ABSTRACT

Title of dissertation: UNIVERSAL DEFORMATIONS AND *P*-ADIC *L*-FUNCTIONS

Arijit Sehanobish, Doctor of Philosophy, 2019

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

In this thesis we study deformations of certain 2-dimensional reducible representations whose image is in the Borel subgroup of $GL_2(\mathbb{F})$. Our method of understanding the universal deformation ring is via the Jordan-Hölder factors of the residual representation. Using the vanishing of cup products of appropriate cohomology classes we can compute the tangent space of the universal deformation ring and some obstruction classes to lifting representations. In this process, we can also explicitly construct certain big meta-abelian extensions inside the fixed field of the kernel of the universal representation. We give an explicit example of our construction of an unramified extension in the case of elliptic curves of conductor 11. We also give an Iwasawa theoretic description of various fields that are cut out by the universal representation. The Galois theoretic description of the constructed meta-abelian unramified extension is then later used as an ingredient for the isomorphism criterion in the modularity lifting results. When the isomorphism criterion is satisfied, we could prove some modularity lifting results allowing us to recover some results of Skinner-Wiles and prove a conjecture of Wake in this special case. We also show that the representations considered by Skinner-Wiles have big image inside the universal

deformation ring.

UNIVERSAL DEFORMATIONS AND *P*-ADIC *L*-FUNCTIONS

by

Arijit Sehanobish

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2019

Advisory Committee:
Professor Lawrence Washington, Chair
Professor Patrick Brosnan
Professor Thomas Haines
Professor Niranjan Ramachandran
Professor William Gasarch

Dedication

To my parents and to the wonderful Leah A. Drew.

Acknowledgments

It is nearly impossible to thank everyone that I have met in this long journey and had a hand in my successful completion of this dissertation. In fact, some of the people mentioned below might not remember their contribution, but their impact was substantial and will not be forgotten.

First and foremost, I would like to thank my adviser Lawrence Washington for being a truly great adviser. He has spent countless hours discussing various aspects of Iwasawa theory and carefully going through my thesis. Without his guidance, encouragement and perseverance, this thesis would not have been possible.

Next I would like to thank Professor Tom Haines for giving me the opportunity to spend a year in France. I will forever be grateful to the Hadamard Fondation for the generous support that allowed me to do research at Universite Paris Sud and to Universite Paris Sud for being a wonderful host. I would like to Professor Laurent Clozel for facilitating my visit there and also for patiently answering many questions about automorphic forms and Ihara's lemma. The main idea for this thesis came from long conversations with Olivier Fouquet who asked me to look at Skinner-Wiles and explaining the difficulties that the authors had to overcome. I thank him for that insight. Finally I thank Jacques Tilouine and Ariane Mezard for answering various questions about Eisenstein Hecke algebras and reducible representations.

I would finally like to express my gratitude to University of Maryland and to the many faculty members (including my thesis committee members) for making this a truly wonderful place to work.

I would also like to thank the close friends who were with me through this period of my life. Special thanks to (in no particular order) Giovanni, Arthur, Andrew, Arno, Przemyslaw, Richard, Ran, Alex, Sam, Jonathan, Catie, Amy, Tim and the list actually goes on. You know who you are and I appreciate your support.

My family: my parents. Well without them, I would not have been born. And to my girlfriend Leah Drew who has brightened up many a dreary day with her smile, love and encouragement.

Table of Contents

Chapter 1: Introduction

One of the central themes in modern number theory is to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The standard way to understand an abstract group is via representations which in this case are called Galois representations. A large class of naturally occurring representations comes from the etale cohomology of smooth projective varieties defined over $\mathbb{Q}$.

Definition 1.0.1. We call a Galois representation geometric if it occurs in a subquotient of the cohomology of a smooth projective variety.

Definition 1.0.2. Let c be a complex conjugation in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. A representation $\rho : G_{\mathbb{Q}} \to GL(V)$ is called odd if $\det(\rho(c)) = -1$

Conjecture 1.0.3. (Fontaine-Mazur): now a theorem by Breuil, Emerton, Kisin, Paskunas, Colmez et al (for $n = 2$): Any odd Galois representation $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{Q}_p)$ which is unramified outside a finite set of primes and De Rham at p is geometric.

In view of this theorem, it is natural to study $\mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q})$, i.e. the maximal extension unramified outside a finite set S. The first case of understanding this group is via characters (or 1-dimensional representations) or to understand $\mathrm{Gal}(\mathbb{Q}_S^{ab}/\mathbb{Q})$ and this is achieved by Class Field Theory.

To prove the conjecture, one proves a $R = T$ theorem and one needs a local-global compatibility result supplied by the p-adic local Langlands conjecture. In this thesis, we revisit $R = T$ theorem of [57] and reinterpret and reprove some of their results. To be precise:

Let p be an odd prime number. Let $\bar{\rho}$: $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to Gl_2(\mathbb{F})$ be an odd continuous representation unramified outside a finite set S of rational primes, where $\mathbb{F}$ is a finite field of characteristic p. In that situation, $\bar{\rho}$ factors through $G_S = \mathrm{Gal}(K_{S,p}/\mathbb{Q})$ where K denotes the field fixed by Ker $\bar{\rho}$ in $\bar{\mathbb{Q}}$ and $K_{S,p}$ is the maximal pro-p-extension of K, unramified outside S. We will throughout assume that all our representations have conductor N which is a squarefree integer.

Mazur's deformation theory of Galois representations shows the existence of a (uni)versal deformation ring $\mathscr{R}_{\bar{\rho}}^{univ}$ and the associated (uni)versal representation ρ^{univ} which allow us to parametrize all deformations $\tilde{\rho} : G_S \to Gl_2(R)$ of $\bar{\rho} : G_S \to Gl_2(\mathbb{F})$ where R stands for any complete noetherian local ring with residual field $\mathbb{F}$. By application of Schlessinger's criterion, Mazur ([37] subsection 1.2) shows that $\mathscr{R}_{\bar{\rho}}^{univ}$ is a quotient ring of a formal power series ring whose minimal number of variables is $d = \dim_{\mathbb{F}} H^1(G_S, Ad(\bar{\rho}))$. In this paper, we consider $\bar{\rho}$ whose image is contained in upper triangular matrices and whose diagonal characters χ_1 and χ_2 satisfy a particular assumption. In this case, we would expect to understand quite a bit of the structure just by studying the one-dimensional pieces. Indeed, we give a simple formula for d, where all the terms in the formula are given by class field theory.

Definition 1.0.4. We call a prime l difficult if $l \equiv 1 \pmod{p}$ and $\bar{\rho} : G_{\mathbb{Q}_l} \to GL_2(\mathbb{F})$ be such that $\bar{\rho} = \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$, where $*|_{I_l} \neq 0$.

In fact a main result of this thesis is the following theorem. Assume $\mathrm{Ext}^1(\chi_2, \chi_1) = \mathbb{F}$ (we call this **Hypothesis 1**) and $\chi_1 \neq \chi_2$ and we do not have any difficult primes in the deformation problem, then

Theorem 1.0.5. *There exists an exact sequence*

$$0 \longrightarrow \mathrm{Ext}^1(\chi_1,\chi_1) \oplus \mathrm{Ext}^1(\chi_2,\chi_2) \xrightarrow{f} t_{\mathscr{R}^{univ}_{\bar{\rho}}} \xrightarrow{g} \mathrm{Ext}^1(\chi_1,\chi_2) \longrightarrow 0$$

There is an exactly similar result by [2] for the pseudo-deformation ring. Our guiding principle in this thesis is to understand various arithmetic objects (which we will make precise) by one-dimensional objects. We can also handle the case of difficult primes, but we have to tweak the deformation problem by adding a Steinberg condition. See remark 3.4.3. Going back to the structure of deformation rings, Mazur shows $\mathscr{R}^{univ}_{\bar{\rho}} = \mathscr{O}[[Y_1,...,Y_d]]/J$ where J will be called the ideal of relations (sometimes also called obstruction classes) so now the determination of $\mathscr{R}^{univ}_{\bar{\rho}}$ amounts to that of J. But finding explicit obstruction classes is quite difficult and they relate to non-vanishing of cup products or more generally Massey products. But nonetheless, we manage to explicitly compute an obstruction class in a very specific situation and we can relate it to some cohomology class coming from one-dimensional representations. We set up the following problem.

Given a surjective ring homomorphism $A_1 \twoheadrightarrow A_0$ between complete local Noetherian $\mathscr{O}$-algebras with kernel I, generated by a single element with $I.m_{A_1} = 0$, let ρ be a representation to A_0 lifting $\bar{\rho}$ and $\tilde{\rho}$ be any lift of ρ to A_1. Now assume ρ is an upper triangular lift of $\bar{\rho}$ to A_0. We will find the obstruction to lift ρ to a not necessarily upper triangular representation to A_1. We know that this obstruction class is independent of the choice of lift and will only depend on ρ. We call that class $O(\rho) \in Z^2(\bar{\rho},\bar{\rho}) \otimes I$. We assume a technical condition called **Neben**, in which we fix the non-p part of the diagonal characters in our deformation problems. This allows us to rule out p-power non-trivial characters ε_l which are congruent to 1 mod p.

Theorem 1.0.6. *Assume* **Neben** *and* **Hypothesis 1** *and* $b \cup c = 0$ *where* $b \in Ext^1(\chi_2,\chi_1)$

and $c \in Ext^1(\chi_1, \chi_2)$. *Then*

$$O(\rho) = 0 \text{ iff } f_{21} \in B^2(a,d) \otimes I$$

We then try to understand the fields that are cut out by our representation, since this is ultimately our object of study. And surprisingly we can construct some big meta-abelian extensions via our Galois representations. To state the next theorem we have to prepare some notations.

Definition 1.0.7. The ideal of reducibility is the smallest ideal I^{red} of $\mathscr{R}^{univ}_{\bar{\rho}}$ such that ρ^{univ} mod I is reducible.

To simplify notation, we will use I instead of I^{red}, when there is no chance of confusion. To be consistent with the notations of the later sections, let $\bar{\rho} = \begin{pmatrix} \theta\omega & * \\ & \psi \end{pmatrix}$. Let F be a field that is cut out by the kernels of the characters θ and ψ where $\theta\psi(-1) = 1$, and they are of finite order and their orders are prime to p and their conductors are squarefree and prime to each other. Assume $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$. Let F_∞ be the cyclotomic $\mathbb{Z}_p$ extension of $F(\mu_p)$. Now let K_∞ be the maximal abelian p extension of F_∞, unramified outside Np, with $\theta\psi^{-1}\omega$-action and let L_∞ be the maximal abelian p extension of F_∞, unramified outside N, with $\psi\theta^{-1}\omega^{-1}$-action. Then we have the following theorem:

Theorem 1.0.8. *Let* M_∞ *be the maximal extension abelian p-extension of* $K_\infty L_\infty$*, unramified everywhere with trivial* $\Gamma \times \Delta$*-action. Then*

$$Gal(M_\infty/L_\infty K_\infty) \cong I/I^2$$

Moreover, we have a much stronger statement in the case where $\theta = \psi = 1$, then

Theorem 1.0.9. *Assume* **Hypothesis 1**. *Let M_∞ be the maximal extension abelian p-extension of $K_\infty L_\infty$, unramified everywhere with trivial $\Gamma \times \Delta$-action. Then*

$$Gal(M_\infty/L_\infty K_\infty) \cong I/I^2 \cong (I_G Gal(K'/K_\infty)/I_G^2 Gal(K'/K_\infty))_{\Gamma\times\Delta}$$

where I is the ideal of reducibility of $\mathscr{R}_{\bar{\rho}}^{univ}$, G=Gal $(K_\infty/\mathbb{Q}(\mu_{p^\infty}))$, and K' is the maximal extension of K_∞ unramified outside N and $\Delta = Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

Similar identification is possible in our general case but one has to assume some extra hypothesis on $\mathrm{Gal}(K_\infty/F_\infty)$ and $\mathrm{Gal}(L_\infty/F_\infty)$. This identification was first done by Sharifi, [54]. But our result is different than his theorem as we allow ramification at auxiliary primes in our intermediate fields and thus it applies in greater generality. Finally we give a description of these methods in constructing these fields explicitly in the case of elliptic curves of conductor 11.

Continuing on our theme of understanding these Galois representations, we asked Chris Skinner at the Arizona Winter School in 2017, if he knew if the Galois representations used in his paper [57] have big image, i.e. contains an open subgroup of $SL_2(\mathbb{F}[[T]])$. Big image questions are particularly important to cut down the size of Selmer groups and recent works of Kato have shown that they are a crucial ingredient in his Euler systems. We have a positive answer to that question.

Theorem 1.0.10. *Let $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F}[[T]])$ be such that*

i) ρ is irreducible, mod p distinguished and ordinary. (cf. Definition 3.3.1 and Definition 3.3.3)

ii) Determinant is of infinite order.

iii) There exists $\sigma \in I_p$ such that $\rho(\sigma) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ where $* \neq 0$.

Then Im(ρ) contains an open subgroup of $SL_2(\mathbb{F}[[T]])$.

On the other side of the picture, we have the rich theory of ordinary modular forms which is primarily developed by Hida. In our special case, we have a complete description of these Hecke algebras. Let $\mathfrak{H}_m$ and $\mathfrak{h}_m$ be the Hida ordinary Hecke algebras acting on spaces of modular forms and cusp forms respectively of fixed tame level N and Nebentypus $\theta\psi$. Let us assume **Neben**. Then we have the following theorem:

Theorem 1.0.11. *$\mathfrak{H}_m = \mathfrak{h}_m \times_{\Lambda/(A_{\theta,\psi})} \Lambda$, where $\mathfrak{h}$ is the cuspidal Hecke algebra and $\mathfrak{H}$ is the Hecke algebra of modular forms. We define the annihilator of the unique Eisenstein series $\tilde{\mathscr{E}}(\theta,\psi)$ by $I(\theta,\psi)$ and we denote by $I_{\theta,\psi}$ the image of $I(\theta,\psi)$ under the canonical projection $\mathfrak{H} \twoheadrightarrow \mathfrak{h}$. And*

$$A_{\theta,\psi} := \left(\prod_{\substack{l|N \\ l\nmid cond(\theta\psi^{-1})}} ((1+X)^{s(l)} - \psi\theta^{-1}\omega^{-2}(l)l^{-2}) \right) G(T, \theta\psi^{-1}\omega^2)$$

where $G(T,\theta\psi^{-1}\omega^2)$ is a twist of the Deligne-Ribet p-adic L-function as follows:

$$G(\varepsilon(u)u^s - 1, \theta\psi^{-1}\omega^2) = L_p(-1-s, \theta\psi^{-1}\omega^2\varepsilon)$$

where ε is a Dirichlet character of the second kind.

An important corollary of this theorem is the following:

Corollary 1.0.12. *Assume $p|L_p(-1,\theta\psi^{-1}\omega^2)$ but $p^2 \nmid L_p(-1,\theta\psi^{-1}\omega^2)$, then $(\mathfrak{H}_2^{ord})_m$ is Gorenstein iff $(\mathfrak{h}_2^{ord})_m \cong \mathscr{O}$ or some ramified DVR over O, where $(\mathfrak{H}_2^{ord})_m$ and $(\mathfrak{h}_2^{ord})_m$ are the ordinary Hida Hecke algebras acting on weight 2 modular and cusp forms with level N and Nebentypus $\theta\psi$ respectively. In particular, $(\mathfrak{h}_2^{ord})_m$ is a regular local ring of dimension* 1.

Now going back to our problem at hand: we want to show that there is an isomorphism $R_{\bar{\rho}}^{univ} \cong T$, where T is some suitable Hecke algebra. But this is where one faces serious

difficulties in proving modularity lifting results as there may not even be a map $\phi : R \to T$. This is where we again need **Hypothesis 1** to construct the map. The ϕ is shown to be an isomorphism using a numerical criterion.

The second problem in proving an "$R = T$" theorem in this reducible case is that T is no longer always Gorenstein and thus the numerical criterion fails. Then one can still hope to prove $R = T$ by some other method bypassing the numerical criterion. But in view of Fontaine-Mazur conjecture, we should recover these representations in cohomology of some geometric object. Indeed by the results of Hida, the cohomology of the towers of modular curves $\varprojlim H^1(Y(Np^r), \mathbb{Z}_p)_{\mathfrak{m}}$ is our natural candidate. But results of Tilouine-Mazur show that $\varprojlim H^1(Y(Np^r), \mathbb{Z}_p)_{\mathfrak{m}}$ is free over T_m iff T_m is Gorenstein and thus we lose the crucial geometric input to prove such a result. Thus we need new ideas to prove "$R = T$" results where some appropriate cohomology group is not free over the Hecke algebra. See the results of Erickson-Wake in this direction, where they work with pseudo-deformation rings. But one can ask for the next best case scenario.

Question 1.0.13. Is $\varprojlim H^1(Y(Np^r), \mathbb{Z}_p)_{\mathfrak{m}}$ representable by a perfect complex of T_m-modules when the residual Galois representation is mod-p distinguished?

In that case one can use Nekovar's machinery of Selmer complexes to construct a 2-variable p-adic L-function, the existence of which is only known in the free case.

Even though the Hecke algebras are not Gorenstein, we have the following conjecture by P. Wake.

Conjecture 1.0.14. (Wake): Let $I_{\mathfrak{h}}$ and $I_{\mathfrak{H}}$ be the Eisenstein ideals in $\mathfrak{h}^{ord}$ and $\mathfrak{H}^{ord}$. Then for all height 1 prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ such that $I_{\mathfrak{h}} \subset \mathfrak{p}$ and $I_{\mathfrak{H}} \subset \mathfrak{q}$, $\mathfrak{h}^{ord}_{\mathfrak{p}}$ and $\mathfrak{H}^{ord}_{\mathfrak{q}}$ are Gorenstein. In that case we say $\mathfrak{H}^{ord}$ and $\mathfrak{h}^{ord}$ are weakly Gorenstein.

Using our characterization of I/I^2 and the structure of the Hecke algebras, we prove Wake's conjecture in our special case.

Theorem 1.0.15. *(Wake's conjecture) $\mathfrak{H}_m^{ord}$ is weakly Gorenstein where m is an Eisenstein maximal ideal of $\mathfrak{H}^{ord}$. (cf. Definition 6.2.16)*

And finally we reprove some results of Skinner-Wiles in [56] and [57]. Our proof also shows that the Hecke algebras considered by Ohta in [43] are Gorenstein. To prove the next theorem, let us assume the following additional hypothesis:

- $p \nmid \phi(N)$ or **Neben**.
- $(\theta, \psi) \neq (\omega^{-2}, 1)$
- $p | B_{1,\psi\theta^{-1}\omega^{-1}}$
- (Vandiver type conjecture) $\mathrm{Gal}(L_\infty/F_\infty)$ is cyclic as a Λ module, cf. section 3.5.

Theorem 1.0.16. *We have an isomorphism $\mathscr{R}_{\bar{\rho}}^{univ} \cong \mathfrak{H}_m$ of complete local intersections over Λ.*

Definition 1.0.17. (Skinner-Wiles) A prime $\mathfrak{p}$ in $\mathscr{R}_{\bar{\rho}}^{univ}$ is nice if it is height 1, contains p and $\mathfrak{p}$ does not contain the ideal of reducibility and is an inverse image of a prime $\mathfrak{q}$ in $\mathfrak{h}_m$.

Theorem 1.0.18. *(a) There is an isomorphism $(\mathscr{R}_{\bar{\rho}}^{univ})_{\mathfrak{p}} \cong (\mathfrak{H}_m)_{\mathfrak{q}}$ of complete local intersections over Λ_p, where $\mathfrak{p} \subset \mathscr{R}_{\bar{\rho}}^{univ}$ and $\mathfrak{q} \subset \mathfrak{H}_m$ are any height 1 prime ideal (sometimes referred to prime divisors) over $(p) \subset \Lambda$ such that $\pi^{-1}(\mathfrak{q}) = \mathfrak{p}$*
(b) (Skinner-Wiles) Under the isomorphism above, $(\mathscr{R}_{\bar{\rho}}^{univ})_{\mathfrak{p}} \cong (\mathfrak{h}_m)_{\mathfrak{q}}$ for all nice primes $\mathfrak{p}$ and both the rings are complete local intersections.

The organization of the thesis is as follows:
Chapter 2 : Sections 1 and 2 deal with basic definitions. In section 3, we prove some technical Galois cohomology results and give some criteria for the cup products. These results are then used throughout Chapter 3, 6 and 7. We also provide examples where **Hypothesis 1**

is satisfied in the form of proposition 2.3.8.

Chapter 3 : Sections 1 and 2 are respectively about basic definitions and properties of Galois representations and Mazur's results about the structure of universal deformation ring and in section 3, we recall some properties of ordinary deformation rings. In section 4, we compute the tangent space of the universal deformation ring in theorem 3.4.1 which is one of the main results of the section. We then carry our analysis further by trying to find explicit obstructions to lifting Galois representations. In some special cases, we manage to find our obstruction classes as in theorem 3.4.19. Some of these computations give alternate proofs of the smoothness of local deformation rings. At the end of the section, we show how **Hypothesis 1** can be used to simplify some arguments in [57]. In section 5, we make a deeper look at the fields that are cut out by the Galois representations constructed in the previous sections. We construct unramified extensions in theorem 3.5.15 and 3.5.25. We also prove various Iwasawa theoretic properties of some intermediate fields which will be quite important for us in Chapter 6. In section 6, we use our ideas to explicitly construct these fields in the case of elliptic curves of conductor 11. Section 7 is about pseudo-representations and gives us a link between pseudo-representations and representations and this will be important for us to construct the map $\phi : R \to T$.

Chapter 4 : Chapter 4 is basically a crash course on Hida theory and the properties of the Galois representations attached to modular forms.

Chapter 5 : We start with some history and motivation behind big image questions and in section 2, we prove our big image theorem (theorem 5.2.5).

Chapter 6 : In Section 2, we introduce the Eisenstein series and compute the congruence modules attached to the Hecke algebras and prove the structure theorem for Hida Hecke algebras in proposition 6.2.26. We also construct a cusp form which is congruent to our Eisenstein series. In section 3, we state Wake's conjecture and state the various isomorphism criteria. We then use these criteria to prove the modularity lifting results and Wake's

conjecture.

Chapter 7 : We revisit Selmer groups and we show a factorization property for Selmer groups.

Chapter 2: Galois cohomology and Selmer groups

In this chapter, we recall some main results on Galois cohomology and use them to compute tangent spaces of deformation rings and study Selmer groups. Most of the exposition can be found in Milne, Tate, Rubin, Neukirch-Schmidt-Wingberg and Wiles in the references.

2.1 Basic definitions

Let G be a group and M be a module with an action of G. The cases of interest are when both G and M are discrete or G is profinite and M is discrete and finally both G and M are profinite. In any case, we will always require the action of G on M to be continuous. For a topological group G and a module M, the i-th group of continuous cochains $C^i(G,M)$ is the group of continuous maps $G^i \to M$. There is a differential $d : C^i(G,M) \to C^{i+1}(G,M)$ satisfying

$$(df)(g_1,...g_{i+1}) = g_1.f(g_2,...g_{i+1}) + \sum(-1)^j f(g_1,..g_jg_{j+1},..g_{i+1}) + (-1)^{i+1} f(g_1,...g_i)$$

It is easy to check $d^2 = 0$, so we have a complex $C^\bullet(G,M)$. Then we define $H^i(G,M) := \ker d/\mathrm{im}\, d$.

In the sequel, we will drop the term continuous, where all our cocycles will be continuous maps. Let ρ_1, ρ_2, ρ_3 be 3 representations of G in $Gl_{d_1}(A), Gl_{d_2}(A)$ and $Gl_{d_3}(A)$ respectively. Then one can define the 4 modules:

- $Z^1_G(\rho_2,\rho_1) = \{c : G \to M_{d_1,d_2}(A) : \forall g_1, g_2 \in G, c_{g_1g_2} = \rho_1(g_1)c_{g_2} + c_{g_1}\rho_2(g_2)\}$
- $B^1_G(\rho_2,\rho_1) = \{c : G \to M_{d_1,d_2}(A) : \exists M \in M_{d_1,d_2}, \forall g \in G, c_g = \rho_1(g)M + M\rho_2(g)\}$
- $Z^2_G(\rho_2,\rho_1) = \{c : G\times G \to M_{d_1,d_2}(A) : \forall g_1,g_2,g_3 \in G, \rho_1(g_1)c_{g_2,g_3} - c_{g_1g_2,g_3} + c_{g_1,g_2g_3} - c_{g_1,g_2}\rho_2(g_3) = 0\}$
- $B^2_G(\rho_2,\rho_1) = \{c : G\times G \to M_{d_1,d_2}(A), \exists f : G \to M_{d_1,d_2}(A), \forall g_1,g_2 \in G, c_{g_1,g_2} = f(g_1g_2) - \rho_1(g_1)f(g_2) - f(g_1)\rho_2(g_2)\}$

The elements in Z^i and B^i are called i-homogeneous cocycles and i-homogeneous coboundaries. It is easy to see that $B^i_G(\rho_2,\rho_1) \subset Z^i_G(\rho_2,\rho_1)$ and the quotient is denoted as $Ext^i_G(\rho_2,\rho_1)$. We will drop G from the notation whenever the group G is clear from the context. The case that is important for us is when ρ_i are characters then it is easy to see $Ext^i(\chi_2,\chi_1) = H^i(G,\chi_1\chi_2^{-1})$. We will use this identification throughout this thesis.
Finally the Yoneda product is defined as follows:

$$Ext^1(\rho_2,\rho_1) \times Ext^1(\rho_3,\rho_2) \longrightarrow Ext^2(\rho_3,\rho_1)$$

given by

$$(c_1,c_2) \to (g_1,g_2 \mapsto c_1(g_1)c_2(g_2))$$

It is easy to see that it maps

$$Z^1(\rho_2,\rho_1) \times Z^1(\rho_3,\rho_2) \to Z^2(\rho_3,\rho_1)$$

and maps

$$Z^1(\rho_2,\rho_1) \times B^1(\rho_3,\rho_2) + B^1(\rho_2,\rho_1) \times Z^1(\rho_3,\rho_2) \text{ to } B^2(\rho_3,\rho_1).$$

Thus it induces a bilinear map on

$$Ext^1(\rho_2,\rho_1)\times Ext^1(\rho_3,\rho_2)\longrightarrow Ext^2(\rho_3,\rho_1).$$

In the context of inhomogeneous cocycles, the Yoneda product is also called the cup product.

Proposition 2.1.1. *(Tate) (a) Let $T=\varprojlim T_n$ and assume the T_n's are finite. If $i>0$ and $H^i(G,T_n)$ is finite for all n, then $H^i(G,T)=\varprojlim H^i(G,T_n)$.*
(b) If T is a finitely generated Z_p-module and $i\geq 0$, then $H^i(G,T)$ has no divisible elements and $H^i(G,T)\otimes\mathbb{Q}_p\cong H^i(G,T\otimes\mathbb{Q}_p)$.

Proposition 2.1.2. *Suppose H is a closed normal subgroup of G, and let M be a discrete, finitely generated $\mathbb{Z}_p$-module or a finite dimensional $\mathbb{Q}_p$-vector space. There is a Hochschild-Serre (inflation-restriction) exact sequence*

$$0\to H^1(G/H,M^H)\to H^1(G,M)\to H^1(H,M)^{G/H}\to H^2(G/H,M^H)\to H^2(G,M)$$

2.2 Local duality theorems

Let K be a finite extension of $\mathbb{Q}_p$ and let μ_n be the n-th roots of unity inside $\bar{K}$, where $\bar{K}$ is an algebraic closure of K. We will write $H^i(K,-)$ to denote $H^i(\mathrm{Gal}(\bar{K}/K),-)$

Proposition 2.2.1. *(a)* $H^0(K,\mu_n) = \mu_n \cap K$

(b) $H^1(K,\mu_n) = K^*/(K^*)^n$

(c) $H^2(K,\mu_n) = \mathbb{Z}/n\mathbb{Z}$

(d) $H^2(K,\mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$

(e) $H^i(K,\mu_n) = 0$ *for* $i \geq 3$.

Corollary 2.2.2. *If M is a finite G_K module, then $H^i(K,M)$ is finite.*

Now we can state Tate's local duality theorem.

Theorem 2.2.3. *Let M be a finite G_K-module and let $M' = \mathrm{Hom}(M,\mathbb{G}_m)$. Then for $0 \leq i \leq 2$, the cup-product*

$$H^i(K,M) \times H^{2-i}(K,M') \longrightarrow H^2(K,\mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing.

For a finite G_K-module M, we define the local Euler-Poincare characteristic to be

$$\chi(M) = \frac{\#H^0(K,M)\cdot\#H^2(K,M)}{\#H^1(K,M)}.$$

We can extend the concept to the case where M is a finite free $\mathbb{Z}_p$-module or a finite-dimensional $\mathbb{Q}_p$-vector space by making the more familiar definition

$$\chi_{add}(M) = h^0(M) - h^1(M) + h^2(M)$$

where $h^i(M) = \text{rank } H^i(K,M)$. We have the following useful formula for the Euler characteristic.

Proposition 2.2.4. $\chi(M) = p^{-v_p(\#M).N} = \frac{1}{[\mathcal{O}:\#M\mathcal{O}]}$

where $N = [K:\mathbb{Q}_p]$ and $\mathcal{O}$ is the ring of integers in K. In particular, $\chi(M) = 1$ if order of M is coprime to p.

Corollary 2.2.5. *Let χ be the mod p cyclotomic character. If $l \not\equiv 1$ mod p, then the deg p extension of $\mathbb{Q}_l(\mu_p)$ given by the fixed field of the kernel of c, where c is any non trivial cocycle in $H^1(\mathbb{Q}_l, \chi)$, is ramified (tamely) at l.*

Proof. This is a straightforward application of the Hochschild-Serre exact sequence 2.1.2 by noting that the restriction $H^1(\mathbb{Q}_l, \chi) \to H^1(I_l, \chi)$ is an injection. □

We will end this section by recalling some facts about unramified cohomology.
We define $H^i_{nr}(K,M) := H^i(K^{nr}/K, M^I)$ to be the unramified classes, i.e. classes vanishing on inertia.
By inflation-restriction exact sequence we get

$$H^1_{nr}(K,M) = \ker(H^1(K,M) \to H^1(K^{nr}/K,M)) \tag{2.1}$$

and since $H^2(\hat{\mathbb{Z}}, M) = 0$, we get the following exact sequence

$$0 \longrightarrow M^{G_K} \longrightarrow M^I \xrightarrow{\text{Frob-id}} M^I \longrightarrow M^I/(\text{Frob} - \text{id})M^I \longrightarrow 0 \tag{2.2}$$

In particular, if M is finite, we get

$$\#H^1_{nr}(K,M) = \#H^0(K,M) \tag{2.3}$$

and

$$H^2_{nr}(K,M) = 0 \tag{2.4}$$

Proposition 2.2.6. *If #M is relatively prime to p, then* $H^1_{nr}(K,M)$ *and* $H^1_{nr}(K,M')$ exactly *annihilate each other under the Tate pairing.*

Proof. Note that the inclusion $H^1_{nr}(K,M) \hookrightarrow H^1(K,M)$ is compatible with cup-products so the map

$$H^1_{nr}(K,M) \times H^1_{nr}(K,M') \longrightarrow H^2(K,\mathbb{G}_m)$$

factors through $H^2_{nr}(K,\mathbb{G}_m)$ which is 0. The only thing left to show is that

$$\#H^1_{nr}(K,M) \cdot \#H^1_{nr}(K,M') = \#H^1(K,M).$$

Now, $\#H^1_{nr}(K,M) = \#H^0(K,M)$ and $\#H^1_{nr}(K,M') = \#H^0(K,M')$ and $H^0(K,M')$ is dual to $H^2(K,M)$ via Tate pairing. And finally since $(\#M,p) = 1$, $\chi(M) = 1$ and this gives the desired result. □

2.3 Restricted ramification and Global duality

In this section we will be concerned with the cohomology of $G_{\mathbb{Q},S}$ where S is a finite set of primes containing p and ∞. One of the main reasons for doing so is that the cohomology of $G_{\mathbb{Q}}$ is not well-behaved.

For a finite module M, we define $M' = \mathrm{Hom}(M, \mathbb{G}_m)$. We will start with a few lemmas, the results of which are used later.

Lemma 2.3.1. $h^1(G_{\mathbb{Q},S}, \mathbb{F}) = \#\{q \in S : q \equiv 1 \bmod p\} + 1$, *where* $\mathbb{F} = \mathbb{F}_{p^r}$ *and* $r \geq 1$.

Proof. $H^1(G_{\mathbb{Q},S}, \mathbb{F}) = \mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{F})$, so this reduces to finding cyclic extensions of $\mathbb{Q}$ of degree p unramified outside of S. Now take any prime $q \in S$ such that $q \equiv 1 \bmod p$. Then the field of q-th roots of unity has a cyclic subfield of degree p. And finally we can construct a degree p extension from $\mathbb{Q}(\zeta_{p^2})$. And it's easy to see that these are the only ones. □

Lemma 2.3.2. $h^2(G_{\mathbb{Q},S}, \mathbb{F}) = \#\{q \in S : q \equiv 1 \bmod p\}$

Proof. This is corollary 8.7.5 in [50]. It is a trivial consequence of the global Euler Poincare characteristic formula (2.9). □

Recall we have the restriction maps:

$$res : H^i(G_{\mathbb{Q}_S}, M) \to H^i(G_{\mathbb{Q}_q}, M) \tag{2.5}$$

which gives rise to a map called localization

$$loc : H^i(G_{\mathbb{Q}_S}, M) \to \prod H^i(G_{\mathbb{Q}_q}, M) \tag{2.6}$$

The next lemma is a well-known local-global principle in algebraic number theory.

Lemma 2.3.3. *loc:* $H^2(G_{\mathbb{Q}_S}, \mathbb{F}) \to \bigoplus_{q \in S : q \equiv 1 \pmod p} H^2(G_{\mathbb{Q}_q}, \mathbb{F})$ *is an isomorphism.*

Proof. By local Tate duality (theorem 2.2.3), $H^2(G_{\mathbb{Q}_q}, \mathbb{F}) \neq 0$ iff $l \equiv 1 \pmod{p}$. Thus both the sides have the same $\mathbb{F}$-dimension. So it suffices to show that the map is an injection. But the the injectivity is (i) of Corollary 9.1.10 in [50]. □

It is customary to write $\bigoplus_{q \in S} H^2(\mathbb{Q}_q, M) := P^2(G_{\mathbb{Q},S}, M)$. See theorem 2.3.12 for more details. This lemma is quite useful as it allows us to check if some 2-cocycle is 0, by checking it locally.

The next lemma also allows us to detect vanishing of cup products.

Lemma 2.3.4. *If $a \in Ext^1(\chi_2, \chi_1)$ and $b \in Ext^1(\chi_1, \chi_2)$, then $a \cup b = 0$ is equivalent to the existence of a representation of the form* $\begin{pmatrix} \chi_1 & a & * \\ 0 & \chi_2 & b \\ 0 & 0 & \chi_1 \end{pmatrix}$

Proof. $a \cup b = 0$ is equivalent to the existence of a function f such that $df = a \cup b$, i.e. $f(gh) = \chi_1(g)f(h) + a(g)b(h) + \chi_2(h)f(g)$. Now construct the matrix $\begin{pmatrix} \chi_1 & a & f \\ 0 & \chi_2 & b \\ 0 & 0 & \chi_1 \end{pmatrix}$ and one can easily see it's a representation. We remark that the choice of f is not unique but can differ by an element in $Z^1(\chi_1, \chi_1)$. □

Since our goal in the next chapter is to construct these meta-abelian extensions, we would like to come up with some criteria for the vanishing of the above cup-products. Note that the cup product trivially vanishes if there are no primes congruent to 1 in S. To formulate our problem: let χ be a non-trivial character of order prime to p and let $\mathbb{Q}(\mu_p) \subseteq K_\chi$, where K_χ is the fixed field of the kernel of χ. In view of lemma 2.3.3, we can check the vanishing of the cup products locally since cup products are compatible with restriction. The cases of interest are the primes congruent to 1 $\pmod{p}$. Let q be such a prime and let χ be ramified at q, then by theorem 2.2.3 and proposition 2.2.4,

$H^1(\mathbb{Q}_q, \chi^{\pm 1})$ is trivial. Again note that by the same argument if χ is unramified but non-trivial, $H^1(\mathbb{Q}_q, \chi^{\pm 1})$ is trivial. Thus we have nothing to prove. Thus the only case of interest is when $q \equiv 1 \pmod{p}$ and $\chi|_{G_{\mathbb{Q}_q}} = 1$. In that case, $H^1(\mathbb{Q}_q, \mathbb{F})$ is a 2 dimensional $\mathbb{F}$ vector space spanned by a ramified cocycle and an unramified cocycle. The cup product of any two unramified cocycles is trivially zero and since the Tate pairing is non degenerate, the cup product of two ramified cocycles is zero iff they lie on the same line. We summarize this discussion in the form of the following proposition:

Proposition 2.3.5. *Let χ be any finite order non-trivial character of order prime to p. Let*

$$H^1(G_{\mathbb{Q},S}, \chi) \otimes H^1(G_{\mathbb{Q},S}, \chi^{-1}) \xrightarrow{\cup} H^2(G_{\mathbb{Q},S}, \mathbb{F})$$

be the usual cup-product. Then $\cup = 0$ if one of the following conditions are satisfied:

- *There are no primes congruent to $1 \pmod{p}$ in S.*
- *χ is ramified or non-trivial at all primes $q \in S$ which are congruent to $1 \pmod{p}$*

Moreover let $H^1(G_{\mathbb{Q},S}, \chi)$ be one-dimensional as a F-vector space and let b be a basis for this space. Let $c \in H^1(G_{\mathbb{Q},S}, \chi^{-1})$, then $b \cup c = 0$, iff the following hold.
b and c are both unramified at q, or if b is ramified at q, then c must be ramified at q and $c|_{G_{\mathbb{Q}_q}}$ must be a multiple of the basis element of $H^1(\mathbb{Q}_q, \chi^{-1})$, i.e. when $q \equiv 1 \pmod{p}$, $c|_{G_{\mathbb{Q}_q}} = kb|_{G_{\mathbb{Q}_q}}$ for some $k \in \mathbb{F}$.

Remark 2.3.6. We will only use this proposition in the case where $h^1(G_{\mathbb{Q},S}, \chi) = 1$. Then we can drop the assumption that χ is non-trivial. If χ is trivial, then in that case b and c are $\mathbb{F}$ multiples of each other and since the cup product is anti-symmetric $b \cup c = 0$

In fact we can try to see how to find obstructions in constructing upper triangular rep-

resentations of the form

$$\begin{pmatrix} \chi_1 & a & f_1 & * \\ 0 & \chi_2 & b & f_2 \\ 0 & 0 & \chi_1 & a \\ 0 & 0 & 0 & \chi_2 \end{pmatrix}$$

where $a \cup b = 0 = b \cup a$. So define $df_2 = b \cup a$ and $f_1 = f$ in the previous lemma (lemma 2.3.4). If a representation were to exist, the top right corner, call it α, should satisfy

$$\alpha_{gh} = \chi_1(g)\alpha(h) + a(g)f_2(h) + f_1(g)a(h) + \alpha(g)\chi_2(h) \tag{2.7}$$

A brute force computation shows that

$$a(g)f_2(h) + f_1(g)a(h) \in Z^2(\chi_2, \chi_1)$$

So the same calculation from the previous corollary shows that existence of the representation is equivalent to the fact that $a(g)f_2(h) + f_1(g)a(h)$ is a coboundary.

Remark 2.3.7. $a(g)f_2(h) + f_1(g)a(h)$ is called a triple Massey product and the higher Massey products measure obstructions to constructing higher dimensional representations.

But we do not know of any necessary or sufficient conditions to make the above triple Massey product a coboundary in such a general situation, except when the target group is trivial, nor can we compute it explicitly in any generality.

Now we will give some conditions and examples where our **Hypothesis 1** is satisfied. Let χ be a character of order prime to p and let K' be the fixed field of the kernel of χ. Let $K = K'(\zeta_p)$, so $p \nmid [K : \mathbb{Q}]$. The characters associated to K are $\chi^i \omega^j$. Assume the values of χ lie in $\mathbb{F}$ and we will use χ to denote the one-dimensional space over $\mathbb{F}$ on which $\mathrm{Gal}(K/\mathbb{Q})$

acts via χ. Let S be the set of primes that divide the conductor of K. By inflation-restriction (proposition 2.1.2), we get the following exact sequence:

$$0 \to H^1(K/\mathbb{Q},\chi) \to H^1(\mathbb{Q}_S/\mathbb{Q},\chi) \to H^1(\mathbb{Q}_S/K,\chi)^{\mathrm{Gal(K/\mathbb{Q})}} \to H^2(K/\mathbb{Q},\chi).$$

Since $p \nmid [K:\mathbb{Q}]$, $H^1(K/\mathbb{Q},\chi) = H^2(K/\mathbb{Q},\chi) = 0$. Therefore,

$$H^1(\mathbb{Q}_S/\mathbb{Q},\chi) \cong H^1(\mathbb{Q}_S/K,\chi)^{\mathrm{Gal(K/\mathbb{Q})}}$$

Since $\mathrm{Gal}(\mathbb{Q}_S/K)$ acts trivially on χ, we get

$$H^1(\mathbb{Q}_S/K,\chi)^{\mathrm{Gal(K/\mathbb{Q})}} \cong \mathrm{Hom}(\mathrm{Gal}(\mathbb{Q}_S/K),\chi)^{\mathrm{Gal(K/\mathbb{Q})}}$$

Let $\phi \in \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/K),\chi)^{\mathrm{Gal(K/\mathbb{Q})}}$, $h \in \mathrm{Gal}(K/\mathbb{Q})$ and let h lift to $\tilde{h} \in \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. Then $\phi(\tilde{h}g\tilde{h}^{-1}) = \chi(h)\phi(g)$ for all h,g.

By Kummer theory,

$$\phi(g) = \frac{g(b^{1/p})}{b^{1/p}} = \langle g,b\rangle$$

where $b \in K^*/(K^*)^p$ and $\langle,\rangle$ is the Kummer pairing that takes values in μ_p. Therefore,

$$\langle g,b\rangle^{\chi(h)} = \langle g^h,b\rangle = \langle g,h^{-1}b\rangle^h = \langle g,h^{-1}b\rangle^{\omega(h)}.$$

The non-degeneracy of the Kummer pairing implies that

$$h^{-1}b \equiv b^{\chi(h)\omega^{-1}(h)} \bmod (K^*)^p.$$

Changing h to h^{-1},

$$b^h \equiv b^{\chi^{-1}(h)\omega(h)} \bmod (K^*)^p.$$

Now $K(b^{1/p})/K$ is unramified outside S and assume the $\chi^{-1}\omega$-component of the class group of K is prime to p. It follows that b is an S-unit (times a p-th power). Let E_S be the S-units in K. Then we have shown the following proposition.

Proposition 2.3.8. *Let χ be a character whose order is prime to p. Assume $\chi^{-1}\omega$ component of the p-part of the class group of K is trivial. Then*

$$H^1(\mathbb{Q}_S/\mathbb{Q},\chi) \cong (E_S/(E_S)^p)^{\chi^{-1}\omega}$$

Finally, we need to decompose $E_S/(E_S)^p$ into irreducible components under the action of Galois. Since $p \nmid [K:\mathbb{Q}]$, the representation is semi-simple. Let E be the group of units in K. The units E^+ in K^+ have an unit whose Galois conjugates generate a finite index subgroup L of $E^+/\{\pm 1\}$ (cf. 5.27 in [67]). Therefore L/L^p decomposes into one-dimensional components corresponding to the non-trivial even characters of $\mathrm{Gal}(K/\mathbb{Q})$. By the Brauer-Nesbitt theorem 3.1.8, the same is true for $E^+/(E^+)^p$. Since E^+ and ζ_p generate a subgroup of index 1 or 2, we find the characters that occur in E/E^p are the non-trivial even characters and ω.

For simplicity, assume the conductor of χ is q where $q \equiv 1 \bmod p$ and q is a prime. So q splits completely in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Therefore the primes over q contribute to one-dimensional $\mathbb{F}$ vector spaces on which $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts via ω^i, for $0 \le i < p-1$. Let ψ be a character of conductor q in the group generated by χ and ω. Then ψ is a character of $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ of order dividing the degree of the extension. Let f be the order of the root of unity $\psi(p)$. Then the prime of $\mathbb{Q}(\zeta_p)$ over p splits into $g = [K:\mathbb{Q}(\zeta_p)]/f$ primes in K. Therefore, the primes of K above p contribute to the characters $1, \psi^f, \psi^{2f}, \ldots \psi^{(g-1)f}$. Note that they all have conductors q or 1. Putting all of the above arguments together, we obtain exactly what characters occur (with multiplicities) in $E_S/(E_S)^p$.

If $\chi \neq \omega$ is odd, then $\chi\omega^{-1}$ is even and non-trivial and so occurs at least once. If $\chi\omega^{-1}$

has conductor pq, then it does not occur in the representations coming from p or q. Therefore, it occurs exactly once. This implies that if both χ and $\chi\omega^{-1}$ have conductor pq, then $H^1(\mathbb{Q}_S/\mathbb{Q},\chi)$ is one-dimensional.

In the final part of this section, we introduce cohomology classes that have special local behavior. Recall we have the map

$$\text{res} : H^i(G_K,M) \to H^i(G_{K_v},M) \tag{2.8}$$

Definition 2.3.9. A Greenberg-Wiles Selmer system is a collection $\mathscr{L} = \{L_v\}$ of subgroups $L_v \subset H^1(G_v,M)$ such that for almost all primes $v \neq p$,

$$L_v = H^1_{nr}(K_v,M) = \ker(H^1(K_v,M) \to H^1(K_v^{nr}/K_v,M))$$

The condition at p is subtle and one generally uses the Greenberg condition. And generally we will require some conditions on the primes where the representation is ramified. For a more complete list of local conditions see [60].

Definition 2.3.10. The Selmer group associated to a set of local conditions is given by

$$H^1_{\mathscr{L}}(\mathbb{Q},M) = \ker\left(H^1(\mathbb{Q},M) \to \prod_v H^1(\mathbb{Q}_v,M)/L_v\right)$$

Definition 2.3.11. Define $L_v^\perp \subset H^1(G_v,M^*(1))$ to be the annihilator of L_v under the local Tate pairing. Then we call $\mathscr{L}^\perp$ the dual Selmer system for $\mathscr{L}$ and $H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*(1))$ the dual Selmer group.

Now we state the main results of this section, which allow us to compute various Selmer

groups.

Theorem 2.3.12. *(Poitou-Tate) Let K be a number field, S be a finite set of primes containing the archimedean primes and all places v such that $v(\#M) \neq 0$. Then we have the following 9-term exact sequence.*

$$\begin{aligned} 0 \to H^0(G_{K,S},M) \to P^0(G_{K,S},M) \to H^2(G_{K,S},M^*)^\wedge \to \\ \to H^1(G_{K,S},M) \to P^1(G_{K,S},M) \to H^1(G_{K,S},M^*)^\wedge \to \\ \to H^2(G_{K,S},M) \to P^2(G_{K,S},M) \to H^0(G_{K,S},M^*)^\wedge \to 0, \end{aligned}$$

where $A^\wedge = Hom(A,\mathbb{Q}/\mathbb{Z})$, and

$$P^i(G_{K,S},M) = \prod_{p\in S}{}' H^i(K_p,M),\ i \geq 0$$

where the restricted product is taken with respect to the subgroups $H^i_{nr}(K_p,M)$ of $H^i(K_p,M)$. Note that we take $\hat{H}^0$ at the Archimedean primes.

We define the global Euler-Poincare characteristic to be

$$\chi(M) := \frac{\#H^0(G_{K,S},M)\cdot\#H^2(G_{K,S},M)}{\#H^1(G_{K,S},M)} \tag{2.9}$$

We have the following useful formula to compute the Euler-Poincare characteristic.

Proposition 2.3.13. $\chi(M) = \prod_{v\in S_\infty} \frac{\#H^0(K_v,M)}{\|\#M\|} = \prod_{v\in S_\infty} \frac{\#\hat{H}^0(K_v,M)}{\#H^0(K_v,M')}$

Theorem 2.3.14. *(Greenberg-Wiles) Let M be a finite $G_\mathbb{Q}$ module and let $\mathscr{L}$ be a set of Selmer conditions. Then $H^1_\mathscr{L}(\mathbb{Q},M)$ and $H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*)$ are finite and*

$$\frac{\#H^1_\mathscr{L}(\mathbb{Q},M)}{\#H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*)} = \frac{\#H^0(\mathbb{Q},M)}{\#H^0(\mathbb{Q},M^*)}\prod\frac{\#\mathscr{L}_v}{\#H^0(\mathbb{Q}_v,M)}$$

Note that this formula makes sense as $\#\mathscr{L}_v = \#H^0(\mathbb{Q}_v, M)$ for all unramified primes.

Chapter 3: Universal Deformation Rings

In this chapter we will study deformations of various Galois representations and study the tangent spaces of these rings.

3.1 Basic Definitions and preliminaries on representations

Let G be a profinite (compact), Hausdorff topological group. In our applications, G arises from one of the following situations.

- *Local Fields*: Let L be a local field, i.e. a finite extension of $\mathbb{Q}_p$, and $\bar{L}$ be an algebraic closure. Then G= Gal$(\bar{L}/L)$
- *Global fields*: Let K be an extension $\mathbb{Q}$ and let S be a finite set of primes in K. Let K_S be the maximal extension of K unramified outside S. Then G= Gal(K_S/K)

Definition 3.1.1. A Galois representation is a continuous group homomorphism from G to $GL_n(R)$ where R is a topological ring and G is as above. We call a Galois representation a local (Galois) representation if G is the Galois group of the local field and we call the representation global if G is the Galois group of the global field.

Now we state a few well-known lemmas without proofs.

Lemma 3.1.2. *Let G be as above. And let*

$$\rho : G \longrightarrow GL_n(\bar{\mathbb{Q}}_p)$$

be a continuous representation. Then there exists L, a finite extension of $\mathbb{Q}_p$ *such that* $\rho(G) \subset GL_n(L)$.

Lemma 3.1.3. *Let* $\rho : G \longrightarrow GL_n(L)$ *be a continuous representation. Then there exists* $M \in GL_n(L)$ *such that* $M\rho(G)M^{-1} \subset GL_n(\mathcal{O}_L)$.

The above lemma shows that there is at least one lattice stable under the action of G.

Proposition 3.1.4. *The number of stable lattices (up to homothety) is finite iff* ρ *is irreducible.*

In fact, in our situation the number of stable lattices will not be 1. As an example, take 2 elliptic curves E_1 and E_2 over $\mathbb{Q}$. If they have $\mathbb{Q}$-rational 2-isogeny between them, then they give rise to non-isomorphic Galois stable lattices for their associated 2-adic representations. This motivates the following proposition. But we need some notations and definitions before we can state it.

Definition 3.1.5. The semi-simplification of a representation G on a finite dimensional vector space V over a field k is the direct sum of all the Jordan-Hölder constituents of the $k[G]$-module V. We usually denote it by V^{ss}. In this definition, we take multiplicities into account so that $\dim_k V = \dim_k V^{ss}$.

Definition 3.1.6. The representation V is semi-simple iff $V \cong V^{ss}$ as k[G]-modules. Concretely, if (V_i) is an increasing filtration of sub-representations of V such that V_{i+1}/V_i is irreducible, then $V^{ss} \cong \oplus_i V_{i+1}/V_i$.

Example 3.1.7. *Let k be any field and let* $\rho : G \longrightarrow GL_2(k)$ *be given by*

$$g \mapsto \begin{pmatrix} a(g) & b(g) \\ 0 & d(g) \end{pmatrix}$$

then $\rho^{ss} = a \oplus d$

Let $\Lambda \subset L^n$ be a stable lattice under the action of G.

Proposition 3.1.8. *(Brauer-Nesbitt) The semi-simplification of the representation of G on $\Lambda/\pi\Lambda$ is independent of the choice of Λ.*

Corollary 3.1.9. *G has a unique stable lattice in L^n (up to homotheties) iff G acts irreducibly on k_L^n, where k_L is the residue field.*

Proof. This is exercise 4 in [52] page 3. We give a quick sketch. Let G act irreducibly on the residue field and assume we have 2 stable lattices call them L_1 and L_2 and moving them by homothety, assume $L_2 \subset L_1$ and $L_2 \not\subset \pi L_1$. Now, $L_2/(L_2 \cap \pi L_1) \hookrightarrow L_1/\pi L_1$. Since G acts irreducibly on the residue field, we get $L_2/(L_2 \cap \pi L_1) = 0$ or $L_1/\pi L_1$. If $L_2 = \pi L_1$, then L_1 and L_2 are homothetic. So assume $L_2/(L_2 \cap \pi L_1) = L_1/\pi L_1$. Then we can see that $L_2/\pi L_2 \twoheadrightarrow L_1/\pi L_1$ and by irreducibility $L_2/\pi L_2 \cong L_1/\pi L_1$. Thus there is a matrix $\bar{M} \in GL_2(k_L)$ that sends $L_1/\pi L_1$ to $L_2/\pi L_2$. By Nakayama's lemma, we can lift $\bar{M}$ to $GL_2(\mathscr{O})$ that sends L_1 to L_2. Thus the two lattices are isomorphic.
The converse is easy. □

The above proposition motivates the following definition.

Definition 3.1.10. Let L be a finite extension of $\mathbb{Q}_p$ and $\rho : G \longrightarrow GL_n(L)$ be a Galois representation. We denote by $\bar{\rho}^{ss} : G \longrightarrow GL_n(k_L)$ the semi-simple representation defined above. It is called the residual representation of ρ.

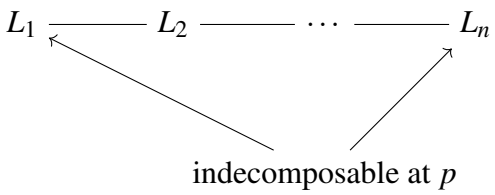
Definition 3.1.11. We call $\bar{\rho}$ absolutely irreducible if $\bar{\rho} \otimes \bar{k}_L$ is irreducible where $\bar{k}_L$ is an algebraic closure of k_L.

Recall the following well-known lemma by Ribet.

Lemma 3.1.12. *(Ribet) If $\rho : G \to GL_2(L)$ is irreducible but $\bar{\rho}^{ss}$ is reducible, then there exists a G-stable lattice where $\bar{\rho}$ is indecomposable.*

Proof. This is Prop. 2.1 in [48]. We recall some key aspects of the proof as those ideas will be important for us. Ribet considers the graph of stable lattices (up to scaling by L^*), where 2 lattices $[L_1]$ and $[L_2]$ are connected by an edge if $\pi L_1 \subset L_2 \subset L_1$. Let us call the graph $\mathfrak{X}$. He shows $\mathfrak{X}$ is a tree. Note that $\mathfrak{X}$ is bounded by Prop 2.1.4 and note that $\bar{\rho}$ is indecomposable iff it has one neighbor. Such a vertex is called a leaf. We recall a theorem from [53] which say trees have leaves, and this gives us the desired lattice. □

In this thesis, we will be dealing with reducible, indecomposable representations. In view of Ribet's lemma, we would like to pin down our choice of lattice. Note that the proof of Ribet's lemma gives us not one but two lattices sitting on opposite sides of our tree.



And $\bar{\rho}$ is indecomposable for exactly 2 lattices, and let us denote the 2 representations by $\bar{\rho}_1$ and $\bar{\rho}_2$. If $\bar{\rho}^{ss} = \chi_1 \oplus \chi_2$, then $\bar{\rho}_1 \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ and $\bar{\rho}_2 \cong \begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix}$ Since we are dealing with odd representations, i.e $\det(\rho(c)) = -1$ for any choice of complex conjugation c, the order the diagonal characters is determined by fixing a basis for the complex conjugation. So one still manages to get a unique lattice, even if the $\bar{\rho}$ is not irreducible. In fact one has the following corollary.

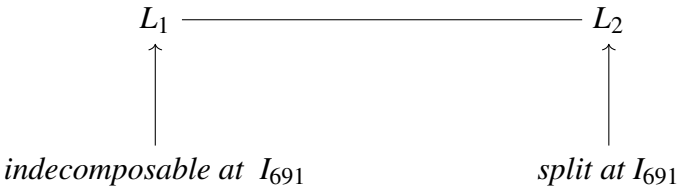
Corollary 3.1.13. *At least one of the indecomposable $\bar{\rho}$ constructed above has the added property that $\bar{\rho}$ restricted to inertia group at p is indecomposable.*

Proof. This is corollary 5 on page 190 in [38]. □

Example : Let $p = 691$, Deligne constructs a Galois representation attached to the Ramanujan cusp form Δ. The following is an unpublished result of Greenberg-Monsky, the

proof of which can recently be found in [70].

Proposition 3.1.14. *(Greenberg-Monsky, Yan) There are exactly* 2 *lattices (up to homothety) for the Galois representation associated to* Δ *such that the mod* 691 *representation is reducible and indecomposable with the diagonal characters* 1 *and* ω^{11} *occurring in opposite orders. So the lattice chain looks like:*



Remark 3.1.15. Our previous discussion shows that at least one of the $\bar{\rho}$ is not semi-simple at I_{691}. Note that the $\bar{\rho}_2$ which is the reduction of the lattice L_2 has the shape $\begin{pmatrix} 1 & * \\ 0 & \omega^{11} \end{pmatrix}$. Since $\mathbb{Q}(\mu_{691})$ has a cyclic 691 degree extension, unramified everywhere with ω^{-11}-action, we see that $*$ on I_{691} is trivial. In fact, exercise 8.9 in [67] shows how to find a Kummer generator for the extension. So this implies that $\bar{\rho}_1$ contains a wildly ramified 691 degree extension over $\mathbb{Q}(\mu_{691})$. This can also be verified by checking that the ω^{11} component of the 691 class group of $\mathbb{Q}(\mu_{691})$ is trivial.

Remark 3.1.16. Serre in [51] observed that the number of lattices is tied to the fact that ρ_Δ is not reducible mod 691^2. Greenberg and Monsky used that idea and showed that the piece of the 691-Hilbert class field of $\mathbb{Q}(\mu_{691})$ corresponding to the character ω^{-11} is contained in the field extension of $\mathbb{Q}$ cut out by Deligne's 691-adic representation of $G_\mathbb{Q}$ associated with Δ. We use Serre's observation as our motivation to carry out these investigations for the elliptic curves of conductor 11 and more general reducible representations in Section 3.5 and 3.6.

Lemma 3.1.17. *(Schur) If* $\bar{\rho}$ *is absolutely irreducible, then* $\mathrm{End}_{k_L[G]}(\bar{\rho}) = k_L$.

Note: The converse is not true. For example the centralizer of the Borel in $Gl_2(k_L)$ is k_L.

Definition 3.1.18. We call a representation $\bar{\rho}$ Schur if $End_{k_L[G]}(\bar{\rho}) = k_L$.

From now on, let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$ (with discrete topology) and let $\mathscr{O}$ be a complete local Noetherian algebra with maximal ideal $\mathfrak{m}_{\mathscr{O}}$ with residue field $\mathbb{F}$ and we fix an isomorphism $\mathscr{O}/\mathfrak{m}_{\mathscr{O}} \cong \mathbb{F}$. Let $\mathscr{C}_{\mathscr{O}}$ be the category of complete, local Noetherian $\mathscr{O}$-algebras with residue field $\mathbb{F}$. The objects are A with maximal ideals $\mathfrak{m}_A$ such that the structural map $\mathscr{O} \to A$ induces an isomorphism $\mathscr{O}/\mathfrak{m}_{\mathscr{O}} \cong A/\mathfrak{m}_A$. Maps are local ring homomorphisms compatible with the identification of residue fields with $\mathbb{F}$.
We will now prove a version of Schur's lemma for objects in $\mathscr{C}_{\mathscr{O}}$.

Lemma 3.1.19. *Let $A \in \mathscr{C}_{\mathscr{O}}$, $\rho : G \to GL_n(A)$ and $End_{\mathbb{F}[G]}(\bar{\rho}) = \mathbb{F}$. Then $End_{\mathbb{F}[G]}(\rho) = A^*$.*

Proof. This is essentially the proof of Mazur in [37]. So we only give a sketch. The idea is to use completeness and reduce to the case of Artinian local $\mathscr{O}$-algebras and then induct on the length of A. The base case is when length of A is 0, i.e. $A = \mathbb{F}$ and the induction step is $\mathbb{F}[\varepsilon]/(\varepsilon^2)$. Assume now A is local Artinian:

$$0 = \mathfrak{m}_A^{e+1} \subsetneq \mathfrak{m}_A^e \subsetneq ...\mathfrak{m}_A \subsetneq A$$

with each quotient an $\mathbb{F}$-vector space. Choose a minimal non-zero ideal $I \in \mathfrak{m}_A^e$ which is a 1-dimensional $\mathbb{F}$-vector space, and by choosing an $\mathbb{F}$ basis, we identify I with $\mathbb{F}$. Now let $M \in GL_n(A)$ commute with ρ. The induction hypothesis implies $M \bmod I \in \mathrm{End}_{A/I}(\rho \bmod I) \cong (A/I)^*$. So M is of the form $M = \alpha I_n + M_0$, where $M_0 \in M_n(I)$. Now for all $g \in G$, $(\alpha I_n + M_0)\rho(g) = \rho(g)(\alpha I_n + M_0)$, which implies $M_0\rho(g) = \rho(g)M_0$. And by the above identification, we can view the above equation in $M_n(\mathbb{F})$. And Schur's lemma holds in this case. So M_0 is also a scalar and this proves the lemma. □

Lemma 3.1.20. *(Carayol, Serre) Let $A, B \in \mathscr{C}_{\mathcal{O}}$ and $B \subset A$ closed. Let $\rho : G \to GL_n(A)$. Assume $\bar{\rho}$ is irreducible and tr(ρ) lies in B. Then there exists $M \in \ker(GL_n(A) \to GL_n(\mathbb{F}))$ such that $M\rho(G)M^{-1} \in GL_n(B)$.*

Proof. This is proposition 2.13 in [24]. □

Remark 3.1.21. This lemma is the main ingredient to show that $R_{\bar{\rho}}^{univ}$ is generated by the traces of the Frobenii.

Remark 3.1.22. One can also replace the finite field $\mathbb{F}$ by any other other field k with trivial Brauer group, i.e. $H^2(k, \bar{k}^*) = 0$.

However there is a generalization of Carayol's lemma due to Kisin which will be used throughout the thesis. The main application of this lemma will appear in Chapter 3. See the section on Pseudorepresentations for more details.

3.2 Preliminaries on deformation theory

Definition 3.2.1. Let $\bar{\rho} : G \to GL_n(\mathbb{F})$ be Schur (definition 3.1.18) and define the deformation problem $\mathscr{R}_{\bar{\rho}}$ from $\mathscr{C}_{\mathscr{O}}$ to SETS to be given by:

$$A \mapsto \{\rho : G \to GL_n(A) : \rho \bmod \mathfrak{m}_A = \bar{\rho}\}/\cong$$

Note:

$$\rho_1 \cong \rho_2 \Leftrightarrow \exists M \in \ker(GL_n(A) \to GL_n(\mathbb{F})), M\rho_1 M^{-1} = \rho_2$$

Theorem 3.2.2. *(Mazur):(a) (Existence) $\mathscr{R}_{\bar{\rho}}$ is representable by a ring, say $\mathscr{R}_{\bar{\rho}}^{univ}$.*
(b) (Twisting by character) If $\bar{\rho}'$ is another representation equivalent to $\bar{\rho} \otimes \chi$ where χ is a character, then there is a canonical isomorphism between $\mathscr{R}_{\bar{\rho}}^{univ}$ and $\mathscr{R}_{\bar{\rho}'}^{univ}$

Proof. See [37]. □

Before we delve into deeper properties of this ring and define interesting deformation problems, let us state the $n = 1$ case. This will be important to us later on.

Proposition 3.2.3. *The universal deformation ring for a character $\bar{\chi} : G_{\mathbb{Q}} \to \mathbb{F}^*$ is $W(\mathbb{F})([[G_{\mathbb{Q}}^{ab,(p)}]])$ where $W(\mathbb{F})$ is the ring of Witt vectors, $G_{\mathbb{Q}}^{ab,(p)}$ is the abelianization of its pro-p completion. In fact $R \cong W(\mathbb{F})[[X_1, ...X_k, Y]]/((1+X_i)^{p_i^e} - 1))$, where k is the number of primes in S congruent to 1 mod p and $e_i = val_p(l_i - 1)$. We will call it the Iwasawa algebra. The reason for this will be clear at the end of the next example.*

Remark 3.2.4. Even though the above ring is formally smooth, its special fiber is complicated. To work with the special fiber, Mazur-Wiles introduced sheets. We will restrict ourselves to a very special case to avoid dealing with sheets.

Example 3.2.5. *Let p be an odd prime, $S = \{p\}$, $\mathbb{F} = \mathbb{F}_p$ and G =Gal ($\mathbb{Q}_S/\mathbb{Q}$). In that case, the deformation ring is $\mathbb{Z}_p[[1 + p\mathbb{Z}_p]]$, which is the usual Iwasawa algebra.*

Remark 3.2.6. Given a residual representation $\bar{\rho}$, $\det(\bar{\rho})$ is a 1-dimensional representation. If ρ is a deformation to a ring R, then clearly $\det(\rho)$ is a deformation of $\det(\bar{\rho})$. If ρ^{univ} is the universal deformation, then it follows $\det(\rho^{univ})$ is a deformation of $\det(\bar{\rho})$ to $\mathscr{R}_{\bar{\rho}}^{univ}$. By the universal property, there exists a unique map, which we will call "det", from the Iwasawa algebra to $\mathscr{R}_{\bar{\rho}}^{univ}$ which allows us to view $\mathscr{R}_{\bar{\rho}}^{univ}$ as an algebra over the Iwasawa algebra.

In certain situations, we will demand our deformations to have a fixed determinant. One can then easily show the existence of a universal deformation ring $\mathscr{R}_{\bar{\rho}}^{univ,det}$ as parametrizing deformations of $\bar{\rho}$ to $\mathscr{C}_{\mathscr{O}}$ with a fixed determinant.
We now define and compute tangent spaces of some deformation rings.

Definition 3.2.7. For a ring $R \in \mathscr{C}_{\mathscr{O}}$, its tangent space is defined as

$$t_R := \text{Hom}_{\mathscr{O}}(R, \mathbb{F}[\varepsilon]/\varepsilon^2) \cong \text{Hom}_{\mathbb{F}}(\mathfrak{m}_R/(\mathfrak{m}_R^2 + \mathfrak{m}_{\mathscr{O}}R), \mathbb{F})$$

Remark 3.2.8. Given two deformations of $\bar{\rho}$ to $\mathbb{F}[\varepsilon]/(\varepsilon^2)$ given by the matrices

$$A_i = \begin{pmatrix} a + a_i'\varepsilon & b + b_i'\varepsilon \\ c_i'\varepsilon & d + d_i'\varepsilon \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{bmatrix} 1 + M_i\varepsilon \end{bmatrix}$$

then one can define the sum A as follows:

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{bmatrix} 1 + (M_1 + M_2)\varepsilon \end{bmatrix}.$$

This will be used in our calculation of tangent spaces.

Proposition 3.2.9. *a)* $t_{\mathscr{R}_{\bar{\rho}}^{univ}} \cong \text{H}^1(G, ad\bar{\rho})$, *where* $ad\,\bar{\rho}$ *is the space of* 2×2 *matrices over* $\mathbb{F}$ *on which* $\bar{\rho}$ *acts by conjugation.*

b) $t_{\mathscr{R}_{\bar{\rho}}^{univ,det}} \cong H^1(G,\ ad^0\bar{\rho})$ *where* $ad^0\bar{\rho}$ *is the space of* 2×2 *matrices with trace* 0 *over* $\mathbb{F}$ *on which* $\bar{\rho}$ *acts by conjugation.*

c) $\mathscr{R}_{\bar{\rho}}^{univ}$ *has a presentation* $\mathscr{R}_{\bar{\rho}}^{univ} \cong \mathscr{O}[[T_1,T_2,..,T_d]]/J$ *where d is the dimension of* $H^1(G,\ ad\bar{\rho})$ *as an* $\mathbb{F}$*-vector space, and there exists a surjective homomorphism*

$$H^2(G,\ ad\bar{\rho})^* \twoheadrightarrow J/\mathfrak{m}_{\mathscr{O}[[T_1,..T_d]]}J$$

where $H^2(G,ad\bar{\rho})^*$ *is the* $\mathbb{F}$*-dual of the* $\mathbb{F}$*-vector space* $H^2(G,ad\bar{\rho})$.

d) $\mathscr{R}_{\bar{\rho}}^{univ,det}$ *has a presentation* $\mathscr{R}_{\bar{\rho}}^{univ,det} \cong \mathscr{O}[[T_1,T_2,..,T_{d_1}]]/J_1$ *where* d_1 *is the dimension of* $\mathrm{H}^1(G,\ ad^0\bar{\rho})$ *as an* $\mathbb{F}$*-vector space, and there exists a surjective homomorphism*

$$H^2(G,\ ad^0\bar{\rho})^* \twoheadrightarrow J_1/\mathfrak{m}_{\mathscr{O}[[T_1,..T_d]]}J_1$$

Proof. See [18] □

The previous discussions show

$$R_{\bar{\rho}}^{univ} \cong \mathscr{R}_{\bar{\rho}}^{univ,det}\hat{\otimes}_{W(\mathbb{F})}W(\mathbb{F})[[G^{ab,(p)}]]$$

So we don't really lose any information or restrict the problem if we fix a determinant. On the automorphic side, this corresponds to fixing the central character (in general) or the weight of the modular form (in our particular case).

Instead of fixing the determinant, or rather allowing the determinant to arbitrarily vary, we will impose the following condition on the determinant:

Definition 3.2.10. Define the deformation problem from $\mathscr{C}_{\mathscr{O}}$ to SETS

$A \mapsto \{\rho : G \to GL_2(A) : \rho \bmod m_A = \overline{\rho},$

$\det\rho = \chi_1\chi$, where χ is trivial on $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and

$\chi_1 = [\det\overline{\rho}|_{Gal(\mathbb{Q}_S/\mathbb{Q}(\mu_{p^\infty}))}]$, where $[\,]$ denotes the Teichmüller lift.$\}$

We will refer to such a deformation problem as a deformation with a fixed Neben character, i.e. we have fixed the non-p and tame p-part of the determinant, or in short **Neben**.

Remark 3.2.11. About the notation regarding χ_1, these are the characters that are referred to as characters of the first kind by Iwasawa. Recall that a character is of first kind if p^2 does not divide its conductor.

Lemma 3.2.12. *The above is a deformation problem and is given by a quotient of $\mathscr{R}^{univ}$. We will denote it by $\mathscr{R}^{univ,det=\chi_1}$. Furthermore, $\mathscr{R}^{univ,det=\chi_1}$ is a $\Lambda = W(\mathbb{F})[[Y]]$ algebra via the determinant map.*

Proof. (Sketch) Since this condition looks a bit non-standard, we give a quick sketch to show what it means for a collection $\mathscr{D}$ of liftings (R,ρ) of $(\mathbb{F},\overline{\rho})$ to be a deformation problem. Recall that one needs to check the following conditions:

1. $(\mathbb{F},\overline{\rho}) \in \mathscr{D}$

2. If $f : R \to S$ is a morphism in $\mathscr{C}_{\mathscr{O}}$ and $(R,\rho) \in \mathscr{D}$, then $(S, f\circ\rho) \in \mathscr{D}$. The converse holds if f is injective.

3. Suppose $R_1, R_2 \in \mathscr{C}_{\mathscr{O}}$, I_1, I_2 are ideals of R_1, R_2 respectively, such that there is an isomorphism $f : R_1/I_1 \xrightarrow{\sim} R_2/I_2$. Suppose (R_1,ρ_1) and $(R_2,\rho_2) \in \mathscr{D}$ and $f \circ (\rho_1 \bmod I_1) = \rho_2 \bmod I_2$.

$$\text{Then } \ (\{(a,b) \in R_1 \times_{R_1/I_1} R_2; \rho_1 \times_{R_1/I_1} \rho_2\}) \in \mathscr{D}.$$

4. If (R,ρ) is any lifting and $I_1 \supset I_2 \supset \ldots$ is a sequence of ideals in R with $\cap_j I_j = 0$ and $(R/I_j, \rho \bmod I_j) \in \mathscr{D}$ for all j, then $(R,\rho) \in \mathscr{D}$.

5. If $(R,\rho) \in \mathscr{D}$ and $x \in \ker(Gl_2(A) \to GL_2(\mathbb{F}))$, then $(R, x\rho x^{-1}) \in \mathscr{D}$.

Checking these conditions is straightforward. One just needs that Teichmüller lifts are given by $\omega(x) = \lim x^{p^n}$ and f is a continuous homomorphism. Then [20] tells us that there exist a closed ideal in $\mathscr{R}^{univ}_{\bar{\rho}}$ such that the deformation problem is represented by $\mathscr{R}^{univ}_{\bar{\rho}}/I$. □

Remark 3.2.13. This condition on determinants is satisfied by Hida families. See the next chapter. So it's a fairly natural condition to impose on our deformations.

We will finish this section by constraining our deformations to have certain local conditions. These local deformations are well understood. For the remainder of the section, let $l \neq p$. The references are [60] and [12].

Choose an embedding $G_{\mathbb{Q}_l} \hookrightarrow G_{\mathbb{Q}_S}$.

Minimal deformations : Let $p \nmid \bar{\rho}(I_l)$. Take C_l to be the class of lifts of $\bar{\rho}|_{G_{\mathbb{Q}_l}}$ that factor through $G_l/I_l \cap ker(\bar{\rho})$ with fixed determinant. Then Taylor shows that these deformations correspond to the subspace $\mathscr{L}_l \subset H^1(G_{\mathbb{Q}_l}, ad^0\bar{\rho})$ given by $H^1(G_l/I_l, (ad^0\bar{\rho})^{I_l})$. The corresponding deformation problem is smooth and the universal deformation ring is given by $W(\mathbb{F})[[T_d]]$ where $d = H^0(G_{\mathbb{Q}_l}, ad^0\bar{\rho})$.

Steinberg deformations : Suppose $l \not\equiv 1 \pmod{p}$ or $p \mid \bar{\rho}(I_l)$. And let $\bar{\rho} = \begin{pmatrix} \omega\bar{\delta} & * \\ & \bar{\delta} \end{pmatrix}$. Following Taylor in [60], we define C_l to be the class of deformations where ρ (with respect to some basis) is of the form $\begin{pmatrix} \chi_{cyc}\delta & * \\ 0 & \delta \end{pmatrix}$ where χ_{cyc} is the p-adic cyclotomic character. Sometimes, in literature, authors twist the representation by δ and only define Steinberg deformations with cyclotomic determinant. Note that if $l \not\equiv 1 \bmod p$, ω is non-trivial and in this case, if $* \pmod{p} = 0$, we have to use versal deformation rings or one has to choose an inertia fixed line to rigidify the problem. The second method was used by Dickinson

and Calegari-Emerton [8]. In any case, we see that the deformation problem is smooth as well and the (uni)versal ring is given by $W(\mathbb{F})[[T_d]]$ where $d = H^0(G_l, ad^0\bar{\rho})$. Finally if $l \equiv 1 \pmod{p}$ and $* \pmod{p} = 0$, one follows Kisin's method. However we will not be dealing with that case. Before we move to the next section, let us make a few remarks. $\bar{\delta}$ may be unramified but δ can be ramified and this can only happen if $l \equiv 1 \pmod{p}$. However **Neben** prevents such a situation to happen. Finally we will take $* \pmod{p} \neq 0$, then the same computations as before will show that the dimension of the tangent space is $h^0(G_{\mathbb{Q}_l}, ad^0\bar{\rho}) = 0$.

Since we will be dealing with square free level N, we shall take $\delta = 1$, otherwise $f_\delta^2 | N$. The Steinberg condition will be particularly important for us later so we will study it in some detail.

Now let us consider the case when $l \equiv 1 \pmod{p}$ and $*|_{I_l} \pmod{p} \neq 0$, thus $* \pmod{p}$ corresponds to a ramified cocycle in $H^1(\mathbb{Q}_q, \mathbb{F})$, call it $\bar{b}$. Let a characteristic 0 lift ρ be of the form $\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}$. We show that if $c(\tau) = 0$ for all $\tau \in I_l$, then $c = 0$ on $G_{\mathbb{Q}_l}$.

Let σ be the Frobenius at l, then we have the following relation:

$$\sigma\tau\sigma^{-1} = \tau^l. \tag{3.1}$$

Let $\rho(\sigma) = \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}$ and $\rho(\tau) = \begin{pmatrix} 1 & x \\ & \\ 0 & 1 \end{pmatrix}$ and using the above equation, we immediately get $c = 0$.

In fact we can say more. Note by [60], we know the universal deformation ring for Steinberg representations is $W(\mathbb{F}) := \mathscr{O}$. Let λ be an uniformizer of $\mathscr{O}$. Then factoring out an appropriate power of λ, we can consider that c takes values in $\mathscr{O}$. Now

$c \pmod{\lambda}$ is a ramified 1-cocycle with values in $\mathbb{F}$, i.e. $c \pmod{\lambda} \in H^1(\mathbb{Q}_q, \mathbb{F})$. We

know by Tate duality (theorem 2.2.3) and the Local Euler-Poincare characteristic formula (proposition 2.2.4) that $H^1(\mathbb{Q}_q,\mathbb{F})$ is a 2 dimensional $\mathbb{F}$ vector space and is spanned by two cocycles $\bar{b}$ and $\bar{b}'$, where $\bar{b}$ is the ramified cocycle and $\bar{b}'$ is the unramified one. We now show that $\bar{c} := c \pmod{\lambda}$ is an $\mathbb{F}$ multiple of b. If not, let $\bar{c} = x\bar{b} + y\bar{b}'$ Since by definition of Steinberg deformations, any lift of $\bar{\rho}$ can be conjugated into an upper triangular matrix, we can now construct a non-trivial deformation to $\mathbb{F}[\varepsilon]$ by the following $\begin{pmatrix} 1 & \bar{b}+\varepsilon(x\bar{b}+y\bar{b}') \\ & 1 \end{pmatrix}$. But that contradicts the fact the the dimension of the tangent space is 0, i.e., there are no non-trivial upper triangular deformations. We record this discussion in the form of a proposition.

Proposition 3.2.14. *Let $\bar{\rho} : G_{\mathbb{Q}_l} \to GL_2(\mathbb{F})$ be of the form $\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}$, where $b|_{I_l} \neq 0$. Consider the problem of Steinberg deformations. Then $\bar{c}$ constructed above is either split at l, i.e. $\bar{c}(G_{\mathbb{Q}_l}) = 0$ or $\bar{c}$ is totally and tamely ramified at l and $\bar{c} = kb$ for some $k \in \mathbb{F}$.*

This idea will be used later on in our section on pseudo-deformations.

Definition 3.2.15. We call a prime l difficult if $l \equiv 1 \pmod{p}$ and $\bar{\rho} : G_{\mathbb{Q}_l} \to GL_2(\mathbb{F}) = \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$, where $*|_{I_l} \neq 0$.

In fact we can also pin down when $\bar{c}$ is ramified and when it is split.

Let ρ be any lift of $\bar{\rho}$ to A then $\rho(I_l) \subset SL_2(A)$, since $\det(\rho)$ is unramified at l. Since I_l is pro-cyclic, the image of I_l will be a cyclic p group. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(A)$ be a non-identity matrix whose order is a power of p. Since the minimal polynomial of the matrix divides the characteristic polynomial, we immediately get the following equations

- $a + d = 2$

- $ad - bc = 1$

Thus if a or $d = 1$, this forces $bc = 0$, and since b is an unit, $c = 0$. Thus we get an easy criteria to check if $\bar{c}$ is non-zero. We record this result in the form of an easy proposition.

Proposition 3.2.16. *$\bar{c} \neq 0$ iff there exist a lift* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *with a or $d \neq 1$.*

For $l = p$, we choose the ordinary condition. This will be discussed in some detail in the next section. Morally speaking, we would like our deformations to look similar to $\bar{\rho}$ when restricted to various decomposition subgroups. In this thesis, we will not consider the case where $\bar{\rho}|_{G_{\mathbb{Q}_l}}$ is unramified but it's lift is of Steinberg type.

3.3 Ordinary deformations

Definition 3.3.1. We call $\bar{\rho} : G_{\mathbb{Q}_p} \to GL_2(\mathbb{F})$ ordinary if

$$\rho \cong \begin{pmatrix} \bar{\delta} & * \\ 0 & \bar{\psi} \end{pmatrix}$$

where $\bar{\psi}$ is an unramified character.

Remark 3.3.2. The choice of the stable line will depend on the embedding $G_{\mathbb{Q}_p} \subset G_{\mathbb{Q},S}$, but any two embeddings are conjugate by some $g \in G_{\mathbb{Q},S}$ and that g will transport one stable line in one embedding to a stable line to the other embedding. If $G_{\mathbb{Q}_p}$ stabilizes more than one line, we will choose a line and we will call it a special line. Mazur calls this a choice of p-stabilization.

Definition 3.3.3. We call an ordinary representation mod-p distinguished if $\bar{\delta} \neq \bar{\psi}$.

Remark 3.3.4. This definition implies that there are at most two special lines.

Assumption $(\mathbf{Non-CM})$ We will assume the * in the above definition is non-zero.

Remark 3.3.5. The above assumption along with the previous definitions and comments imply that there is an unique special line.

Remark 3.3.6. The non-vanishing of $*$ is strongly related to the fact that if this ρ is attached to a modular form f, then f is not a CM form. For more precise statement, we refer the reader to the papers on local indecomposability of non-CM forms by E. Ghate.

Under the above assumption we have the following theorem:

Theorem 3.3.7. *There exist an universal ordinary deformation of $\bar{\rho}$ call it ρ^{ord} and an universal deformation ring which we call R^{ord} such that $\rho^{ord} \cong \begin{pmatrix} \delta & * \\ 0 & \psi \end{pmatrix}$ where ψ is an unramified character and $* \neq 0$.*

Proof. This is Theorem 3.30 in [24] □

There is a related concept called nearly ordinary deformation rings.

Definition 3.3.8. A representation $\rho : G_{\mathbb{Q}_p} \to GL_2(A)$ is called nearly ordinary if

$$\rho \cong \begin{pmatrix} \bar{\chi}_{cyc}^{i_1}\delta & * \\ 0 & \bar{\chi}_{cyc}^{i_2}\psi \end{pmatrix}$$

and δ and nd ψ are unramified characters and $i_1 > i_2$.

It is not hard to see that this a representable deformation problem and the universal deformation ring is denoted by $R^{n.ord}$ and ordinary deformations form a subfunctor of nearly ordinary deformations. The technical reason for introducing these objects are that they are twist invariant. In fact, if V is an ordinary deformation then $V^*(1)$ in general will not be ordinary but will be nearly ordinary. Nonetheless $V^*(k)$ will be ordinary for some $k \geq 1$.

Remark 3.3.9. If we assumed $* \bmod p = 0$, we will modify the deformation problem by the following: We will consider pairs (V_A, L_A), where $A \in \mathscr{C}_{\mathscr{O}}$ where $\rho : G_p \to GL(V_A)$ with fixed determinant and is given by $\begin{pmatrix} \delta & * \\ 0 & \psi \end{pmatrix}$ and L_A is a free unramified rank 1 A-submodule and L_A reduces to $\bar{\psi}$. One can show that this deformation problem is now representable, call this $R^{ord,det,L}$.

Theorem 3.3.10. $R^{ord} \cong \mathscr{O}[[T]]$.

Proof. This is well-known to due to works of Wiles and Mazur. For example one can see section 2 of [12] or Proposition 3.6 in [30] or example 6.5 Case-2, subcase (ii) in [5]. Of all the references, the computations in [5] with upper triangular lifts are similar to our computations on obstructions in the next section. □

3.4 Computations of some tangent spaces and obstruction classes

For the rest of the section, fix a $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ where $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$ and

$$\bar{\rho} \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \text{ with } \chi_1 \neq \chi_2$$

such that $\bar{\rho}$ is unramified outside of a finite set of primes, i.e. $\bar{\rho}$ factors through $G_{\mathbb{Q},S}$ where $G_{\mathbb{Q},S}$ is the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside S and S is a finite set of primes including p and ∞.

Under the above hypothesis, Theorem 3.2.2 guarantees the existence of the universal deformation ring, which we call $\mathscr{R}_{\bar{\rho}}^{univ}$.

Before stating the main theorem, let us make the following assumption.

Hypothesis 1 : $\dim_{\mathbb{F}} \mathrm{Ext}^1(\chi_2, \chi_1) = 1$.

Let us now fix a non-zero element in $\mathrm{Ext}^1(\chi_2, \chi_1)$ and let us call it b.

The main result of this section gives a complete description of the tangent space of this ring in terms of the Jordan-Hölder factors of $\bar{\rho}$ and assume we are in any one of the conditions satisfied by proposition 2.3.5.

Theorem 3.4.1. *Assume we do not have any difficult primes in our deformations. Then there exists an exact sequence*

$$0 \longrightarrow \mathrm{Ext}^1(\chi_1, \chi_1) \oplus \mathrm{Ext}^1(\chi_2, \chi_2) \xrightarrow{f} t_{\mathscr{R}_{\bar{\rho}}^{univ}} \xrightarrow{\kappa} \mathrm{Ext}^1(\chi_1, \chi_2) \xrightarrow{\cup} 0$$

Proof. Let ρ be any lift of $\bar{\rho}$ to $GL_2(\mathbb{F}[\varepsilon]/\varepsilon^2)$ given by the matrix $\begin{pmatrix} a + a'\varepsilon & b + b'\varepsilon \\ c'\varepsilon & d + d'\varepsilon \end{pmatrix}$.

For the above lift to be a group homomorphism, the coefficients satisfy the following relations.

1. $a = \chi_1$
2. $a'_{gh} = a_g a'_h + a_h a'_g$ or in other words a'/a is a continuous group homomorphism from $G_{\mathbb{Q},S} \to \mathbb{F}$. Lemma 2.3.1 counts the number of such homomorphisms.
3. $d = \chi_2$
4. $d'_{gh} = d_g d'_h + d_h d'_g$
5. $c'_{gh} = d_g c'_h + c'_g a_h$ or in other words $c' \in \mathrm{Ext}^1(\chi_1, \chi_2)$.
6. $b_{gh} = a_g b_h + b_g d_h$
7. $b'_{gh} = a'_g b_h + a_g b'_h + b'_g d_h + b_g d'_h$

The map κ is defined by sending $\left[\begin{pmatrix} a+a'\varepsilon & b+b'\varepsilon \\ c'\varepsilon & d+d'\varepsilon \end{pmatrix}\right]$ to c'.
First we show that the map is well-defined. Suppose we are given two deformations which are equivalent, i.e. there exists a matrix $\begin{pmatrix} 1+x\varepsilon & y\varepsilon \\ z\varepsilon & 1+w\varepsilon \end{pmatrix}$ that conjugates a deformation ρ_1 to ρ_2. Let c_i be the bottom left corner of ρ_i. Then

$$c_2 = c_1 + (a-d)z$$

To show that the map is well-defined, we want to show c_i's give rise to the same extensions up to isomorphism. Indeed, the matrix $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ conjugates $\begin{pmatrix} d & c_1 \\ 0 & a \end{pmatrix}$ to $\begin{pmatrix} d & c_2 \\ 0 & a \end{pmatrix}$.
Thus the map is well defined.

To show that it is a group homomorphism: Note that by remark 3.2.8, the bottom left corner of the sum of two deformations is given by $(c_1+c_2)\varepsilon$ and so the fact that g is a group homomorphism is obvious.

Then we show that the map is surjective. Given an extension class $c \in \mathrm{Ext}^1(\chi_1,\chi_2)$, the cup products $b_g c_h$ and $c_g b_h$ are a priori in $Z^2(a,a)$ and $Z^2(d,d)$ respectively but by proposition 2.3.5, we know that these cocycles are actually in $B^2(a,a)$ and $B^2(d,d)$ respectively. Thus there exist functions $\alpha,\beta : G \to \mathbb{F}$, such that

- $b_g c_h = \alpha(gh) - a_g\alpha(h) - a_h\alpha(g)$
- $c_g b_h = \beta(gh) - d_g\beta(h) - d_h\beta(g)$

Consider the map $r : G\times G \to \mathbb{F}$, given by $r(g,h) = \alpha(g)b_h + b_g\beta(h)$. An easy but long and tedious calculation shows that $r \in Z^2(\chi_2,\chi_1)$. Again, by the global Euler characteristic formula 2.3.13, we see that $Z^2(\chi_2,\chi_1) = B^2(\chi_2,\chi_1)$. Thus there exists a function μ such that $\mu(gh) = r(g,h) - a_g\mu(h) - d_h\mu(g)$. Finally, we can construct a lift of $\bar{\rho}$ as $\begin{pmatrix} a+\alpha\varepsilon & b-\mu\varepsilon \\ c\varepsilon & d+\beta\varepsilon \end{pmatrix}$. The kernel of the map κ is the group of all upper triangular lifts.

To define the map f, let us observe the following facts.

(a) If $\begin{pmatrix} a & b+b'\varepsilon \\ 0 & d \end{pmatrix}$ is a lift $\bar{\rho}$, then an easy calculation shows that $b'_{gh} = a_g b'_h + b'_g d_h$ and by taking strict equivalence into account, $b' \in \mathrm{Ext}^1(\chi_2,\chi_1)$ so by our assumption $b' = kb$. And finally note that $\begin{pmatrix} a & b+kb\varepsilon \\ 0 & d \end{pmatrix} \cong \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ as the matrix $\begin{pmatrix} 1+k\varepsilon & 0 \\ 0 & 1 \end{pmatrix}$ conjugates $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ to $\begin{pmatrix} a & b+kb\varepsilon \\ 0 & d \end{pmatrix}$.

(b) Finally given a,a',b,d,d', we can construct a unique upper triangular lift by hand. Note that $a'_g b_h$ and $b_g d'_h$ lie in $Z^2(\chi_2,\chi_1)$. By our assumption and by the Global Euler-Poincare

characteristic formula (cf. proposition 2.3.13), we get $Z^2(\chi_2,\chi_1)$ is $B^2(\chi_2,\chi_1)$. So there exist functions α and β such that

1. $b_h a'_g = a_g\alpha(h) - \alpha(gh) + d_h\alpha(g)$

2. $b_g d'_h = a_g\beta(h) - \beta(gh) + d_h\beta(g)$

Our desired lift is then of the form $\begin{pmatrix} a+a'\varepsilon & b+(-\alpha-\beta+kb)\varepsilon \\ 0 & d+d'\varepsilon \end{pmatrix}$

Finally , if $\begin{pmatrix} a+a'\varepsilon & b+b'_1\varepsilon \\ 0 & d+d'\varepsilon \end{pmatrix}$ and $\begin{pmatrix} a+a'\varepsilon & b+b'_2\varepsilon \\ 0 & d+d'\varepsilon \end{pmatrix}$ are 2 lifts, then $b'_{1,gh} - b'_{2,gh} = a_g(b'_{1,h} - b'_{2,h}) + d_h(b'_{1,g} - b'_{2,g})$, i.e. $b'_1 - b'_2 = kb$. And the same calculation as before shows that these matrices are conjugate. The same calculations also show that changing our functions α and β do not change the strict equivalence class of our lift. Thus in our lift, we can take $k = 0$.

We are now in a position to define the map f.

Given a' in $\mathrm{Ext}^1(\chi_1,\chi_1)$, we map it to $\begin{pmatrix} a+a'\varepsilon & b-\alpha\varepsilon \\ 0 & d \end{pmatrix}$ and $d' \in \mathrm{Ext}^1(\chi_2,\chi_2)$, we map it to $\begin{pmatrix} a & b-\beta\varepsilon \\ 0 & d+d'\varepsilon \end{pmatrix}$. By looking at the conjugacy classes to these matrices just as before we see that these maps are well defined, so that gives a map f from $\mathrm{Ext}^1(\chi_1,\chi_1) \oplus \mathrm{Ext}^1(\chi_2,\chi_2)$ to $t_{\mathscr{R}^{univ}_{\bar{\rho}}}$

From the discussion above, we see that f sends $(0,0)$ to the identity. To check that the map is an injection, note that if $M \in \ker(GL_2(\mathbb{F}[\varepsilon] \to GL_2(\mathbb{F}))$ and $M\begin{pmatrix} a+a'\varepsilon & b+b'\varepsilon \\ 0 & d+d'\varepsilon \end{pmatrix}M^{-1} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, then by a tedious matrix calculation one can see that a' and d' are constant multiples of a and d as desired. But this is precisely the 1-coboundary relation. Thus the map is injective. The homomorphism is clear by matrix

multiplication and formulae satisfied by a' and d'. And this gives us the desired theorem.

□

An important consequence is that we can now readily compute the dimension of the tangent space. Since we will be needing this later, we record it in the form of the following corollary.

Corollary 3.4.2. *dim* $t_{R^{univ}_{\bar{\rho}}} = 2\#\{q \equiv 1 \pmod{p}+1\}$ + *dim* $Ext^1(\chi_1,\chi_2)$.

Proof. Follows easily from the previous theorem and Lemma 2.3.1. □

Remark 3.4.3. If we have difficult primes in our deformation problem, then we take $\mathscr{R}^{univ,st}_{\bar{\rho}}$ to be the universal deformation ring parametrizing Steinberg deformations. Then proposition 3.2.14 shows that the cocycles appearing the lower left corner must be either ramified or completely split at l. Let $Ext^1_{ram}(\chi_1,\chi_2) \subset Ext^1(\chi_1,\chi_2)$ be the subspace of all cocycles that are split or ramified at the difficult primes. Then if $c \in Ext^1_{ram}(\chi_1,\chi_2)$, then $b \cup c = 0$ by proposition 2.3.5. Then we have an exact sequence just like in theorem 3.4.1

$$0 \longrightarrow \mathrm{Ext}^1(\chi_1,\chi_1) \oplus \mathrm{Ext}^1(\chi_2,\chi_2) \xrightarrow{f} t_{\mathscr{R}^{univ,st}_{\bar{\rho}}} \xrightarrow{\kappa} \mathrm{Ext}^1_{ram}(\chi_1,\chi_2) \xrightarrow{\cup} 0$$

The proof of this statement is exactly the same as the proof of theorem 3.4.1 since all the relevant cup products are now 0.

Remark 3.4.4. These above exact sequences also appear in the work of Chenevier-Bellaiche, and our proof, even though similar in spirit, is slightly different.

Remark 3.4.5. Define a function $f : G \times G \to \mathbb{F}$ given by

$$f(g,h) = b'_{gh} - a'_g b_h - a_g b'_h - b_g d'_h - b'_g d_h \tag{3.2}$$

where a, a', d, d' are as before but b' is any set theoretic map. An extremely tedious but simple calculation will show $f \in Z^2(\chi_2, \chi_1)$. Or in other words if one twists $\bar{\rho}$ to the following form $\begin{pmatrix} \chi_1\chi_2^{-1} & * \\ 0 & 1 \end{pmatrix}$. The above calculation and previous observations immediately show us that the obstruction to lifting $*$ lies in $H^2(G_{\mathbb{Q},S}, \chi_1\chi_2^{-1})$ which is 0. So there is no obstruction to lifting the top right corner. This observation is actually used in computing the tangent spaces of ordinary deformations and Steinberg deformations.

We define I^{red} to be the smallest ideal such that every lift ρ mod I^{red} is reducible. We call I^{red} the ideal of reducibility and R^{red} the quotient of $\mathscr{R}_{\bar{\rho}}^{univ}$ by I^{red}. One can easily see that R^{red} is the universal ring parameterizing upper triangular lifts. An easy upshot of the above discussion is the following lemma.

Lemma 3.4.6. *$I^{red} \neq 0$ iff $Ext^1(\chi_1, \chi_2) \neq 0$.*

Proof. Suppose $I^{red} \neq 0$, then by our setup, we have an irreducible lift to $\mathbb{F}[\varepsilon]$. The previous calculations then imply the bottom left corner of the lift is a non-trivial element in $\mathrm{Ext}^1(\chi_1, \chi_2)$. Conversely, if $\mathrm{Ext}^1(\chi_1, \chi_2) \neq 0$, then we can construct a non-trivial irreducible lift to $\mathbb{F}[\varepsilon]$, thus $I^{red} \neq 0$. □

In fact one can do better.

Proposition 3.4.7. *If n is the minimal number of generators of I^{red}, then*

$$\dim \mathrm{Ext}^1(\chi_1, \chi_2) \geq n.$$

Proof. The proof follows from noticing that the representation is reducible when $bc = 0$, but one can identify b and c with the appropriate extension classes. Up to scaling by $\mathbb{F}$, we have an unique extension class. For more details see [2], Prop: 1.7.1. □

The following proposition is well-known and gives a complete description of I^{red}.

Proposition 3.4.8. *I^{red} is generated by any of the following sets:*

$\{trace(\rho^{univ}(Frob_l) - [\chi_1](Frob_l) - [\chi_2](Frob_l)) \ : l \notin S\}$

$\{a(\sigma) - [\chi_1](\sigma)\}$

$\{d(\sigma) - [\chi_2](\sigma)\}$

$\{b(\sigma)c(\tau)\}$

where $\rho^{univ} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and by abuse of notation, we denote* $[\chi_i]$ *as the Teichmüller lift of* χ_i *to* $W(\mathbb{F})$ *which is then mapped to* $\mathscr{R}^{univ}_{\bar{\rho}}$ *via the structure map.*

Proof. See [24] or [2]. □

Proposition 3.4.9. $\dim_{\mathbb{F}} t_{R^{red}} = 2\#\{q \equiv 1 \bmod p\} + 2$.

Proof. R^{red} parametrizes upper triangular lifts. Now from the exact sequence in Theorem 3.4.1, the subspace of all lifts (up to equivalence) where $c' = 0$ is given by $\mathrm{Ext}^1(\chi_1, \chi_1) \oplus \mathrm{Ext}^1(\chi_2, \chi_2)$ and we have already seen b' is uniquely determined once these above quantities are fixed. The result follows immediately. □

Remark 3.4.10. It is really important for us that $\dim \mathscr{R}^{univ}_{\bar{\rho}} > \dim R^{red}$.

We will now try to find the obstruction to lifting to an upper triangular representation. Given a surjective ring homomorphism $A_1 \twoheadrightarrow A_0$ with kernel I, generated by a single element with $I \cdot m_{A_1} = 0$, let ρ be a representation to A_0 lifting $\bar{\rho}$ and $\tilde{\rho}$ be any lift of ρ to A_1. To measure if this is a representation we calculate

$$M_{gh} = \tilde{\rho}(gh) - \tilde{\rho}(g)\tilde{\rho}(h) = \begin{pmatrix} \tilde{a}_{gh} - \tilde{a}_g\tilde{a}_h & \tilde{b}_{gh} - \tilde{a}_g\tilde{b}_h - \tilde{b}_g\tilde{d}_h \\ 0 & \tilde{d}_{gh} - \tilde{d}_g\tilde{d}_h \end{pmatrix} \tag{3.3}$$

One can easily see that the above matrix is in $Z^{2,up}(\bar{\rho},\bar{\rho})\otimes I \subset Z^2(\bar{\rho},\bar{\rho})\otimes I$, where $Z^{2,up}$ is the set of matrices with the lower left entry is 0. Write an element in $Z^{2,up}$ as $\begin{pmatrix} f_{11} & f_{12} \\ 0 & f_{22} \end{pmatrix}$. One can see the following relations:

- $f_{11} \in Z^2(a,a)$.
- $f_{22} \in Z^2(d,d)$.
- $a_g f_{12}(g',g'') + b_g f_{22}(g',g'') - f_{12}(gg',g'') + f_{12}(g,g'g'') - f_{11}(g,g')b_{g''} - f_{12}(g,g')d_{g''} = 0$.

Finally if an element $\begin{pmatrix} f_{11} & f_{12} \\ 0 & f_{22} \end{pmatrix}$ is in $B^{2,up}(\bar{\rho},\bar{\rho})$, and we let $\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ 0 & \alpha_{22} \end{pmatrix}$ be the matrix that realizes that coboundary, then we have the following relations:

- $f_{11} \in B^2(a,a)$.
- $f_{22} \in B^2(d,d)$.
- $f_{12}(g,g') = \alpha_{12}(gg') - a_g\alpha_{12}(g') - b_g\alpha_{22}(g') - \alpha_{11}(g)b_{g'} - \alpha_{12}(g)d_{g'}$.

Finally we note M_{gh} is independent (up to a coboundary, i.e. in $B^2(\bar{\rho},\bar{\rho})$, of the choice of a lift $\tilde{\rho}$). Now let us start by assuming that there exists a lift of the diagonal characters to A_1, i.e. we assume that f_{11} and f_{22} are coboundaries. In fact we now choose $\tilde{a}$ and $\tilde{d}$ to be those diagonal characters. This forces $f_{11} = f_{22} = 0$. And the upper right corner takes a very simple form, i.e.

$$a_g f_{12}(g',g'') - f_{12}(gg',g'') + f_{12}(g,g'g'') - f_{12}(g,g')d_{g''} = 0,$$

i.e. $f_{12} \in Z^2(d,a)$. Now let us change $\tilde{b}$ by any function, call it $\tilde{b}^{(1)}$, keeping $\tilde{a}$ and $\tilde{d}$ fixed. Then define $f_{12}^{(1)}$ via

$$f_{12}^{(1)} := \tilde{b}_{gh}^{(1)} - \tilde{a}_g\tilde{b}_h^{(1)} - \tilde{b}_g^{(1)}\tilde{d}_h.$$

Now $\tilde{b}^{(1)} - \tilde{b} \in I$ and

$$f_{12}^{(1)}(g,h) - f_{12}(g,h) = \tilde{b}_{gh}^{(1)} - \tilde{b}_{gh} - \tilde{a}_g(\tilde{b}_h^{(1)} - \tilde{b}_h) - \tilde{d}_h(\tilde{b}_g^{(1)} - \tilde{b}_g)$$

$$= \tilde{b}_{gh}^{(1)} - \tilde{b}_{gh} - a_g(\tilde{b}_h^{(1)} - \tilde{b}_h) - d_h(\tilde{b}_g^{(1)} - \tilde{b}_g)$$

changes f_{12} by an element in $B^2(d,a)$. Let us now summarize the above discussion in the form of two propositions.

Proposition 3.4.11. *There exists an injection $Ext^2(d,a) \hookrightarrow Ext^2(\bar{\rho},\bar{\rho})$.*

Proof. Let $f_{12} \in \mathrm{Ext}^2(d,a)$, then define a class $\begin{pmatrix} 0 & f_{12} \\ 0 & 0 \end{pmatrix}$ in $\mathrm{Ext}^2(\bar{\rho},\bar{\rho})$. The above discussion shows that this map is well-defined. To show injectivity: Let $f,g \in \mathrm{Ext}^2(d,a)$ map to the same element in $\mathrm{Ext}^2(\bar{\rho},\bar{\rho})$, i.e $\begin{pmatrix} 0 & f-g \\ 0 & 0 \end{pmatrix}$ in $B^2(\bar{\rho},\bar{\rho})$. By the previous discussion $f-g \in B^2(d,a)$. This proves the injectivity. □

Proposition 3.4.12. *Assuming the diagonal characters can be lifted, $R^{red} \cong \mathscr{O}[[X_1,...,X_t]]$, where $t = 2\#\{q \equiv 1 \pmod{p}\} + 2$.*

Proof. Under our assumption and by our previous discussion the obstruction to lifting to an upper triangular representation is in $\mathrm{Ext}^2(d,a)$. But our assumption (**Hypothesis 1**) that $\mathrm{Ext}^1(d,a)$ is 1-dimensional and the Euler-Poincare characteristic formula in 2.3.13 immediately tells us that $\dim \mathrm{Ext}^2(d,a) = 0$. Thus the obstruction vanishes. And the proposition follows immediately. □

Corollary 3.4.13. *Assume Hypothesis* 1, **Neben** *and let the deformations be ordinary at p, then $R^{red} \cong R^{ord}$.*

Proof. By previous proposition, we know that the deformation problem is unobstructed and we have also calculated the tangent space. Under **Neben**, the relative dimension of the

tangent space is 1, i.e. $R^{red} \cong \mathscr{O}[[X]]$. There is a canonical surjective map from $R^{ord} \to R^{red}$, since under **Neben** any reducible deformation is automatically ordinary. But a surjection from $\mathscr{O}[[X]] \to \mathscr{O}[[X]]$ is an isomorphism. □

Remark 3.4.14. The above corollary can be summarized by the following statement: There are no non-trivial upper triangular deformations of $\bar{\rho}$ of fixed determinant to $\mathbb{F}[\varepsilon]$.

To conclude our study of the universal deformation ring, we need to study the obstructions to lifting. Recall $A_1 \twoheadrightarrow A_0$ is a map $\mathscr{O}$-algebras with kernel I, generated by a single element with $I \cdot m_{A_1} = 0$. Now let $M := \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$ be a lift to A_1 and we are measuring the failure for this lift to be a homomorphism. Define a function $f_{gh} := \tilde{c}_{gh} - \tilde{c}_g \tilde{a}_h - \tilde{d}_g \tilde{c}_h$. It's easy to check $f_{gh} \in \mathrm{Ext}^2(\mathrm{a},\mathrm{d}) \otimes \mathrm{I}$. Just as before, write the matrix in $Z^2(\bar{\rho},\bar{\rho})$ as $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$.

Proposition 3.4.15. *There exists a surjection $Ext^2(\bar{\rho},\bar{\rho}) \twoheadrightarrow Ext^2(\chi_1,\chi_2)$.*

Proof. First we note that given a matrix in $Z^2(\bar{\rho},\bar{\rho})$ written as $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$, then we immediately see f_{21} satisfies the following relation:

$$d_g f_{21}(g',g'') - f_{21}(gg',g'') + f_{21}(g,g'g'') - f_{21}(g,g')a_{g''} = 0, \ \ \forall\, g,g',g'' \in G.$$

Thus f_{21} is an element in $Z^2(\chi_1,\chi_2)$. Now, if $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \in B^2(\bar{\rho},\bar{\rho})$, then

$$f_{21}(g,h) = \alpha_{21}(gh) - d_g\alpha_{21}(h) - \alpha_{21}(g)a_h,$$

where α_{21} is a function from G to $\mathbb{F}$. Thus the map sending $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \to f_{21}$ is a

well-defined map. It is clearly an $\mathbb{F}$-linear homomorphism. Finally we have to show that the map is surjective. Note that $b_g f_{21}(g',g'') \in Z^3(a,a)$ and $f_{21}(g,g')b_{g''} \in Z^3(d,d)$ but $Z^3(a,a) = B^3(a,a)$ and $Z^3(d,d) = B^3(d,d)$. So there exist functions κ and $\nu : G \times G \to \mathbb{F}$, such that

$$b_g f_{21}(g',g'') = a_g \kappa(g',g'') - \kappa(gg',g'') + \kappa(g,g'g'') - a_{g''}\kappa(g,g')$$

$$f_{21}(g,g')b_{g''} = d_g \nu(g',g'') - \nu(gg',g'') + \nu(g,g'g'') - d_{g''}\nu(g,g').$$

Thus one can construct an element in $Z^2(\rho,\rho)$ given by $\begin{pmatrix} \kappa & 0 \\ f_{21} & \nu \end{pmatrix}$ which maps to f_{21}.

□

Corollary 3.4.16. *Suppose there are no difficult primes then Krull dimension of* $R^{univ}_{\bar{\rho}} \geq 2\#\{q \in S : q \equiv 1 \pmod{p}\} + 3$

Proof. We know that Krull dimension of $R^{univ}_{\bar{\rho}} \geq d_1 - d_2$, where $d_i := H^i(G_{\mathbb{Q},S}, ad\,\bar{\rho})$ Writing down the formulae for d_1 and d_2, and noting that

$$\dim \mathrm{H}^1(G_{\mathbb{Q},S}, \chi_2\chi_1^{-1}) - \dim \mathrm{H}^2(G_{\mathbb{Q},S}, \chi_2\chi_1^{-1}) = 1$$

by the Euler-Poincare characteristic formula in 2.3.13. So we obtain the result. □

In the subsequent discussion, we will assume that there is no obstruction to lifting the lower left corner. Under that assumption, we will try to calculate other obstructions. In fact just like before, we choose $\tilde{c}$ such that $f_{21} = 0$, i.e. $\tilde{c} \in \mathrm{Ext}^1(a,d) \otimes I$.

Lemma 3.4.17. *If there is a* $\tilde{c}$ *which makes* $f_{21} = 0$*, then* $\tilde{c}$ *is independent of choices of* $\tilde{a}$ *and* $\tilde{d}$*.*

Proof.

$$\tilde{c}_{gh} \stackrel{?}{=} (\tilde{a}_h + \alpha_h)\tilde{c}_g + (\tilde{d}_g + \beta_g)\tilde{c}_h.$$

$$= \tilde{a}_h\tilde{c}_g + \tilde{d}_g\tilde{c}_h + (\alpha_h\tilde{c}_g + \beta_g\tilde{c}_h).$$

where $\alpha, \beta : G \to I$ are arbitrary functions and since $\tilde{\rho}$ mod m_{A_1} is upper triangular, $\tilde{c}$ takes values in m_{A_1}. But $I.m_{A_1} = 0$, so $\alpha_h\tilde{c}_g = \beta_g\tilde{c}_h = 0$ and hence the lemma follows. □

Proposition 3.4.18. *Assume we have lifted the bottom left corner such that $f_{21} = 0$. Then the diagonal entries satisfy the following properties:*

i. $f_{11} \in Z^2(a,a) \otimes I$.

ii. $f_{22} \in Z^2(d,d) \otimes I$.

iii. Changing $\tilde{a}$ by any arbitrary function changes f_{11} by an element in $B^2(a,a) \otimes I$.

iv. Changing $\tilde{d}$ by any arbitrary function changes f_{22} by an element in $B^2(d,d) \otimes I$.

Proof. We will give two proofs of part *i*.

The first proof: *i* and *ii* are clear from the previous discussion and the proof is exactly the same since $f_{21} = 0$.

The second proof: This is a more direct formal computation. Let ρ_0 be any lift of $\bar{\rho}$ to A_0 given by $\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ which is a homomorphism. Let ρ be any lift of ρ_0 to A_1 given by $\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$. The map $A_1 \to A_0$ is surjective with kernel I and $Im_{A_1} = 0$. Recall

$$f_{11}(g,h) = \tilde{a}_{gh} - \tilde{a}_g\tilde{a}_h - \tilde{b}_g\tilde{c}_h$$

And we now want to compute

$$a_g f_{11}(g',g'') - f_{11}(gg',g'') + f_{11}(g,g'g'') - a_{g''} f_{11}(g,g')$$

$=a_g(\tilde{a}_{g'g''} - \tilde{a}_{g'}\tilde{a}_{g''} - \tilde{b}_{g'}\tilde{c}_{g''}) - (\tilde{a}_{gg'g''} - \tilde{a}_{gg'}\tilde{a}_{g''} - \tilde{b}_{gg'}\tilde{c}_{g''}) + (\tilde{a}_{gg'g''} - \tilde{a}_g\tilde{a}_{g'g''} - \tilde{b}_g\tilde{c}_{g'g''}) - a_{g''}(\tilde{a}_{gg'} - \tilde{a}_g\tilde{a}_{g'} - \tilde{b}_g\tilde{c}_{g'})$

Now, we can write $\tilde{b}\tilde{c} = b_0\tilde{c},\ \tilde{a}\tilde{c} = a_0\tilde{c},\ \tilde{d}\tilde{c} = d_0\tilde{c}$, since $\tilde{c}$ takes values in m_{A_1}. And we know that:

I. $b_0(gh) = a_0(g)b_0(h) + b_0(g)d_0(h)$.

II. $\tilde{c}_{gh} = \tilde{c}_g\tilde{a}_h + \tilde{c}_h\tilde{d}_g$.

Now in the above formula, we can replace a by $\tilde{a}$ and we get

$\tilde{a}_g(\tilde{a}_{g'g''} - \tilde{a}_{g'}\tilde{a}_{g''} - \tilde{b}_{g'}\tilde{c}_{g''}) - (\tilde{a}_{gg'g''} - \tilde{a}_{gg'}\tilde{a}_{g''} - \tilde{b}_{gg'}\tilde{c}_{g''}) + (\tilde{a}_{gg'g''} - \tilde{a}_g\tilde{a}_{g'g''} - \tilde{b}_g\tilde{c}_{g'g''}) - \tilde{a}_{g''}(\tilde{a}_{gg'} - \tilde{a}_g\tilde{a}_{g'} - \tilde{b}_g\tilde{c}_{g'})$

After canceling out the terms and using the formula for $\tilde{c}$ in II, we get $\tilde{c}_{g''}(\tilde{b}_{gg'} - \tilde{a}_g\tilde{b}_{g'} - \tilde{b}_g\tilde{d}_{g''})$. But by using the formula for b_0, we get $\tilde{b}_{gg'} - \tilde{a}_g\tilde{b}_{g'} - \tilde{b}_g\tilde{d}_{g''} \in I$ and $\tilde{c}_{g''}(\tilde{b}_{gg'} - \tilde{a}_g\tilde{b}_{g'} - \tilde{b}_g\tilde{d}_{g''}) \in m_{A_1} \cdot I = 0$ and hence the claim follows.

iii and *iv* are exactly similar so let us prove *iii*. Let $\alpha : G \to I$ be any function. Now

$$(\tilde{a}_{gh} + \alpha_{gh}) - (\tilde{a}_g + \alpha_g)(\tilde{a}_h + \alpha_h) - \tilde{b}_g\tilde{c}_h$$

$$= (\tilde{a}_{gh} - \tilde{a}_g\tilde{a}_h - \tilde{b}_g\tilde{c}_h) + (\alpha_{gh} - \tilde{a}_g\alpha_h - \tilde{a}_h\alpha_g) - \alpha_g\alpha_h$$

Now since $I^2 = 0$, $\alpha_g\alpha_h = 0$ and $\alpha_{gh} - \tilde{a}_g\alpha_h - \tilde{a}_h\alpha_g = \alpha_{gh} - a_g\alpha_h - a_h\alpha_g$ but this quantity is a coboundary, i.e it belongs to $B^2(a,a) \otimes I$. □

We are ready to state and prove one of the main theorems of this sub-section.

Let ρ be an upper triangular lift of $\bar{\rho}$ to A_0. We will find the obstruction to lift ρ to

a not necessarily upper triangular representation to A_1. We know that this obstruction class is independent of the choice of lift and will only depend on ρ. We call that class $O(\rho) \in Z^2(\bar{\rho}, \bar{\rho}) \otimes I$.

Theorem 3.4.19. *Assume* **Neben**, **Hypothesis 1** *and* $b \cup c = 0$ *where* $b \in Ext^1(\chi_2, \chi_1)$ *and* $c \in Ext^1(\chi_1, \chi_2)$. *Then*

$$O(\rho) = 0 \text{ iff } f_{21} \in B^2(a,d) \otimes I$$

Proof. Recall: $f_{21} = \tilde{c}_{gh} - \tilde{c}_g \tilde{a}_h - \tilde{c}_h \tilde{d}_g$. We have already seen f_{21} is not a coboundary, and that gives rise to an obstruction class.

Conversely, assume we have chosen a $\tilde{c}$ such that $f_{21} = 0$. So now we are reduced to showing the existence of a lift of a to A_1 which makes $f_{11} = 0$. We can lift a to a multiplicative character to A_1, call that character χ. Write $\tilde{a} = \chi + \lambda$. We are looking for the existence of λ such that the following equations holds:

- $\tilde{a}_{gh} = \tilde{a}_g \tilde{a}_h - \tilde{b}_g \tilde{c}_h$
- $\chi_{gh} + \lambda_{gh} = (\chi_g + \lambda_g)(\chi_h + \lambda_h) + \tilde{b}_g \tilde{c}_h$

So λ should satisfy :

$$\lambda_{gh} = \lambda_g \chi_h + \lambda_h \chi_g + \tilde{b}_g \tilde{c}_h$$

And $\tilde{b}_g \tilde{c}_h = b_g \tilde{c}_h$, since $\tilde{c}$ takes values in I.

Now $b\tilde{c} \in Z^1(d,a) \times Z^1(a,d) \otimes I \xrightarrow{\cup} Z^2(a,a) \otimes I$ and by our assumption this is a coboundary. So there exists a function that realizes this coboundary. In fact λ is a function that works.

The same proof works verbatim for f_{22} and the only difference is that the coboundary lies in $Z^2(d,d)$. So, now we choose lifts such that $f_{11} = f_{22} = 0$. The matrix representing $O(\rho)$

can be written as $\begin{pmatrix} 0 & f_{12} \\ 0 & 0 \end{pmatrix}$. Now f_{12} satisfies

$$a_g f_{12}(g',g'') - f_{12}(gg',g'') + f_{12}(g,g'g'') - d_{g''} f_{12}(g,g') = 0,$$

i.e. $f_{12} \in Z^2(d,a)$. Changing the lift changes f_{12} by an element in $B^2(d,a)$. Now our assumption on 1-dimensionality of $Z^1(d,a)$ (**Hypothesis 1**) and the Euler-Poincare characteristic formula 2.3.13 shows $Z^2(d,a) = B^2(d,a)$, or in other words we can find a $\tilde{b}$ such that $f_{12} = 0$. Hence we have shown that we can construct a lift that forces the vanishing of the relevant cohomology class. □

We finish this section by talking about some special prime ideals in $\mathscr{R}^{univ}_{\bar{\rho}}$.

Lemma 3.4.20. *Let* $\mathfrak{p}$ *be any dimension* 1 *prime in* $\mathscr{R}^{univ}_{\bar{\rho}}$*, not containing the ideal of reducibility, let A be the normalization of* $\mathscr{R}^{univ}_{\bar{\rho}}/\mathfrak{p}$*, let E be the fraction field of A and* ρ *be the induced representation* $\rho : G_{\mathbb{Q},S} \to GL_2(A)$*. Then* $\rho \otimes_A E$ *is absolutely irreducible.*

Proof. This is lemma 3.33 in [62]. □

Definition 3.4.21. (Skinner-Wiles) The primes in the above lemma are called good primes, if the residue characteristic is p.

Remark 3.4.22. These primes were used in [57] to do level raising. However their argument is unnecessarily complicated and the whole patching process can be simplified using Kisin's method. That was carried by Lue Pan [45] in their thesis. Our simplifying assumption makes the patching arguments quite simple but since the arguments already exist in literature in quite generality, we do not repeat it here.

Finally we give a sketch of the construction of such good primes under **Hypothesis 1** and **Neben**. These are the main results in Chapter 4.3 of [57]. The point here is to impress

on the reader about how strong **Hypothesis 1** is and how it can be used to significantly simplify the proof of a key proposition, Proposition 4.3 in [57].

Lemma 3.4.23. *Let $\rho : G_{\mathbb{Q}_S} \to GL_2(R^{red}/Q)$ be such that $\det \rho$ is of finite order, where Q is any prime ideal of R^{red} containing p. Then $\dim R^{red}/Q = 0$.*

Proof. Since Q contains (p) and we reduce to the case where Q has height 1, thus we get $R^{red}/Q = \mathbb{F}[[X]]$. We assume that $\mathbb{F}$ is chosen large enough to contain the values of the diagonal characters. Now since the $\det \rho$ is of finite order, under **Neben**, we can make the diagonal characters to be of finite order as well, which implies the characters take values in $\mathbb{F}^*$. So now we can represent ρ via the matrix $\begin{pmatrix} a & b+\sum b_\alpha X^\alpha \\ 0 & d \end{pmatrix}$. Since this is a homomorphism and the target space is a domain, we get, $b_\alpha(gh) = a_g b_\alpha(h) + b_\alpha(g)d_h$. This implies $b_\alpha = k_\alpha b$, for some constant $k_\alpha \in \mathbb{F}$ by our **Hypothesis 1**. Thus the matrix becomes $\begin{pmatrix} a & b(1+\sum k_\alpha X^\alpha) \\ 0 & d \end{pmatrix}$. But $1+\sum k_\alpha X^\alpha$ is an invertible power series so one can conjugate the above matrix by $\begin{pmatrix} 1+\sum k_\alpha X^\alpha & 0 \\ 0 & 1 \end{pmatrix}$ and one immediately gets $\rho \cong \bar{\rho}$. Thus the result follows. □

Proposition 3.4.24. *There exist good primes in every component of $R^{univ}_{\bar{\rho}}$.*

Proof. This is Proposition 4.2 in [57]. In this case, one should take Q to be a minimal prime in $R^{univ}_{\bar{\rho}}/m_\Lambda R^{univ}_{\bar{\rho}}$. Then by our calculations on tangent spaces, $\dim Q \geq 1$. Now if Q contains I^{red}, then the induced Galois representation

$$\rho_Q : G_{\mathbb{Q}} \to GL_2(R^{univ}_{\bar{\rho}}/Q)$$

is reducible. By the choice of Q, $\det(\rho_Q)$ has finite order. But the previous lemma contradicts that $\dim Q \geq 1$. Thus Q does not contain I^{red} and hence ρ_Q is irreducible. For

complete details of the above steps and to complete the rest of the proof, one should follow the rest of the arguments in [57]. □

3.5 Understanding extension classes and cup-products

In this section we will generalize Sharifi's method in [54] to construct big non-abelian extensions of $\mathbb{Q}$. We set up a general framework. Let $\rho^{univ} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the universal deformation to $Gl_2(\mathscr{R}_{\bar{\rho}}^{univ})$. We are interested in understanding the kernel of the fixed field of ρ^{univ}. To simplify notation we will use I to denote I^{red}. We can define two ideals of $\mathscr{R}_{\bar{\rho}}^{univ}$

$B := \langle b(\sigma) : \sigma \in G_{\mathbb{Q}} \rangle$ and $C := \langle c(\sigma) : \sigma \in G_{\mathbb{Q}} \rangle$

Recall we have a product map

$$B/IB \otimes C/IC \longrightarrow I/I^2$$

which comes from the fact that $BC = I$. Since R^{red} is a domain we know that I is a prime ideal and our method will give a complete description of the cotangent space at I in terms of Iwasawa theory. Our arguments are general and do not need that I is a prime ideal. However this description combined with the numerical criteria will be used to prove cases of modularity lifting theorems and Wake's conjectures in Chapter 6. However most of the results in this chapter are quite general and are completely independent of the hypotheses in the previous chapter.

Note that by proposition 3.4.8, I is generated by $\langle a(\sigma) - \chi_1(\sigma) \rangle = \langle d(\sigma) - \chi_2(\sigma) \rangle$ where χ_1 and χ_2 are defined as before. Now one can check the following formulae:

$$b(\sigma)c(\tau) = (a(\sigma\tau) - \chi_1(\sigma)\chi_1(\tau) - \chi_1(\sigma)(a(\tau) - \chi_1(\tau)) - \chi_1(\tau)(a(\sigma) - \chi_1(\sigma)) \pmod{I^2}$$

Similar formula holds for $c(\sigma)b(\tau)$ where we use $d-\chi_2$, instead of $a-\chi_1$. Checking the statement is routine and we leave it to the reader.

The above formula can also be summarized via this matrix representation $\begin{pmatrix} \chi_1 & \bar{b} & \bar{a}-\bar{\chi}_1 \\ 0 & \chi_2 & \bar{c} \\ 0 & 0 & \chi_1 \end{pmatrix}$ (or equivalently by $\begin{pmatrix} \chi_2 & \bar{c} & \bar{d}-\bar{\chi}_2 \\ 0 & \chi_1 & \bar{b} \\ 0 & 0 & \chi_2 \end{pmatrix}$), where $\bar{b} \in B/IB,\ \bar{c} \in C/IC,\ \bar{a}-\bar{\chi}_1,\ \bar{d}-\bar{\chi}_2 \in I/I^2$ or by the following diagram of fields.

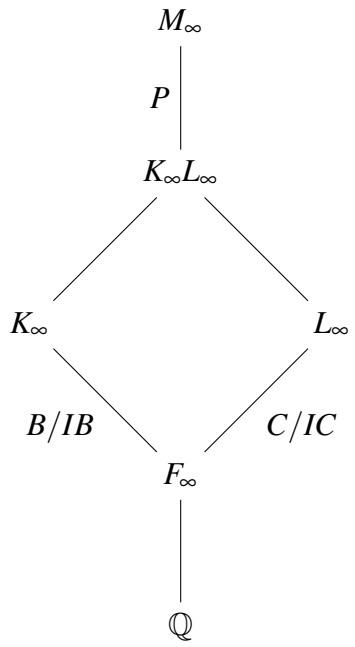


Figure 3.1: A field diagram explaining the subfields cut out the above matrix

where F_∞ is the fixed field of the kernel of the diagonal characters. In what follows, we will work out the above picture explicitly in the case where χ_2 is the trivial character, $\chi_1 = \chi$, the cyclotomic character and generalize it later. Thus F_∞ in this case is just $\mathbb{Q}(\mu_{p^\infty})$. The matrix representation that we will be working with is: $\begin{pmatrix} 1 & c & d-1 \\ 0 & \chi & b \\ 0 & 0 & 1 \end{pmatrix}$.

Remark 3.5.1. One can also work with $\begin{pmatrix} \chi & b & a-\chi \\ 0 & 1 & c \\ 0 & 0 & \chi \end{pmatrix}$, but one must work with homogeneous cocycles or Ext-groups. All arguments otherwise remain unchanged.

In any case, K_∞ is the maximal abelian pro-p extension of F_∞, unramified outside S with a χ_{cyc} action of Γ and an action of ω by $\Delta := \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. L_∞ is the maximal abelian pro-p extension unramified outside $S \setminus \{p\}$ with a χ_{cyc}^{-1} action of Γ and an action of ω^{-1} by

Δ, and M_∞ is an abelian pro-p extension of $K_\infty L_\infty$ with trivial action of $\Gamma \times \Delta$.
Before we start with the structure of the above Galois groups, let us recall some basic facts about Iwasawa theory.

Definition 3.5.2. We say M and M' are pseudo-isomorphic if there exist a homomorphism $M \to M'$ with finite kernel and cokernel.

The next theorem is a structure theorem for Λ-modules.

Theorem 3.5.3. *(Iwasawa) Let M be a finitely generated Λ module. Then M is pseudo-isomorphic to $\Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{a_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{b_j}$ where F_j is an irreducible Weierstrass polynomial, i.e., it is an irreducible polynomial of the form*

$$F_j(T) = T^k + c_1 T^{k-1} + \ldots + c_k$$

where $c_i \in m_\Lambda$.

Following Iwasawa's theorem one can define the following invariants attached to M.

- $r(M) = r = \Lambda$ rank of M
- $\mu(M) = \sum_{i=1}^{s} a_i$ (Iwasawa μ-invariant)
- $\lambda(M) = \sum_{j=1}^{t} b_j \deg(F_j)$ (Iwasawa λ-invariant)
- $F_{M,\gamma} = \prod_{j=1}^{t} (F_j)^{b_j}$ (characteristic polynomial of M)

Note that $r(M), \mu(M)$ and $\lambda(M)$ are independent of the choice of a generator γ but not the characteristic polynomial, where γ is a topological generator of $\Gamma \cong \mathbb{Z}_p$ (non-canonically). Let F be a totally real field and let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension. Let H_∞ be the maximal unramified abelian p-extension of F_∞. Let $X_\infty := \mathrm{Gal}(H_\infty/F_\infty)$. Then X_∞ is naturally a Λ-module.

Conjecture 3.5.4. (Iwasawa): $\mu(X_\infty) = 0$

Remark 3.5.5. This is known to be true for abelian F by the work of Ferrero-Washington and this result will be used throughout in our thesis.

Conjecture 3.5.6. (Leopoldt): Let K be any number field and S be the set containing all infinite primes and all primes over p, then

$$H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

Remark 3.5.7. This conjecture is known for abelian number fields and this will also be used throughout in this section.

Now let us summarize some basic Iwasawa theoretic results about the Galois groups at the intermediate levels of this diagram. Let $\Sigma = S_p \cup S_\infty$, i.e. the primes above p and ∞. Let X_Σ and X_S be the Galois groups of the maximal abelian pro-p extensions of $\mathbb{Q}(\mu_{p^\infty})$ unramified outside Σ and S respectively. The following theorem gives a complete structure of X_Σ and X_S.

Theorem 3.5.8. *(Iwasawa) X_Σ is pseudo-isomorphic to $\Lambda^{\frac{p-1}{2}} \oplus$ (Λ-torsion)*

Proof. This is theorem 13.31 in [67]. □

However we are only interested in the ω-component of X_Σ. In that case, we have a precise statement due to Theorem 11.3.18 in [50].

Proposition 3.5.9. *X_Σ^ω is isomorphic to Λ.*

Theorem 3.5.10. *X_Σ has no finite nontrivial Λ-modules. Moreover we have an exact sequence of Λ-modules*

$$0 \to \bigoplus_{\substack{l \in S-\Sigma \\ l \equiv 1 mod p}} \mathbb{Z}_p(1) \to X_S \to X_\Sigma \to 0$$

In particular X_S also has no finite Λ-submodules.

Proof. See [50] page 750. □

In fact one can say more about the ω-component of X_S.

$$X_S^{\omega} = \Lambda \bigoplus_{l \equiv 1 \bmod(p)} \mathbb{Z}_p(1) \tag{3.4}$$

And each $\mathbb{Z}_p(1)$ extension is totally ramified at p and totally (tamely) ramified at l that contributes to it. And the Λ extension is only ramified at p. Finally we also see that our **Hypothesis 1** forces $\mathrm{Gal}(K_\infty/F_\infty)$ to be cyclic. In fact we say more. If $*$ in the upper right corner of $\bar{\rho}$ is ramified only at p, then we get Λ but if $*$ is ramified at p and another prime q, then we get a $\mathbb{Z}_p(1)$-extension, just like in our case of the elliptic curve X ($11A2$ in Cremona tables). See section 3.6.

Remark 3.5.11. Theorem 3.5.10 is true for any totally real base field F if one assumes Leopoldt's conjecture for the field F and p.

Proposition 3.5.12. *$Gal(L_\infty/F_\infty)$ does not have any finite Λ submodules. Moreover $Gal(L_\infty/F_\infty)$ is a pseudo-cyclic Λ-module, if one assumes Vandiver's conjecture.*

Proof. Let S be the set of primes dividing N. Consider the exact sequence coming from class field theory

$$\widehat{E_{F_n}} \to \oplus_{q|N} (\widehat{\mathcal{O}_{F_n}/q})^{\times} \to Gal(M_S(F_n)/H(F_n)) \to 0 \tag{3.5}$$

where $\widehat{G}$ is the p-adic completion of G and E_{F_n} are the group of units of $F_n = \mathbb{Q}(\mu_{p^n})$ and the first map is the diagonal embedding, $H(F_n)$ is the p-Hilbert class field and $M_S(F_n)$ is the maximal p extension of F_n unramified outside of S. Now taking projective limits under

the norm maps, one obtains the following exact sequence:

$$E_\infty \to \bigoplus_{q|N} R_q \to Gal(M_S(F_\infty)/H(F_\infty)) \to 0 \tag{3.6}$$

where $R_q = \varprojlim(\widehat{\mathcal{O}_{F_n}/q})^\times$. Note that $E_\infty = E_\infty^+ \oplus E_\infty^-$, under the action of complex conjugation and $(E_\infty)^+_{\omega^{-1}} = 0$ and $E_\infty^- = \mathbb{Z}_p(1)$ as Galois modules so $(E_\infty)^-_{\omega^{-1}} = 0$ as well. Now one can look at ω^{-1}- component of the exact sequence by taking ω^{-1}-coinvariants which is an exact functor, so we now get an isomorphism $\bigoplus_{q|N}(R_q)_{\omega^{-1}} \cong (Gal(M_S(F_\infty)/H(F_\infty)))_{\omega^{-1}}$. We will write down the exact structure of $(R_q)_{\omega^{-1}}$ but we note that this has no finite submodules by lemma 3.5.13. So all we have to understand is the structure of $Gal(H(F_\infty)/F_\infty)^-$ as a Λ-module. But it is a theorem of Iwasawa that the above module does not have any finite submodules. This final statement is quite well known, see for example [67], Proposition 13.28.

Finally note that Vandiver implies the maximal abelian unramified p-extension of F_∞ is cyclic as a Λ-module. Now lemma 3.5.22 shows that the characteristic ideal of R_q and that of $H(F_\infty)$ are coprime. And this proves that $\mathrm{Gal}(L_\infty/F_\infty)$ is pseudo-cyclic. □

Lemma 3.5.13. *$(R_q)_{\omega^{-1}} \cong \Lambda/f_q(T)$ where $f_q(T) = (1+T)^{p^r} - \omega(q)(1+p)^{p^r}$, where r is the number of primes over q in K_∞. In particular, R_q is non-trivial iff $1-\omega(q) = 0 \pmod p$, i.e. $q \equiv 1 \pmod p$.*

Proof. See [28] page 528. □

We will use a general version of this lemma later.

The following corollary of Proposition 3.5.12 will be a key in our modularity lifting theorem (theorem 6.3.6).

Corollary 3.5.14. *$Gal(L_\infty/F_\infty)$ is cyclic if one of the following two conditions are satisfied:*

(a) $H(F_\infty)/F_\infty$ is cyclic and f_q are units or

(b) $H(F_\infty)/F_\infty$ is trivial and there is only one non-unit f_q.

Proof. The corollary follows from the fact if f, g are two relatively prime distinguished polynomials in Λ, then the map $\Lambda/(fg) \to \Lambda/(f) \times \Lambda/(g)$ has finite kernel and co-kernel.

□

Theorem 3.5.15. *$M_\infty/K_\infty L_\infty$ is unramified everywhere and under* **Hypothesis 1**

$$Gal(M_\infty/L_\infty K_\infty) \cong I/I^2 \cong (I_G Gal(K'/K_\infty)/I_G^2 Gal(K'/K_\infty))$$

where K' is the maximal abelian p-extension of K_∞, unramified outside N with ω^{-1}-action.

Proof. First we show that it is unramified at p. But this is obvious since $d = 1$ on I_p by ordinarity of ρ. Now let $l \in S$. First let us assume that the inertia subgroup at l inside $\mathrm{Gal}(K_\infty/F_\infty)$ or $\mathrm{Gal}(L_\infty/F_\infty)$ is non-trivial. Then by the previous results 3.5.10 and 3.5.12, l must be infinitely ramified. Otherwise if the inertia subgroup is finite, it will generate a finite Λ-submodule. Without any loss of generality, assume that l is infinitely ramified in $\mathrm{Gal}(K_\infty/F_\infty)$. Now, we localize our field diagram at l. We let M_l over $K_{l,\infty}L_{l,\infty}$ be a totally tamely ramified at l extension. This extension is given by a root α of some irreducible polynomial f with coefficients in $K_{l,\infty}L_{l,\infty}$. But since $L_{l,\infty}$ is a compositum of $L_{l,n}$ at finite levels, we can assume that the coefficients lie in some $K_{l,\infty}L_{l,n}$. Thus we can think of M_l as some degree p^r totally tamely ramified extension of $K_{l,\infty}$ with Galois group H_l. By the same argument we can reduce this to some finite extension C_l given by the coefficients of this polynomial. Now H_l injects into $\mathrm{Aut}(C_l(\alpha)/C_l)$. Let D_l be the fixed field of H_l. Now $C_l(\alpha)/D_l$ is totally tamely ramified hence by Abhyankar's lemma $C_l(\alpha) = D_l(\pi^{p^{-n}})$ for some uniformizer π of D_l. But $\pi = \lambda^{p^n} u$ for some unit u and λ in $K_{l,\infty}$ as l is infinitely ramified. Hence $M_l = K_{l,\infty}(u^{p^{-n}})$. Hence M_l is unramified at l. So this takes care of all

primes that are ramified in either K_∞ or L_∞. To finish the proof: let l be a prime that is unramified in $K_\infty L_\infty/F_\infty$ but ramifies in $M_\infty/K_\infty L_\infty$. In that case, localizing the entire field diagram at l, $K_{l,\infty}L_{l,\infty}$ is the unique unramified $\mathbb{Z}_p$ extension of $F_{l,\infty}$. Now, $\mathbb{Z}_p$ acts on the inertia subgroup at l inside $M_\infty/K_\infty L_\infty$ via lifting and conjugating and this action is given by $\tau \to \tau^l$. But from our matrix calculations we know that this action must be trivial. Hence $M_\infty/K_\infty L_\infty$ is unramified everywhere. This finishes the proof of the first part of the theorem.

Let us denote by $P := Gal(M_\infty/K_\infty L_\infty)$. Note that

$$\begin{pmatrix} 1 & b & x \\ 0 & a & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b & x \\ 0 & a & c \\ 0 & 0 & 1 \end{pmatrix}$$

Thus P is central in Gal $(M_\infty/\mathbb{Q})$. A simple matrix multiplication shows that P is the commutator subgroup of Gal(M_∞/F_∞). We will now show how to construct M_∞ and in the process will identify Gal$(M_\infty/K_\infty L_\infty)$. But first note that $\overline{d} - 1 \mod I^2$ gives an isomorphism between P and I/I^2. We will make the map explicit. Let $\sigma, \tau \in G_{F_\infty}$ be such that $b(\sigma) = c(\tau) = 0$ and let f be any function that satisfies $df = c \cup b$. Then one computes mod I^2,

$$f([\sigma,\tau]) = f(\sigma\tau\sigma^{-1}\tau^{-1})$$

$$= f(\sigma\tau) + f(\sigma^{-1}\tau^{-1}) + c(\sigma\tau)b(\sigma^{-1}\tau^{-1})$$

$$= f(\sigma) + f(\tau) + c(\sigma)b(\tau) + f(\sigma^{-1}) + f(\tau^{-1}) + c(\sigma^{-1})b(\tau^{-1}) + c(\sigma)b(\tau^{-1})$$

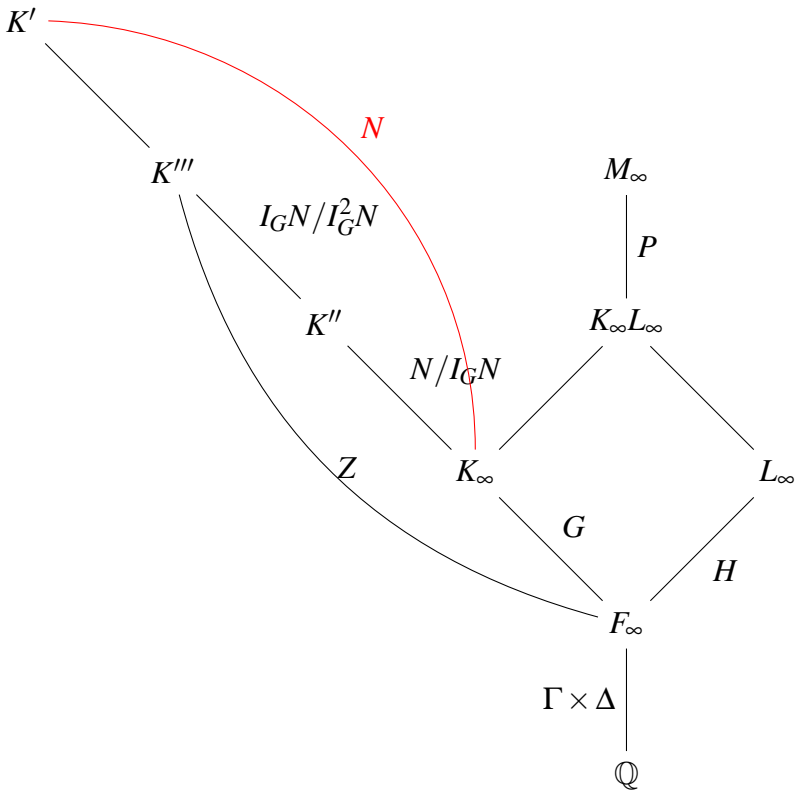
Now note that $f(x^{-1}) = -f(x),\ b(y^{-1}) = -b(y),\ c(z^{-1}) = -c(z)$, and for $g,h \in G_{F_\infty}$, $b(gh) = b(g) + b(h)$ and $c(gh) = c(g) + c(h)$

Using the above relations we get the formula:

$$f([\sigma\tau]) = c(\sigma)b(\tau).$$

Let K' be the maximal abelian extension of K_∞ unramified outside S with ω^{-1} action by Δ and let K'' be the maximal subextension of K' on which G:= $\mathrm{Gal}(K_\infty/F_\infty)$ acts trivially. Then K'' is abelian over F_∞ and $\mathrm{Gal}(K''/K_\infty) = \mathrm{Gal}(K'/K_\infty)/I_G$, where I_G is the augmentation ideal. Note that by Abhyankar's lemma, K' is unramified everywhere. Similarly Abhyankar's lemma shows $L_\infty K_\infty/K_\infty$ is unramified at all l, and also at p, since L_∞/F_∞ is. Thus K' contains $L_\infty K_\infty$. Now there is a field $\mathscr{K}/F_\infty$, such that $\mathrm{Gal}(\mathscr{K}/F_\infty) = \mathrm{Gal}(K''/K_\infty)$. Now Δ acts on $\mathrm{Gal}(\mathscr{K}/F_\infty)$ by ω^{-1}. Furthermore $\mathscr{K}/F_\infty$ is unramified outside N. By construction, it is the maximal such extension. Thus $\mathscr{K} = L_\infty$. Since P is the center and the commutator inside $\mathrm{Gal}(M_\infty/F_\infty)$, we seek to construct an extension of K'', call it K''', such that $\mathrm{Gal}(K'''/K'')$ is central and the commutator subgroup of $\mathrm{Gal}(K'''/F_\infty)$. We also demand that $\Gamma \times \Delta$ act trivially on $\mathrm{Gal}(K'''/K'')$.

Let us draw a picture summarizing what we have so far.



Let us focus on the K'''/F_∞, and let Z be the Galois group. Note that Z is necessarily non-abelian. Observe that K''/F_∞ is abelian and Z sits inside the following exact sequence:

$$0 \to I_GN/I_G^2N \to Z \to N/I_GN \times G \to 0$$

and I_GN/I_G^2N lies in the center of Z. We will make a quick sketch of that fact. Pick some g and lift it inside Z and by abuse of notation continue to call it g. We would like to show the conjugation by g on I_GN/I_G^2N is trivial.

Note $(g-1)(h-1)n = 0$ for all g,h, so $g(h-1)n = (h-1)n$ and similarly for any lift of an element from N/I_GN. Since G is cyclic as a Λ-module (by **Hypothesis 1**), we get that every element of I_GN/I_G^2N is a commutator. By the general theory of central extensions,

one get a map from

$$\wedge^2(G\times N/I_GN)\to[G,N/I_GN]=I_GN/I_G^2N$$

given by $x\wedge y\mapsto[x,y]$, where all the commutators are taken in the group Z, where the elements x and y are arbitrarily lifted and then taken commutators. It is trivial to check that such an action is well-defined. Finally note that $\wedge^2(G\times N/I_GN)$ can be identified with $G\otimes N/I_GN$ and there is a canonical map :

$$G\otimes N/I_GN\twoheadrightarrow I_GN/I_G^2N$$

given by $g\otimes n\mapsto(g-1)n$.

The upshot of the above discussion is that this map is given by taking commutators. Thus we have a commutative diagram:

$$\begin{array}{ccc} G\otimes N/I_GN & \twoheadrightarrow & I_GN/I_G^2N \\ \downarrow\cong & & \downarrow \\ B/IB\otimes C/IC & \twoheadrightarrow & I/I^2 \end{array}$$

And this gives us the desired isomorphism, i.e

$$Gal(M_\infty/K_\infty L_\infty)\cong I/I^2\cong I_GN/I_G^2N$$

Finally we note that the action of $\Gamma\times\Delta$ on I_GN/I_G^2N is necessarily trivial since $g(a\otimes b)=\chi(g)\omega(g)a\otimes\chi^{-1}(g)\omega^{-1}(g)b=a\otimes b$ □

Question 3.5.16. *(Comm)* Are there any weaker conditions to ensure that every element of I_GN/I_G^2N is a commutator even if G or H is not cyclic?

Remark 3.5.17. **Hypothesis 1** is only used to ensure that G is cyclic.

Remark 3.5.18. There is a similar picture on the other side of our diagram. Let us briefly recall the construction. Call H:=Gal(L_∞/F_∞). let L' be the maximal unramified extension of L_∞ outside Np with ω action. By Abhyankar's lemma, L'/L_∞ is unramified at N, since H does not have any finite submodules so all primes that ramify are infinitely ramified. Let L'' be the maximal subextension on which H acts trivially on Gal(L''/F_∞). Thus L''/F_∞ is abelian and Gal$(L''/L_\infty) = Gal(L'/L_\infty)/I_H$. Thus there is a $\mathscr{L}/F_\infty$ such that Gal$(\mathscr{L}/F_\infty) = Gal(L''/L_\infty)$. Now note that $\mathscr{L}/F_\infty$ is unramified outside Np and is the maximal such extension and Gal$(\mathscr{L}/F_\infty)$ has a ω action of Δ . Thus $\mathscr{L} = K_\infty$.

Remark 3.5.19. Another alternate and equivalent construction will be to look at the maximal abelian p-extension of K_∞, unramified outside N, call it X, then look at $(I_G X/I_G^2 X)_{\Gamma\times\Delta}$

Remark 3.5.20. Our proof also shows that M_∞ is the maximal abelian p-extension of $K_\infty L_\infty$ with trivial $\Gamma\times\Delta$ action.

Remark 3.5.21. Note that in the proof of unramifiedness, we do not require the Galois modules to be cyclic. All we need is that there are no finite non-trivial Λ-submodules. This observation will be very useful to us later. See theorem 5.2.5.

Lemma 3.5.22. *G does not contain any submodule isomorphic to $\mathbb{Z}_p(-1)$ and H does not contain any submodule isomorphic to a submodule of $\mathbb{Z}_p(1)$.*

Proof. First we show that H does not contain any submodule isomorphic to a submodule of $\mathbb{Z}_p(1)$. If this was the case, then the characteristic polynomial of H would have a common factor with $(1+T)^{p^k} - (1+p)^{p^k}$ for some k. Now the characteristic polynomial for $(R_q)_{\omega^{-1}}$ is coprime to the characteristic ideal of $X_{\omega^{-1}}$, where X is the Galois group of the maximal abelian p-extension of F_∞ unramified everywhere. Let $f(T)$ be the characteristic power series of $X_{\omega^{-1}}$. Then

$$f(\zeta_\nu(1+p)^s - 1, \theta) = L_p(s, \nu\theta)$$

where θ is a character of first kind and ν is a character of second kind.

If $(1+T)-\zeta(1+p)|f(T)$, where ζ is some p-power root of unity, then

$$((\zeta_\nu(1+p))^s-\zeta(1+p))|L_p(s,\nu\theta)$$

This implies $L_p(1,\nu\theta)=0$ where ν is chosen so that $\zeta=\zeta_\nu$. But this contradicts a result of Brumer.

And finally $(1+T)^{p^k}-(1+p)^{p^k}$ is clearly coprime to $f_q(T)$ as $\omega(q)\neq 1$. Thus H does not contain any submodule isomorphic to a submodule of $\mathbb{Z}_p(1)$.

First we show that X_ω does not have any submodule isomorphic to $\mathbb{Z}_p(-1)$. By a theorem of Coates [9], there is an isomorphism

$$K_2(\mathcal{O}_k)(p)\cong(Cl(k(\mu_{p^\infty})\otimes\mathbb{Z}_p(1))^{Gal(k(\mu_{p^\infty})/k)}$$

We use the above non-trivial result of Coates by taking $k=\mathbb{Q}$. The group on the left is finite. If X_ω has a submodule isomorphic to $\mathbb{Z}_p(-1)$, then $(Cl(k(\mu_{p^\infty})\otimes\mathbb{Z}_p(1))$ must be infinite and is fixed by $\Gamma\times\Delta$. This shows that $(Cl(k(\mu_{p^\infty})\otimes\mathbb{Z}_p(1))^{Gal(k(\mu_{p^\infty})/k)}$ contains a subgroup of infinite order which is a contradiction.

Now let us handle the case where we consider the maximal abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$, unramified outside with ω action. Denote the Galois group of the maximal abelian p-extension unramified outside p by Y. We recall a construction of Soule. Let E_n be the group of p-units of $\mathbb{Q}(\mu_{p^n})$, define $\bar{E}:=\varprojlim E/E^{p^n}$, under the norm map. For each $e=(e_n)\in\bar{E}$, define

$$\varepsilon_n^{(m)}(e):=\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})}e_n^{\sigma\cdot\langle\chi(\sigma)^{m-1}\rangle_n},\ \ n\geq 1$$

where χ is the p-adic cyclotomic character and for each $a \in \mathbb{Z}_p$, $\langle a \rangle_n$ is the unique integer in the interval $[0, p^n)$ that is congruent to a modulo p^n. The Kummer map associated with the system of p-units $\{\varepsilon_n^{(m)}(e)\}_n$ is the unique homomorphism $\kappa : Y \to \mathbb{Z}_p$ determined by the following formula:

$$\kappa(\tau) := \{(\varepsilon_n^{(m)}(e))^{1/p^n}\}^{\tau-1}, \quad \tau \in Y, n \geq 1$$

Thus we get a pairing :

$$\bar{E}(m-1)_\Gamma \times Y^\Gamma \to \mathbb{Z}_p$$

$$(e_n \otimes \zeta^{\otimes m-1})_n, \tau \mapsto \kappa(\tau)$$

We can see that the map factors through $Y(m)$. We apply this pairing for $m = 2$. Then Soule's theorem says $Y(m)^\Gamma$ is finite. Applying this to our group G, we see that $G(1)^\Gamma$ must be finite. But this contradicts that G does not have any finite submodules. Thus $G(1)^\Gamma = 0$. The case for the auxiliary primes dividing N are handled exactly in the same manner as earlier. $\square$

A generalization of the above picture : Let us consider the case where: $\bar{\rho} = \begin{pmatrix} \omega\theta & * \\ 0 & \psi \end{pmatrix}$, where ψ is unramified at p and $\theta\psi$ is an even character and the conductor of $\bar{\rho}$ is squarefree. We still demand that $* \neq 0$ on I_p. As before, we consider the universal ordinary, minimally ramified deformation ring. Write $\rho^{univ} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. I is the ideal of reducibility and we assume $I \neq 0$. Then $\theta\psi^{-1}$ cuts out a totally real abelian number field F and our hypotheses on θ and ψ force $\theta\psi$ to be of type S (in Greenberg's terminology), i.e. $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$. Let B and respectively C be the ideals generated by $b(\sigma)$ and $c(\sigma)$, then $BC = I$. Just like before, we have an explicit function $d - \psi$ that gives rise to the following matrix: $\begin{pmatrix} [\psi] & \bar{c} & \bar{d} - [\psi] \\ 0 & \chi_{cyc}[\theta] & \bar{b} \\ 0 & 0 & [\psi] \end{pmatrix}$ where $[\,]$ denotes the Teichmüller character, $\bar{b}, \bar{c}$ and $\bar{d} \in B/IB, C/IC, R^{univ}_{\bar{\rho}}/I^2$ respectively. However to be consistent with the notations in [54] and notational convenience of working with H^i, rather than homogeneous cocycles, we instead consider the matrix: $\begin{pmatrix} 1 & \bar{c} & \bar{d} - 1 \\ 0 & \chi_{cyc}[\theta][\psi]^{-1} & \bar{b} \\ 0 & 0 & 1 \end{pmatrix}$. By abuse of notation we still use the notation $\bar{b}, \bar{c}, \bar{d}$. We summarize the above matrix in the form of the following diagram of fields:

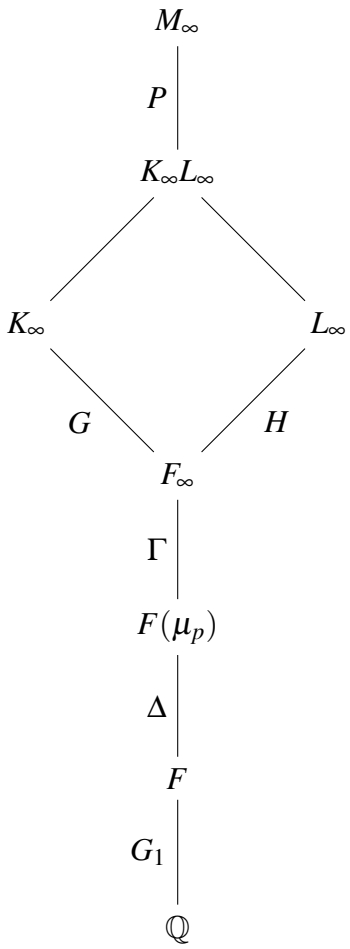


Figure 3.2: Description of the fields cut out by the above matrix

The following properties are straightforward and the proofs are exactly the same as before. $M_\infty/K_\infty L_\infty$ is unramified at p. $G_1 \times \Delta \times \Gamma$ act trivially on P and P is the commutator subgroup of $\mathrm{Gal}(M_\infty/F_\infty)$. Furthermore,

$$(d-\psi)([\sigma,\tau]) = c(\sigma)b(\tau) \bmod I^2.$$

Note that **Hypothesis 1** ensures that K_∞/F_∞ is a cyclic Λ module. Then Theorem 3.5.10 and the remark after the theorem shows that $\mathrm{Gal}(K_\infty/F_\infty) \cong \Lambda$ if K_∞/F_∞ is only ramified at

p. Moreover $\mathrm{Gal}(K_\infty/F_\infty) \cong \mathbb{Z}_p(1)$ as Galois modules if K_∞/L_∞ is ramified at p and some auxiliary prime q and $q \equiv 1 \pmod{p}$.

Before we state the next theorem, let us recall the p-adic L-function of Kubota-Leopoldt. Let F be a totally real abelian field and λ be an even character of type S and let F_λ be the extension attached to λ. Kubota and Leopoldt proved existence of a function $L_{p,S}(s,\lambda)$ which satisfies the following interpolation property:

$$L_{p,S}(1-n,\lambda) = L(1-n,\lambda\omega^{-n}) \prod_{\mathfrak{p}\in S\cup S_p} (1-\lambda\omega^{-n}(\mathfrak{p})N\mathfrak{p}^{n-1}) \tag{3.7}$$

where S_p contains all primes above p. Let γ be a topological generator of $\mathrm{Gal}(F_\infty/F)$ and let $u \in \mathbb{Z}_p^*$ be such that $\zeta^\gamma = \zeta^u$ for any $\zeta \in \mu_{p^\infty}$. Deligne-Ribet and Wiles also proved that there exist a unique $G_{\lambda,S}(T) \in \mathbb{Z}_p[\lambda][[T]] \otimes \mathbb{Q}_p$ such that:

$$L_{p,S}(1-s,\lambda) = G_{\lambda,S}(u^s - 1) \tag{3.8}$$

Moreover if ν is of type W then

$$G_{\nu\mu}(T) = G(\nu(\gamma)(1+T)-1) \tag{3.9}$$

Theorem 3.5.23. *char(Gal(L_∞/F_∞)) =* $G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1) \prod_{l\mid \frac{N}{cond(\theta\psi^{-1})}} f_q(T)$ *where* $f_q(T) = (1+T)^{p^r} - \omega\theta\psi^{-1}(q)(1+p)^{p^r}$. *Moreover $f_q(T)$ is coprime to $L_p(s,\theta^{-1}\psi\omega^2)$.*

Proof. Let S be the set of primes dividing $N/\mathrm{conductor}(\theta\psi^{-1})$. Recall the exact sequence (3.5) in the previous section

$$\widehat{E_{F_n}} \to \oplus_{q\in S}\widehat{(\mathcal{O}_{F_n}/q)}^\times \to Gal(M_S(F_n)/H(F_n)) \to 0 \tag{3.10}$$

where E_{F_n} is the group of units of F_n and the first map is the diagonal embedding, $H(F_n)$ is the p-Hilbert class field and $M_S(F_n)$ is the maximal p extension of F_n unramified outside of S. Note by our hypothesis $\theta\psi^{-1} \neq \omega^i$. Taking the $\omega^{-1}\theta^{-1}\psi$ components of the above exact sequence we get

$$\oplus_{q\in S}(\widehat{\mathcal{O}_{F_n}/q})^{\times}{}_{\omega^{-1}\theta^{-1}\psi} \cong Gal(M_S(F_n)/H(F_n))_{\omega^{-1}\theta^{-1}\psi} \tag{3.11}$$

Taking the inverse limits, we get

$$\oplus_{q\in S}(R_q)_{\theta^{-1}\omega^{-1}\psi} \cong \mathrm{Gal}(M_S(F_\infty)/H_\infty)_{\theta^{-1}\omega^{-1}\psi}$$

where H_∞ is the p-Hilbert class field of F_∞. The same proof as in 3.5.9 (this is also calculated in Itoh [28] section 6), shows $(R_q)_{\theta^{-1}\omega^{-1}\psi} \cong \Lambda/f_q(T)$, where $f_q(T) = (1+T)^{p^k} - \theta\omega\psi^{-1}(q)(1+p)^{p^k}$. In particular R_q has no finite submodules. See the remark below to see when f_q is not an unit. Now let $X_\infty = \mathrm{Gal}(H_\infty/F_\infty)$, then by solution of Iwasawa main conjecture by Wiles we get

$$\mathrm{char}_\Lambda((X_\infty)_{\omega^{-1}\theta^{-1}\psi} = G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1) \tag{3.12}$$

To finish the proof of the first part of the theorem, we note that by lemma 3.5.26, L_∞/F_∞ is unramified at primes dividing the conductor of $\theta\psi^{-1}$. For simplicity write $\zeta = \theta\omega\psi^{-1}(q)$. So the only thing left for us to check is: $G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1)$ and $f_q(T)$ are co-prime. Plugging in $\zeta(1+p)$ for $(1+T)$ in $G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1)$, taking $u = 1+p$ we get $G_{\theta\psi^{-1}\omega^2}(\zeta^{-1}-1)$. Plugging this back inside the p-adic L-function, we get $L_p(1,\theta\psi^{-1}\omega^2)$ which is non-zero. □

Remark 3.5.24. Note that if $\sigma = Frob_q$ and $\tau \in I_q$, then $\sigma\tau\sigma^{-1} = \tau^q$. Using this equation

we get $\theta\psi^{-1}(q) = 1$. Finally we see f_q is not an unit iff $1 - \omega(q)\theta\psi^{-1}(q) \equiv 0 \pmod{p}$, i.e., $q \equiv 1 \pmod{p}$.

We note that $\mathrm{Gal}(L_\infty/K_\infty)$ has no submodule isomorphic to a submodule of $\mathbb{Z}_p(1)$. Thus we get the following theorem which summarizes all the Iwasawa theoretic properties of I/I^2.

Theorem 3.5.25. *(a) $char_\Lambda(I/I^2) = sym(char(Gal(L_\infty/F_\infty)) \cdot char(Gal\ (K_\infty/F_\infty)))$, where sym of 2 polynomials is the symmetric product of two polynomials.*
(b) $char_\Lambda(I/I^2)$ does not have multiple roots iff $char((X_\infty)_{\theta\psi^{-1}\omega^2}$ does not have multiple roots.
(c) $\lambda(I/I^2) = \lambda(Gal(L_\infty/F_\infty)$ where $\lambda(M)$ is the Iwasawa's λ-invariant. In particular, I is cyclic iff $Gal(L_\infty/F_\infty)$ is cyclic.

Note that Iwasawa's theorem 3.5.8 and theorem 3.5.10 also holds in this case. Thus we get

$$\mathrm{Gal}(K_\infty/F_\infty) \cong \Lambda \oplus (\mathbb{Z}_p(1))^k \text{ as } \Lambda \text{ modules} \tag{3.13}$$

Thus under **Hypothesis 1**, we get the cyclicity of $\mathrm{Gal}(K_\infty/F_\infty)$.
If a prime l is infinitely ramified at either K_∞/F_∞ or L_∞/F_∞, we repeat the same argument. Now let l be a prime that divides the conductor of θ or ψ, then by the squarefree assumption l divides the conductor of both $\theta\psi^{-1}$ and $\psi\theta^{-1}$.Then,

Lemma 3.5.26. *K_∞/F_∞ and L_∞/F_∞ are both unramified at l.*

Proof. This argument appears in the work of Wiles, Sharifi, Ohta and Itoh. We merely repeat the standard arguments in our case.
Let H_∞ be the p-Hilbert class field of F_∞. and let N_∞ be the the maximal p-extension of F_∞ unramified outside l. Define N^* to be the maximal subextension of N_∞ which is unramified over F_∞ at all primes dividing l. Then by class field theory, $\mathrm{Gal}(N_\infty/N^*)$ is isomorphic

to a quotient of $\varprojlim \prod_{\lambda|l} \mathcal{O}^*_{F_{n,\lambda}}$. Since $l \nmid p$ and N_∞ is a pro-p extension of F_∞, the above Galois group is in fact a quotient of $J := \varprojlim \prod_{\lambda|l} \mathcal{O}^*_{k_{n,\lambda}}$, where $k_{n,\lambda}$ is the residue field of $F_{n,\lambda}$. Now I_l acts trivially on J. Now let $\mu = \theta\psi^{-1}$ or $\psi\theta^{-1}$. Then $\mu(I_l) \neq 1$. Thus, $(\mathrm{Gal}(N_\infty/N^*))^\mu = 0$. This ends the proof of the lemma. □

Note that theorems 11.3.5 and 11.3.18 ensure that $\mathrm{Gal}(K_\infty/F_\infty)$ does not have any finite Λ modules. In this above situation, $K_{l,\infty}L_{l,\infty}$ is the unique unramified $\mathbb{Z}_p$-extension of $F_{l,\infty}$. Then we can repeat the above proof and the proof in the previous section to show that $\mathrm{Gal}(M_\infty/K_\infty L_\infty)$ is unramified everywhere. We summarize this in the form of the next theorem. Also note that this is perhaps one of the few results that is true in this thesis even without **Hypothesis 1**.

Theorem 3.5.27. *$M_\infty/L_\infty K_\infty$ is unramified everywhere.*

Proof. We have already proved most of this theorem. We just summarize the steps for the convenience of the reader.

$M_\infty/L_\infty K_\infty$ is unramified outside N and unramified at p. If there is any prime l that is infinitely ramified at either K_∞ or L_∞, then by applying Abhyankar's lemma as in 3.5.15, we can show $M_\infty/K_\infty L_\infty$ is unramified at l. Since any prime that ramifies in K_∞/F_∞ or L_∞/F_∞ has to be infinitely ramified since $\mathrm{Gal}(K_\infty/F_\infty)$ and $\mathrm{Gal}(L_\infty/F_\infty)$ have no finite Λ submodules, so this implies l is unramified in $K_\infty L_\infty/F_\infty$. Then looking locally at a prime $\mathfrak{l}|l$, $K_{\infty,\mathfrak{l}}L_{\infty,\mathfrak{l}}$ is the unique unramified $\mathbb{Z}_p$ extension of $F_{\infty,\mathfrak{l}}$. Now if the inertia subgroup J of $M_{\infty,\mathfrak{l}}/K_{\infty,\mathfrak{l}}L_{\infty,\mathfrak{l}}$ is non-trivial, then choosing a generator γ for the Galois group $\mathrm{Gal}(K_{\infty,\mathfrak{l}}L_{\infty,\mathfrak{l}}/F_{\infty,\mathfrak{l}}$, we see that conjugation action of γ on J sends $j \to j^l$. Thus the action is non-trivial but this contradicts that the fact that action on $M_\infty/K_\infty L_\infty$ is trivial. □

To summarize the results of the last two sections, one can always construct big unramified extensions over $K_\infty L_\infty$ under the following condition:

- $\mathrm{Gal}(K_\infty/F_\infty)$ and $\mathrm{Gal}(L_\infty/F_\infty)$ do not have any finite Λ submodules.

However to determine it explicitly in terms of some known Iwasawa modules, we need the following condition, which seems extremely hard to check in general

- Every element of I/I^2 is a commutator.

As remarked before, that is certainly true if $\mathrm{Gal}(K_\infty/F_\infty)$ or $\mathrm{Gal}(L_\infty/F_\infty)$ is cyclic. In that case, the proof of theorem 3.5.15 works out verbatim and we get

$$\mathrm{Gal}(M_\infty/K_\infty L_\infty) \cong I/I^2 \cong \mathrm{Gal}(K_\infty/F_\infty) \otimes_\Lambda \mathrm{Gal}(L_\infty/F_\infty) \tag{3.14}$$

Remark 3.5.28. One can follow the above procedure to construct big meta-abelian extensions, starting with a totally real base field F, if one assumes Leopoldt's conjecture and Iwasawa's $\mu = 0$ conjecture.

Remark 3.5.29. The f_q appearing in the theorem 3.5.23 are exactly the same as the factors of $B(T;\theta,\psi)$ appearing in [43], appendix A.

3.6 An explicit construction of a meta-abelian extension

We will give an explicit construction of the fields considered in a special case of elliptic curves of conductor 11. These computations can also be found in [17]. We will be working with

$$X_1(11) : y^2 + y = x^3 - x^2 \quad 11A3$$

$$X : y^2 + y = x^3 - x^2 - 7820x - 263580 \quad 11A2$$

and their mod 5 Galois representations (under suitable choice of basis) can respectively be given by the following $\begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix}$ and $\begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$, where * in both cases is non-zero. The ideal of reducibility I (proposition 3.4.8) in both the cases is (25) as we have a degree 25 isogeny between the curves but to make our calculations easier we will be working with the maximal ideal $\mathfrak{m} = (5)$. Call ρ_1 and ρ_2 the associated 5-adic Galois representations attached to each curve. Then the ideal generated by the $b(\sigma)$ in each case is $\mathbb{Z}_5$ and that of $c(\sigma)$ is (25). In fact, we can say more: By Kummer theory, we can identify $B/\mathfrak{m}B$ as the field generated by the 5-division polynomial over $\mathbb{Q}(\mu_5)$. Then $B_1/\mathfrak{m}B_1$ can be identified by $\mathrm{Gal}(K_1/\mathbb{Q}(\mu_5))$ where K_1 is the splitting field of the polynomial: $x^5 + 2x^4 + 6x^3 - 2x^2 + 4x - 1$. One can easily check that 11 ramifies in this extension and the primes above 5 split and $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ acts via ω^{-1}. And $B_2/\mathfrak{m}B_2$ can be identified with $\mathrm{Gal}(K_2/\mathbb{Q}(\mu_5))$ where K_2 is the splitting field of the polynomial $x^5 - 11$ and in this case both 5 and 11 ramify and $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ acts via ω. One can now identify $C_1/\mathfrak{m}C_1$ with $\mathrm{Gal}(K_2/\mathbb{Q}(\mu_5))$ and $C_2/\mathfrak{m}C_2$ with $\mathrm{Gal}(K_1/\mathbb{Q}(\mu_5))$. In this case, one can come to this conclusion by looking at the 125 division points. But we take a slight digression to explain this phenomenon in a more theoretical context as this is not an accident but one of the main driving forces behind the theory of modularity and p-adic L-functions.

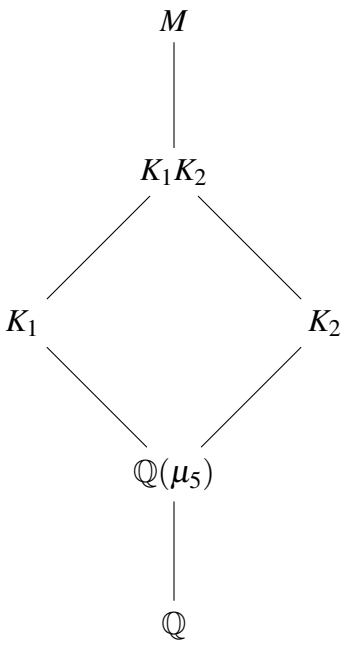
Let f be a modular form such that its associated mod p Galois representation is reducible. Then by Ribet's lemma (proposition 3.1.12), there exists at least one lattice such that the representation is non-semisimple. Up to a twist, the representation is given by $\begin{pmatrix} \omega\psi & * \\ 0 & 1 \end{pmatrix}$. Then following Ribet's proof in 3.1.13, one can show that there exists another lattice in $\mathbb{Q}_p^2$ where the mod p Galois representation can be given by $\begin{pmatrix} 1 & * \\ 0 & \omega\psi \end{pmatrix}$ where * in both cases is non-zero. Call these lattices ρ_1 and ρ_2. In fact these 2 lattices sit at two opposite extremes of the chain of lattices which realizes the Galois representation attached to f. One of them has the highest μ-invariant and the other the lowest, which is called the μ-deprived quotient.

Conjecture 3.6.1. (Greenberg): The μ-deprived quotient lattice has μ-invariant 0.

In our case, $X_1(11)$ indeed has μ-invariant 0 and X has μ-invariant 2 and they are on two extreme edges of the isogeny graph with $X_0(11)$ sitting between them. Now let us look at the first lattice. B/mB can be identified with $H^1(\mathbb{Q}_S, \mathbb{F}_p(\omega\psi))$ and C/mC can be identified with $H^1(\mathbb{Q}_S, \mathbb{F}_p(\omega^{-1}\psi^{-1}))$. Now let us assume the Hecke algebra associated to ρ_1 (or ρ_2) is Gorenstein. Then the above cohomology groups are 1-dimensional. In fact it's an if and only if statement by the work of Mazur-Tilouine. Now it's easy to see that $B/\mathfrak{m}B$ in the 2nd lattice is the $C/\mathfrak{m}C$ in the first lattice and vice versa.

Now we turn our attention to the following matrix over $\mathbb{F}_5$ given by $\begin{pmatrix} 1 & c & * \\ 0 & \omega & b \\ 0 & 0 & 1 \end{pmatrix}$ where we regard $c \in H^1(G_{\mathbb{Q}_{5,11}}, \omega^{-1})$ and $b \in H^1(G_{\mathbb{Q}_{5,11}}, \omega)$. Then the above computations show that the fixed field of the kernel of c is K_1 and the fixed field of the kernel of b is K_2. Since the cup product $c \cup b = 0$, we have the above 3-dimensional representation by lemma 2.3.4.

In fact, write the 5-adic representation of X as the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $* = d - 1 \bmod I/\mathfrak{m}I$. And this gives rise to the following diagram of fields given by the fixed field of the kernel of the representation. So the only unknown object in the following diagram is the degree 5-extension M of K_1K_2.



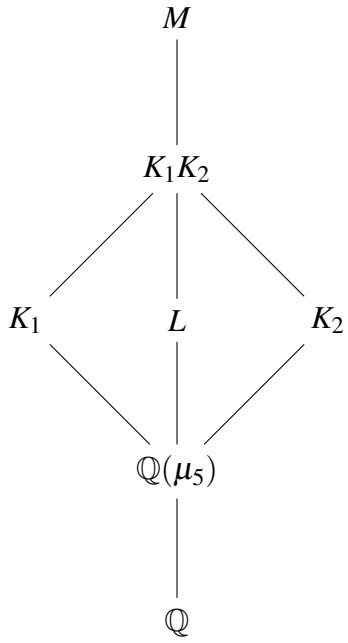
But before we write down what M is, we want to make some preliminary observations. $\mathrm{Gal}(M/K_1K_2)$ has trivial action of $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ and it is central and the commutator subgroup of $\mathrm{Gal}(M/\mathbb{Q}(\mu_5))$ and these can be easily seen by the matrix representation of the field diagram.

Now, conversely given any field diagram as above with the above properties, we claim that $\mathrm{Gal}(M/\mathbb{Q}(\mu_5)) = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$. Let $G := \mathrm{Gal}(M/\mathbb{Q}(\mu_5))$. Note that G is necessarily

non-abelian. We have an exact sequence

$$0 \to \mathbb{Z}/5 \to G \to \mathbb{Z}/5 \oplus \mathbb{Z}/5 \to 0.$$

So we have a non-abelian group of order 5^3. In fact we know that there are only 2 non-abelian groups of order p^3; one of them is the group of unipotent matrices with exponent p and the other is a group of exponent p^2. We now show that the latter situation can not happen. If there is an element of order 25, consider the fixed field of the subgroup generated by that element, call it L. Now since any subgroup of index 5 is necessarily normal, we see that L is a degree 5 Galois extension over $\mathbb{Q}(\mu_5)$. Now we need to show that L is Galois over $\mathbb{Q}$. To see this, note that the number of elements of order 25 in G is $125-25$. These give rise to $\frac{125-25}{\phi(25)} = 5$ distinct subgroups, where ϕ is the Euler phi function. Now $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ permutes these subgroups and already fixes K_1 and K_2. Thus $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ permutes the other 3 subgroups so there is a fixed point for this action. Call it L. Thus we can take L to be Galois over $\mathbb{Q}$ and L is necessarily disjoint from both K_1 and K_2. In fact we have the following diagram that explains our situation:



Now Gal($\mathbb{Q}(\mu_5)/\mathbb{Q}$) acts semi-simply on Gal($K_1K_2/\mathbb{Q}(\mu_5)$), since their orders are co-prime and there are two eigenvectors for this action, which contradicts the above picture as K_1, K_2 and L correspond to 3 different eigenvectors. Thus we have shown any diagram of the above form is in one-one correspondence with a matrix as described above. To get hold of the group Gal($M/\mathbb{Q}$), note that order of Gal($\mathbb{Q}(\mu_5)/\mathbb{Q}$) is coprime to Gal($M/\mathbb{Q}(\mu_5)$, so $H^2(G,(\mathbb{Z}/p)^*) = 0$. Thus Gal($M/\mathbb{Q}$) $= G \rtimes$ Gal($\mathbb{Q}(\mu_5)/\mathbb{Q}$) and now it is straightforward to see that Gal($M/\mathbb{Q}$) is of the form $\begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & 0 & 1 \end{pmatrix}$.
Now let M' be another field and let f' be the function in the top right corner of the matrix. Let f be a function such that $df = df' = c \cup b$. Thus

$$(f-f')(\sigma\tau) = (f-f')(\sigma) + (f-f')(\tau) \text{ for all } \sigma,\tau \in G_{\mathbb{Q}}$$

Thus $f - f'$ is a homomorphism, which corresponds to a degree 5 Galois extension of $\mathbb{Q}$

with possible ramifications only at 5 and 11. Thus once we find one M, we can get hold of all such M' by just composing with these fields. So that gives a complete description of all such M'. So now all we have to find is one such field. Now the 5-class group of K_1 is $\mathbb{Z}/5$ and is generated by any prime over 5 or 11 and the action of $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ is trivial on the 5-class group of K_1. For proof see [17] Prop 6.2. Call H_1 the 5- Hilbert class field. Since $[H_1 : \mathbb{Q}(\mu_5)] = 25$, H_1 is abelian over $\mathbb{Q}(\mu_5)$. Thus we can take M to be $H_1K_1K_2$. An alternative construction would be to see that the 5-class group for K_2 is $\mathbb{Z}/5 \oplus \mathbb{Z}/5$ and is generated by the primes above (5) and (11). One can see that the class generated by the prime over (5) is acted on trivially by $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$. Call that unramified 5-extension H_2. Then $H_2K_1K_2$ is our desired extension.

We think of the above picture as the base of the cyclotomic tower and thus this allows us to find non-trivial examples.

Finally one can put $X_1(11)$ in the Hida family. For a precise definition, see chapter 4. The Hida family in this case is just Λ and one can ask the same question for this Hida family. Since 5 is a regular prime, and the Hecke algebra is particularly nice, it is fairly straightforward to figure out the Λ-adic picture. Note the field K_∞ is a Kummer extension and is explicitly given by $\mathbb{Q}(\mu_{5^\infty}, (11)^{1/5^\infty})$. The Λ-module $\mathrm{Gal}(K_\infty/\mathbb{Q}(\mu_{5^\infty}))$ is cyclic and isomorphic to $\Lambda/(T-5)$. L_∞ is given by adjoining a compatible sequence of 5^∞-roots of $\pi/\bar{\pi}$. We also see that $\mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_{5^\infty}))$ is also a cyclic module. A theorem of Iwasawa (Theorem 2 in [29]) and the vanishing of μ by Ferrero-Washington shows that maximal extension of $\mathbb{Q}(\mu_{5^\infty})$ unramified outside 5 and 11 is a free pro-5 group on 2 generators. Thus the compositum of the two independent $\mathbb{Z}_5$ extensions that we constructed is the maximal abelian 5-extension and the field M_∞ is the field fixed by the commutator subgroup. Thus, by Nakayama's lemma, I is cyclic. For more precise results relating Gorensteinness of an universal deformation ring and the cyclicity of the ideal of reducibility, we refer the reader to [2].

Remark 3.6.2. The reader can clearly see an easy generalization of this above picture. Take a prime $q \equiv 1 \bmod p$. Then one can work out the entire picture, basically replacing 11 with q, for regular primes p. However for irregular primes, one needs Vandiver's conjecture to ensure the cyclicity of the appropriate Galois group as a Λ module. Thus Vandiver's conjecture implies the cyclicity of I. This should be reminiscent of the results in [36].

Remark 3.6.3. An example of the above type is worked out in [54] for the prime $p = 37$, $N = 1$ and for $\bar{\rho}^{ss} = 1 \oplus \omega^{32}$. And it seems to the author that Greenberg and Monsky in proposition 3.1.14 used very similar ideas in their unpublished note on the Ramanujan Δ function.

Remark 3.6.4. The Galois group of the maximal abelian extension of $\mathbb{Q}(\mu_{5^\infty})$ unramified outside 5 and 11 with ω action is $\Lambda \oplus \mathbb{Z}_5$. Λ extension is only ramified at 5 and so we can not recover that extension in our construction.

3.7 Pseudo-deformations

In this section, we make a slight digression into pseudo-deformations. All the results in this section are fairly standard and readily available in the literature. We follow the notations of Taylor [59].

Let G be a group and R is a commutative ring with 1. We will assume $d!$ is invertible in R.

Definition 3.7.1. A R-valued (continuous) pseudo-character of dimension d is a R-linear (continuous) function $T : G \to R$ such that

- $T(e) = d$
- $T(g_1 g_2) = T(g_2 g_1) \ \ \forall g_1, g_2 \in G.$
- $\sum_{\sigma \in S_{d+1}} \varepsilon(\sigma) T^{\sigma}(g_1, \ldots g_{d+1}) = 0$

where $T^{\sigma} : G^{d+1} \to R$ is given by the following.

Let $x = (x_1, \ldots x_{d+1}) \in G^{d+1}$. Let σ be the cycle $(j_1, \ldots j_m)$, then $T^{\sigma} := T(x_{j_1} \ldots . x_{j_m})$. Now for any general σ, define $T^{\sigma} := \prod T^{\sigma_i}$, where $\sigma = \prod \sigma_i$ be it's cycle decomposition.

Of course trace of a representation satisfies the above 3 conditions. All our pseudo-characters will be continuous so we will drop the word continuous in the sequel. Taking R to be $\mathbb{F}$, one can consider deformations of T to $\mathscr{C}_{\mathscr{O}}$. Let $D_T^{ps}(A)$ be the set of deformations of T to A.

Lemma 3.7.2. *The functor D_T^{ps} is (pro)represented by a complete local Noetherian $\mathscr{O}$-algebra R_T^{ps}.*

Now Carayol-Serre lemma 3.1.20 immediately shows that if $\bar{\rho}$ is absolutely irreducible and T is it's trace, then there is an isomorphism: $R_{\bar{\rho}}^{univ} \cong R_T^{ps}$. In the sequel, let $d = 2$. However if $\bar{\rho}$ is reducible, such an isomorphism does not hold in general as the following example in [31] shows. Suppose that $\chi_1,\ \chi_2 : G \to \mathbb{F}^*$ are characters and $c_1,\ c_2 \in \mathrm{Ext}^1(\mathscr{O}_2, \mathscr{O}_1)$.

Then $\begin{pmatrix} \chi_1 & c_1+c_2T \\ 0 & \chi_2 \end{pmatrix}$ is a representation of $G \to GL_2(\mathbb{F}[T])$. More naturally, one obtains a family of representations of G over $\mathbb{P}(\mathrm{Ext}^1(\emptyset_2,\emptyset_1))$, the projectivization of $\mathrm{Ext}^1(\emptyset_2,\emptyset_1)$, and all have same the pseudo-character $\chi_1+\chi_2$. However our **Hypothesis 1** will enable us to compare the two rings.

Lemma 3.7.3. *Assume* **Hypothesis 1**. *Let $V_{\mathbb{F}[\varepsilon]/\varepsilon^2}$ be a deformation of $\bar{\rho}$. If $V_{\mathbb{F}[\varepsilon]/\varepsilon^2}$ induces the trivial deformation on pseudo-characters, then $V_{\mathbb{F}[\varepsilon]/\varepsilon^2}$ is the trivial deformation.*

Proof. This is lemma 1.4.3 of [32]. In fact we gave a different proof of this result in our proof of Theorem 3.4.1, even though we did not state this result explicitly. In fact, there we showed that if $a'=d'=0$, then $b'=kb$ and the above lemma follows from that. □

Corollary 3.7.4. *(a) Under* **Hypothesis 1**, *there exists a surjection $\pi : R_T^{ps} \twoheadrightarrow R_{\bar{\rho}}^{univ}$ induced by sending a representation to it's trace.*

(b) $t_{R^{ps}} \cong t_{R_{\bar{\rho}}^{univ}}$

Proof. This is corollary 1.4.4 of [32].

(b) These modules are finite and have the same cardinality due to a result of Chenevier-Bellaiche [2] and corollary 3.4.2. And the map induced by the trace map is surjective so it's an isomorphism. □

Proposition 3.7.5. *Assume Hypothesis* 1 *and* **Neben** *and fix the determinant (for simplicity). There are no non-trivial upper triangular deformations to $\mathbb{F}[\varepsilon]$ and so $\mathscr{R}_{\bar{\rho}}^{univ,det}$ is generated by the traces of the Frobenii.*

Proof. We first show that there are no non-trivial upper triangular deformations. Under **Neben**, we see that we have unique lifts of our diagonal characters to $\mathbb{F}[\varepsilon]$ and in fact we will take these lifts to be trivial. Thus our deformation has the shape of $\begin{pmatrix} \bar{\chi}_1 & b+b'\varepsilon \\ 0 & \bar{\chi}_2 \end{pmatrix}$.

A simple matrix calculation shows that $b' \in \mathrm{Ext}^1(\bar{\emptyset}_2, \bar{\emptyset}_1)$, thus $b' = kb$. Calculations in 3.3 immediately show that this is a trivial deformation.

The next statement follows from the surjection π in the previous lemma. We give a sketch of another proof following the lines of Carayol-Serre. This is a fairly standard and straightforward argument. It suffices to show that any non-trivial deformation of $\bar{\rho}$ to $GL_2(\mathbb{F}[\varepsilon])$ is generated by traces. The proof is similar to Carayol's proof. Let ρ be a deformation of $\bar{\rho}$ to $GL_2(\mathbb{F}[\varepsilon])$. Write the matrix entries of ρ as functions $a + a'\varepsilon, b + b'\varepsilon, \varepsilon c$ and $d + d'\varepsilon$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let K be the fixed field of the kernels of $\bar{\chi}_1$ and $\bar{\chi}_2$, by **Neben**, $\det(\rho)$ factors through K. Thus if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, then $\mathrm{Det}(\rho(\sigma)) = 1 = 1 + a'\varepsilon + d'\varepsilon - bc\varepsilon$. Since c is non-trivial (by assumption), the Cebotarev density theorem implies there exists a σ such that $b(\sigma)c(\sigma) = 0$. But $\mathrm{trace}(\rho(\sigma)) = 1 + a'\varepsilon + d'\varepsilon = 1$, it follows that the traces of ρ generate $\mathbb{F}[\varepsilon]$. Since $\mathscr{R}_{\bar{\rho}}^{univ,det}$ is generated a Λ-algebra by the generators of $m_{\mathscr{R}_{\bar{\rho}}^{univ,det}}/m^2_{\mathscr{R}_{\bar{\rho}}^{univ,det}}$ and the result follows via Nakayama's lemma. □

Chapter 4: Hida theory of ordinary modular forms and Hecke algebras

We will assume the reader is familiar with the definition of modular forms and Hecke operators. In this section, we will give a summary of facts about Galois representations attached to modular forms and Hida theory. We will end this chapter by giving an explicit structure of the Hida Hecke algebra. We follow the exposition in Hida, Emerton-Pollack-Weston, Ohta and Fukaya-Kato-Sharifi. Just to set up our notation, for any congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$, we denote by $M_k(\Gamma)$ (resp. by $S_k(\Gamma)$) the space of all modular forms (resp. cusp forms) of weight k and level Γ. For any Dirichlet character χ and $\alpha := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, we define

$$\chi(\alpha) := \chi(d)$$

Definition 4.0.1. We say a modular form f on $\Gamma_1(N)$ has Nebentypus χ if $\Gamma_0(M)$ acts on f via the character χ.

Note that by considering q-expansions one can define

$$M_k(\Gamma)_{\mathbb{Z}} := M_k(\Gamma) \cap \mathbb{Z}[[q]]$$

and for any ring R,

$$M_k(\Gamma)_R := M_k(\Gamma)_{\mathbb{Z}} \otimes_{\mathbb{Z}} R \hookrightarrow R[[q]]$$

and similarly for $S_k(\Gamma)_{\mathbb{Z}}$ and $S_k(\Gamma)_R$. Now let $\Gamma = \Gamma_1(N)$. Then one has the double coset operators given by the following:

For all primes l, we define T_l to be the double coset operator

$$T_l = \Gamma \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} \Gamma$$

and for d coprime to N, we define $\langle d \rangle$ to be the operator, $\langle d \rangle = \Gamma \alpha_d \Gamma$, where $\alpha_d \in \Gamma_0(N)$ satisfies

$$\alpha_d \equiv \begin{pmatrix} * & 0 \\ 0 & d \end{pmatrix} \bmod (N)$$

The Hecke algebra $\mathbb{T}$ is the commutative algebra defined over $\mathbb{Z}$ by the operators T_l and $\langle d \rangle$. The action of the Hecke operators on modular forms is well known and $M_k(\Gamma)$ and $S_k(\Gamma)$ are stable under the Hecke operators. With this in mind, we define the Hecke algebra (resp. cuspidal Hecke algebra) $\mathfrak{H}_k(\Gamma)$ (resp. $\mathfrak{h}_k(\Gamma)$) to be the image of $\mathbb{T}$ inside $\mathrm{End}_{\mathbb{Z}}(M_k(\Gamma)_{\mathbb{Z}}$ (resp. $\mathrm{End}_{\mathbb{Z}}(S_k(\Gamma)_{\mathbb{Z}})$. Note that these are the $\mathbb{Z}$ subalgebra of $\mathrm{End}_{\mathbb{Z}}(M_k(\Gamma)_{\mathbb{Z}}$ and $\mathrm{End}_{\mathbb{Z}}(S_k(\Gamma)_{\mathbb{Z}}$ generated by T_l and $\langle d \rangle$. For any ring R, we define

$$\mathfrak{H}(\Gamma)_R := \mathfrak{H}(\Gamma)_{\mathbb{Z}}$$

$\mathfrak{h}(\Gamma)_R$ is defined analogously.

4.1 Galois representations attached to classical modular forms

Let f be a normalized i.e. $a_1 = 1$, cuspidal newform for $\Gamma_1(Np^r)$, of weight $k \geq 2$ and nebentypus χ which is a Hecke eigenform for all Hecke operators. Let K_f denote the field generated by the coefficients of the q-expansion of f. It is well-known that K_f is a number field.

Definition 4.1.1. We call a modular (cusp) form f ordinary if a_p is a p-adic unit.

The next theorem is a landmark result in the theory of modular forms. It is the culmination of the work of Shimura, Carayol, Deligne, Serre, Mazur and Wiles.

Theorem 4.1.2. *Let f be as above. Choose a prime $\mathfrak{p}$ above p in K_f and let $K_{f,\mathfrak{p}}$ denote the $\mathfrak{p}$-adic completion of K_f. Then there exists a compatible system of absolutely irreducible p-adic representations $\rho_{f,p}$ of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ in $GL_2(K_{f,\mathfrak{p}})$ satisfying*

1. *$\rho_{f,p}$ is unramified outside Np.*
2. *For any prime $q \nmid Np$,*

$$\det(1 - \rho_{f,p}(Frob_q)T) = 1 - a_q T + q^{k-1}\chi(q)T^2$$

3. *$\det(\rho_{f,p}(c)) = -1$, where c is a complex conjugation.*
4. *Let ν_p be the p-adic cyclotomic character, then $\det\rho_{f,p} = \chi\nu_p^{k-1}$, where we view χ as a Galois character by defining $\chi(Frob_q) := \chi(q)$ for all $q \nmid Np$.*
5. *(ordinary) (Deligne, Mazur-Wiles) The restriction of $\rho_{f,p}$ to the decomposition sub-*

group at p is isomorphic to an upper triangular representation of the form

$$g \mapsto \begin{pmatrix} \varepsilon(g) & * \\ 0 & \delta(g) \end{pmatrix}$$

where δ is unramified and $\delta(Frob_p)$ is the unique p-adic root of

$$x^2 - a_p x + \chi(p)p^{k-1} = 0$$

Here we take $\chi(p) = 0$ if $p|N$, so then $\delta(Frob_p) = a_p$.

6. *(Langlands, Carayol) Let $q \neq p$ and $q|N$, let C be the conductor of χ. Write $N = q^e N'$ (resp. $C = q^{e'} C'$) so that $q \nmid N'$ (resp. $q \nmid C'$).*

   (a) If $e = e' > 0$, then $\rho_{f,p}$ restricted to inertia subgroup at q is equivalent to the following form: $\begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$. Moreover $\rho_{f,p}$ restricted to the Decomposition subgroup at q is still diagonal. Let δ_q be the unique unramified character appearing in $\rho_{f,p}|_{D_q}$, we have $\delta_q(Frob_q) = a_q$.

   (b) (Steinberg case) If $e = 1$ and $e' = 0$, $\rho_{f,p}$ restricted to the Decomposition subgroup at q is ramified and is equivalent to the following form: $\begin{pmatrix} \eta(1) & * \\ 0 & \eta \end{pmatrix}$. where η is an unramified character that takes $Frob_q$ to a_q and $\eta(1)$ is the twist of η by the p-adic cyclotomic character.

   (Note: In this case the image of inertia is infinite)

Remark 4.1.3. The representation depends on the choice of $\mathfrak{p}$ above p and we have abused notation to write the representation as $\rho_{f,p}$.

4.2 Hida theory of Λ-adic modular forms

Given integers $k \geq 2$ a prime $p \geq 5$, and N, such that $p \nmid N$ and let $\mathscr{O}$ be the ring of integers in some complete subring of $\mathbb{C}_p$, we note the inclusion

$$\iota : M_k(\Gamma_1(Np^\alpha)) \to M_k(\Gamma_1(Np^\beta)) \text{ for any } \alpha \leq \beta$$

commutes with the action of Hecke operators. Thus the restriction of a Hecke operator from level Np^β is an Hecke operator for level Np^α. This map induces a projection morphism $\mathfrak{H}_k(\Gamma_1(Np^\beta)) \twoheadrightarrow \mathfrak{H}_k(\Gamma_1(Np^\alpha))$ taking T_l to T_l. Now, we define $S_k(Np^\infty, \mathscr{O})$ and $M_k(Np^\infty, \mathscr{O})$ to be the space of weight k cusp forms and modular forms respectively that are in $\Gamma_1(Np^r)$ for some $r \geq 0$ and whose q-expansion (at the cusp at ∞) lie in $\mathscr{O}$. We have an action on these spaces by the groups $(\mathbb{Z}/N)^*$ via the nebentypus character and $\mathbb{Z}_p^*$ via the product of the nebentypus character along with the map $\gamma \mapsto \gamma^k$ (weight map/action). This action makes the above spaces an $\mathscr{O}[[\mathbb{Z}_p^*]]$-module, which we will call (by abuse of notation) Λ. For all $l \nmid Np$ we have the action of the Hecke operator T_l, and U_p and U_q for primes $q|N$ on these spaces. Thus $S_k(Np^\infty, \mathbb{Z}_p)$ and $M_k(Np^\infty, \mathbb{Z}_p)$ are naturally $\mathfrak{h}_k(N) := \varprojlim \mathfrak{h}_k(\Gamma_1(Np^r))$ and $\mathfrak{H}_k(N)$-modules. One can also define the ring of p-adic modular forms (cusp forms) via p-adic completion of the divided congruences of the ring $\oplus_k M_k(Np^\infty, \mathscr{O})$ (respectively $S_k(Np^\infty, \mathscr{O})$). Hida has defined an ordinary projector on these spaces

$$e := \lim_{n \to \infty} U_p^{n!}.$$

If f is an eigenform for the operator U_p with eigenvalue a_p, one can easily check $ef = f$ iff a_p is a p-adic unit, otherwise $ef = 0$. By using the projector e, we denote the space of ordinary modular forms (resp. cusp forms) by $M_k^{ord}(N)$ (resp. $S_k^{ord}(N)$). We also denote the ordinary Hecke algebra (resp. cuspidal Hecke algebra) by $\mathfrak{H}_k^{ord}(N)$ (resp. by $\mathfrak{h}_k^{ord}(N)$).

Theorem 4.2.1. *(Hida) The spaces $S_k^{ord}(N)$ and $M_k^{ord}(N)$ are finite free Λ modules and moreover these spaces are independent of k as long as $k \geq 2$.*

Proof. See [22] Theorem 1. □

Before we state the next definition, let us introduce some special prime ideals in Λ. An arithmetic prime of Λ is a prime ideal of the form

$$P_{k,\varepsilon} := (1+T-\varepsilon(1+p)(1+p)^k) \tag{4.1}$$

for $k \geq 2$ and character $\varepsilon : 1+p\mathbb{Z}_p \to \mathscr{O}^\times$ of p power order, say $p^{r(\varepsilon)}$. If $\mathbb{I}$ is a finite extension of Λ, we call a prime of $\mathbb{I}$ arithmetic if it lies over some $P_{k,\varepsilon}$.

Definition 4.2.2. (Hida-Wiles) Fix a finite flat integral domain $\mathbb{I}$ over Λ. A $\mathbb{I}$-adic form F of level N and character χ: $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}_p^*$ is a formal q-expansion

$$F = \sum_{n=0}^{\infty} a_n(F)q^n \ \in \mathbb{I}[[q]]$$

such that for almost all arithmetic primes $P_{k,\varepsilon}$, $F \bmod P_{k,\varepsilon} \in M_k^{ord}(Np^{r(\varepsilon)}, \varepsilon\chi\omega^{-k})$. One can similarly define a $\mathbb{I}$-adic cusp form.

To ease notation, we will drop N when the tame level is understood. The following theorem gives a brief summary of Hida theory.

Theorem 4.2.3. *(Hida) (a) $\mathfrak{H}^{ord}(\chi)$ and $\mathfrak{h}^{ord}(\chi)$ are free of finite rank over Λ.*
(b) We have the following specialization property: For every arithmetic prime of the form $P_{k,\varepsilon}$, $k \geq 2$, there are isomorphisms

$$\mathfrak{H}^{ord}(\chi)/P_{k,\varepsilon}\mathfrak{H}^{ord}(\chi) \cong \mathfrak{H}_k^{ord}(Np^{r(\varepsilon)+1}, \chi\varepsilon\omega^{-k})$$

$$\mathfrak{h}^{ord}(\chi)/P_{k,\varepsilon}\mathfrak{h}^{ord}(\chi) \cong \mathfrak{h}_k^{ord}(Np^{r(\varepsilon)+1}, \chi\varepsilon\omega^{-k})$$

sending T_l to T_l.

(c) Both $\mathfrak{H}^{ord}(\chi)$ and $\mathfrak{h}^{ord}(\chi)$ are etale over all arithmetic points of Λ.

Proof. See [24], Corollary 3.20 for (a), Corollary 3.19 for (b), Corollary 1.4 in [22] for (c) and Theorem 1.2 in [22] for (a). □

We have a duality between modular forms and Hecke algebras.

Theorem 4.2.4. *(Hida-Ohta) There is a non-degenerate pairing*

$$S^{ord}(\chi) \times \mathfrak{h}^{ord}(\chi) \to \Lambda$$

given by $(f,T) \mapsto a_1(f|T)$. The pairing induces isomorphisms $Hom_\Lambda(\mathfrak{h}^{ord}(\chi),\Lambda) \cong S^{ord}(\chi)$ and $Hom_\Lambda(S^{ord}(\chi),\Lambda) \cong \mathfrak{h}^{ord}(\chi)$

Define $\mathbb{M}^{ord}(\chi) := \{f \in M^{ord}(\chi)_{Q(\Lambda)} : a_n(f) \in \Lambda,\ \forall\ n \geq 1\}$, then $\mathbb{M}^{ord}(\chi)$ and $\mathfrak{H}^{ord}(\chi)$ are duals of each other via the above map.

Proof. This is theorem 3.17 in [24]. □

Remark 4.2.5. There seems to be no consensus in literature about how these maps should be normalized. We have followed Hida's notations in this chapter. The reader should make sure that the normalizations are consistent when they are checking other references.

4.3 Structure of Hida Hecke algebras and big modular Galois representations

For the rest of the section, let us assume that N is squarefree.

Lemma 4.3.1. *$\mathfrak{H}^{ord}$ and $\mathfrak{h}^{ord}$ are reduced.*

Proof. This is corollary 1.3 in [26]. □

Lemma 4.3.2. *$\mathfrak{H}^{ord}$ is a complete semi-local ring, with maximal ideals m_1,..,m_s and the maximal ideals correspond to a mod p system of eigenvalues of modular forms of tame level N.*

Proof. It's a fairly standard argument in Hida theory to reduce to the weight 2 case and then there are only finitely many mod p modular forms of weight 2 and level N. For more details see [24] Chapters 3.1 and 3.2. □

Piecing together the above arguments, we get the following well-known proposition. This can also be found in Chapter 3 in [24].

Proposition 4.3.3. *$\mathfrak{H}_m^{ord}$ is equidimensional, reduced of dimension 2 and any minimal prime ideal has characteristic 0. M_m^{ord} is a Cohen-Macaulay $\mathfrak{H}_m^{ord}$-module.*

Proof. (Sketch) We know that $\mathfrak{H}_m^{ord}$ is a finite free Λ algebra, thus $\dim \mathfrak{H}_m^{ord} = \dim \Lambda = 2$. Equidimensionality follows from the fact that any finite torsion-free algebra M over Λ is necessarily equidimensional. Theorem 17.3 from [35] shows for any minimal prime $\mathfrak{p}$ of X, $\dim X/\mathfrak{p} = \dim X$. Since $p \in \mathfrak{H}_m^{ord}$ can be extended into a regular sequence, $\mathfrak{p}$ must be characteristic 0. Finally,

$$\mathrm{depth}_{\mathfrak{H}_m^{ord}} M_m^{ord} \geq \mathrm{depth}_{\Lambda} M_m^{ord} = \dim \Lambda = 2$$

Thus M_m^{ord} is a Cohen Macaulay $\mathfrak{H}_m^{ord}$ module. □

Remark 4.3.4. This proposition is crucial for imposing various hypotheses on class groups on the deformation theory side. We saw that the tangent space on the deformation rings can be arbitrarily large depending on the size of the class groups or ray class groups, whereas the Hecke algebra is quite small.

Now we come to the one of main theorems of this section.

Theorem 4.3.5. *(Hida, Wiles) There exist a continuous 2-dimensional pseudo-character $T : G_{\mathbb{Q}} \to \mathfrak{H}_m^{ord}$, such that $T(Frob_l) = T_l$, for $l \nmid Np$. Or in other words one has a continuous 2-dimensional representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathfrak{H}_m^{ord} \otimes Q(\Lambda))$, such that tr($\rho$)= T and $\rho|_{D_p} = \begin{pmatrix} \varepsilon(g) & * \\ 0 & \delta(g) \end{pmatrix}$, where δ is unramified and $\delta(Frob_p) = U_p$.*

Remark 4.3.6. Note that there is no reason why we can choose our representation to take values in $GL_2(\mathfrak{H}_m)$, such that $\rho \bmod \mathfrak{m} = \bar{\mathfrak{E}}$. So to remedy the situation, from now on we will be assuming **Hypothesis 1** and **Neben**.

Let us summarize our discussion in the form of the following commutative diagram, which we view as a special case of local-global compatibility. The complete details of the proof of the next proposition can be found in [25] page 230 and 232.

Proposition 4.3.7. *(Local-Global compatibility) We have a commutative diagram as follows:*

$$\begin{array}{ccccc} R^{ord} & \longrightarrow & \mathscr{R}_{\rho}^{univ} & \twoheadrightarrow & \mathfrak{h}_m \\ & \nwarrow & & \nearrow & \\ & & \Lambda & & \end{array}$$

Proof. Before giving the proof, we explain why we call it a Local-Global compatibility, we think of the top map coming from the Galois side and the map from $\Lambda \to \mathfrak{h}_m$ is coming from

the automorphic side. The top arrow is constructed via the following: Note $\mathscr{R}_{\bar{\rho}}^{univ}$ is generated by the traces by Proposition 3.7.5 and by the modularity of $\bar{\rho}$ (cf. Proposition 6.2.35) the map $\pi : R_{\bar{\rho}}^{univ} \twoheadrightarrow \mathfrak{h}_m$ is given by $\mathrm{Tr}(\rho^{univ}(Frob_l)) \mapsto T_l$ and $\delta(Frob_p) \mapsto U_p$. The map from $R^{ord} \to R_{\bar{\rho}}^{univ}$ is given by taking a representation and restricting it to D_p. The map $\Lambda \to \mathfrak{h}_m$ is given by $l \mapsto \langle l \rangle$ for $l \nmid Np$. Now the map from $\Lambda \to R^{ord}$ is essentially given by the "weight" character. We refer the reader to page 232 in [25] for a detailed description of this map and the commutativity of the two Λ actions. □

Corollary 4.3.8. *The map $R^{ord} \longrightarrow \mathfrak{h}_m$ is finite.*

Proof. This is straightforward since $\Lambda \cong R^{ord}$ by theorem 3.3.10 and $\Lambda \to \mathfrak{h}_m$ is finite by theorem 4.2.3 and the diagram commutes. □

Remark 4.3.9. The corollary basically says that there are only finitely many ordinary modular forms of a fixed tame level N with a given mod p representation at D_p. Such a statement is extremely hard to prove in the non-ordinary case and is a result of Emerton-Breuil-Paskunas, using their solution of the p-adic local Langlands correspondence. In fact even in our special case, we needed an automorphic input and to get that automorphic input in the non-ordinary case, one needs the full power of Colmez's Montreal functor.

Chapter 5: Images of Galois representations

The goal of this section is to prove a big image result and deduce some consequences. We will start the section with summarizing the motivation and known results. Then we will then use modularity lifting results to prove the Galois representation is big in $GL_2(\mathbb{F}[[T]])$.

5.1 History of related results

Understanding the images of Galois representations was first initiated by Serre who showed non CM elliptic curves have big images. The work was then extended by Momose and Hida-Lang in the Λ-adic setting. The big image question appears naturally in controlling the sizes of Selmer groups which are used in the calculations of Wiles [69] and others in the context of modularity lifting. The big image also appears in the work of Kato in constructing an Euler system in his proof of the main conjecture for elliptic curves.

5.2 A new big image theorem

Our goal in this section is to give a very simple proof of the big image properties of the representations studied by Skinner and Wiles. This question was inspired by a comment of Hida in [27] and subsequent discussions with Chris Skinner at the Arizona Winter School in 2017.

We start off with a couple of group theoretic lemmas.

Lemma 5.2.1. *Let ρ be an irreducible 2-dimensional representation of a group G. Let G' be an finite index normal subgroup of G such that $\rho|_{G'}$ is a sum of 2-distinct characters, then there exist a subgroup H of G of index 2 and a character ψ of H such that $\rho = Ind_H^G \psi$.*

Proof. Call the characters appearing in the lemma χ_i. Since G' is normal in G and χ_i are distinct characters, we claim G acts transitively on the set $\{\chi_1, \chi_2\}$.

Proof of claim: Suppose on the contrary, G fixes χ_1. Let L_1 and L_2 be the two G'-lines on which G' acts via the characters χ_i. Let l_i be the G'-bases of L_i. Then there exist a $g \in G$, such that

$$gl_1 = al_1 + bl_2$$

with $b \neq 0$, otherwise L_1 will be G-stable contradicting the irreducibility of V. Then, for $h \in G'$,

$$ghl_1 = g\chi_1(h)l_1 = \chi_1(h)(al_1 + bl_2)$$

Now $gh = h'g$ for some $h' \in G'$. This implies

$$h'gl_1 = h'(al_1 + bl_2) = a\chi_1(h')l_1 + b\chi_2(h')l_2 = a\chi_1(h)l_1 + b\chi_1(h)l_2$$

Thus $\chi_1(h) = \chi_2(h')$, since $ghg^{-1} = h'$ and $\chi_1(h') = \chi_1(ghg^{-1}) = \chi_1(h)$, since G fixes χ_1. Thus we get $\chi_1 = \chi_2$, which is a contradiction.

Thus G can not fix χ_1. Let H be the stabilizer of χ_i under this action. Then clearly H is of index 2. Now we show that we can extend χ_i to characters on H.

Let $h' \in H$ and let $h'l_1 = al_1 + bl_2$. Let $g \in G'$ and $h' = g^{-1}hg$, where $h \in H$. Then

$$gh'l_1 = a\chi_1(g)l_1 + b\chi_2(g)l_2$$

But

$$hgl_1 = h\chi_1(g)l_1.$$

Therefore $hl_1 = al_1$. So L_1 is a H-stable 1-dimensional vector space so χ_1 extends to H i.e. $\mathrm{Hom}_H(\rho, \chi_i) \neq 0$. Call the extended character ψ. By Frobenius reciprocity, we get $\mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G \psi) \neq 0$. But since ρ is irreducible, this proves $\rho = \mathrm{Ind}_H^G \psi$. □

Definition 5.2.2. We call a representation dihedral if it is induced from a character from a quadratic extension. Note that the projective image of the reduction of such a representation is a dihedral group.

We now need to show that the restriction of any irreducible representation to any finite index normal subgroup is semi-simple. But this is Clifford's theorem. We give a quick sketch of the proof.

Lemma 5.2.3. *(Clifford) Let W be a simple G-module. Let H be a finite index normal subgroup of G. Then W is a direct sum of simple H-modules.*

Proof. Let U be any simple H-submodule of W. Then the conjugates of U are H-submodules since H is normal. The intersection of one with the sum of others is another H-submodule but this intersection must be 0 as U is simple. Since the span of all G-conjugates is a G-submodule of W, it must be all of W. □

We give a short and quick exposition to Pink's theory of Lie algebras in [46].
Let A be any complete semi-local p-profinite ring, where $p > 2$. In our examples, A will be $\mathbb{F}[[T]]$ where $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$ which contains all the relevant eigenvalues (see below). Pink defines a map

$$\Theta : SL(2) \to \mathfrak{sl}(2)$$

$$M \mapsto M - (tr(M)/2)Id.$$

Let $\mathfrak{G}$ be a p-profinite subgroup of $SL(2)$. Then define $L_1(\mathfrak{G})$ to be the closed subgroup of $\mathfrak{sl}(2)$ that is topologically generated by $\Theta(\mathfrak{G})$. Let $L_1 \cdot L_1$ be the closed additive subgroup of $M_2(A)$ that is topologically generated by $\{\Theta(x)\Theta(y) : x, y \in \mathfrak{G}\}$. Let $C = Tr(L_1 \cdot L_1)$ which we view as scalar matrices. In fact we can define subgroups inductively by

$$L_2 = [L_1, L_1],\ L_{n+1} = [L_1, L_n] \text{ for all } n \geq 1$$

$$H_n := \{x \in SL_2(A) : \Theta(x) \in L_n \text{ and } tr(x) - 2 \in C\} \text{ for all } n \geq 1.$$

We summarize the main results of Pink's theory in the following theorem.

Theorem 5.2.4. *(Pink) The map $\Theta : H_n \to L_n$ is a homeomorphism. H_n is a pro-p subgroup of $SL_2(A)$ and H_n is normalized by H_1. Conversely if $\mathfrak{G}$ is any pro-p subgroup and L is the closed additive group generated by $\Theta(\mathfrak{G})$, then $\mathfrak{G} \subset H_1$ and the commutator subgroup of $\mathfrak{G}$ is H_2.*

The main facts that we will use from Pink's theory are as follows:

- $C \cdot L \subset L$.
- If $g \in GL_2(A)$ normalizes $\mathfrak{G}$, then g normalizes $L(\mathfrak{G})$.

With the above results in hand, we show that the images of the representations are big, i.e. they contain an open subgroup of $SL(2)$.

Theorem 5.2.5. *Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}[[T]])$ be such that*

i) ρ is irreducible, mod p distinguished and ordinary. (cf. Definition 3.3.1 and Definition 3.3.3)

ii) Determinant is of infinite order.

iii) There exists $\sigma \in I_p$ such that $\rho(\sigma) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ where $* \neq 0$

Then Im(ρ) contains an open subgroup of $SL_2(\mathbb{F}[[T]])$.

Proof. Let $\tau \in I_p$ and let $\overline{\rho}(\tau) = \begin{pmatrix} \bar{a} & \bar{b} \\ 0 & 1 \end{pmatrix}$. Since $\det(\bar{\rho}) \mid_{I_p} = \bar{\chi}_{cyc}$ and $p \geq 5$, we can always choose $\bar{a}$ to have order greater than 2. Now $\rho(\tau)$ is upper triangular by ordinarity of ρ. Call the lift $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Since $\bar{a} \neq \bar{d}$, $a-d$ is a unit power series in $\mathbb{F}[[T]]$. Conjugating the image of ρ by the matrix $M := \begin{pmatrix} 1 & b/(a-d) \\ 0 & 1 \end{pmatrix}$, we can assume that $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{Im}(\rho)$. Note that by raising τ to p^n powers and taking limits, we can assume that $a, d \in \mathbb{F}$, since $\lim_{n\to\infty} T^{p^n} = 0$. The action of $\mathrm{Ad}(\rho(\tau))$ on L has 3 distinct eigenvalues, namely $1, ad^{-1}$ and $a^{-1}d$. Call $\lambda = ad^{-1}$. Thus the Lie-algebra L decomposes into the corresponding eigenspaces, $L = L[1] \oplus L[\lambda] \otimes L[\lambda^{-1}]$, where $L[1] = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$, $L[\lambda] = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, $L[\lambda^{-1}] = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$, where $L[i]$ is the eigenspace corresponding to eigenvalue i. Let γ be a topological generator of $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_p))$, such that $\chi_{cyc}(\gamma) = 1+T \in \mathbb{F}[[T]]$. Hence we get $\rho(\gamma) = \begin{pmatrix} 1+T & u \\ 0 & 1 \end{pmatrix}$. Since we are looking at the image of ρ conjugated by M, we need to conjugate $\rho(\gamma)$ by M and thus we get $\begin{pmatrix} 1+T & u - \frac{Tb}{a-d} \\ 0 & 1 \end{pmatrix}$ is in $M\mathrm{Im}(\rho)M^{-1}$. Finally note that M commutes with unipotent matrices. Thus conjugating the image of ρ by M does not change our underlying assumptions about $\mathrm{Im}(\rho)$. Now, by Pink's result, $\rho(\gamma)$ normalizes L. Conjugating $L[\lambda]$ with $\rho(\gamma)^s$, we get $\begin{pmatrix} 0 & b(1+T)^s \\ 0 & 0 \end{pmatrix} \in L[\lambda]$ for all $s \in \mathbb{Z}_p$. And similar computation with $L[\lambda^{-1}]$ shows that both $L[\lambda], L[\lambda^{-1}]$ are $\mathbb{F}[[T]]$-modules. Since we know that there exist a b whose constant term is non-zero, we

have just shown that $L[\lambda]$ is isomorphic to $\mathbb{F}[[T]]$. Note that $[L[\lambda], L[\lambda^{-1}]] \subset L[1]$. Thus if $L[\lambda^{-1}] = \mathfrak{a}$, where $\mathfrak{a}$ is a non zero $\mathbb{F}[[T]]$ ideal, then $\mathfrak{a} \subset L[1]$. Now we are left to show that $L[\lambda^{-1}]$ is non-trivial. Let K be the fixed field of the kernel of $\det(\overline{\rho})$ and H= Gal$(\overline{\mathbb{Q}}/K)$. Thus H is a finite index normal subgroup of $G_{\mathbb{Q}}$. Now we claim that $\rho|_H$ is irreducible. If not, then it is a sum of characters by lemma 5.2.3, which implies that ρ is induced from a character by lemma 5.2.1. In that case the image of ρ is contained in diagonal and anti-diagonal matrices. By our hypothesis, we have a non-trivial unipotent element in Im(ρ). Thus raising σ to an appropriate power, we can assume $\sigma \in H$ and $\rho(\sigma)$ is a non-trivial unipotent matrix, since the index of H is prime to p. So ρ is not induced and hence $\rho|_H$ is irreducible. Thus there exist an element in Im$(\rho|_H)$ of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \neq 0$. Now $\det(\rho|_H)$ is of the form $1 + Tf(T)$ and so admits an unique square root. Twisting $\rho|_H$ by $\det(\rho|_H)^{-1/2}$, we see that the image now lies in $SL(2)$. But this is a p-power character and so does not change the image, so by abuse of notation we assume that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in the image of the twisted representation. Now applying Pink's Θ map and projecting onto the $L[\lambda^{-1}]$ subspace we get a non-zero element in $L[\lambda^{-1}]$. Now since $F_p[[T]]$ is a PID, we can identify $L[\lambda^{-1}]$ with a non-zero element, call it $\mathfrak{a}$. Now it's an easy exercise to see the image contains the principal congruence subgroup defined by $\mathfrak{a}$. Now if the image contains a principal congruence subgroup, then the image is open in $SL(2)$ is lemma 2.4 in [27]. □

Remark 5.2.6. i) Skinner-Wiles instead of using condition (iii) impose the condition that ρ is not induced.

ii) They assume that the the image contains a diagonal matrix of infinite order with determinant 1, and this is now known from the works of Hida and others.

iii) If $\mathfrak{p} \subset R^{univ}_{\bar{\rho}}$ is a good prime, then the Galois representation

$\rho : G_{\mathbb{Q}} \to GL_2(R^{univ}_{\bar{\rho}}/\mathfrak{p})$ satisfies conditions (i) and (ii).

iv) Hida assumes that there exists a σ such that $\bar{\rho}(\sigma) = diag(\bar{\alpha}, \bar{\beta})$, with $\bar{\alpha} \neq \bar{\beta}$. Then he claims that one can assume that $\rho(\sigma)$ is diagonal as well. We give a proof of that claim.

Proof. Let $A \in \mathscr{C}_{\mathscr{O}}$ and let ρ be a lift of $\bar{\rho}$ to A. Write $\rho(\sigma) = \begin{pmatrix} \tilde{\alpha} & x \\ y & \tilde{\beta} \end{pmatrix}$. Now the characteristic polynomial of $\rho(\sigma)$ has distinct roots in A, as $(\tilde{\alpha} - \tilde{\beta})^2 + 4xy$ has a non-zero square root in $A^\times$ since $xy \in m_A$ and $\tilde{\alpha} - \tilde{\beta} \in A^\times$ and the roots reduce to $\bar{\alpha}$ and $\bar{\beta}$. Call these roots r_1 and r_2. Let V_A be the A module on which ρ acts. Thus we can use the roots of the characteristic polynomial to decompose V_A into 1-dimensional eigenspaces. Let e_1, e_2 be an A-basis of M lifting the basis $\bar{e}_1, \bar{e}_2$. Thus one writes the eigenvectors $v = e_1 + m_2 e_2$ and $v_2 = e_2 + m_1 e_1$, for unique elements $m_1, m_2 \in m_A$. Thus $\rho(\sigma) = \begin{pmatrix} 1 & m_1 \\ m_2 & 1 \end{pmatrix} \begin{pmatrix} r_1 & \\ & r_2 \end{pmatrix} \begin{pmatrix} 1 & m_1 \\ m_2 & 1 \end{pmatrix}^{-1}$. Conjugating by $\begin{pmatrix} 1 & m_1 \\ m_2 & 1 \end{pmatrix}$ does not change the strict equivalence class of the lift. Thus we can assume that the lift ρ contains a diagonal element.

□

Remark 5.2.7. A direct application of lemma 1.5 in [27] shows that the image of ρ^{univ} is big in $\mathscr{R}^{univ}_{\bar{\rho}}$.

Remark 5.2.8. Condition (iii) is by far the most difficult condition. It relates to non-CM ness of the Hida family. See the papers of Bin Zhao, Hida, Ghate on local indecomposability and non-CM forms.

Chapter 6: Modularity lifting and Wake's conjectures

6.1 Introduction

In this chapter, we will reprove a weaker but a more explicit version of Skinner-Wiles [57] and we can also treat the case where $\psi \neq 1$. The proof uses our calculation of I/I^2 and various isomorphism criteria. To apply the criteria, we relate the congruence module of Wiles to the congruence module of Hida. As a byproduct, under Vandiver's conjecture, we prove that the Hecke algebras considered in Ohta [43] are Gorenstein. Finally we apply our ideas to prove Wake's conjecture for the Hecke algebras considered in the Chapter 4. Since we are only dealing with ordinary Hecke algebras, we will drop *ord* from the superscript.

6.2 Congruence Modules

In this section we briefly recall Hida's formalism of congruence modules and apply the setup to understand the congruences between cusp forms and Eisenstein series. In fact we will show the two concepts of congruence modules, one by Hida and one by Wiles, are the same and we will freely use the results of Hida-Ohta to get results towards modularity lifting and Wake's conjecture.

Setup: We follow the notations in [23]. Let A be an integral noetherian domain of characteristic 0, and let R, S be A-algebras. Let F be the quotient field of A and let $\theta : R \twoheadrightarrow S$ and $\mu : S \twoheadrightarrow A$ be A-algebra homomorphisms. Define $\lambda := \mu \circ \theta$.

We assume the following:

- R, S are reduced and finite flat over A.
- θ and μ induce unique F -algebra decompositions as follows:

$$R \otimes_A F = F \oplus X, \;\; S \otimes_A F = F \oplus Y, \;\; R \otimes_A F = (S \otimes_A F) \oplus Z \quad (**)$$

Let R_X (respectively S_Y, R_Z) be the images of R (respectively S, R) in X (respectively Y, Z)

Definition 6.2.1. Define modules of congruence by

$$C_0(\mu; A) = (A \oplus S_Y)/S, \;\; C_0(\theta; S) = (S \oplus R_Z)/R, \;\; C_0(\lambda; A) = (A \oplus R_X)/R$$

By chasing through some diagrams, one can easily prove this lemma.

Lemma 6.2.2. $C_0(\mu; A) \cong S/(\mathfrak{a}) \cong A/(\mu(\mathfrak{a})) \cong S_Y/\mathfrak{b} \cong S/(\mathfrak{a} \oplus \mathfrak{b})$, *where* $\mathfrak{a} = ker(S \to Y)$ *and* $\mathfrak{b} = ker(\mu)$.

Proof: See lemma 5.2 in [23].

Lemma 6.2.3. $C_0(\mu; A) = S_Y \otimes_S A$, $C_0(\theta; S) = S \otimes_R R_Z$ *and* $C_0(\lambda; A) = R_X \otimes_R A$, *where* A *and* S *are* R*-modules via* λ *and* θ.

Proof. This is lemma 6.3 in [23]. □

Even though $C_0(\theta; S)$ is defined as a module, it is actually a ring. Observe that if A_1 and A_2 are A-algebras, then $\mathrm{Spec}(A_1 \otimes_A A_2) = \mathrm{Spec}(A_1) \times_{\mathrm{Spec}(A)} \mathrm{Spec}(A_2)$., i.e. tensor products correspond to fiber products. Then using previous lemma, we make the following remark:

Remark 6.2.4. $\mathrm{Spec}(C_0(\theta; S))$ is the scheme theoretic intersection of $\mathrm{Spec}(S)$ and $\mathrm{Spec}(R_Z)$, inside $\mathrm{Spec}(R)$.

Consider the setup where $R = R^{univ}_{\bar{\rho}}$, $A = \Lambda = R^{red}$, ϕ is the canonical projection of $R^{univ}_{\bar{\rho}} \twoheadrightarrow R^{red}$. Note that $R^{univ}_{\bar{\rho}}$ is reduced. If a prime $\mathfrak{p}$ is in the support of $C_0(\phi, A)$, then by the discussions above it is clear $\mathfrak{p} \supset I$, where I is the ideal of reducibility which is the kernel of ϕ. The upshot is if a prime is in the support of the congruence module, then the Galois representation is reducible, i.e. it measures the congruences between irreducible and reducible Galois representations. Thus if $\mathfrak{q} \subset R^{univ}_{\bar{\rho}}$ is a good prime, we get that $\mathfrak{q}$ is not in the support of the congruence ideal.

In fact one can define higher congruence modules C_i for $i > 0$.

Definition 6.2.5. $C_i(\mu; A) = Tor_i^S(A, A)$, $C_i(\lambda; A) = Tor_i^R(A, A)$,
$C_i(\theta; S) = Tor_i^R(S, S)$, where we view these modules as R-modules via the maps λ and θ as previous lemma.

Then another diagram chasing gives the following easy lemma:

Lemma 6.2.6. 1) $C_1(\mu; A) = \Omega_{S/A} \otimes_{S,\mu} A$. *If S is an universal deformation ring, then this module is nothing but the dual of an adjoint Selmer group as discussed and calculated in Chapter* 3.
2) $C_1(\theta; S) = I/I^2$ *where* $I = ker(R \twoheadrightarrow S)$. *If R, S are as in the previous discussion, I is the ideal of reducibility.*

Proof. Since we will not be needing them, we refer the reader to see page 276 in [24] and various references in the book. But nonetheless, this description gives another way to think about the invariants that we already defined and calculated. □

Since throughout this section, we will be using Ohta's results, we would like to state the setup in Ohta. To begin the comparison between various congruence modules, let us recall the following definition/setup in Ohta.

Let

$$0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0 \tag{6.1}$$

be an exact sequence of finite flat reduced R-modules. We consider C as a B-module via the map π. Suppose we are given a B-module section over Q =Frac(R), i.e.

$$0 \leftarrow A \otimes Q \xleftarrow{t} B \otimes Q \xleftarrow{\sigma} C \otimes Q \leftarrow 0 \tag{6.2}$$

such that

$$t \circ (i \otimes 1_Q) = 1_{A \otimes Q} \text{ and } (\pi \otimes 1_Q) \circ s = 1_{C \otimes L} \tag{6.3}$$

Then one defines the congruence module as

$$\mathscr{C}_{Ohta} = C/\pi(B \cap \sigma(C)) \cong t(B)/A$$

For more details about congruence modules and Ohta's setup, we refer the reader to section 1 in [43]. Note that the two definitions are the same. Applying lemma 6.2.2, to $C_0(\pi, C)$ in Ohta's setup, we see that

$$B \otimes Q = (C \otimes Q) \oplus (A \otimes Q)$$

and $C_0(\pi, C) = (\text{Im}(B \to A \otimes Q))/\ker(\pi)$, which is exactly $t(B)/A$ as desired.

In the introduction of [43], Ohta introduces this module as the module that measures the failure of this section to be defined over R.

Let the setup be as before. Wiles in [69] defines a congruence module via:

$$\mathscr{C}_{Wiles} = C/\pi(\text{Ann}_B((\ker(\pi))).$$

It is very easy to see that this module measures the failure of the splitting of the exact

sequence 6.1. The next lemma shows that these modules are in fact the same.

Lemma 6.2.7. $B \cap \sigma(C) = Ann_B(A)$.

Proof. Let $x \in Ann_B(A)$, then $x \cdot i(a) = 0$. Applying t to it, we get, $t(x) \cdot a = 0$. Since A is flat over R, by clearing denominators, we can assume $t(x) \in A$. So $i(t(x)) \in Ann_B(A)$. But $i(t(x)) \in ker(\pi)$. So $i(t(x)) \in ker(\pi) \cap Ann_B(A)$.

Claim 1: $ker(\pi) \cap Ann_B(A) = 0$

Let $b \in \ker(\pi) \cap \mathrm{Ann}_B(A) = 0$. Since $b \in \ker(\pi)$, then $b \in i(A)$. Now $b \cdot b = 0$, since $b \in \mathrm{Ann}_B(A)$, but B is reduced so $b = 0$.

This claim implies that $t(x) = 0$, therefore $x \in \sigma(C)$, so $\mathrm{Ann}_B(A) \subset B \cap \sigma(C)$.

Conversely, let $x \in B \cap \sigma(C)$, now $\pi(x \cdot i(a)) = 0$ and $t(x \cdot i(a)) = t(x) \cdot a = 0$, as x is in the image of C. So $x \cdot i(a) \in ker(\pi) \cap ker(t)$.

Claim 2: $ker(\pi) \cap ker(t) = 0$.

Proof: Let $\alpha \in ker(\pi) \cap ker(t)$, then $\alpha = i(a)$. Since $t(\alpha) = t(i(a)) = a = 0$, this shows $\alpha = 0$ and thus proves the lemma. □

It is useful to know all the above viewpoints when dealing with congruence modules.

Remark 6.2.8. In the original work of Wiles in [69], $\mathscr{C}_{Wiles}$ is controlled by the special value of some adjoint L-function coming from the work of Doi-Hida which was further axiomatized by Diamond-Flach-Guo. But $\mathscr{C}_{Ohta}$ is controlled by the Kubota-Leopoldt p-adic L-function as will be explained later. The motivation and evidence for such a strategy for comparing the two modules comes from the work of Mazur-Wiles and Fukaya-Kato-Sharifi that the cuspidal Hecke algebra mod the Eisenstein ideal is controlled by the Kubota-Leopoldt p-adic L-function. In particular cases, where the Eisenstein ideal is "nice", one can get hold of the full Hecke algebra.

Finally to finish the discussion about our general setup, let us prove the following easy proposition:

Proposition 6.2.9. *Consider a commutative diagram of rings:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ C & \xrightarrow{\pi} & D \end{array}$$

Suppose all the maps are surjective. Then the following are equivalent.

i. g *induces an isomorphism* $ker(f) \cong ker(\pi)$

ii. f *induces an isomorphism* $ker(g) \cong ker(h)$.

iii. the canonical map from $A \to B \times_D C$ *is an isomorphism.*

Proof. We show that *i* and *iii* are equivalent. Let $(b,c) \in B \times_D C$, then pick any lift of b in A, call it a. Now $g(a)$ and c have the same image in D, thus $g(a) - c \in \ker(\pi)$. Thus there is an unique element in $\ker f$ which maps to this element via g. Call that element a'. Then $a - a'$ maps to (b,c). Thus the map is surjective. To show injectivity, if there exists an a mapping to 0 in both B and C, then $a \in \ker(f)$. But g is an isomorphism from $\ker(f)$ to $\ker(\pi)$. Thus a must be 0. Conversely suppose A is the fiber product of B and C over D, then A can be written as $\{(b,c) \in B \times C : h(b) = \pi(c)\}$. So $\ker(f) = \{(0,c) \in B \times C : \pi(c) = 0\}$ =$\ker(\pi)$. The proof of the other equivalences are similar. □

Since we want apply our results towards Wake's conjectures in [63], we would like to have a better understanding about the prime ideals in fiber products of rings. The following proposition gives a complete description of all prime ideals in fiber products.

Proposition 6.2.10. *Let the setup be as in the previous proposition, then*

$$Spec(A) = U \cup V \cup W$$

where

$$U := \{f^{-1}(\mathfrak{p}) : \mathfrak{p} \in Spec(B) \text{ and } ker(h) \not\subset \mathfrak{p}\}$$

$$V := \{g^{-1}(\mathfrak{p}) : \mathfrak{p} \in Spec(C) \text{ and } ker(\pi) \not\subset \mathfrak{p}\}$$

$$W := \{\phi^{-1}(\mathfrak{p}) : \mathfrak{p} \in Spec(D)\} \text{ where } \phi := \pi \circ g = h \circ f\}$$

Proof. If $\mathfrak{p} \in W$, then $\mathfrak{p}$ must contain $\ker(f)$ and $\ker(g)$. This is clear since $\ker(f) \cong \ker(\pi)$ and $\ker(g) \cong \ker(h)$. Conversely any prime ideal in A containing both $\ker(\pi)$ and $\ker(h)$, must lie in W as the image of this prime ideal under the surjective homomorphism ϕ is a prime ideal. In fact W is a closed subset of $\mathrm{Spec}(A)$. Now, let us pick an arbitrary prime ideal $\mathfrak{q}$ in A. We want to show that $\mathfrak{q}$ lies in either U or V. Now without loss of generality assume $\mathfrak{q}$ do not contain $\ker(f)$. Then pick an element $\alpha \in \ker(f) \setminus \mathfrak{q}$. Now localizing at α, we get a commutative diagram

$$\begin{array}{ccc} A_\alpha & \xrightarrow{f} & B \otimes_A A_\alpha \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ C \otimes_A A_\alpha & \xrightarrow{\pi} & D \otimes_A A_\alpha \end{array}$$

Now A_α is flat over A and we can think of the above diagram as a fiber product. Now note that $B \otimes_A A_\alpha = 0 = D \otimes_A A_\alpha$. Thus (by abuse of notation) g is an isomorphism from A_α to $C \otimes_A A_\alpha$. Thus there exists an unique prime $\mathfrak{p}$ that maps to $\mathfrak{q}$, under g^{-1}. Similarly for the case where $\mathfrak{p}$ does not contain $\ker(g)$.

Finally we show that there does not exist any prime $\mathfrak{p}$ in A such that $\mathfrak{p} \not\supseteq \ker(f)$ and $\mathfrak{p} \not\supseteq \ker(g)$. Note that $A_\mathfrak{p} = 0$ by using the above argument and choosing elements from $\ker(f) \setminus \mathfrak{p}$ and $\ker(g) \setminus \mathfrak{p}$. Thus we see that U and V are disjoint subsets. The argument also shows the open set U is isomorphic to the the open subset of Spec C defined by $\ker(\pi)$. □

Now we will apply our above setup in the case of Hecke algebras. This work is already

done by Ohta in [43] and Lafferty in [33]. We will briefly recall their work in our squarefree level case N. We warn the reader that the notation in Hida and that of Ohta-Lafferty and Wiles differs by a twist of the p-adic cyclotomic character.

Let θ and ψ be Dirichlet characters mod u, v with $uv \mid Np$, v prime to p, and $\theta\psi(-1) = 1$. We shall also extend our ground field to K, some extension of $\mathbb{Q}_p$ which contains all the values of θ and ψ. Let $\mathscr{O}$ be its ring of integers and ϖ be its uniformizer. Define $U_r := 1 + p^r\mathbb{Z}_p$ and fix u a topological generator of U_1. Then under the identification: $\mathscr{O}[U_1] = \mathscr{O}[[T]], u \leftrightarrow 1+T$. The Eisenstein series we are interested in are of the following form :

$$\mathscr{E}(\theta,\psi;c) := \delta(\psi)G(T,\theta\omega^2) + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<t\mid n\\ p\nmid t}}\theta(t)\psi(n/t)A_t(T)\right)q^{cn} \tag{6.4}$$

Here, c is a positive divisor of Np/uv, prime to p,

$$\delta(\psi) := \begin{cases} 1/2 & \text{if } \psi = \text{trivial} \\ 0 & \text{otherwise} \end{cases}$$

$$A_t(T) := t(1+T)^{s(t)} = t\iota(\langle t\rangle), \text{ if } \langle t\rangle = u^{s(t)} \tag{6.5}$$

and

$$G(\varepsilon(u)u^s - 1, \theta\omega^2) = L_p(-1-s, \theta\omega^2\varepsilon) \tag{6.6}$$

for every character ε of finite order on U_1, which we can identify with a Dirichlet character of the second kind. G lies in Λ unless $\theta\omega^2 = 1$, in which case it has a simple pole at $s = 1$. Finally we set

$$\mathscr{E}(\theta,\psi) := \mathscr{E}(\theta,\psi;1) \tag{6.7}$$

Then by the work of Hida [22], we know that $\mathscr{E}(\theta,\psi)$ generates all Eisenstein series. For

the rest of the thesis, we will assume that $(\theta, \psi) \neq (\omega^{-2}, 1)$.

Lemma 6.2.11. *$\mathscr{E}(\theta, \psi)$ is an eigenvector for T_l for $l \nmid N$ with eigenvalue $\theta(l)\chi(l) + \psi(l)$ and for U_p with eigenvalue $\psi(p)$.*

Remark 6.2.12. But $\mathscr{E}(\theta, \psi)$ is not an eigenvector for all U_l if $uv \neq N$. If $l|N/uv$, then if one writes down the double coset operator for T_l and works out explicitly the action of T_l on $\mathscr{E}(\theta, \psi)$, one gets that T_l acts via the eigenvalue $\theta(l)\chi(l) + \psi(l)$. But one does not get any such formula for the action of U_l on $\mathscr{E}(\theta, \psi)$. But since $l|N$, we have the Hecke operator U_l and not T_l. However, if $l|uv$, then $\mathscr{E}(\theta, \psi)$ is indeed an eigenvector for U_l with the appropriate eigenvalue.

The method of l-stabilization of a newform f for level N produces two newforms of level Nl by the following formulae:

$$f_1(z) = f(z) - \alpha f(lz) \tag{6.8}$$

and

$$f_2(z) = f(z) - \beta f(lz) \tag{6.9}$$

where α and β are roots of the characteristic polynomial of U_l acting on the 2-dimensional space spanned by $f(z)$ and $f(lz)$. In particular, the L-function of f_1 and f_2 is the L-function of f with the Euler factors $(1 - \alpha l^{-z})^{-1}$ and $(1 - \beta l^{-z})^{-1}$ respectively removed.
The method of l-stabilization gives us a way to remedy our problem. We diagonalize the action of U_l on the 2-dimensional space spanned by $\langle \mathscr{E}(\theta, \psi)(z), \mathscr{E}(\theta, \psi)(lz) \rangle$ and this action has no eigenvalues $\psi(l)$ and $\theta(l)\chi(l)$. We choose our l-stabilized Eisenstein series with the eigenvalue at l to be $\psi(l)$. Or in other words, this forces θ to be an imprimitive character. We denote $\tilde{\mathscr{E}}(\theta, \psi)$ this new stabilized Eisenstein series. For ease of the reader, we write down its eigenvalues.

Lemma 6.2.13. *The eigenvalues of $\tilde{\mathscr{E}}(\theta,\psi)$ for T_l, $l\nmid Np$, U_l for $l|N$ and U_p are respectively*

- $\theta(l)\chi(l)+\psi(l)$ *for* $l\nmid N$ *or* $l|uv$
- $\psi(l)$ *for* $l|N/(uv)$
- $\psi(p)$ *for* $l=p$

Proof. It follows from lemma 6.2.11 and the previous remark. □

Remark 6.2.14. In $\tilde{\mathscr{E}}(\theta,\psi)$, θ is generally chosen as the imprimitive character, whereas ψ is always a primitive character. We will write θ^{prim} to denote the primitive character that induces θ.

Remark 6.2.15. This method of level raising is necessary to find congruences between Eisenstein series and cusp forms. This cusp form was constructed in proposition 6.2.35.

Definition 6.2.16. We define the Eisenstein ideal to be the ideal generated by

$$\langle T_l-\theta(l)\chi(l)-\psi(l), U_l-\theta(l)\chi(l) \text{ for } l|v, U_l-\psi(l) \text{ for } l|N/u, U_p-\psi(p)\rangle$$

and let $\mathfrak{m}_{\theta,\psi}$ be the maximal ideal containing the Eisenstein ideal. We will refer to $\mathfrak{m}_{\theta,\psi}$ as the maximal Eisenstein ideal and all our Hecke algebras will be localized at this maximal ideal. To simplify notation, we will just use m to denote this maximal ideal.

Now we would like to write down some conditions such that $\tilde{\mathscr{E}}(\theta,\psi)$ is the unique Eisenstein series in the localized Hecke algebra with the given system of eigenvalues mod the maximal ideal.

Lemma 6.2.17. *Let $\mathscr{E}(\theta_1,\psi_1)\in M_\Lambda$. Then the eigenvalues of $T(l)$ for $\mathscr{E}(\theta_1,\psi_1)$ and $\tilde{\mathscr{E}}(\theta,\psi)$ are congruent modulo (ϖ,T) for all $l\nmid Np$ iff one of the following conditions hold:*

$\psi_1 \equiv \psi_2$ *and* $\theta_1\omega \equiv \theta_2\omega$ *mod*(ϖ)

$\psi_1 \equiv \omega\theta_2$ *and* $\psi_2 \equiv \theta_1\omega$ *mod*(ϖ)

Proof. This is lemma 1.4.9 in [43] and the proof is standard and follows from independence of characters. □

The following proposition is a strengthening of the above lemma.

Proposition 6.2.18. *Assume* **Neben** *then* $\tilde{\mathscr{E}}^{\varphi}(\theta,\psi)$ *is the unique Eisenstein series in our localized Hecke algebra with the given system of eigenvalues mod the maximal ideal.*

Proof. By linear independence of characters, we get either

- $\theta \equiv \theta_1 \pmod{p}$ and $\psi \equiv \psi_1 \pmod{p}$ or
- $\psi \equiv \omega\theta_1$ and $\psi_2 \equiv \theta\omega$

But **Neben** forces the congruence into an equality as we do not have any non-trivial p-power characters congruent to 1 mod p.
We now show that the second case can not happen. The same argument with **Neben** shows that

$$\psi = \theta_1\omega \text{ and } \psi_1 = \theta\omega$$

As the U_p eigenvalues are also congruent, we get $\psi(p) \equiv \psi_1(p) \pmod{\omega}$. Since the conductors and orders of ψ_1 and ψ are prime to p, we get $\psi(p) = \psi_1(p)$. Combining these facts just like in lemma 1.4.9 in [43], we get $\theta_i|_{(\mathbb{Z}/p)^*} = \omega^{-1}$ and $\theta\psi\omega^{-1} = 1$, but this forces the conductor of θ to be divisible by p, which contradicts our assumption that $p \nmid N$. □

Recall the Residue map of Ohta in [43] which is essentially the constant term map which sends an Eisenstein series to the formal sum of (cusps)· residue at each cusp.

Theorem 6.2.19. *(Lafferty-Ohta) Suppose $\mathscr{E}(\theta,\psi;c) \in M_\Lambda$, then*

$$Res(\mathscr{E}(\theta,\psi;c)) = A_{\theta,\psi}.\mathfrak{c}_{\theta,\psi;c} \tag{6.10}$$

and $\mathfrak{c}_{\theta,\psi;c} \notin m\Lambda$, where

$$A_{\theta,\psi} := \left(\prod_{\substack{l|N \\ l\nmid cond(\theta\psi^{-1})}} ((1+X)^{s(l)} - \psi\theta^{-1}\omega^{-2}(l)l^{-2}) \right) G(T,\theta\psi^{-1}\omega^2) \tag{6.11}$$

where $G(T,\theta\psi^{-1}\omega^2)$ is a twist of the Kubota-Leopoldt p-adic L-function as follows:

$$G(\varepsilon(u)u^s - 1, \theta\psi^{-1}\omega^2) = L_p(-1-s, \theta\psi^{-1}\omega^2\varepsilon) \tag{6.12}$$

where ε is a Dirichlet character of the second kind.

Proof. This is theorem 4.2 in [33]. □

In fact Ohta constructs the following exact sequence:

Theorem 6.2.20.

$$0 \to S_\Lambda \to M_\Lambda \xrightarrow{Res} C_\Lambda \to 0$$

and the sequence canonically splits over Frac(Λ) with the Hecke-equivariant splitting given explicitly by $\mathfrak{c}_{\theta,\psi;c} \to \frac{\mathscr{E}(\theta,\psi;c)}{A_{\theta,\psi}}$.

Proof. This is the exact sequence 2.4.6 and Theorem 2.4.10 in [43]. □

Recall the following proposition from Lafferty.

Proposition 6.2.21. *$\Lambda(\mathfrak{c}_{\theta,\psi;c})$ is a free Λ module.*

Proof. This is proposition 3.3.2 in [33]. □

So now we can generalize Ohta's exact sequence using the above results. Our strategy is exactly the same as in Ohta's in [43]. We will start with the maximal ideal in the Hecke algebra and Proposition 6.2.18 allows us to isolate an unique Eisenstein series $\tilde{\mathscr{E}}(\theta,\psi)$ and then localizing Ohta's exact sequence immediately gives us:

Proposition 6.2.22. *Assume either one of two the following conditions are satisfied:*
1) $p \nmid \phi(N)$ *or*
2) **Neben**
then we have a fundamental exact sequence

$$0 \to S_m \to M_m \to C_m \to 0,$$

where C_m *is a free* Λ*-module of rank* 1 *with generator* $\mathfrak{c}_{\theta,\psi}$ *and* $\mathfrak{c}_{\theta,\psi} \notin m\Lambda$*. The sequence canonically splits over Frac*(Λ) *and the congruence module is given by* $\Lambda/A_{\theta,\psi}$*.*

Proof. This is the sequence when we get after localizing the exact sequence Theorem 6.2.19 at m. This is the also the exact sequence 3.1.4 in [43], the only difference being our proofs showing the existence of a unique Eisenstein series with the given system of mod p eigenvalues. □

We would like to apply the formalism of congruence modules to the context of Hecke algebras. For a slightly more general formalism, we refer the reader to page 253 in [43]. Recall from theorem 4.2.4 we have the following

- $\mathrm{Hom}_\Lambda(M_m,\Lambda) = \mathfrak{H}_m$
- $\mathrm{Hom}_\Lambda(S_m,\Lambda) = \mathfrak{h}_m$

Recall that $\mathfrak{H}_m$ and $\mathfrak{h}_m$ are reduced, flat and finite over Λ. Tensoring the exact sequence in

Proposition 6.2.22 by $\mathrm{Frac}(\Lambda)$, and taking $\mathrm{Hom}(-,\mathrm{Frac}(\Lambda))$, we get

$$\mathfrak{H}_m \otimes \mathrm{Frac}(\Lambda) = (\mathfrak{h}_m \otimes \mathrm{Frac}(\Lambda)) \oplus (C_m^\vee \otimes \mathrm{Frac}(\Lambda)) \tag{6.13}$$

Let π_1 and π_2 be the projections of $\mathfrak{H}_m^{ord}$ in the respective components. Thus we get the two exact sequences

$$0 \to \mathfrak{a} \to \mathfrak{H}_m \xrightarrow{\pi_1} \mathfrak{h}_m \to 0 \tag{6.14}$$

$$0 \to I(\theta,\psi)_m \to \mathfrak{H}_m \xrightarrow{\pi_2} \Lambda \to 0 \tag{6.15}$$

The second exact sequence (6.15) comes from identifying C_m with Λ by choosing a basis and $\mathfrak{a}$ and $I(\theta,\psi)_m$ are ideals in $\mathfrak{H}_m$ defined to make the above sequences exact.

Remark 6.2.23. $I(\theta,\psi)_m$ is better known in the literature as $\mathrm{Ann}_{\mathfrak{H}_m}(\mathscr{E}(\theta,\psi))$. One can also see that π_1 is the canonical surjection induced by the inclusion of $S_m \hookrightarrow M_m$. Unraveling the definitions, one can see that π_2 is given by $T_l(a_1(\tilde{\mathscr{E}}(\theta,\psi)))$.

The congruence module attached to the exact sequence (6.14) is generated by a single element as a Λ-module by lemma 1.19 and then lemma 1.1.12 in [43] shows that the congruence module attached to that exact sequence is isomorphic to the congruence module from Proposition 6.2.22 and is equal to $\Lambda/A_{\theta,\psi}$. In fact Ohta in page 254 in [43] shows the congruence module attached to the exact sequence (6.15) is also $\Lambda/A_{\theta,\psi}$ as $\mathfrak{H}_m$ modules. For a more detailed description of the congruence modules attached to the Hecke algebras, we refer the reader to section 3.2, pages 253-255 in [43]. Alternatively one can show this directly using the definitions and the lemmas at the beginning of this section. Now using the second exact sequence we can define $\mathscr{C}_{Wiles} = \Lambda/\pi_2(\mathrm{Ann}_{\mathfrak{H}_m}(\ker(\pi_2)))$

Proposition 6.2.24. $\mathscr{C}_{Wiles} = \Lambda/(A_{\theta,\psi})$.

Proof. We have shown in Lemma 6.2.7, $\mathscr{C}_{Wiles} = \mathscr{C}_{Ohta}$. And the rest follows from the previous paragraph. □

Recall the main result of Mazur-Wiles in [39]:

Theorem 6.2.25. *Let $\mathfrak{h}$ be the cuspidal Hecke algebra and denote by $I_{\theta,\psi}$ the image of $I(\theta,\psi)$ under the canonical projection $\mathfrak{H} \twoheadrightarrow \mathfrak{h}$. Then*

$$\mathfrak{h}_m/(I_{\theta,\psi})_m \cong \Lambda/(A_{\theta,\psi}).$$

In view of our abstract algebra and the deep result of Mazur-Wiles, we immediately obtain:

Proposition 6.2.26. $\mathfrak{H}_m = \mathfrak{h}_m \times_{\Lambda/(A_{\theta,\psi})} \Lambda$.

Proof. We already know from (6.13), $\mathfrak{H}_m \otimes Q(\Lambda) = \mathfrak{h}_m \otimes Q(\Lambda) \oplus Q(\Lambda)$ and using the exact sequences (6.14) and (6.15) above we have a commutative diagram:

$$\begin{array}{ccc} \mathfrak{H}_m & \xrightarrow{pr_1} & \mathfrak{h}_m \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ \Lambda & \xrightarrow{\pi_2} & \Lambda/(A_{\theta,\psi}) \end{array}$$

In view of the proposition 6.2.9 we have to show $\ker(pr_2) \cong \ker(\pi_1)$. Now, $\ker(pr_2) = I(\theta,\psi)_m$ and the $\ker(\pi_1) = (I_{\theta,\psi})_m$. And $(I_{\theta,\psi})_m$ is defined as the image of $I(\theta,\psi)_m$ under the projection map. So the hypotheses of the proposition 6.2.9 are satisfied. □

Recall the following definition.

Definition 6.2.27. Let R be a n-dimensional local Noetherian ring. Then R is Gorenstein if $\mathrm{Ext}^i_R(\mathbb{F},R) = 0$ for all $i < n$ and $\mathrm{Ext}^n_R(\mathbb{F},R) = \mathbb{F}$.

Note that this definition takes a particularly simple form if R has dimension 0. In that case R is Gorenstein iff $\mathrm{Hom}_R(\mathbb{F},R) \cong \mathbb{F}$ as $\mathbb{F}$-vector spaces. Gorensteinness of Hecke algebras is important because in that case the spaces of modular forms are free of rank 1 over the Hecke algebras and one can then realize Hida's big Galois representation inside the cohomology of towers of modular curves.

Sometimes when checking whether the big Hecke algebra is Gorenstein, it is convenient to check at a finite level or weight. In fact restricting ourselves to the weight 2 Hecke algebra, we get this corollary. Let λ be an uniformizer of $\mathscr{O}$. Then

Corollary 6.2.28. *Assume $\lambda | L_{p,S}(-1,\theta\psi^{-1}\omega^2)$ but $\lambda^2 \nmid L_{p,S}(-1,\theta\psi^{-1}\omega^2)$, then $(\mathfrak{H}_2)_m$ is Gorenstein iff $(\mathfrak{h}_2)_m \cong \mathscr{O}$ or some ramified DVR over $\mathscr{O}$.*

Proof. Note that from proposition 6.2.26 we have a fiber product diagram:

$$\begin{array}{ccc} (\mathfrak{H}_2)_m & \xrightarrow{pr_1} & (\mathfrak{h}_2)_m \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ \mathscr{O} & \xrightarrow{\pi_2} & \mathscr{O}/(L_{p,S}(-1,\theta\omega^2\psi^{-1})) \end{array}$$

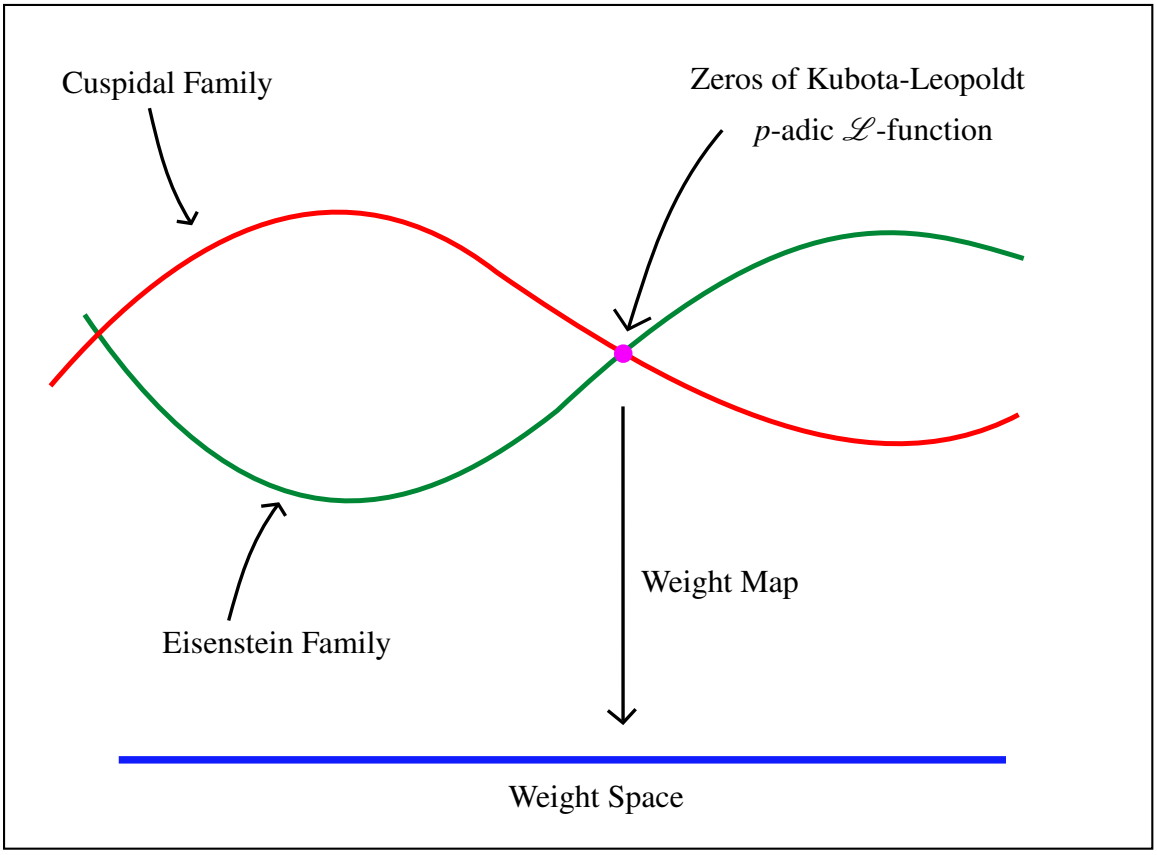
The existence of such a diagram was clear in the works on Mazur-Wiles, Kurihara and Harder-Pink. Our fiber product diagram also appears in [43], section 2.4, the exact sequence 2.4.1. The fact that the specialization to the weight 2 using (4.1) corresponds to $L_{p,S}(-1,\theta\omega^2\psi^{-1})$ is clear from the calculations in [43], section 2.5, particularly the formula in 2.5.3. The rest of the proof is surprisingly a commutative algebra result from [58], corollary 2.7 which says $R \times_{\mathbb{F}} S$ is Gorenstein iff R and S are DVRs. The corollary follows directly from that statement. □

Remark 6.2.29. This result is an analog of a theorem of Mazur in [36]. In fact we can say more here: let $k \equiv 2 \pmod{p-1}$, assume $p | L_{p,S}(1-k,\theta\psi^{-1}\omega^2)$ but $p^2 \nmid L_{p,S}(1-k,\theta\psi^{-1}\omega^2)$, then $(\mathfrak{H}_k)_m$ is Gorenstein iff $(\mathfrak{h}_k)_m \cong \mathscr{O}$ or some ramified DVR over $\mathscr{O}$. This

is analogous to some results of P. Wake and C. Erickson in this higher weight case.

Remark 6.2.30. Calegari and Emerton in [8] used this above description of Hecke algebra in their case to compute the ramification of the cuspidal Hecke algebra by using deformation theory arguments. More explicitly, if e is the ramification index of the cuspidal Hecke algebra over $\mathscr{O}$, then e is given by a non-trivial deformation to $\mathbb{F}[X]/X^{e+1}$. However, if our tame level N is prime and $p||N-1$, our **Hypothesis 1** forces the cuspidal Hecke algebra to be $\mathscr{O}$ by theorem 1.2 in [8].

The above corollary can be summarized by the following picture:



This is the picture of our space of modular forms. The weight map is etale over classical points. We do not know in general the nature of these intersections. It is widely believed that the zeros are simple zeros but we do not know how to prove it.

Remark 6.2.31. Given this description of the Hecke algebra, it is very easy to see that $C_{Wiles} = \Lambda/(A_{\theta,\psi})$. In fact $\ker(\mathrm{pr}_2) = I_{\theta,\psi} \times 0$ and since $\mathrm{Ann}_{\mathfrak{h}_m} I_{\theta,\psi} = 0$, we immediately get $\mathrm{Ann}_{\mathfrak{H}_m} \ker(\mathrm{pr}_2) = A_{\theta,\psi} \times 0$.

We give some further properties our Hecke algebras in the form of a couple of lemmas which will be used in the next section.

Lemma 6.2.32. *$Ann_{\mathfrak{H}_m}(I(\theta,\psi)) = ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m)$*

Proof. Let $x \in \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi))$, then localizing the fiber product diagram in Proposition 6.2.9, we get

$$\begin{array}{ccc} (\mathfrak{H}_m)_x & \xrightarrow{pr_1} & \mathfrak{h}_m \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ \Lambda \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x & \xrightarrow{\pi_2} & \Lambda/(A_{\theta,\psi}) \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x \end{array}$$

Since $I(\theta,\psi)$ is the kernel of pr_2, so localizing at x, (by abuse of notation) pr_2 is an isomorphism. Since the above is a fiber product diagram, this forces $\mathfrak{h}_m \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x = 0 = (\mathfrak{h}_m)_{\bar{x}}$, where $\bar{x}$ is the image of x inside $\mathfrak{h}_m$. Since $\mathfrak{h}_m$ is reduced, this forces $\bar{x} = 0$, as desired. Conversely, let $x \in \ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m)$, then localizing the fiber product diagram as before, we get $(\mathfrak{H}_m)_x \cong \Lambda_{\bar{x}}$, where $\bar{x}$ is the image of x in Λ. This implies $I(\theta,\psi)_x = 0$. Since $\mathfrak{H}_m$ is reduced this shows that x kills $I(\theta,\psi)$. This proves the claim. □

Lemma 6.2.33. *$pr_1|_{I(\theta,\psi)}$ is injective.*

Proof. If $pr_1(x) = 0$, then $x \in \ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m) \cap I(\theta,\psi)$. But $\mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi)) = \ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m)$ by lemma 6.2.32, thus $x \cdot x = 0$, but $\mathfrak{H}_m$ is reduced, so $x = 0$. □

The proof of this theorem also proves a familiar statement about cuspidal Hecke algebras.

Corollary 6.2.34. *$I_{\theta,\psi}$ is a faithful $\mathfrak{h}_m$ module.*

Proof. Note that we have a commutative square:

$$\begin{array}{ccc} I(\theta,\psi) & \hookrightarrow & \mathfrak{H}_m \\ \cong\downarrow & & \downarrow\twoheadrightarrow \\ I_{\theta,\psi} & \hookrightarrow & \mathfrak{h}_m \end{array}$$

Let $y \in \mathrm{Ann}_{\mathfrak{h}_m}(I_{\theta,\psi})$, then we can lift y to some $x \in \mathfrak{H}_m$. If $x \in \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi))$, then the previous theorem shows $y = 0$ and so we are done. So assume $x \notin \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi))$, then localizing the fiber product diagram at x, we get:

$$\begin{array}{ccc} (\mathfrak{H}_m)_x & \xrightarrow{\quad pr_1 \quad} & (\mathfrak{h}_m)_y \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ \Lambda \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x & \xrightarrow{\pi_2} & \Lambda/(A_{\theta,\psi}) \otimes_{\mathfrak{H}_m} (\mathfrak{H}_m)_x \end{array}$$

where π_1 is an isomorphism but pr_2 is not, which is a contradiction. □

To finish off this section, we would like to show that the $\overline{\rho}$ considered in Chapter 3 is reduction mod p of some cusp form. Recall $\bar{\rho} = \begin{pmatrix} \theta\omega & * \\ & \psi \end{pmatrix}$ where ψ is unramified at p, $\theta\psi(-1) = 1$ and $*$ is ramified at p and all primes where θ and ψ are unramified.

Proposition 6.2.35. *Assume $A_{\theta,\psi}$ is not an unit. Then there exists a cusp form f such that $\overline{\rho}_f \cong \overline{\rho}$.*

Proof. S^{ord} is free of finite rank over Λ and let $\{f_1, ...f_k\}$ be a Λ-basis. By Hida duality (theorem 4.2.4), there exist a dual Λ basis for $\mathfrak{h}$, i.e.

$$a_1(f_i|h_j) = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i = j \end{cases}$$

Let H_i be arbitrary lifts of h_i under the canonical surjection $\mathfrak{H} \twoheadrightarrow \mathfrak{h}$. Since the residue map

is surjective, there exists a modular form g such that $\mathrm{Res}(g) = \mathfrak{c}_{\theta,\psi}$. Now define

$$g' := g - \sum a_1(g|h_i) f_i.$$

Since $\mathrm{Res}(A_{\theta,\psi} g' - \mathscr{E}_{\theta,\psi}) = 0$, it follows that $A_{\theta,\psi} g' - \mathscr{E}_{\theta,\psi} = -F$ is a cusp form. Obviously $F \equiv \mathscr{E}_{\theta,\psi} \bmod A_{\theta,\psi}$. Thus F is a mod $A_{\theta,\psi}$ eigenform with the same eigenvalues as $\mathscr{E}_{\theta,\psi}$. We would like to apply Deligne-Serre lifting lemma to lift these mod p system of eigenvalues to characteristic 0. However to apply the lifting lemma, we have to work with a DVR. To remedy the problem, we look at the specialization of F and $\mathscr{E}_{\theta,\psi}$ at weight 2, since the prime ideal corresponding to arithmetic specializations is a height 1 prime. Then the constant term of $E^{(2)}_{\theta,\psi}$ vanishes mod p. Thus we get $F^{(2)} \cong E^{(2)}_{\theta,\psi} \bmod p$. Now by the Deligne-Serre lemma, we can lift this mod p-eigenform into our desired eigenform. $\square$

6.3 Modularity lifting and Wake's conjecture

Now let us recall Wake's conjecture in [63].

Conjecture 6.3.1. (Wake): Let $I_{\mathfrak{h}}$ and $I_{\mathfrak{H}}$ be the Eisenstein ideals in $\mathfrak{h}^{ord}$ and $\mathfrak{H}^{ord}$. Then for all height 1 prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ such that $I_{\mathfrak{h}} \subset \mathfrak{p}$ and $I_{\mathfrak{H}} \subset \mathfrak{q}$, $\mathfrak{h}^{ord}_{\mathfrak{p}}$ and $\mathfrak{H}^{ord}_{\mathfrak{q}}$ are Gorenstein.

Recall proposition 6.2.10 gives us a complete description of all the prime ideals in $\mathfrak{H}^{ord}_m$. Since in this thesis, we are only concerned with ordinary Hecke algebras, we will drop *ord* from the superscript.

Let $\mathfrak{p}$ be a height 1 prime of $\mathfrak{H}_m$ such that $I(\theta,\psi) \subset \mathfrak{p}$. Let $\mathfrak{p}_1 := pr_1(\mathfrak{p})$. Then $\mathfrak{p}_1 \supset I_{\theta,\psi}$, i.e. $\mathfrak{p} \in W$ in our terminology, i.e. in that case $\mathfrak{p}$ is the inverse image of some prime divisor of $A_{\theta,\psi} \in \Lambda$.

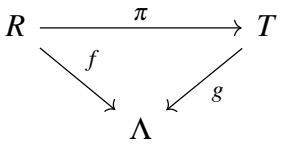
Conversely given a height 1 prime $\mathfrak{p}$ in $\mathfrak{h}_m$ such that $I_{\theta,\psi} \subset \mathfrak{p}$. Let $\mathfrak{p}' := pr_1^{-1}(\mathfrak{p})$. Then $\mathfrak{p}'$ is either in V or W. If it is V, then it is not in the support of the congruence module, then Theorem 4.1 in [26] shows that $\mathfrak{h}_{\mathfrak{p}'}$ and $\mathfrak{H}_{\mathfrak{p}}$ are Gorenstein.

Now let us recall some facts about Fitting ideals in the appendix of [39]. Let M be a R module. Then

- $\mathrm{Fit}_R(M) \subset \mathrm{Ann}_R(M)$
- If M is generated by n elements, then $\mathrm{Ann}_R(M)^n \subset \mathrm{Fit}_R(M)$
- If I is an ideal of R, then $\mathrm{Fit}_{R/I}(M/IM)$ is the image of $\mathrm{Fit}_R(M)$ in R/I
- If M is a direct sum of cyclic R-modules, i.e. $M = R/p_1 \times ... \times R/p_k$, then $\mathrm{Fit}_R(M) = p_1....p_k$

Now we need some isomorphism criterion to prove our modularity lifting results.

Theorem 6.3.2. *(Isomorphism criterion) Let us consider the following commutative triangle*



Let I be ker(f), then the map π is an isomorphism between complete intersections over Λ iff $\pi(Fit_R(I)) \not\subset m_\Lambda T$.

Proof. See [11] □

Corollary 6.3.3. *If T is Gorenstein over Λ or if we replace Λ by a DVR, then π is an isomorphism iff $\pi(Fit_R(I)) = Ann_T(J)$, where J=ker$(T \to \Lambda)$.*

Proof. See [11] □

We use this theorem to state Wiles numerical criterion. Let J be the kernel g. Define the Λ-module η by $g(\mathrm{Ann}_T(J))$.

Corollary 6.3.4. *Let $\mathcal{O}$ be a DVR and assume we have a commutative triangle as before where we replace Λ by $\mathcal{O}$. Assume further that T is free as $\mathcal{O}$-module and $\eta \neq 0$. Then π is an isomorphism of complete local intersections over $\mathcal{O}$ iff length$_{\mathcal{O}}(I/I^2) =$ length$_{\mathcal{O}}(\mathcal{O}/\eta)$.*

Proof. See [11]. □

Remark 6.3.5. Note that for a surjection π as above, length$_{\mathcal{O}}(I/I^2) \geq$ length$_{\mathcal{O}}(\mathcal{O}/\eta)$. The difficult part in the above corollary is to show the reverse inequality.

Now we are ready to use the various isomorphism criteria. We assume **hypothesis 1** throughout the rest of the section. Let us recall our deformation problem.

Fix a squarefree tame level N. Let $\bar{\rho} = \begin{pmatrix} \theta\omega & * \\ & \psi \end{pmatrix}$, where

- $\theta\psi(-1) = 1$
- ψ is unramified at p

- $*$ is ramified at all $l|N/cond(\theta\psi^{-1})$ and $*|_{I_p} \neq 0$.

- $\bar{\rho}$ is mod p distinguished.

Then we have shown in proposition 6.2.35 that $\bar{\rho} \cong \rho_f$, for some cusp form f. We consider the universal deformation ring $\mathscr{R}_{\bar{\rho}}^{univ}$ parametrizing lifts which are ordinary at p, Steinberg at all primes where $*$ is ramified and we take the minimal lifts at primes where the diagonal characters are ramified. Note that Galois representation attached to the modular form f constructed in proposition 6.2.35 has all the above properties by theorem 4.1.2. Using the results in Chapter 3 and proposition 3.7.5, we get a commutative triangle

$$\begin{array}{ccc} \mathscr{R}_{\bar{\rho}}^{univ} & \xrightarrow{\quad\pi\quad} & \mathfrak{H}_m \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle pr_2} & \\ & \Lambda & \end{array}$$

where $\pi : \mathscr{R}_{\bar{\rho}}^{univ} \to \mathfrak{H}_m$ given explicitly by

$$tr(\rho^{univ})(Frob_l) \mapsto (T_l, T_l(\tilde{\mathscr{E}}(\theta, \psi))) \tag{6.16}$$

pr_2 is the projection onto the Eisenstein component and f is the canonical surjection $f : \mathscr{R}_{\bar{\rho}}^{univ} \twoheadrightarrow R^{red} \cong \Lambda$. Thus the kernel of f is the ideal of reducibility as defined before.
Assuming cyclicity conjecture we will use the isomorphism criterion to give a new simple proof of the Gorensteinness of the Hecke algebras constructed by Ohta.
Skinner-Wiles in [56] and [57] have proved modularity lifting results for reducible representations. However in both their works they only treat the case where $\psi = 1$. However, we bypass that problem by using Ohta's residue map. Calculation of the cotangent space I/I^2 was inspired by Sharifi's results in [54] and our results generalize his results. The computation of the congruence modules is already done by Ohta and the following hypotheses are required to ensure that the isomorphism criterion is satisfied. Moreover our proof is explicit

in the sense that our proof shows that the reducibility locus coincides with the Eisenstein series which is a rather intuitive situation. However just like [56], we have to assume **Hypothesis 1**, otherwise we can not get a map from $R_{\bar{\rho}}^{univ} \to \mathfrak{H}_m$. This was explained in our section on pseudo-representations. Skinner-Wiles in [57] removed **Hypothesis 1**, but their proof is not explicit. In the current literature, one works with pseudodeformations and this work is been carried by P. Wake and C. Erickson in a series of papers.
To prove the next theorem, let us assume the following additional hypothesis:

- $p \nmid \phi(N)$ or **Neben**.
- $(\theta, \psi) \neq (\omega^{-2}, 1)$
- $p | B_{1,\psi\theta^{-1}\omega^{-1}}$
- (Vandiver-type cyclicity conjecture) C/IC is cyclic as a Λ module, cf. section 3.5

Theorem 6.3.6. *(Skinner-Wiles, Ohta) We have an isomorphism $\mathscr{R}_{\bar{\rho}}^{univ} \cong \mathfrak{H}_m$ of complete local intersections over Λ.*

Proof. Let I^{red} be the ideal of reducibility, then we get by the commutative triangle that I^{red} surjects onto $I(\theta, \psi)$ via π. Thus using the properties of Fitting ideals, we have the chain of inclusions:

$$\pi(\mathrm{Fit}_{\mathscr{R}_{\bar{\rho}}^{univ}}(I^{red})) \subset \mathrm{Fit}_{\mathfrak{H}_m}(I(\theta, \psi)) \subset \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta, \psi))$$

Now, $\mathrm{Ann}_{\mathfrak{H}_m}(I(\theta, \psi)) = \ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m)$ by lemma 6.2.32 and by remark 6.2.31, we know that
$\mathrm{Ann}_{\mathfrak{H}_m}(I(\theta, \psi)) = A_{\theta,\psi} \subset \Lambda$, where we view Λ as a $\mathfrak{H}_m$ module via pr_2. By Hida duality (theorem 4.2.4),

$$\ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m) = \mathrm{Image(Res)}$$

But by Lafferty-Ohta (theorem 6.2.19), the image does not lie in m_Λ. To complete the proof of the theorem via theorem 6.3.2, we need to show

$$\pi(\mathrm{Fit}_{\mathscr{R}^{univ}_{\bar{\rho}}}(I^{red})) = \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi)) = A_{\theta,\psi}$$

Since for any R module M, and for any ideal $I \subset R$, $M \otimes_R R/I \cong M/IM$, and by the properties of Fitting ideals, we see that

$$\mathrm{Fit}_\Lambda(I^{red}/(I^{red})^2) = f(\mathrm{Fit}_{\mathscr{R}^{univ}_{\bar{\rho}}}(I^{red})) = pr_2(\pi(\mathrm{Fit}_{\mathscr{R}^{univ}_{\bar{\rho}}}(I^{red})))$$

and the above inclusions show that $\mathrm{Fit}_\Lambda(I^{red}/(I^{red})^2) \subset A_{\theta,\psi}$. Under the Vandiver type assumption, we get I^{red} is cyclic as a Λ-module by theorem 3.5.15 and theorem 3.5.25. Thus we get $Fit_\Lambda(I^{red}/(I^{red})^2) = \mathrm{Ann}_\Lambda(I^{red}/(I^{red})^2$. Under the assumption of cyclicity, proposition 3.5.12 and theorem 3.5.23 shows that either

$$C/IC \cong \Lambda/(G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1))$$

or $G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1)$ is a unit and $C/IC \cong R_q$ but the p-divisibility of $B_{1,\psi\theta^{-1}\omega^{-1}}$ contradicts $(G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1))$ is a unit. Thus all the f_q's are units. Note that $B/IB \cong \Lambda$. Thus $I^{red}/(I^{red})^2 = C/IC$. Thus $\mathrm{Ann}_\Lambda(I^{red}/(I^{red}))^2 = (G_{\theta\psi^{-1}\omega^2}(u(1+T)^{-1}-1))$. Now $\mathrm{Gal}(L_\infty/F_\infty)$ is unramified everywhere by lemma 3.5.26. Since all the f_q's are units, by the formula (6.11), we see that there are no Euler factors in the definition of $A_{\theta,\psi}$. Combining this observation with theorem $A.1.13$ and the displayed formula $A.1.12$ in [43] shows that $A_{\theta,\psi}$ is the characteristic polynomial of C/IC. Thus $A_{\theta,\psi} \subset \mathrm{Fit}_\Lambda(I^{red}/(I^{red})^2)$. Thus $Fit_\Lambda(I^{red}/(I^{red})^2) = A_{\theta,\psi}$ which implies $pr_2(\pi(\mathrm{Fit}_{R^{univ}_{\bar{\rho}}}(I^{red})) = pr_2(\mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi))$. Similar arguments as in lemma 6.2.33 shows that $pr_2|_{\ker(\mathfrak{H}_m \twoheadrightarrow \mathfrak{h}_m)}$ is injective and maps $\mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi)$ isomorphically onto $A_{\theta,\psi}$. Thus, $\pi(\mathrm{Fit}_{R^{univ}_{\bar{\rho}}}(I^{red})) = \mathrm{Ann}_{\mathfrak{H}_m}(I(\theta,\psi))$ $\square$

Remark 6.3.7. The proof actually shows that Gorensteinness of the Hecke algebra is "almost" equivalent to the cyclicity conjecture.

Remark 6.3.8. We want to make a few comments regarding the hypotheses made at the beginning of the theorem.

- Ohta used the condition $p \nmid \phi(N)$ but we can remove that condition with a slightly general **Neben**.

- (Trivial zero case) $p|B_{1,\psi\theta^{-1}\omega^{-1}}$ along with $p \nmid \phi(N)$(or **Neben**) ensures $I^{red} \neq 0$. However if $p \nmid B_{1,\psi\theta^{-1}\omega^{-1}}$, then I^{red} is non zero iff there is a trivial zero coming from the Euler factor at the auxiliary primes. Recall the example of $X_1(11)$ worked out earlier where $I^{red} \neq 0$ and the trivial zero came from the Euler factor at 11. This is the so called case of trivial zero which was first solved by Greenberg-Stevens in their proof of Mazur-Tate-Teitelbaum. Moreover since C/IC is cyclic, we get that there is only prime q congruent to $1 \pmod{p}$ and $C/IC = R_q$ by proposition 3.5.13. And $A_{\theta,\psi}$ is f_q. This is theorem 6.3.1 in [65]. Note that our cyclicity of B/IB ensures the hypothesis of theorem 6.3.1 in [65] are satisfied. In this case, one also gets that $\mathfrak{H}_m$ is Gorenstein.

Definition 6.3.9. (Skinner-Wiles) A prime $\mathfrak{p}$ in $\mathscr{R}_{\bar{\rho}}^{univ}$ is nice if it is good (see definition 3.4.21) and is an inverse image of a prime $\mathfrak{q}$ in $\mathfrak{h}_m$.

Theorem 6.3.10. *(a) There is an isomorphism $(\mathscr{R}_{\bar{\rho}}^{univ})_{\mathfrak{p}} \cong (\mathfrak{H}_m)_{\mathfrak{q}}$ of complete local intersections over Λ_p, where $\mathfrak{p} \subset \mathscr{R}_{\bar{\rho}}^{univ}$ and $\mathfrak{q} \subset \mathfrak{H}_m$ are any height 1 prime ideal (sometimes referred to prime divisors) over $(p) \subset \Lambda$ such that $\pi^{-1}(\mathfrak{q}) = \mathfrak{p}$*
(b) (Skinner-Wiles) Under the isomorphism above, $(\mathscr{R}_{\bar{\rho}}^{univ})_{\mathfrak{p}} \cong (\mathfrak{h}_m)_{\mathfrak{q}}$ for all nice primes $\mathfrak{p}$ and both the rings are complete local intersections.

Proof. Proposition 2.1 in [26] shows that

$$(\mathfrak{H}_m)_p = (\mathfrak{h}_m)_p \times \Lambda_p$$

or in other words the congruence ideal vanishes when localized over any prime divisor above (p). We will abuse notation and use the letter p to denote the prime ideals above (p) in the following commutative diagram of rings.

$$\begin{array}{ccc} (\mathscr{R}^{univ}_{\bar{\rho}})_p & \xrightarrow{\quad\pi\quad} & (\mathfrak{H}_m)_p \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle pr_2} & \\ & (\Lambda)_p & \end{array}$$

Now, annihilator of $\ker(pr_2)$ is clearly Λ_p from the formula above. Thus, $\eta = \Lambda_p$ and so $\text{length}_\Lambda(\Lambda/\eta) = 0$. To use the numerical criterion, we need to find the length of $(I^{red}/(I^{red})^2)_p$. But theorems 3.5.15 and 3.5.25 give us a description of the Λ module $(I^{red}/(I^{red})^2)_p$ in terms of the tensor product of two Iwasawa modules. Now support of $\text{Supp}(M \otimes N) \subset \text{Supp}(M) \cap \text{Supp}(N)$. Finally note that $(C/IC)_p = (R_q)_p \times \Lambda_p/(A_{\theta,\psi})_p$ but $A_{\theta,\psi}$ and the characteristic ideals of R_q all have μ-invariant 0, or in other words, localizing at the prime ideal (p) above the prime $(p) \subset \Lambda$, makes them all units. Thus $(C/IC)_p = 0$, and thus $(I^{red}/(I^{red})^2)_p = 0$, thus the length is also 0 and so the numerical criterion is satisfied (corollary 6.3.4). So to summarize, we have shown an isomorphism

$$(\mathscr{R}^{univ}_{\bar{\rho}})_p \cong (\mathfrak{H}_m)_p$$

Now, note that if $\mathfrak{p}$ is a good prime, then the height of $\mathfrak{q}$ is necessarily 1. Suppose not, if the height is 0, then $\mathfrak{q}$ is a minimal prime but minimal primes are in characteristic 0, but $\mathfrak{p}$ has characteristic p. Thus $\mathfrak{q}$ has characteristic p and thus sits over $(p) \subset \Lambda$. In this case $\mathfrak{q}$

pulls back to a height 1 prime $\mathfrak{q}' \subset \mathfrak{H}_m$ and

$$(\mathfrak{h}_m)_{\mathfrak{q}} \cong (\mathfrak{H}_m)_{\mathfrak{q}'} \cong (\mathscr{R}^{univ}_{\bar{\rho}})_{\mathfrak{p}}$$

Since the map $pr_2 : (\mathfrak{h}_m)_q \to \Lambda_p$ is the 0 map, (by abuse of notation) π can not factor through R^{red} which implies the Galois representation with values in $(\mathfrak{H}_m)_{q'}$ is irreducible. Theorem 4.1 in [26] shows that $(\mathfrak{H}_m)_{\mathfrak{q}'}$ is Gorenstein. □

Remark 6.3.11. In theorem 3.29 in [24] Hida constructs a pseudorepresentation with values in $\mathfrak{h}$, and to upgrade that pseudorepresentation into a representation, we need

Hypothesis 1.

Remark 6.3.12. Our proof also shows that the Eisenstein locus of $(\mathfrak{H}_m)_{\mathfrak{q}}$ coincides with the reducibility locus in the universal deformation ring. Indeed in that case, we will get

$$(\mathscr{R}^{univ}_{\bar{\rho}})_{\mathfrak{p}} \cong (\mathfrak{H}_m)_{\mathfrak{q}} \cong \Lambda_p$$

Theorem 6.3.13. *(Wake's conjecture)* $\mathfrak{H}^{ord}_m$ *is weakly Gorenstein.*

Proof. From the discussions before, we are also concerned about the prime divisors of $A_{\theta,\psi}$. Let f be a prime divisor of $A_{\theta,\psi}$, then we get a commutative triangle

$$\begin{array}{ccc} (\mathscr{R}^{univ}_{\bar{\rho}})_{\mathfrak{p}} & \xrightarrow{\quad\pi\quad} & (\mathfrak{H}_m)_f \\ & {\scriptstyle \pi_1} \searrow \quad \swarrow {\scriptstyle pr_2} & \\ & \Lambda_f & \end{array}$$

where Λ_f is a DVR and $\mathfrak{p}$ is the prime above f. To prove the conjecture, it is enough to use the numerical criterion. Now $\text{length}_{\Lambda}(I/I^2)_{\mathfrak{p}} =$ multiplicity of f in $A_{\theta,\psi}$, by Theorem 3.4.14, since $A_{\theta,\psi}$ does not share any prime factors with R_q and $T - p \nmid A_{\theta,\psi}$. And the congruence module on the right is nothing but $(A_{\theta,\psi})_f$,which has length equal to multi-

plicity of f in $A_{\theta,\psi}$. Thus by the numerical criteria, π is an isomorphism of complete local intersections over Λ_f. □

Remark 6.3.14. The two theorems above have two different flavors. One of them deals with primes above p and needs deep results like the vanishing of μ invariants whereas the previous theorem deals with characteristic zero primes and needs results like the coprimality of characteristic ideals of various Iwasawa modules.

Chapter 7: Selmer groups

7.1 Review of some basic definitions

We start by recalling the definitions of various Selmer groups. We will be assuming **Neben** throughout the section.

Let $\bar{\rho} \cong \begin{pmatrix} \theta\omega & * \\ 0 & \psi \end{pmatrix}$, where $\theta\psi(-1) = 1$ and ψ and θ are both unramified at p. Let M be the $\mathbb{F}$ vector space on which $\bar{\rho}$ acts.

Definition 7.1.1. The residual Greenberg Selmer group associated to a set of local conditions is given by

$$\mathrm{Sel}(\mathbb{Q}, M) = \ker\left(H^1(\mathbb{Q}_S, M) \to \prod_v H^1(\mathbb{Q}_v, M)/L_v \right)$$

where

- $L_p := \ker(H^1(\mathbb{Q}_p, M) \to H^1(I_p, \psi))$
- for $v \in S$ and $v \nmid p$, $L_v := H^1_{nr}(\mathbb{Q}_v, M)$

where S contains all primes dividing N and p and ∞. Note that since p is odd, the primes above ∞ will not contribute towards our calculations of Selmer groups.

Remark 7.1.2. There is also a version of Selmer groups in which we replace I_p by D_p. Those Selmer groups are called strict Selmer groups.

We recall the definition of imprimitive residual Selmer groups.

Definition 7.1.3. Let Σ_0 be any finite subset of S, not containing p and ∞, then

$$\mathrm{Sel}^{\Sigma_0}(\mathbb{Q},M) := \ker\left(H^1(\mathbb{Q}_S,M) \to \prod_{v\in S\setminus\Sigma_0} H^1(\mathbb{Q}_v,M)/L_v\right)$$

where L_v are defined as above.

Now we come to some other Selmer groups. We closely follow the definitions in [49]. Let V be an ordinary Galois representation and let T be any Galois stable lattice. Let $M := V/T$, then we define the Selmer group. Let S be the set containing all ramified primes and p and ∞.

Definition 7.1.4.

$$\mathrm{Sel}(\mathbb{Q},M) := \ker\left(H^1(\mathbb{Q},M) \to H^1(\mathbb{Q}_v,M)/L_v\right)$$

Since V is ordinary, there is a D_p stable line V_1 and I_p acts trivially on V/V_1. Let M_1 denote the image of V_1 in M and let $M_2 := M/M_1$, then we define

$L_p := \ker(H^1(\mathbb{Q}_p,M) \to H^1(I_p,M_2))$.

for $v \in S,\ v \neq p$, $L_v := H^1_{nr}(\mathbb{Q}_l,M)$.

We can analogously define the imprimitive Selmer group as before.

7.2 Some calculations on Selmer groups

Let $\psi \neq 1$. Then we have an exact sequence

$$0 \to H^1(\mathbb{Q}, \theta\omega) \to H^1(\mathbb{Q}, M) \to H^1(\mathbb{Q}, \psi) \to H^2(\mathbb{Q}, \theta\omega) \tag{7.1}$$

We want to understand what elements in $H^1(\mathbb{Q}, \theta\omega)$ land inside L_p.

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathbb{Q}_p, \theta\omega) & \longrightarrow & H^1(\mathbb{Q}_p, M) & \longrightarrow & H^1(\mathbb{Q}_p, \psi) \\ & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} \\ 0 & \longrightarrow & H^1(I_p, \theta\omega) & \longrightarrow & H^1(I_p, M) & \longrightarrow & H^1(I_p, \psi) \end{array}$$

from the diagram above, we see that image of $H^1(\mathbb{Q}_p, \theta\omega)$ lies in L_p. In fact even if $\psi = 1$, we still get $H^1(\mathbb{Q}_p, \theta\psi)$ lands inside L_p. This is clear from the diagram below:

$$\begin{array}{ccccccc} \mathbb{F} & \longrightarrow & H^1(\mathbb{Q}_p, \theta\omega) & \longrightarrow & H^1(\mathbb{Q}_p, M) & \longrightarrow & H^1(\mathbb{Q}_p, \mathbb{F}) \\ & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} & \searrow & \downarrow{\scriptstyle \text{res}} \\ \mathbb{F} & \longrightarrow & H^1(I_p, \theta\omega) & \longrightarrow & H^1(I_p, M) & \longrightarrow & H^1(I_p, \mathbb{F}) \end{array}$$

Finally assume $\theta \neq 1$, by Tate duality (theorem 2.2.3) we get $H^2(\mathbb{Q}_p, \theta\omega) = 0$. And as a consequence, we see that

$$0 \to H^1(\mathbb{Q}_p, \theta\omega) \to L_p \to H^1_{nr}(\mathbb{Q}_p, \psi) \to 0$$

is exact.

We remark that in the case of strict Selmer groups, we replace $H^1_{nr}(\mathbb{Q}_p, \psi)$ by $H^1(\mathbb{Q}_p, \psi)$. Now we need to deal with other auxiliary primes. We break it down into a few cases. First we assume that the conductor of $\theta\psi$ is N, and N will always be square free.

Let $l|N$, then $H^1_{nr}(\mathbb{Q}_l, \theta\omega) = H^0(\mathbb{Q}_l, \theta\omega)$ from (2.3). Thus $H^1_{nr}(\mathbb{Q}_l, \theta\omega) \neq 0$ iff $\theta\omega = 1$. In particular, θ is unramified so ψ is ramified. In that case by (2.3), $H^1_{nr}(\mathbb{Q}_l, \psi) = 0$. Also note that $H^1_{nr}(\mathbb{Q}_l, M) \neq 0$ iff $\theta\omega$ or ψ is the trivial character.

Thus when ψ is ramified, we get an isomorphism $H^1_{nr}(\mathbb{Q}_l, \theta\psi) \cong H^1_{nr}(\mathbb{Q}_l, M)$ as both of them are 1-dimensional vector spaces over $\mathbb{F}$. Now if ψ is the trivial character, we have the long exact sequence,

$$H^0(\theta\omega) \to H^0(M) \to H^0(\mathbb{F}) \to H^1(\theta\omega) \to H^1(M) \to H^1(\mathbb{F}) \to H^2(\theta\omega) \tag{7.2}$$

Now θ is ramified at l, thus $H^0(\theta\omega) = H^2(\theta\omega) = 0$ and $H^0(M) = \mathbb{F}$

This shows that we have an isomorphism $H^1_{nr}(\mathbb{Q}_l, M) \cong H^1_{nr}(\psi)$. Combining all the cases, we get an injection:

$$H^1_{\mathscr{L}}(\mathbb{Q}_S, \theta\omega) \to \mathrm{Sel}(\mathbb{Q}, M)$$

In the case where $f_\theta f_\psi \neq N$, we will use the imprimitive Selmer groups. Now pick a prime l dividing N but not $f_\theta f_\psi$. Then $*$ is necessarily ramified at I_l. In that case, we relax the local condition at l by defining $L_l = 0$. Thus we get an injection of $H^1_{\mathscr{L}}(\mathbb{Q}, \theta\omega) \hookrightarrow Sel^{\Sigma_0}(\mathbb{Q}, M)$. We summarize the above discussion in the form of the following proposition:

Proposition 7.2.1. *Let $f_\theta, f_\psi = N$ and $\theta \neq 1$, then we have an exact sequence of Selmer groups,*

$$0 \to Sel(\mathbb{Q}, \theta\omega) \to Sel(\mathbb{Q}, M) \to Sel(\mathbb{Q}, \psi)$$

Note the right group is 0 if $\psi = 1$ as there are no unramified extensions of $\mathbb{Q}$. It is also 0 if $Cl_p(K_\psi)^\psi = 0$ where K_ψ is the fixed field of the kernel of ψ.

Finally we would like to estimate the size of $H^1_{\mathscr{L}}(\mathbb{Q}, \theta\omega)$. This estimation is a standard application of the Greenberg-Wiles formula. Let $M = \mathbb{F}(\theta\omega)$. Then $M^* = \mathbb{F}(\theta^{-1})$. We define $H^1_{\mathscr{L}^\perp}(\mathbb{Q}, M^*)$ by requiring the classes to be locally trivial at p and unramified

everywhere else. Recall the Greenberg-Wiles formula from Chapter 2 :

$$\frac{\#H^1_{\mathscr{L}}(\mathbb{Q},M)}{\#H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*)} = \frac{\#H^0(\mathbb{Q},M)}{\#H^0(\mathbb{Q},M^*)} \prod \frac{\#\mathscr{L}_v}{\#H^0(\mathbb{Q}_v,M)}.$$

To analyze this, we will study each of the terms separately. Under our hypotheses, we are just left to calculate $\mathscr{L}_v$ and $H^0(\mathbb{Q}_v,M)$. If $l|f_\theta$, then $H^0(\mathbb{Q}_v,M) = 0 = \mathscr{L}_l$. If $l \nmid f_\theta$, then M is unramified at l and so $L_l = H^0(\mathbb{Q}_l,M)$. Finally we are left to calculate $l = \infty$. $H^1_{nr}(\mathbb{R},M) = 0$ and $H^0(\mathbb{R},M) = p^r$ iff θ is odd, where $p^r = \#\mathbb{F}$.

Remark 7.2.2. In [19] and [3], $\mathrm{Sel}(\mathbb{Q},M)$ is defined by taking $L_v = 0$, for all $v \in S$ and $v \neq p$, i.e., Σ_0 contains all ramified primes, except p. In that case, a similar diagram chase as above shows $H^1(\mathbb{Q}_S,\theta\omega) \hookrightarrow \mathrm{Sel}^{\Sigma_0}(\mathbb{Q},M)$.

The group $H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*)$ can be seen as the $Cl_p(K_\theta)^{\theta^{-1}}$ by noting that under **Neben** $[K_\theta : \mathbb{Q}]$ is prime to p and the rest follows from [49]. We remark that if θ is even, then $H^1_{\mathscr{L}^\perp}(\mathbb{Q},M^*)$ is given by the p-adic L-function by the work of Wiles [68].

Now we relate the Selmer groups and the residual Selmer groups. Most of these results are standard calculations in Iwasawa theory so we only provide a sketch.

Since M is π-divisible, we have an exact sequence

$$0 \to M[\pi] \to M \xrightarrow{\pi} M \to 0 \tag{7.3}$$

Under the assumptions in this section we note that $H^0(\mathbb{Q},M[\pi]) = 0$, thus we get an isomorphism

$$H^1(\mathbb{Q},M[\pi]) \cong H^1(\mathbb{Q},M)[\pi] \tag{7.4}$$

We want to show the following proposition:

Proposition 7.2.3. *The exact sequence above induces a map $f : Sel(\mathbb{Q},M[\pi]) \to Sel(\mathbb{Q},M)[\pi]$ and f is an isomorphism if $f_\theta f_\psi = N$. Otherwise, let Σ_0 contain all primes except p, then*

$Sel^{\Sigma_0}(\mathbb{Q},M[\pi]) \to Sel^{\Sigma_0}(\mathbb{Q},M)[\pi]$ is an isomorphism.

Proof. Let $c \in \mathrm{Sel}(\mathbb{Q},M[\pi])$, let $v \in S$ and $v \neq p$, and if v is such that $H^0(\mathbb{Q}_v,M[\pi]) = 0$, then by (2.3), $H^1_{nr}(\mathbb{Q}_v,M[\pi]) = 0$, thus there is no local condition and we have nothing to check. Now suppose that $H^1_{nr}(\mathbb{Q}_v,M[\pi]) = H^0(\mathbb{Q}_v,M[\pi]) \neq 0$, by a long exact sequence in cohomology we still get $H^1(\mathbb{Q}_v,M[\pi]) \cong H^1(\mathbb{Q}_v,M)[\pi]$. We just have to check $H^1_{nr}(\mathbb{Q}_v,M[\pi]) \subset H^1_{nr}(\mathbb{Q}_v,M)[\pi]$. Taking the I_v cohomology of the exact sequence (7.3), we get $H^1(I_v,M[\pi]) \cong H^1(I_v,M)[\pi]$, since M^{I_v} and $M[\pi]^{I_v}$ are one dimensional $K/\mathscr{O}$ and $\mathbb{F}$ modules respectively and M is divisible. And finally we have a commutative square

$$\begin{array}{ccc} H^1(\mathbb{Q}_v,M[\pi]) & \xrightarrow{\cong} & H^1(\mathbb{Q}_v,M)[\pi] \\ \Big\downarrow{\scriptstyle res} & & \Big\downarrow{\scriptstyle res} \\ H^1(I_l,M[\pi]) & \xrightarrow{\cong} & H^1(I_l,M)[\pi] \end{array}$$

And this takes care of all the primes $v \neq p$. For the prime p, see [3].

The map f is obviously injective. Now we would like to show that the map f is surjective. Let $c \in \mathrm{Sel}(\mathbb{Q},M)[\pi]$. Now let $v \in S$ and $v \neq p$, then $c(\sigma) = \sigma(\beta_v) - \beta_v$ for some $\beta_v \in M$ and for all $\sigma \in I_v$. We want to show $\beta_v \in M[\pi]$. Also note that $\sigma(\pi\beta_v) = \pi\beta_v$. From the exact sequence (7.3), c comes from $H^1(\mathbb{Q},M[\pi])$, which implies $\sigma(\beta_v) - \beta_v = t_v$, where $t_v \in M[\pi]$. Now under some choice of basis $\{e_1,e_2\}$, $M|_{I_v} = 1 \oplus \mu$, where μ is a ramified character. Thus $\pi\beta_v = x_v e_1$ for some $x \in K/\mathscr{O}$. Let y be such that $\pi y_v = x_v$, then combining the above relations, we get

$$\beta_v = y_v e_1 + t_v$$

and since $\sigma(e_1) = e_1$, we immediately get

$$c(\sigma) = \sigma(t_v) - t_v$$

Checking the condition at p is well known. For example, see [19] or [3].

When $f_\theta f_\psi \neq N$, one must work with imprimitive Selmer groups and the second part of this proposition is essentially the crux of [19] □

Remark 7.2.4. We think of the above proposition and proposition 7.2.1 as a factorization (or congruence) statement between algebraic p-adic L-functions. For the corresponding statement about analytic p-adic L-functions, one needs that the Hecke algebra is Gorenstein and to prove a similar factorization statement for analytic p-adic L-functions led us to this thesis. When the Hecke algebra is Gorenstein, this is known from the work of [19] or recently by [3].

Bibliography

[1] J. Bellaiche. Pseudodeformations. *Math. Zeitschrift*, 270:1–18, 2012.

[2] J. Bellaiche and G. Chenevier. Families of galois representations and selmer groups. *Asterisque*, 324, 2009.

[3] J. Bellache and R. Pollack. Congruences with eisenstein series and μ-invariants. `http://arxiv.org/abs/1806.04240v1`, 2018. preprint.

[4] S. Bloch and K. Kato. l-functions and tamagawa numbers of motives. *The Grothendieck Festschrift*, pages 334–400, 1990. Progress in Math. 86, Birkhauser.

[5] G. Böckle. Presentations of universal deformation rings in : l-functions and galois representations. *LMS Lecture Note Series*, 320:24–58, 2007. Cambridge Univ. Press, Cambridge.

[6] W. Bruns and J. Herzog. *Cohen Macaulay rings*. Cambridge studies in Adv. Math. Cambridge University Press, 1986.

[7] F. Calegari. Eisenstein deformation rings. *Compositio Mathematica*, 142(1):63–83, 2006.

[8] F. Calegari and M. Emerton. On the ramification of hecke algebras at eisenstein primes. *Invent. Math*, 160(1):97–144, 2005.

[9] J. Coates. k-theory and iwasawa's analog of the jacobian. *Algebraic K-theory II, Lecture Notes in Math.*, pages 502–520, 1973. Springer 342.

[10] J. Coates and S.T. Yau. *Elliptic curves, Modular forms and Fermat's Last theorem*. International Press, Cambridge, 1995.

[11] B. de Smit, K. Rubin and R. Schoof. Criteria for complete intersections. pages 343 – 355, 1995.

[12] B. Conrad , F. Diamond and R. Taylor. Modularity of certain potentially barsotti-tate galois representations. *J. Amer. Math. Soc.*, 12:521–567, 1999.

[13] F. Diamond. On deformation rings and hecke rings. *Annals of Math.*, 144:131–160, 1996.

[14] F. Diamond and R. Taylor. Lifting modular mod l representations. *Duke Math. J.*, 74:253–269, 1994.

[15] Brian Conrad, Karl Rubin, eds. *Arithmetic Algebraic Geometry*, volume 9. IAS/Park City Math. Series, 2001.

[16] G. Cornell, J.Silverman, G. Stevens, eds. *Proceedings of the Conference on Fermat's Last Theorem, Boston University, August 9-18*. Springer, 1995.

[17] T. Fisher. Descent calculations for the elliptic curves of conductor 11. *Proc. Lond. Math. Soc. (3)*, 86:583–606, 2003.

[18] F. Gouvea. Deformations of galois representations, arithmetic algebraic geometry (park city, ut, 1999). *Amer. Math. Soc., Providence, RI*, pages 233–406, 2001. IAS/Park City Math. Ser., 9.

[19] R. Greenberg and V. Vatsal. On the iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17–63, 2000.

[20] L. Clozel , M. Harris and R. Taylor. Automorphy of some l-adic lifts of automorphic mod l representations. *Publ. Math. IHES*, 108:1–181, 2008.

[21] H. Hida. Congruences of cusp forms and special values of their zeta functions. *Inv. Math.*, 63:225–261, 1981.

[22] H. Hida. Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[x]])$ attached to ordinary cusp forms. *Invent. Math.*, 85(3):545–613, 1986.

[23] H. Hida. Modules of congruence of hecke algebras and l-functions associated with cusp forms. *Amer. J. Math.*, 110:323–382, 1988.

[24] H. Hida. *Modular forms and Galois cohomology*. Cambridge studies in Adv. Math No. 69, Cambridge University Press, 2000.

[25] H. Hida. *Hilbert modular forms and Iwasawa theory*. Oxford Mathematical Monographs, Oxford University Press, 2006.

[26] H. Hida. Image of λ-adic galois representations modulo p. *Inventiones Math.*, 194:1–40, 2013.

[27] H. Hida. Big galois representations and p-adic l-functions. *Compositio Math.*, 151:603–664, 2015.

[28] T. Itoh. On tamely ramified iwasawa modules for the cyclotomic $\mathbb{Z}_p$-extension of abelian fields. *Osaka J. Math.*, 51(2):513–537, 2014.

[29] K. Iwasawa. Riemann-hurwitz formula and p-adic galois representations for number fields. *Tohoku Math. J.*, 33(2):263–288, 1981.

[30] C. Khare and J.P. Wintenberger. Serre's modularity conjecture ii. *Inventiones Mathematicae*, 178(3):505–586, 2009.

[31] M. Kisin. Lectures on deformations of galois representations. Clay summer school on Galois representations, Honolulu, 6/15-7/10/09.

[32] M. Kisin. The fontaine-mazur conjecture for GL_2. *J.A.M.S.*, 22(3):641–690, 2009.

[33] M. Lafferty. *Eichler-Shimura cohomology groups and the Iwasawa main conjecture*. PhD thesis, The University of Arizona, 2015. 89 pp.

[34] H. W. Lenstra. Complete intersections and gorenstein rings. In *[10]*, pages 99–109, 1995.

[35] H. Matsumura. *Commutative Ring Theory*. Number 8 in Cambridge Studies in Adv. Math. Cambridge University Press, 1986.

[36] B. Mazur. Modular curves and the eisenstein ideal. *Publications mathématiques de l'I.H.É.S.*, 47:33–186, 1977.

[37] B. Mazur. Deforming galois representations, in galois groups over $\mathbb{Q}$. In *Y. Ihara, K. Ribet, J.P. Serre, eds., MSRI Publ.*, volume 16, pages 385–437. Springer-Verlag, 1989.

[38] B. Mazur. Constructing abelian extensions of basic number fields. *Bulletin (New Series) Of the American Mathematical Society*, 48(2):155–209, 2011.

[39] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathfrak{q}$. *Invent. Math.*, 76:179–330, 1984.

[40] J.S. Milne. *Arithmetic Duality Theorems, Perspectives in Math.* Academic Press, 1986.

[41] M. Ohta. Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. *Compositio Math.*, 115(3):241–301, 1999.

[42] M. Ohta. Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves ii. *Math. Ann.*, 318(3):557–583, 2000.

[43] M. Ohta. Congruence modules related to eisenstein series. *Ann. Sci. École Norm. Sup.*, 36 (4)(2):225–269, 2003.

[44] M. Ohta. Companion forms and the structure of p-adic hecke algebras. *J. Reine Angew. Math.*, 585:141–172, 2005.

[45] L. Pan. *The Fontaine-Mazur conjecture in the residually reducible case*. PhD thesis, Princeton University, 2018. 179 pp.

[46] R. Pink. Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime. *Compositio Math.*, 88(3):251–264, 1993.

[47] R. Ramakrishna. On a variation of mazur's deformation functor. *Compositio Math.*, 87:269–286, 1993.

[48] K. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Inv. Math.*, 34(3):151–162, 1976.

[49] Karl Rubin. *Euler Systems*. Princeton University Press, New York, 2000.

[50] J. Neukirch, A. Schmidt and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *A series of Comprehensive Studies in Mathematics*. Springer, 2007.

[51] J.-P. Serre. *Jean-Pierre Serre, Oeuvres, Collected Papers, Volume II (1960-1971)*, chapter Une interprétation des congruences relatives á la fonction τ de Ramanujan, pages 498–511. Springer, 1986.

[52] J.P. Serre. *Abelian l-adic representations and Elliptic Curves*. Number 7 in Research Notes in Mathematics. CRC Press, 1968.

[53] J.P. Serre. *Trees*. Springer-Verlag Berlin Heidelberg, 1980.

[54] R. Sharifi. Iwasawa theory and the eisenstein ideal. *Duke Mathematical Journal*, 137(1):63–101, 2007.

[55] R. Sharifi. On galois groups of unramified pro-p extensions. *Mathematische Annalen*, 342(2):297–308, 2008.

[56] C. Skinner and A. Wiles. Ordinary representations and modular forms. *PNAS*, 94(20):10520–10527, 1997.

[57] C. Skinner and A. Wiles. Residually reducible representations and modular forms. *Publications Mathematiques de l' IHES*, 89:5–126, 1999.

[58] S. Nasseh, S. Sather-Wagstaff, R. Takahashi and K. VandeBogert. Applications and homological properties of local rings with decomposable maximal ideals. *Journal of Pure and Applied Algebra*, 223(3):1272–1287, 2019.

[59] R. Taylor. Galois representations associated to siegel modular forms of low weight. *Duke Math. J.*, 63(2):281–332, 1991.

[60] R. Taylor. On icosahedral artin representations, ii. *American Journal of Mathematics*, 125:549–566, 2003.

[61] R. Taylor and A. Wiles. Ring theoretic properties of certain hecke algebras. *Annals of Math.*, 141:553–572, 1995.

[62] J. Thorne. Automorphy lifting for residually reducible l-adic galois representations. *J. Amer. Math. Soc.*, 28(3):785–870, 2015.

[63] P. Wake. Eisenstein hecke algebras and conjectures in iwasawa theory. *Algebra and Number Theory*, 9(1):53–75, 2015.

[64] C. Wang-Erickson and P. Wake. The rank of mazur's eisenstein ideal. `http://www.math.ias.edu/~pwake/EisensteinRank2.pdf`, 2017. preprint.

[65] C. Wang-Erickson and P. Wake. The eisenstein ideal with squarefree level. `http://www.math.ias.edu/~pwake/SqfreeEisen2.pdf`, 2018. preprint.

[66] C. Wang-Erickson and P. Wake. Pseudo-modularity and iwasawa theory. *American Journal of Mathematics*, 140(4):977–1040, 2018.

[67] L. Washington. *Cyclotomic Fields*. 83. Graduate Text in Mathematics, 1997.

[68] A. Wiles. The iwasawa conjecture for totally real fields. *Ann. of Math.*, 131:493–540, 1990.

[69] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Math.*, 141:445–551, 1995.

[70] D. Yan. Stable lattices in modular galois representations and hida deformations. *Journal of Number Theory*, 197:62–88, 2019.