha(\sigma)}N,$$

where $q = \#k$.

Remark 2.1.13. (1) The endomorphism N is necessarily nilpotent.

(2) There is an object called the Weil-Deligne group whose representations are the Weil-Deligne representations of W_K defined above, hence the name.

(3) If (r, N) is a Weil-Deligne representation, then the pair (r^{ss}, N), where r^{ss} denotes the semi-simplification of r, is also a Weil-Deligne representation, called the Frobenius semi-simplification of (r, N) (which from now on will be written as $(r, N)^{\mathrm{ss}}$ or $(r, N)^{\text{F-ss}}$). If r is semi-simple, then (r, N) is called Frobenius semisimple.

One of the advantages of Weil-Deligne representations is that there is no need to worry about topological issues since the field E is given the discrete topology. This will prove to be useful later on.

There are two more definitions needed before introducing the main theorem of the section.

Definition 2.1.14. (1) If $L/\mathbb{Q}_l$ is algebraic, then $A \in \mathrm{GL}_n(L)$ is called *bounded* if $\det(A) \in \mathcal{O}_L^\times$ and the characteristic polynomial of A is in $\mathcal{O}_L[X]$.

(2) A Weil-Deligne representation (r, N) of W_K over L is *bounded* if $r(\sigma)$ is bounded for all $\sigma \in W_K$.

The upshot of all these definitions is the following theorem of Grothendieck.

Theorem 2.1.15 ([16, Proposition 2.14])**.** Suppose $l \neq p$ (which has been the running assumption). There is an equivalence of categories from the category of continuous representations of G_K over L to the category of bounded Weil-Deligne representations over L.

As remarked earlier, this means that studying l-adic representations of G_K is equivalent to studying this new class of representations for which topology is not as big of an issue.

2.1.3 Local Representations: $l = p$

As in the previous section, let $K/\mathbb{Q}_p$ be a finite extension, except now let $l = p$, which is the so called p-adic representation setting. Namely, we will examine representations

$$\rho : G_K \to \mathrm{GL}_n(L),$$

where $L/\mathbb{Q}_p$ is an algebraic extension. These representations are much more difficult to study than the $l \neq p$ case, simply because there are many more representations to consider. In the $l \neq p$ case, representations of G_K had to be trivial on some open subgroup of the wild inertia group, but this is not the case in the $l = p$ setting.

The study of p-adic representations has been carried out in detail by Fontaine and others. The two types of representations which we will need most are Hodge-Tate and de Rham representations. To study these in detail would require the study of Fontaine's period rings ([11, 12]). We will briefly describe the idea of the period rings, omitting proofs, and then examine Hodge-Tate, de Rham, and crystalline representations (the latter two in minimal detail).

2.1.3.1 Fontaine's Period Rings

In this section, we follow [13, Chapters 2,5] and [3]. Let B be a topological ring with fraction field $C = \mathrm{Frac}(B)$, and G a topological group which acts continuously on B. Assume that the subring $B^G \subset B$ is a field, and let $F \subset B^G$ be a subfield. If B is a domain, then the action of G can be extended to C in the natural way. Further assume:

Definition 2.1.16 ([13, Definition 2.8]). An (F, G)*-regular ring* B is a topological ring such that:

(1) B is a domain.

(2) $B^G = C^G$

(3) If $0 \neq b \in B$ such that $F \cdot b$ is stable under under the action of G, then $b \in B^\times$.

Remark 2.1.17. Eventually, the rings of periods will be $(\mathbb{Q}_p, G_K)$-regular rings, so for the purposes of the dissertation, the reader may think $F = \mathbb{Q}_p$ and $G = G_K$.

We will want to consider F-representations of G (i.e. representations of G over F) and somehow transform them into B-representations of G.

Definition 2.1.18 ([13, Definitions 2.2, 2.3, 2.5]). (1) A B*-representation of* G is a B-module V of finite type equipped with a semi-linear and continuous action of G, i.e.

$$g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2, \quad g(bv) = g(b)g(v)$$

for $v_1, v_2, v \in V$, $b \in B$, and $g \in G$.

(2) If the module V is free over B, then V is called a *free* B*-representation* of G.

(3) The B-representation V is called *trivial* if there is a basis for V consisting of elements of V^G.

Let V be a F-representation of G. Notice that under the definition above, this is just a usual linear representation of G over F since G acts trivially on $F \subset B^G$. Consider the module $B \otimes_F V$, which is a free B-module of rank $\dim_F(V)$. The G-action on the tensor product is $g(b \otimes v) = g(b) \otimes g(v)$.

Definition 2.1.19. Let V be a F-representation of G. Then V is B*-admissible* if $B \otimes_F V$ is a trivial B-representation of G.

There is an equivalent formulation of B-admissible representations. Consider

$$D_B(V) := (B \otimes_F V)^G.$$

This is a B^G-vector space on which G acts trivially. There is a natural map

$$\alpha : B \otimes_{B^G} D_B(V) \to B \otimes_F V$$

given by $b \otimes x \mapsto bx$. This map is B-linear and commutes with the action of G.

Theorem 2.1.20 ([13, Theorem 2.13])**.** If B is a period ring, then the map α is injective and $\dim_{B^G}(D_B(V)) \leq \dim_F(V)$. Moreover, α is an isomorphism if and only if equality holds and if and only if V is B-admissible.

The specific classes of p-adic representations of interest are B-admissible representations for various choices of B.

2.1.3.2 Hodge-Tate Representations

Now let $K/\mathbb{Q}_p$ be a finite extension, $L/\mathbb{Q}_p$ be an algebraic extension, and V a p-adic representation of G_K of dimension n (i.e. an n-dimensional L-vector space on which G_K acts). Let $\mathbb{C}_p = \widehat{\overline{K}}$, the p-adic completion of the algebraic closure of K. The action of G_K on $\overline{K}$ extends, by continuity, to an action of G_K on $\mathbb{C}_p$. The Hodge-Tate period ring will be:

Definition 2.1.21. The Hodge-Tate ring B_{HT} is

$$B_{\mathrm{HT}} = \bigoplus_{i \in \mathbb{Z}} \mathbb{C}_p(i),$$

where $\mathbb{C}_p(i)$ is the i-th Tate twist of $\mathbb{C}_p$ (see section 2.1.1.5).

Proposition 2.1.22 ([13, Proposition 5.2])**.** The ring B_{HT} is $(\mathbb{Q}_p, G_K)$-regular, and $B_{\mathrm{HT}}^{G_K} = K$.

Definition 2.1.23. The p-adic representation V is Hodge-Tate if it is B_{HT}-admissible (where we regard V as a $\mathbb{Q}_p$-representation of G_K instead of one over L).

Write $D_{\mathrm{HT}}(V) = D_{B_{\mathrm{HT}}}(V)$. By Theorem 2.1.20, we have the following:

Proposition 2.1.24. The natural map

$$\alpha_{\mathrm{HT}} : B_{\mathrm{HT}} \otimes_K D_{\mathrm{HT}}(V) \to B \otimes_{\mathbb{Q}_p} V$$

is an injection, and $\dim_K D_{\mathrm{HT}}(V) \leq \dim_{\mathbb{Q}_p}(V)$, with equality if and only if α_{HT} is an isomorphism, and if and only if V is Hodge-Tate.

Hodge-Tate representations acquire additional structure from grading of B_{HT}. If V is a p-adic representation of G_K over L, then $D_{\mathrm{HT}}(V)$ is a graded ring. Indeed,

$$D_{\mathrm{HT}}(V) = \left(\bigoplus_{i \in \mathbb{Z}} \mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V \right)^{G_K} = \bigoplus_{i \in \mathbb{Z}} (\mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Definition 2.1.25. Let $h_i = \dim_K(\mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V)^{G_K}$. The i's for which $h_i \neq 0$ are called the Hodge-Tate weights of V, and the multiplicity of the weight i is h_i. If V is Hodge-Tate, the multiset of Hodge-Tate weights will be denoted $\mathrm{HT}(V)$.

Note that if V is Hodge is Hodge-Tate, then the sum of the multiplicities of the weights should be $\dim_{\mathbb{Q}_p}(V)$.

Example 2.1.26. If $V = T_p(\overline{K}^{\times}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, then V is a Hodge-Tate representation of G_K of weight -1.

As it is, the sum of the multiplicities of the weights is $\dim_{\mathbb{Q}_p}(V)$ if V is Hodge-Tate. However, there is more to be said here. Suppose L contains the normal closure of $K/\mathbb{Q}_p$. The direct summand $(V \otimes_{\mathbb{Q}_p} \mathbb{C}_p(i))^{G_K}$, a priori a K-vector space, is actually an $(L \otimes_{\mathbb{Q}_p} K)$-module. The tensor $L \otimes_{\mathbb{Q}_p} K$ is a direct sum

$$L \otimes_{\mathbb{Q}_p} K = \bigoplus_{\iota : K \hookrightarrow L} L,$$

and so $D_{\mathrm{HT}}(V)$ becomes the direct sum of vector spaces over L, each n-dimensional and graded. In this case, attached to each embedding $\iota : K \hookrightarrow L$ is a multiset $\mathrm{HT}_\iota(V)$ of Hodge-Tate weights. Written another way, for an embedding $\iota : K \hookrightarrow L$, an integer i is a Hodge-Tate weight of V with respect to ι if

$$\dim_L(V \otimes_{K,\iota} \mathbb{C}_p(i))^{G_K} \neq 0.$$

2.1.3.3 de Rham Representations

A p-adic representation V of G_K is de Rham if it is B_{dR}-admissible, where B_{dR} denotes the appropriate ring of periods. See [3] or [13] for details. Since it will not be strictly necessary for this dissertation, the definition of B_{dR} will not be included. Instead, the relevant facts about de Rham representations will be presented without proof.

Theorem 2.1.27. Let $K/\mathbb{Q}_p$ be a finite extension, $L/\mathbb{Q}_p$ an algebraic extension and V a finite dimensional L-vector space with a continuous action of G_K. Then:

(1) ([3, Theorem 14.2]) The representation V is de Rham if and only if V is potentially semistable.

(2) ([3]) If V is potentially de Rham, then V is de Rham.

(3) ([13, Theorem 5.30]) If V is de Rham, then V is Hodge-Tate.

(4) ([13, Theorem 5.32]) If X/K is a proper, smooth variety over K, then the étale cohomology groups $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ are de Rham representations of G_K.

(5) ([3]) If V is de Rham, then there is an associated Weil-Deligne representation $\mathrm{WD}(V)$ of W_K.

Remark 2.1.28. (1) Statement (4) of the theorem says that de Rham representations capture those p-adic representations which come from geometry.

(2) There are examples of representations which are Hodge-Tate but not de Rham, but because of statement (4) they cannot come from geometry.

2.1.3.4 Crystalline Representations

The last type of representation needed is a crystalline representation. A p-adic representation V of G_K is crystalline if it is B_{cris}-admissible, where B_{cris} denotes another ring of periods (see [13]). As with de Rham representations, no details will be given. In fact, this section is only included because the term will be used occasionally in the next chapter. The useful facts about crystalline representations are:

Proposition 2.1.29. (1) If the representation V is crystalline, then V is de Rham.

(2) ([16]) If $\mathrm{WD}(V) = (r, N)$ denotes the corresponding Weil-Deligne representation (see (5) of Theorem 2.1.27), then V is crystalline if and only if r is unramified and $N = 0$.

2.1.4 Compatible System of Representations

In the examples of Galois representations given in the beginning of the chapter, the geometric objects (e.g. elliptic curves) produced not just one Galois representation, but a whole collection of them, one for each prime in an appropriate number field. Such representations are interesting individually, but are often more useful together. This leads into the notion of compatible systems of representations, which will be a central object in Chapter 5. Essentially, compatible systems of representations are collections of representations which share useful properties, some away from p and some at p.

Definition 2.1.30. ([16]) Let F and K be number fields, n be a positive integer, and $\mathcal{P}$ be the set of finite places of K. Let S denote a finite set of places of F. A weakly compatible system of l-adic representations is a family of continuous semisimple representations

$$\rho_\lambda : G_F \to \mathrm{GL}_n(\overline{K}_\lambda)$$

for $\lambda \in \mathcal{P}$, such that:

- If $v \notin S$ is a finite place of F, for all λ not dividing the characteristic of the residue field of v, the representation ρ_λ is unramified at v and the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_v)$ is in $K[X]$ and is independent of λ.

- Each representation ρ_λ is de Rham at the places of F above the residue characteristic of λ.

- For each embedding $\iota : F \hookrightarrow \overline{K}$, the ι-Hodge-Tate numbers are independent of λ.

Example 2.1.31. (1) If F is a number field, then the cyclotomic characters $\epsilon_l : G_F \to \mathbb{Z}_l^\times$ form a compatible system of representations with $S = \emptyset$.

(2) If E is an elliptic curve over a number field F, then the representations $\rho_{E,p}$ form a compatible system of representations, where S can be taken to be the set of places where E has bad reduction.

There is also the notion of a strictly compatible system of representations, but as these are not needed, they will not be defined here.

2.2 Galois Cohomology

The results of this dissertation rely heavily on Galois cohomology groups, so they will be introduced fairly thoroughly here. Often times, the results stated are not in the greatest generality, and this is done intentionally. Some sources for this material are [31], [27, Chapter 1], and [42].

2.2.1 Definition of Cohomology Groups

Let G be a group (could be either finite or profinite). The cases to keep in mind are $G = G_{F,S}$ for some number field F and finite set of places S of F, or $G = G_K$ for some finite extension $K/\mathbb{Q}_p$. Let A be a G-module, namely some abelian group on which G acts. For example, if $G = G_F$ for a number field F, then an example of A would be $A = \overline{F}^\times$. Of course, this does not require F to be a number field, but this is usually the situation we will be in. If G and A have topologies (for example, if G is profinite and A is given the discrete topology), then we will require that the action of G on A be continuous, and that all the maps we consider in this section be continuous.

We will follow [27] for most of this section. Let $C^0(G,A) = A$ and $C^i(G,A)$ be the set of (continuous) maps $\phi : G^i \to A$ for $i \geq 1$. These C^i are naturally abelian groups (from the structure on A). There are homomorphisms $\delta^{i+1} : C^i(G,A) \to C^{i+1}(G,A)$ defined as follows: $\delta^1(a)(g) = ga - a$, and for $i \geq 2$,

$$\delta^i(\phi)(g_1,\ldots,g_i) = g_1\phi(g_2,\ldots,g_i) + \sum_{j=1}^{q-1}(-1)^i\phi(g_1,\ldots,g_jg_{j+1},\ldots,g_i) + (-1)^i\phi(g_1,\ldots,g_{i-1}).$$

A standard exercise shows $\delta^{i+1}\circ\delta^i = 0$, which means there is a cochain complex:

$$C^0(G,A) \xrightarrow{\delta^1} C^1(G,A) \xrightarrow{\delta^2} C^3(G,A) \xrightarrow{\delta^3} C^4(G,A) \to \cdots.$$

Definition 2.2.1. The group of *i-cocycles* is $Z^i(G,A) = \ker\delta^{i+1}$. The group of *$i$-coboundaries* is $B^i(G,A) = \operatorname{im}\delta^i$.

The condition $\delta^{i+1}\circ\delta^i = 0$ shows $B^i(G,A) \subseteq Z^i(G,A)$, and so we can consider the quotient.

Definition 2.2.2. For $i \geq 1$, the *i-th cohomology group*, denoted $H^i(G,A)$, is defined to be

$$H^i(G,A) = Z^i(G,A)/B^i(G,A).$$

The zeroth cohomology group is defined to be the group $H^0(G,A) = Z^0(G,A)$.

In fact, the only cohomology groups which will be needed are $H^i(G,A)$ for $i = 0,1,2$, so we examine these groups more concretely.

2.2.2 The groups $H^i(G,A)$ for $i = 0,1,2$

2.2.2.1 Zeroth Cohomology Group

The cohomology group $H^0(G,A)$ is the easiest to describe, since $H^0(G,A) = Z^0(G,A)$. By definition,

$$H^0(G,A) = Z^0(G,A) = \ker\delta^1 = \{a \in A : ga = a \quad \forall g \in G\} = A^G,$$

the fixed points of A under the action of G.

Example 2.2.3. Taking $G = G_F$ for a field F and $A = \overline{F}^\times$, we have

$$H^0(G_F, \overline{F}^\times) = F^\times.$$

2.2.2.2 First Cohomology Group

The group $H^1(G, A)$ is a bit more complex. If $f : G \to A$ be a (continuous) map, then f is a 1-cocycle if $f(g_1 g_2) = f(g_1) + g_1 \cdot f(g_2)$ for all $g_1, g_2 \in G$. The map f is a 1-coboundary if there exists $a \in A$ such that $f(g) = ga - a$ for all $g \in G$. The first cohomology group is $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

A special case to consider is the one where G acts trivially on A. In this case, $Z^1(G, A)$ just becomes the set of continuous homomorphisms $f : G \to A$, and a 1-coboundary is automatically the zero map, i.e. $B^1(G, A) = 0$. Thus, in this setting,

$$H^1(G, A) = \mathrm{Hom}_{\mathrm{cts}}(G, A).$$

Another case to consider is the one where G is infinite cyclic or a profinite completion of an infinite cyclic group, and A is finite. Let g be a topological generator of G.

Lemma 2.2.4. In the situation described above,

$$H^1(G, A) \cong A/(g - 1)A.$$

Proof. See [42]. □

This lemma will be primarily used in the Galois deformation theory section.

2.2.2.3 Second Cohomology Group

Just as in the previous subsection, the group $H^2(G, A)$ will be the quotient of the 2-cocyles by the 2-coboundaries. A function $f : G \times G \to A$ is a 2-cocycle if for all $\sigma, \tau, \mu \in G$,

$$f(\sigma\tau, \mu) - f(\sigma, \tau\mu) - \sigma f(\tau, \mu) - f(\sigma, \tau) = 0.$$

The map f is a 2-coboundary if there is a map $g : G \to A$ such that

$$f(\sigma, \tau) = \sigma g(\tau) - g(\sigma\tau) + g(\sigma),$$

for all $\sigma, \tau \in G$.

The group $H^2(G, A)$ naturally appears when studying group extensions of A by G. For a description of this process, see [27].

These definitions seem mysterious at first glance, and the groups appear difficult to compute. As we will see, this is true in many cases. Instead, there are several theorems which enable us compute the sizes of these groups without digging into the definitions.

To illustrate how these groups arise, we state a theorem which shows how they are used in some classical settings.

Example 2.2.5. (1) (Hilbert's Theorem 90) If L/K is a Galois extension of fields, then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

(2) (Local Class Field Theory) [42, Proposition 1] If p is a prime, then $H^2(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}}_p^\times) \cong \mathbb{Q}/\mathbb{Z}$.

2.2.2.4 General Facts

We briefly state a few facts, directing the reader to the sources for proofs. The first is standard result in homological algebra which provides a method to move from short exact sequences of G-modules to a long exact sequences in cohomology.

Theorem 2.2.6. Suppose $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules. Then there is a long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A)$$

$$\to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots .$$

Example 2.2.7. Let K be a field, and let $n \geq 1$ be prime to the characteristic of K. Consider $\mu_n = \mu_n(\overline{K}^\times)$, the n-th roots of unity of $\overline{K}^\times$ (see Section 2.1.1.1). There is an exact sequence

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times.$$

By Theorem 2.2.6, this induces a long exact sequence in cohomology

$$\cdots \to H^0(G_K, \overline{K}^\times) \to H^0(G_K, \overline{K}^\times) \to H^1(G_K, \mu_n) \to H^1(G_K, \overline{K}^\times).$$

This first map is induced by the n-th power map on $\overline{K}^{\times}$, and by Example 2.2.5, the last group is 0. Thus,

$$H^1(G_K, \mu_n) \cong K^{\times}/(K^{\times})^n.$$

Another useful fact is the following:

Proposition 2.2.8. [19, Proposition 4.1] If both G and A are finite with coprime cardinalities, then $H^i(G, A) = 0$ for $i > 0$.

The next example highlights how the proposition will be utilized in later chapters.

Example 2.2.9. If V is a finite dimensional vector space over a finite field of characteristic p, and F is a number field, then $H^1(\mathrm{Gal}(F(\zeta_p)/F), V) = 0$, where ζ_p is a primitive p-th root of unity in $\overline{F}^{\times}$. Indeed, $[F(\zeta_p) : F]$ is coprime to p, so the statement follows from the proposition.

Remark 2.2.10. Since it showed up in the example, at this point it is useful to remark that if A is a finite dimensional vector space over a field k, then $H^i(G, A)$ also becomes an k-vector space.

The next theorem about the Galois cohomology of the Galois group of a local field will be used continuously.

Theorem 2.2.11. If $K/\mathbb{Q}_p$ is a finite extension, and A is a finite G_K-module, then $H^i(G_K, A)$ is finite as well.

Corollary 2.2.12. If A is a finite dimensional vector space over a finite field k, and $K/\mathbb{Q}_p$ is a finite extension, then $H^i(G_K, A)$ is a finite dimensional k-vector space. We often write $h^i(G_K, A) = \dim h^i(G_K, A)$.

Remark 2.2.13. If K is assumed to be a number field instead of a local field, then the theorem is no longer true.

2.2.3 Inflation-Restriction Exact Sequence

Theorem 2.2.6 in the previous section showed that an exact sequence of G-modules induces a long exact sequence in cohomology. Namely, it produced morphisms on cohomology from a sequence morphisms of the coefficients. This section is about getting maps on cohomology by considering subgroups and quotients of G as opposed to the coefficients.

Let G be as in the previous section, namely either finite or profinite. Let $H \leq G$ be a normal subgroup of G, closed if G is profinite. Let A be a G-module. In this section, the term cocycle will mean either a 1- or 2-cocycle, i.e. $i = 1$ or 2.

First, note that if A is a G-module, then A becomes an H-module by simply restricting the G-action to H. It therefore makes sense to restrict cocycles for G to cocycles for H. This gives restriction maps

$$\text{res}_H : H^i(G, A) \to H^i(H, A).$$

Now consider the quotient G/H. Any cocycle of G/H can be regarded as a cocycle of G by composing with the projection $G \to G/H$. Though A is not naturally a G/H-module, the subgroup A^H (fixed points of A under the action of H) is one. Thus, there are inflation maps

$$\inf : H^i(G/H, A^H) \to H^i(G, H).$$

Lastly, G/H acts on the cohomology group $H^1(H, A)$. The action is as follows: if g is a representative for a coset in G/H and $f : H \to A$ is a 1-cocycle, then

$$(g \cdot f)(h) = g \cdot f(g^{-1}hg).$$

A simple calculation shows that this action is well-defined as an action of G/H on the group $H^1(H, A)$.

The following proposition shows that the inflation and restriction maps produce an exact sequence, known as the inflation-restriction sequence.

Proposition 2.2.14. [42, Proposition 2] We have an exact sequence

$$0 \to H^1(G/H, A^H) \overset{\inf}{\to} H^1(G, A) \overset{\text{res}_H}{\to} H^1(H, A)^{G/H} \to H^2(G/H, A^H) \overset{\inf}{\to} H^2(G, X).$$

2.2.4 Unramified Cohomology

There is a specific application of Proposition 2.2.14 that we want to consider. Let $K/\mathbb{Q}_p$ be a finite extension, and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be its absolute Galois group. Write K^{ur} for the maximal unramified extension of K inside $\overline{K}$, and let $I_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{ur}}) \leq G_K$ be the inertia subgroup. Then $G_K/I_K \cong \mathrm{Gal}(K^{\mathrm{ur}}/K)$.

If A is a G_K-module, then consider the first cohomology group $H^1(G_K, A)$. By inflation-restriction, the map $H^1(G_K/I_K, A^{I_K}) \hookrightarrow H^1(G_K, A)$ is an injection.

Definition 2.2.15. A class $[\phi] \in H^1(G_K, A)$ is called *unramified* if $[\phi] \in H^1(G_K/I_K, A^{I_K})$.

We write $H^1_{\mathrm{ur}}(G_K, A) := H^1(G_K/I_K, A^{I_K})$ and refer to this group as the unramified cohomology. By the inflation-restriction sequence,

$$H^1_{\mathrm{ur}}(G_K, A) = \ker(H^1(G_K, A) \to H^1(I_K, A)),$$

so the unramified cohomology classes are those in $H^1(G_K, A)$ whose restriction to I_K is trivial, hence the name unramified.

The next proposition will help us compute the size of the unramified cohomology.

Proposition 2.2.16. [42, Lemma 1] Let A be a finite G_K-module. Then $\#H^1_{\mathrm{ur}}(G_K, A) = \#H^0(G_K, A) = \#A^{G_K}$. In particular, the unramified cohomology is finite.

Proof. The proof follows from the exact sequence

$$0 \to A^{G_K} \to A^{I_K} \xrightarrow{\mathrm{Frob}_K - 1} A^{I_K} \to A^{I_K}/(\mathrm{Frob} - 1)A^{I_K} \to 0$$

and Lemma 2.2.4. □

2.2.5 Local Computations

This subsection will introduce two theorems which reduce the time needed to compute the sizes of the first and second cohomology groups in the local field setting.

Again, let $K/\mathbb{Q}_p$ be a finite extension. If A is a finite G_K-module of size m, let μ_m denote the set of m-th roots of unity in $\overline{K}^{\times}$, and let $A^*(1)$ denote the G_K-module

$$A^*(1) = \mathrm{Hom}_{\mathbb{Z}}(A, \mu_m),$$

with the action of G_K being by $(\sigma \cdot f)(a) = \sigma \cdot f(\sigma^{-1}a)$. This is the Tate twist of the usual dual. For this reason, this is sometimes called the Tate dual.

Theorem 2.2.17 (Local Tate Duality)**.** For $0 \le i \le 2$, there is a perfect pairing

$$H^i(G_K, A) \times H^{2-i}(G_K, A^*(1)) \to \mathbb{Q}/\mathbb{Z}.$$

Moreover, if $i = 1$ and m is relatively prime to p, the unramified cohomology groups $H^1_{\mathrm{ur}}(G_K, A)$ and $H^1_{\mathrm{ur}}(G_K, A^*(1))$ are mutual annihilators under the pairing.

Remark 2.2.18.

(1) The pairing itself is induced by the cup product. However, the cup product is never mentioned in the dissertation so it will not be defined here.

(2) When $i = 2$, the theorem implies $\#H^2(G_K, A) = \#H^0(G_K, A^*(1))$. The latter is much easier to compute, as it just counts fixed points under the G_K-action.

The next theorem will assist in calculating the size of H^1.

Theorem 2.2.19 (Local Euler Characteristic Formula)**.** [19, Theorem 4.52] Let A be a finite G_K-module of size m. Then

$$\frac{\#H^0(G_K, A) \cdot \#H^2(G_K, A)}{\#H^1(G_K, A)} = p^{-v_p(m)[K:\mathbb{Q}_p]}.$$

Remark 2.2.20. If m is coprime to p, then the right hand side is just 1.

Since we can compute $\#H^2(G_K, A)$ as $\#H^0(G_K, A^*(1))$, Theorem 2.2.19 gives us a way of computing $\#H^1(G_K, A)$ in terms of two H^0 terms.

2.2.6 Global Computations

Theorem 2.2.11 guaranteed the finiteness of the cohomology groups in the case of local fields and finite modules. The remark following the theorem mentioned how this was not true with global fields. However, if it is guaranteed that only finitely many primes ramify, then the theorem will hold. This section will introduce an analogues for formulas such as 2.2.19 in the global setting.

The two main results of this section are the Poitou-Tate exact sequence and the global Euler characteristic formula. Let F be a number field, let S be a finite set of primes of F, and consider the group $G_{F,S}$ as in Section 2.1.1. Recall that there are embeddings $G_{F_v} \hookrightarrow G_F$ for places v of F. If $v \in S$, then the map $G_{F_v} \to G_{F,S}$ is still an embedding. If $v \notin S$, then the composite $G_{F_v} \to G_{F,S}$ factors through G_{F_v}/I_{F_v}.

Let M be a finite $G_{F,S}$-module. If $v \in S$, then we can restrict a class in $H^i(G_{F,S}, M)$ to G_{F_v} to get a class in $H^i(G_{F_v}, M)$. Considering all $v \in S$ together produces a map

$$H^i(G_{F,S}, M) \to \prod_{v \in S} H^i(G_{F_v}, M).$$

The Poitou-Tate exact sequence describes the kernel and cokernel of the maps for $i = 0, 1, 2$ by fitting them into an exact sequence.

Theorem 2.2.21 (Poitou-Tate Exact Sequence)**.** [19, Theorem 4.50] Let S be a finite set of primes of F containing all the infinite places. Let M be a finite $G_{F,S}$-module with $v(\#M) = 0$ for all $v \notin S$ (equivalently, S contains the places above the primes dividing $\#M$). Then there is an exact sequence

$$\begin{aligned} 0 \to H^0(G_{F,S}, M) \to \prod_{v \in S} H^0(G_{F_v}, M) \to H^2(G_{F,S}, M^*(1))^* \\ \to H^1(G_{F,S}, M) \to \prod_{v \in S} H^1(G_{F_v}, M) \to H^1(G_{F,S}, M^*(1)) \\ \to H^2(G_{F,S}, M) \to \prod_{v \in S} H^2(G_{F_v}, M) \to H^0(G_{F,S}, M^*(1))^* \to 0. \end{aligned}$$

It is a fact that in the setting of Theorem 2.2.21, the groups $H^i(G_{F,S}, M)$ are finite. The second big theorem of the section is an analogue of Theorem 2.2.19.

Theorem 2.2.22 (Global Euler-Poincaré Characteristic Formula)**.** [19, Theorem 4.53] Let S and M be as in Theorem 2.2.21. Then

$$\frac{\#H^0(G_{F,S}, M) \cdot \#H^2(G_{F,S}, M)}{\#H^1(G_{F,S}, M)} = \frac{1}{(\#M)^{[F:\mathbb{Q}]}} \prod_{v \in S_\infty} H^0(G_{F_v}, M).$$

This theorem is useful in part because in the global setting, it is often nice to know the difference in sizes between $H^1(G_{F,S}, M)$ and $H^2(G_{F,S}, M)$, which is easy to get from the theorem.

Remark 2.2.23. In the case M is a finite dimensional vector space over a finite field, both Theorems 2.2.19 and 2.2.22 can be translated to formulae involving the dimension of the H^i. This is done freely later on.

2.2.7 Selmer Groups

In the last section, there were restriction maps which paved a way to move from global to local cohomology groups. This is closely tied to the idea that we will ultimately want global Galois representations to have very specific local behavior. However, this is not always enough. For example, if F is a number field and $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ is a continuous representation, then it is sometimes useful to impose, for example, that $\rho|_{G_{F_v}}$ is crystalline at the places above p, or is unramified at places above 3. In such cases, simply restricting global cohomology classes to local ones will not be sufficient. In fact, it will be required that the restriction lies in a certain subgroup of the local cohomology, where these subgroups somehow parametrize the desired local behavior (this is the idea of the Galois deformation theory section). First, we need some machinery for dealing with such situations from the cohomology standpoint.

Continue with setting from the previous section. Namely, let F be a number field, and let S be a finite set of places including the infinite places. Let M be a finite $G_{F,S}$-module such that S contains the places above the primes dividing $\#M$. For each $v \in S$ (including the infinite places), choose a subgroup $\mathcal{L}_v \subset H^1(G_{F_v}, M)$, and let $\mathcal{L} = (\mathcal{L}_v)_{v \in S}$ denote the collection of subgroups (usually called the collection of local conditions).

Definition 2.2.24. The *Selmer group* with respect to $\mathcal{L}$ is the group

$$H^1_{\mathcal{L}}(G_{F,S}, M) = \ker \left(H^1(G_{F,S}, M) \to \prod_{v \in S} \frac{H^1(G_{F_v}, M)}{\mathcal{L}_v} \right).$$

Thus, the Selmer group is the set of classes in $H^1(G_{F,S}, M)$ whose restrictions to each G_{F_v} lies in the desired subgroup $\mathcal{L}_v$.

Recall from Theorem 2.2.17 that there is a perfect pairing

$$H^1(G_{F_v}, M) \times H^1(G_{F_v}, M^*(1)) \to \mathbb{Q}/\mathbb{Z}.$$

For each $v \in S$, we will let $\mathcal{L}_v^\perp \subseteq H^1(G_{F_v}, M^*(1))$ denote the annihilator of $\mathcal{L}_v$ under this pairing, and $\mathcal{L}^\perp = (\mathcal{L}_v^\perp)_{v\in S}$.

Definition 2.2.25. The *dual Selmer group* with respect to $\mathcal{L}^\perp$ is

$$H^1_{\mathcal{L}^\perp}(G_{F,S}, M^*(1)) = \ker\left(H^1(G_{F,S}, M^*(1)) \to \prod_{v\in S} \frac{H^1(G_{F_v}, M^*(1))}{\mathcal{L}_v^\perp}\right).$$

The dual Selmer group will be one of the most important objects of this dissertation, in particular because it is usually necessary to have $H^1_{\mathcal{L}^\perp}(G_{F,S}, M^*(1)) = 0$ (for a specific M). In fact, the goal will, most of the time, be to add primes to S so that this happens.

Both the Selmer and dual Selmer groups are finite groups, and there is a formula which relates the sizes of the two groups.

Theorem 2.2.26 (Greenberg-Wiles)**.** [42, Theorem 2] In the setting described above,

$$\frac{\#H^1_{\mathcal{L}}(G_{F,S}, M)}{\#H^1_{\mathcal{L}^\perp}(G_{F,S}, M^*(1))} = \frac{\#H^0(G_{F,S}, M)}{\#H^0(G_{F,S}, M^*(1))} \prod_{v\in S} \frac{\#\mathcal{L}_v}{\#H^0(G_{F_v}, M)}.$$

This is a powerful theorem, and [42] gives a nice illustration of how it can be applied to prove the Kronecker-Weber theorem.

2.3 Galois Deformation Theory: Two Dimensional Setting

2.3.1 Definitions and Universal Rings

Let p be an odd prime number. Let $K/\mathbb{Q}_p$ be a finite extension, $\mathcal{O} \subset K$ the integer ring with maximal ideal $\mathfrak{m}$, and residue field $k = \mathcal{O}/\mathfrak{m}$. Let G be either:

- $G_{F,S}$ for some number field F and finite set of places S of F, or

- G_K, where K is a finite extension of $\mathbb{Q}_l$ for l prime (both $l \neq p$ and $l = p$ are allowed).

Denote by $\mathrm{CNL}_{\mathcal{O}}$ the category of complete Noetherian local $\mathcal{O}$-algebras with residue field k. If $A \in \mathrm{CNL}_{\mathcal{O}}$, then $\mathfrak{m}_A$ will denote its maximal ideal. Let $\bar{\rho} : G \to \mathrm{GL}_2(k)$ be a continuous representation.

Definition 2.3.1. Let $A \in \mathrm{CNL}_{\mathcal{O}}$.

(1) A *lift* ρ of $\bar{\rho}$ to A is a continuous representation $\rho : G \to \mathrm{GL}_2(A)$ such that $\rho \bmod \mathfrak{m}_A = \bar{\rho}$, i.e. the following diagram commutes:

$$\begin{array}{ccc} & & \mathrm{GL}_2(A) \\ & \overset{\rho}{\nearrow} & \downarrow \\ G & \xrightarrow[\bar{\rho}]{} & \mathrm{GL}_2(k) \end{array}$$

(2) A *deformation* of $\bar{\rho}$ to A is an equivalence class of lifts, where two lifts ρ and ρ' to A are equivalent if there exists a matrix $M \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(k))$ such that $\rho' = M\rho M^{-1}$.

Out of this definition comes two functors:

- $\mathcal{D}^{\square}_{\bar{\rho}} : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Sets}$ will be the functor which sends A to the set of lifts of $\bar{\rho}$ to A.
- $\mathcal{D}_{\bar{\rho}} : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Sets}$ will be the functor which sends A to the set of deformations of $\bar{\rho}$ to A.

Theorem 2.3.2. (1) The functor $\mathcal{D}^{\square}_{\bar{\rho}}$ is representable with representing object $R^{\square}_{\bar{\rho}} \in \mathrm{CNL}_{\mathcal{O}}$.

(2) If $\mathrm{End}_{k[G]}(\bar{\rho}) = k$, then $\mathcal{D}_{\bar{\rho}}$ is representable by $R^{\mathrm{univ}}_{\bar{\rho}} \in \mathrm{CNL}_{\mathcal{O}}$.

Proof. See [4], Proposition 1.3.1. □

Remark 2.3.3. (1) The object $R^{\square}_{\bar{\rho}}$ is called the universal lifting ring, and $R^{\mathrm{univ}}_{\bar{\rho}}$ is called the universal deformation ring, when it exists.

(2) If $\bar{\rho}$ satisfies the condition $\mathrm{End}_{k[G]}(\bar{\rho}) = k$, then $\bar{\rho}$ is said to be Schur.

(3) One very useful example to keep in mind is the case when $K = \mathbb{Q}_p$ and $\bar{\rho}$ is the representation $\bar{\rho} = \bar{\rho}_{E,p}$ for some elliptic curve over a number field F. Then the representation $\rho_{E,p}$ is a lift of $\bar{\rho}_{E,p}$ to the ring $\mathbb{Z}_p$.

2.3.2 Tangent Spaces

Definition 2.3.4. The *Zariski tangent space* of $\mathcal{D}_{\bar{\rho}}^{\square}$ is defined to be the k-vector space $\mathcal{D}_{\bar{\rho}}^{\square}(k[\epsilon]/(\epsilon^2))$. Similarly, the Zariski tangent space of $\mathcal{D}_{\bar{\rho}}$ is $\mathcal{D}_{\bar{\rho}}(k[\epsilon]/(\epsilon^2))$.

Perhaps it is not immediately clear why these tangent spaces are k-vector spaces at all. One way to see this is from the following lemma.

Lemma 2.3.5. Let $\mathcal{D}$ be either the functor $\mathcal{D}_{\bar{\rho}}$ or $\mathcal{D}_{\bar{\rho}}^{\square}$, and let R be the corresponding universal object (assuming it exists in the former case). Then there is a natural bijection between $\mathcal{D}(k[\epsilon]/(\epsilon^2))$ and $\mathrm{Hom}_k(\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}), k)$.

Proof. See [26], page 271. □

There is a nice cohomological interpretation of the Zariski tangent spaces. Before stating the lemma, recall the definition of the adjoint representation from Section 2.1.1.4.

Lemma 2.3.6. (1) There is a natural isomorphism of k-vector spaces $\mathcal{D}_{\bar{\rho}}^{\square}(k[\epsilon]/(\epsilon^2)) \to Z^1(G, \mathrm{ad}\,\bar{\rho})$.

(2) There is also a natural isomorphism of k-vector spaces $\mathcal{D}_{\bar{\rho}}(k[\epsilon]/(\epsilon^2)) \to H^1(G, \mathrm{ad}\,\bar{\rho})$.

Proof. The inverse map for both (1) and (2) sends a cocycle ϕ to the representation $\rho : G \to \mathrm{GL}_2(k[\epsilon]/(\epsilon^2))$ given by $\rho(g) = (1+\phi(g)\epsilon)\bar{\rho}(g)$. In the latter case, this is a map of equivalence classes. The details are left to the reader, and good references for alternate proofs are [4] and [26]. □

Corollary 2.3.7. (1) The tangent space for $\mathcal{D}_{\bar{\rho}}$ is finite dimensional over k.

(2) We have $\dim_k \mathcal{D}_{\bar{\rho}}^{\square}(k[\epsilon]/(\epsilon^2)) = \dim_k H^1(G, \mathrm{ad}\,\bar{\rho}) + 4 - \dim_k H^0(G, \mathrm{ad}\,\bar{\rho})$, so the tangent space for $\mathcal{D}_{\bar{\rho}}^{\square}$ is finite dimensional as well.

Proof. Part (1) follows from the lemma and the fact that $H^1(G, \operatorname{ad} \bar{\rho})$ is finite dimensional. Part (2) follows from Lemma 2.3.6 and the exact sequence

$$0 \to (\operatorname{ad} \bar{\rho})^G \to \operatorname{ad} \bar{\rho} \to Z^1(G, \operatorname{ad} \bar{\rho}) \to H^1(G, \operatorname{ad} \bar{\rho}) \to 0.$$

□

We can actually say more about the relationship between $R_{\bar{\rho}}^{\square}$ and $R_{\bar{\rho}}^{\mathrm{univ}}$. First, a definition.

Definition 2.3.8. [4, Definition 1.4.5] Let $\mathcal{D}, \mathcal{D}' : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Sets}$ be two functors, and $\varphi : \mathcal{D}' \to \mathcal{D}$ a natural transformation. Then φ is called *formally smooth* if for any surjection $A \to A' \in \mathrm{CNL}_{\mathcal{O}}$, the map

$$\mathcal{D}'(A) \to \mathcal{D}'(A) \times_{\mathcal{D}(A')} \mathcal{D}(A)$$

is surjective.

Remark 2.3.9. If $\mathcal{D}$ and $\mathcal{D}'$ are representable with representing objects R and R', respectively, then φ is formally smooth if and only if R' is a power series ring over R ([30, Proposition 2.5]).

Going back to the situation at hand, observe that there is a natural transformation $\varphi : \mathcal{D}_{\bar{\rho}}^{\square} \to \mathcal{D}_{\bar{\rho}}$, where on objects $A \in \mathrm{CNL}_{\mathcal{O}}$, the map $\mathcal{D}_{\bar{\rho}}^{\square}(A) \to \mathcal{D}_{\bar{\rho}}(A)$ sends a lift to A to the corresponding deformation (i.e. its equivalence class).

Lemma 2.3.10. [4, Corollary 1.4.6] The map φ just described is formally smooth.

Thus, by the remark preceding the lemma:

Corollary 2.3.11. If $\mathcal{D}_{\bar{\rho}}$ is representable, then $R_{\bar{\rho}}^{\square}$ is a power series ring over $R_{\bar{\rho}}^{\mathrm{univ}}$, of relative dimension $4 - h^0(G, \operatorname{ad} \bar{\rho})$.

Remark 2.3.12. Recall that $h^i(G, \operatorname{ad} \bar{\rho})) = \dim_k H^i(G, \operatorname{ad} \bar{\rho})$.

2.3.3 Obstruction Classes and Presentations

This section briefly outlines the concept and construction of obstruction classes, following [25]. The notion of an "unobstructed deformation problem" will be central in the last chapter of this thesis. The construction leads nicely into a presentation result for the rings $R^{\square}_{\bar\rho}$ and $R^{\text{univ}}_{\bar\rho}$ over $\mathcal{O}$.

Choose a surjection $A \to A'$ of artinian local rings in $\text{CNL}_{\mathcal{O}}$. Suppose that the kernel I satisfies $I \cdot \mathfrak{m}_A = 0$, meaning I can be viewed as a finite dimensional k-vector space. Suppose there is a deformation $\rho_{A'} : G \to \text{GL}_2(A')$ of $\bar\rho$. The question is: when we can deform this to a deformation $\rho_A : G \to \text{GL}_2(A)$ of $\bar\rho$ compatible with $\rho_{A'}$? In fact, there is a cohomology class which vanishes when such a deformation exists.

To construct the class, choose a representative lifting in the equivalence class of $\rho_{A'}$ let $\gamma : G \to \text{GL}_2(A)$ be a set-theoretic lift of this representative. If γ is a homomorphism, then we are done. To determine whether γ is a homomorphism, consider the function

$$c(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} \in 1 + I \cdot M_2(k) \cong I \otimes \operatorname{ad}\bar\rho.$$

One checks that c is a 2-cocycle, and so it determines a class $[c] \in H^2(G, \operatorname{ad}\bar\rho \otimes I) = H^2(G, \operatorname{ad}\bar\rho) \otimes I$. If this class is 0, then there is a deformation of $\rho_{A'}$ to a ρ_A, as desired.

For this reason, if $H^2(G, \operatorname{ad}\bar\rho) = 0$, then the lifting problem for $\bar\rho$ is said to be *unobstructed*.

Recall that the tangent space for $R^{\square}_{\bar\rho}$ is isomorphic to $Z^1(G, \operatorname{ad}\bar\rho)$, and the tangent space for $R^{\text{univ}}_{\bar\rho}$ is isomorphic to $H^1(G, \operatorname{ad}\bar\rho)$. Let the dimension of these two spaces be d and d', respectively. There are surjections

$$\phi : \mathcal{O}[\![x_1, \ldots, x_d]\!] \to R^{\square}_{\bar\rho}, \quad \phi' : \mathcal{O}[\![x_1, \ldots, x'_d]\!] \to R^{\text{univ}}_{\bar\rho}.$$

The following result is due to Mazur:

Proposition 2.3.13. [25, Proposition 2] The number of generators for $\ker\phi$ and $\ker\phi'$ is bounded by $\dim H^2(G, \operatorname{ad}\bar\rho)$. Thus, if we are in the unobstructed setting, both $R^{\square}_{\bar\rho}$ and $R^{\text{univ}}_{\bar\rho}$ are power series rings over $\mathcal{O}$.

2.3.4 Fixing Determinants

In many instances, it is useful to consider lifts and deformations which fix the determinant. Namely, given the residual representation $\bar{\rho} : G \to \mathrm{GL}_2(k)$, fix a character $\mu : G \to \mathcal{O}^\times$ which lifts $\det \bar{\rho}$. We then look at lifts $\rho : G \to \mathrm{GL}_2(A)$, where $A \in \mathrm{CNL}_\mathcal{O}$ such that $\det \rho$ agrees with the composition

$$G \xrightarrow{\mu} \mathcal{O}^\times \to A^\times,$$

the latter map coming from the structural morphism of A as an $\mathcal{O}$-algebra. Since determinants are invariant under conjugation, this notion makes sense for both lifts and deformations.

Even in this setting, the work we have done goes through similarly. The only difference to make is that one uses $\mathrm{ad}^0 \bar{\rho}$ instead of $\mathrm{ad}\, \bar{\rho}$, where $\mathrm{ad}^0 \bar{\rho}$ denotes the set of traceless matrices in $M_2(k)$ with the same action of G. One way to see that this is the correct change is by examining the Zariski tangent spaces of the new functors/representing objects. Recall that the isomorphism between $Z^1(G, \mathrm{ad}\, \bar{\rho})$ and $\mathcal{D}^\square_{\bar{\rho}}(k[\epsilon]/(\epsilon^2))$ sends a cocycle ϕ to the representation given by $\rho(g) = (1 + \phi(g)\epsilon)\bar{\rho}(g)$. Taking determinants and using that $\epsilon^2 = 0$, we get

$$\det \rho(g) = \mu(g)(1 + \mathrm{tr}\, \phi(g)\epsilon).$$

Thus, we need $\mathrm{tr}\, \phi(g) = 0$ for all $g \in G$, which means ϕ takes values in $\mathrm{ad}^0 \bar{\rho}$, as desired.

2.3.5 Local Deformation Problems

For this section, we will not work in the greatest generality, and instead restrict to the setting necessary for the next chapter. Keep all the notation from the beginning of the section, except now let $G = G_F$ for some number field F (so, for example $\bar{\rho}$ is a representation $\bar{\rho} : G_F \to \mathrm{GL}_2(k)$). Assume that k is large enough to contain all the eigenvalues of all the elements in the image $\bar{\rho}(G_F)$. Fix a finite set of finite places S of F. Ultimately, the goal will be to consider deformations of $\bar{\rho}$, but it will be useful to impose some restrictions on the deformations of local representations $\bar{\rho}|_{G_{F_v}}$.

For reasons that we will see in the next chapter, for $v \in S$, fix a ring $\Lambda_v \in \mathrm{CNL}_{\mathcal{O}}$. This is in greater generality than most references on the subject, but it is the setting of [41], which is needed later on. Most works on the subject simply take $\Lambda_v = \mathcal{O}$. For the remainder of the chapter, we will consider only lifts and deformations to objects in the subcategory CNL_{Λ_v} of $\mathrm{CNL}_{\mathcal{O}}$, though the reader can just as easily think of working in $\mathrm{CNL}_{\mathcal{O}}$.

Definition 2.3.14. If $v \in S$, then a local deformation problem at v is a collection $\mathcal{D}_v$ of liftings of $\bar{\rho}|_{G_{F_v}}$ to objects in CNL_{Λ_v} satisfying:

(1) $(k, \bar{\rho}|_{G_{F_v}}) \in \mathcal{D}_v$.

(2) If $f : R \to S$ is a morphism and $(R, \rho) \in \mathcal{D}_v$, then $(S, f \circ \rho) \in \mathcal{D}_v$.

(3) Suppose (R_1, ρ_1) and $(R_2, \rho_2) \in \mathcal{D}_v$, and let I_i be a closed ideal of R_i, and suppose there is an isomorphism $f : R_1/I_1 \xrightarrow{\sim} R_2/I_2$ in CNL_{Λ_v} such that $f(\rho_1 \bmod I_1) = \rho_2 \bmod I_2$. If $R_3 \subset R_1 \oplus R_2$ denotes the subring of elements with the same image in $R_1/I_1 \cong R_2/I_2$, then $(R_3, \rho_1 \oplus \rho_2) \in \mathcal{D}_v$.

(4) If $(R_j, \rho_j) \in \mathcal{D}_v$ forms an inverse system, then

$$(\varprojlim R_j, \varprojlim \rho_j) \in \mathcal{D}_v.$$

(5) If $(R, \rho) \in \mathcal{D}_v$, then so is any equivalent lifting.

(6) If $S \hookrightarrow R$ is an injective morphism in CNL_{Λ_v} and $\rho : G_{F_v} \to \mathrm{GL}_2(S)$ is a lifting of $\bar{\rho}|_{G_{F_v}}$ with $(R, \rho) \in \mathcal{D}_v$, then $(S, \rho) \in \mathcal{D}_v$.

Let $R_v^\square$ denote the universal lifting ring of $\bar{\rho}|_{G_{F_v}}$. It would be nice to know when lifts are in $\mathcal{D}_v$ in terms of the ring $R_v^\square$. First observe that an element $A \in \ker(\mathrm{GL}_2(R_v^\square) \to \mathrm{GL}_2(k)) = I_2 + M_2(\mathfrak{m}_{R_v^\square})$ acts on $R_v^\square$. Indeed, if $\rho^\square : G_{F_v} \to \mathrm{GL}_2(R_v^\square)$ denotes the universal lift, then A acts on $\rho^\square$ via $A^{-1}\rho^\square A$, and by universality, this gives a map $R_v^\square \to R_v^\square$, which is defined to be the action of A on $R_v^\square$. With this in mind, we can give a description of local deformation problems in terms of the universal lift.

Lemma 2.3.15. [6, Lemma 2.2.3] Let $\mathfrak{m}_v = \mathfrak{m}_{R_v^\square}$.

(1) If I is a $I_2 + M_2(\mathfrak{m}_v)$-invariant ideal of $R_v^\square$, then the collection of all liftings ρ over rings R such that $I \subset \ker(R_v^\square \to R)$ is a local deformation problem.

(2) If $\mathcal{D}_v$ is a local deformation problem, then there is a $I_2 + M_2(\mathfrak{m}_v)$-invariant ideal I_v of $R_v^\square$ such that $\mathcal{D}_v$ is the deformation problem from (1). Namely, $(R, \rho) \in \mathcal{D}_v$ if and only if $I_v \subset \ker(R_v^\square \to R)$.

The lemma allows for an alternate definition of a local deformation problem, as is done in [41, Definition 5.5].

Definition 2.3.16. Let $\mathcal{D}_v^\square = \mathcal{D}_{\bar{\rho}|_{G_{F_v}}}^\square$. A local deformation problem is a subfunctor $\mathcal{D}_v \subset \mathcal{D}_v^\square$ such that:

(1) $\mathcal{D}_v$ is represented by a quotient R_v of $R_v^\square$.

(2) For all $R \in \mathrm{CNL}_{\Lambda_v}$ and $A \in \ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(k))$, if $\rho \in \mathcal{D}_v(R)$, then $A\rho A^{-1} \in \mathcal{D}_v(R)$.

By viewing local deformation problems as a subfunctor of $\mathcal{D}_v^\square$, we can also get a description of its tangent space as a subspace of the tangent space of $\mathcal{D}_v^\square$, which is isomorphic to $Z^1(G_{F_v}, \mathrm{ad}\,\bar{\rho})$ by Lemma 2.3.6. Also recall that Lemma 2.3.5 gives an isomorphism between $\mathcal{D}_v^\square(k[\epsilon]/(\epsilon^2))$ (the Zariski tangent space) and $\mathrm{Hom}_k(\mathfrak{m}_v/(\mathfrak{m}_v^2, \mathfrak{m}), k)$.

Definition 2.3.17. ([6]) Suppose $\mathcal{D}_v$ is a local deformation problem, and let $I_v \subset R_v^\square$ be the ideal as in the previous lemma.

(1) Let $\mathcal{L}_v^1 \subset Z^1(G_{F_v}, \mathrm{ad}\,\bar{\rho})$ be the annihilator of the image of I_v in $\mathfrak{m}_v/(\mathfrak{m}_v^2, \mathfrak{m})$ under the isomorphism

$$\mathrm{Hom}_k(\mathfrak{m}_v/(\mathfrak{m}_v^2, \mathfrak{m}), k) \cong Z^1(G_{F_v}, \mathrm{ad}\,\bar{\rho}).$$

(2) Let $\mathcal{L}_v = \mathcal{L}_v(\mathcal{D}_v)$ be the image of $\mathcal{L}_v^1$ in $H^1(G_{F_v}, \mathrm{ad}\,\bar{\rho})$.

Remark 2.3.18. (1) Because I_v is $I_2 + M_2(\mathfrak{m}_v)$-invariant, the subspace $\mathcal{L}_v^1$ is the preimage of $\mathcal{L}_v$.

(2) The isomorphism $\mathrm{Hom}_k(\mathfrak{m}_v/(\mathfrak{m}_v^2, \mathfrak{m}), k) \cong Z^1(G_{F_v}, \mathrm{ad}\,\bar{\rho})$ induces an isomorphism

$$\mathrm{Hom}_k(\mathfrak{m}_v/(\mathfrak{m}_v^2, I_v, \mathfrak{m}), k) \cong \mathcal{L}_v^1.$$

(3) The exact sequence

$$0 \to H^0(G_{F_v}, \mathrm{ad}\,\bar{\rho}) \to \mathrm{ad}\,\bar{\rho} \to Z^1(G_{F_v}, \mathrm{ad}\,\bar{\rho}) \to H^1(G_{F_v}, \mathrm{ad}\,\bar{\rho}) \to 0$$

and remark (2) above give

$$\dim_k \mathcal{L}_v^1 = 4 + \dim_k \mathcal{L}_v - \dim_k H^0(G_{F_v}, \mathrm{ad}\,\bar{\rho}).$$

We will look at specific examples of local deformation problems in the next chapter. Just as before, if determinants are fixed, then everything goes through unchanged, except $\mathrm{ad}\,\bar{\rho}$ is replaced by $\mathrm{ad}^0\,\bar{\rho}$ (which may lead to a slight change in the dimension counts).

2.3.6 Global Deformations

2.3.6.1 Global Deformation Problems and T-framed deformations

Keep the notation from the previous subsection. Having defined local deformation problems, the focus will shift to global deformations. However, as remarked in the beginning of the previous section, we will want our global lifts to adhere to some local restrictions.

At this point, fix a continuous character $\mu : G_F \to \mathcal{O}^\times$ which lifts $\det \bar{\rho}$. Also assume that $\bar{\rho}$ is absolutely irreducible. Recall that for $v \in S$, there is a fixed ring $\Lambda_v \in \mathrm{CNL}_{\mathcal{O}}$. Let $\Lambda = \widehat{\bigotimes}_v \Lambda_v$, the tensor product being over $\mathcal{O}$. As with the previous section, references for this section typically have $\Lambda_v = \mathcal{O}$, in which case $\Lambda = \mathcal{O}$.

Definition 2.3.19. [41, Definition 5.6] A global deformation problem $\mathcal{S}$ is a tuple

$$\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S}),$$

where:

(1) The objects $\bar{\rho}$, μ, and Λ_v are as already defined.

(2) The $\mathcal{D}_v$ for $v \in S$ are local deformation problems for $\bar{\rho}|_{G_{F_v}}$.

Remark 2.3.20. In most of the references (e.g. [16], [6]) $\Lambda_v = \mathcal{O}$, and this is usually removed from the notation.

We will only want to consider deformations of $\bar{\rho}$ which are "of type $\mathcal{S}$." We define what this means.

Definition 2.3.21. Let $\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S})$ be a global deformation problem. A continuous lift $\rho : G_F \to \mathrm{GL}_2(R)$ to $R \in \mathrm{CNL}_\Lambda$ is of type $\mathcal{S}$ if:

(1) The lift ρ is unramified outside S.

(2) For each $v \in S$, the representation $\rho|_{G_{F_v}} \in \mathcal{D}_v(R)$, where R is regarded as a Λ_v algebra through the natural map $\Lambda_v \to \Lambda$.

(3) $\det \rho = \mu$ (when considered as characters $G_F \to R^\times$).

We have the usual equivalence relation on lifts of type $\mathcal{S}$ since this relation preserves the property of being type $\mathcal{S}$. It therefore makes sense to speak of deformations of $\bar{\rho}$ of type $\mathcal{S}$. In keeping with our usual notation, let $\mathcal{D}_{\mathcal{S}}^{\square} : \mathrm{CNL}_\Lambda \to \mathrm{Sets}$ be the functor which maps an object R to the set of lifts of $\bar{\rho}$ to R of type $\mathcal{S}$, and $\mathcal{D}_{\mathcal{S}}$ will be the functor mapping R to the set of deformations of $\bar{\rho}$ of type $\mathcal{S}$.

Theorem 2.3.22. [41, Theorem 5.9] Both $\mathcal{D}_{\mathcal{S}}^{\square}$ and $\mathcal{D}_{\mathcal{S}}$ are representable functors, with representing objects denoted $R_{\mathcal{S}}^{\square}$ and $R_{\mathcal{S}}$ of CNL_Λ, respectively.

Now fix a subset $T \subseteq S$.

Definition 2.3.23. (1) A T-framed lifting of $\bar{\rho}$ to $R \in \mathrm{CNL}_\Lambda$ is a tuple $(\rho; \alpha_v)_{v\in T}$ where ρ is a lifting of $\bar{\rho}$ and $\alpha_v \in I_2 + M_2(\mathfrak{m}_R)$.

(2) Two framed liftings $(\rho; \alpha_v)_{v\in T}$, $(\rho'; \alpha'_v)_{v\in T}$ are equivalent if there exists $\beta \in I_n + M_n(\mathfrak{m}_R)$ such that

$$\rho' = \beta\rho\beta^{-1} \quad \text{and} \quad \alpha'_v = \beta\alpha_v.$$

(3) A T-framed deformation of $\bar{\rho}$ is an equivalence class of framed lifts.

Remark 2.3.24. From the definition, any T-framed deformation $[(\rho;\alpha_v)_{v\in T}]$ gives rise to a deformation $[\rho]$ of $\bar{\rho}$ and, for each $v \in T$, a well-defined lifting $\alpha_v^{-1}\rho|_{G_{F_v}}\alpha_v$ of $\bar{\rho}|_{G_{F_v}}$. It is well defined because if $[(\rho;\alpha_v)]$ and $[(\rho';\alpha_v')]$ are two tuples which define the same equivalence class, then there exists $\beta \in I_2 + M_2(\mathfrak{m}_R)$ such that $\alpha_v' = \beta\alpha_v$ and $\rho' = \beta\rho\beta^{-1}$. But then

$$\alpha_v'^{-1}\rho'|_{G_{F_v}}\alpha_v' = \alpha_v^{-1}\beta^{-1}(\beta\rho|_{G_{F_v}}\beta^{-1})\beta\alpha_v = \alpha_v^{-1}\rho|_{G_{F_v}}\alpha_v.$$

The point of T-framed deformations is that it facilitates the study of deformations of $\bar{\rho}$ even when some of the local representations $\bar{\rho}|_{G_{F_v}}$ are reducible. By the remark, the α_v allow us to get well-defined elements of $\mathcal{D}_v(R)$.

Definition 2.3.25. A T-framed deformation $[(\rho;\alpha_v)_{v\in T}]$ is of type $\mathcal{S}$ if ρ is of type $\mathcal{S}$. Let $\mathcal{D}_{\mathcal{S}}^{\square_T} : \mathrm{CNL}_\Lambda \to \mathrm{Sets}$ denote the functor which takes R to the set of T-framed deformations of $\bar{\rho}$ to R of type $\mathcal{S}$.

Theorem 2.3.26. [41, Theorem 5.9] The functor $\mathcal{D}_{\mathcal{S}}^{\square_T}$ is representable by an object $R_{\mathcal{S}}^T \in \mathrm{CNL}_\Lambda$.

One more bit of notation is needed before moving on to cohomology. For a global deformation problem $\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S})$, let R_v denote the representing object of $\mathcal{D}_v$. Following [41], let

$$\Lambda_T = \widehat{\bigotimes}_{v\in T}\Lambda_v, \quad A_{\mathcal{S}}^T = \widehat{\bigotimes}_{v\in T} R_v.$$

Then $A_{\mathcal{S}}^T$ is canonically a Λ_T-algebra. It is very easy to see what role $A_{\mathcal{S}}^T$ plays: it represents the functor $\mathrm{CNL}_{\Lambda_T} \to \mathrm{Sets}$ which maps an object R to the set of tuples $(\rho_v)_{v\in T}$, where ρ_v is a lift of $\bar{\rho}|_{G_{F_v}}$ to R. There is a map $A_{\mathcal{S}}^T \to R_{\mathcal{S}}^T$ induced by the natural transformation of functors:

$$(\rho, \{\alpha_v\}_{v\in T}) \mapsto (\alpha_v^{-1}\bar{\rho}|_{G_{F_v}}\alpha_v).$$

This map is a homomorphism of Λ_T-algebras.

2.3.6.2 Cohomology

Recall that the object $R_v^\square$ from Section 2.3.5 has a Zariski tangent space isomorphic to $Z^1(G_{F_v}, \operatorname{ad}\bar{\rho})$. It was noted that if $\mathcal{D}_v$ is a local deformation problem, the tangent space of the representing object R_v is a subspace $\mathcal{L}_v^1$ of this set of 1-cocycles. If

$$\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S})$$

is a global deformation problem, since the determinant is fixed, the tangent space is now a subspace of $Z^1(G_{F_v}, \operatorname{ad}^0\bar{\rho})$. That is, there is an isomorphism

$$\operatorname{Hom}_k(\mathfrak{m}_{R_v}/(\mathfrak{m}_{R_v}^2, \mathfrak{m}_{\Lambda_v}), k) \cong \mathcal{L}_v^1.$$

Lastly, recall from Proposition 2.3.13 and the preceding remarks that there is a presentation for the universal lifting rings $R_v^\square$ over $\mathcal{O}$ in terms of a power series in some number of variables, given by the dimension of the tangent space, which in turn is given by the dimension of a cohomology group.

The goal of this section is to generalize these ideas to global deformations. Specifically, we want to examine $R_{\mathcal{S}}^T$, figure out the tangent space of the corresponding functor, and determine whether this ring can be expressed as a quotient of a power series over $A_{\mathcal{S}}^T$ in some number of variables. All of this will require cohomology. However, the usual cohomology groups will not be sufficient, as global deformations need to keep track of local information as well. Thus, cohomology groups which keep track of both the global and local information are needed. The result is a cone construction.

Let $T \subset S$ be a nonempty subset, and assume $\Lambda_v = \mathcal{O}$ for $v \in S - T$. In this case, $\Lambda_T \cong \Lambda$, and the map $A_{\mathcal{S}}^T \to R_{\mathcal{S}}^T$ is a homomorphism of Λ-algebras.

If G is a group and A is a G-module, then let $C^i(G, A)$ be as in Section 2.2.1. The cochain complex to consider is $C_{\mathcal{S},T}^i(G_{F,S}, \operatorname{ad}^0\bar{\rho})$, defined as follows:

$$C_{\mathcal{S},T}^0(G_{F,S}, \operatorname{ad}^0\bar{\rho}) = C^0(G_{F,S}, \operatorname{ad}\bar{\rho}),$$

$$C_{\mathcal{S},T}^1(G_{F,S}, \operatorname{ad}^0\bar{\rho}) = C^1(G_{F,S}, \operatorname{ad}^0\bar{\rho}) \oplus \bigoplus_{v\in T} C^0(G_{F_v}, \operatorname{ad}\bar{\rho}),$$

$$C^2_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) = C^2(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \oplus \bigoplus_{v \in T} C^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho}) \oplus \bigoplus_{v \in S-T} \frac{C^1(G_{F_v}, \operatorname{ad}^0(\bar{\rho}))}{\mathcal{L}^1_v},$$

$$C^i_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) = C^i(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \oplus \bigoplus_{v \in S} C^{i-1}(G_{F_v}, \operatorname{ad}^0 \bar{\rho}), \quad i \geq 3.$$

Essentially, the complexes for the global cohomology and each of the local cohomology groups are put together. The coboundary maps are given by

$$\delta^{i+1} : C^i_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to C^{i+1}_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}),$$

where $(\phi, (\psi_v)) \mapsto (\delta\phi, (\phi|_{G_{F_v}} - \delta\psi_v))$, where the δ's are the usual coboundary maps from Section 2.2.1. The cohomology groups $H^i_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho})$ are then defined to be the cohomology of this cochain complex.

Perhaps unsurprisingly, there is a long exact sequence in cohomology, relating the new cohomology groups to the old ones.

Lemma 2.3.27. We have a long exact sequence

$$\begin{aligned}
0 \;\to\;& H^0_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to H^0(G_{F,S}, \operatorname{ad} \bar{\rho}) \to \bigoplus_{v \in T} H^0(G_{F_v}, \operatorname{ad} \bar{\rho}) \\
\to\;& H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to H^1(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to \bigoplus_{v \in S-T} H^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho})/L_v \oplus \bigoplus_{v \in T} H^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho}) \\
\to\;& H^2_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to H^2(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to \bigoplus_{v \in S} H^2(G_{F_v}, \operatorname{ad}^0 \bar{\rho}) \\
\to\;& \cdots
\end{aligned}$$

Remark 2.3.28. Observe that if $T = \emptyset$, then in the above exact sequence, the first few terms are

$$0 \to H^1_{\mathcal{S}}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to H^1(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) \to \bigoplus_{q \in S} H^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho})/L_v,$$

so that $H^1_{\mathcal{S}}(G_{F,S}, \operatorname{ad}^0 \bar{\rho})$ just becomes a Selmer group.

Before stating the big consequence of all this work, we need one more definition. Since p is odd (by assumption), the representation $\operatorname{ad}^0 \bar{\rho}$ is self-dual, i.e. $(\operatorname{ad}^0 \bar{\rho})^* = \operatorname{ad}^0 \bar{\rho}$ (coming from the trace pairing). The group that will play the role of the dual Selmer group is:

$$H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)) = \ker \left(H^1(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)) \to \bigoplus_{v \in S-T} \frac{H^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho}(1))}{\mathcal{L}^\perp_v} \right),$$

where $\mathcal{L}_v^\perp$ is as in Section 2.2.7. Notice that this is essentially Definition 2.2.25 for the places outside T.

Recall that if $H^i(G, V)$ denotes the cohomology of a group G with coefficients in a finite dimensional vector space V over a field $\mathbb{F}$, then $h^i(G, V)$ will denote the dimension $h^i(G, V) = \dim_{\mathbb{F}} H^i(G, V)$ (assuming this is finite). Going back to our notation, let $l_v = \dim \mathcal{L}_v$, and $h^i_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) = \dim H^i_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho})$. In other words, lower case letters simply mean the dimension of the corresponding group.

Proposition 2.3.29. ([16, Proposition 3.24], [41, Proposition 5.10]) Keep all the assumptions as above.

(1) The ring $R^T_{\mathcal{S}}$ is a quotient of a power series ring over $A^T_{\mathcal{S}}$ in $h^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho})$ variables.

(2) There is a canonical isomorphism

$$\operatorname{Hom}_k(\mathfrak{m}_{R^T_{\mathcal{S}}}/(\mathfrak{m}^2_{R^T_{\mathcal{S}}}, \mathfrak{m}_{A^T_{\mathcal{S}}}, \mathfrak{m}), k) \cong H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}).$$

(3) There is an equality

$$h^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) = h^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)) - h^0(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)) - 1 + \#T$$
$$+ \sum_{v \in S-T} (l_v - h^0(G_{F_v}, \operatorname{ad}^0 \bar{\rho})) - \sum_{v|\infty} h^0(G_{F_v}, \operatorname{ad}^0 \bar{\rho}).$$

Proof. Though we omit the proof, we note that it involves comparing the exact sequence from the lemma to the Poitou-Tate exact sequence. □

2.4 Automorphic Representations

The full theory of automorphic representations is much too long to describe in detail. We will only present the material needed for the later chapters. As such, we will not work in full generality, and we will direct the reader to appropriate sources for proofs.

Keep the notation from Section 1.3. Let F be a number field.

2.4.1 Representations of $\mathrm{GL}_n(F_v)$

Let v be a finite place of F. The representations of $\mathrm{GL}_n(F_v)$ to consider will be on $\mathbb{C}$-vector spaces, usually infinite dimensional. Let W be a representation of $\mathrm{GL}_n(F_v)$ (i.e. a $\mathbb{C}$-vector space with a map $\pi : \mathrm{GL}_n(F_v) \to \mathrm{Aut}(W)$).

Definition 2.4.1. (1) The representation (π, W) is *smooth* if for any $w \in W$, the stabilizer of w in $\mathrm{GL}_n(F_v)$ is open.

(2) The representation is *admissible* if it is smooth and if for any compact open subgroup $U \subset \mathrm{GL}_n(F_v)$, the space W^U is finite dimensional.

Example 2.4.2. ([16]) Consider the case $n = 2$. Let $B \subset \mathrm{GL}_2(F_v)$ be the subset of upper triangular matrices. Define a map $\delta : B \to K^\times$ by

$$\delta\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = ad^{-1}.$$

Suppose that there are two characters $\chi_1, \chi_2 : K^\times \to \mathbb{C}^\times$. The tensor product $\chi_1 \otimes \chi_2$ can be viewed as a representation of B via:

$$(\chi_1 \otimes \chi_2)\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \chi_1(a)\chi_2(d).$$

The normalized induction, denoted $i_B^{\mathrm{GL}_2}$, gives a representation $\chi_1 \times \chi_2$ of $\mathrm{GL}_2(F_v)$. As a set, $\chi_1 \times \chi_2 = i_B^{\mathrm{GL}_2}(\chi_1 \otimes \chi_2)$ is

$$\{\phi : \mathrm{GL}_2(F_v) \to \mathbb{C} : \phi \text{ smooth}, \phi(bg) = (\chi_1 \otimes \chi_2)(b)|\delta(b)|_v^{1/2}\phi(g) \quad \forall b \in B, g \in \mathrm{GL}_2(F_v)\},$$

and $\mathrm{GL}_2(F_v)$ acts on this set by right translation, i.e. $(g'\phi)(g) = \phi(gg')$, giving a representation of $\mathrm{GL}_2(F_v)$.

Definition 2.4.3. If $\chi_1 \times \chi_2$ is irreducible, it is called a *principal series representation.*

However, $\chi_1 \times \chi_2$ need not be irreducible. In fact:

Proposition 2.4.4. The representation $\chi_1 \times \chi_2$ is irreducible if and only if $\chi_1/\chi_2 \neq |\cdot|_v^{\pm 1}$. The representation $\chi \times \chi|\cdot|$ has a one-dimensional irreducible subrepresentation, and the corresponding quotient is irreducible.

Remark 2.4.5. The irreducible quotient in the proposition is denoted $\mathrm{Sp}_2(\chi)$.

2.4.2 Local Langlands Correspondence

The local Langlands correspondence gives a family of bijections rec_{F_v} between the set of isomorphism classes of irreducible admissible representations of $\mathrm{GL}_n(F_v)$ over $\mathbb{C}$ and the set of isomorphism classes of two-dimensional Frobenius-semisimple Weil-Deligne representations of W_{F_v} over $\mathbb{C}$. Since there is a family of maps, there needs to be some way of normalizing the map, and there is a method using an equality of certain ϵ- and L-factors, neither of which we are going to discuss here. Instead, we direct the reader to [18] and [17] for details. Instead, we will follow [16] and simply state some of the properties.

Before we state the proposition, we need one more normalization. From local class field theory, there is a local Artin map $\mathrm{Art}_{F_v} : F_v^\times \to W_{F_v}^{ab}$, and we normalize it so that uniformisers are sent to geometric Frobenius elements. For future reference, we make the same normalization for the global Artin map $\mathrm{Art}_F : \mathbb{A}_F^\times \to G_F^{ab}$.

Proposition 2.4.6. [16, Fact 4.5] Let rec_{F_v} be normalized as stated above.

(1) If $n = 1$, then $\mathrm{rec}_{F_v}(\chi) = \chi \circ \mathrm{Art}_{F_v}^{-1}$.

(2) If χ is a smooth character, then $\mathrm{rec}_{F_v}(\pi \otimes (\chi \circ \det)) = \mathrm{rec}_{F_v}(\pi) \otimes \mathrm{rec}_{F_v}(\chi)$.

(3) We have $\mathrm{rec}_{F_v}(\mathrm{Sp}_2(\chi)) = \mathrm{Sp}_2(\mathrm{rec}_{F_v}(\chi))$.

Following Thorne [41], there is a new map $\mathrm{rec}_{F_v}^T$ defined by

$$\mathrm{rec}_{F_v}^T(\pi) = \mathrm{rec}_{F_v}(\pi \otimes |\cdot|_v^{-1/2}).$$

The map $\mathrm{rec}_{F_v}^T$ commutes with automorphisms of $\mathbb{C}$, and so it makes sense over any field Ω which is isomorphic to $\mathbb{C}$. For example, one could take $\Omega = \overline{\mathbb{Q}}_p$.

Let $\chi : W_{F_v} \to \Omega^\times$ be a character with open kernel. Consider the Weil-Deligne representation (r, N), where $r = \chi \oplus \chi|\cdot|_v^{-1}$ and $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Write $\mathrm{St}_2(\chi \circ \mathrm{Art}_{F_v}) = (\mathrm{rec}_{F_v}^T)^{-1}(r, N)$.

Definition 2.4.7. If $\Omega = \mathbb{C}$, the representation $\mathrm{St}_2(1)$ is called the Steinberg representation, and we will denote it St_2.

Remark 2.4.8. The Steinberg representaion is what was called $\mathrm{Sp}_2(|\cdot|_v^{-1/2})$ in the previous section.

2.4.3 Galois Representations Attached to Automorphic Representations

In the next chapter, following [41], the automorphic representations to be considered are those $\pi = \bigotimes_v' \pi_v$ of $\mathrm{GL}_2(\mathbb{A}_F)$ such that for each $v|\infty$, the representation π_v is the local discrete series representation of $\mathrm{GL}_2(\mathbb{R})$ with trivial central character. Such a representation will be called a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2.

Theorem 2.4.9. If π is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, for every isomorphism $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$, there is an associated Galois representation $r_\iota(\pi) : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ such that:

(1) The representation $r_\iota(\pi)$ is de Rham, and for every embedding $\tau : F \hookrightarrow \overline{\mathbb{Q}}_p$, we have $\mathrm{HT}_\tau(\rho) = \{0, 1\}$.

(2) If v is a finite place of F, then

$$\mathrm{WD}(r_\iota(\pi)|_{G_{F_v}})^{\text{F-ss}} \cong \mathrm{rec}_{F_v}^T(\iota^{-1}\pi_v).$$

(3) If $\omega_\pi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times$ denotes the central character of π, then

$$\det r_\iota(\pi) = \epsilon^{-1}\iota^{-1}(\omega_\pi \circ \mathrm{Art}_F^{-1}),$$

where Art_F is the global Artin map.

Remark 2.4.10. Recall from section 1.3 that ϵ denotes the p-adic cyclotomic character.

2.5 Modularity Lifting

This section gives the idea, but not many of the details, of two methods of modularity lifting. The first is due to Taylor and Wiles [45], and the second is due to Khare [22]. Let $K/\mathbb{Q}_p$ be a finite extension with integer ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field k. Let $\mathbb{Q}$ be a number field, and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ be a representation whose reduction $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ is modular. In this section we will not be terribly precise, as the ideas are more important for later use.

2.5.1 Taylor-Wiles Method

The goal is to somehow lift the modularity of $\bar{\rho}$ to deduce the modularity of ρ. Let S_0 denote the set of primes at which $\bar{\rho}$ is ramified, and let $S \supset S_0$ denote a set of places containing S_0. One way of proving the modularity of ρ is through the use of an $R = \mathbb{T}$ theorem.

Given the set S, we can consider a global deformation problem $\mathcal{S}_S$ similar to the ones defined in Section 2.3. For now, it is enough to know that $\mathcal{S}_S$ should consider deformations of $\bar{\rho}$ which are unramified outside S and share the same local properties as $\bar{\rho}$ at the primes in S. Associated to this deformation problem is a universal deformation ring R_S.

On the other hand, one can prove the existence of a universal modular deformation ring $\mathbb{T}_S$, which parametrizes deformations of $\bar{\rho}$ of type $\mathcal{S}_S$ which are also modular. By universality of R_S, there is a map $\varphi_S : R_S \to \mathbb{T}_S$. It is not hard to show the surjectivity of φ_S. An $R = \mathbb{T}$ theorem is the assertion that φ_S is an isomorphism.

Taylor and Wiles [45] proved that φ_{S_0} is an isomorphism, which is the so-called minimal case. The passage from the minimal to the non-minimal case (when $S \supset S_0$) was carried out by Wiles [44]. Right now, we will focus on the minimal case.

The strategy to prove that φ_{S_0} is an isomorphism is known as the Taylor-Wiles method. We now work only with $S = S_0$ and drop it from the notation. An issue with proving $R = \mathbb{T}$ is that the ring R, in theory, can be much bigger than the ring $\mathbb{T}$. To get around this, Taylor and Wiles introduced auxiliary rings R_{Q_n} and $\mathbb{T}_{Q_n}$ for $n \geq 1$, where Q_n is a set of primes such that, for $q \in Q$, $q \equiv 1 \bmod p^n$ and $\bar{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues. The primes are chosen so that there is some control on the size of the rings R_{Q_n}. In fact, the number of generators of this ring as an $\mathcal{O}$-algebra is finite and independent of n. With these auxiliary rings in hand, they were able to pass to a limit to get rings R_∞ and $\mathbb{T}_\infty$ which they showed are isomorphic, and then deduced that R and $\mathbb{T}$ are isomorphic. This is sometimes called a patching method. In essence, they were able to patch all the rings together to deduce the isomorphism in the limit.

They key to bounding the sizes of the R_{Q_n} is Proposition 2.3.29. If the size of Q_n is independent of n and the dual Selmer group term can be made 0, then the number of generators of R_{Q_n} would be independent of n as well. Thus, the goal becomes to find auxiliary primes which, when added, "kills dual Selmer," in the sense that the augmented deformation problem has vanishing dual Selmer group.

2.5.2 Khare's Method

For this section, assume $\mathcal{O} = W(k)$. An $R = \mathbb{T}$ does not seem like the most natural approach to modularity approach. In some sense, what an $R = \mathbb{T}$ theorem is doing is putting ρ into a collective family of representations and showing that the set is the same as the set of representations arising from modular forms. Perhaps the simpler approach would be to lift the modularity of $\bar{\rho}$ one step at a time. Namely, consider the mod p^n representation $\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(W_n(k))$, where $W_n(k)$ denotes the Witt vectors of length n of k, so that $\bar{\rho} = \rho_1$. Since ρ_1 is modular, there might be a way to show that each ρ_n is modular and somehow pass to the limit to deduce the modularity of ρ. The advantage of this approach would be that it deals directly with ρ and its reductions instead of considering the collection of ρ and many other representations. This method is carried out by Khare [22].

Khare also introduces auxiliary primes with additional ramification conditions, as was done in the Taylor-Wiles method (though the conditions for the primes are different). These conditions are not satisfied by ρ, but he shows they are satisfied by the mod p^n representation ρ_n. From this, he is able to show that ρ_n arises from a modular form of level N_n, a priori dependent on n. In order to effectively pass to the limit to deduce the modularity of ρ, this level should be independent of n.

At this point, Khare uses Mazur's principle [28, Section 8] to deduce that each ρ_n arises from a modular form of fixed level N, independent of n. He then passes to the limit to deduce the modularity of ρ.

CHAPTER 3

Two-Dimensional Residually Dihedral Representations

3.1 Introduction and Main Theorems

3.1.1 Automorphy Theorems

Let F be a totally real field, and let $\mathcal{O}$ be the integer ring of a finite extension of $\mathbb{Q}_p$. In a change from the previous chapter, write $\lambda \subset \mathcal{O}$ for the maximal ideal, and $k = \mathcal{O}/\lambda$ for the residue field. Let $\rho : G_F \to \mathrm{GL}_2(\mathcal{O})$ be a geometric representation. In proving the automorphy of ρ, there is usually an assumption made (the Taylor-Wiles hypothesis) on the residual representation, namely that $\bar{\rho}|_{G_{F(\zeta_p)}}$ be absolutely irreducible. This was the setting of Wiles [44] and Taylor-Wiles [45] in their proof of the modularity conjecture for semistable elliptic curves over $\mathbb{Q}$.

Since the original proof, there have been a few attempts to remove the Taylor-Wiles hypothesis. Skinner and Wiles [34] were able to remove the assumption in the case that ρ is ordinary. Recently, Thorne [41] removed the Taylor-Wiles hypothesis in many cases, asking that $\bar{\rho}$ be absolutely irreducible and the quadratic subfield K of $F(\zeta_p)/F$ be totally real.

The purpose of this chapter is to prove the automorphy of representations ρ which do not satisfy the Taylor-Wiles hypothesis, and in fact the main automorphy theorem of this chapter is slightly more general than the corresponding one in [41]. Namely, the assumption that K be totally real is replaced by the assumption that there is a "level raising" place v of F that splits in K such that the ratio of eigenvalues of $\bar{\rho}(\mathrm{Frob}_v)$ is q_v with $q_v \not\equiv 1 \bmod p$. The details will be provided in the next section. However, it is useful to note that this assumption is automatic when K is totally real, so the results of this chapter do generalize the ones in loc. cit.

The main theorem we prove is the following:

Theorem 3.1.1. ([21]) Let F be a totally real number field, let p be an odd prime, and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be a continuous representation satisfying the following:

(1) The representation ρ is almost everywhere unramified.

(2) For each $v|p$ of F, the local representation $\rho|_{G_{F_v}}$ is de Rham. For each embedding $\tau : F \hookrightarrow \overline{\mathbb{Q}}_p$, we have $\mathrm{HT}_\tau(\rho) = \{0, 1\}$.

(3) For each complex conjugation $c \in G_F$, we have $\det \rho(c) = -1$.

(4) The residual representation $\bar{\rho}$ is absolutely irreducible, but $\bar{\rho}|_{G_{F(\zeta_p)}}$ is a direct sum of two distinct characters. If K denotes the unique quadratic subfield of $F(\zeta_p)/F$ and $\bar{\gamma} : G_K \to k^\times$ is the ratio of the two characters, then further suppose $F(\zeta_p) \not\subset K(\bar{\gamma}\bar{\epsilon}^{-1}) \cap K(\bar{\gamma}\bar{\epsilon})$.

Then ρ is automorphic: there exists a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, an isomorphism $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$, and an isomorphism $\rho \cong r_\iota(\pi)$.

Note that the hypothesis on K in item (4) is equivalent to the existence of the "level raising" place described above. Also note that there is no assumption on the residual automorphy of $\bar{\rho}$.

The proof has two parts: a Galois theory argument and an automorphic forms argument. The Galois theory argument contains the original arguments for the purposes of the dissertation (and will be in Section 3.4), and the automorphic side is the same as [41]. As such, all the proofs from the Galois theory side are provided, but we will refer to loc. cit. for the proofs of the automorphic arguments.

The proof will blend the Taylor-Wiles method and the method of Khare of proving automorphy of ρ by using p-adic approximation (see Section 2.5). Along the way, we will describe how our arguments differ from the arguments of Thorne [41].

3.1.2 Automorphy of Elliptic Curves

It was once a conjecture that all elliptic curves over $\mathbb{Q}$ are modular, i.e. that the representations $\rho_{E,p}$ are modular for some (equivalently all) prime p. Wiles [44] and Taylor-Wiles [45] were able to prove that all semistable elliptic curves over $\mathbb{Q}$ are modular. This has since been extended to all elliptic curves over $\mathbb{Q}$ by work of Breuil, Conrad, Diamond, and Taylor ([5], [7], [9]).

Since then, the question has shifted to proving the automorphy of elliptic curves over totally real fields. After proving Theorem 3.1.1, we will describe this work and prove a new result in this setting. Specifically, we will prove:

Theorem 3.1.2. ([21]) Let F be a totally real field, and let E be an elliptic curve over F. Suppose:

(1) $F \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$.

(2) E has no F-rational 7-isogeny.

(3) Either $\bar{\rho}_{E,7}(G_{F(\zeta_7)})$ is absolutely irreducible, or it is reducible and is conjugate to a subgroup of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$.

Then E is modular.

Throughout this chapter, we will adhere to the notation and normalizations described in the opening chapter of the dissertation.

3.1.3 Structure of Chapter

The chapter will begin with a discussion about Shimura curves and Hida varieties. We will introduce Hecke operators acting on an appropriate $\mathcal{O}$-module, and introduce the Galois representations to be considered later. In addition, there will be theorems outlining the procedure for level raising and level lowering.

At that point, there will be a brief discussion on ordinary Galois representations before the bulk of the original work for the chapter is done in Section 3.4. When this is done, we go through the arguments to prove an $R = \mathbb{T}$ theorem which will be applied to proving the main theorem in Section 3.6. The chapter ends with an application to elliptic curves.

The original work for the purposes of this dissertation is concentrated in Section 3.4 and the final section on elliptic curves. The other arguments are unchanged from [41].

3.2 Shimura Curves and Hida Varieties

3.2.1 Quaternion Algebras and Reductive Groups

The source material for this section is [41]. Let F be a totally real number field of degree d over $\mathbb{Q}$, and assume d is even. Write $\tau_1, \tau_2, \ldots, \tau_d$ for the d real embeddings $F \hookrightarrow \mathbb{R}$. Let Q be a finite set of finite places of F. For each Q, fix a choice of quaternion algebra B_Q over F, where:

- If $\#Q$ is odd, then B_Q is ramified at $Q \cup \{\tau_2, \ldots, \tau_d\}$, and
- If $\#Q$ is even, then B_Q is ramified at $Q \cup \{\tau_1, \ldots, \tau_d\}$.

Remark 3.2.1. Recall that a quaternion algebra D over F is ramified at v if $D \otimes_v F_v$ is a division algebra. The places where the algebra ramifies determines the quaternion algebra up to isomorphism, and it can be any set of places of even cardinality. This is why the cases for $\#Q$ odd and even are separated.

For each Q, fix a maximal order $\mathcal{O}_Q \subset B_Q$. This means an isomorphism

$$\mathcal{O} \otimes_{\mathcal{O}_F} \prod_{v \nmid Q\infty} \mathcal{O}_{F_v} \cong \prod_{v \nmid Q\infty} M_2(\mathcal{O}_{F_v})$$

can be found and fixed.

Associated to this maximal order is a reductive group G_Q over $\mathcal{O}_F$. Indeed, its functor of points is given by $G_Q(R) = (\mathcal{O}_Q \otimes_{\mathcal{O}_F} R)^\times$. Notice that, by the above isomorphism, if $v \notin Q$ is a finite place, then

$$G_Q(\mathcal{O}_{F_v}) = (\mathcal{O}_Q \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v})^\times \cong M_2(\mathcal{O}_{F_v})^\times = \mathrm{GL}_2(\mathcal{O}_{F_v}),$$

so $G_Q(\mathcal{O}_{F_v}) \cong \mathrm{GL}_2(\mathcal{O}_{F_v})$.

Now let v be any finite place of F. For each $n \geq 1$, we can define a sequence of compact open subgroups of $\mathrm{GL}_2(\mathcal{O}_{F_v})$. Letting ϖ_v denote a uniformizer of $\mathcal{O}_{F_v}$:

- $U_0(v^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{F_v}) : c \equiv 0 \bmod \varpi_v^n \right\}$
- $U_1(v^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{F_v}) : c \equiv 0 \bmod \varpi_v^n, ad^{-1} \equiv 1 \bmod \varpi^n \right\}$
- $U_1^1(v^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{F_v}) : c \equiv 0 \bmod \varpi_v^n, a \equiv d \equiv 1 \bmod \varpi^n \right\}$

Observe that $U_1^1(v^n) \subset U_1(v^n) \subset U_0(v^n)$. If $v \notin Q$, use the same notation to denote the open compact subgroups of $G_Q(\mathcal{O}_{F_v})$ under the isomorphism $\mathrm{GL}_2(\mathcal{O}_{F_v}) \cong G_Q(\mathcal{O}_{F_v})$.

Let v_0 be a fixed placed of F such that $q_{v_0} > 4^d$. We will always assume that the sets Q are chosen so that $v_0 \notin Q$.

Definition 3.2.2. Let $U \subset G_Q(\mathbb{A}_F^\infty)$ be an open compact subgroup. Then U is called a *good subgroup* if:

(1) $U = \prod_v U_v$ for open compact subgroups $U_v \subset G_Q(F_v)$.

(2) If $v \in Q$, then U_v is the unique maximal compact subgroup of $G_Q(F_v)$.

(3) $U_{v_0} = U_1^1(v_0)$.

The set of good subgroups $U \subset G_Q(\mathbb{A}_F^\infty)$ will be denoted $\mathcal{J}_Q$.

3.2.2 Hecke Operators

The goal of this section is to define Hecke operators acting on certain $G_Q(F_v)$-modules. Let Q be a finite set of finite places of F (again, assuming $v_0 \notin Q$), and let $U \in \mathcal{J}_Q$.

Definition 3.2.3. [41, Section 4.1] If v is a finite place of F, write $\mathcal{H}(G_Q(F_v), U_v)$ for the $\mathbb{Z}$-algebra of compactly supported U_v-biinvariant functions $f : G(F_v) \to \mathbb{Z}$.

Remark 3.2.4. A basis for this algebra as a $\mathbb{Z}$-module is given by the characteristic functions of the double cosets $U_v g_v U_v$. Write $[U_v g_v U_v]$ for this characteristic function.

Let M be a smooth $\mathbb{Z}[G_Q(F_v)]$-module. Then M^{U_v} is a $\mathcal{H}(G_Q(F_v), U_v)$-module. Indeed, writing $U_v g_v U_v = \coprod_i h_i U_v$, for any $m \in M^{U_v}$:

$$[U_v g_v U_v] \cdot m = \sum_i h_i \cdot x.$$

We will now isolate a few elements of interest. Assume $v \notin Q$ and that $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$. We write

$$T_v = \left[\mathrm{GL}_2(\mathcal{O}_{F_v}) \begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathcal{O}_{F_v})\right], \quad S_v = \left[\mathrm{GL}_2(\mathcal{O}_{F_v}) \begin{pmatrix} \varpi_v & 0 \\ 0 & \varpi_v \end{pmatrix} \mathrm{GL}_2(\mathcal{O}_{F_v})\right].$$

Then $T_v, S_v \in \mathcal{H}(\mathrm{GL}_2(F_v), \mathrm{GL}_2(\mathcal{O}_{F_v})) \cong \mathcal{H}(G_Q(F_v), \mathrm{GL}_2(\mathcal{O}_{F_v}))$. If $v \notin Q$ and U_v is a smaller subgroup, say $U_1^1(v^n) \subset U_v \subset U_0(v^n)$, then write

$$\mathbf{U}_v = \left[U_v \begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix} U_v\right].$$

If $v \in Q$, then as U is a good subgroup by assumption, we know U_v is the maximal compact subgroup of $G_Q(F_v) = (B_Q \otimes_F F_v)^\times$ by definition, and define

$$\mathbf{U}_v = [U_v \tilde{\varpi}_v U_v],$$

where $\tilde{\varpi}_v \in \mathcal{O}_Q \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$ is a uniformizer. In this case, $\mathcal{H}(G_Q(F_v), U_v) = \mathbb{Z}[\mathbf{U}_v, \mathbf{U}_v^{-1}]$.

It is true that we have used $\mathbf{U}_v$ to mean two different things. However, we have the following lemma.

Lemma 3.2.5. [41, Lemma 4.1] If $v \in Q$ and $\chi : F_v^\times \to \mathbb{C}^\times$ is an unramified character, then let $\pi = \mathrm{St}_2(\chi)$. Write $\mathrm{JL}(\pi) = \chi \circ \det$ for the one-dimensional representation of $G_Q(F_v)$ associated to π under the local Jacquet-Langlands correspondence. Then

$$\mathrm{rec}^T_{F_v}(\pi) = \left(\chi \oplus \chi|\cdot|^{-1}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right).$$

The $\mathbf{U}_v$-eigenvalues on $\pi^{U_0(v)}$ and $\mathrm{JL}(\pi)^{U_v}$ coincide, and are both equal to the eigenvalue of Frob_v on $\mathrm{rec}^T_{F_v}(\pi)^{N=0}$.

This lemma justifies the use of $\mathbf{U}_v$ for the two different operators.

Let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 (in the sense of Chapter 2). Let p be a prime and let $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$ be an isomorphism. Let v be a place dividing p. For each $n \geq 1$, the operator $\mathbf{U}_v$ acts on $\iota^{-1}\pi_v^{U_1^1(v^n)}$. The eigenvalues for the operator lie in $\overline{\mathbb{Z}}_p$.

Definition 3.2.6. We say π_v is ι-ordinary if there exists $n \geq 1$ such that $\iota^{-1}\pi_v^{U_1^1(v^n)} \neq 0$, and $\mathbf{U}_v$ has an eigenvalue which lies in $\overline{\mathbb{Z}}_p^{\times}$.

We will eventually see how this notion relates to the usual definition of an ordinary Galois representation.

3.2.3 Hida Varieties and Shimura Curves

Suppose $\#Q$ is even, and let $U \in \mathcal{J}_Q$ be a good subgroup. Consider the double quotient

$$X_Q(U) = G_Q(F)\backslash G_Q(\mathbb{A}_F^{\infty})/U.$$

If $g \in G_Q(\mathbb{A}_F^{v_0,\infty})$, then $g^{-1}Ug \in \mathcal{J}_Q$ as well, and there is a map

$$X_Q(U) \to X_Q(g^{-1}Ug)$$

induced by right multiplication on $G(\mathbb{A}_F^{\infty})$. This gives a right action of $G_Q(\mathbb{A}_F^{v_0,\infty})$ on the projective system $\{X_Q(U)\}_{U\in\mathcal{J}_Q}$.

Now assume $\#Q$ is odd. Fix an isomorphism $B_Q \otimes_{F,\tau_1} \mathbb{R} \cong M_2(\mathbb{R})$, and let X denote the $G_Q(F \otimes_{\mathbb{Q}} \mathbb{R})$-conjugacy class of the homomrphism $h : \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \mathbb{G}_m \to (\mathrm{Res}_{F/\mathbb{Q}}\, G_Q)_{\mathbb{R}}$ which maps $z = x + iy$ to the element

$$\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{-1}, 1, 1, \ldots, 1 \right).$$

For $U \in \mathcal{J}_Q$, we can consider the space

$$M_Q(U)(\mathbb{C}) = G_Q(F)\backslash G_Q(\mathbb{A}_F^{\infty}) \times X/U.$$

Associated to this topological space is a projective algebraic curve $M_Q(U)_{/F}$ such that $M_Q(U)(\mathbb{C})$ is the set of complex points. As before, right multiplication in $G_Q(\mathbb{A}_F^\infty)$ induces a system of isomorphisms $M_Q(U)(\mathbb{C}) \to M_Q(g^{-1}Ug)(\mathbb{C})$, and this gives a right action of $G_Q(\mathbb{A}_F^{v_0,\infty})$ on the projective system $\{M_Q(U)(\mathbb{C})\}_{U\in\mathcal{J}_Q}$. It can be shown, as is done in [41, Section 4.4, 4.5] that the curves $M_Q(U)$ admit integral models over $\mathcal{O}_{F_v}$. From now on, we will use $M_Q(U)$ to denote these integral models.

3.2.4 Hecke Algebras

Let p be a prime, and let $L/\mathbb{Q}_p$ be a finite extension with integer ring $\mathcal{O}$, and let $\lambda \subset \mathcal{O}$ denote the maximal ideal. Let $k = \mathcal{O}/\lambda$ for the residue field.

Let Q be a finite set of finite places of F, with $v_0 \notin Q$. Let S be a finite set of finite places with $Q \subset S$. Write $\mathbb{T}^{S,\mathrm{univ}} = \mathcal{O}[T_v, S_v]_{v\notin S}$, and $\mathbb{T}_Q^{S,\mathrm{univ}}$ for the polynomial algebra over $\mathbb{T}^{S,\mathrm{univ}}$ in the $\mathbf{U}_v$ for $v \in Q$. If $U \in \mathcal{J}_Q$, then define

$$H_Q(U) = \begin{cases} H^1(M_Q(U)_{\overline{F}}, \mathcal{O}) & \text{if } \#Q \text{ odd} \\ H^0(X_Q(U), \mathcal{O}) & \text{if } \#Q \text{ even} \end{cases}.$$

The $\mathcal{O}$-module $H_Q(U)$ is finite and free over $\mathcal{O}$.

Now assume that S is chosen so that if $v \notin S$, then $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$. Then $\mathbb{T}_Q^{S,\mathrm{univ}}$ acts on $H_Q(U)$. If $\#Q$ is odd, then the action commutes with the action of G_F, and the Eichler-Shimura relation holds: for finite $v \notin S \cup S_p$ of F, the action of G_{F_v} is unramified and

$$\mathrm{Frob}_v^2 - S_v^{-1} T_v \,\mathrm{Frob}_v + q_v S_v^{-1} = 0 \in \mathrm{End}_{\mathcal{O}}(H_Q(U)).$$

If M is a $\mathbb{T}^{S,\mathrm{univ}}$-module (resp. $\mathbb{T}_Q^{S,\mathrm{univ}}$-module), we write $T^S(M)$ (resp. $T_Q^S(M)$) for the image of $\mathbb{T}^{S,\mathrm{univ}}$ (resp. $\mathbb{T}_Q^{S,\mathrm{univ}}$) in $\mathrm{End}_{\mathcal{O}}(M)$. If $U \in \mathcal{J}_Q$ is a good subgroup, then $T^S(H_Q(U))$ and $T_Q^S(H_Q(U))$ are reduced and $\mathcal{O}$-torsion free.

Suppose that k'/k is a finite extension, and that there is a homomorphism $\mathbb{T}^{S,\mathrm{univ}} \to k'$ with kernel $\mathfrak{m}$. If $\mathfrak{m} \in \mathrm{Supp}(H_Q(U))$ for some Q and some $U \in \mathcal{J}_Q$, then there is a semi-simple Galois representation

$$\bar{\rho}_{\mathfrak{m}} : G_F \to \mathrm{GL}_2(\mathbb{T}^{S,\mathrm{univ}}/\mathfrak{m}),$$

uniquely determined by the following: if $v \notin S \cup S_p$, then $\bar{\rho}_{\mathfrak{m}}|_{G_{F_v}}$ is unramified, and $\bar{\rho}_{\mathfrak{m}}(\mathrm{Frob}_v)$ has characteristic polynomial $X^2 - T_v X + q_v S_v$ (here, the symbols represent their images in $\mathbb{T}^{S,\mathrm{univ}}/\mathfrak{m}$).

Definition 3.2.7. If $\bar{\rho}_{\mathfrak{m}}$ is absolutely reducible, then $\mathfrak{m}$ is called Eisenstein. Otherwise, $\bar{\rho}_{\mathfrak{m}}$ is non-Eisenstein.

If, on the other hand, we have a homomorphism $\mathbb{T}_Q^{S,\mathrm{univ}} \to k'$ with kernel $\mathfrak{m}$, then $\mathfrak{m}$ is called Eisenstein if $\mathfrak{m} \cap \mathbb{T}^{S,\mathrm{univ}}$ is Eisenstein, and otherwise is called non-Eisenstein. In either case, there is an associated Galois representation $\bar{\rho}_{\mathfrak{m}} : G_F \to \mathrm{GL}_2(\mathbb{T}_Q^{S,\mathrm{univ}}/\mathfrak{m})$. The next proposition gives the existence of a lift of $\bar{\rho}_{\mathfrak{m}}$.

Proposition 3.2.8. [41, Proposition 4.7] Assume $\#Q$ is odd, and let $\mathfrak{m} \subset \mathbb{T}^S(H_Q(U))$ be a non-Eisenstein maximal ideal. Then there exists:

(1) A continuous representation $\rho_{\mathfrak{m}} : G_F \to \mathrm{GL}_2(\mathbb{T}^S(H_Q(U))_{\mathfrak{m}})$ lifting $\bar{\rho}|_{\mathfrak{m}}$ and satisfying: for finite $v \notin S \cup S_p$ of F, the representation $\rho_{\mathfrak{m}}|_{G_{F_v}}$ is unramified, and $\rho_{\mathfrak{m}}(\mathrm{Frob}_v)$ has characteristic polynomial $X^2 - T_v X + q_v S_v$.

(2) A finite $\mathbb{T}^S(H_Q(U))_{\mathfrak{m}}$ module M, together with an isomorphism of $\mathbb{T}^S(H_Q(U))_{\mathfrak{m}}[G_F]$-modules

$$H_Q(U)_{\mathfrak{m}} \cong \rho_{\mathfrak{m}} \otimes_{\mathbb{T}^S(H_Q(U))_{\mathfrak{m}}} (\epsilon \det \rho_{\mathfrak{m}})^{-1} \otimes_{\mathbb{T}^S(H_Q(U))_{\mathfrak{m}}} M.$$

3.2.5 Level-Raising

The next two sections will be devoted to stating the relevant level-raising and level-lowering results needed to prove the main automorphy lifting theorem. The relevant source is [41, Sections 4.8, 4.9].

Fix a finite set R of finite places of F, and assume $\#R$ is even and $R \cap (S_p \cup \{v_0\}) = \emptyset$. Let $U \in \mathcal{J}_R$ be a good subgroup. Now let Q be a finite set of finite places of F, disjoint from $S_p \cup R \cup \{v_0\}$ and of even cardinality, satisfying the following: if $w \in Q$, then $q_w \not\equiv 1 \bmod p$ and $U_w = \mathrm{GL}_2(\mathcal{O}_{F_w})$. If $J \subset Q$ is a subset, define a new subgroup $U_J \subset G_{R \cup J}(\mathbb{A}_F^\infty)$ by the following:

- If $w \notin J$, then $U_{J,w} = U_w$.

- If $w \in J$, then $U_{J,w}$ is the unique maximal compact subgroup of $G_{R\cup J}(F_w)$.

Let S be a finite set of finite places of F with $S_p \cup R \cup Q \subset S$ and such that S contains all the places w such that $U_w \neq \mathrm{GL}_2(\mathcal{O}_{F_w})$. Let $\mathfrak{m} \subset \mathbb{T}^{S,\mathrm{univ}}$ denote a non-Eisenstein maximal ideal with $\mathfrak{m} \in \mathrm{Supp}(H_R(U))$. By definition, $\bar{\rho}_{\mathfrak{m}}$ is absolutely irreducible, and for each $v \in Q$, the restriction $\bar{\rho}_{\mathfrak{m}}|_{G_{F_v}}$ is unramified. Assume k is large enough that for all $v \in Q$, the eigenvalues α_v, β_v of $\bar{\rho}_{\mathfrak{m}}(\mathrm{Frob}_v)$ lie in k (if not, enlarge the field L). Also assume that for $v \in Q$, the ratio $\beta_v/\alpha_v = q_v$. This is a well-known level-raising congruence for the place v.

Lemma 3.2.9. [41, Lemma 4.11] If $J \subset Q$, let $\mathfrak{m}_J \subset \mathbb{T}_J^{S,\mathrm{univ}}$ denote the maximal ideal generated by $\mathfrak{m}$ and the elements $\mathbf{U}_v - \alpha_v$ for $v \in J$. Then $\mathfrak{m}_J \in \mathrm{Supp}(H_{R\cup J}(U_J))$.

Proof. See the proof of Lemma 4.11 in [41]. □

More relevant for us will be the following two propositions. Again, we refer the reader to loc. cit. for the proofs.

Proposition 3.2.10. [41, Proposition 4.12] We have

$$1 \leq \dim_k(H_{R\cup J}(U_Q) \otimes_{\mathcal{O}} k) \leq 4^{\#Q} \dim_k(H_R(U) \otimes_{\mathcal{O}} k)[\mathfrak{m}].$$

Proposition 3.2.11. [41, Lemma 4.13] Let $\sigma \subset S_p$, and let $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$ be an isomorphism. Let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 which satisfies:

- The representation $\overline{r_\iota(\pi)}$ is irreducible.

- If $v \in \sigma$, then π_v is ι-ordinary and $\pi_v^{U_0(v)} \neq 0$.

- If $v \in S_p \backslash \sigma$, then π_v is not ι-ordinary and π_v is unramified.

- If $v \in R$, then π_v is an unramified twist of the Steinberg representation.

- If $v = v_0$, then $\pi_{v_0}^{U_1^1(v_0)} \neq 0$

- If $v \notin S_p \cup R \cup \{v_0\}$ is a finite place of F, then π_v is unramified.

- If $v \in Q$, then the eigenvalues α_v, β_v of $\overline{r_\iota(\pi)}(\mathrm{Frob}_v)$ satisfy $\beta_v/\alpha_v = q_v$.

Then there exists a cuspidal automorphic representation π' of weight 2 satisfying:

- There is an isomorphism $\overline{r_\iota(\pi)} \cong \overline{r_\iota(\pi')}$.
- If $v \in \sigma$, then π'_v is ι-ordinary and $(\pi')_v^{U_0(v)} \neq 0$.
- If $v \in S_p \backslash \sigma$, then π'_v is not ι-ordinary and π'_v is unramified.
- If $v \in R \cup Q$, then $\pi'_v \cong \mathrm{St}_2(\chi_v)$ for some unramified character $\chi_v : F_v^\times \to \mathbb{C}$. If $v \in Q$, then $\iota^{-1}\chi_v(\varpi_v)$ is congruent to α_v modulo the maximal ideal of $\overline{\mathbb{Z}}_p$.
- If $v = v_0$, then $(\pi')_{v_0}^{U_1^1(v_0)} \neq 0$
- If $v \notin S_p \cup R \cup Q \cup \{v_0\}$ is a finite place of F, then π'_v is unramified.

Essentially, we have increased the set of ramification for our automorphic representation but have left the residual representation unchanged.

3.2.6 Level-Lowering

As in the previous section, fix a finite set R of finite places of F with $R \cap (S_p \cup \{v_0\}) = \emptyset$ and $\#R$ even. Let $U = \prod_w U_w \in \mathcal{J}_R$ be a good subgroup. If Q is a finite set of finite places of F, disjoint from $S_p \cup R \cup \{v_0\}$, with $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$ for all $v \in Q$, then define $U_Q = \prod_v U_{Q,v} \in \mathcal{J}_{R \cup Q}$ as follows:

- If $v \notin Q$, then $U_{Q,v} = U_v$.
- If $v \in Q$, then $U_{Q,v} \subset G_{R \cup Q}(F_v)$ is the unique maximal compact subgroup.

Let S be a finite set of finite places of F with $S_p \subset S$, and such that $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$ for $v \notin S$. Let $\mathfrak{m} \subset \mathbb{T}^{S,\mathrm{univ}}$ be a non-Eisenstein maximal ideal with $\mathfrak{m} \in \mathrm{Supp}(H_R(U))$.

We now state a theorem and subsequent corollary from [41]. Essentially, the idea is to model Khare's method in [22].

Theorem 3.2.12. [41, Theorem 4.14] Fix an integer $N \geq 1$, and let $\rho : G_F \to \mathrm{GL}_2(\mathcal{O}/\lambda^N)$ be a continuous representation lifting $\bar{\rho}_{\mathfrak{m}}$. Assume that:

(1) The representation ρ is unramified outside S.

(2) There exists a set Q (as above) with $\#Q$ even, and a homomorphism

$$f : \mathbb{T}_Q^{S\cup Q}(H_{R\cup Q}(U_Q)) \to \mathcal{O}/\lambda^N$$

such that:

- For each $v \in Q$, the size of the residue field satisfies $q_v \not\equiv 1 \bmod p$.
- For each finite $v \notin S \cup Q$ of F, we have $f(T_v) = \mathrm{tr}\,\rho(\mathrm{Frob}_v)$.
- If $I = \ker f$, then $(H_{R\cup Q}(U_Q) \otimes_{\mathcal{O}} \mathcal{O}/\lambda^N)[I]$ contains a submodule isomorphic to $\mathcal{O}/\lambda^N$.

Then there exists a homomorphism $f' : \mathbb{T}^{S\cup Q}(H_R(U)) \to \mathcal{O}/\lambda^N$ such that for all $v \notin S \cup Q$, we have $f(T_v) = \mathrm{tr}\,\rho(\mathrm{Frob}_v)$.

Corollary 3.2.13. [41, Corollary 4.15] Let $\rho : G_F \to \mathrm{GL}_2(\mathcal{O})$ be a continuous lift of $\bar{\rho}_{\mathfrak{m}}$ unramified outside S. Suppose that for each $N \geq 1$, there exists a set Q (depending on N) as in the previous theorem and a homomorphism $f : \mathbb{T}_Q^{S\cup Q}(H_{R\cup Q}(U)) \to \mathcal{O}/\lambda^N$ satisfying:

- For each $v \in Q$, the size of the residue field satisfies $q_v \not\equiv 1 \bmod p$.
- For each finite $v \notin S \cup Q$ of F, we have $f(T_v) = \mathrm{tr}\,\rho(\mathrm{Frob}_v)$.
- If $I = \ker f$, then $(H_{R\cup Q}(U_Q) \otimes_{\mathcal{O}} \mathcal{O}/\lambda^N)[I]$ contains a submodule isomorphic to $\mathcal{O}/\lambda^N$.

Then ρ is automorphic. That is, there exists a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight two and an isomorphism $\rho \otimes_{\mathcal{O}} \overline{\mathbb{Q}}_p \cong r_\iota(\pi)$.

3.3 Ordinary Galois Representations

In this section, we will state a series of lemmas which will be necessary in later arguments. The material comes from [41, Section 5.1]. For this section, let p be odd and $L/\mathbb{Q}_p$ a finite extension. Let $\rho : G_L \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be a representation such that:

- ρ is de Rham, and
- for each $\tau : L \hookrightarrow \overline{\mathbb{Q}}_p$, we have $\mathrm{HT}_\tau(\rho) = \{0, 1\}$.

Definition 3.3.1. The representation ρ is *ordinary* if it is conjugate to a representation of the form

$$\rho \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \epsilon^{-1} \end{pmatrix},$$

where $\psi_1, \psi_2 : G_L \to \overline{\mathbb{Q}}_p^\times$ are continuous characters such that $\psi_i|_{I_L}$ has finite order. If ρ is not ordinary, we say it is non-ordinary.

Recall from item (5) of Theorem 2.1.27 that, as ρ is de Rham, there is an associated Weil-Deligne representation $\mathrm{WD}(\rho)$. The first lemma we state describes how the condition of being ordinary is detected by the Weil-Deligne representation.

Lemma 3.3.2. [41, Lemma 5.1] Let ρ be as above. Then one of the following must be true:

(1) The Frobenius semi-simplification $\mathrm{WD}(\rho)^{F-ss}$ is irreducible, in which case ρ is non-ordinary.

(2) We have $\mathrm{WD}(\rho)^{F-ss}$ is indecomposable, in which case ρ is ordinary.

(3) The representation $\mathrm{WD}(\rho)^{F-ss}$ is decomposable, and is the direct sum of two smooth characters $\chi_i : W_L \to \overline{\mathbb{Q}}_p^\times$, i.e. $\mathrm{WD}(\rho)^{F-ss} = \chi_1 \oplus \chi_2$. If $\mathrm{Frob}_L \in W_L$ denotes a geometric Frobenius element, assume that $\mathrm{val}_p(\chi_1(\mathrm{Frob}_L)) \leq \mathrm{val}_p(\chi_2(\mathrm{Frob}_L))$. Then

$$\mathrm{val}_p(\chi_1(\mathrm{Frob}_L)) + \mathrm{val}_p(\chi_2(\mathrm{Frob}_L)) \leq [L_0 : \mathbb{Q}_p],$$

where L_0 is the maximal absolutely unramified subfield of L. The representation ρ is ordinary if and only if equality holds.

Let F be a totally real field, and let $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$ be a fixed isomorphism. Let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 (in the sense of Chapter 2).

If $v \in S_p$, recall the definition of being ι-ordinary (see Definition 3.2.6). This next lemma describes when the component π_v is ι-ordinary. We will then see how π_v being ι-ordinary relates to $r_\iota(\pi)$ being ordinary at places above p.

Lemma 3.3.3. Let π be as above, and let $v \in S_p$. Then exactly one of the following must be true:

(1) The local component π_v is supercuspidal. In this case, π_v is not ι-ordinary.

(2) There is a character $\chi : F_v^\times \to \overline{\mathbb{Q}}_p^\times$ of finite order and an isomorphism $\pi_v \cong \mathrm{St}_2(\iota\chi)$ (recall the definition of $\mathrm{St}_2(\iota\chi)$ from the remarks preceding Definition 2.4.7). In this case, π_v is ι-ordinary.

(3) There exist characters $\chi_1, \chi_2 : F_v^\times \to \overline{\mathbb{Q}}_p^\times$ with open kernel and an isomorphism $\pi_v \cong i_B^{\mathrm{GL}_2} \iota\chi_1 \otimes \iota\chi_2$. Suppose the χ_i are labelled so that $\mathrm{val}_p(\chi_1(\varpi_v)) \leq \mathrm{val}_p(\chi_2(\varpi_v))$. Then $-\mathrm{val}_p(q_v)/2 \leq \mathrm{val}_p(\chi_1(\varpi_v))$, and π_v is ι-ordinary if and only if equality holds.

In some sense, the previous two lemmas seem to be mirroring one another. One should believe, then, that there is some relationship between an automorphic representation being ι-ordinary at a local component and the associated Galois representation being ordinary. The next lemma shows this is the case.

Lemma 3.3.4. [41, Lemma 5.3] Let π be as above, and let $v \in S_p$.

(1) The representation $r_\iota(\pi)|_{G_{F_v}}$ is ordinary if and only if π_v is ι-ordinary.

(2) If π_v is supercuspidal and if L/F_v is a finite extension such that $\mathrm{rec}_{F_v}^T(\pi_v)|_{W_L}$ is unramified, then $r_\iota(\pi)|_{G_L}$ is crystalline and non-ordinary.

Ultimately, we are going to want to consider automorphic representations whose local components are ι-ordinary at some places above p and supercuspidal at others. The next (and last) lemma of this section shows that if we have a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, then we can find another with the above property whose associated residual Galois representation is isomorphic to the original's.

Lemma 3.3.5. [41, Theorem 5.4] Assume $[F : \mathbb{Q}]$ is even, and let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2. Suppose that, for each finite place $v \notin S_p$ of F, either π_v is unramified or $q_v \equiv 1 \bmod p$ and π_v is an unramified twist of the Steinberg representation. Suppose further that if $v \in S_p$, then π_v is ι-ordinary and $\pi_v^{U_0(v)} \neq 0$. Lastly, suppose $\overline{r_\iota(\pi)}$ is irreducible and $[F(\zeta_p) : F] \geq 4$. Let $\sigma \subset S_p$ be any subset (possibly empty). Then there exists a cuspidal automorphic representation π' of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 such that:

(1) There is an isomorphism of residual representations $\overline{r_\iota(\pi)} \cong \overline{r_\iota(\pi')}$.

(2) The representations π and π' have the same central character.

(3) If $v \in \sigma$, then π'_v is ι-ordinary. If $v \in S_p - \sigma$, then π'_v is supercuspidal.

(4) If $v \nmid p\infty$ is a place of F and v is unramified, then π'_v is unramified. If π_v is ramified, the π'_v is a ramified principal series representation.

3.4 Killing Dual Selmer

We now move to the crux of our work, which is finding auxiliary primes that do the job of killing the mod p dual Selmer group. There is some care needed when doing so, because we need to make sure these places fit into our general strategy of automorphy lifting (recall this will be a blend of the Taylor-Wiles primes and Khare's method). We will first describe the local deformation problems used, and then move to the process of choosing the auxiliary primes. Along the way we will make note of which arguments are from [41] and which are new.

3.4.1 Notation

The theory for this chapter has been developed in Chapter 2, specifically Section 2.3. However, we will remind the reader of the notation now. This notation will apply to the rest of Section 3.4. Let p be an odd prime, and let $\mathcal{O}$ be the integer ring of a finite extension L of

$\mathbb{Q}_p$. We let $\mathfrak{m} \subset \mathcal{O}$ be the maximal ideal, and $k = \mathcal{O}/\mathfrak{m}$ the residue field.

Let F be a totally real number field, and suppose $\bar{\rho} : G_F \to \mathrm{GL}_2(k)$ is an absolutely irreducible, continuous representation. Let $\mu : G_F \to \mathcal{O}^\times$ be a continuous character lifting $\det \bar{\rho}$. Assume k contains the eigenvalues of all elements in $\bar{\rho}(G_F)$. Let S be a finite set of finite places of F, with S containing S_p and the places at which $\bar{\rho}$ and μ are ramified. For each place $v \in S$, fix a ring $\Lambda_v \in \mathrm{CNL}_{\mathcal{O}}$, and define $\Lambda = \widehat{\bigotimes}_{v \in S} \Lambda_v$, the tensor product being over $\mathcal{O}$. As in Section 2.3.6, the ring $\Lambda \in \mathrm{CNL}_{\mathcal{O}}$.

Lastly, if $v \in S$, then $R_v^\square \in \mathrm{CNL}_{\Lambda_v}$ will be the representing object for the functor $\mathcal{D}_v^\square : \mathrm{CNL}_{\Lambda_v} \to \mathrm{Sets}$ which takes R to the set of lifts of $\bar{\rho}|_{G_{F_v}}$ to R such that the determinant agrees with the composite $G_{F_v} \to \mathcal{O}^\times \to R^\times$.

We refer the reader to Sections 2.3.5 and 2.3.6 for the definitions of local and global deformation problems.

3.4.2 Local Deformation Problems

We are going to be defining four different local deformation problems. For the first three, we define the local deformation problem by defining the representing ring.

3.4.2.1 Ordinary Deformations

Assume $v \in S_p$ and $\bar{\rho}|_{G_{F_v}}$ is trivial. Assume L contains the image of all embeddings $F_v \hookrightarrow \overline{\mathbb{Q}}_p^\times$. If G is a profinite group, let $G(p)$ denote the maximal pro-p subgroup of G.

Set $\Lambda_v = \mathcal{O}[\![\mathcal{O}_{F_v}^\times(p)]\!]$. Write $\eta_{\mathrm{univ}} : \mathcal{O}_{F_v}^\times \to \Lambda^\times$ for the universal character. Let $I_{F_v}^{\mathrm{ab}}$ denote the inertia subgroup of the Galois group of the maximal abelian extension of F_v. The local Artin map Art_{F_v} gives an isomorphism $\mathcal{O}_{F_v}^\times(p) \cong I_{F_v}^{\mathrm{ab}}(p)$.

Definition 3.4.1. The *ordinary deformation ring* R_v^{ord} is defined as follows: let $x : R_v^\square \to \overline{\mathbb{Q}}_p$ be a homomorphism. The map x factors through R_v^{ord} if and only if $x \circ \rho_v^\square$ is $\mathrm{GL}_2(\overline{\mathbb{Z}}_p)$-

conjugate to a representation

$$x \circ \rho_v^\square \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix},$$

where $\psi_1|_{I_{F_v}^{\mathrm{ab}}(p)} = x \circ \eta^{\mathrm{univ}} \circ \mathrm{Art}_{F_v}^{-1}$.

Remark 3.4.2. This ring exists, and defines a local deformation problem. See, for example, [41, Proposition 5.13].

Let $\mathcal{D}_v^{\mathrm{ord}}$ be the local deformation problem with representing object R_v^{ord}.

3.4.2.2 Crystalline non-ordinary deformations

Again assume that $v \in S_p$ and $\bar{\rho}|_{G_{F_v}}$ is trivial. For this problem, let $\Lambda_v = \mathcal{O}$.

Proposition 3.4.3. [41, Proposition 5.14] There is a reduced $\mathcal{O}$-torsion free quotient $R_v^{\text{non-ord}}$ of $R_v^\square$ satisfying the following property: If E/L is a finite extension and $x : R_v^\square \to L$ is a homomorphism, then x factors through $R_v^{\text{non-ord}}$ if and only if $x \circ \rho_v^\square$ is crystalline of Hodge-Tate weights $\mathrm{HT}_\tau(x \circ \rho_v^\square) = \{0, 1\}$ and is non-ordinary.

If $R_v^{\text{non-ord}} \neq 0$, then R_v defines a local deformation problem whose corresponding subfunctor of $\mathcal{D}_v^\square$ we denote by $\mathcal{D}_v^{\text{non-ord}}$.

3.4.2.3 Steinberg Deformations when $q_v \equiv 1 \bmod p$

Suppose $v \in S \backslash S_p$, and assume $q_v \equiv 1 \bmod p$ and $\bar{\rho}|_{G_{F_v}}$ is trivial. As with the non-ordinary deformations, for this deformation problem we will have $\Lambda_v = \mathcal{O}$.

Proposition 3.4.4. [41, Proposition 5.15] There is a reduced $\mathcal{O}$-torsion free quotient R_v^{St} of $R_v^\square$ satisfying the following property: If E/L is a finite extension and $x : R_v^\square \to L$ is a homomorphism, then x factors through R_v^{St} if and only if $x \circ \rho_v^\square$ is $\mathrm{GL}_2(\mathcal{O}_E)$-conjugate to a representation of the form

$$x \circ \rho_v^\square \sim \begin{pmatrix} \chi & * \\ 0 & \chi\epsilon^{-1} \end{pmatrix},$$

where $\chi : G_{F_v} \to E^\times$ is an unramified character.

As with the previous cases, this ring R_v^{St} defines a local deformation problem which we denote by $\mathcal{D}_v^{\mathrm{St}}$.

3.4.2.4 Special Deformations when $q_v \not\equiv 1 \bmod p$

This deformation problem was originally defined in [41]. For reasons discussed later, Thorne imposed the stricter restriction that $q_v \equiv -1 \bmod p$. We remove this assumption, asking only that $q_v \not\equiv 1 \bmod p$.

Let $v \in S$ be a prime not dividing p, and suppose that $q_v \not\equiv 1 \bmod p$. Suppose further that $\bar{\rho}|_{G_{F_v}}$ is unramified, and that $\bar{\rho}(\mathrm{Frob}_v)$ has two distinct eigenvalues $\alpha_v, \beta_v \in k$ such that $\beta_v/\alpha_v = q_v$. Let $\Lambda_v = \mathcal{O}$. We define a subfunctor $\mathcal{D}_v^{\mathrm{St}(\alpha_v)} \subset \mathcal{D}_v^{\square}$ directly. Let $R \in \mathrm{CNL}_{\mathcal{O}}$ and let $r : G_{F_v} \to \mathrm{GL}_2(R)$ be an element of $\mathcal{D}_v^{\square}(R)$. If $\phi_v \in G_{F_v}$ is a choice of geometric Frobenius, then by Hensel's lemma the characteristic polynomial of $r(\phi_v)$ factors as $(X - A_v)(X - B_v)$, where $A_v, B_v \in R^{\times}$ with A_v lifting α_v and B_v lifting β_v. We will say $r \in \mathcal{D}_v^{\mathrm{St}(\alpha_v)}(R)$ if $B_v = q_v A_v$ and I_{F_v} acts trivially on $(r(\phi_v) - B_v)R^2$, which is a direct summand R-submodule of R^2. One checks that this condition is independent of the choice of ϕ_v.

Proposition 3.4.5. The functor $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is a local deformation problem. The representing object $R_v^{\mathrm{St}(\alpha_v)}$ is formally smooth over $\mathcal{O}$ of (absolute) dimension 4.

Proof. That $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is a local deformation problem is easy. Let $R_v^{\mathrm{St}(\alpha_v)}$ denote the representing object. To see that the dimension of $R_v^{\mathrm{St}(\alpha_v)}$ is 4, consider the unframed deformations of this type and its representing object S_v. Then S_v is smooth of relative dimension 1 over $\mathcal{O}$. There is a map $S_v \to R_v^{\mathrm{St}(\alpha_v)}$ which is formally smooth, and $R_v^{\mathrm{St}(\alpha_v)}$ is a power series ring over S_v in

$$\dim_k \mathrm{ad}\,\bar{\rho} - \dim_k H^0(F_v, \mathrm{ad}\,\bar{\rho}) = 4 - 2 = 2$$

variables. Thus $R_v^{\mathrm{St}(\alpha_v)}$ has relative dimension 3 over $\mathcal{O}$, as desired. □

3.4.3 Existence of Auxiliary Primes

Continue with the notation from the previous section, and assume further that $\bar{\rho}$ is totally odd, i.e. that $\mu(c) = -1$ for all choices of complex conjugation $c \in G_F$. Write $\zeta_p \in \overline{F}$ for a primitive p-th root of unity, and now fix a choice of complex conjugation $c \in G_F$.

Assume that $\bar{\rho}|_{G_{F(\zeta_p)}}$ is the direct sum of two distinct characters (so that the Taylor-Wiles hypothesis does not hold). By Clifford theory, the representation $\bar{\rho}$ is induced from a continuous character $\bar{\chi} : G_K \to k^\times$, where K is the unique quadratic subfield of $F(\zeta_p)/F$. That is, $\bar{\rho} \cong \operatorname{Ind}_{G_K}^{G_F} \bar{\chi}$. Write $w \in G_F$ for a fixed choice of element with nontrivial image in $\operatorname{Gal}(K/F)$. Consider the twisted character $\bar{\chi}^w : G_K \to k^\times$, which is defined by $\bar{\chi}^w(g) = \bar{\chi}(w^{-1}gw)$. We can assume that, possibly after conjugation, that $\bar{\rho}$ has the form:

$$\bar{\rho}(\sigma) = \begin{pmatrix} \bar{\chi}(\sigma) & 0 \\ 0 & \bar{\chi}^w(\sigma) \end{pmatrix}, \qquad \text{for } \sigma \in G_K,$$

$$\bar{\rho}(w) = \begin{pmatrix} 0 & \bar{\chi}(w^2) \\ 1 & 0 \end{pmatrix}.$$

Now let $\bar{\gamma} = \bar{\chi}/\bar{\chi}^w$. By assumption, as $\bar{\rho}|_{G_{F(\zeta_p)}}$ is the direct sum of two distinct characters, the character $\bar{\gamma}$ is nontrivial, even after restriction to $G_{F(\zeta_p)}$.

Lemma 3.4.6. The adjoint representation $\operatorname{ad}^0 \bar{\rho}$ decomposes as $\operatorname{ad}^0 \bar{\rho} \cong k(\delta_{K/F}) \oplus \operatorname{Ind}_{G_K}^{G_F} \bar{\gamma}$ as a G_F-module, where $\delta_{K/F} : \operatorname{Gal}(K/F) \to k^\times$ is the unique nontrivial character.

Proof. As a G_K-representation, the representation $\operatorname{ad}^0 \bar{\rho}$ decomposes as $k \oplus k(\bar{\gamma}) \oplus k(\bar{\gamma}^{-1})$. Therefore, by Frobenius reciprocity and Clifford theory, the representation $\operatorname{Ind}_{G_K}^{G_F} \bar{\gamma}$ is an irreducible subrepresentation of $\operatorname{ad}^0 \bar{\rho}$ as a G_F-module. The $k(\delta_{K/F})$ term comes from considering the G_F action on the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \operatorname{ad}^0 \bar{\rho}$. □

From now on, we will let $M_0 = k(\delta_{K/F})$ and $M_1 = \operatorname{Ind}_{G_K}^{G_F} \bar{\gamma}$. Fix the standard basis for $\operatorname{ad}^0 \bar{\rho}$:

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

If $M \in \operatorname{ad}^0 \bar{\rho}$, we write $k_M \subset \operatorname{ad}^0 \bar{\rho}$ for the line that it spans.

We have the following easy lemma:

Lemma 3.4.7. Let $v \nmid p$ be a finite place of F which splits in K, and suppose that the local deformation problem $\mathcal{D}_v = \mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined.

(1) The subspace $\mathcal{L}_v \subset H^1(F_v, \operatorname{ad}^0 \bar{\rho})$ respects the decomposition $\operatorname{ad}^0 \bar{\rho} = M_0 \oplus M_1$. That is,

$$\mathcal{L}_v = (\mathcal{L}_v \cap H^1(F_v, M_0)) \oplus (\mathcal{L}_v \cap H^1(F_v, M_1)).$$

(2) The subspace $\mathcal{L}_v^\perp \subset H^1(F_v, \operatorname{ad}^0 \bar{\rho}(1))$ respects the decomposition $\operatorname{ad}^0 \bar{\rho}(1) = M_0(1) \oplus M_1(1)$.

Proof. The second part is dual to the first, so we only prove the first part. The fact that $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined means $q_v \not\equiv 1 \bmod p$, that $\bar{\rho}|_{G_{F_v}}$ is unramified, and that $\bar{\rho}(\mathrm{Frob}_v)$ takes two distinct eigenvalues $\alpha_v, \beta_v \in k$ with $\beta_v/\alpha_v = q_v$. The fact that v splits in K means $M_0 = k_H$ and $M_1 = k_E(1) \oplus k_F(-1)$ as $k[G_{F_v}]$-modules. The case $q_v \equiv -1 \bmod p$ was proved in [41]. Namely, if $q_v \equiv -1 \bmod p$, then $M_1 = k_E(1) \oplus k_F(1)$ as $k[G_{F_v}]$-modules, as $\bar{\epsilon} = \bar{\epsilon}^{-1}$ in this case. The subspace $\mathcal{L}_v \subset H^1(G_{F_v}, \operatorname{ad}^0 \bar{\rho})$ is one-dimensional, and lies in $H^1(G_{F_v}, M_1)$, being spanned by either $H^1(G_{F_v}, k_E(1))$ or $H^1(G_{F_v}, k_F(1))$. If $q_v \not\equiv \pm 1 \bmod p$, then $\mathcal{L}_v$ is 1-dimensional, and is contained in $H^1(G_{F_v}, M_1)$, being spanned by $H^1(G_{F_v}, k_E(1))$. □

Remark 3.4.8. The difference between this lemma and the corresponding Lemma 5.18 from [41] is that we do not make the assumption that the inducing field K is totally real. However, we do need to make sure that we choose primes of F which split in K for the rest of the method to work. In *loc. cit.*, the assumption that K be totally real coupled with the assumption that $q_v \equiv -1 \bmod p$ guaranteed the place v split in K.

Let $\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v \in S}, \{\mathcal{D}_v\}_{v \in S})$ be a global deformation problem, and let $T \subset S$ be a subset containing S_p (the set of places above p). Suppose that for $v \in S - T$, the local deformation problem $\mathcal{D}_v = \mathcal{D}_v^{\mathrm{St}(\alpha_v)}$. For ease of notation, for the global cohomology groups, write

$$H^1_{\mathcal{S},T}(M) := H^1_{\mathcal{S},T}(G_{F,S}, M),$$

which makes sense because the set S is encoded in $\mathcal{S}$. The lemma implies we can decompose

$$H^1_{\mathcal{S},T}(\mathrm{ad}^0\,\bar{\rho}(1)) = H^1_{\mathcal{S},T}(M_0(1)) \oplus H^1_{\mathcal{S},T}(M_1(1)).$$

We now show that we can kill the $M_1(1)$ portion of dual Selmer using the special deformation problem we defined in the previous section, and then kill the $M_0(1)$ portion using traditional Taylor-Wiles primes.

3.4.3.1 Killing the $M_1(1)$ portion

First, we show that lemmas 5.21, 5.22, and 5.23 of [41] continue to hold even if K is not totally real. Indeed, the only one which requires proof is the second, since this is the only place where Thorne used this assumption. However, we will need to impose an additional restriction. We state the other two lemmas here for convenience.

Lemma 3.4.9. Let Γ be a group, and $\alpha : \Gamma \to k^\times$ a character. Let $k' \subset k$ be the subfield generated by the values of α. Then $k'(\alpha)$ is a simple $\mathbb{F}_p[\Gamma]$-module. If $\beta : \Gamma \to k^\times$ is another character, then $k'(\alpha)$ is isomorphic to a $\mathbb{F}_p[\Gamma]$-submodule of $k(\beta)$ if and only if there is an automorphism τ of k such that $\beta = \tau \circ \alpha$.

Proof. See the proof of [41, Lemma 5.21]. □

Lemma 3.4.10. Let $K(\overline{\gamma})$ be the fixed field of $\ker\bar{\gamma}$, let $L = F(\zeta_p) \cap K(\overline{\gamma})$ and assume that $\#\bar{\epsilon}(G_L) > 1$. Then the $\mathbb{F}_p[G_K]$-module $k(\overline{\epsilon\gamma})$ has no Jordan-Holder factors in common with k, $k(\overline{\gamma})$, or $k(\overline{\gamma}^{-1})$. The characters $\overline{\epsilon\gamma}$ and $\overline{\gamma}$ are nontrivial.

Proof. The second claim follows from the fact that $\overline{\gamma}|_{G_{F(\zeta_p)}}$ is nontrivial. For the first claim, we show there are no $\mathbb{F}_p[G_K]$-module homomorphisms from $k(\overline{\epsilon\gamma})$ to $k(\overline{\gamma})$ or $k(\overline{\gamma}^{-1})$. Let $f : k(\overline{\epsilon\gamma}) \to k(\overline{\gamma})$ be such a homomorphism, choose $a \in k(\overline{\epsilon\gamma})$, and assume $f(a) = b$. By the hypothesis of the lemma, there is an element $\tau \in G_L \subset G_K$ such that $\bar{\epsilon}(\tau) \neq 1$ and $\bar{\gamma}(\tau) = 1$. Since f is a $\mathbb{F}_p[G_K]$-module homomorphism and $\bar{\epsilon}(\tau) \in \mathbb{F}_p^\times$, we know

$$f(\bar{\epsilon}(\tau)\overline{\gamma}(\tau)a) = \bar{\epsilon}(\tau)f(a).$$

On the other hand,

$$f(\bar{\epsilon}(\tau)\overline{\gamma}(\tau)a) = \overline{\gamma}(\tau)b = b.$$

Thus, $\bar{\epsilon}(\tau)b = b$, which implies $b = 0$. Since $a \in k(\overline{\epsilon\gamma})$ was arbitrary, this implies $f = 0$. Thus, there are no nontrivial homomorphisms between $k(\overline{\epsilon\gamma})$ and $k(\overline{\gamma})$.

The same proof shows there are no nontrivial homomorphisms between $k(\overline{\epsilon\gamma})$ and $k(\overline{\gamma}^{-1})$ or k. □

Lemma 3.4.11. Let $N \geq 1$ and let $K_N = F(\zeta_{p^N}, \rho_N)$, i.e. K_N is the splitting field of $\rho_N|_{F(\zeta_{p^N})}$. Then $H^1(K_N/F, M_1(1)) = 0$.

Proof. When K is totally real, this is proved in Lemma 5.23 of [41]. The same proof proves the lemma in the case K is CM using the preceding lemma. □

The following proposition is the analog of [41, Proposition 5.20] and is the only place where we argue differently from Thorne because of not having (in the case that K is not totally real) the luxury to choose places v such that $\rho_N(\mathrm{Frob}_v)$ is the image of complex conjugation under ρ_N. This convenient choice is part of the reason Thorne imposed the restriction $q_v \equiv -1 \bmod p$.

The proof relies on the simple observation that given an element g in $\mathrm{GL}_2(\mathcal{O}/p^M)$, then for $N >> 0$, the element g^{q^N} has a ratio of eigenvalues that are the Teichmüller lift of the ratio of eigenvalues of the reduction of g.

Proposition 3.4.12. Let $\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S})$ be a global deformation problem, and let $T = S$. Let $N_0 \geq 1$ be an integer. Let $\rho : G_F \to \mathrm{GL}_2(\mathcal{O})$ be a lifting of type $\mathcal{S}$. Let $K(\overline{\gamma}\bar{\epsilon})$ (resp. $K(\overline{\gamma}\bar{\epsilon}^{-1})$) be the fixed field of $\ker \overline{\gamma}\bar{\epsilon}$ (resp. $\ker \overline{\gamma}\bar{\epsilon}^{-1}$), and assume that $F(\zeta_p) \not\subset K(\overline{\gamma}\bar{\epsilon}) \cap K(\overline{\gamma}\bar{\epsilon}^{-1})$. Then for any $m \geq h^1_{\mathcal{S},T}(G_{F,S}, M_1(1))$, there exists a set Q_0 of primes, disjoint from S, and elements $\alpha_v \in k^\times$, satisfying the following:

(1) The size $\#Q_0 = m$.

(2) For each $v \in Q_0$, the local deformation problem $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined. We define the augmented deformation problem

$$\mathcal{S}_{Q_0} = (\bar{\rho}, \mu, S \cup Q_0, \{\Lambda_v\}_{v \in S} \cup \{\mathcal{O}\}_{v \in Q_0}, \{\mathcal{D}_v\}_{v \in S} \cup \{\mathcal{D}_v^{\mathrm{St}(\alpha_v)}\}_{v \in Q_0}).$$

(3) Let $\rho_{N_0} = \rho \bmod \lambda^{N_0} : G_F \to \mathrm{GL}_2(\mathcal{O}/\lambda^{N_0}\mathcal{O})$. Then $\rho_{N_0}(\mathrm{Frob}_v)$ has distinct eigenvalues whose ratio is q_v for each $v \in Q_0$.

(4) $H^1_{\mathcal{S}_{Q_0},T}(M_1(1)) = 0$.

Proof. We wish to find a set Q_0 of primes such that $h^1_{\mathcal{S}_{Q_0},T}(M_1(1)) = 0$. Suppose $r = h^1_{\mathcal{S},T}(G_{F,S}, M_1(1)) \geq 0$. Using induction, it suffices to find a single prime v satisfying the conditions of the theorem such that $h^1_{\mathcal{S}_{\{v\}},T}(M_1(1)) = \max(r-1, 0)$. The case $r = 0$ is easy, so assume $r \geq 1$.

Let $0 \neq [\varphi] \in H^1_{\mathcal{S},T}(M_1(1))$ be a nonzero class. We wish to find a place $v \notin S$ such that:

(i) v splits in K

(ii) $\rho_{N_0}(\mathrm{Frob}_v)$ has distinct eigenvalues with ratio $q_v \bmod \lambda^{N_0}$.

(iii) $q_v \not\equiv 1 \bmod \lambda^{N_0}$

(iv) $\varphi(\mathrm{Frob}_v) \neq 0$ $(\in M_1(1))$.

Indeed, the first three conditions imply that $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined for the appropriate choice of α_v. We also have an exact sequence

$$0 \to H^1_{\mathcal{S}_{\{v\}},T}(G_{F,S\cup\{v\}}, M_1(1)) \to H^1_{\mathcal{S},T}(G_{F,S}, M_1(1)) \to k.$$

If $q_v \not\equiv \pm 1 \bmod \lambda$, then the last map in the sequence comes from the restriction map $H^1_{\mathcal{S},T}(M_1(1)) \to H^1(G_{F_v}, M_1(1)) \cong k$. If $q_v \equiv -1 \bmod \lambda$, then this last map is either $\phi \mapsto \langle E, \phi(\mathrm{Frob}_v)\rangle$ (if $\alpha_v = 1$) or $\phi \mapsto \langle F, \phi(\mathrm{Frob}_v)\rangle$ (if $\alpha_v = -1$). By choosing α_v appropriately, we can ensure the sequence is exact on the right. Condition (iv) implies the final map is surjective, which gives $h^1_{\mathcal{S}_{\{v\}},T}(G_{F,S\cup\{v\}}, M_1(1)) < h^1_{\mathcal{S},T}(G_{F,S}, M_1(1))$, as desired.

By the Cebotarev density theorem, it suffices to find an element $\sigma \in G_K$ such that:

(a) $\rho_{N_0}(\sigma)$ has distinct eigenvalues with ratio $\epsilon(\sigma) \bmod \lambda^{N_0}$.

(b) $\epsilon(\sigma) \not\equiv 1 \bmod \lambda^{N_0}$

(c) $\varphi(\sigma) \neq 0$.

If $N_0 = 1$, then the assumption in the Proposition ensures we can find σ_1 in G_K such that $\overline{\gamma}(\sigma_1) = \epsilon(\sigma_1) \bmod \lambda$. Indeed, the assumption $F(\zeta_p) \not\subset K(\overline{\gamma}\overline{\epsilon}) \cap K(\overline{\gamma}\overline{\epsilon}^{-1})$ ensures that either $G_{K(\overline{\gamma}\overline{\epsilon})}$ or $G_{K(\overline{\gamma}\overline{\epsilon}^{-1})}$ is not contained in $G_{F(\zeta_p)}$. This means there exists σ_1 in either $G_{K(\overline{\gamma}\overline{\epsilon})}$ or $G_{K(\overline{\gamma}\overline{\epsilon}^{-1})}$ such that $\epsilon(\sigma_1) \not\equiv 1 \bmod p$. In the latter case, we find our desired σ_1. In the former case, by exchanging the roles of the eigenvalues, we get our desired σ_1.

If $\varphi(\sigma_1) \neq 0$, then take $\sigma = \sigma_1$, so suppose $\varphi(\sigma_1) = 0$. We have the inflation-restriction sequence:

$$0 \to H^1(K_1/F, M_1(1)^{G_{K_1}}) \to H^1(F, M_1(1)) \to H^1(K_1, M_1(1))^{\mathrm{Gal}(K_1/F)}.$$

By the previous lemma, the first group is zero, so the image of φ in $H^1(K_1, M_1(1))$ is nonzero. This restriction is a nonzero homomorphism $\varphi|_{G_{K_1}} : G_{K_1} \to M_1(1)$. Thus, we can find $\tau \in G_{K_1}$ such that $\varphi(\tau) \neq 0$. Then take $\sigma = \tau\sigma_1$. Then

$$\overline{\rho}(\sigma) = \overline{\rho}(\tau)\overline{\rho}(\sigma_1) = \overline{\rho}(\sigma_1)$$

as $\tau \in \ker(\overline{\rho})$. We also find

$$\epsilon(\sigma) = \epsilon(\tau)\epsilon(\sigma_1) \equiv \epsilon(\sigma_1) \bmod \lambda$$

as $\epsilon(\tau) \equiv 1 \bmod \lambda$. Thus, $\overline{\gamma}(\sigma) \equiv \epsilon(\sigma) \bmod \lambda$. Moreover,

$$\varphi(\sigma) = \varphi(\tau) + \varphi(\sigma_1),$$

meaning $\varphi(\sigma) \neq 0$, as required.

If $N_0 > 1$, then consider the element σ_1 defined above. Then $\rho_{N_0}(\sigma_1)$ has distinct eigenvalues by Hensel's lemma, and we know this ratio modulo λ is $\overline{\gamma}(\sigma_1) \equiv \epsilon(\sigma_1) \bmod \lambda$. Consider $\sigma_{N_0} = \sigma_1^{q^M}$ for some M to be determined and $q = \#k$. For some sufficiently high power of M, $\epsilon(\sigma_{N_0}) \bmod \lambda^{N_0}$ will be the Teichmuller lifting of $\epsilon(\sigma_1) \bmod \lambda$ to the $\bmod \lambda^{N_0}$ ring (indeed, $M = q^{N_0 - 1}$ should do). But since $\overline{\gamma}(\sigma_1) \equiv \epsilon(\sigma_1) \bmod \lambda$, we deduce that the ratio of the eigenvalues of $\rho_{N_0}(\sigma_{N_0})$ will be equivalent to $\epsilon(\sigma_{N_0}) \bmod \lambda^{N_0}$.

We still need to make sure $\varphi(\sigma) \neq 0$. If $\varphi(\sigma_{N_0}) \neq 0$, then we can take $\sigma = \sigma_{N_0}$. If $\varphi(\sigma_{N_0}) = 0$, consider $\tau \in G_{K_N}$ with $\varphi(\tau) \neq 0$ as before. Let $\sigma = \tau\sigma_{N_0}$. By the same reasoning as in the $N_0 = 1$ case, the ratio of the eigenvalue of $\rho_N(\sigma)$ will still be equivalent to $\epsilon(\sigma) \bmod \lambda^{N_0}$, and moreover $\varphi(\sigma) = \varphi(\tau) + \varphi(\sigma_{N_0}) \neq 0$ by construction. This concludes the proof. □

Remark 3.4.13. (1) Crucial to the proof was the idea that while the subspace $\mathcal{L}_v^{\perp}$ is not contained in the unramified cohomology group $H^1_{\mathrm{ur}}(G_{F_v}, \mathrm{ad}^0 \bar{\rho}(1))$, the subspace $\mathcal{L}_v^{\perp} \cap H^1(G_{F_v}, M_1(1))$ is contained in the unramified cohomology group $H^1_{\mathrm{ur}}(G_{F_v}, M_1(1)) = H^1_{\mathrm{ur}}(G_{F_v}, \mathrm{ad}^0 \bar{\rho}(1))$. In some sense, while the cohomology class is not unramified, the ramification is simply being pushed to the $M_0(1)$-portion of dual Selmer. This will be handled by the Taylor-Wiles primes next.

(2) Note that the assumption $F(\zeta_p) \not\subset K(\overline{\gamma}\bar{\epsilon}) \cap K(\overline{\gamma}\bar{\epsilon}^{-1})$ is implied by the more checkable condition that $(\#\bar{\epsilon}(G_L), \#\overline{\gamma}(G_L)) > 1$, where $L = F(\zeta_p) \cap K(\overline{\gamma})$. Indeed, the condition implies that there exist $\sigma, \tau \in G_L$ such that $\bar{\epsilon}(\sigma) = \bar{\gamma}(\tau)$. Since $\bar{\epsilon}$ and $\bar{\gamma}$ induce maps on $\mathrm{Gal}(F(\zeta_p)/L)$ and $\mathrm{Gal}(K(\bar{\gamma})/L)$, respectively, we can project σ and τ to the quotient groups, yielding (non-identity) elements $\bar{\sigma} \in \mathrm{Gal}(F(\zeta_p)/L)$ and $\bar{\tau} \in \mathrm{Gal}(K(\bar{\gamma})/L)$ such that $\bar{\epsilon}(\bar{\sigma}) = \bar{\gamma}(\bar{\tau}) \in k^{\times}$. Letting $M = K(\bar{\gamma})F(\zeta_p)$, we can find an element $\bar{\nu} \in \mathrm{Gal}(M/L)$ such that $\bar{\nu}|_{K(\bar{\gamma})} = \bar{\tau}$ and $\bar{\nu}|_{F(\zeta_p)} = \bar{\sigma}$. Lifting $\bar{\nu}$ to G_L produces an element $\nu \in G_L$ such that $\bar{\gamma}(\nu) = \bar{\epsilon}(\nu)$, meaning $\nu \in G_{K(\bar{\gamma}\bar{\epsilon}^{-1})}$. However, $\nu \notin G_{F(\zeta_p)}$ since $\bar{\sigma}$ was not the identity element in $\mathrm{Gal}(F(\zeta_p)/F)$, and the claim follows.

3.4.3.2 Killing the $M_0(1)$ portion

Having killed the $M_1(1)$ portion of dual Selmer, we can try and get auxiliary primes that take care of the remaining part of the group. First, we have an easy lemma.

Lemma 3.4.14. If $N \geq 1$, then $H^1(\mathrm{Gal}(F(\zeta_{p^N})/F), M_0(1)) = 0$.

Proof. See the proof of [41, Lemma 5.25]. □

Proposition 3.4.15. Let $\mathcal{S} = (\bar{\rho}, \mu, S, \{\Lambda_v\}_{v\in S}, \{\mathcal{D}_v\}_{v\in S})$ be a global deformation problem. Let $T \subset S$, and suppose for $v \in S - T$ we have $\mathcal{D}_v = \mathcal{D}_v^{\mathrm{St}(\alpha_v)}$. Suppose further that $h^1_{\mathcal{S},T}(M_1(1)) = 0$, and let $N_1 \geq 1$ be an integer. Then there exists a finite set Q_1 of finite places of F, disjoint from S, satisfying:

(1) We have $\#Q_1 = h^1_{\mathcal{S},T}(M_0(1))$, and for each $v \in Q_1$, the norm $q_v \equiv 1 \bmod p^{N_1}$ and $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues.

(2) Define the augmented deformation problem

$$\mathcal{S}_{Q_1} = (\bar{\rho}, \mu, S \cup Q_1, \{\Lambda_v\}_{v\in S} \cup \{\mathcal{O}\}_{v\in Q_1}, \{\mathcal{D}_v\}_{v\in S} \cup \{\mathcal{D}_v^{\square}\}_{v\in Q_1}).$$

Then $h^1_{\mathcal{S}_{Q_1},T}(\mathrm{ad}^0\,\bar{\rho}(1)) = 0$.

Proof. We give the proof from [41, Proposition 5.24], as this argument is unchanged. Let $r = h^1_{\mathcal{S},T}(G_{F,S}, M_0(1)) = h^1_{\mathcal{S},T}(G_{F,S}, \mathrm{ad}^0\,\bar{\rho}(1))$. Assume $r \geq 1$. If $v \notin S$ satisfies item (1) above, then $h^1_{\mathcal{S}_{\{v\}},T}(G_{F,S\cup\{v\}}, M_1(1)) = h^1_{\mathcal{S},T}(G_{F,S}, M_1(1)) = 0$. Therefore, it is enough to find a place $v \notin S$ satisfying (1) above, and such that $h^1_{\mathcal{S}_{\{v\}},T}(G_{F,S\cup\{v\}}, M_0(1)) = r - 1$.

Let $0 \neq [\varphi] \in H^1_{\mathcal{S},T}(G_{F,S}, M_0(1))$ be a nontrivial class. It suffices to find a place $v \notin S$ such that:

- $q_v \equiv 1 \bmod p^{N_1}$
- $\bar{\gamma}(\mathrm{Frob}_v) \neq 1$.
- $\varphi(\mathrm{Frob}_v) \neq 0$.

Indeed, the first two points show that v satisfies point (1) from the theorem. We have an exact sequence

$$0 \to H^1_{\mathcal{S}_{\{v\}},T}(G_{F,S\cup\{v\}}, M_0(1)) \to H^1_{\mathcal{S},T}(G_{F,S}, M_0(1)) \to k,$$

where this last map is given by $\varphi \mapsto \varphi(\mathrm{Frob}_v)$, and the third point shows this sequence is exact on the right, whence the desired effect on the dual Selmer group occurs.

By the Cebotarev density theorem, it is enough to find an element $\sigma \in G_F$ such that:

- $\epsilon(\sigma) \equiv 1 \bmod p^{N_1}$
- $\bar{\gamma}(\sigma) \neq 1$
- $\varphi(\sigma) \neq 0$.

Write $F_N = F(\zeta_{p^N})$. We know $\bar{\gamma}|_{G_{F_1}} \neq 1$ by assumption. Since $\bar{\chi}$ has order prime to p, we know $\bar{\gamma}|_{G_{F_{N_1}}} \neq 1$ as well. Choose an element $\sigma_0 \in G_{F_{N_1}}$ with $\bar{\gamma}(\sigma_0) \neq 1$. If $\varphi(\sigma_0) \neq 0$, we are done with $\sigma = \sigma_0$.

If, on the other hand, $\varphi(\sigma_0) = 0$, then let $\tau \in G_{K_1(\zeta_{p^{N_1}})}$ be an element with $\varphi(\tau) \neq 0$. To see that such an element exists, notice we have the inflation-restriction exact sequence

$$0 \to H^1(\mathrm{Gal}(K_1(\zeta_{p_1^N})/F), M_0(1)) \to H^1(G_{F,S}, M_0(1)) \to H^1(G_{K_1(\zeta_{p^{N_1}})}, M_0(1)).$$

Since $\mathrm{Gal}(K_1(\zeta_{p^{N_1}})/F_{N_1})$ has order prime to p, Proposition 2.2.8 and the previous lemma give that this first group is zero, meaning the restriction map is injective. Thus, the image of φ in this last group is nonzero, so such a τ exists. Then simply take $\sigma = \tau\sigma_0$, and this σ will satisfy all the desired points. □

3.5 $R = \mathbb{T}$

For this section, the arguments are unchanged from [41]. For this reason, we will not go into much detail with regards to proofs, as the reader can simply refer to loc. cit.

As usual, let p be an odd prime, and let $L/\mathbb{Q}_p$ be a finite extension with integer ring $\mathcal{O}$. Let $\lambda \subset \mathcal{O}$ denote the maximal ideal, and $k = \mathcal{O}/\lambda$ the residue field. Let F be a totally real number field with $[F : \mathbb{Q}]$ even. Fix a continuous, absolutely irreducible representation $\bar{\rho} : G_F \to \mathrm{GL}_2(k)$. Assume k is large enough that it contains the eigenvalues of every element in $\bar{\rho}(G_F)$. Write $\psi : G_F \to \mathcal{O}^\times$ for the Teichmuller lift of $\bar{\epsilon} \det \bar{\rho}$. We will also write ψ for $\psi \circ \mathrm{Art}_F : \mathbb{A}_F^{\infty,\times} \to \mathcal{O}^\times$. Suppose $\bar{\rho}$ satisfies:

- If $K \subset F(\zeta_p)$ is the unique quadratic subfield of $F(\zeta_p)/F$, then there exists a continuous character $\bar{\chi} : G_K \to k^\times$ such that $\bar{\rho} \cong \mathrm{Ind}_{G_K}^{G_F} \bar{\chi}$. As in the previous section, $w \in G_F$ will denote an element with nontrivial image in $\mathrm{Gal}(K/F)$.

- We have $F(\zeta_p) \not\subset K(\bar{\gamma}\bar{\epsilon}) \cap K(\bar{\gamma}\bar{\epsilon}^{-1})$, where $\bar{\gamma} = \bar{\chi}/\bar{\chi}^w$. (This is a deviation from [41].)
- The character $\bar{\gamma}$ is nontrivial, even after restricting to $G_{F(\zeta_p)}$.
- For each place $v \nmid p$ of F, the representation $\bar{\rho}|_{G_{F_v}}$ is unramified.
- For each place $v|p$ of F, the restriction $\bar{\rho}|_{G_{F_v}}$ is trivial.
- The character $\bar{\epsilon} \det \bar{\rho}$ is everywhere unramified.
- There is a finite set R of finite places of F, of even cardinality, such that for $v \in R$, we have $q_v \equiv 1 \bmod p$ and $\bar{\rho}|_{G_{F_v}}$ is trivial.
- There is a finite set Q_0 of finite places of F, again of even cardinality, disjoint from $S_p \cup R$, and a tuple $(\alpha_v)_{v \in Q_0}$ of elements of k, such that for each $v \in Q_0$, the local deformation problem $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined.
- There is an isomorphism $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$ and a cuspidal automorphic representation π_0 of weight 2 such that:
  - There is an isomorphism $\overline{r_\iota(\pi_0)} \cong \bar{\rho}$.
  - The central character of π_0 is $\iota\psi$
  - For each finite place $v \notin S_p \cup Q_0 \cup R$ of F, we have $\pi_{0,v}$ is unramified.
  - For each $v \in R \cup Q_0$, there is an unramified character $\chi_v : F_v^\times \to \overline{\mathbb{Q}}_p^\times$ and an isomorphism $\pi_{0,v} \cong \mathrm{St}_2(\iota\chi_v)$. For each $v \in Q_0$, the element $\chi_v(\varpi_v)$ is congruent to α_v modulo the maximal ideal of $\overline{\mathbb{Z}}_p$.
  - If $\sigma \subset S_p$ denotes the places where $\pi_{0,v}$ is ι-ordinary, then for each $v \in \sigma$, we have $\pi_{0,v}^{U_0(v)} \neq 0$, and for each $v \in S_p \backslash \sigma$, we have $\pi_{0,v}$ is unramified.

We have the following lemma.

Lemma 3.5.1. [41, Lemma 6.1] There exists $v_0 \notin S_p \cup Q_0 \cup R$ such that $q_{v_0} > 4^{[F:\mathbb{Q}]}$ and $\operatorname{tr} \bar{\rho}(\mathrm{Frob}_{v_0})^2 / \det \bar{\rho}(\mathrm{Frob}_{v_0}) \neq (1+q_{v_0})^2/q_{v_0}$.

Throughout this section, a place v_0 from the lemma will be fixed. We will consider the global deformation problem

$$\mathcal{S} = (\bar{\rho}, \epsilon^{-1}\psi, S_p \cup Q_0 \cup R, \{\mathcal{O}[\![\mathcal{O}_{F_v}^{\times}(p)]\!]\}_{v\in\sigma} \cup \{\mathcal{O}\}_{v\in(S_p\setminus\sigma)\cup Q_0\cup R},$$

$$\{\mathcal{D}_v^{\mathrm{ord}}\}_{v\in\sigma} \cup \{\mathcal{D}_v^{\text{non-ord}}\}_{v\in S_p\setminus\sigma} \cup \{\mathcal{D}_v^{\mathrm{St}(\alpha_v)}\}_{v\in Q_0} \cup \{\mathcal{D}_v^{\mathrm{St}}\}_{v\in R}).$$

Let $T = S_p \cup R$, so that the rings $R_{\mathcal{S}}$ and $R_{\mathcal{S}}^T$ from section 2.3.6 are defined.

3.5.1 Automorphic Forms

In order to get the theorem we want, we need to study congruences between automorphic forms. We do this by working through a quaternion algebra as in section 3.2.1.

Let $B = B_{Q_0\cup R}$ be a quaternion algebra ramified at $Q_0 \cup R \cup \{v|\infty\}$. Note that, by all the assumptions, this is a set with even cardinality. Let $\mathcal{O}_B \subset B$ be a maximal order. As in section 3.2.1, we there is an associated reductive group G over $\mathcal{O}_F$, given by $G(R) = (\mathcal{O}_B \otimes_{\mathcal{O}_F} R)^{\times}$. If $v \notin Q_0 \cup R$ is a finite place of F, we will fix an isomorphism $\mathcal{O}_B \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v} \cong M_2(\mathcal{O}_{F_v})$, which yields an isomorphism $G(F_v) \cong \mathrm{GL}_2(F_v)$ and $G(\mathcal{O}_{F_v}) \cong \mathrm{GL}_2(\mathcal{O}_{F_v})$.

We will now define an open compact subgroup $U = \prod_v U_v \subset G(\mathbb{A}_F^{\times})$ as follows:

- If $v \notin Q_0 \cup R \cup \{v_0\}$, then $U_v = G(\mathcal{O}_{F_v}) \cong \mathrm{GL}_2(\mathcal{O}_{F_v})$.
- If $v \in Q_0 \cup R$, then U_v will be the unique maximal compact subgroup of $G(F_v)$.
- If $v = v_0$, then $U_{v_0} = U_1^1(v_0)$.

We can now define the space of automorphic forms which we want to study.

Definition 3.5.2. If $V = \prod_v V_v \subset U$ is an open compact subgroup and A is an $\mathcal{O}$-module, then we will write $H_\psi(V, A)$ for the set of functions $f : G(F)\backslash G(\mathbb{A}_F^{\times}) \to A$ satisfying

$$f(zgu) = \psi(z)f(g) \quad \forall z \in \mathbb{A}_F^{\infty,\times}, g \in G(\mathbb{A}_F^{\times}), u \in V.$$

Choose a double coset decomposition

$$G(\mathbb{A}_F^\infty) = \coprod_i G(F) g_i V \mathbb{A}_F^{\infty,\times}.$$

Let $A(\psi^{-1})$ denote the $\mathcal{O}[U\mathbb{A}_F^{\infty,\times}]$-module with underlying set A on which U acts trivially and $\mathbb{A}_F^{\infty,\times}$ acts by ψ^{-1}. The double coset decomposition above yields an injection

$$H_\psi(V, A) \to \bigoplus_i A(\psi^{-1}), \quad f \mapsto (f(g_i))_i.$$

Determining the image amounts to asking when $g_i = g g_i u z$ for $g \in G(F)$, $u \in V$, and $z \in \mathbb{A}_F^{\infty,\times}$. Thus, we see we have an isomorphism

$$H_\psi(V, A) \cong \bigoplus_i A(\psi^{-1})^{(g_i G(F) g_i^{-1} \cap V \mathbb{A}_F^{\infty,\times})/F^\times}.$$

(See [16, Section 5.2] for further explanation.) In fact, the groups $(g_i G(F) g_i^{-1} \cap V\mathbb{A}_F^{\infty,\times})/F^\times$ are finite of order prime to p. Consequently, we have the following:

Lemma 3.5.3. The map $H_\psi(V, \mathcal{O}) \otimes_{\mathcal{O}} A \to H_\psi(V, A)$ is an isomorphism.

We also have the following lemma.

Lemma 3.5.4. [41, Lemma 6.2] Suppose $V_1 = \prod_v V_{1,v} \subset V_2 = \prod_v V_{2,v}$ are open compact subgroups of U with V_1 normal in V_2 and $V_2 \cap \mathbb{A}_F^{\infty,\times} = V_1 \cap \mathbb{A}_F^{\infty,\times}$. Suppose further that V_2/V_1 is abelian of p-power order. Then:

(1) The trace map $\mathrm{tr}_{V_2/V_1} : H_\psi(V_1, \mathcal{O}) \to H_\psi(V_2, \mathcal{O})$ factors through an isomorphism $H_\psi(V_1, \mathcal{O})_{V_2} \cong H_\psi(V_2, \mathcal{O})$.

(2) The space $H_\psi(V_1, \mathcal{O})$ is a free $\mathcal{O}[V_2/V_1]$-module.

In truth, we will actually want to work with an ordinary subspace of $H_\psi(V, A)$, and so we take the time to define it now. To do this, we first define two families of open compact subgroups of U.

Definition 3.5.5. For each $n \geq 1$, we define $U_0(\sigma^n) = \prod_v U_0(\sigma^n)_v$ and $U_1(\sigma^n) = \prod_v U_1(\sigma^n)_v$ as follows:

(1) If $v \in \sigma$, then $U_0(\sigma^n)_v = U_0(v^n)$ and $U_1(\sigma^n)_v = U_1(v^n)$.

(2) If $v \notin \sigma$, then $U_0(\sigma^n)_v = U_1(\sigma^n)_v = U_v$.

Remark 3.5.6. If $n = 1$, then it is dropped from the notation.

Recall from the definition of the global deformation problem $\mathcal{S}$ that if $v \in \sigma$, then $\Lambda_v = \mathcal{O}[\![\mathcal{O}_{F_v}^\times(p)]\!]$. Write $\Lambda = \widehat{\bigotimes}_{v\in\sigma}\Lambda_v$ (this agrees with the definition of Λ from section 2.3.6).

Definition 3.5.7. If S is a finite set of finite places of F, then we write $\mathbb{T}^{\Lambda,S,\text{univ}}$ for

$$\mathbb{T}^{\Lambda,S,\text{univ}} = \Lambda[T_v, S_v]_{v\notin S}.$$

If $Q \subset S$, then we write $\mathbb{T}_Q^{\Lambda,S,\text{univ}}$ for the polynomial ring

$$\mathbb{T}_Q^{\Lambda,S,\text{univ}} = \mathbb{T}^{\Lambda,S,\text{univ}}[\mathbf{U}_v]_{v\in Q}.$$

Fix $S = \sigma \cup Q_0 \cup R \cup \{v_0\}$. If $v \in S_p \backslash \sigma$, then by definition, we have $T_v \in \mathbb{T}^{\Lambda,S,\text{univ}}$.

Definition 3.5.8. (1) If M is a $\mathbb{T}^{\Lambda,S,\text{univ}}$-module, we write $\mathbb{T}^{\Lambda,S}(M)$ for the image of $\mathbb{T}^{\Lambda,S,\text{univ}}$ in $\text{End}_\Lambda(M)$.

(2) If M is a $\mathbb{T}_Q^{\Lambda,S,\text{univ}}$-module, we write $\mathbb{T}_Q^{\Lambda,S}(M)$ for the image of $\mathbb{T}_Q^{\Lambda,S,\text{univ}}$ in $\text{End}_\Lambda(M)$.

It turns out we can make each of the spaces $H_\psi(U_i(\sigma^n), A)$, for $n \geq 1$ and $i \in \{0,1\}$, into a $\mathbb{T}_{Q_0}^{\Lambda,S,\text{univ}}$-module. Indeed, the operators $T_v, S_v, \mathbf{U}_v \in \mathbb{T}_{Q_0}^{\Lambda,S,\text{univ}}$ acts by the Hecke operators of the same name, as in Section 3.2.2. We therefore only need to define the action of Λ, and for this it is enough to define an action of $\prod_{v\in\sigma} \mathcal{O}_{F_v}^\times(p)$ on each $H_\psi(U_i(\sigma^n), A)$ (already an $\mathcal{O}$-module). To do this, if $\alpha \in \mathcal{O}_{F_v}^\times(p)$ act via the double coset operator

$$\langle\alpha\rangle = \left[U_i(\sigma^n)_v \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} U_i(\sigma^n)_v \right].$$

The inclusions $H_\psi(U_i(\sigma^n), A) \hookrightarrow H_\psi(U_i(\sigma^{n+1}), A)$ are maps of $\mathbb{T}_{Q_0}^{\Lambda,S,\text{univ}}$-modules.

Set $\mathbf{U}_\sigma = \prod_{v\in\sigma} \mathbf{U}_v$. Note that $\mathbf{U}_\sigma$ acts on $H_\psi(U_1(\sigma^n), \mathcal{O})$. We form the ordinary idempotent

$$e = \lim_{N\to\infty} \mathbf{U}_\sigma^{N!},$$

which acts on $H_\psi(U_1(\sigma^n), \mathcal{O})$ for each $n \geq 1$, and hence on $H_\psi(U_1(\sigma^n), A)$ for any $\mathcal{O}$-module A (by Lemma 3.5.3). We can define the ordinary subspace

$$H_\psi^{\mathrm{ord}}(U_1(\sigma^n), \mathcal{O}) = eH_\psi(U_1(\sigma^n), A),$$

and

$$H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty)) = \varinjlim_n H_\psi^{\mathrm{ord}}(U_1(\sigma^n), L/\mathcal{O}).$$

Write

$$\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))) = \varprojlim_n \mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^n), L/\mathcal{O})).$$

This algebra is reduced, since each of the algebras in the inverse limit is reduced. We have the following lemma:

Lemma 3.5.9. [41, Lemma 6.3] Let A be an $\mathcal{O}$-module.

(1) For any $n \geq 1$, the inclusion $H_\psi^{\mathrm{ord}}(U_0(\sigma), A) \to H_\psi^{\mathrm{ord}}(U_0(\sigma^n), A)$ is an isomorphism.

(2) If $n \geq m \geq 1$, then the inclusion $H_\psi^{\mathrm{ord}}(U_1(\sigma^m), A) \to H_\psi^{\mathrm{ord}}(U_1(\sigma^m) \cap U_0(\sigma^n), A)$ is an isomorphism.

We can use this lemma to relate $H_\psi^{\mathrm{ord}}(U_1(\sigma^n), A)$ with $H_\psi^{\mathrm{ord}}(U_1(\sigma^m), A)$. To do this, we define some more notation. If $v \in \sigma$ and $n \geq 1$, let $\Lambda_{v,n} = \mathcal{O}[(1+\varpi_v\mathcal{O}_{F_v})/(1+\varpi_v^n\mathcal{O}_{F_v})]$ (so $\Lambda_{v,1} = \mathcal{O}$). We let $\Lambda_n = \widehat{\bigotimes}_{v\in\sigma}\Lambda_{v,n}$, and $\mathfrak{a}_n$ for the kernel of the surjection

$$\mathfrak{a}_n = \ker(\Lambda \to \Lambda_n).$$

Then for $n \geq m \geq 1$, the lemma gives

$$H_\psi^{\mathrm{ord}}(U_1(\sigma^n), A)[\mathfrak{a}_m] = H_\psi^{\mathrm{ord}}(U_0(\sigma^n) \cap U_1(\sigma^m), A) = H_\psi^{\mathrm{ord}}(U_1(\sigma^m), A).$$

Before we state the proposition, recall that the Pontryagin dual of an $\mathcal{O}$-module M is defined to be $M^\vee = \mathrm{Hom}_{\mathcal{O}}(M, L/\mathcal{O})$.

Proposition 3.5.10. [41, Proposition 6.4]

(1) For each $n \geq 1$, there is an isomorphism

$$H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))^\vee/\mathfrak{a}_n H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))^\vee \cong \mathrm{Hom}_{\mathcal{O}}(H_\psi^{\mathrm{ord}}(U_1(\sigma^n),\mathcal{O}),\mathcal{O}).$$

(2) The space $H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))^\vee$ is a free Λ-module of rank $\dim_k H_\psi^{\mathrm{ord}}(U_1(\sigma),k)$.

(3) The algebra $\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty)))$ is a finite faithful Λ-module.

3.5.2 Galois Representations

Recall the hypothesis of the section included a cuspidal automorphic representation π_0 of weight 2. Associated to this automorphic representation is a homomorphism

$$\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma),L/\mathcal{O})) \to \overline{\mathbb{F}}_p.$$

Notice that, since $\bar{\rho}$ is defined over k, and each α_v (for $v \in Q_0$) lies in k, this homomorphism is really a homomorphism

$$\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma),L/\mathcal{O})) \to k.$$

Consider the composition

$$\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))) \to \mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma),L/\mathcal{O})) \to k,$$

and let $\mathfrak{m} \subset \mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty)))$ denote the kernel.

Proposition 3.5.11. [41, Proposition 6.5] There is a lift of $\bar{\rho}$ to a continuous representation

$$\rho_{\mathfrak{m}} : G_F \to \mathrm{GL}_2(\mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))_{\mathfrak{m}}))$$

of type $\mathcal{S}$ such that, for all finite places $v \notin S_p \cup Q_0 \cup R \cup \{v_0\}$, the representation $\rho_{\mathfrak{m}}$ is unramified, and $\rho_{\mathfrak{m}}(\mathrm{Frob}_v)$ has characteristic polynomial $X^2 - T_v X + q_v S_v$.

By universality, there is a map $R_{\mathcal{S}} \to \mathbb{T}_{Q_0}^{\Lambda,S}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty)))_{\mathfrak{m}}$ and, consequently, the space $H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))_{\mathfrak{m}}$ has an $R_{\mathcal{S}}$-module structure.

Before stating the main theorem, recall that $T = S_p \cup R$.

Theorem 3.5.12. [41, Theorem 6.6] If $h^1_{\mathcal{S},T}(M_1(1)) = 0$, then $\mathrm{Fitt}_{R_{\mathcal{S}}} H^{\mathrm{ord}}_{\psi}(U_1(\sigma^{\infty}))^{\vee}_{\mathfrak{m}} = 0$.

The proof of Theorem 3.5.12 will utilize the Taylor-Wiles patching argument. We will then use this theorem as a tool for Khare's method of modularity lifting via the following corollary.

Corollary 3.5.13. [41, Corollary 6.7] Suppose $C, N, n \geq 1$ are all integers. Assume

$$\dim_k H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n), k)[\mathfrak{m}] \leq C,$$

and suppose we have the following commutative diagram:

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_n \\ \downarrow & & \downarrow \\ R_{\mathcal{S}} & \longrightarrow & \mathcal{O}/\Lambda^N \end{array}$$

corresponding to a lift $\rho_N : G_F \to \mathrm{GL}_2(\mathcal{O}/\lambda^N)$ of type $\mathcal{S}$. Let $I = \ker(R_{\mathcal{S}} \to \mathcal{O}/\lambda^{\lfloor N/C \rfloor})$. Then $(H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n), \mathcal{O})_{\mathfrak{m}} \otimes_{\mathcal{O}} \mathcal{O}/\lambda^{\lfloor N/C \rfloor})[I]$ contains an $\mathcal{O}$-submodule isomorphic to $\mathcal{O}/\lambda^{\lfloor N/C \rfloor}$, and the map $R_{\mathcal{S}} \to \mathcal{O}/\lambda^{\lfloor N/C \rfloor}$ factors as

$$R_{\mathcal{S}} \to \mathbb{T}^{\Lambda, S \cup S_p}_{Q_0}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n), L/\mathcal{O})_{\mathfrak{m}}) \to \mathcal{O}/\lambda^{\lfloor N/C \rfloor}.$$

The rest of the section is devoted to proving Theorem 3.5.12. To do this, we introduce the Taylor-Wiles primes and a patching argument. Sources for the overall method, aside from [41], are [16] and [19].

Suppose there is a finite Q_1 of finite places of F with $Q_1 \cap (S_p \cup R \cup Q_0 \cup \{v_0\}) = \emptyset$, such that:

- For each $v \in Q_1$, we have $q_v \equiv 1 \bmod p$, and
- For each $v \in Q_1$, the matrix $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues $\alpha_v, \beta_v \in k$.

For $v \in Q_1$, we let Δ_q denote the maximal p-power quotient of $k(v)^{\times}$, and $\Delta_{Q_1} = \prod_{v \in Q_1} \Delta_q$, which is the maximal p-power quotient of $\prod_{v \in Q_1} k(v)^{\times}$ (here, $k(v)$ denotes the residue field at v). Let $\mathfrak{a}_{Q_1} \subset \mathcal{O}[\Delta_{Q_1}]$ denote the augmentation ideal, namely the ideal generated by the $\sigma - 1$ for $\sigma \in \Delta_{Q_1}$. We will define an augmented global deformation problem

$$\mathcal{S}_{Q_1} = (\bar{\rho}, \epsilon^{-1}\psi, S_p \cup Q_0 \cup R \cup Q_1, \{\mathcal{O}[\![\mathcal{O}_{F_v}^{\times}(p)]\!]\}_{v\in\sigma} \cup \{\mathcal{O}\}_{v\in(S_p\setminus\sigma)\cup Q_0\cup R\cup Q_1},$$

$$\{\mathcal{D}_v^{\text{ord}}\}_{v\in\sigma} \cup \{\mathcal{D}_v^{\text{non-ord}}\}_{v\in S_p\setminus\sigma} \cup \{\mathcal{D}_v^{\text{St}(\alpha_v)}\}_{v\in Q_0} \cup \{\mathcal{D}_v^{\text{St}}\}_{v\in R} \cup \{\mathcal{D}_v^{\square}\}_{v\in Q_1}).$$

Let $\rho_{\mathcal{S}_{Q_1}} : G_F \to \mathrm{GL}_2(R_{\mathcal{S}_{Q_1}})$ denote a representative of the universal deformation. For each $v \in Q_1$, there are characters $A_v, B_v : G_{F_v}^{\text{ab}} \to R_{\mathcal{S}_{Q_1}}^{\times}$ such that $A_v \bmod \mathfrak{m}_{R_{\mathcal{S}_{Q_1}}}$ and $B_v \bmod \mathfrak{m}_{R_{\mathcal{S}_{Q_1}}}$ are unramified (since $\bar{\rho}$ is unramified at v by assumption), and such that

$$A_v(\text{Frob}_v) \bmod \mathfrak{m}_{R_{\mathcal{S}_{Q_1}}} = \alpha_v, \quad B_v(\text{Frob}_v) \bmod \mathfrak{m}_{R_{\mathcal{S}_{Q_1}}} = \beta_v.$$

Moreover, there is an isomorphism

$$\rho_{\mathcal{S}_{Q_1}}|_{G_{F_v}} \sim \begin{pmatrix} A_v & 0 \\ 0 & B_v \end{pmatrix}.$$

The ring $R_{\mathcal{S}_{Q_1}}$ is naturally a $\mathcal{O}[\Delta_{Q_1}]$-algebra from the maps

$$k(v)^{\times} \to R_{\mathcal{S}_{Q_1}}^{\times}, \quad \sigma \mapsto A_v(\text{Art}_{F_v}(\sigma)).$$

A deformation of type $\mathcal{S}$ is automatically of type $\mathcal{S}_{Q_1}$, and so there is a map $R_{\mathcal{S}_{Q_1}} \to R_{\mathcal{S}}$ with kernel $\mathfrak{a}_{Q_1} R_{\mathcal{S}_{Q_1}}$, i.e.

$$R_{\mathcal{S}_{Q_1}}/\mathfrak{a}_{Q_1} R_{\mathcal{S}_{Q_1}} \cong R_{\mathcal{S}}.$$

These $R_{\mathcal{S}_{Q_1}}$ will be our auxiliary Galois deformation rings, but we need corresponding auxiliary Hecke modules.

To do this, let $H_0 = H_{\psi}^{\text{ord}}(U_1(\sigma^{\infty}))_{\mathfrak{m}}^{\vee}$.

Lemma 3.5.14. [41, Lemma 6.8] There exists an $R_{\mathcal{S}_{Q_1}}$-module H_{Q_1} which is free over $\Lambda[\Delta_{Q_1}]$ and such that

$$H_{Q_1}/\mathfrak{a}_{Q_1} H_{Q_1} \cong H_0$$

as $R_{\mathcal{S}}$-modules.

Proof. We replicate the proof from [41] here. We first define new open compact subgroups of U to deal with the new primes in Q_1. Before giving the definitions, notice that if $v \in Q_1$, there is a canonical homomorphism $g : U_0(v) \to \Delta_v$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad^{-1}.$$

We will let $U_0(Q_1) = \prod_v U_0(Q_1)_v$ and $U_1(Q_1) = \prod_v U_1(Q_1)_v$, where:

- If $v \notin Q_1$, then $U_0(Q_1)_v = U_1(Q_1)_v = U_v$, and
- If $v \in Q_1$, then $U_0(Q_1)_v = U_0(v)$, and $U_1(Q_1)_v = \ker g$, where g is as above.

Notice that $U_1(Q_1)$ is a normal subgroup of $U_0(Q_1)$, and (essentially by definition)

$$U_0(Q_1)/U_1(Q_1) \cong \Delta_{Q_1}.$$

The Hecke algebra $\mathbb{T}^{\Lambda, S\cup Q_1, \mathrm{univ}}_{Q_0 \cup Q_1}$ acts on each $H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n) \cap U_i(Q_1), A)$ for $i = 0, 1$. Recall from the beginning of this subsection that there is a homomprphism

$$f : \mathbb{T}^{\Lambda, S}_{Q_0}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma), L/\mathcal{O})) \to k$$

with $\mathfrak{m} = \ker f$. Write $\mathfrak{m}_{Q_1} \subset \mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0\cup Q_1}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma) \cap U_0(Q_1), L/\mathcal{O}))$ for the maximal ideal generated by m_Λ, $T_v - f(T_v)$ for $v \notin S \cup Q_1$, and $\mathbf{U}_v - \alpha_v$ for $v \in Q_0 \cup Q_1$. We use the same $\mathfrak{m}_{Q_1}$ to denote the pullback of this maximal ideal to $\mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0\cup Q_1}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma) \cap U_1(Q_1), L/\mathcal{O}))$ as well. By the same arguments made in [37, Section 2], we have the following:

(1) For each $n \geq 1$, there is an isomorphism

$$H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n) \cap U_0(Q_1), L/\mathcal{O})_{\mathfrak{m}_{Q_1}} \cong H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n), L/\mathcal{O})_{\mathfrak{m}}$$

of Hecke modules, and an isomorphism

$$\mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0\cup Q_1}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n) \cap U_0(Q_1), L/\mathcal{O}))_{\mathfrak{m}_{Q_1}} \cong \mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0\cup Q_1}(H^{\mathrm{ord}}_{\psi}(U_1(\sigma^n), L/\mathcal{O}))_{\mathfrak{m}}$$

of Λ-algebras.

(2) For each $n \geq 1$, the Λ-subalgebra of $\mathrm{End}_\Lambda(H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_1(Q_1), L/\mathcal{O}))_{\mathfrak{m}_{Q_1}}$ generated by $\mathcal{O}[\Delta_{Q_1}]$ is a subset of $\mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0 \cup Q_1}(H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_1(Q_1), L/\mathcal{O}))_{\mathfrak{m}_{Q_1}}$, and there is a map $R_{\mathcal{S}_{Q_1}} \to \mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0 \cup Q_1}(H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_1(Q_1), L/\mathcal{O}))_{\mathfrak{m}_{Q_1}}$ of $\Lambda[\Delta_{Q_1}]$-algebras such that $\mathrm{tr}\, \rho_{\mathcal{S}_{Q_1}}(\mathrm{Frob}_v) \mapsto T_v$ and $\det \rho_{\mathcal{S}_{Q_1}}(\mathrm{Frob}_v) \mapsto S_v$ for $v \notin S_p \cup R \cup Q_0 \cup \{v_0\} \cup Q_1$.

For $i \in \{0, 1\}$, define

$$H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty) \cap U_i(Q_1)) = \varinjlim_n H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_i(Q_1), L/\mathcal{O}),$$

so that

$$\mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0 \cup Q_1}(H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty) \cap U_i(Q_1))) = \varprojlim_n \mathbb{T}^{\Lambda, S\cup Q_1}_{Q_0 \cup Q_1}(H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_i(Q_1), L/\mathcal{O})).$$

We will let $H_{Q_1} = H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty) \cap U_1(Q_1))^\vee_{\mathfrak{m}_{Q_1}}$. By Lemma 3.5.4, we know that $H_\psi^{\mathrm{ord}}(U_1(\sigma^n) \cap U_1(Q_1), L/\mathcal{O})^\vee$ is free over $\Lambda_n[\Delta_{Q_1}]$, and, by taking limits, we see H_{Q_1} is free over $\Lambda[\Delta_{Q_1}]$. Moreover, by the isomorphism in (1) above, we know

$$\begin{aligned} H_{Q_1}^\vee[\mathfrak{a}_{Q_1}] &= H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty) \cap U_1(Q_1))_{\mathfrak{m}_{Q_1}}[\mathfrak{a}_{Q_1}] \\ &= H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty) \cap U_0(Q_1))_{\mathfrak{m}_{Q_1}} \\ &\cong H_\psi^{\mathrm{ord}}(U_1(\sigma^\infty))_{\mathfrak{m}} \\ &= H_0^\vee. \end{aligned}$$

By dualizing, we get the result. □

The following lemma is a consequence of Proposition 2.3.29 and the work on killing the $M_0(1)$ portion of the dual Selmer group.

Lemma 3.5.15. Assume $h^1_{\mathcal{S},T}(M_1(1)) = 0$, and let $q = h^1_{\mathcal{S},T}(M_0(1))$. Then for any $N \geq 1$, there exists a finite set Q_N of finite places of F such that:

(1) The set Q_N is disjoint from $S_p \cup Q_0 \cup R \cup \{v_0\}$ and $\#Q_N = q$.

(2) For each $v \in Q_N$, the size of the residue field satisfies $q_v \equiv 1 \bmod p^N$, and $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues $\alpha_v, \beta_v \in k$.

(3) We have $h^1_{\mathcal{S}_{Q_N},T}(\mathrm{ad}^0\,\bar\rho(1)) = 0$.

(4) The ring $R^T_{\mathcal{S}_{Q_N}}$ can be written as a power series over $A^T_{\mathcal{S}_{Q_N}} = A^T_{\mathcal{S}}$ in $q-[F:\mathbb{Q}]-1+\#T$ variables.

With these sets Q_N in hand, let $m = q-[F:\mathbb{Q}]-1+\#T$ and $R_\infty = A^T_{\mathcal{S}}[\![X_1, X_2, \ldots, X_m]\!]$. The ring R_∞ is reduced, and for any minimal prime $Q \subset \Lambda$, the space $\operatorname{Spec} R_\infty/(Q)$ is geometrically irreducible of dimension

$$\dim A^T_{\mathcal{S}} + m = \dim \Lambda + q - 1 + 4\#T,$$

and the generic point is of characteristic zero. Fix a place $v' \in T$, and let

$$\mathcal{T} = \mathcal{O}[\![\{Y_{v,i,j}\}_{v\in T, 1\le i,j\le 2}\}]\!]/(Y_{v',1,1}).$$

Fix representatives $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}_{Q_N}}$ for every $N \geq 1$ for the universal deformations over $R_{\mathcal{S}}$ and $R_{\mathcal{S}_{Q_N}}$, respectively, such that each $\rho_{\mathcal{S}_{Q_N}}$ specializes to $\rho_{\mathcal{S}}$. This yields compatible isomorphisms

$$R^T_{\mathcal{S}} \cong R_{\mathcal{S}} \hat\otimes_{\mathcal{O}} \mathcal{T}, \quad R^T_{\mathcal{S}_{Q_N}} \cong R_{\mathcal{S}_{Q_N}} \hat\otimes_{\mathcal{O}} \mathcal{T}$$

corresponding to the equivalence classes of the T-framed lifts $(\rho_{\mathcal{S}}, (1 + (Y_{v,i,j}))_{v\in T})$ and $(\rho_{\mathcal{S}_{Q_N}}, (1 + (Y_{v,i,j}))_{v\in T})$, respectively.

Let $\Delta_\infty = \mathbb{Z}_p^q$. For each N, fix a surjection $\Delta_\infty \to \Delta_{Q_N}$. Let $S_\infty = \Lambda[\![\Delta_\infty]\!]\hat\otimes_{\mathcal{O}} \mathcal{T}$, and let $\mathfrak{a}_\infty \subset S_\infty$ denote the kernel of the augmentation map $S_\infty \to \Lambda$. The isomorphisms above give $R^T_{\mathcal{S}}$ and $R^T_{\mathcal{S}_{Q_N}}$ an S_∞-algebra structure, and the auxiliary Hecke modules $H^T_0 = H_0 \otimes_{R_{\mathcal{S}}} R^T_{\mathcal{S}}$ and $H^T_{Q_N} = H_{Q_N} \otimes_{R_{\mathcal{S}_{Q_N}}} R^T_{\mathcal{S}_{Q_N}}$ are free over $\Lambda\hat\otimes_{\mathcal{O}}\mathcal{T}[\Delta_{Q_N}]$. A standard patching argument (cf. [39]) yields the following:

- A finitely generated R_∞-module H_∞.
- A homomorphism $S_\infty \to R_\infty$ of Λ-algebras, which makes H_∞ a free S_∞-module.
- A surjection $R_\infty/\mathfrak{a}_\infty R_\infty \to R_{\mathcal{S}}$ and an isomorphism $H_\infty/\mathfrak{a}_\infty H_\infty \cong H_0$ of $R_{\mathcal{S}}$-modules.

To finish the argument, let $P \subset \Lambda$ be a minimal prime. Then $H_\infty/(P)$ is a free $S_\infty/(P)$-module, and $S_\infty/(P)$ is a regular local ring. In particular, we have

$$\operatorname{depth}_{R_\infty/(P)}(H_\infty/(P)) \geq \operatorname{depth}_{S_\infty(p)} H_\infty/(P) = \dim S_\infty/(P) = \dim R_\infty/(P).$$

Consequently (cf. [38]), $H_\infty/(P)$ is a nearly faithful $R_\infty/(P)$-module. As P is arbitrary, H_∞ is a faithful R_∞-module, which means $\operatorname{Fitt}_{R_\infty} H_\infty = 0$. Therefore

$$0 = \operatorname{Fitt}_{R_{\mathcal{S}}}(H_\infty \otimes_{R_\infty} R_{\mathcal{S}}) = \operatorname{Fitt}_{R_{\mathcal{S}}} H_0.$$

3.6 Proof of the Main Theorem

The goal is to now prove Theorem 3.1.1. Here we differ only in the slightest fashion from [41], replacing Thorne's condition that the quadratic subfield of $F(\zeta_p)/F$ be totally real with the condition from section 3.4. As such, we only give a proof of the theorem where the level-raising and level-lowering developed in the earlier sections are used, and refer to [41, Section 7] for the rest of the proofs.

There are necessary preliminary results before moving to the main theorem.

Lemma 3.6.1. Let F be a totally real number field, and let F'/F be a totally real, soluble extension. Let p be a prime and let $\iota : \overline{\mathbb{Q}}_p \xrightarrow{\sim} \mathbb{C}$ be a fixed isomorphism.

(1) Let π be a cuspidal automorphic representaion of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, and suppose that $r_\iota(\pi)|_{G_{F'}}$ is irreducible. Then there exists a cuspidal automorphic representation $\pi_{F'}$ of $\mathrm{GL}_2(\mathbb{A}_{F'})$ of weight 2, called the *base change* of π, such that $r_\iota(\pi_{F'}) \cong r_\iota(\pi)|_{G_{F'}}$.

(2) Let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be a continuous representation such that $\rho|_{G_{F'}}$ is irreducible. Let π' be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_{F'})$ of weight 2 with $\rho|_{G_{F'}} \cong r_\iota(\pi')$. Then there exists a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 such that $\rho \cong r_\iota(\pi)$.

Proof. This is stated in [41, Lemma 5.1]. The proof follows from results of [24], using arguments of [2, Lemma 1.3]. □

Theorem 3.6.2. Let F be a totally real field, and let p be an odd prime. Let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be a continuous representation. Suppose that:

(1) $[F : \mathbb{Q}]$ is even.

(2) Letting K be the quadratic subfield of $F(\zeta_p)/F$, there exists a continuous character $\bar{\chi} : G_K \to \overline{\mathbb{F}}_p^\times$ such that $\bar{\rho} \cong \mathrm{Ind}_{G_K}^{G_F} \bar{\chi}$.

(3) Letting $w \in \mathrm{Gal}(K/F)$ be the nontrivial element, the character $\bar{\gamma} = \bar{\chi}/\bar{\chi}^w$ remains nontrivial even after restriction to $G_{F(\zeta_p)}$ (in particular, $\bar{\rho}$ is irreducible).

(4) We have $F(\zeta_p) \not\subset K(\bar{\gamma}\bar{\epsilon}^{-1}) \cap K(\bar{\gamma}\bar{\epsilon})$.

(5) The character $\psi = \epsilon \det \rho$ is everywhere unramified.

(6) The representation ρ is almost everywhere unramified.

(7) For each place $v|p$, $\rho|_{G_{F_v}}$ is semi-stable, and $\bar{\rho}|_{G_{F_v}}$ is trivial. For each embedding $\tau : F \hookrightarrow \overline{\mathbb{Q}}_p$, we have $\mathrm{HT}_\tau(\rho) = \{0, 1\}$.

(8) If $v \nmid p$ is a finite place of F at which ρ is ramified, then $q_v \equiv 1 \bmod p$, $\mathrm{WD}(\rho|_{G_{F_v}})^{F-ss} \cong \mathrm{rec}^T_{F_v}(\mathrm{St}_2(\chi_v))$ for some unramified character $\chi_v : F_v^\times \to \overline{\mathbb{Q}}_p^\times$, and $\bar{\rho}|_{G_{F_v}}$ is trivial. The number of such places is even.

(9) There exists a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 and an isomorphism $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$ satisfying:

   (a) There is an isomorphism $\overline{r_\iota(\pi)} \cong \bar{\rho}$.

   (b) If $v|p$ and ρ is ordinary, then π_v is ι-ordinary and $\pi_v^{U_0(v)} \neq 0$. If $v|p$ and ρ is non-ordinary, then π_v is not ι-ordinary and π_v is unramified.

   (c) If $v \nmid p\infty$ and $\rho|_{G_{F_v}}$ is unramified, then π_v is unramified. If $v \nmid p\infty$ and $\rho|_{G_{F_v}}$ is ramified, then π_v is an unramified twist of the Steinberg representation.

Then ρ is automorphic: there exists a cuspidal automorphic representation π' of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2 and an isomorphism $\rho \cong r_\iota(\pi')$.

Remark 3.6.3. Here, $U_0(v)$ is the set of matrices in $\mathrm{GL}_2(\mathcal{O}_{F_v})$ whose reduction modulo a fixed uniformizer of $\mathcal{O}_{F_v}$ is upper triangular.

Remark 3.6.4. This is [41, Theorem 7.2] with the necessary modifications (namely, the addition of condition (4) instead of the condition that K be totally real). One can just repeat the proof the author gives in that paper, replacing Proposition 5.20 of *loc. cit.* with the corresponding theorem from section 3.4. For completeness, we will give the proof from [41] now, with the aforementioned modifications.

Proof. After replacing ρ by a conjugate, we can find a finite extension $L/\mathbb{Q}_p$ such that ρ takes values in $\mathrm{GL}_2(\mathcal{O})$ and $\bar{\chi}$ takes values in $k^\times$. The goal is to show that ρ satisfies the conditions of Corollary 3.2.13. To do this, we will use Theorem 3.5.12 and the subsequent corollary. Fix $N \geq 1$, and write $\sigma \subset S_p$ for the set of places such that $\rho|_{G_{F_v}}$ is ordinary. Let R denote the set of places away from p at which π_v is ramified.

The global deformation problem we will consider is

$$\mathcal{S} = (\bar{\rho}, \epsilon^{-1}\psi, S_p \cup R, \{\Lambda_v\}_{v\in\sigma} \cup \{\mathcal{O}\}_{v\in(S_p\setminus\sigma)\cup R}, \{\mathcal{D}_v^{\mathrm{ord}}\}_{v\in\sigma} \cup \{\mathcal{D}_v^{\text{non-ord}}\}_{v\in S_p\setminus\sigma} \cup \{\mathcal{D}_v^{\mathrm{St}(\alpha_v)}\}_{v\in R}).$$

Let $T = S_p \cup R$. By Proposition 3.4.12, there exists a finite set Q_0 of finite places of F and $\alpha_v \in k$ (for $v \in Q_0$) such that:

- Q_0 is disjoint from $S_p \cup R$.
- $\#Q_0 = 2\lceil h^1_{\mathcal{S},T}(M_1(1))/2\rceil$.
- For each $v \in Q_0$, the local deformation problem $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ is defined.
- If $\mathcal{S}_{Q_0}$ is the global deformation problem:

$$\mathcal{S} = (\bar{\rho}, \epsilon^{-1}\psi, S_p \cup R \cup Q_0, \{\Lambda_v\}_{v\in\sigma} \cup \{\mathcal{O}\}_{v\in(S_p\setminus\sigma)\cup R\cup Q_0},$$

$$\{\mathcal{D}_v^{\mathrm{ord}}\}_{v\in\sigma} \cup \{\mathcal{D}_v^{\text{non-ord}}\}_{v\in S_p\setminus\sigma} \cup \{\mathcal{D}_v^{\mathrm{St}(\alpha_v)}\}_{v\in R} \cup \{\mathcal{D}_v^{\mathrm{St}(\alpha_v)}\}_{v\in Q_0}),$$

  then $h^1_{\mathcal{S}_{Q_0},T}(M_1(1)) = 0$.

To apply Lemma 3.2.11, we need to fix a place v_0. Let v_0 be any place satisfying Lemma 3.5.1. By Lemma 3.2.11, we can find a cuspidal automorphic representation π_0 of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, satisfying the following conditions:

- There is an isomorphism $\overline{r_\iota(\pi_0)} \cong \overline{\rho}$.
- If $v \in \sigma$, then $\pi_{0,v}$ is ι-ordinary and $\pi_{0,v}^{U_0(v)} \neq 0$. If $v \in S_p \backslash \sigma$, then $\pi_{0,v}$ is not ι-ordinary and $\pi_{0,v}$ is unramified.
- If $v \notin S_p \cup R \cup Q_0$ is a finite place of F, then $\pi_{0,v}$ is unramified. If $v \in R \cup Q_0$ then $\pi_{0,v}$ is an unramified twist of the Steinberg representation. If $v \in Q_0$, then the eigenvalue of $\mathbf{U}_v$ on $\iota^{-1}\pi_{0,v}^{U_0(v)}$ is congruent to α_v modulo the maximal ideal of $\overline{\mathbb{Z}}_p$.

After replacing π_0 by a character twist, we can assume π_0 has central character $\iota\psi$. Theorem 3.5.12 now applies to the deformation problem $\mathcal{S}_{Q_0}$.

Let $S = S_p \cup R \cup \{v_0\}$. Let $\mathfrak{m}_\emptyset \subset \mathbb{T}^{S,\mathrm{univ}}$ be the maximal ideal corresponding to π, so that $\mathfrak{m}_\emptyset \in \mathrm{Supp}(H_R(U))$. Let $C_0 = \dim_k(H_R(U) \otimes_{\mathcal{O}} k)[\mathfrak{m}_\emptyset]$. By Proposition 3.2.10, we know

$$\dim_k(H_{R\cup Q_0}(U_{Q_0}) \otimes_{\mathcal{O}} k)[\mathfrak{m}_{Q_0}] \leq 4^{\#Q_0} C_0.$$

Now apply the corollary to Theorem 3.5.12 with $C = 4^{\#Q_0}C_0$ and $n = 1$. This produces a homomorphism $f : \mathbb{T}_{Q_0}^{S\cup Q_0}(H_{R\cup Q_0}(U_{Q_0})) \to \mathcal{O}/\lambda^{\lfloor N/C \rfloor}$ such that:

- For each finite $v \notin S \cup Q_0$, we have $f(T_v) = \mathrm{tr}\,\rho(\mathrm{Frob}_v) \bmod \lambda^{\lfloor N/C \rfloor}$.
- If $I = \ker f$, then $(H_{R\cup Q_0}(U_{Q_0}) \otimes_{\mathcal{O}} \mathcal{O}/\lambda^{\lfloor N/C \rfloor})[I]$ contains an $\mathcal{O}$-submodule isomorphic to $\mathcal{O}/\lambda^{\lfloor N/C \rfloor}$.

Now use Corollary 3.2.13. □

Using this theorem, we arrive at the main theorem.

Theorem 3.6.5. Let F be a totally real number field, let p be an odd prime, and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be a continuous representation satisfying the following:

(1) The representation ρ is almost everywhere unramified.

(2) For each $v|p$ of F, the local representation $\rho|_{G_{F_v}}$ is de Rham. For each embedding $\tau : F \hookrightarrow \overline{\mathbb{Q}}_p$, we have $\mathrm{HT}_\tau(\rho) = \{0, 1\}$.

(3) For each complex conjugation $c \in G_F$, we have $\det \rho(c) = -1$.

(4) The residual representation $\bar{\rho}$ is absolutely irreducible, but $\bar{\rho}|_{G_{F(\zeta_p)}}$ is a direct sum of two distinct characters. Further suppose that if K is the unique quadratic subfield of $F(\zeta_p)/F$ and $\bar{\gamma} : G_K \to k^\times$ is the ratio of the two characters, then we have $F(\zeta_p) \not\subset K(\bar{\gamma}\bar{\epsilon}^{-1}) \cap K(\bar{\gamma}\bar{\epsilon})$.

Then ρ is automorphic: there exists a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight 2, an isomorphism $\iota : \overline{\mathbb{Q}}_p \to \mathbb{C}$, and an isomorphism $\rho \cong r_\iota(\pi)$.

Proof. The proof is exactly the same as [41, Theorem 7.5], replacing Theorem 7.2 of loc. cit. with Theorem 3.6.2 above. The idea is to construct a soluble extension F'/F such that $\bar{\rho}|_{G_{F'}}$ satisfies the conditions of Theorem 3.6.2 above. We then apply Lemma 3.6.1 to deduce the automorphy of ρ. We should note that in [41], the author makes use of Corollary 7.4 in loc. cit., but that goes unchanged for us because that corollary made no assumptions on the quadratic subfield K. □

3.7 Application to Elliptic Curves

In this section we give the application of Theorem 3.6.5 to elliptic curves. As mentioned in Section 3.1.2, through the work of Wiles [44], Taylor-Wiles [45], and Breuil, Conrad, Diamond and Taylor ([5], [7], [9]), it was shown that all elliptic curves over $\mathbb{Q}$ are modular. Since then, the question has shifted to proving the automorphy of elliptic curves over totally real fields.

In a paper of Freitas, Le Hung, and Siksek (see [14]) the authors prove there are only finitely many non-automorphic elliptic curves over any given totally real field. The major idea in their proof is the idea of a "3-7 switch", building off the idea of Wiles' "3-5 switch". After Wiles proved an appropriate $R = \mathbb{T}$ theorem, he applied it to the setting of elliptic curves as follows (note that each of the following points is a theorem in its own right, but we merely want the reader to see the logic of the argument, not the details of the proofs):

- If $E/\mathbb{Q}$ is any elliptic curve with $\bar{\rho}_{E,3}$ irreducible, then $\bar{\rho}_{E,3}$ is modular. (This is a consequence of a deep theorem of Langlands and Tunnell.)

- Let $E/\mathbb{Q}$ be a semistable elliptic curve and suppose $\bar{\rho}_{E,p}$ is irreducible and modular for some prime $p \geq 3$. Then E is modular.

  Remark 3.7.1. This is a consequence of Serre's observation that for a semistable elliptic curve, the residual representation $\bar{\rho}_{E,p}$ is either surjective or reducible for every prime $p \geq 3$. Then apply the first point and Wiles' $R = \mathbb{T}$ theorem.

- If $E/\mathbb{Q}$ is a semistable elliptic curve and suppose $\bar{\rho}_{E,5}$ is irreducible. Then there is another semistable elliptic curve $E'/\mathbb{Q}$ for which $\bar{\rho}_{E',3}$ is irreducible and $\bar{\rho}_{E',5} \cong \bar{\rho}_{E,5}$.

- If $E/\mathbb{Q}$ is a semistable elliptic curve, then at least one of $\bar{\rho}_{E,3}$ or $\bar{\rho}_{E,5}$ is irreducible.

The "3-5" switch is the following: Let E be a semistable elliptic curve over $\mathbb{Q}$. If $\bar{\rho}_{E,3}$ is irreducible, then it is modular by the first and second points above. If it is reducible, then the fourth point implies $\bar{\rho}_{E,5}$ is irreducible, and the third point gives a curve $E'/\mathbb{Q}$ with $\bar{\rho}_{E',3}$ irreducible, which implies E' is modular. Since the mod 5 representations of E and E' are isomorphic $\bar{\rho}_{E,5}$ is modular, which implies E is modular.

In [14], the authors show that for elliptic curves over totally real fields, there is a similar "3-7 switch" that can be performed. The following theorem is [14], Theorems 3 and 4.

Theorem 3.7.2. Let $p \in \{3, 5, 7\}$. Let E be an elliptic field over a totally real field F and let $\bar{\rho}_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ be the representation given by the action on the p-torsion of E. If $\bar{\rho}_{E,p}(G_{F(\zeta_p)})$ is absolutely irreducible, then E is modular.

We make the following definition.

Definition 3.7.3. If E/F is an elliptic curve over a totally real field F, then E is called p-bad if $E[p]$ is an absolutely reducible $\mathbb{F}_p[G_{F(\zeta_p)}]$-module. Otherwise E is p-good.

Theorem 3.7.2 says exactly that the only elliptic curves E which are potentially non-modular are those which are p-bad for $p = 3, 5$, and 7. In [41], the author deals with some of these remaining cases:

Theorem 3.7.4. Let E be an elliptic curve over a totally real field F. Suppose:

(1) 5 is not a square in F.

(2) E has no F-rational 5-isogeny.

Then E is modular.

The reason Thorne used $p = 5$ is that he needed the quadratic subfield of $F(\zeta_p)/F$ to be totally real, which implies $p \equiv 1 \bmod 4$. Our modifications allow us to work with $p = 7$ instead. Before stating and proving our main theorem for the section, we recall [14, Proposition 9.1].

Proposition 3.7.5. Let F be a totally real number field and let E be an elliptic curve over F. Suppose $F \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$ and write $\bar{\rho} = \bar{\rho}_{E,7}$. Suppose $\bar{\rho}$ is irreducible but $\bar{\rho}(G_{F(\zeta_7)})$ is absolutely reducible. Then $\bar{\rho}(G_F)$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to one of the groups

$$H_1 = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \right\rangle, \quad H_2 = \left\langle \begin{pmatrix} 0 & 5 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 3 & 2 \end{pmatrix} \right\rangle.$$

The group H_1 has order 36 and is contained as a subgroup of index 2 in the normalizer of a split Cartan subgroup. The group H_2 has order 48 and is contained as a subgroup of index 2 in the normalizer of a non-split Cartan subgroup. The images of H_1 and H_2 in $\mathrm{PGL}_2(\mathbb{F}_7)$ are isomorphic to $D_3 \cong S_3$ and D_4, respectively.

We can now prove our main application.

Theorem 3.7.6. Let F be a totally real field, and let E be an elliptic curve over F. Suppose:

(1) $F \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$.

(2) E has no F-rational 7-isogeny.

(3) Either $\bar{\rho}_{E,7}(G_{F(\zeta_7)})$ is absolutely irreducible, or it is reducible and $\bar{\rho}_{E,7}(G_F)$ is conjugate to the group H_1 from the previous proposition.

Then E is modular.

Proof. Let $\rho : G_F \to \mathrm{GL}_2(\mathbb{Q}_7)$ be the representation given by the action of G_F on the étale cohomology $H^1(E_{\overline{F}}, \mathbb{Z}_7)$, after a choice of basis. The goal is to show ρ is automorphic. Hypothesis (2) is equivalent to $\bar{\rho}$ being irreducible, hence absolutely irreducible because of complex conjugation. If $\bar{\rho}|_{G_{F(\zeta_7)}}$ is irreducible, then ρ is automorphic by Theorem 3.7.2 above. We now deal with the case when this restriction is not irreducible.

If $\bar{\rho}|_{G_{F(\zeta_7)}}$ is absolutely reducible, the third hypothesis combined with the previous proposition gives that the projective image of $\bar{\rho}$ in $\mathrm{PGL}_2(\mathbb{F}_7)$ is isomorphic to D_3. This implies that $\bar{\rho}|_{G_{F(\zeta_7)}}$ cannot be scalar since $\mathrm{Gal}(F(\zeta_7)/F)$ is cyclic, and therefore cannot surject onto D_3.

Let K be the quadratic subfield of $F(\zeta_7)/F$, so that $[F(\zeta_7) : K] = 3$ by hypothesis (1). Let $\bar{\gamma} : G_K \to \mathbb{F}_7^\times$ be the character which gives the ratio of the eigenvalues. We need to examine the subgroup

$$H_1 = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{F}_7).$$

It is easy to check that these two matrices generate the projective image as well. By simply checking the ratio of eigenvalues of each of the matrices, one can check that the possible values for the image of $\bar{\gamma}$ are elements of $\{1, 2, 4\}$. Therefore, $[K(\bar{\gamma}) : K] = 3$ or 1. However, it cannot be the latter as $\bar{\gamma}$ is nontrivial as a character on G_K by assumption. Therefore $[K(\bar{\gamma}) : K] = 3$, so $K(\bar{\gamma}) \cap F(\zeta_7) = K$ or $F(\zeta_7)$. But we know it cannot be $F(\zeta_7)$ since the image of $\bar{\rho}|_{G_{F(\zeta_7)}}$ is non-scalar. Thus, $K(\bar{\gamma})$ is disjoint over K from $F(\zeta_7)$ and $[K(\bar{\gamma}) : K] = [F(\zeta_7) : K] = 3$. Thus, hypothesis (4) of the main theorem above is satisfied, and the theorem implies E is modular. □

We can extend Theorem 3.7.6 to primes other than $p = 7$, and we prove this more general version.

Theorem 3.7.7. Let F be a totally real field, and let E be an elliptic curve over F. Let $p \geq 7$ be a prime such that $(p-1)/2 = q^n$ for some odd prime q and $n \geq 1$. Suppose:

(1) $F \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

(2) E has no F-rational p-isogeny.

(3) $\bar{\rho}_{E,p}(G_F)$ normalizes a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

Then E is modular.

Proof. Let $\rho : G_F \to \mathrm{GL}_2(\mathbb{Q}_p)$ be the representation given by the action of G_F on the étale cohomology $H^1(E_{\overline{F}}, \mathbb{Z}_p)$, after a choice of basis. The goal is to show ρ is automorphic. Hypothesis (2) is equivalent to $\bar{\rho} = \bar{\rho}_{E,p}$ being irreducible, hence absolutely irreducible because of complex conjugation. Hypothesis (3) says $\bar{\rho}(G_F)$ is contained in the normalizer of a split Cartan subgroup. Note that the absolute irreducibility of $\bar{\rho}$ implies the projective image is non-cyclic, for if it were cyclic, the image of $\bar{\rho}$ would be abelian. Thus, $\bar{\rho}(G_{F(\zeta_p)})$ cannot be scalar, since $\mathrm{Gal}(F(\zeta_p)/F)$ is cyclic, and hence cannot surject onto a non-cylic group.

Let K be the quadratic subfield of $F(\zeta_p)/F$, so that $[F(\zeta_p) : K] = q^n = (p-1)/2$ by hypothesis (1). Let $\bar{\gamma} : G_K \to \mathbb{F}_p^\times$ be the character which gives the ratio of eigenvalues of $\bar{\rho}|_{G_K}$. We want to examine $[K(\bar{\gamma}) : K]$, where $K(\bar{\gamma}) = \bar{F}^{\ker(\bar{\gamma})}$ as always. In particular, we will show that $K(\bar{\gamma}) \cap F(\zeta_p)$ is a field L which satisfies $(\#\bar{\epsilon}(G_L), \#\bar{\gamma}(G_L)) > 1$, which implies hypothesis (4) of the main theorem. Note that hypothesis (1) implies that, as a character of G_K, that $\bar{\epsilon}$ takes values in $(\mathbb{F}_p^\times)^2$.

Using the fact that $\det \bar{\rho}$ is the mod p cyclotomic character, we find that $\bar{\chi}\bar{\chi}^w = \bar{\epsilon}$, so that $\bar{\gamma} = \bar{\chi}/\bar{\chi}^w = \bar{\chi}^2\bar{\epsilon}^{-1}$, which is a character $G_K \to (\mathbb{F}_p^\times)^2$. Thus, the order of $\bar{\gamma}$ divides $(p-1)/2 = q^n$, and moreover cannot equal 1 as $\bar{\gamma}$ is a nontrivial character of G_K. Thus, $1 < [K(\bar{\gamma}) : K] \big| q^n$. Moreover, $[F(\zeta_p) : K] = q^n$ by hypothesis (1) of the theorem. Lastly, we know $K(\bar{\gamma}) \not\subseteq F(\zeta_p)$ since $\bar{\gamma}$ is nontrivial upon restriction to $G_{F(\zeta_p)}$, and thus $K(\bar{\gamma}) \cap F(\zeta_p)$ is neither $K(\bar{\gamma})$ nor $F(\zeta_p)$. This intersection is therefore a field L which satisfies $(\#\bar{\epsilon}(G_L), \#\bar{\gamma}(G_L)) > 1$ as q divides both quantities. Thus, hypothesis (4) of the main theorem is satisfied, and therefore E is modular. $\square$

3.8 Future Work

Khare and Thorne [23] are jointly working on dealing with the cases not handled by the work above and [41]. However, there is still work to be done. One case not being considered is the $p = 2$ setting. Recently, Allen [1] proved the modularity of nearly ordinary 2-adic residually dihedral representations. The case when the representation is not nearly ordinary has not yet been treated.

One of the main issues in the $p = 2$ case is that the deformation problem $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ used in the work above may not be smooth. Instead, it may be possible to consider primes v such that $\bar{\rho}(\mathrm{Frob}_v)$ of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, but this has not been examined in any detail as of yet. This is a natural direction to move given what has been done already in the $p > 2$ setting in the work of [21], [23], and [41].

CHAPTER 4

Higher Dimensional Setting

The previous chapter examined residually dihedral representations in the two-dimensional setting. Ideally, there would be some way of generalizing the methods of that work to the higher dimensional case.

Technically, all the work from Section 2.3 works for representations valued in GL_n, though dimension arguments need to be modified accordingly. However, to prove automorphy lifting theorems, one works with a modified group, denoted $\mathcal{G}_n$, in part because the Taylor-Wiles argument does not carry over well to the GL_n setting (see [6, Section 1] for more details). This modified group looks very similar to GL_n, but carries additional information. Also, importantly, the l-adic points of this group are connected to automorphic forms on unitary groups, and so there is hope for proving automorphy lifting theorems in this setting as well.

This chapter is incomplete, in the sense that there is still much work to be done in this setting before getting full results. This chapter can essentially be regarded as the basis for a future project. From that perspective, the ideas of this chapter are preliminary and will hopefully lead to a nice automorphy lifting theorem.

In this chapter, we will first introduce this group $\mathcal{G}_n$, and rather than developing the full deformation theory again, we will simply remark that the same definitions as in Section 2.3 apply. We will then describe the results, which try to emulate the Galois theory work of Section 3.4, and the future work, which involves the automorphic arguments.

4.1 The group $\mathcal{G}_n$

The main source for this section is [6], though [39] is also a good reference. We first define the group $\mathcal{G}_n$:

Definition 4.1.1. (1) If $n > 0$ is a positive integer, then $\mathcal{G}_n$ is defined to be the group scheme over $\mathbb{Z}$ given by

$$\mathcal{G}_n = (\mathrm{GL}_n \times \mathrm{GL}_1) \rtimes \{1, j\},$$

where the group $\{1, j\}$ acts on $\mathrm{GL}_n \times \mathrm{GL}_1$ by

$$j(g, \mu)j^{-1} = (\mu \cdot (g^{-1})^t, \mu).$$

(2) There is a homomorphism $\nu : \mathcal{G}_n \to \mathrm{GL}_1$ given by

$$\nu(g, \mu) = \mu, \quad \nu(j) = -1.$$

(3) $\mathcal{G}_n^0$ will be the connected component of $\mathcal{G}_n$.

(4) $\mathfrak{g}_n$ will denote $\mathrm{Lie}\, GL_n \subset \mathrm{Lie}\, \mathcal{G}_n$, and ad will denote the adjoint action of $\mathcal{G}_n$ on $\mathfrak{g}_n$. In particular,

$$(\mathrm{ad}(g, \mu))(x) = gxg^{-1}, \quad (\mathrm{ad}(j))(x) = -x^t.$$

(5) $\mathfrak{g}_n^0 \subset \mathfrak{g}_n$ will be the subspace of trace zero elements.

Throughout this section, let Γ be a group, and $\Delta \leq \Gamma$ an index 2 subgroup. If Γ is a topological group, assume Δ is closed (and hence open as it is closed of finite index). This is the setting of [6], but we will only apply these results to the situation where $\Gamma = G_{F^+,S}$ and $\Delta = G_{F,S}$, where F/F^+ is a quadratic imaginary extension of number fields, F^+ is a totally real field, and S some finite set of primes of F^+ split in F. We want to consider homomorphisms $r : \Gamma \to \mathcal{G}_n(R)$, where R is a ring. The following will help us define these homomorphisms.

Lemma 4.1.2. [6, Lemma 2.1.1] Let R be a ring, and $\gamma_0 \in \Gamma - \Delta$. Then there is a natural bijection between:

(1) Homomorphisms $r : \Gamma \to \mathcal{G}_n(R)$ which induce isomorphisms $\Gamma/\Delta \cong \mathcal{G}_n/\mathcal{G}_n^0$.

(2) Triples $(\rho, \mu, \langle -, - \rangle)$, where $\rho : \Delta \to \mathrm{GL}_n(R)$ and $\mu : \Gamma \to R^\times$ are homomorphisms, and

$$\langle -, - \rangle : R^n \times R^n \to R$$

is a perfect R-linear pairing such that for all $x, y \in R^n$ and $\delta \in \Delta$, we have

(i) $\langle x, \rho(\gamma_0^2) y \rangle = -\mu(\gamma_0) \langle y, x \rangle$

(ii) $\mu(\delta) \langle x, y \rangle = \left\langle \rho(\delta) x, \rho(\gamma_0 \delta \gamma_0^{-1}) y \right\rangle$.

Under the correspondence, $\mu = \nu \circ r$, and if $r(\gamma_0) = (A, -\mu(\gamma_0))j$, then

$$\langle x, y \rangle = x^t \cdot A^{-1} \cdot y.$$

This lemma gives us a way of translating between GL_n-representations of Δ and $\mathcal{G}_n$-representations of Δ. If $r : \Gamma \to \mathcal{G}_n(R)$ is a homomorphism, then we will also let $r : \Delta \to \mathrm{GL}_n(R)$ by restricting to Δ and then projecting the image to GL_n, though most of the time we denote this restriction as $r|_\Delta$.

Now given a homomorphism $\rho : \Gamma \to \mathrm{GL}_n(R)$, the question is when it will lift to a homomorphism $r : \Gamma \to \mathcal{G}_n(R)$.

Lemma 4.1.3. [6, Lemma 2.1.2] Let R be a ring, and $(-, -)$ a perfect bilinear pairing $R^n \times R^n \to R$, which satisfies

$$(x, y) = (-1)^a (y, x),$$

say $(x, y) = x^t J y$ for $J \in M_n(R)$. Let $\delta_{\Gamma/\Delta} : \Gamma/\Delta \to \{\pm 1\}$ be an isomorphism, and suppose $\mu : \Gamma \to R^\times$ and $\rho : \Gamma \to \mathrm{GL}_n(R)$ are homomorphisms satisfying

$$(\rho(\gamma) x, \rho(\gamma) y) = \mu(\gamma)(x, y)$$

for all $\gamma \in \Gamma$ and $x, y \in R^n$. Then there is a homomorphism $r : \Gamma \to \mathcal{G}_n(R)$ defined by

$$r(\delta) = (\rho(\delta), \mu(\delta)), \quad r(\gamma) = (\rho(\gamma) J^{-1}, (-1)^a \mu(\gamma)) j$$

for $\delta \in \Delta$ and $\gamma \in \Gamma - \Delta$. Moreover,

$$\nu \circ r = \delta_{\Gamma/\Delta}^{a+1} \mu.$$

Another question is when homomorphisms $\Delta \to \mathrm{GL}_n(k)$, where k is a field, can be lifted to a homomorphism $\Gamma \to \mathcal{G}_n(k)$.

Lemma 4.1.4. [6, Lemma 2.1.4]

(1) Suppose that k is a field, and $\gamma_0 \in \Gamma - \Delta$. Suppose further that $\chi : \Gamma \to k^\times$ is a homomorphism, and

$$\rho : \Delta \to \mathrm{GL}_n(k)$$

is absolutely irreducible and satisfies $\chi\rho^\vee \cong \rho^{\gamma_0}$. Then there exists a homomorphism

$$r : \Gamma \to \mathcal{G}_n(k)$$

such that $r|_\Delta = (\rho, \chi|_\Delta)$ and $r(\gamma_0) \in \mathcal{G}_n(k) - \mathrm{GL}_n(k)$.

(2) If $\alpha \in k^\times$, define

$$r_\alpha : \Gamma \to \mathcal{G}_n(k)$$

by $r_\alpha|_\Delta = \rho$, and if $\gamma \in \Gamma - \Delta$ and $r(\gamma) = (A, \mu)j$, then

$$r_\alpha(\gamma) = (\alpha A, \mu)j.$$

This produces a bijection between $\mathrm{GL}_n(k)$-conjugacy classes of extensions of ρ to $\Gamma \to \mathcal{G}_n(k)$ and $k^\times/(k^\times)^2$.

Proof. There exists a perfect pairing

$$\langle -, - \rangle : k^n \times k^n \to k$$

such that

$$\chi(\delta) \left\langle \rho(\delta)^{-1}x, y \right\rangle = \left\langle x, \rho(\gamma_0 \delta \gamma_0^{-1}) y \right\rangle,$$

for $x, y \in k^n$ and $\delta \in \Delta$. As ρ is absolutely irreducible, $\langle -, - \rangle$ is unique up to $k^\times$-multiples.

Set

$$\langle x, y \rangle' = \left\langle y, \rho(\gamma_0^2) x \right\rangle.$$

One checks that

$$\chi(\delta)\left\langle \rho(\delta)^{-1}x, y\right\rangle' = \left\langle x, \rho(\gamma_0\delta\gamma_0^{-1})y\right\rangle'.$$

By uniqueness,

$$\langle -, -\rangle' = \epsilon \langle -, -\rangle$$

for some $\epsilon \in k^\times$. Notice

$$\langle x, y\rangle'' = \left\langle \rho(\gamma_0^2)x, \rho(\gamma_0^2)y\right\rangle = \left\langle \rho(\gamma_0^2)x, \rho(\gamma_0\gamma_0^2\gamma_0^{-1})y\right\rangle = \chi(\gamma_0^2)\langle x, y\rangle.$$

Thus

$$\epsilon^2 = \chi(\gamma_0)^2.$$

Now use Lemma 1.2 with $(\rho, \chi, \langle -, -\rangle)$ to get r. □

The classical deformation theory usually requires some $\bar{\rho}: G \to \mathrm{GL}_n(k)$ to be absolutely irreducible. There is an analogue of this criterion in this modified setting.

Definition 4.1.5. Let k be a field, and $r : \Gamma \to \mathcal{G}_n(k)$ be a homomorphism with $\Delta = r^{-1}(\mathrm{GL}_n \times \mathrm{GL}_1)(k)$. Suppose $\gamma_0 \in \Gamma - \Delta$. Then r is called *Schur* if all irreducible Δ-subquotients of k^n are absolutely irreducible, and if for all Δ-invariant subspaces $W_2 \subset W_1 \subset k^n$ with k^n/W_1 and W_2 irreducible, we have

$$W_2^\vee(\nu \circ r) \ncong (k^n/W_1)^{\gamma_0}.$$

This is independent of the choice of γ_0.

Remark 4.1.6. If $r|_\Delta$ is absolutely irreducible, then clearly r is Schur. In general, this is enough for the deformation theory to work, but it also works in this more general setting.

Lemma 4.1.7. [6, Lemma 2.1.7] Let k be a field, and $r : \Gamma \to \mathcal{G}_n(k)$ be a homomorphism with $\Delta = r^{-1}(\mathrm{GL}_n \times \mathrm{GL}_1)(k)$. If r is Schur, then the following hold:

(1) $r|_\Delta$ is semisimple.

(2) If $r' : \Gamma \to \mathcal{G}_n(k)$ is another representation with $\Delta = (r')^{-1}(\mathrm{GL}_n \times \mathrm{GL}_1)(k)$ and $\mathrm{tr}\, r|_\Delta = \mathrm{tr}\, r'|_\Delta$, then r' is $\mathrm{GL}_n(\overline{k})$-conjugate to r.

(3) If $\operatorname{char} k \neq 2$, then $\mathfrak{g}_n^\Gamma = 0$.

Proof. We may suppose $k = \overline{k}$. For (1), choose $\gamma_0 \in \Gamma - \Delta$. As in Lemma 1.2, r corresponds to a triple $(r|_\Delta, \mu, \langle -, - \rangle)$. Let $V \subset k^n$ be an irreducible Δ-submodule.

Claim. $(k^n/V^\perp)^{\gamma_0} \cong V^\vee(\nu \circ r)$.

Proof of Claim. We have a homomorphism of vector spaces

$$\varphi : k^n \to V^\vee, \quad x \mapsto (v \mapsto \langle v, x \rangle).$$

The kernel is clearly $V^\perp$, and surjectivity is standard linear algebra (using dual bases). Thus, we need to show it is a Δ-module homomorphism, i.e. $\varphi(\delta x)(v) = \delta\varphi(x)(v)$ for $\delta \in \Delta$ and $v \in V$. The left side is $\varphi(r(\gamma_0 \delta \gamma_0^{-1})x)(v) = \left\langle v, r(\gamma_0\delta\gamma_0^{-1})x \right\rangle$. The right side is

$$(\nu \circ r)(\delta)\varphi(x)(r(\delta)^{-1}v) = (\nu \circ r)(\delta) \left\langle r(\delta)^{-1}v, x \right\rangle.$$

The claim follows from the properties of the inner product.

By definition of Schur, we cannot have $V \subset V^\perp$, and thus $k^n \cong V \oplus V^\perp$ as Δ-modules. Iterate this recursively to get a decomposition

$$k^n = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

and

$$\langle -, - \rangle = \langle -, - \rangle_1 \perp \langle -, - \rangle_2 \perp \ldots \perp \langle -, - \rangle_r,$$

where each V_i is an irreducible $k[\Delta]$-module, each $\langle -, - \rangle_i$ is a perfect pairing on V_i, each $V_i \not\cong V_j$ for $i \neq j$, and $V_i^{\gamma_0} \cong V_i^\vee(\nu \circ r)$.

For (2), if ρ and τ are representations $\Delta \to \mathrm{GL}_n(k)$ with ρ semi-simple and $\operatorname{tr}\rho = \operatorname{tr}\tau$, then the semisimplifications of ρ and τ are equivalent. Thus $r'|_\Delta$ has the same Jordan-Holder factors as $r|_\Delta$. So r' satisfies same hypotheses as r, and thus $r'|_\Delta$ is semisimple as well, meaning $r'|_\Delta \cong r|_\Delta$, and we may assume they are equal. The triple for r' is thus

$$(r|_\Delta, \mu, \mu_1 \langle -, - \rangle_1 \perp \ldots \perp \mu_r \langle -, - \rangle_r),$$

since the inner products are unique up to $k^\times$-multiples. Conjugation by the element of $\mathrm{GL}_n(\bar{k})$ which acts on V_i by $\sqrt{\mu_i}$ will take r to r'.

Lastly, for (3), note

$$\begin{aligned} \mathfrak{g}_n^\Delta &= \{A \in M_n(k) : r(\delta)Ar(\delta)^{-1} = A\} \\ &= \mathrm{End}_{k[\Delta]}(k^n) \\ &= \mathrm{End}_{k[\Delta]}(V_1) \oplus \cdots \oplus \mathrm{End}_{k[\Delta]}(V_r) \\ &= k^r, \end{aligned}$$

as $V_i \not\cong V_j$ are irreducible submodules and k is algebraically closed. Then γ_0 sends $(\alpha_1, \ldots, \alpha_r)$ to $(-\alpha_1^{*_1}, \ldots, -\alpha_r^{*_r}) = (-\alpha_1, \ldots, -\alpha_r)$, since $-\alpha_i^{*_i} = -\alpha_i$, where $*_i$ denotes the adjoint with respect to $\langle -, - \rangle_i$. Thus $\mathfrak{g}_n^\Gamma = 0$. □

4.2 Notation

We now introduce the notation for the remainder of the chapter. Let p be an odd prime, and $k/\mathbb{F}_p$ be a finite extension. Let K be a totally ramified extension of $W(k)$, and let $\mathcal{O} \subset K$ denote the integer ring with maximal ideal λ (so $\mathcal{O}/\lambda = k$).

Let F^+ be a totally real number field, and F/F^+ a totally imaginary quadratic extension split at all primes above p. Let S be a finite set of finite places of F^+ which split in F, and let $F(S)/F$ be the maximal extension unramified outside S and ∞. Notice that $F(S)/F^+$ may ramify at places outside S if they ramify in F/F^+. We will let $G_{F^+,S} = \mathrm{Gal}(F(S)/F^+)$ and $G_{F,S} = \mathrm{Gal}(F(S)/F)$, so that $G_{F,S}$ is an index two subgroup of $G_{F^+,S}$. For $v \in S$, choose a place $\tilde{v}$ of F above v, and write $\tilde{S} = \{\tilde{v}\}_{v \in S}$, so that $\#\tilde{S} = \#S$.

Suppose $\bar{r} : G_{F^+,S} \to \mathcal{G}_n(k)$ is a continuous homomorphism with $G_{F,S} = \bar{r}^{-1}(\mathrm{GL}_n \times \mathrm{GL}_1)(k)$. Let $\chi : G_{F^+,S} \to \mathcal{O}^+$ be a continuous lift of $\nu \circ \bar{r} : G_{F^+,S} \to k^\times$. If $\tilde{v}$ is a finite place of F, we let $\bar{r}|_{G_{F_{\tilde{v}}}}$ denote the composite

$$G_{F_{\tilde{v}}} \to G_{F,S} \xrightarrow{\bar{r}} \mathcal{G}_n(k) \to \mathrm{GL}_n(k).$$

In this context, it makes sense to define local deformation problems as was done in Section 2.3. For $v \in S$, let $\mathcal{D}_v$ be a local deformation problem for $\bar{r}|_{G_{F_{\tilde{v}}}}$. A global deformation problem for $\bar{r}$ will be the collection of data

$$\mathcal{S} = (F/F^+, S, \tilde{S}, \mathcal{O}, \bar{r}, \chi, \{\mathcal{D}_v\}_{v \in S}).$$

Notice that this is slightly different than what was done in Section 2.3.6.

4.3 Highlights of the Two-Dimensional Argument

If one were to make a broad summary of the arguments in Section 3.4 without fretting the details, it might look something like this:

(1) Firstly, for a representation $\bar{\rho} : G_F \to \mathrm{GL}_2(k)$ whose restriction to $G_{F(\zeta_p)}$ is reducible, the corresponding adjoint representation $\mathrm{ad}\,\bar{\rho}$ also decomposes.

(2) If the deformation problems are chosen nicely and the tangent spaces $\mathcal{L}_v$ respect the decomposition of $\mathrm{ad}\,\bar{\rho}$, then the dual Selmer group also decomposes into the diagonal and off-diagonal pieces.

(3) In killing dual Selmer, the first step is to kill the off-diagonal piece. For this argument it is important that:

   - The off-diagonal component of the tangent space of the deformation problem lies in the unramified cohomology of this off-diagonal component.
   - The mod p^n has primes for which the local deformation problem is defined.
   - The deformation problem serves as a level-raising tool.

   As mentioned in Remark 3.4.13, essentially all the ramification for the cohomology group is being pushed into the diagonal piece.

(4) Use Taylor-Wiles primes to kill the diagonal component of the dual Selmer group.

For the remainder of this chapter, we will discuss the corresponding ideas in the higher dimensional setting.

4.4 Reducible Restriction

The goal is to study higher dimensional representations whose restriction to $G_{F(\zeta_p)}$ is reducible, as was done in the previous chapter. The immediate consequences of this reducibility are similar to the beginning of Section 3.4.

Let $\bar{r} : G_{F^+,S} \to \mathcal{G}_n(k)$ be a homomorphism with $G_{F,S} = \bar{r}^{-1}(\mathrm{GL}_n \times \mathrm{GL}_1)(k)$. The composite $G_{F,S} \to (\mathrm{GL}_n \times \mathrm{GL}_1)(k) \to \mathrm{GL}_n(k)$ will still be denoted $\bar{r}$. Suppose $\bar{r}|_{G_{F(\zeta_p),S}}$ is reducible, where ζ_p is a primitive p-th root of unity. By Clifford theory, the restriction is semisimple, and there is a decomposition

$$k^n \cong a \bigoplus_{i=1}^{m} S_i,$$

where the S_i are simple $k[G_{F(\zeta_p),S}]$-modules, and the $\dim S_i$ is independent of i, call it d. By dimension counting, we get $n = amd$. Suppose $a = 1$, $m = n$, and $d = 1$. (As a side note, observe if n is prime and the restriction is reducible, then the only other case is the one in which there is only one isotypic component.) This means $\bar{r}|_{G_{F(\zeta_p),S}}$ is the direct sum of n distinct characters. Assuming $\bar{r}|_{G_{F,S}}$ is irreducible, then letting $D = [F(\zeta_p) : F]$, Clifford theory says that $n|D$ (which implies $p \equiv 1 \bmod n$) and $\bar{r}|_{G_{F,S}}$ is induced from a character $\bar{\chi}$ of $G_{K,S}$, where K/F is the (unique) degree n extension contained in $F(\zeta_p)/F$. Moreover, G_F/G_K is cyclic of order n, and if σ is a generator, then

$$\bar{r}|_{G_{K,S}} = \bigoplus_{i=0}^{n-1} \bar{\chi}^{\sigma^i},$$

where $\bar{\chi}^{\sigma^i}(\tau) = \bar{\chi}(\sigma^{-i}\tau\sigma^i)$.

4.5 Decomposition of ad

Write $\mathrm{GL}_n(k) = \mathrm{GL}(V)$. The adjoint representation of V is $\mathrm{ad}(V) = \mathrm{End}(V)$, so $\mathrm{ad}(V) = V \otimes V^*$. As a $G_{K,S}$-representation, $\mathrm{ad}(V)$ therefore decomposes as

$$\begin{aligned} \mathrm{ad}(V) &= \left(\bar{\chi} \oplus \bar{\chi}^{\sigma} \oplus \cdots \oplus \bar{\chi}^{\sigma^{n-1}}\right) \otimes \left(\bar{\chi}^{-1} \oplus (\bar{\chi}^{\sigma})^{-1} \oplus \cdots \oplus (\bar{\chi}^{\sigma^{n-1}})^{-1}\right) \\ &= \mathbb{I}^{\oplus n} \oplus \bigoplus_{0 \le i < j \le n-1} \left(\bar{\chi}^{\sigma^i}/\bar{\chi}^{\sigma^j} \oplus \bar{\chi}^{\sigma^j}/\bar{\chi}^{\sigma^i}\right). \end{aligned}$$

Namely, identifying $\mathrm{ad}(V) = M_n(k)$, this decomposition is a reflection of that fact that $G_{K,S}$ acts trivially on the diagonal entries and acts on the (i,j)-entry via $\bar{\chi}^{\sigma^{i-1}}/\bar{\chi}^{\sigma^{j-1}}$. For each $j \geq 1$, $\bar{\chi}/\bar{\chi}^{\sigma^j}$ has n distinct conjugates, and therefore $\mathrm{Ind}_K^F(\bar{\chi}/\bar{\chi}^{\sigma^j})$ is an irreducible subrepresentation of $\mathrm{ad}(V)$.

Remark 4.5.1. The fact that $\mathrm{Ind}_K^F(\bar{\chi}/\bar{\chi}^{\sigma^j})$ is irreducible is from Clifford theory, and $\mathrm{Ind}_K^F(\bar{\chi}/\bar{\chi}^{\sigma^j})$ is a subrepresentation of $\mathrm{ad}(V)$ by Frobenius reciprocity.

While $\mathrm{Ind}_K^F \mathbb{I}$ is not irreducible, it is a $G_{F,S}$-subrepresentation of $\mathrm{ad}(V)$. By dimension counting, all the pieces are accounted for, and therefore

$$\mathrm{ad}(V) = \mathrm{Ind}_K^F \mathbb{I} \oplus \bigoplus_{j=1}^{n-1} \mathrm{Ind}_K^F(\bar{\chi}/\bar{\chi}^{\sigma^j}) = M_0 \oplus M_1,$$

where $M_0 = \mathrm{Ind}_K^F \mathbb{I}$ and $M_1 = \bigoplus_{j=1}^{n-1} \mathrm{Ind}_K^F(\bar{\chi}/\bar{\chi}^{\sigma^j})$. Notice that this is precisely what occurred in the Section 3.4, and this takes care of item (1) in Section 4.3.

4.6 Modified Taylor-Wiles Primes

We can now move to point (2) of Section 4.3 in trying to define appropriate local deformation problems. It is important that the tangent space respect the decomposition of $\mathrm{ad}\,\bar{r}$ above.

There is a modification of Taylor-Wiles primes, first introduced in [39], which we can use to kill the $M_0(1)$ portion of the dual Selmer group. What we do not have as of yet is an analogue of the deformation condition $\mathcal{D}_v^{\mathrm{St}(\alpha_v)}$ from Section 3.4. This will be talked about more in the section on future work. We can, however, define these modified Taylor-Wiles primes.

Suppose $q_{\tilde{v}} \equiv 1 \bmod p$, and that $\bar{r}$ is unramified at $\tilde{v}$. Write $\bar{r}|_{G_{F_{\tilde{v}}}} = \bar{\psi}_v \oplus \bar{s}_v$, where $\bar{\psi}_v$ is an eigenspace of Frobenius corresponding to an eigenvalue α_v on which $\mathrm{Frob}_{\tilde{v}}$ acts semisimply. Let $\mathcal{D}_v^{JT}$ be the set of lifts which are strictly equivalent to one of the form $\psi_v \oplus s_v$, where s_v is an unramified lift of $\bar{s}_v$ and does not contain ψ_v as a subquotient, and ψ_v may be ramified but the image of inertia under ψ_v is contained in the set of scalar matrices.

Thus $\mathcal{L}_v^{JT}$ is the subspace of

$$H^1(G_{F_{\tilde{v}}}, \mathrm{ad}(\bar{r})) = H^1(G_{F_{\tilde{v}}}, \mathrm{ad}(\bar{\psi}_v)) \oplus H^1(G_{F_{\tilde{v}}}, \mathrm{ad}(\bar{s}_v))$$

whose projection to $H^1(I_{F_{\tilde{v}}}, \mathrm{ad}(\bar{s}_v))$ is trivial and the projection to $H^1(I_{F_{\tilde{v}}}, \mathrm{ad}(\bar{\psi}_v))$ actually lives in $H^1(I_{F_{\tilde{v}}}, Z(\bar{\psi}_v))$.

It turns out these primes will do the work of killing the $M_0(1)$ portion of the mod p dual Selmer group. The following is an easy lemma:

Lemma 4.6.1. Suppose $v \nmid p$ is a finite place of F^+ which splits in F and suppose that the local deformation problem $\mathcal{D}_v^{JT}$ is defined. Then both $\mathcal{L}_v$ and $\mathcal{L}_v^\perp$ respect the decomposition $\mathrm{ad}(\bar{r}) = M_0 \oplus M_1$. That is:

(1) $\mathcal{L}_v = (\mathcal{L}_v \cap H^1(G_{F_{\tilde{v}}}, M_0)) \oplus (\mathcal{L}_v \cap H^1(G_{F_{\tilde{v}}}, M_1))$, and

(2) $\mathcal{L}_v^\perp = (\mathcal{L}_v^\perp \cap H^1(G_{F_{\tilde{v}}}, M_0(1))) \oplus (\mathcal{L}_v^\perp \cap H^1(G_{F_{\tilde{v}}}, M_1(1)))$.

Proof. We know v splits in F, and if $\tilde{v}$ is a prime of F above v, then the condition $q_{\tilde{v}} \equiv 1 \bmod p$ means $\tilde{v}$ splits in K (as it splits in $F(\zeta_p)$). Thus $\mathrm{ad}\,\bar{r}$ splits into the direct sum of 1-dimensional modules as a $k[G_{F_{\tilde{v}}}]$-module, from which the lemma follows easily. □

4.7 Killing Dual Selmer

Suppose $\mathcal{S} = (F/F^+, S, \tilde{S}, \mathcal{O}, \bar{r}, \chi, \{\mathcal{D}_v\}_{v \in S})$ is a global deformation problem and $T \subset S$ a set of places containing all those above p. Suppose that for each $v \in S \backslash T$, the deformation problem $\mathcal{D}_v$ has a tangent space $\mathcal{L}_v$ which respects the decomposition of $\mathrm{ad}\,\bar{r}$. Then as in [41] and the previous chapter, the dual Selmer group decomposes as

$$H^1_{\mathcal{L}^\perp, T}(G_{F^+,S}, \mathrm{ad}(\bar{r})(1)) = H^1_{\mathcal{L}^\perp, T}(G_{F^+,S}, M_0(1)) \oplus H^1_{\mathcal{L}^\perp, T}(G_{F^+,S}, M_1(1)).$$

The object is to kill this dual Selmer group, and so we can just work to add primes to S so that each summand vanishes. As mentioned in the previous section, we need to find an appropriate deformation condition which does the job of killing the $M_1(1)$ portion, and such that we can prove a proposition which mirrors Proposition 3.4.12.

However, using primes for which the deformation problem $\mathcal{D}_v^{JT}$ is defined, we can kill the $M_0(1)$ portion.

In [39], the author defines what it means for a subgroup $G \subseteq \mathrm{GL}_n(k)$ to be adequate, which built off a definition of a big subgroup in [6]. We will not need that full notion, so let us make the following definition.

Definition 4.7.1. (1) Let $G \leq GL_n(k) = GL(V)$ be a subgroup. Then G is *sufficient* if for every irreducible $k[G]$-submodule $W \subset \mathrm{ad}^0(V)$, there exists $g \in G$ with an eigenavalue α with $\mathrm{tr}\, e_{g,\alpha} W \neq 0$, where $e_{g,\alpha} : V \to V$ is the g-equivariant projection onto the generalized α-eigenspace of V.

(2) Let $G \leq \mathcal{G}_n(k)$ be a subgroup. Then G is *sufficient* if for every irreducible $k[G]$-submodule $W \subset \mathrm{ad}(V)$, there exists $g \in G \cap \mathcal{G}_n^0(k)$ with an eigenvalue α such that $\mathrm{tr}\, e_{g,\alpha} W \neq 0$.

Remark 4.7.2. As sufficiency is just the fourth condition of adequacy from [39], we have big $\Longrightarrow$ adequate $\Longrightarrow$ sufficient.

Theorem 4.7.3. Suppose $p > 2$ and satisfies the necessary congruence conditions as above. Suppose we are given a deformation problem

$$\mathcal{S} = (F/F^+, S, \tilde{S}, \mathcal{O}, \bar{r}, \chi, \{\mathcal{D}_v\}_{v \in S}),$$

and $T \subset S$ is a subset containing the places above p and where for $v \in S - T$, the corresponding $\mathcal{L}_v$ decomposes according to the decomposition of $\mathrm{ad}(\bar{r})$ as in the previous section. Suppose further that $h^1_{\mathcal{L}^\perp, T}(G_{F^+,S}, M_1(1)) = 0$, and let $N \geq 1$ be an integer. Finally, assume that $\bar{r}(G_{F^+(\zeta_p)})$ is sufficient. Then there are sets Q and $\tilde{Q}$ such that:

(1) $|Q| = h^1_{\mathcal{L}^\perp, T}(G_{F^+,S}, M_0(1))$, and for each $q \in Q$, $q_v \equiv 1 \bmod p^N$.

(2) The augmented deformation problem

$$\mathcal{S}[Q] = (F/F^+, S \cup Q, \tilde{S} \cup \tilde{Q}, \mathcal{O}, \bar{r}, \chi, \{\mathcal{D}_v\}_{v \in S \cup Q}),$$

where for $v \in Q$, $\mathcal{D}_v = \mathcal{D}_v^{JT}$, satisfies $H^1_{\mathcal{L}[Q]^\perp, T}(G_{F^+, S \cup Q}, \mathrm{ad}(\bar{r})(1)) = 0$.

Proof. Let $m = h^1_{\mathcal{L}^\perp,T}(G_{F^+,S}, M_0(1))$, and suppose $m \geq 1$. Observe that $(\mathcal{L}_v^{JT})^\perp$ is the subspace of unramified cohomology classes in $H^1(G_{F_{\tilde{v}}}, \mathrm{ad}(\bar{r})(1))$ whose projection to $H^1(G_{F_{\tilde{v}}}, \mathrm{ad}(\bar{\psi}_v)(1))$ actually takes values in $H^1(G_{F_{\tilde{v}}}, \mathrm{ad}^0(\bar{\psi}_v)(1))$. Thus, if $v \notin S$ satisfies $q_v \equiv 1 \bmod p$, then

$$h^1_{\mathcal{L}[\{v\}]^\perp,T}(G_{F^+,S\cup\{v\}}, M_1(1)) = h^1_{\mathcal{L}^\perp,T}(G_{F^+,S}, M_1(1)) = 0.$$

We have an exact sequence

$$0 \to H^1_{\mathcal{L}[Q]^\perp,T}(G_{F^+,S\cup Q}, M_0(1)) \to H^1_{\mathcal{L}^\perp,T}(G_{F^+,S}, M_0(1)) \to \bigoplus_{v\in Q} k,$$

where the last map is given by $[\phi] \mapsto (\mathrm{tr}\, e_{\mathrm{Frob}_{\tilde{v}},\alpha_v}\phi(\mathrm{Frob}_{\tilde{v}}))_{v\in Q}$. Let $[\phi] \in H^1_{\mathcal{L}^\perp,T}(G_{F^+,S}, M_0(1))$ be a nonzero class. We want a place v of F^+, with $v \notin S$, such that v splits in $F(\zeta_{p^N})$ and $\mathrm{tr}\, e_{\mathrm{Frob}_{\tilde{v}},\alpha_v}\phi(\mathrm{Frob}_{\tilde{v}}) \neq 0$. By Cebotarev, it suffices to find $\sigma_0 \in G_{F(\zeta_{p^N})}$ with $\mathrm{tr}\, e_{\sigma_0,\alpha}\phi(\sigma_0) \neq 0$ for some eigenvalue α of $\bar{r}(\sigma_0)$.

Now, as $M_0(1)^{G_{F^+(\zeta_{p^N})}} = 0$, inflation-restriction yields

$$0 \to H^1(G_{F^+,S}, M_0(1)) \to H^1(G_{F^+(\zeta_{p^N})}, M_0(1)).$$

Thus ϕ is nonzero after restricting to $G_{F^+(\zeta_{p^N})}$. Moreover, as $[F(\zeta_{p^N}) : F^+(\zeta_{p^N})] \leq 2$ and $p > 2$, Lemma 2.2.8 yields an injection

$$0 \to H^1(G_{F^+(\zeta_{p^N})}, M_0(1)) \to H^1(G_{F(\zeta_{p^N})}, M_0(1))^{G_{F^+(\zeta_{p^N})}} = \mathrm{Hom}_{G_{F^+(\zeta_{p^N})}}(G_{F(\zeta_{p^N})}, M_0(1)).$$

Thus $\phi(G_{F(\zeta_{p^N})})$ is a nonzero $G_{F^+(\zeta_{p^N})}$-submodule of $M_0(1)$. Thus the existence of σ_0 and α follow from the definition of sufficiency. □

4.8 Future Work

We have already outlined a few things that need to be done, but here we expand on the checklist of things still left to do to complete this project.

Firstly, in order to complete the Galois theory arguments of the previous section, there needs to be a deformation problem $\mathcal{D}_v$ such that:

- The tangent space $\mathcal{L}_v$ respects the decomposition of $\operatorname{ad} \bar{r}$.

- The intersection of $\mathcal{L}_v$ with $H^1(G_{F_{\tilde{v}}}, M_1(1))$ lies in the unramified cohomology $H^1_{\mathrm{ur}}(G_{F_v}, M_1(1))$. This is necessary to have an exact sequence similar to the one used in the proof of Proposition 3.4.12.

- The deformation problem can be used in some level raising arguments similar to the ones used in the previous chapter. The issue here is the yet unproven Ihara's lemma for GL_n (for $n > 2$). In the previous chapter, there was no explicit mention of the lemma (which is known for GL_2), but it does appear in the proof of Lemma 3.2.11 (see [41] for details).

A potential candidate for such a deformation problem can be found in [6] and [40]. However, this has not been thoroughly examined, and it will certainly need to be the first order of business before continuing.

After this is done, the automorphic arguments need to be filled in. At this point in time, no work on this aspect of the argument has been done. Certainly, both [6] and [39] will be extraordinarily useful, but once again Ihara's lemma will be one of the major obstacles. Analogues of Lemma 3.2.11 and Corollary 3.2.13 will need to be proven, and this will also be closely tied to the Galois work mentioned above.

CHAPTER 5

Generic Unobstructedness

This chapter, the final of the dissertation, details work completed jointly with Chandrashekhar Khare, Gebhard Böckle, and David Guiraud. The project is computational in nature, and does not address one question in particular, but rather a broad idea which is examined in several specific situations. The chapter begins by describing possible motivation for the type of question being asked. We then state a result of Weston which shows how one may obtain results using $R = \mathbb{T}$ theorems. The situations new to this dissertation are ones where this $R = \mathbb{T}$ machinery does not exist, and as such, theorems are hard to prove. However, we describe heuristics and expectations, and provide some computer evidence for these heuristics.

5.1 Motivation

Let F be a number field, and let r_1 and r_2 denote the number of real and complex places of F, respectively. Note that $[F : \mathbb{Q}] = r_1 + 2r_2$. The following is a famous conjecture of Leopoldt.

Conjecture 5.1.1 (Leopoldt)**.** The number of $\mathbb{Z}_p$-extensions of F is $r_2 + 1$.

Put another way, it asserts that the Galois group of the maximal pro-p extension of F unramified outside the places above p and infinity has $\mathbb{Z}_p$-rank equal to $r_2 + 1$. This question can be framed in terms of Galois cohomology as well. Indeed, consider the group $G_{F,S}$, where $S = S_p \cup S_\infty$ (the places above p and the places above infinity), and let it act trivially on $\mathbb{Z}_p$. Then as in Section 2.2.2.2, the cohomology group $H^1(G_{F,S}, \mathbb{Z}_p) = \mathrm{Hom}_{\mathrm{cts}}(G_{F,S}, \mathbb{Z}_p)$. Thus, Leopoldt's conjecture can be stated in terms of the $\mathbb{Z}_p$-rank of this cohomology group.

Indeed, Leopoldt's conjecture is equivalent to the assertion that

$$\operatorname{rank}_{\mathbb{Z}_p} H^1(G_{F,S}, \mathbb{Z}_p) = r_2 + 1.$$

Using the global Euler-Poincaré characteristic formula (Theorem 2.2.22), this is equivalent to $\operatorname{rank}_{\mathbb{Z}_p} H^2(G_{F,S}, \mathbb{Z}_p) = 0$, which means $H^2(G_{F,S}, \mathbb{Z}_p)$ is finite. By considering the tensor product of each of these two $\mathbb{Z}_p$-modules with $\mathbb{Q}_p$, the conjecture is equivalent to $\dim_{\mathbb{Q}_p} H^1(G_{F,S}, \mathbb{Q}_p) = r_2 + 1$ and also to $\dim_{\mathbb{Q}_p} H^2(G_{F,S}, \mathbb{Q}_p) = 0$.

Recall from Section 2.3.3 that the vanishing of second cohomology groups is important in deformation theory, as it says that an associated lifting problem is unobstructed. For this reason, the focus will be on this final form of Leopoldt's conjecture.

An interesting question to ask is whether there is a mod p analogue:

Question 5.1.2. Is $H^2(G_{F,S}, \mathbb{Z}/p\mathbb{Z}) = 0$ for almost all primes p?

Remark 5.1.3. Here, "almost all" can mean either "all but finitely many" or "all outside a set of density zero." Indeed, we would be satisfied with either answer.

Note that, by the global Euler-Poincaré characteristic formula, Question 5.1.2 is equivalent to $\dim H^1(G_{F,S}, \mathbb{Z}_p) = r_2 + 1$, which confirms Leopoldt's conjecture for the primes in question.

Question 5.1.2 has an affirmative answer when $F = \mathbb{Q}$. Indeed, the group $H^2(G_{\mathbb{Q},S}, \mathbb{Z}/p\mathbb{Z}) = 0$ for all $p > 2$ and $\dim H^2(G_{\mathbb{Q},S}, \mathbb{Z}/2\mathbb{Z}) = 1$ when $p = 2$. This follows from the fact that when p is odd there is a unique Galois extension of $\mathbb{Q}$ of degree p unramified outside p and ∞, whereas when $p = 2$ there are two such extensions, namely $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$.

The question also has an affirmative answer when F is an imaginary quadratic field. However, if F is a real quadratic field, then the answer is unknown, despite the fact that $H^2(G_{F,S}, \mathbb{Q}_p) = 0$ is easy.

One way to view Question 5.1.2 is the following: view $\mathbb{Z}/p\mathbb{Z}$ as a trivial representation of $G_{F,S}$, so the adjoint representation $\operatorname{ad} \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ as a $G_{F,S}$-module. Thus, the question is asking for the unobstructedness of the trivial representation, and whether this happens "generically."

In this chapter, we will be asking questions related to the vanishing of this second cohomology group with coefficients arising from compatible systems of representations. In general, proving the “generic vanishing” (which will be defined in the next section) is difficult, but we can examine the question in various settings and make guesses as to the answer and the heuristics behind them.

5.2 Modular Forms Setting

Before giving the definition of generic unobstructedness, we recall a result of Weston which gives the type of answer we are looking for. Let f be a newform of level N, weight $k \geq 2$, and character χ, and let $K = \mathbb{Q}(a_n(f))$ denote the number field gotten by adjoining the Fourier coefficients of the q-expansion of f. Let S denote a finite set of places of $\mathbb{Q}$, including all primes dividing N and the infinite place. Section 2.1.1.3 introduced the representations $\rho_{f,\lambda}$ and the residual representations $\bar{\rho}_{f,\lambda}$ for finite places λ of F. The collection of $(\rho_{f,\lambda})_\lambda$, as λ ranges over the finite places of F, form a compatible system in the sense of Section 2.1.4.

Let $R_{f,S,\lambda}$ be the universal deformation ring parametrizing deformations of $\bar{\rho}_{f,\lambda}$ which are unramified outside $S \cup \{l\}$, where l denotes the residue characteristic of λ. Weston [43, Section 5.3] proved the following:

Theorem 5.2.1. (1) If $k \geq 3$, then for almost all but finitely many places λ, the deformation ring is unobstructed, i.e. $H^2(G_{\mathbb{Q},S\cup\{l\}}, \mathrm{ad}(\bar{\rho}_{f,\lambda})) = 0$ and $R_{f,S,\lambda} \cong W(k_\lambda)[[X_1, X_2, X_3]]$.

(2) If $k = 2$, then the above is true for all λ outside a set of places of density zero. More precisely, it is true for all but finitely many λ such that $a_l(f)^2 \neq \epsilon(l) \bmod \lambda$.

Sketch of Proof. For the full proof of the theorem, see [43, Section 5.3]. The sketch is as follows. Consider the minimal deformation ring R associated to $\bar{\rho}_{f,\lambda}$, where λ is of characteristic $l \gg 0$. By the modularity lifting theorems of Wiles and Taylor-Wiles, one shows that R is isomorphic to a Hecke ring acting on $S_2(\Gamma_1(N), \mathcal{O})_{\mathfrak{m}_\lambda}$. This Hecke ring is isomorphic to $W(k_\lambda)$, whence the isomorphism $R \cong W(k_\lambda)$ follows. Thus, the Zariski tangent space of R is trivial, which means that a Selmer group $H^1_{\mathcal{L}}(G_{\mathbb{Q},S\cup\{l\}}, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})) = 0$. One then applies the

Greenberg-Wiles formula to obtain the vanishing of the corresponding dual Selmer group $H^1_{\mathcal{L}^\perp}(G_{\mathbb{Q},S\cup\{l\}}, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})(1)) = 0$.

Poitou-Tate yields the following exact sequence:

$$0 \to H^1(G_{\mathbb{Q},S\cup\{l\}}, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})) \to \bigoplus_{v\in S\cup\{l\}} H^1(\mathbb{Q}_v, \mathrm{ad}^0(\bar{\rho}_{f,\lambda}))/\mathcal{L}_v \to$$

$$0 \to H^2(G_{\mathbb{Q},S\cup\{l\}}, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})) \to \bigoplus_{v\in S\cup\{l\}} H^2(\mathbb{Q}_v, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})) \to H^0(G_{\mathbb{Q}}, \mathrm{ad}^0(\bar{\rho}_{f,\lambda})(1)).$$

If $k > 2$, then the local H^2-terms vanish for sufficiently large l. If $k = 2$, then the local term $H^2(\mathbb{Q}_l, \mathrm{ad}^0(\bar{\rho}_{f,\lambda}))$ may not vanish if l is in the exceptional set of primes described in the theorem. This is why the two cases are split in the statement of the theorem. □

In the spirit of the above theorem, we make the following definition.

Definition 5.2.2. Let F be a number field, and let $(\rho_\lambda : G_F \to \mathrm{GL}_n(\overline{K}_\lambda))_\lambda$ be a compatible system of Galois representations with ramification set S, where λ runs over the set of finite places of some number field K. Let $\bar{\rho}_\lambda : G_F \to \mathrm{GL}_n(k_\lambda)$ denote the residual representations. Then the compatible system is called generically unobstructed if $H^2(G_{F,S\cup\{l\}}, \mathrm{ad}\,\bar{\rho}_\lambda) = 0$ for almost all λ, where l is the residue characteristic of λ.

5.3 Wieferich Primes

The sketch of the proof of Theorem 5.2.1 took advantage of the existence of an $R = \mathbb{T}$ theorem. In general, this tool will not exist for the situations we want to consider, so instead we are left to describe heuristics for the various settings and examine them computationally. The overarching theme of the heuristics throughout the chapter is illustrated by Wieferich primes.

Definition 5.3.1. A prime p of $\mathbb{Z}$ is a Wieferich prime if $2^{p-1} \equiv 1 \bmod p^2$.

Since $2^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem, Wieferich primes require divisibility by an additional power of p. Such primes are connected to Fermat's Last Theorem, but it is unknown whether infinitely many Wieferich primes exist. However, there are guesses as to how many there should be, based on the following heuristic argument.

Since $2^{p-1} \equiv 1 \bmod p$, the number 2^{p-1} modulo p^2 must be of the form $2^{p-1} \equiv 1 + kp \bmod p^2$, where $0 \leq k \leq p-1$. If $k = 0$, then p is a Wieferich prime. Treating this as a genuinely random event where each possible k is equally likely, the probability of this happening should be $1/p$. If the primes are treated as "independent events," then the number of Wieferich primes less than or equal to X can roughly be modeled by

$$\sum_{p \leq X} \frac{1}{p} \sim \log(\log(X)).$$

Perhaps the better way to view this analysis is the following. There is a set, in this case $K = \ker(\mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z})$, and a desired point, namely $1+p^2\mathbb{Z} \in K$. The analysis comes from treating the object $2^{p-1} + p^2\mathbb{Z} \in K$ as a random point in K, and asking for the probability that this random point is the desired target point.

5.4 Trivial Motive

We return to Question 5.1.2. To remind the reader of the notation, F is a number field, and $S = S_p \cup S_\infty$. The goal is to examine $H^2(G_{F,S}, \mathbb{Z}/p\mathbb{Z})$.

By the Euler-Poincaré characteristic formula, if $h^i = \dim_{\mathbb{Z}/p\mathbb{Z}} H^i(G_{F,S}, \mathbb{Z}/p\mathbb{Z})$, then

$$h^1 = 1 + h^2.$$

If p does not divide the class number of F, the group $H^1(G_{F,S}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G_{F,S}, \mathbb{Z}/p\mathbb{Z})$ is dual to the p-part of the ray class group of F of conductor p^2. Therefore, there is an exact sequence

$$1 \to \frac{\mathcal{O}_F^\times \cap (1 + p\mathcal{O}_F)}{\mathcal{O}_F^\times \cap (1 + p^2\mathcal{O}_F)} \to \frac{(1 + p\mathcal{O}_F)}{(1 + p^2\mathcal{O}_F)} \to H^1(G_{F,p}, \mathbb{Z}/p\mathbb{Z})^\vee \to 1.$$

By counting dimensions, we see that

$$h^1 = 2 - \dim_{\mathbb{Z}/p\mathbb{Z}} \frac{\mathcal{O}_F^\times \cap (1 + p\mathcal{O}_F)}{\mathcal{O}_F^\times \cap (1 + p^2\mathcal{O}_F)}.$$

Comparing the two expressions, the dimension $h^2 = 0$ precisely when

$$\dim_{\mathbb{Z}/p\mathbb{Z}} \frac{\mathcal{O}_F^\times \cap (1 + p\mathcal{O}_F)}{\mathcal{O}_F^\times \cap (1 + p^2\mathcal{O}_F)} = 1.$$

If ϵ denotes the fundamental unit of F, then $h^2 \neq 0$ is the same as saying that $\epsilon^{p^2-1} \in \mathcal{O}_F^\times \cap (1 + p\mathcal{O}_F)$ is p-th power. Equivalently, that $\epsilon^{p^2-1} \equiv 1 \bmod p^2\mathcal{O}_F$. One would expect this to happen with probability $1/p$, and so the number of primes p up to X for which $h^2 \neq 0$ should be

$$\sum_{p \leq X} \frac{1}{p},$$

which again grows like $\log(\log(X))$ as in the Wieferich primes setting. From this, we should expect a density one set of primes for which $H^2(G_{F,S}, \mathbb{Z}/p\mathbb{Z}) = 0$. We used magma to check the primes $1 < p < 10000$ for which $H^2(G_{F,S}, \mathbb{Z}/p\mathbb{Z}) \neq 0$ as F ranges over real quadratic fields $F = \mathbb{Q}(\sqrt{D})$ for $2 \leq D \leq 30$. The data is shown in Table 5.1 at the end of the chapter. In these small cases, the nonvanishing of $H^2(G_{F,S}, \mathbb{Z}/p\mathbb{Z})$ seems to be quite rare. One should check a larger set of primes to see if the $\log(\log(X))$ heuristic holds.

5.5 Weight 2 forms

Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ be a representation, where k is a finite field of characteristic p. Suppose $\bar{\rho}$ arises from $S_2(\Gamma_0(N))$, corresponding to a maximal ideal $\mathfrak{m}$ of the Hecke algebra acting on this space. The set X of primes q such that $\bar{\rho}(\mathrm{Frob}_q)$ has eigenvalues with ratio q has positive density. Let $q \in X$, and let $\mathfrak{m}'$ denote the maximal ideal of the Hecke algebra acting on $S_2(\Gamma_0(Nq))$, which is the same as $\mathfrak{m}$ away from q, and such that $U_q^2 - 1 \in \mathfrak{m}'$. The question we want to ask is the following:

Question 5.5.1. Is $\dim S_2(\Gamma_0(Nq))_{\mathfrak{m}'}^{q-new} = 1$ for a density one set of primes $q \in X$?

We have analyzed this question a bit in the case $N = 11$ and $p = 11$, building off numerical investigations carried out by Tommaso Centeleghe. In this case $S_2(\Gamma_0(11), \mathbb{F}_{11}) = S_{12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_{11}) = \mathbb{F}_{11} \cdot \Delta$ as Hecke modules, where Δ denotes the Ramanujan delta function with Fourier coefficients $\tau(n)$. Suppose $\bar{\rho} = \bar{\rho}_{\Delta,11}$, and consider primes q for which $\tau(q) \equiv$

$\pm(q+1) \bmod 11$. Question 5.5.1 in this setting asks whether there is a unique q-new form in $S_2(\Gamma_0(11q))$ which gives rise to $\bar{\rho}$.

Before presenting our findings, we analyze this problem from a deformation theory perspective. Consider as before the primes q for which Ribet's level raising condition $\tau(q) \equiv \pm(q+1) \bmod 11$ is satisfied, but ignore those primes for which $q \equiv 1 \bmod 11$ and $\bar{\rho}(\mathrm{Frob}_q)$ is a scalar matrix. Let R denote the deformation ring parametrizing deformations of $\bar{\rho}$ which are unramified outside 11 and q, and which at 11 and q are of the form

$$\begin{pmatrix} \epsilon_{11} & * \\ 0 & 1 \end{pmatrix},$$

(up to sign) where ϵ_{11} denotes the 11-adic cyclotomic character. (The reason for ignoring the primes 1 mod 11 for which $\bar{\rho}(\mathrm{Frob}_q)$ is scalar is that the problem may not be representable in this case.) The cases $q \not\equiv -1 \bmod 11$ and $q \equiv -1 \bmod 11$ behave slightly differently.

The tangent space for this deformation problem is given by a Selmer group. Indeed, the local problems at 11 and q give subspaces $\mathcal{L}_v \subset H^1(G_{\mathbb{Q}_v}, \mathrm{ad}^0(\bar{\rho}))$ for $v \in \{11, q\}$. If $\mathcal{L} = (\mathcal{L}_v)_{v \in \{11,q\}}$, then the tangent space is the Selmer group $H^1_{\mathcal{L}}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho}))$, where $S = \{11, q\}$. By the Greenberg-Wiles formula, we have

$$\dim H^1_{\mathcal{L}}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho})) \leq \dim H^0(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho})(1)) = \begin{cases} 2 & \text{if } q \equiv -1 \bmod 11 \\ 1 & \text{if } q \not\equiv \pm 1 \bmod 11 \end{cases}.$$

We have the following dimensions of the local problems:

$$q \equiv -1 \bmod 11: \quad \dim H^1(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho})) = 3, \quad \dim \mathcal{L}_q = 1,$$

$$q \not\equiv \pm 1 \bmod 11: \quad \dim H^1(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho})) = 2, \quad \dim \mathcal{L}_q = 1.$$

Now let us consider a relaxed Selmer group. Define $\mathcal{L}' = (\mathcal{L}'_v)_{v \in \{11,q\}}$, where $\mathcal{L}'_{11}$ corresponds to the ordinary condition above, but at q there is no condition imposed, meaning $\mathcal{L}'_q = H^1(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho}))$. Consider the Selmer group $H^1_{\mathcal{L}'}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho}))$. Let R' be the universal deformation ring corresponding to this deformation problem, so that this relaxed Selmer group is the tangent space of R'. Then it is known $R' \cong \mathbb{T}$, where $\mathbb{T}$ is the Hecke algebra acting on $S_2(\Gamma_0(11))$, a one-dimensional space. Greenberg-Wiles then gives that

$$\dim H^1_{\mathcal{L}'}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho})) = \dim H^0(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho})(1)).$$

We want to compute $\dim H^1_{\mathcal{L}}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho}))$, and to do that we need to see what the image of our relaxed Selmer group is in the local cohomology $H^1(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho}))$, and compare this image to the line given by $\mathcal{L}_q$ giving the local tangent space at q.

If $q \not\equiv -1 \bmod 11$, then the image overlaps with $\mathcal{L}_q$ if and only if they are the same line in $H^1(G_{\mathbb{Q}_q}, \mathrm{ad}^0(\bar{\rho}))$. We know $\mathcal{L}_q$ is not the unramified line. The probability that a random line in $\mathbb{F}_{11}^2$ is the same as our given line is therefore $1/11$, as there are 11 distinct 1-dimensional subspaces of $\mathbb{F}_{11}^2$ once the distinguished unramified line is removed.

If $q \equiv -1 \bmod 11$, then the probability that the two subspaces intersect is the same as the probability of a random hyperplane in $\mathbb{F}_{11}^3$ containing the given line $\mathcal{L}_q$. There are 145 total subspaces of $\mathbb{F}_{11}^3$ of dimension at most 2. There are 12 which contain the given line $\mathcal{L}_q$, so the probability of the two subspaces intersecting is roughly $12/145$.

Thus, it seems like $\dim H^1_{\mathcal{L}}(G_{\mathbb{Q},S}, \mathrm{ad}^0(\bar{\rho})) > 0$ roughly $1/12$ of the time, meaning $\dim S_2(\Gamma_0(11q))^{q-new}_{\mathfrak{m}'} > 1$ this often.

We used magma to see when there was a unique Ribet level-raising form congruent to Δ in $S_2(\Gamma_0(11q))^{q-new}$. It is easy to check which primes satisfy Ribet's level-raising condition: $\tau(q)^2 \equiv (q+1)^2 \bmod 11$. Table 5.2 (at the end of the chapter) gives all such q up to 10000.

For each such prime, there was a "coarse check" done to quickly determine whether there was a unique level-raising form. The check considered the l-th Hecke polynomial of the operator T_l acting on the two spaces $S_2(\Gamma_0(11), \mathbb{F}_{11})$ and $S_2(\Gamma_0(11q), \mathbb{F}_{11})$, call them $p_{l,s}$ and $p_{l,b}$, respectively (with s and b meaning smaller and bigger spaces). The polynomial $p_{l,b}$ will have $p_{l,s}$ as a factor. If the exponent is three, then uniqueness is shown, as two factors will come from the old forms and one from the (unique) q-new form.

The output of this quick check was a list of primes for which there was a unique form, and the rest were deemed "exceptional primes." The exceptional primes up to 10000 are:

$$593, 1117, 2221, 2767, 3187, 3251, 3331, 3343, 3557, 3727, 3761, 3889, 4241, 4243,$$

$$4483, 4817, 4861, 5081, 5387, 5521, 6271, 6959, 7451, 7937, 8053, 8093, 9007, 9221.$$

This set seems small compared to the number of primes for which the level-raising condition is satisifed. For these exceptional primes, a more thorough analysis was needed. In these cases, we simply tried to count the number of forms congruent to Δ modulo 11. For the primes 593 and 1117, magma produced precisely two level-raising forms, each prime containing two forms which happened to be Galois conjugates. For the larger primes, a more efficient algorithm will be necessary as the computation time was unreasonable.

5.6 Future Work

Jointly with Gebhard Böckle, David Guiraud, and Chandrashekhar Khare, this project will continue after the writing of this dissertation. There are two main questions we wish to study:

- Per a suggestion by Professor David Roberts, we will try a smaller prime than $p = 11$ for the setting of the previous section. Namely, instead of considering the mod 11 representation of the Δ function in $S_2(\Gamma_0(11), \mathbb{F}_{11})$, we can try to consider mod 3 or mod 5 coefficients in a different space of forms. We may be able to push our computations further to obtain more sets of data since right now there is an obstruction in the computational power of our algorithm.

- We can consider a similar question the p-adic weight one forms. Namely, given a classical form $f \in S_1(\Gamma_0(N))$, we can consider the forms in $S_p(\Gamma_1(N))^{\text{ord}}$ which are congruent to f. If this number is bounded, then the space of ordinary p-adic weight one forms localized at the maximal ideal associated to f is bounded in dimension.

In each case, it will probably be necessary to develop more efficient algorithms in order to avoid the computational obstructions we have hit so far. The last question, in particular, seems difficult at first glance, since the dimension of the space of weight p forms grows quickly with p.

5.7 Tables

D	p
2	13, 31
3	103
5	
6	7, 523
7	
10	191, 643
11	
13	241
14	2
15	181, 1039, 2917
17	
19	79
21	
22	43, 73, 409
23	7, 733
26	2683, 3967
29	3, 11

Table 5.1: Primes p to 10000 for which $H^2(G_{\mathbb{Q}(\sqrt{D}),S}, \mathbb{Z}/p\mathbb{Z}) \neq 0$

n	primes q with $n - 1000 < q \leq n$ which satisfy level raising condition
1000	59, 103, 151, 157, 179, 191, 193, 251, 281, 367, 379, 383, 397, 409, 419, 467, 491, 509, 541, 587, 593, 673, 701, 733, 743, 827, 883, 911, 937, 983
2000	1039, 1091, 1097, 1103, 1117, 1123, 1223, 1249, 1279, 1283, 1303, 1487, 1667, 1931, 1999
3000	2017, 2039, 2113, 2131, 2137, 2141, 2221, 2239, 2311, 2341, 2383, 2399, 2531, 2549, 2609 2633, 2689, 2741, 2767, 2791, 2801, 2897, 2971, 2999
4000	3037, 3061, 3083, 3109, 3137, 3163, 3187, 3229, 3251, 3331, 3343, 3391, 3449, 3491, 3539, 3557, 3659, 3677, 3691, 3727, 3761, 3767, 3793, 3823, 3847, 3889, 3917
5000	4013, 4241, 4243, 4283, 4373, 4397, 4441, 4451, 4481, 4483, 4513, 4517, 4523, 4583, 4637, 4639, 4649, 4691, 4759, 4787, 4817, 4861, 4877, 4889, 4919, 4933, 4987, 4993
6000	5081, 5087, 5101, 5171, 5231, 5281, 5303, 5387, 5443, 5449, 5521, 5563, 5749, 5839, 5857, 5987
7000	6047, 6053, 6067, 6151, 6163, 6221, 6271, 6299, 6301, 6317, 6323, 6329, 6367, 6427, 6571, 6701, 6719, 6829, 6857, 6949, 6959, 6977
8000	7027, 7057, 7103, 7109, 7129, 7283, 7297, 7307, 7333, 7351, 7417, 7451, 7547, 7559, 7561, 7673, 7703, 7717, 7789, 7817, 7823, 7883, 7993, 7937, 7949
9000	8053, 8069, 8093, 8287, 8291, 8297, 8363, 8377, 8419, 8423, 8429, 8501, 8537, 8669, 8677, 8753, 8839, 8867, 8923, 8941, 8971
10000	9007, 9067, 9187, 9221, 9337, 9467, 9533, 9587, 9689, 9721, 9739, 9787, 9791, 9851, 9941

Table 5.2: Primes q up to 10000 for which $\tau(q)^2 \equiv (q+1)^2 \bmod 11$

REFERENCES

[1] Patrick Allen. Modularity of nearly ordinary 2-adic residually dihedral galois representations. *Compositio Math.*, 150(8), 2014.

[2] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of calabi-yau varieties and potential automorphy ii. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[3] Laurent Berger. On p-adic galois representations. In *Elliptic Curves, Hilbert Modular Forms, and Galois Deformations*, pages 3–21. Springer Basel, 2013.

[4] Gebhard Böckle. Deformations of galois representations, 2011.

[5] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over q: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4), 2001.

[6] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l representations. *Pub. Math. IHES*, 108, 2008.

[7] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of certain potentially barsotti-tate galois representations. *Journal of the American Mathematical Society*, 12(2), 1999.

[8] Pierre Deligne. Formes modulaires et représentations l-adiques. *Séminaire N. Bourbaki*, 11:139–172, 1968-1969.

[9] Fred Diamond. On deformation rings and hecke rings. *Annals of Mathematics, Second Series*, 144(1), 1996.

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

[11] Jean-Marc Fontaine. Le corps des périodes p-adiques. *Astérisque*, (223):59–111, 1994.

[12] Jean-Marc Fontaine. Représentations p-adiques semi-stables. *Astérisque*, (223):113–184, 1994.

[13] Jean-Marc Fontaine and Yi Ouyang. Theory of p-adic galois representations.

[14] Nuno Freitas, Bao V. Le Hung, and Samir Sikek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201:521–567, 2015.

[15] Gerhart Frey. Links between solutions of $a-b=c$ and elliptic curves. In H.P. Schlickewei and E. Wirsing, editors, *Number Theory: Proceedings of the Journees Arithmetiques*. Springer-Verlag New York, 1989.

[16] Toby Gee. Modularity lifting theorems - notes for arizona winter school. 2013.

[17] Michael Harris and Richard Taylor. *The geometry and cohomology of some simple Shimura varieties*. Annals of Mathematics Studies. Princeton University Press, 2001.

[18] Guy Henniart. Caractérisation de la correspondance de langlands locale par les facteurs ϵ de paires. *Invent. Math.*, 113(2):339–350, 1993.

[19] Haruzo Hida. *Modular Forms and Galois Cohomology*. Cambridge University Press., 2000.

[20] Bao V. Le Hung. Modularity of some elliptic curves over totally real fields. *Preprint. Available at http://arxiv.org/abs/1309.4134*, 2013.

[21] Sudesh Kalyanswamy. Remarks on automorphy of residually dihedral representations. *Preprint. Available at https://arxiv.org/abs/1607.04750*, 2016.

[22] Chandrashekhar Khare. Modularity of p-adic galois representations via p-adic approximations. *Journal de Théorie des Nombres de Bordeaux*, 16(1), 2004.

[23] Chandrashekhar Khare and Jack Thorne. Automorphy of some residually dihedral galois representations, ii. *Preprint*, 2015.

[24] Robert P. Langlands. Base change for gl(2). *Annals of Mathematics Studies*, 96, 1980.

[25] Barry Mazur. Deforming galois representations. In *Galois Groups over Q*, volume 16, pages 385–437. Mathematical Sciences Research Institute Publications, 1989.

[26] Barry Mazur. An introduction to the deformation theory of galois representations. In *Modular Forms and Fermat's Last Theorem*, pages 243–311. Springer-Verlag New York, 1997.

[27] Jürgen Neukirch. *Class Field Theory*. Springer-Verlag Berlin Heidelberg, 2013.

[28] Kenneth A. Ribet. Report on mod l representations of gal($\overline{Q}/q$). In *Proceedings of Symposia in Pure Mathematics*, volume 55, pages 639–676, 1994.

[29] Kenneth A. Ribet and William A. Stein. Lectures on modular forms and hecke operators. 2011.

[30] Michael Schlessinger. Functors of artin rings. *Transactions of the American Mathematical Society*, pages 208–222, 1968.

[31] Jean-Pierre Serre. *Galois Cohomology*. Springer-Verlag Berlin Heidelberg, 1997.

[32] Joseph H. Silverman. A survey of the arithmetic theory of elliptic curves. In *Modular Forms and Fermat's Last Theorem*, pages 17–40. Springer-Verlag New York, 1997.

[33] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2009.

[34] CM. Skinner and Andrew J. Wiles. Nearly ordinary deformations of irreducible residual representations. *Annales de la Faculté des sciences de Toulouse : Mathématiques*, 10(1):185–215, 2001.

[35] Glenn Stevens. An overview of the proof of fermat's last theorem. In *Modular Forms and Fermat's Last Theorem*, pages 1–16. Springer-Verlag New York, 1997.

[36] Richard Taylor. Galois representations. *Annales de la Faculte des Sciences de Toulouse*, (13):73–119, 2004.

[37] Richard Taylor. On the meromorphic continuous of degree two l-functions. *Doc. Math.*, 2006.

[38] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l representations. ii. *Pub. Math. IHES*, 108, 2008.

[39] Jack Thorne. On the automorphy of l-adic galois representations with small residual image. *Journal of the Inst. of Math. Jussieu*, 11(4), 2012.

[40] Jack Thorne. Automorphy lifting for residually reducible l-adic galois representations. *Journal of the American Mathematical Society*, 2015.

[41] Jack Thorne. Automorphy of some residually dihedral galois representations. *To appear in Math. Annalen.*, 2015.

[42] Lawrence C. Washington. Galois cohomology. In Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 101–120. Springer-Verlag, 1997.

[43] Tom Weston. Unobstructed modular deformation problems. *American Journal of Mathematics*, 126(6), 2004.

[44] Andrew J. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics, Second Series*, 141(3), 1995.

[45] Andrew J. Wiles and Richard Taylor. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics, Second Series*, 141(3):553–572, 1995.