SELMER GROUPS AND RANKS OF HECKE RINGS

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Benjamin Lundell

May 2011

SELMER GROUPS AND RANKS OF HECKE RINGS

Benjamin Lundell, Ph.D.

Cornell University 2011

In this work, we investigate congruences between modular cuspforms. Specifically, we start with a given cuspform and count the number of cuspforms congruent to it as we vary the weight or level. This counting problem is equivalent to understanding the ranks of certain completed Hecke rings. Using the deep modularity results of Wiles, et al., we investigate these Hecke rings by studying the deformation theory of the residual representation corresponding to our given cuspform. This leads us to consider certain Selmer groups attached to this residual representation. In this setting, we can apply standard theorems from local and global Galois cohomology to achieve our results.

BIOGRAPHICAL SKETCH

Benjamin Lundell was born in Plainfield, New Jersey. After moving with his family to the Chicago suburbs, he graduated from Libertyville High School in 2001. He then attended the University of Illinois at Urbana-Champaign, graduating in 2004 with a Bachelor of Science degree in Mathematics. In 2005, he enrolled at King's College, University of Cambridge, to complete Part III of the Mathematical Tripos. The following year, he joined the Mathematics Department at Cornell University. Starting in September 2011, he will be a Visiting Assistant Professor in the Department of Mathematics and Statistics at the University of Massachusetts-Amherst.

For Helen

ACKNOWLEDGEMENTS

It has been a pleasure to be a member of the Mathematics Department at Cornell University, and I have found my fellow graduate students, the faculty, and the staff to be nothing but helpful and supportive. Specifically, I would like to thank John Hubbard, Samuel Kolins, Greg Muller, Mike Stillman, and Shankar Sen for their willingness to answer questions, big and small, over the last few years. Álvaro Lozano-Robledo has also been a constant sounding board for many ideas, mathematical or otherwise. I greatly appreciate his patience in this role.

I also owe an enormous debt of gratitude to my adviser, Ravi Ramakrishna. Anyone familiar with his work who reads this dissertation will surely notice his impact throughout. I have greatly enjoyed five years worth of conversations about mathematics and baseball.

I never would have had the chance to come to Cornell if I had not had the unconditional love and support of my family. My sisters, Eva, Sydney, and Emily, have always believed in me, even when they have their own families to care for. My parents have always put my best interests before their own. Finally, my wife, Helen, has had to do all of the above, and more, in person, every day. Thank you all.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Congruences Between Modular Forms

For the last century, congruences between modular forms have played a central role in number theory. Ramanujan's work on the τ-function, Ribet's work on the converse to Herbrand's Theorem, Mazur's work on the Eisenstein ideal, and Wiles' work on Fermat's Last Theorem all concern congruences between modular forms. Much of the work on this topic has centered on proving that congruent forms exist. That is, one starts with a modular form, and then proves the existence of at least one congruent modular form. The goal of this dissertation is to count the number of congruent modular forms when at least one is known to exist. We will begin by giving some basic definitions (following [2]) and examples, which will serve to motivate our main results.

The group $\mathrm{SL}_2(\mathbf{Z})$ acts on the complex upper half plane by linear fractional transformation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+b},$$

where Im(z) > 0. Now, let $N > 0$ be an integer and let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$ be the subset of 2×2 matrices whose lower left hand entry is divisible by N.

Definition 1.1. Let k be a positive even integer. A *modular form* of weight k and level N is a holomorphic function on the upper half plane satisfying:

1. $f(\gamma \cdot z) = (cz+d)^k f(z)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, and

2. for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z})$, the function $(cz+d)^{-k} f(\gamma \cdot z)$ has a series expansion

$$\sum_{n=0}^{\infty} a_n q^{n/h},$$

where $q = e^{2\pi i z}$, for some h. This expansion is called the Fourier series at the cusp $\gamma(i\infty)$.

In what follows, we will be interested in the case when $\gamma = \mathrm{Id}$, that is, in the Fourier series of f at $i\infty$. We will refer to the coefficients in this series as the *Fourier coefficients of* f. If the constant coefficient $a_0 = 0$ for all γ, then we call f a *cuspform*. We will denote by $S_k(\Gamma_0(N))$ the space of all cuspforms of weight k and level N.

Example 1.2. Let $f(z)$ be the function defined by

$$f(z) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2,$$

where $q = e^{2\pi i z}$. This is a cusp form of weight 2 and level 11. Moreover, for p a prime number, the pth Fourier coefficient of f is closely related to the number of $\mathbb{F}_p$-valued points of the elliptic curve

$$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20;$$

we have that $a_p(f) = p + 1 - \#E(\mathbb{F}_p)$. For small primes p, the Fourier coefficients $a_p(f)$ are listed in Table 1.

It is natural to ask if one can find a canonical basis for the space of cuspforms $S_k(\Gamma_0(N))$. To do this we need to introduce a family of commuting operators, called *Hecke* operators.

Definition 1.3. Let $f = \sum a_n(f)q^n$ be a cuspform in $S_k(\Gamma_0(N))$, and let p be a prime number. The pth Hecke operator, T_p, is given by[1]

$$T_p(f) = \begin{cases} \sum_{p|n} a_n(f)q^{n/p} + p^{k-1}\sum a_n(f)q^{pn} & \text{if } p \nmid N \\ \sum_{p|n} a_n(f)q^{n/p} & \text{if } p \mid N. \end{cases}$$

It is a fact that for p and q distinct prime numbers, we have that $T_pT_q = T_qT_p$. Thus, to define the Hecke operators for all positive integers, we need only do it for prime powers. Accordingly, for a positive integer r, we define the p^rth Hecke operator by

$$T_{p^r} = \begin{cases} T_pT_{p^{r-1}} - p^{k-1}T_{p^{r-2}} & \text{if } p \nmid N \\ (T_p)^r & \text{if } p \mid N. \end{cases}$$

Thus, if n is any positive integer, we define the nth Hecke operator by

$$T_n = \prod_i T_{p_i^{e_i}},$$

where $n = \prod p_i^{e_i}$.

Definition 1.4. A nonzero cuspform $f \in S_k(\Gamma_0(N))$ is called a *normalized eigenform* if f is a simultaneous eigenform for all Hecke operators T_n and $a_1(f) = 1$. It is a standard fact that the Fourier coefficients of a normalized eigenform are algebraic integers.

The following theorem is due to Atkin and Lehner (see [1]).

Theorem 1.5. *There is a basis of $S_k(\Gamma_0(N))$ of normalized eigenforms.*

Example 1.6. Consider the cusp form

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n,$$

[1]Some authors use the notation U_p for the pth Hecke operator when $p \mid N$.

where $q = e^{2\pi iz}$. This is the unique normalized eigenform of weight 12 and level 1.[2] At first glance, the cuspform f from Example 1.2 and Δ seem to be unrelated. However, by looking at Table 1, one can see directly that $\tau(p) \equiv a_p(f) \bmod 11$ for small values of p. It turns out that this congruence is true for all primes p and that Δ is the unique modular form of weight 12 and level dividing 11 which satisfies this property.

p	2	3	5	7	11	13	17	19
$a_p(f)$	-2	-1	1	-2	1	4	-2	0
$\tau(p)$	-24	252	4830	-16744	534612	-577738	-6905934	10661420
$a_p(g)$	1	-1	-2	4	1	-2	-2	0

Table 1: Fourier coefficients of f, Δ, and g.

Definition 1.7. Let f and g be two normalized eigenforms (possibly of different weights and levels). Let K be a number field which contains all the Fourier coefficients of both f and g, and let $\wp$ be a prime ideal in the ring of integers, $\mathcal{O}_K$. We call f and g *congruent* modulo $\wp$ if

$$a_\ell(f) \equiv a_\ell(g) \bmod \wp,$$

for all but finitely many prime numbers ℓ.

In the previous example, we saw a congruence between modular forms of different weights. Hida proved the following theorem ([9]) which explains this example in general.

Theorem 1.8. *Suppose that f is a normalized eigenform in $S_k(\Gamma_0(N))$. Let K be a number field containing the Fourier coefficients of f, and let $\wp$ be a prime of K*

[2] In fact, Hecke operators were initially developed to gain a better understanding the Fourier coefficients $\tau(n)$.

lying above p. If $a_p(f)$ is a $\wp$-adic unit,[3] *then, for all $j \geq 1$, there is a normalized eigenform, g_j, of weight j and level dividing Np such that f is congruent to g_j modulo a prime above $\wp$.*

The next theorem addresses congruences between two cuspforms of different levels. It is due to Ribet [25] and Diamond-Taylor [4].

Theorem 1.9. *Suppose that $f \in S_2(\Gamma_0(N))$ and $p \nmid N$ is a prime number. For all prime numbers $q \nmid N$, there exists a cuspform $g \in S_2(Nq)$ such that f and g are congruent modulo (a prime above) p if and only if $a_q(f)^2 \equiv (q+1)^2 \bmod p$.*

Example 1.10. Let f be the cuspform in Example 1.2. We see that $a_3(f) = -1$ and so $a_3(f)^2 \equiv (3+1)^2 \bmod 3$. Consequently, there is a cuspform of weight 2 and level 33 congruent to f modulo 3. Let g be such a cuspform. Then g corresponds to the elliptic curve

$$A = X_0(33) : y^2 + xy = x^3 + x^2 - 11x,$$

in the sense that for all primes p, we have that $a_p(g) = p + 1 - \#A(\mathbb{F}_p)$. For small values of p, one can check that $a_p(f) \equiv a_p(g) \bmod 3$ in Table 1. Moreover, since $S_2(\Gamma_0(33))$ is one-dimensional (over $\mathbb{C}$), g is the unique form of weight 2 and level 33 with this property.

Example 1.11. Consider instead $a_{29}(f) = 0$. Then, as $a_{29}(f)^2 \equiv (29+1)^2 \bmod 3$, there is at least one cuspform in $S_2(\Gamma_0(319))$ (note that $319 = 11 \times 29$) congruent to f modulo 3. However, the space $S_2(\Gamma_0(319))$ has dimension 23 over $\mathbb{C}$, so could there be more than one?

According to the Modular Forms Database ([28]), there exist cuspforms $h_1, h_2 \in S_2(\Gamma_0(319))$ whose Fourier coefficients generate number fields of degrees 3 and 7,

[3] This is the condition that f be *ordinary* at p.

respectively (actually, we have only chosen these forms up to Galois conjugacy here, but we ignore that for the time being). The first few Fourier coefficients of h_1 and h_2 satisfy the polynomials $s_p(x)$ and $t_p(x)$, respectively, that are listed in Tables 2 and 3.

Let α be a root of the polynomial $s_2(x) = x^3 - 3x - 1$ and set $K = \mathbf{Q}(\alpha)$. Then h_1 is defined over K, since all of the Fourier coefficients generate a degree 3 extension which must contain K (if we take a different root α', we are getting a Galois conjugate form). Using SAGE, one can check that the ideal $3\mathcal{O}_K$ factors as $(-\alpha^2+1)^3$. In particular, 3 is totally ramified in K and, if we let $\wp = (-\alpha^2+1)$, then $\mathcal{O}_K/\wp = \mathbb{F}_3$. Therefore, to check for a congruence modulo $\wp$ with h_1, we need only consider the roots of the polynomials $s_p(x)$ in $\mathbb{F}_3$! A simple check shows that for small p, we have that $s_p(a_p(f)) \equiv 0 \bmod 3$ (this is the third column of Table 2). In fact, this holds all primes except 29, and thus, $h_1 \equiv f \bmod \wp$.

Let β be a root of the polynomial $t_2(x) = x^7 - 3x^6 - 4x^5 + 15x^4 + x^3 - 14x^2 + 1$, and let $L = \mathbf{Q}(\beta)$. Then, as above, h_2 is defined over L, since all of its Fourier coefficients generate a degree 7 extension which must contain L (again, if we take a different root, we are getting a Galois conjugate form). The ideal $3\mathcal{O}_L$ factors as $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, with

- $\mathfrak{p}_1 = (3, \beta^2 - 2)$,
- $\mathfrak{p}_2 = (3, \beta^4 - 2\beta^3 - 4\beta^2 + 5t + 2)$, and
- $\mathfrak{p}_3 = (3, \beta - 1)$.

These primes have residual degrees 2, 4 and 1 respectively. Since we are looking for a congruence with f, whose Fourier coefficients are defined over $\mathbf{Z}$, we will work with $\mathfrak{p}_3$. Now we are in the exact same situation as before. We need only check

that $t_p(a_p(f)) \equiv 0 \bmod 3$. For small p, this is the third column of Table 3. Again, this holds for all primes except 29, and so $h_2 \equiv f \bmod \mathfrak{p}_3$.

p	$s_p(x)$	$s_p(a_p(f))$
2	$x^3 - 3x - 1$	-3
3	$x^3 - 3x + 1$	3
5	$x^3 + 6x^2 + 3x - 19$	-9
7	$x^3 + 3x^2 - 9x - 19$	3
11	$x^3 - 3x^2 + 3x - 1$	0
13	$x^3 + 6x^2 + 3x - 19$	153
17	$x^3 + 12x^2 + 45x + 53$	3
19	$x^3 + 12x^2 + 45x + 51$	51

Table 2: Minimal polynomials of the Fourier coefficients of h_1.

p	$t_p(x)$	$t_p(a_p(f))$
2	$x^7 - 3x^6 - 4x^5 + 15x^4 + x^3 - 14x^2 + 1$	-15
3	$x^7 - 17x^5 + 3x^4 + 78x^3 - 8x^2 - 96x + 16$	45
5	$x^7 - 4x^6 - 14x^5 + 59x^4 + 36x^3 - 225x^2 + 81x + 81$	15
7	$x^7 - x^6 - 25x^5 + 9x^4 + 136x^3 - 56x^2 - 152x + 16$	-240
11	$x^7 - 7x^6 + 21x^5 - 35x^4 + 35x^3 - 21x^2 + 7x - 1$	0
13	$x^7 - 51x^5 + 57x^4 + 440x^3 - 768x^2 - 152x + 464$	-5520
17	$x^7 - 18x^6 + 110x^5 - 241x^4 + 50x^3 + 167x^2 - 87x + 9$	-8205
19	$x^7 - 10x^6 - 42x^5 + 631x^4 - 524x^3 - 8961x^2 + 23681x - 11805$	-11805

Table 3: Minimal polynomials of the Fourier coefficients of h_2.

Considering Examples 1.6, 1.10, and 1.11 leads to the following general questions: Given a fixed normalized eigenform $f \in S_k(\Gamma_0(N))$ and a fixed prime p, for which weights j is there a *unique* normalized eigenform g_j congruent to f modulo p? Similarly, for which primes q is there a *unique* normalized eigenform $h_q \in S_k(\Gamma_0(Nq))$ such that h_q is congruent to f modulo p? Of course, Theorems 1.8 and 1.9 tell us when at least one congruent form exists. We are interested in counting the number of such forms when at least one is known to exist.

Theorem A. *Let $f \in S_k(\Gamma_0(N))$ and let p be a prime such that*

1. *f is ordinary at p;*
2. *N is not divisible by any primes that are congruent to 1 modulo p; and*
3. *f is not congruent to any other modular forms modulo any prime above p.*

Then, for all $j \geq 1$, there is a unique normalized eigenform of weight j and level dividing Np which is congruent to f modulo a prime above p.

Theorem B. *Let $f, g \in S_2(\Gamma_0(N))$ be given such that $a_\ell(f) \equiv a_\ell(g) \bmod \wp$ for all but finitely many ℓ. Suppose that f is not congruent to an Eisenstein series modulo $\wp$. Then, there exist Chebotarev sets of prime numbers $\mathfrak{Q}$ and $\mathfrak{L}$ such that:*

1. *For all $q \in \mathfrak{Q}$, there is a unique normalized eigenform in the new subspace of $S_2(\Gamma_0(Nq))$ which is congruent to f modulo a prime above p;*
2. *For all $\ell \in \mathfrak{L}$, there are at least two distinct normalized eigenforms (possibly Galois conjugate) in the new subspace of $S_2(\Gamma_0(N\ell))$ that are congruent to f modulo a prime above p;*
3. *For all but finitely many $q \in \mathfrak{Q}$, there exist infinitely many $\ell \in \mathfrak{L}$ such that there are at least two distinct normalized eigenforms (possibly Galois conjugate) in $S_2(\Gamma_0(Nq\ell))$, new at both q and ℓ, that are congruent to f modulo a prime above p; and*
4. *For all but finitely many $q \in \mathfrak{Q}$, there exist infinitely many $\ell \in \mathfrak{L}$ such that there is a unique normalized eigenform in $S_2(\Gamma_0(Nq\ell))$, new at both q and ℓ, that is congruent to f modulo a prime above p.*

1.2 Ranks of Hecke Rings

We start with a brief overview of how we plan to count congruent cuspforms. See sections 1.6 and 4.1 of [2] for the details of the ideas here. Let $\mathbf{T}_{\mathbf{Z}} \subseteq \mathrm{End}(S_k(\Gamma_0(N)))$ be the ring generated over $\mathbf{Z}$ by the Hecke operators T_n acting on the space of cuspforms of weight k and level N. It is well known that $\mathbf{T}_{\mathbf{Z}}$ is a finitely generated $\mathbf{Z}$-module. Let $\mathcal{O}$ be the ring of integers of a p-adic field K, and let $\mathbf{k}$ be the residue field of $\mathcal{O}$. Now consider $\mathbf{T}_{\mathcal{O}} = \mathbf{T}_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathcal{O}$; it is free of finite rank over $\mathcal{O}$. Since $\mathcal{O}$ is a complete local ring, we have a decomposition

$$\mathbf{T}_{\mathcal{O}} = \prod_{\mathfrak{m}} \mathbf{T}_{\mathfrak{m}},$$

where the product runs over the maximal ideals $\mathfrak{m} \subset \mathbf{T}_{\mathcal{O}}$. Each localization $\mathbf{T}_{\mathfrak{m}}$ is a complete, local $\mathcal{O}$-algebra, free of finite rank over $\mathcal{O}$. The maximal ideals $\mathfrak{m}$ are in one-to-one correspondence with $\mathrm{Gal}(\bar{\mathbf{k}}/\mathbf{k})$-conjugacy classes of normalized eigenforms in $S_k(\Gamma_0(N), \mathbf{Z}) \otimes_{\mathbf{Z}} \bar{\mathbf{k}}$.[4]

If $\mathbf{T}_K = \mathbf{T}_{\mathbf{Z}} \otimes_{\mathbf{Z}} K$, then

$$\mathbf{T}_{\mathfrak{m}} \otimes_{\mathcal{O}} K \simeq \prod_{\wp} \mathbf{T}_{K,\wp},$$

where the product runs over the maximal ideals $\wp \subseteq \mathbf{T}_K$ lying over $\mathfrak{m}$. The maximal ideals of $\mathbf{T}_K$ are in one-to-one correspondence with $\mathrm{Gal}(\bar{K}/K)$-conjugacy classes of normalized eigenforms in $S_k(\Gamma_0(N), \mathbf{Z}) \otimes_{\mathbf{Z}} \bar{K}$.

From this, we conclude that if f and g are cuspforms in $S_k(\Gamma_0(N), \mathcal{O})$ and satisfy $a_\ell(f) \equiv a_\ell(g) \bmod \mathfrak{m}_{\mathcal{O}}$ for almost all primes ℓ, then $\mathrm{rank}_{\mathcal{O}} \mathbf{T}_{\mathfrak{m}} > 1$, where $\mathfrak{m}$ is the maximal ideal associated to the $\mathrm{Gal}(\bar{k}/k)$-conjugacy class of f (and g). When $\mathfrak{m}$ is the Eisenstein ideal (used for measuring congruences between cuspforms

[4] Using Theorem 1.5, one can show that there is a basis of $S_2(\Gamma_0(N))$ consisting of forms with integral Fourier coefficients. We denote by $S_2(\Gamma_0(N), \mathbf{Z})$ the $\mathbf{Z}$-span of this basis.

and Eisenstein series), Mazur posed the question, "Is there anything general that can be said about [this rank]?" ([18], p. 140) Here, we explore this question for congruences between two cuspforms.

One can carry out an entirely analogous analysis for Λ-adic modular forms. Let $h^0(N, \mathcal{O})$ be Hida's ordinary Hecke ring ([9],[10], or Section 2 of [5] for an overview), generated over $\Lambda = \mathcal{O}[[T]]$ by the Hecke operators acting on the space of ordinary Λ-adic modular forms. This ring is free of finite rank over Λ. Thus, we again obtain a decomposition

$$h^0(N, \mathcal{O}) = \prod_{\mathfrak{m}} h^0(N, \mathcal{O})_{\mathfrak{m}},$$

where each localization $h^0(N, \mathcal{O})_{\mathfrak{m}}$ is a complete local Λ-algebra, free of finite rank over Λ. As before, we see that if two ordinary Λ-adic modular forms are congruent modulo $\mathfrak{m}$, then we have that $\operatorname{rank}_{\Lambda} h^0(N, \mathcal{O})_{\mathfrak{m}} > 1$.

The main results of this dissertation involve studying the ranks of these completed Hecke rings as we vary the weight or the level. As such, we aim to prove the following theorems, from which Theorems A and B follow immediately.

Theorem A′. *Let $f \in S_k(\Gamma_0(N), \mathcal{O})$ and let p be a prime such that*

1. *f is ordinary at p;*
2. *N is not divisible by any primes that are congruent to 1 modulo p; and*
3. *$\bar{\rho}_f$ is absolutely irreducible.*

Let $\mathfrak{m} \subset \mathbf{T}_{\mathcal{O}}$ be the maximal ideal corresponding to f, and $\mathfrak{m}_H \subset h^0(N, \mathcal{O})$ be the maximal ideal corresponding to the Λ-adic modular form associated to f. If $\mathbf{T}_{\mathfrak{m}}$ has rank one as an $\mathcal{O}$-module, then $h^0(N, \mathcal{O})_{\mathfrak{m}_H}$ has rank one as an $\mathcal{O}[[T]]$-module.

Theorem B′. *Let $f, g \in S_2(\Gamma_0(N), \mathcal{O})$ be given such that $a_\ell(f) \equiv a_\ell(g) \bmod \mathfrak{m}_\mathcal{O}$ for all but finitely many ℓ. Suppose that the residual representation $\bar{\rho}_f$ is absolutely irreducible. Then, there exist Chebotarev sets of prime numbers $\mathfrak{Q}$ and $\mathfrak{L}$ such that,*

1. $\operatorname{rank}_\mathcal{O} \mathbf{T}_{Nq}^{q-new} = 1$ *for all* $q \in \mathfrak{Q}$;
2. $\operatorname{rank}_\mathcal{O} \mathbf{T}_{N\ell}^{\ell-new} > 1$ *for all* $\ell \in \mathfrak{L}$;
3. *For all but finitely many* $q \in \mathfrak{Q}$, *there exist infinitely many* $\ell \in \mathfrak{L}$ *such that* $\operatorname{rank}_\mathcal{O} \mathbf{T}_{Nq\ell,\mathfrak{m}}^{q,\ell-new} > 1$; *and*
4. *For all but finitely many* $q \in \mathfrak{Q}$, *there exist infinitely many* $\ell \in \mathfrak{L}$ *such that* $\operatorname{rank}_\mathcal{O} \mathbf{T}_{Nq\ell,\mathfrak{m}}^{q,\ell-new} = 1$,

where the superscripts '$q-new$' and '$q,\ell-new$' denote the quotients which act faithfully on cuspforms which are new at the prime q and at the primes q and ℓ, respectively.

1.3 Selmer Groups

If $f, g \in S_k(\Gamma_0(N), \mathcal{O})$ satisfy $a_\ell(f) \equiv a_\ell(g) \bmod \mathfrak{m}_\mathcal{O}$, then the Brauer-Nesbitt Theorem shows that the residual representations $\bar{\rho}_f$ and $\bar{\rho}_g$ are equivalent (see Theorem 2.4.6 and Remark 2.4.7 of [31]). Thus, to prove Theorems A′ and B′, we will start with a residual Galois representation and study its deformation theory.

Let S be a finite set of primes containing $\{p, \infty\}$ and G_S be the Galois group over $\mathbf{Q}$ of the maximal algebraic extension of $\mathbf{Q}$ unramified outside S. Suppose that $\mathbf{k}$ is a field of characteristic p and $\bar{\rho} : G_S \to \mathrm{GL}_2(\mathbf{k})$ is a continuous, odd, absolutely irreducible representation with determinant equal to a finite order character times a

power of the mod p cyclotomic character. By the work of Khare and Wintenberger ([12], [13], [14]) on Serre's conjecture ([27]), such a representation is necessarily modular.

Associated to such a Galois representation, there is a universal deformation ring, R_S, and a universal deformation $\rho_S \colon G_S \to \mathrm{GL}_2(R_S)$. It is well known that R_S is a compact local Noetherian algebra over the ring of Witt vectors of $\mathbf{k}$, $W(\mathbf{k})$. We study how the $W(\mathbf{k})$-rank of such deformation rings vary in two different settings. First, we consider deformations where the set S remains constant, but the determinant of the deformation can vary. This corresponds to Theorem A$'$ and the varying weight case. Second, we consider deformations where we vary the set S but fix the determinant of all deformations. This corresponds to Theorem B$'$ and the varying level case. In both cases, this is accomplished by studying the dimensions of certain Selmer groups.

Let $\mathrm{Ad}^0(\bar{\rho})$ be the 2×2 trace zero matrices over $\mathbf{k}$ with Galois acting via $\bar{\rho}$ and conjugation. A Selmer group is the kernel of a restriction map

$$H^1(G_S, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))}{\mathcal{M}_v}$$

for some collection of subspaces $\{\mathcal{M}_v \subseteq H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))\}$. Associated to such a collection (called a set of local conditions), there is a universal deformation ring, $R_{\mathcal{M}}$, parameterizing all deformations to compact local Noetherian $W(\mathbf{k})$-algebras which 'satisfy' these local conditions.

The connection between modular forms and deformation theory comes from an appropriate choice of local conditions. Indeed, the local conditions in this work are chosen for the express purpose of considering only deformations of $\bar{\rho}$ which come from modular forms. In this case, we get an isomorphism $R_{\mathcal{M}} \simeq \mathbf{T}_{\mathfrak{m}}$, where

$\mathfrak{m}$ is the maximal ideal associated to the modular form giving rise to $\bar{\rho}$. Thus, in this dissertation, we are using the full strength of the modularity results of Wiles, Taylor-Wiles, Kisin, et al. In particular, we see that studying the ranks of deformation rings is equivalent to studying ranks of Hecke rings!

Our task then becomes finding a method for studying the rank of a deformation ring. It is a standard fact that the deformation ring corresponding to a set of local conditions is a quotient of a power series ring over $W(\mathbf{k})$ in d variables, where d is the dimension of the associated Selmer group. Thus, if we could just determine the generators of the defining idea, we would know the rank. This is a difficult question in general. However, it is known that completed Hecke rings are finite flat complete intersections; that is,

$$\mathbf{T}_{\mathfrak{m}} \simeq \mathcal{O}[[X_1, \ldots X_d]]/(f_1, \ldots, f_d)$$

Thus, with the appropriate choice of local conditions, our deformation ring is also a finite flat complete intersection. Thus, by studying when the Selmer group is either trivial or one dimensional (as we vary the weight or level we consider), we can determine when the rank of the deformation ring (and hence the Hecke ring) is one or larger than one.

CHAPTER 2

RECOLLECTIONS

For the remainder of this work, we fix a prime number $p \geq 3$, a finite field $\mathbf{k}$ of characteristic p, and a totally real number field F satisfying the following technical hypotheses:

1. F is linearly disjoint from $\mathbf{Q}(\mu_p)$, the field of pth roots of unity, over $\mathbf{Q}$ (This is required so that we can apply the results of [6], and [22]), and
2. the $\bar{\chi}$-eigenspace of the class group of $F(\mu_p)$ is trivial (this is required in the proof of Lemma 3.9).

It is worth mentioning that $F = \mathbf{Q}$ satisfies both of these hypotheses for all prime numbers. For all places v of $\mathbf{Q}$, we fix once and for all an embedding $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_v$, and will view any subfield of $\bar{\mathbf{Q}}$ as a subfield of $\bar{\mathbf{Q}}_v$ by this embedding. We denote by χ the p-adic cyclotomic character and by $\bar{\chi}$ the reduction of χ modulo p.

We also fix a finite set of places of F, S, which contains all of those dividing the rational p and ∞. Let $G_{F,S}$ be the Galois group of the maximal extension of F which is unramified outside the primes in S. Fix an absolutely irreducible, totally odd, continuous representation $\bar{\rho}\colon G_{F,S} \to \mathrm{GL}_2(\mathbf{k})$ that is modular (in the sense that $\bar{\rho}$ is the reduction of a p-adic representation attached to a Hilbert modular eigenform of parallel weight k). We assume throughout that $\mathrm{SL}_2(\mathbf{k}) \subseteq \mathrm{Im}(\bar{\rho})$. In particular this implies that the trace-zero adjoint of $\bar{\rho}$, $\mathrm{Ad}^0\,\bar{\rho}$, is absolutely irreducible and that $\mathbf{k}$ is the minimal field of definition for both the representation $\bar{\rho}$ and $\mathrm{Ad}^0\,\bar{\rho}$ (see Lemma 17 of [23]).

Many of the background results in this section as well as some of the preliminary results of Chapters 3 and 4 are true in more generality. However, the main results do require these assumptions, so we carry them throughout.

2.1 Galois Cohomology and Selmer Groups

We begin by recalling some basic ideas from Galois cohomology; two good references are [20] and [21]. All of our Galois modules will be finite dimensional $\mathbf{k}$-vector spaces, and hence annihilated by p (as such, we do not note this specifically in the hypotheses of any of the results below). Consequently, all of the cohomology groups $H^i(G, M)$ (where G is some Galois group) we deal with will also be $\mathbf{k}$-vector spaces. Finally, denote by $M(j)$, the Galois module M where the Galois action is twisted by $\bar{\chi}^j$.

Lemma 2.1. *For any G_F-module M, we have an isomorphism*

$$M^* := \mathrm{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p(1)) \simeq \mathrm{Hom}_{\mathbf{k}}(M, \mathbf{k}(1))$$

of G_F modules.

Proof. This is Proposition 32 of [8]. □

Definition 2.2. For a place v of F let G_v denote $\mathrm{Gal}(\bar{F}_v/F_v)$, and, if v is a finite place, $I_v \subset G_v$ the inertia subgroup and Frob_v the Frobenius element which topologically generates G_v/I_v. For a G_v-module M, denote the image of the inflation map

$$H^1(G_v/I_v, M^{I_v}) \to H^1(G_v, M)$$

by $H^1_{nr}(G_v, M)$. If $M^{I_v} = M$, then we will call M an *unramified* G_v-module.

Lemma 2.3. *Let v be a finite place of F; then*

$$\#H^1_{nr}(G_v, M) = \#H^0(G_v, M).$$

Proof. This is Lemma 1 of [30]. □

Theorem 2.4 (Tate's Local Duality)**.** *Let v be a finite place of F and M a G_v-module. Then $H^i(G_v, M)$ is finite for all i, and*

1. *For $i = 0, 1, 2$, the cup product induces a perfect pairing*

$$\mathrm{inv}_v \colon H^i(G_v, M) \times H^{2-i}(G_v, M^*) \to H^2(G_v, \mathbf{k}(1)) \simeq \mathbf{k};$$

2. *If $v \nmid p$ and M is an unramified G_v-module, then the groups $H^1_{nr}(G_v, M)$ and $H^1_{nr}(G_v, M^*)$ are exact annihilators of one another under the pairing in (1); and*

3. *There is a local Euler characteristic where*

   (a) $\#H^1(G_v, M) = \#H^0(G_v, M)\#H^2(G_v, M)$ if $v \nmid p$, or

   (b) $\#H^1(G_v, M) = \#H^0(G_v, M)\#H^2(G_v, M)p^{[F_v:\mathbf{Q}_p]v_p(\#M)}$ if $v \mid p$.

Proof. See Chapter 1, Section 2 of [20]. □

Note. The perfect pairing (1) is usually taken to have values in $H^2(G_v, \mu_p) = H^2(G_v, \mathbb{F}_p(1)) \simeq \mathbb{F}_p$. In light of Lemma 2.1, however, we can take this pairing to be a $\mathbf{k}$-vector space pairing.

The following is a restatement of Lemma 3 from [23].

Lemma 2.5. *Let M be a $\mathbf{k}[G_v]$-module. Then $H^2(G_v, M) \neq 0$ if and only if M has a one-dimensional (as a $\mathbf{k}$-vector space) quotient by a G_v-stable subspace on which G_v acts by $\bar{\chi}$.*

Proof. By local duality, $H^2(G_v, M) \neq 0$ if and only if $H^0(G_v, M^*) \neq 0$. But $H^0(G_v, M^*) = (M^*)^{G_v} \neq 0$ if and only if M^* has a one-dimensional G_v-stable subspace. Such a subspace of M^* corresponds to a quotient of M on which G_v acts by $\bar{\chi}$. □

Definition 2.6. Let M be a $G_{F,S}$-module, and suppose that for each $v \in S$, we have a subgroup $\mathcal{M}_v \subseteq H^1(G_v, M)$. A collection of such subgroups will be called a set of *local conditions*. Denote by $\mathcal{M}_v^\perp$ the annihilator of $\mathcal{M}_v$ under the pairing in Theorem 2.4 (1); the kernels

$$H^1_{\mathcal{M}}(G_{F,S}, M) := \mathrm{Ker}\left(G_{F,S} \to \bigoplus_{v \in S} \frac{H^1(G_v, M)}{\mathcal{M}_v}\right),$$

and

$$H^1_{\mathcal{M}^\perp}(G_{F,S}, M^*) := \mathrm{Ker}\left(G_{F,S} \to \bigoplus_{v \in S} \frac{H^1(G_v, M^*)}{\mathcal{M}_v^\perp}\right)$$

are called the *Selmer* and *dual Selmer* groups, respectively.

The following theorem is due to Wiles (Proposition 1.6 of [32]). It gives us a way to measure the relative size of the Selmer and dual Selmer groups. Recall that the set S contains all of the archimedean primes of F.

Theorem 2.7. *For a set of local conditions $\{\mathcal{M}_v\}_{v \in S}$, we have that*

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

2.2 Deformation Theory

We now give a short introduction to the deformation theory of Galois representations; two good references are [7] and [19].

Let G be either $G_{F,S}$ or G_v, and $\bar{\rho}\colon G \to \mathrm{GL}_2(\mathbf{k})$ be a continuous representation. Let $\mathrm{Ad}\,\bar{\rho}$ denote the adjoint representation of $\bar{\rho}$: the underlying space is the set of 2-by-2 matrices over $\mathbf{k}$, and the G-action is given by conjugation via $\bar{\rho}$. Let $\mathcal{C}$ be the category whose objects are Artinian, local $W(\mathbf{k})$-algebras with residue field $\mathbf{k}$ and whose morphisms are local $W(\mathbf{k})$-algebra homomorphisms which induce the identity on $\mathbf{k}$.

Definition 2.8. Let R be an object of $\mathcal{C}$. A *lift* of $\bar{\rho}$ is a homomorphism $\rho\colon G \to \mathrm{GL}_2(R)$ such that $\rho \equiv \bar{\rho} \bmod \mathfrak{m}_R$, where $\mathfrak{m}_R$ is the maximal ideal of R. Two lifts ρ_1 and ρ_2 to R are *strictly equivalent* if there is a matrix $A \in \mathrm{GL}_2(R)$, congruent to the identity modulo $\mathfrak{m}_R$, such that $\rho_1(\sigma) = A\rho_2(\sigma)A^{-1}$. A *deformation* of $\bar{\rho}$ to R is a strict equivalence class of lifts of $\bar{\rho}$ to R.

The following theorem is due to Mazur. Recall our hypothesis that $\bar{\rho}$ is absolutely irreducible.

Theorem 2.9. *There exists compact, local, Noetherian $W(\mathbf{k})$-algebra with residue field $\mathbf{k}$, R^u, and a homomorphism $\rho^u\colon G \to \mathrm{GL}_2(R^u)$, of $\bar{\rho}$ such that*

1. *The reduction of ρ^u modulo the maximal ideal of R^u gives $\bar{\rho}$; and*
2. *If R is any element of $\mathcal{C}$, and ρ is any deformation of $\bar{\rho}$ to R, then there is a unique, local $W(\mathbf{k})$-algebra morphism inducing the identity on $\mathbf{k}$, $f\colon R^u \to R$, such that $\rho = f \circ \rho^u$ as deformations.*

In other words, the functor $\mathbf{D}\colon \mathcal{C} \to \underline{Sets}$, which assigns to R the set of deformations of $\bar{\rho}$ to R, is pro-representable. Moreover, R^u, is a quotient of $W(\mathbf{k})[[X_1, X_2, \ldots, X_d]]$, where $d = \dim_{\mathbf{k}} H^1(G, \mathrm{Ad}\,\bar{\rho})$.

Note. We will also be interested deformations with fixed determinant. To do this, we note that we simply work with the cohomology of $\mathrm{Ad}^0\,\bar{\rho}$, the set of trace zero matrices under the adjoint action. All of the above goes through identically. In fact, in Chapter 3, we will frequently go between the fixed determinant and non-fixed determinant setting. This is readily done since $\mathrm{Ad}\,\bar{\rho} = \mathrm{Ad}^0\,\bar{\rho} \oplus \mathbf{k}$ as $G_{F,S}$-modules.

Suppose that $G = G_v$ and ρ_n is a deformation of $\bar{\rho}$ to $W(\mathbf{k})/p^n$. Then $H^1(G_v, \mathrm{Ad}\,\bar{\rho})$ acts on the set of deformations of $\bar{\rho}$ to $W(\mathbf{k})/p^{n+1}$ which lift ρ_n. Indeed, if ρ_{n+1} is such a deformation and $f \in H^1(G_v, \mathrm{Ad}\,\bar{\rho})$, then $(I + p^n f)\rho_{n+1}$ is another such deformation.

Suppose that for each $v \in S$ we have a pair $(\mathcal{C}_v, \mathcal{M}_v)$, where $\mathcal{C}_v$ is a collection of deformations of $\bar{\rho}\,|_{G_v}$ to $W(\mathbf{k})/p^n$ (where n varies, and $n = \infty$ is allowed) and $\mathcal{M}_v \subset H^1(G_v, \mathrm{Ad}\,\bar{\rho})$ such that (c.f. Properties P1-P7 of Section 1 of [29])

1. $(\bar{\rho}, \mathbf{k})$ is in $\mathcal{C}_v$;
2. C_v is closed under inverse limits;
3. If $(\rho_n, W(\mathbf{k})/p^n)$ is in C_v, then $(\rho_n \bmod p^r, W(\mathbf{k})/p^r)$ is in $\mathcal{C}_v$ for all $1 \leq r \leq n-1$;
4. For all n, there is some $(\rho_n, W(\mathbf{k})/p^n)$ in $\mathcal{C}_v$; and
5. C_v is closed under the action of $\mathcal{M}_v \subset H^1(G_v, \mathrm{Ad}\,\bar{\rho})$ described in the previous paragraph.

We call such pairs a set of *local deformation conditions*. In the notation of Section 2.1, we have the following analogue of Theorem 2.9.

Theorem 2.10. *Let $\{(\mathcal{C}_v, \mathcal{M}_v)\}$ be a set of local deformation conditions for $\bar{\rho}$. Then there is a universal deformation ring, $R_{\mathcal{M}}$ and a universal deformation*

$\rho_{\mathcal{M}} \colon G_{F,S} \to \mathrm{GL}_2(R_{\mathcal{M}})$, which parameterizes all deformations of $\bar{\rho}$ which are locally in $\mathcal{C}_v$. Moreover, we have that $R_{\mathcal{M}}$ is a quotient of $W(\mathbf{k})[[X_1, \ldots, X_d]]$, where $d = \dim_k H^1_{\mathcal{M}}(G_{F,S}, \mathrm{Ad}\,\bar{\rho})$.

CHAPTER 3

VARYING THE WEIGHT

In this chapter, we aim to establish a deformation theoretic version of Theorem A′. In addition to the hypothesis listed at the start of Chapter 2, we now also assume that:

1. $\bar{\rho}$ is ordinary at all primes above p; that is,

$$\bar{\rho}|_{G_v} = \begin{pmatrix} \bar{\chi}^{k-1}\varphi_v & * \\ 0 & \psi_v \end{pmatrix},$$

   for all primes $v \mid p$, where φ_v and ψ_v are continuous, $\bar{\mathbf{k}}^\times$-valued characters of G_v with ψ_v unramified, and

2. there are no primes in S such that $\mathrm{N}\, v \equiv 1 \bmod p$.

3.1 Fixed Determinant Deformation Conditions

We begin by recalling a collection of local deformation conditions, $\{(\mathcal{C}_v, \mathcal{L}_v)\}$ constructed in [6].

Definition 3.1. Let $\bar{\rho}$ be as above.

1. Suppose that $v \nmid p$, $p \nmid \#\bar{\rho}(I_v)$, and that $\bar{\rho}\,|_{G_v}$ can be put in the form

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

for some ramified character $\varphi_v \colon G_v \to \mathbf{k}^\times$. We will take $\mathcal{C}_v$ to be deformations of the form

$$\begin{pmatrix} \tilde{\varphi}_v \gamma_v & 0 \\ 0 & \gamma_v^{-1} \end{pmatrix},$$

where $\tilde{\varphi}_v$ is the Teichmüller lift of φ_v and $\gamma_v \colon G_v \to W(\mathbf{k})^\times$ is any unramified character. This is equivalent to considering lifts of $\bar{\rho}$ which factor through $G_v/(I_v \cap \operatorname{Ker} \bar{\rho})$. We will take $\mathcal{L}_v = H^1_{nr}(G_v, \operatorname{Ad}^0 \bar{\rho})$.

2. Suppose that $v \mid 2$ and $p = 3$ and that the image of G_v in the projective representation is S_4. We will take $\mathcal{C}_v$ to be the deformations of $\bar{\rho}$ which factor through $G_v/(I_v \cap \operatorname{Ker} \bar{\rho})$ and have determinant χ^{k-1} times a finite order character. We will take $\mathcal{L}_v = H^1_{nr}(G_v, \operatorname{Ad}^0 \bar{\rho})$.

3. Suppose that either

   (a) $v \nmid p$, or

   (b) $v \mid p$ and $k = 2$,

   and that $\bar{\rho}$ can be put in the form

$$\begin{pmatrix} \bar{\chi}^{k-1} \varphi_v & * \\ 0 & \varphi_v \end{pmatrix},$$

   for some character $\varphi_v \colon G_v \to \mathbf{k}^\times$. If $v \mid p$, assume additionally that φ_v is unramified. We will take $\mathcal{C}_v$ to be deformations of the form

$$\begin{pmatrix} \chi^{k-1} \gamma_v & * \\ 0 & \gamma_v \end{pmatrix},$$

   where γ_v is any lift of φ_v (unramified lift, if $v \mid p$). We will take $\mathcal{L}_v$ to be the image of the map

$$H^1(G_v, U^0) \to H^1(G_v, \operatorname{Ad}^0 \bar{\rho}),$$

   where U^0 is the subset of $\operatorname{Ad}^0 \bar{\rho}$ of upper triangular nilpotent elements.

4. Suppose that $v \mid p$ and that we can take $\bar{\rho}\,|_{G_v}$ to be of the form

$$\begin{pmatrix} \bar{\chi}^{k-1}\varphi_v & * \\ 0 & \psi_v \end{pmatrix},$$

where, if $k = 2$, $\varphi_v, \psi_v \colon G_v \to \mathbf{k}^\times$ are *distinct* characters with ψ_v unramified. Assume also that $\chi^{k-1}\varphi_v \neq \psi_v$. We will take $\mathcal{C}_v$ to be deformations of the form

$$\begin{pmatrix} \chi^{k-1}\gamma_v & * \\ 0 & \delta_v \end{pmatrix},$$

where γ_v and δ_v lift φ_v and ψ_v respectively, and δ_v is unramified. We will take

$$\mathcal{L}_v = \mathrm{Ker}(H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}) \to H^1(I_v, \mathrm{Ad}^0\,\bar{\rho}/U^0)).$$

Note. It is a theorem of Diamond, [3], that for $v \nmid p$, a continuous representation $\bar{\rho} \colon G_v \to \mathrm{GL}_2(\mathbf{k})$ will take one of the forms (1), (2), or (3) above when $F = \mathbf{Q}$. The case of general F is Lemma 3.1 of [6].

Lemma 3.2. *For the $\{(\mathcal{C}_v, \mathcal{L}_v)\}$ just described, we have that*

1. *$\{(\mathcal{C}_v, \mathcal{L}_v)\}$ is a set of local deformation conditions for $\bar{\rho}$;*
2. *If $v \nmid p$, then $\#\mathcal{L}_v = \#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})$; and*
3. *If $v \mid p$, then*

$$\#\mathcal{L}_v = \begin{cases} \#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]} & \text{if } p \nmid \#\bar{\rho}(G_v), \\ \#\mathbf{k}^{[F_v:\mathbf{Q}_p]} & \text{if } p \mid \#\bar{\rho}(G_v). \end{cases}$$

In particular, we get that

$$\frac{\#H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} = 1.$$

Proof. The verification of part (1) is more or less immediate, but we will discuss a similar question below in Lemma 3.4. Part (2) follows from the Galois cohomology results in Section 2.1, see [6] for the details. For Part (3), assume first that $p \nmid \#\bar{\rho}(G_v)$. One easily checks that

$$\mathrm{Ad}^0\,\bar{\rho} \simeq \mathbf{k} \oplus \mathbf{k}(\bar{\chi}^{k-1}\varphi_v/\psi_v) \oplus \mathbf{k}(\psi_v/\bar{\chi}^{k-1}\varphi_v) \text{ and } U^0 \simeq \mathbf{k}(\bar{\chi}^{k-1}\varphi_v/\psi_v),$$

as G_v-modules (here we now allow the possibility of $\varphi_v = \psi_v$ so cover both cases (3) and (4) of Definition 3.1). In particular, we have that $H^0(G_v, U^0) = 0$, since, if $\varphi_v \neq \psi_v$, we are assuming that $\bar{\chi}^{k-1}\varphi_v \neq \psi_v$. Additionally, $H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0) = H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0) = \mathbf{k}$. Thus, in the long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G_v, U^0) \longrightarrow H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}) \longrightarrow H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0) \\ \longrightarrow H^1(G_v, U^0) \longrightarrow H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}) \longrightarrow H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0) \\ \longrightarrow H^2(G_v, U^0) \longrightarrow \dots \end{aligned} ,$$

associated to the short exact sequence

$$0 \to U^0 \to \mathrm{Ad}^0 \to \mathrm{Ad}^0/U^0 \to 0,$$

the first row is just

$$0 \to \mathbf{k} \to \mathbf{k}.$$

In particular, this is an isomorphism, so that we get an exact sequence

$$0 \to H^1(G_v, U^0) \to H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}) \to H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0). \tag{3.1}$$

Now, if we are in case (3) of Definition 3.1, then we simply have that $\mathcal{L}_v = H^1(G_v, U^0)$. Applying Lemma 2.5 and Theorem 2.4 we get

$$\#\mathcal{L}_v = \#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]},$$

as desired.

If we are in case (4) of Definition 3.1, then we see that $H^2(G_v, U^0) = 0$ (again by Lemma 2.5), so that the sequence in 3.1 is actually short exact. Next, the exact sequence arising from inflation-restriction,

$$0 \to H^1(G_v/I_v, (\mathrm{Ad}^0\,\bar{\rho}/U^0)^{I_v}) \to H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0) \to H^1(I_v, \mathrm{Ad}^0\,\bar{\rho}/U^0)^{G_v/I_v},$$

is short exact because $G_v/I_v \simeq \hat{\mathbf{Z}}$ has cohomological dimension 1 (see Section 1 of Chapter XIII of [26]). Thus, splicing these two short exact sequences together, and using the exactness of the sequences shows that

$$\begin{aligned}
\#\mathcal{L}_v &= \frac{\#H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})}{\#H^1(I_v, \mathrm{Ad}^0\,\bar{\rho}/U^0)^{G_v/I_v}} \\
&= \frac{\#H^1(G_v, U^0)\#H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0)\#H^1(G_v/I_v, (\mathrm{Ad}^0\,\bar{\rho}/U^0)^{I_v})}{\#H^1(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0)} \\
&= \#H^1(G_v, U^0)\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}/U^0),
\end{aligned}$$

where the last equality follows from Lemma 2.3. Again, using Lemma 2.5 and Theorem 2.4 we get

$$\#\mathcal{L}_v = \#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]},$$

as desired. An entirely analogous argument gives the result when $p \mid \#\bar{\rho}(G_v)$, so we omit the details here (see the proof of Lemma 3.6).

The final statement of the lemma follows from an easy application of Theorem 2.7:

$$\begin{aligned}
\frac{\#H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} &= \frac{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} \prod_{v\in S} \frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})} \\
&= \prod_{v\in S} \frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})},
\end{aligned}$$

since our assumptions force $\mathrm{Ad}^0\,\bar{\rho}$ and $\mathrm{Ad}^0\,\bar{\rho}^*$ to be absolutely irreducible. Now,

since $\#\mathcal{L}_v = \#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})$ for all $v \nmid p$,

$$\prod_{v\in S} \frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})} = \prod_{v|\infty} \frac{1}{\#\mathbf{k}} \prod_{v|p} \frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})},$$

since $\bar{\rho}$ is totally odd. Now, if $p \nmid \#\bar{\rho}(G_v)$, then, as we saw above, $H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}) = \mathbf{k}$. If $p \mid \#\bar{\rho}(G_v)$, then we have that $H^0(G_v, \mathrm{Ad}^0\,\bar{\rho}) = 0$. Thus, in either case we have that

$$\frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})} = \#\mathbf{k}^{[F_v:\mathbf{Q}_p]}.$$

In particular, this gives that

$$\begin{aligned}\frac{\#H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} &= \prod_{v|\infty} \frac{1}{\#\mathbf{k}} \prod_{v|p} \#\mathbf{k}^{[F_v:\mathbf{Q}_p]} \\ &= \#\mathbf{k}^{-[F:Q]+\sum_{v|p}[F_v:\mathbf{Q}_p]} = 1.\end{aligned}$$

□

The following result is due to Ramakrishna, [24], in the case $F = \mathbf{Q}$ and was generalized to totally real fields by Gee, [6].

Theorem 3.3. *Suppose $\bar{\rho}$ satisfies the assumptions at the start of Chapters 2 and 3. For $v \in S$, let $\{(\mathcal{C}_v, \mathcal{L}_v)\}$ be the local deformation conditions defined above. There exists a finite set of places of F, Q, such that, if we take $\{(\mathcal{C}_q, \mathcal{L}_q)\}$ to be as in Definition 3.1 (3) for each $q \in Q$, then $H^1_{\mathcal{L}^\perp}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0$. Consequently, in the notation of Theorem 2.10, $R_{\mathcal{L}} = W(\mathbf{k})$ and there exists a deformation of $\bar{\rho}$, $\rho\colon G_{F,S\cup Q} \to \mathrm{GL}_2(W(\mathbf{k}))$ with determinant a finite order character times χ^{k-1}, such that $\rho\,|_{G_v} \in \mathcal{C}_v$ for all $v \in S \cup Q$. Moreover, since $\bar{\rho}$ is assumed to be modular of parallel weight k, there exists a Hilbert modular form, g, of parallel weight k, such that the representations ρ and ρ_g are equivalent.*

Note. The statement of the theorem in this form is originally due to Taylor, [29]. There, the proof is split into two steps. First, using the Poitou-Tate long exact

sequence, one shows that if $H^1_{\mathcal{L}^\perp}(G_{F,T}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0$ (for some set of primes T containing S), then one can deform $\bar{\rho}$ step-by-step from $W(\mathbf{k})/p^n$ to $W(\mathbf{k})/p^{n+1}$, making sure that the local representation is in $\mathcal{C}_v$ at each step. The next step is to produce the set of primes Q which annihilate the dual selmer group. The set Q is built recursively by repeated applications of the Chebotarev Density Theorem. We note that $\#Q = \dim_{\mathbf{k}} H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)$. The modularity result comes from applying a deep result of Kisin, [15].

Consider the following modified local deformation conditions, which will parameterize deformations which have determinant a finite order character times χ^{j-1}. Throughout, we let ω be the Teichmüller lift of $\bar{\chi}$.

(1′) Suppose that $v \nmid p$, $p \nmid \#\bar{\rho}(I_v)$, and that $\bar{\rho}\,|_{G_v}$ is twist equivalent to

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

We will take $\mathcal{C}_{v,j}$ to be deformations of the form

$$\begin{pmatrix} \chi^{j-1}\omega^{k-j}\tilde{\varphi}_v\gamma_n & 0 \\ 0 & \gamma_v^{-1} \end{pmatrix}.$$

We will take $\mathcal{L}_v$ as in Definition 3.1 (1).

(2′) Suppose that $v \mid 2$ and $p = 3$ and that the image of G_v in the projective representation is S_4. We will take $\mathcal{C}_v$ to be the deformations of $\bar{\rho}$ which factor through $G_v/(I_v \cap \mathrm{Ker}\,\bar{\rho})$ which have determinant $\chi^{j-1}\omega^{k-j}$ times a finite order character. We will take $\mathcal{L}_v$ in Definition 3.1 (2).

(3′) Suppose that either

1. $v \nmid p$, or

2. $v \mid p$ and $k = 2$,

and that $\bar{\rho}$ can be put in the form

$$\begin{pmatrix} \bar{\chi}^{k-1}\varphi_v & * \\ 0 & \varphi_v \end{pmatrix},$$

for some character $\varphi_v \colon G_v \to \mathbf{k}^\times$. If $v \mid p$, assume additionally that φ_v is unramified. We will take $\mathcal{C}_{v,j}$ to be deformations of the form

$$\begin{pmatrix} \chi^{j-1}\omega^{k-j}\gamma & * \\ 0 & \gamma \end{pmatrix}.$$

where γ_v is any lift of φ_v (unramified lift, if $v \mid p$). We will take $\mathcal{L}_v$ to be as in Definition 3.1 (3).

(4′) Suppose that $v \mid p$ and that we can take $\bar{\rho}\,|_{G_v}$ to be of the form

$$\begin{pmatrix} \bar{\chi}^{k-1}\varphi_v & * \\ 0 & \psi_v \end{pmatrix},$$

where $\varphi_v, \psi_v \colon G_v \to \mathbf{k}^\times$ are *distinct* characters with ψ_v unramified. Assume also that $\chi^{k-1}\varphi_v \neq \psi_v$. We will take $\mathcal{C}_{v,j}$ to be deformations of the form

$$\begin{pmatrix} \chi^{j-1}\omega^{k-j}\gamma_v & * \\ 0 & \delta_v \end{pmatrix},$$

where δ_v is unramified. We will take $\mathcal{L}_v$ to be as in Definition 3.1 (4).

Lemma 3.4. *The set $\{(\mathcal{C}_{v,j}, \mathcal{L}_v)\}$ is a set of local deformation conditions for $\bar{\rho}$.*

Proof. In each case, it is clear that $\mathcal{C}_{v,j}$ satisfies the first four properties listed before Theorem 2.10. We will check property (5) here. In case (1′), we have $\mathcal{L}_v = H^1_{nr}(G_v, \mathrm{Ad}^0\,\bar{\rho})$. As $\mathrm{Ad}^0\,\bar{\rho} \simeq \mathbf{k} \oplus \mathbf{k}(\varphi) \oplus \mathbf{k}(\varphi^{-1})$ in this case, we have that

$\mathrm{Ad}^0\,\bar{\rho}^{I_v}$ is just the trace-zero diagonal matrices. Thus, if $f \in \mathcal{L}_v$ and ρ is in $\mathcal{C}_{v,j}$, one sees that $(I + ap^{n-1})\rho_n$ is again in $\mathcal{C}_{v,j}$. In case $(2')$, there is nothing to check since $\mathcal{L}_v = 0$ (see [6]). In case $(3')$, we have that $\mathcal{L}_v$ is the image of $H^1(G_v, U^0) \to H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$. If $[f]$ is in this image, then f takes values in the upper triangular nilpotent matrices. It follows at once that $\mathcal{L}_v$ preserves $\mathcal{C}_{v,j}$. Case $(4')$ follows similarly. □

Since only the class $\mathcal{C}_{v,j}$ of deformations changes when we change the χ-part of the determinant of the deformation (and not the local conditions $\mathcal{L}_v$), the Selmer and dual Selmer groups are unchanged. Thus, we get the following result immediately from Theorem 3.3.

Proposition 3.5. *Suppose $\bar{\rho}$ satisfies the assumptions at the start of Chapters 2 and 3. For $v \in S$, let $\{(\mathcal{C}_{v,j}, \mathcal{L}_v)\}$ be the local deformation conditions defined above. There exists a finite set of places of F, Q, such that, if we take $\{(\mathcal{C}_{q,j}, \mathcal{L}_q)\}$ to be as in $(3')$ for each $q \in Q$, then $H^1_{\mathcal{L}^\perp}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0$. Consequently, in the notation of Theorem 2.10, $R_{\mathcal{L}} = W(\mathbf{k})$ and there exists a deformation of $\bar{\rho}$, $\rho_j \colon G_{F,S\cup Q} \to \mathrm{GL}_2(W(\mathbf{k}))$ with determinant a finite order character times χ^{j-1}, such that $\rho\,|_{G_v} \in \mathcal{C}_{v,j}$ for all $v \in S \cup Q$. Moreover, since $\bar{\rho}$ is assumed to be modular of parallel weight k, there exists a Hilbert modular form, g, of parallel weight j, such that the representations ρ_j and ρ_g are equivalent.*

3.2 Non-fixed Determinant Deformation Conditions

We are now equipped to understand the structure of the non-fixed determinant deformation ring. Recall that this means considering the cohomology of $\mathrm{Ad}\,\bar{\rho}$, as opposed to just that of $\mathrm{Ad}^0\,\bar{\rho}$. The decomposition $\mathrm{Ad}\,\bar{\rho} = \mathrm{Ad}^0\,\bar{\rho} \oplus \mathbf{k}$ gives rise to

a decomposition $H^i(G, \operatorname{Ad}\bar{\rho}) = H^i(G, \operatorname{Ad}^0\bar{\rho}) \oplus H^i(G, \mathbf{k})$, where G is $G_{F,S}$ or G_v for some v. This decomposition will make it easy to define the necessary local conditions $\{(\mathcal{D}_v, \mathcal{N}_v)\}$.

To start, for all v we will take our class of deformations, $\mathcal{D}_v$, to be lifts of the same shape as those of the $\mathcal{C}_v$ in Definition 3.1, but without any restriction on the determinants of the lifts. To define $\mathcal{N}_v$, we simply take $\mathcal{N}_v = \mathcal{L}_v \oplus H^1(G_v, \mathbf{k})$ for v not dividing p. The case of v dividing p is more difficult.

Assume $v \mid p$. Recall that we are assuming that $\bar{\rho}\,|_{G_v}$ is ordinary, in the sense that we may put $\bar{\rho}\,|_{G_v}$ in the form

$$\begin{pmatrix} \bar{\chi}^{k-1}\varphi_v & \beta_v \\ 0 & \psi_v \end{pmatrix},$$

where, $\varphi_v, \psi_v \colon G_v \to \mathbf{k}^\times$ are characters with ψ_v unramified such that $\chi^{k-1}\varphi_v \neq \psi_v$, and $\beta_v \colon G_v \to \mathbf{k}$ is some function. Note that allow $\varphi_v = \psi_v$.

Set $U \subset \operatorname{Ad}\bar{\rho}$ to be the subset of matrices whose bottom row is zero; that is

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right\},$$

which is a G_v-stable submodule of $\operatorname{Ad}\bar{\rho}$ since $\bar{\rho}\,|_{G_v}$ is ordinary.

Suppose first that $k \neq 2$ or $\varphi_v \neq \psi_v$. Then, we will take $\mathcal{N}_v$ to be the kernel of the map

$$H^1(G_v, \operatorname{Ad}\bar{\rho}) \to H^1(I_v, \operatorname{Ad}\bar{\rho})^{G_v/I_v}.$$

When $k = 2$ and $\varphi_v = \psi_v$, we will take $\mathcal{N}_v$ to be the image of the map

$$H^1(G_v, U) \to H^1(G_v, \operatorname{Ad}\bar{\rho}),$$

if $p \nmid \#\bar{\rho}(G_v)$ (equivalently if $\beta_v = 0$), and we will take $\mathcal{N}_v$ to be the kernel of the map

$$H^1(G_v, \operatorname{Ad}\bar{\rho}) \to H^1(I_v, \operatorname{Ad}\bar{\rho})^{G_v/I_v},$$

if $p \mid \#\bar{\rho}(G_v)$ (equivalently if $\beta_v \neq 0$).

Lemma 3.6. *For all $v \mid p$ we have that*

$$\#\mathcal{N}_v = \begin{cases} \#\mathbf{k}^{2+2[F_v:\mathbf{Q}_p]} & \text{if } p \nmid \#\bar{\rho}(G_v) \\ \#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]} & \text{if } p \mid \#\bar{\rho}(G_v). \end{cases}$$

Proof. The proof of this fact is completely analogous to the proof of Lemma 3.2. So, since we showed the case $p \nmid \#\bar{\rho}(G_v)$ there, we will show the case where $p \mid \#\bar{\rho}(G_v)$ here. In this case, we are concerned with the kernel of the map

$$H^1(G_v, \operatorname{Ad}\bar{\rho}) \to H^1(I_v, \operatorname{Ad}\bar{\rho})^{G_v/I_v}.$$

We start by noting that (as in the proof of Lemma 3.2) the inflation-restriction exact sequence

$$0 \to H^1(G_v/I_v, (\operatorname{Ad}\bar{\rho}/U)^{I_v}) \to H^1(G_v, \operatorname{Ad}\bar{\rho}/U) \to H^1(I_v, \operatorname{Ad}\bar{\rho}/U) \tag{3.2}$$

is short exact since $\hat{\mathbf{Z}}$ has cohomological dimension one.

Next, suppose that

$$M = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

is an element of U. Then for σ in G_v, we have that

$$\bar{\rho}(\sigma) M \bar{\rho}(\sigma^{-1}) = M = \begin{pmatrix} a & -\frac{\beta_v(\sigma)}{\psi_v(\sigma)}a + \frac{\bar{\chi}(\sigma)\varphi_v(\sigma)}{\psi_v(\sigma)}b \\ 0 & 0 \end{pmatrix}.$$

Since we are assuming that β is not the zero map, we see immediately that $H^0(G_v, U) = 0$. Moreover, we also get that $H^2(G_v, U) = 0$ by applying Lemma 2.5. Thus, applying Theorem 2.4 shows that

$$\#H^1(G_v, U) = \#\mathbf{k}^{2[F_v:\mathbf{Q}_p]}.$$

A similar argument (that is, writing out the matrix multiplication), shows that $\#H^0(G_v, \operatorname{Ad}\bar{\rho}) = \#\mathbf{k} = \#H^0(G_v, \operatorname{Ad}\bar{\rho}/U)$.

Now, associated to the short exact sequence

$$0 \to U \to \operatorname{Ad}\bar{\rho} \to \operatorname{Ad}\bar{\rho}/U \to 0,$$

we get the usual long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G_v, U) \longrightarrow H^0(G_v, \operatorname{Ad}\bar{\rho}) \longrightarrow H^0(G_v, \operatorname{Ad}\bar{\rho}/U) \\ \to H^1(G_v, U) \longrightarrow H^1(G_v, \operatorname{Ad}\bar{\rho}) \longrightarrow H^1(G_v, \operatorname{Ad}\bar{\rho}/U) \\ \to H^2(G_v, U) \longrightarrow \dots \end{aligned}$$

As we have just seen, however, the first row is just

$$0 \to \mathbf{k} \to \mathbf{k},$$

which is necessarily an isomorphism. Also, we have seen that $H^2(G_v, U) = 0$. In particular, we get a short exact sequence

$$0 \to H^1(G_v, U) \to H^1(G_v, \operatorname{Ad}\bar{\rho}) \to H^1(G_v, \operatorname{Ad}\bar{\rho}/U) \to 0. \tag{3.3}$$

Thus, to compute the order of $\mathcal{N}_v$, it suffices to take the alternating product of the

sums of terms in the sequences (3.2) and (3.3). In particular,

$$\begin{aligned}\#\mathcal{N}_v &= \frac{\#H^1(G_v, \operatorname{Ad}\bar{\rho})}{\#H^1(I_v, \operatorname{Ad}\bar{\rho}/U)^{G_v/I_v}} \\ &= \frac{\#H^1(G_v, U)\#H^1(G_v, \operatorname{Ad}\bar{\rho}/U)\#H^1(G_v/I_v, (\operatorname{Ad}\bar{\rho}/U)^{I_v})}{\#H^1(G_v, \operatorname{Ad}\bar{\rho}/U)} \\ &= \#H^1(G_v, U)\#H^0(G_v, \operatorname{Ad}\bar{\rho}/U),\end{aligned}$$

where the last equality follows from Lemma 2.3. We saw above that

$$\#H^1(G_v, U)\#H^0(G_v, \operatorname{Ad}\bar{\rho}/U) = \#\mathbf{k}^{2[F_v:\mathbf{Q}_p]}\#\mathbf{k},$$

and the result follows. □

In Tables 4, 5, 6, and 7 we have recorded the sizes of several different cohomology groups. The arguments for the sizes of these groups are completely analogous to those given in the proofs of Lemmas 3.2 and 3.6, so we omit the proofs.

M	$\#H^0(G_v, M)$	$\#H^1(G_v, M)$	$\#H^2(G_v, M)$
U^0	1	$\#\mathbf{k}^{[F_v:\mathbf{Q}_p]}$	1
$\operatorname{Ad}^0\bar{\rho}$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+3[F_v:\mathbf{Q}_p]}$	1
$\operatorname{Ad}^0\bar{\rho}/U^0$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1
U	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1
$\operatorname{Ad}\bar{\rho}$	$\#\mathbf{k}^2$	$\#\mathbf{k}^{2+4[F_v:\mathbf{Q}_p]}$	1
$\operatorname{Ad}\bar{\rho}/U$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1

Table 4: Sizes of various cohomology groups when $p \nmid \#\bar{\rho}(G_v)$ and $\varphi_v \neq \psi_v$ or $k \neq 2$

The following corollary is immediate from Lemmas 3.2 and 3.6.

Corollary 3.7. *For all $v \mid p$, we have that*

$$\frac{\#\mathcal{N}_v}{\#\mathcal{L}_v} = \#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]}.$$

M	$\#H^0(G_v, M)$	$\#H^1(G_v, M)$	$\#H^2(G_v, M)$
U^0	1	$\#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]}$	$\#\mathbf{k}$
$\mathrm{Ad}^0\,\bar{\rho}$	$\#\mathbf{k}$	$\#\mathbf{k}^{2+3[F_v:\mathbf{Q}_p]}$	$\#\mathbf{k}$
$\mathrm{Ad}^0\,\bar{\rho}/U^0$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1
U	$\#\mathbf{k}$	$\#\mathbf{k}^{2+2[F_v:\mathbf{Q}_p]}$	$\#\mathbf{k}$
$\mathrm{Ad}\,\bar{\rho}$	$\#\mathbf{k}^2$	$\#\mathbf{k}^{3+4[F_v:\mathbf{Q}_p]}$	$\#\mathbf{k}$
$\mathrm{Ad}\,\bar{\rho}/U$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1

Table 5: Sizes of various cohomology groups when $p \nmid \#\bar{\rho}(G_v)$ and $\varphi_v = \psi_v$ and $k = 2$

M	$\#H^0(G_v, M)$	$\#H^1(G_v, M)$	$\#H^2(G_v, M)$
U^0	1	$\#\mathbf{k}^{[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}^0\,\bar{\rho}$	1	$\#\mathbf{k}^{3[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}^0\,\bar{\rho}/U^0$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1
U	1	$\#\mathbf{k}^{2[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}\,\bar{\rho}$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+4[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}\,\bar{\rho}/U$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1

Table 6: Sizes of various cohomology groups when $p \mid \#\bar{\rho}(G_v)$ and $\varphi_v \neq \psi_v$ or $k \neq 2$

Lemma 3.8. *Let $\{\mathcal{N}_v\}_{v\in S}$ and $\{\mathcal{L}_v\}_{v\in S}$ be as above. Then*

$$\frac{\#H^1_{\mathcal{N}}(G_{F,S}, \mathrm{Ad}\,\bar{\rho})}{\#H^1_{\mathcal{N}^\perp}(G_{F,S}, \mathrm{Ad}\,\bar{\rho}^*)} = \#\mathbf{k}$$

M	$\#H^0(G_v, M)$	$\#H^1(G_v, M)$	$\#H^2(G_v, M)$
U^0	1	$\#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]}$	$\#\mathbf{k}$
$\mathrm{Ad}^0\,\bar{\rho}$	1	$\#\mathbf{k}^{3[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}^0\,\bar{\rho}/U^0$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1
U	1	$\#\mathbf{k}^{2[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}\,\bar{\rho}$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+4[F_v:\mathbf{Q}_p]}$	1
$\mathrm{Ad}\,\bar{\rho}/U$	$\#\mathbf{k}$	$\#\mathbf{k}^{1+2[F_v:\mathbf{Q}_p]}$	1

Table 7: Sizes of various cohomology groups when $p \mid \#\bar{\rho}(G_v)$ and $\varphi_v = \psi_v$ and $k = 2$

Proof. By Theorem 2.7, we have that

$$\begin{aligned}
\frac{\#H^1_{\mathcal{N}}(G_{F,S}, \mathrm{Ad}\,\bar{\rho})}{\#H^1_{\mathcal{N}^\perp}(G_{F,S}, \mathrm{Ad}\,\bar{\rho}^*)} &= \frac{\#H^0(G_{F,S}, \mathrm{Ad}\,\bar{\rho})}{\#H^0(G_{F,S}, \mathrm{Ad}\,\bar{\rho}^*)} \prod_{v\in S} \frac{\#\mathcal{N}_v}{\#H^0(G_v, \mathrm{Ad}\,\bar{\rho})} \\
&= \frac{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})\#H^0(G_{F,S}, \mathbf{k})}{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)\#H^0(G_{F,S}, \mathbf{k}(1))} \\
&\quad \times \prod_{v\in S} \frac{\#\mathcal{N}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})\#H^0(G_v, \mathbf{k})} \\
&= \frac{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^0(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} \prod_{v\in S} \frac{\#\mathcal{L}_v}{\#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})} \\
&\quad \times \frac{H^0(G_{F,S}, \mathbf{k})}{H^0(G_{F,S}, \mathbf{k}(1))} \prod_{v\in S} \frac{\#\mathcal{N}_v}{\#\mathcal{L}_v\#H^0(G_v, \mathbf{k})} \\
&= \frac{\#H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})}{\#H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)} \#\mathbf{k} \prod_{v\in S} \frac{\#\mathcal{N}_v}{\#\mathcal{L}_v\#H^0(G_v, \mathbf{k})} \\
&= \#\mathbf{k} \prod_{v\in S} \frac{\#\mathcal{N}_v}{\#\mathcal{L}_v\#H^0(G_v, \mathbf{k})}, \text{ by Lemma 3.2.}
\end{aligned}$$

Now, if $v \mid \infty$, then $\mathcal{N}_v = \mathcal{L}_v = 0$ so that

$$\frac{\#\mathcal{N}_v}{\#\mathcal{L}_v\#H^0(G_v, \mathbf{k})} = \frac{1}{\#H^0(G_v, \mathbf{k})} = \frac{1}{\#\mathbf{k}}.$$

If $v \nmid p\infty$, then, since $\mathcal{N}_v = \mathcal{L}_v \oplus H^1(G_v, \mathbf{k})$, we have that

$$\frac{\#\mathcal{N}_v}{\#\mathcal{L}_v\#H^0(G_v, \mathbf{k})} = \frac{\#H^1(G_v, \mathbf{k})}{\#H^0(G_v, \mathbf{k})} = 1$$

since $\mathrm{N}\,v \not\equiv 1 \bmod p$ and F is disjoint from $\mathbf{Q}(\mu_p)$, by assumption.

Finally, suppose that $v \mid p$. Then, by Corollary 3.7, we have that

$$\frac{\#\mathcal{N}_v}{\#\mathcal{L}_v \# H^0(G_v, \mathbf{k})} = \frac{\#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]}}{\#H^0(G_v, \mathbf{k})} = \#\mathbf{k}^{[F_v:\mathbf{Q}_p]}.$$

Combining all of this gives

$$\begin{aligned}\frac{\#H^1_{\mathcal{N}}(G_{F,S}, \operatorname{Ad}\bar{\rho})}{\#H^1_{\mathcal{N}^\perp}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*)} &= \#\mathbf{k} \prod_{v|\infty} \frac{1}{\#\mathbf{k}} \prod_{v|p} \#\mathbf{k}^{[F_v:\mathbf{Q}_p]} \\ &= \#\mathbf{k}^{1-[F:\mathbf{Q}]+\sum_{v|p}[F_v:\mathbf{Q}_p]} \\ &= \#\mathbf{k},\end{aligned}$$

as desired. □

Our next step is to bound the size of $H^1_{\mathcal{N}^\perp}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*)$ in terms of the size of $H^1_{\mathcal{L}^\perp}(G_{F,S}, \operatorname{Ad}^0\bar{\rho}^*)$.

Lemma 3.9. *Suppose that $\{\mathcal{N}_v\}_{v\in S}$ and $\{\mathcal{L}_v\}_{v\in S}$ are as above. Then we have the containment*

$$H^1_{\mathcal{N}^\perp}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*) \subseteq H^1_{\mathcal{L}^\perp}(G_{F,S}, \operatorname{Ad}^0\bar{\rho}^*) \oplus H^1(G_{F,S}, \mathbf{k}(1)).$$

Moreover, if $H^1_{\mathcal{L}^\perp}(G_{F,S}, \operatorname{Ad}^0\bar{\rho}^*) = 0$, then $H^1_{\mathcal{N}^\perp}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*) = 0$.

Proof. Clearly, if $v \nmid p$, then $\mathcal{N}_v \cap H^1(G_v, \operatorname{Ad}^0\bar{\rho}) = \mathcal{L}_v$. If $v \mid p$, then certainly $\mathcal{L}_v \subseteq \mathcal{N}_v \cap H^1(G_v, \operatorname{Ad}^0\bar{\rho})$. To see the reverse containment, let f be a one-cocycle such that the cohomology class $[f]$ is in the intersection. Then, up to coboundary, $f(\sigma) \in U$ for all $\sigma \in I_v$ (because $[f] \in \mathcal{N}_v$) and $f(\tau) \in \operatorname{Ad}^0\bar{\rho}$ for all $\tau \in G_v$ (because $[f] \in H^1(G_v, \operatorname{Ad}^0\bar{\rho})$). Thus, we have that $f(\sigma) \in U^0$ for all $\sigma \in I_v$; that is, $[f] \in \mathcal{L}_v$. Thus, for all $v \in S$, we have that $\mathcal{N}_v \cap H^1(G_v, \operatorname{Ad}^0\bar{\rho}) = \mathcal{L}_v$.

Next, let $\mathcal{N}_v^\perp$ and $\mathcal{L}_v^\perp$ denote the annihilators of $\mathcal{N}_v$ and $\mathcal{L}_v$ in $H^1(G_v, \operatorname{Ad}\bar{\rho})$, and we will let $\mathcal{L}_v^{\perp,0}$ denote the annihilator of $\mathcal{L}_v$ in $H^1(G_v, \operatorname{Ad}^0\bar{\rho})$. Since we have $\mathcal{N}_v \cap H^1(G_v, \operatorname{Ad}^0\bar{\rho}) = \mathcal{L}_v$, we get that $\mathcal{N}_v^\perp \subseteq \mathcal{L}_v^\perp$.

It is not hard to see that $\mathcal{L}_v^{\perp} = \mathcal{L}_v^{\perp,0} \oplus H^1(G_v, \mathbf{k}(1))$, for all v. Thus, $H^1_{\mathcal{N}^{\perp}}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*)$ is contained in the kernel of the map

$$H^1(G_{F,S}, \operatorname{Ad}\bar{\rho}^*) \to \bigoplus_{v \in S} \left(\frac{H^1(G_v, \operatorname{Ad}^0 \bar{\rho})}{\mathcal{L}_v^{\perp,0}} \oplus \frac{H^1(G_v, \mathbf{k}(1))}{H^1(G_v, \mathbf{k}(1))} \right),$$

which is clearly $H^1_{\mathcal{L}^{\perp}}(G_{F,S}, \operatorname{Ad}^0 \bar{\rho}^*) \oplus H^1(G_{F,S}, \mathbf{k}(1))$. This is the first part of the lemma.

Now, suppose that $H^1_{\mathcal{L}^{\perp}}(G_{F,S}, \operatorname{Ad}^0 \bar{\rho}^*) = 0$. Evidently, we then have that $H^1_{\mathcal{N}^{\perp}}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*) \subset H^1(G_{F,S}, \mathbf{k}(1))$. Thus, we need to consider the kernel of the map

$$H^1(G_{F,S}, \mathbf{k}(1)) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathbf{k}(1))}{\mathcal{N}_v^{\perp} \cap H^1(G_v, \mathbf{k}(1))}.$$

For v not dividing p, $\mathcal{N}_v^{\perp} = \mathcal{L}_v^{\perp,0}$, so that $\mathcal{N}_v^{\perp} \cap H^1(G_v, \mathbf{k}(1)) = 0$. We will show the same conclusion hold in the case $v \mid p$. Suppose that we are in this setting. As a subspace of $H^1(G_v, \operatorname{Ad}\bar{\rho})$, we see that $H^1(G_v, \mathbf{k}(1))$ is the exact annihilator of $H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$; that is,

$$\begin{aligned} \mathcal{N}_v^{\perp} \cap H^1(G_v, \mathbf{k}(1)) &= \mathcal{N}_v^{\perp} \cap H^1(G_v, \operatorname{Ad}^0 \bar{\rho})^{\perp} \\ &= \left(\mathcal{N}_v + H^1(G_v, \operatorname{Ad}^0 \bar{\rho})\right)^{\perp}, \end{aligned}$$

by elementary linear algebra. So, if we could prove that $\mathcal{N}_v + H^1(G_v, \operatorname{Ad}^0 \bar{\rho}) = \operatorname{Ad}\bar{\rho}$, we would have that $\mathcal{N}_v^{\perp} \cap H^1(G_v, \mathbf{k}(1)) = 0$. This can be achieved by simply counting the sizes. Indeed, we know that

$$\begin{aligned} \#\left(\mathcal{N}_v + H^1(G_v, \operatorname{Ad}^0 \bar{\rho})\right) &= \frac{\#\mathcal{N}_v \# H^1(G_v, \operatorname{Ad}^0 \bar{\rho})}{\#\left(N_v \cap H^1(G_v, \operatorname{Ad}^0 \bar{\rho})\right)} \\ &= \frac{\#\mathcal{N}_v \# H^1(G_v, \operatorname{Ad}^0 \bar{\rho})}{\#\mathcal{L}_v} \\ &= \#\mathbf{k}^{1+[F_v:\mathbf{Q}_p]} \# H^1(G_v, \operatorname{Ad}^0 \bar{\rho}), \text{ by Corollary 3.7,} \\ &= \#H^1(G_v, \mathbf{k}) \# H^1(G_v, \operatorname{Ad}^0 \bar{\rho}), \text{ by Theorem 2.4,} \\ &= \#H^1(G_v, \operatorname{Ad}\bar{\rho}), \end{aligned}$$

since $H^1(G_v, \operatorname{Ad}\bar{\rho}) = H^1(G_v, \operatorname{Ad}^0\bar{\rho}) \oplus H^1(G_v, \mathbf{k})$.

Thus, we are interested in the kernel of the map

$$H^1(G_{F,S}, \mathbf{k}(1)) \to \bigoplus_{v \in S} H^1(G_v, \mathbf{k}(1)).$$

But the elements of this kernel are locally trivial everywhere and hence unramified everywhere. Hence, a non-trivial element of this kernel would cut out unramified abelian p-extension of $F(\mu_p)$ in the $\bar{\chi}$-eigenspace of the class group. Since we have assumed that this eigenspace is trivial, we are left to conclude that

$$H^1_{\mathcal{N}^\perp}(G_{F,S}, \operatorname{Ad}\bar{\rho}^*) \cap H^1(G_{F,S}, \mathbf{k}(1)) = 0,$$

and the second part of the lemma follows. □

We are now ready to prove the main result of this section. By the modularity results of Khare and Wintenberger, Theorem A′ is an immediate corollary of the following result when $F = \mathbf{Q}$.

Theorem 3.10. *Let $\bar{\rho}\colon G_{F,S} \to \mathrm{GL}_2(\mathbf{k})$ be an absolutely irreducible, totally odd, continuous representation that arises as the reduction of a p-adic representation attached to a Hilbert modular eigenform of parallel weight k. Then there exists a finite set of places of F, Q, such that, if we take $\{(\mathcal{D}_q, \mathcal{N}_q)\}$ to correspond to Definition 3.1 (3) for each $q \in Q$, then $H^1_{\mathcal{L}^\perp}(G_{F,S\cup Q}, \operatorname{Ad}\bar{\rho}^*) = 0$. Additionally, we have that $R_{\mathcal{N}} \simeq W(\mathbf{k})[[X]]$ and a deformation of $\bar{\rho}$, $\rho\colon G_{F,S\cup Q} \to \mathrm{GL}_2(W(\mathbf{k})[[X]])$ such that $\rho\,|_{G_v} \in \mathcal{D}_v$ for all $v \in S \cup Q$.*

Proof. By Proposition 3.5, there is a finite set of places of F, Q, such that

$$H^1_{\mathcal{L}^\perp}(G_{F,S\cup Q}, \operatorname{Ad}^0\bar{\rho}^*) = 0.$$

By Lemma 3.9, we therefore have that

$$H^1_{\mathcal{N}^\perp}(G_{F,S\cup Q}, \operatorname{Ad}\bar{\rho}^*) = 0.$$

Lemma 3.8 and Theorem 2.10 then show that $R_{\mathcal{N}}$ is a quotient of $W(\mathbf{k})[[X]]$, say $R_{\mathcal{N}} \simeq W(\mathbf{k})[[X]]/I$. By universality, we have homomorphisms $\varphi_j \colon R_{\mathcal{N}} \to R_{\mathcal{L},j} \simeq W(\mathbf{k})$ for all j. Moreover, these homomorphisms must all be distinct since the resulting representations have different determinants. Thus, we conclude that $I = (0)$ and $R_{\mathcal{N}} \simeq W(\mathbf{k})[[X]]$. □

CHAPTER 4

VARYING THE LEVEL

In this chapter, we are interested in studying the ranks of the deformation rings as we vary the set S. We now allow $\bar{\rho}$ to be ramified at primes that satisfy $\mathrm{N}\, v \equiv 1 \bmod p$, but we impose the following additional assumptions:

1. The Selmer and dual Selmer groups for the choice of local conditions as in Definition 3.1, $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho}))$ and $H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho}))$, are one-dimensional;
2. $Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$, where $Ш^1_S(\mathrm{Ad}^0(\bar{\rho}))$ denotes the kernel of the restriction map $H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v \in S} H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))$; and
3. $\bar{\rho}$ arises from a Hilbert modular form of parallel weight 2.

The first two of these assumptions are not too onerous. One can make a large Selmer group one dimensional following [6] (this is the content of Theorem 3.3), while one can make a trivial Selmer group one dimensional following [22]. Assumption (3) can also be arranged by methods of [24] and [29]. All of these procedures involve adding primes to the ramification set.

Since $\bar{\rho}$ is assumed to be modular, the deformation ring $R_{\mathcal{L}}$ is isomorphic to a localized Hecke ring by Theorem 3.3. Thus, $R_{\mathcal{L}}$ is a finite, flat, complete intersection over $W(\mathbf{k})$. In particular, by Theorem 2.10, we see that

$$\mathrm{rank}_{W(\mathbf{k})}\, R_{\mathcal{L}} = 1$$

if and only if

$$H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\, \bar{\rho}) = 0.$$

Thus, our strategy for the remainder of the section will be to compute the dimensions of various Selmer and dual Selmer groups. Finally, we note that the results of this section in the case $F = \mathbf{Q}$ appeared as joint work of the author and R. Ramakrishna in [17].

4.1 Nice Primes

Definition 4.1. Suppose $\bar{\rho}$ is given as above. A prime v is nice (for $\bar{\rho}$) if

- $\mathrm{N}\, v \not\equiv \pm 1 \bmod p$
- $\bar{\rho}$ is unramified at v,
- the eigenvalues of $\bar{\rho}(\mathrm{Frob}_v)$ have ratio $\mathrm{N}\, v$.

In particular, we see that we can take

$$\bar{\rho}\,|_{G_v} = \begin{pmatrix} \bar{\chi}\varphi & 0 \\ 0 & \varphi \end{pmatrix},$$

(recall that we are now in a weight 2 setting) so that nice primes fall under case (2) of Definition 3.1.

Note. This definition forces us to take $p \geq 5$ as all primes are ± 1 modulo 3.

Definition 4.2. A Chebotarev set is, up to finitely many elements, a set of prime numbers defined by an application of the Chebotarev density theorem in some extension of number fields L/K.

Lemma 4.3. *For $\bar{\rho}$ as above, the set of nice primes, $\mathfrak{R}$, is a Chebotarev set.*

Proof. This is Proposition 3.3(a) of [22]. □

Recall that $\mathbf{k}(j)$ is the group $\mathbf{k}$ with Galois action via $\bar{\chi}^j$. Since the eigenvalues of $\bar{\rho}(\mathrm{Frob}_r)$ have ratio $\mathrm{N}\, r$ for any nice prime r, the eigenvalues of Frob_r acting on $\mathrm{Ad}^0(\bar{\rho})$ are $\mathrm{N}\, r$, 1 and $(\mathrm{N}\, r)^{-1}$ so there are G_r-module isomorphisms

$$\mathrm{Ad}^0(\bar{\rho}) = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \oplus \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$$

$$\simeq \mathbf{k} \oplus \mathbf{k}(1) \oplus \mathbf{k}(-1)$$

and

$$\mathrm{Ad}^0(\bar{\rho})^* = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}^* \oplus \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}^* \oplus \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}^*$$

$$\simeq \mathbf{k}(1) \oplus \mathbf{k} \oplus \mathbf{k}(2).$$

Since $\mathrm{N}\, r \not\equiv \pm 1 \bmod p$ and F is disjoint from $\mathbf{Q}(\mu_p)$, each of the three terms in the above decompositions is distinct from the others.

Lemma 4.4. *Let r be a nice prime for $\bar{\rho}$. Then we have*

1. $H^1(G_r, \mathbf{k}(j)) = 0$ *for* $j \neq 0, 1$;
2. $H^i(G_r, \mathrm{Ad}^0(\bar{\rho})) \simeq H^i(G_r, \mathbf{k}) \oplus H^i(G_r, \mathbf{k}(1)) \simeq H^i(G_r, \mathrm{Ad}^0(\bar{\rho})^*)$;
3. $H^i(G_r, \mathrm{Ad}^0(\bar{\rho}))$ *and* $H^i(G_r, \mathrm{Ad}^0(\bar{\rho})^*)$ *have dimensions* 1, 2, *and* 1 *for* $i = 0, 1, 2$, *respectively;*
4. $H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho}))$ *and* $H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho})^*)$ *correspond to* $H^1(G_r, \mathbf{k})$ *in the decomposition in (2); and*
5. *The one dimensional subspace $\mathcal{L}_r$ from case (3) of Definition 3.1, is*

$$\mathcal{L}_r = H^1(G_r, \mathbf{k}(1)) \subset H^1(G_r, \mathrm{Ad}^0(\bar{\rho})),$$

which, under local duality, is annihilated by the one dimensional space

$$\mathcal{L}_r^{\perp} = H^1(G_r, \mathbf{k}(1)) \subset H^1(G_r, \mathrm{Ad}^0(\bar{\rho})^*).$$

Therefore, if either

$$f \in H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho})) \text{ and } \psi \in H^1(G_r, \mathrm{Ad}^0(\bar{\rho})^*) \backslash H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho})^*)$$

or

$$f \in H^1(G_r, \mathrm{Ad}^0(\bar{\rho})) \backslash H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho})) \text{ and } \psi \in H^1_{nr}(G_r, \mathrm{Ad}^0(\bar{\rho})^*)$$

with $f, \psi \neq 0$, *then* $\mathrm{inv}_r(f \cup \psi) \neq 0$.

Proof. Statement (1) follows immediately from Theorem 2.4:

$$\begin{aligned} \#H^1(G_r, \mathbf{k}(j)) &= \#H^0(G_r, \mathbf{k}(j)) \#H^2(G_r, \mathbf{k}(j)) \\ &= \#H^0(G_r, \mathbf{k}(j)) \#H^0(G_r, \mathbf{k}(1-j)) \\ &= \begin{cases} \#\mathbf{k} & \text{if } j = 0, 1 \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Statement (2) follows the fact that cohomology commutes with direct sums and a similar argument to (1). Statement (3) follows from statement (2). Statement (4) follows from the fact that $\mathrm{N}\, r \not\equiv \pm 1 \bmod p$ and that F is disjoint from $\mathbf{Q}(\mu_p)$. Statement (5) is immediate from the definition of $\mathcal{L}_r$ given in Definition 3.1. Finally, the statement about the non-vanishing of invariants follows from Theorem 2.4. □

Definition 4.5. Let $\Psi \in H^1(G_F, \mathrm{Ad}^0(\bar{\rho})^*)$ and r be a nice prime such that $\Psi|_{G_r}$ is unramified. Consider

$$H^1(G_F, \mathrm{Ad}^0(\bar{\rho})^*) \xrightarrow{\mathrm{res}} H^1(G_r, \mathrm{Ad}^0(\bar{\rho})^*) \to H^1(G_r, \mathbf{k}) = \mathrm{Hom}(G_r, \mathbf{k}) = \mathrm{Hom}(G_r/I_r, \mathbf{k})$$

where the first map is the restriction map and the second arises from the decomposition of the G_r-module $\mathrm{Ad}^0(\bar{\rho})$ in Lemma 4.4. By $\Psi(\mathrm{Frob}_r)$, we mean the evaluation at Frobenius at r of the image of Ψ under the composition above.

Definition 4.6. For a set of primes $\mathfrak{F}$ set

$$\overline{\mathrm{dens}}(\mathfrak{F}) = \limsup_{x\to\infty} \frac{\mathfrak{F}\cap[1,x]}{\pi(x)} \text{ and } \underline{\mathrm{dens}}(\mathfrak{F}) = \liminf_{x\to\infty} \frac{\mathfrak{F}\cap[1,x]}{\pi(x)}$$

and

$$\mathrm{dens}(\mathfrak{F}) = \lim_{x\to\infty} \frac{(\mathfrak{F})\cap[1,x]}{\pi(x)}$$

when the limit exists.

Theorem 1.3 of [16] shows that Chebotarev sets have density as in Definition 4.6.

Proposition 4.7. *Let $\Psi \in H^1(G_F, \mathrm{Ad}^0(\bar{\rho})^*)$, and let $\mathfrak{R}$ be the (Chebotarev) set of nice primes. Then the set of $r \in \mathfrak{R}$ such that $\Psi(\mathrm{Frob}_r) = \alpha$, for $\alpha \in \mathbf{k}$, is a Chebotarev set having density $\dfrac{\mathrm{dens}\,\mathfrak{R}}{\#\mathbf{k}}$.*

Proof. Recall from the discussion following Definition 4.1 that

$$\mathrm{Ad}^0(\bar{\rho})^* \simeq \mathbf{k}(1)\oplus\mathbf{k}\oplus\mathbf{k}(2)$$

as G_r-modules. The factor with trivial action is dual to the matrices which are zero except of the upper right hand entry.

Let $K = F(\mathrm{Ad}^0(\bar{\rho}), \mu_p)$, so that $\Psi|_{\mathrm{Gal}(\bar{K}/K)}$ is a homomorphism. Then the field cut out by Ψ, L_Ψ, is a Galois extension of K with (abelian) Galois group $\mathrm{Ad}^0(\bar{\rho})^*$. By Definition 4.5, $\Psi(\mathrm{Frob}_r) = \alpha$ is equivalent to Frob_r corresponding to the dual of a matrix with α in the upper right hand entry. Such matrices account for $\dfrac{1}{\#\mathbf{k}}$ of all possibilities. The result follows. □

4.2 The Sets $\mathfrak{Q}$ and $\mathfrak{L}$

Recall that we are assuming both $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho})$ and $H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0\,\bar{\rho}^*)$ are one-dimensional. Let f and ϕ span $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho}))$ and $H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$ respectively.

Definition 4.8. Let $\mathfrak{Q}$ be set of nice primes q satisfying $f|_{G_q} \neq 0$, $\phi|_{G_q} \neq 0$. Let $\mathfrak{L}$ be the set of nice primes ℓ satisfying $f|_{G_\ell} \neq 0$ and $\psi|_{G_\ell} = 0$ for all $\psi \in H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$.

Lemma 4.9. *The sets $\mathfrak{Q}$ and $\mathfrak{L}$ are Chebotarev sets. For $q \in \mathfrak{Q}$ we have that*

$$H^1_{\mathcal{L}}(G_{F,S\cup\{q\}}, \mathrm{Ad}^0(\bar{\rho})) = 0.$$

Proof. That $\mathfrak{Q}$ and $\mathfrak{L}$ are Chebotarev sets is an identical argument to Lemma 8 of [11], working over F instead of $\mathbf{Q}$. The second part comes from the fact that the primes $q \in \mathfrak{Q}$ are chosen to annihilate the dual Selmer group, $H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$; this is essentially the proof of Theorem 3.3. Applying Lemma 3.2 gives the desired result. □

Proposition 4.10. *For any $\ell \in \mathfrak{L}$, the Selmer and dual Selmer groups,*

$$H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \text{ and } H^1_{\mathcal{L}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*),$$

are one dimensional. Moreover, $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ is not spanned by f and $H^1_{\mathcal{L}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ is spanned by ϕ.

Proof. As $\phi|_{G_\ell} = 0$, we have that $\phi \in H^1_{\mathcal{L}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$. In particular, we may conclude that $H^1_{\mathcal{L}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ is not trivial.

As f is a cohomology class for the group $G_{F,S}$, it is unramified at ℓ. Since $f|_{G_\ell} \neq 0$ (by definition of the set $\mathfrak{L}$), Lemma 4.4 implies that

$$f \notin H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})).$$

Thus, any non-zero element of $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ is ramified at ℓ.

Let f_1 and f_2 be non-zero elements of $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. By Lemma 4.4, there is a nontrivial linear combination of f_1 and f_2 which is unramified at ℓ. This linear combination is in $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ and therefore zero by the previous paragraph. Thus, f_1 and f_2 are linearly dependent, and so $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ is at most one-dimensional. The proposition now follows from Lemma 3.2. □

Note. By the discussion at the start of the chapter, Parts (1) and (2) of Theorem B′ follow immediately from Lemma 4.9 and Proposition 4.10.

Proposition 4.11. *For any $\ell \in \mathfrak{L}$ the kernel of*

$$H^1(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v\in S} H^1(G_v, \mathrm{Ad}^0(\bar{\rho})) \tag{4.1}$$

is one dimensional. Moreover, for any nice prime r, the inflation map

$$H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*) \to H^1(G_{F,S\cup\{r\}}, \mathrm{Ad}^0(\bar{\rho})^*)$$

has one dimensional cokernel.

Proof. To prove the first statement, set

$$\mathcal{M}_v = 0,\ \mathcal{M}_v^\perp = H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*),\ \text{for } v \in S$$

and

$$\mathcal{M}_\ell = H^1(G_\ell, \mathrm{Ad}^0(\bar{\rho})),\ \mathcal{M}_\ell^\perp = 0,$$

so that

$$H^1_{\mathcal{M}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*) = H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*).$$

As any $\psi \in H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$ satisfies $\psi|_{G_\ell} = 0$, we have that

$$H^1_{\mathcal{M}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*) \supseteq H^1_{\mathcal{M}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*),$$

and as $\mathcal{M}^\perp_\ell = 0$, all elements of $H^1_{\mathcal{M}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ are trivial (and therefore unramified) at ℓ, showing

$$H^1_{\mathcal{M}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*) = H^1_{\mathcal{M}^\perp}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*).$$

Thus, two applications of Theorem 2.7 imply that

$$\#H^1_{\mathcal{M}}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})) \cdot \#\mathbf{k} = \#H^1_{\mathcal{M}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})).$$

As $H^1_{\mathcal{M}}(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})) = Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$ by our hypotheses, the kernel of Equation (4.1) is $H^1_{\mathcal{M}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. The first part follows.

For the second part set $T = S \cup \{r\}$, and let

$$\mathcal{M}_v = 0,\ \mathcal{M}_v^\perp = H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*), \text{for } v \in T.$$

The Selmer groups for S and T are $Ш^1$s and the dual Selmer groups for S and T are the full H^1s. Two applications of Theorem 2.7 give

$$\frac{\#Ш^1_T(\mathrm{Ad}^0(\bar{\rho}))}{\#Ш^1_S(\mathrm{Ad}^0(\bar{\rho}))} = \frac{\#H^1(G_{F,T}, \mathrm{Ad}^0(\bar{\rho})^*)}{\#H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*) \cdot \#\mathbf{k}}. \tag{4.2}$$

By assumption, $Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$. Any element of $Ш^1_T(\mathrm{Ad}^0(\bar{\rho}))$ is trivial, and therefore unramified, at r, so $Ш^1_T(\mathrm{Ad}^0(\bar{\rho})) \subseteq Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$. Thus, Equation (4.2) becomes

$$\#H^1(G_{F,T}, \mathrm{Ad}^0(\bar{\rho})^*) = \#H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*) \cdot \#\mathbf{k},$$

the desired result. □

The second part of Proposition 4.11 implies $H^1(G_{F,S\cup\{r\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ contains classes ramified at r, for all nice primes r. For $q \in \mathfrak{Q}$, fix $\Phi_q \in H^1(G_{F,S\cup\{q\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ ramified at q and normalized so that $\mathrm{inv}_q(f \cup \Phi_q) = 1$ (recall that our local duality pairing gives invariants that have values in $\mathbf{k}$). Note that f and any $\Psi \in H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$ are unramified at q, so Theorem 2.4 implies $\mathrm{inv}_q(f \cup \Psi) = 0$. Thus, though there is ambiguity in choosing Φ_q, the image of Φ_q in

$$H^1(G_{F,S\cup\{q\}}, \mathrm{Ad}^0(\bar{\rho})^*)/H^1(G_{F,S}, \mathrm{Ad}^0(\bar{\rho})^*)$$

and $\mathrm{inv}_q(f \cup \Phi_q)$ are well-defined after this normalization.

The first part of Proposition 4.11 implies that the kernel of Equation (4.1) contains an element g_ℓ which is ramified at ℓ. By Proposition 4.10,

$$H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$$

is one-dimensional, but

$$f \notin H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})).$$

Let f_ℓ span $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. As f_ℓ and g_ℓ are ramified at ℓ, we can argue as in the proof of Proposition 4.10. Lemma 4.4 implies that some linear combination of f_ℓ and g_ℓ is unramified at ℓ. The coefficients of g_ℓ and f_ℓ in this linear combination are necessarily nonzero. As $f_\ell\,|_{G_v},\ g_\ell\,|_{G_v} \in \mathcal{L}_v$ for $v \in S$, this linear combination is locally in $\mathcal{L}_v$ for all $v \in S$ and so is in $H^1_{\mathcal{L}}(G_S, \mathrm{Ad}^0(\bar{\rho}))$; that is, it is a multiple of f. Thus, after suitably scaling f_ℓ, we have $f_\ell = a_\ell f + g_\ell$. Note that the coefficient a_ℓ is independent of the set $\mathfrak{Q}$.

Proposition 4.12. *Let $q \in \mathfrak{Q}$ and $l \in \mathfrak{L}$. Then, $H^1_{\mathcal{L}}(G_{F,S\cup\{q,\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \neq 0$ if and only if $\mathrm{inv}_q(f_\ell \cup \Phi_q) = 0$.*

Proof. Recall that f_ℓ spans $H^1_{\mathcal{L}}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ and, by Proposition 4.10, ϕ spans

$H^1_{\mathcal{L}^\perp}(G_{F,S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$. The definition of $\mathfrak{Q}$ requires $\phi|_{G_q} \neq 0$, so Lemma 4.4 implies $\phi|_{G_q} \notin \mathcal{L}_q^\perp$. The proof of Theorem 3.3 (see, for instance, the discussion surrounding Lemmas 1.1 and 1.2 of [29]) implies

$$H^1_{\mathcal{L}}(G_{F,S\cup\{q,\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \neq 0$$

if and only if $f_\ell|_{G_q} \in \mathcal{L}_q$. As f_ℓ is unramified at q and $\mathcal{L}_q$ consists of ramified classes, we see $f_\ell|_{G_q} \in \mathcal{L}_q$ if and only if $f_\ell|_{G_q} = 0$. But, Φ_q is ramified at q by definition, so this can only happen if and only if

$$\mathrm{inv}_q(f_\ell \cup \Phi_q) = 0$$

by Lemma 4.4. □

Proposition 4.13. *Let $q \in \mathfrak{Q}$ and $l \in \mathfrak{L}$. Then*

$$\mathrm{inv}_q(f_\ell \cup \Phi_q) = a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_q).$$

Proof. Global reciprocity implies

$$\begin{aligned} 0 &= \sum_{v\in S\cup\{q,\ell\}} \mathrm{inv}_v(g_\ell \cup \Phi_q) \\ &= \mathrm{inv}_\ell(g_\ell \cup \Phi_q) + \mathrm{inv}_q(g_\ell \cup \Phi_q), \end{aligned}$$

since $g_\ell|_{G_v} = 0$ for all $v \in S$. Thus, we have that

$$\begin{aligned} \mathrm{inv}_q(f_\ell \cup \Phi_q) &= \mathrm{inv}_q((a_\ell f + g_\ell) \cup \Phi_q) \\ &= a_\ell \,\mathrm{inv}_q(f \cup \Phi_q) + \mathrm{inv}_q(g_\ell \cup \Phi_q) \\ &= a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_q), \end{aligned}$$

since $\mathrm{inv}_q(f \cup \Phi_q) = 1$. □

Definition 4.14. Fix $q \in \mathfrak{Q}$, $\alpha \in \mathbf{k}$, and set $\mathfrak{L}_{q,\alpha} = \{l \in \mathfrak{L} | \,\mathrm{inv}_q(f_\ell \cup \Phi_q) = \alpha\}$.

Theorem 4.15. *Let $\alpha \in \mathbf{k}$. There exists a finite set $\mathfrak{G} \subset \mathfrak{Q}$ of cardinality at most $\#\mathbf{k} - 1$ such that for any $q \in \mathfrak{Q} \backslash \mathfrak{G}$*

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q,\alpha}) \geq \frac{(\#\mathbf{k})! \, \mathrm{dens}(\mathfrak{L})}{(\#\mathbf{k})^{\#\mathbf{k}+1}}.$$

Proof. Let $\epsilon > 0$, and suppose there are $\#\mathbf{k}$ elements $q_i \in \mathfrak{Q}$ such that

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_i,\alpha}) < \frac{((\#\mathbf{k})! - \epsilon) \, \mathrm{dens}(\mathfrak{L})}{(\#\mathbf{k})^{\#\mathbf{k}+1}}.$$

Let $\mathfrak{C} = \cap_{i=1}^{\#\mathbf{k}} \mathfrak{L}_{q_i,\alpha}^c$, where $\mathfrak{L}_{q,\alpha}^c$ denotes the complement in $\mathfrak{L}$ of $\mathfrak{L}_{q,\alpha}$. We immediately see that

$$\begin{aligned} \underline{\mathrm{dens}}(\mathfrak{C}) &\geq \left(1 - \#\mathbf{k} \frac{(\#\mathbf{k})! - \epsilon}{(\#\mathbf{k})^{\#\mathbf{k}+1}}\right) \mathrm{dens}(\mathfrak{L}) \\ &= \left(1 - \frac{(\#\mathbf{k})! - \epsilon}{(\#\mathbf{k})^{\#\mathbf{k}}}\right) \mathrm{dens}(\mathfrak{L}). \end{aligned}$$

Next, consider the set

$$\mathfrak{D} = \{\ell \in \mathfrak{L} | \Phi_{q_i}(\mathrm{Frob}_\ell) \neq \Phi_{q_j}(\mathrm{Frob}_\ell) \text{ for } 1 \leq i < j \leq \#\mathbf{k}\}.$$

Using Proposition 4.7, it is an exercise to see $\mathfrak{D}$ is a Chebotarev set with density $\frac{(\#\mathbf{k})!}{(\#\mathbf{k})^{\#\mathbf{k}}} \mathrm{dens}(\mathfrak{L})$.

As $1 - \frac{(\#\mathbf{k})! - \epsilon}{(\#\mathbf{k})^{\#\mathbf{k}}} + \frac{(\#\mathbf{k})!}{(\#\mathbf{k})^{\#\mathbf{k}}} > 1$, we must have $\mathfrak{C} \cap \mathfrak{D} \neq \emptyset$; let $\ell \in \mathfrak{C} \cap \mathfrak{D}$. In particular, we have that

$$\mathrm{inv}_{q_i}(f_\ell \cup \Phi_{q_i}) = a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_{q_i}) \neq \alpha \tag{4.3}$$

for $i = 1, 2, \ldots, \#\mathbf{k}$, since $\ell \in \mathfrak{C}$.

Next, for ℓ fixed, $\mathrm{inv}_\ell(g_\ell \cup \Phi_{q_i})$ depends only on the value of Φ_{q_i} at Frob_ℓ, since

$$\mathrm{inv}_\ell(g_\ell \cup \Phi_{r_1}) - \mathrm{inv}_\ell(g_\ell \cup \Phi_{r_2}) = 0$$

if and only if $(\Phi_{r_1} - \Phi_{r_2})(\mathrm{Frob}_\ell) = 0$, for any nice primes r_1, r_2. Since $\ell \in \mathfrak{D}$ the values $\Phi_{q_i}(\mathrm{Frob}_\ell)$ for $i = 1, 2, \ldots, \#\mathbf{k}$ are all distinct. Combining this with Equation 4.3 gives a contradiction. Thus,

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_i,\alpha}) \geq \frac{((\#\mathbf{k})! - \epsilon)\,\mathrm{dens}(\mathfrak{L})}{(\#\mathbf{k})^{\#\mathbf{k}+1}}$$

for all but $\#\mathbf{k} - 1$ elements $q \in \mathfrak{Q}$. Since ϵ is arbitrary, the result follows. □

Note. The first part of Theorem B′ follows immediately from this. If $\overline{\mathrm{dens}}\mathfrak{L}_{q,0} > 0$, then there are infinitely many ℓ such that the Selmer group $\dim H^1_{\mathcal{L}}(G_{F,S\cup\{q,\ell\}}, \mathrm{Ad}^0\,\bar{\rho}) = 1$. As in the discussion at the start of the chapter, this automatically shows that the rank of the corresponding deformation ring $R_{\mathcal{L}}$ is greater than one.

Now that we have established that the sets $\mathfrak{L}_{q,\alpha}$ are infinite (after possibly discarding some finite number of q), we turn our attention to showing that these sets are not too large.

Proposition 4.16. *Let $\alpha \in \mathbf{k}$ and $q_1, q_2 \in \mathfrak{Q}$ be distinct. Then*

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_1,\alpha} \cap \mathfrak{L}_{q_2,\alpha}) \leq \frac{\mathrm{dens}(\mathfrak{L})}{\#\mathbf{k}}.$$

Proof. Observe that

$$\begin{aligned}
\mathfrak{L}_{q_1,\alpha} \cap \mathfrak{L}_{q_2,\alpha} &= \{\ell \in \mathfrak{L} |\, \mathrm{inv}_{q_1}(f_\ell \cup \Phi_{q_1}) = \alpha = \mathrm{inv}_{q_2}(f_\ell \cup \Phi_{q_2})\} \\
&\subseteq \{\ell \in \mathfrak{L} |\, \mathrm{inv}_{q_1}(f_\ell \cup \Phi_{q_1}) - \mathrm{inv}_{q_2}(f_\ell \cup \Phi_{q_2}) = 0\} \\
&= \{\ell \in \mathfrak{L} |\, \mathrm{inv}_\ell(g_\ell \cup (\Phi_{q_2} - \Phi_{q_1})) = 0\}, \text{ by Proposition 4.13,} \\
&= \{\ell \in \mathfrak{L} | (\Phi_{q_2} - \Phi_{q_1})(\mathrm{Frob}_\ell) = 0\}.
\end{aligned}$$

By Proposition 4.7, the set of $\ell \in \mathfrak{L}$ satisfying $(\Phi_{q_2} - \Phi_{q_1})(\mathrm{Frob}_\ell) = 0$ is a Chebotarev set with density $\dfrac{\mathrm{dens}(\mathfrak{L})}{\#\mathbf{k}}$. □

Remark. The moral of Proposition 4.16 is that while we do not know how to control $\mathfrak{L}_{q,\alpha}$ by a Chebotarev condition, we can control the 'difference' between $\mathfrak{L}_{q_i,\alpha}$ and $\mathfrak{L}_{q_j,\alpha}$. Moreover, suppose for some q_0 that $\mathrm{inv}_{q_0}(f_\ell \cup \Phi_{q_0}) = \alpha$ for all $\ell \in \mathfrak{L}$; that is, suppose that $\mathfrak{L} = \mathfrak{L}_{q_0,\alpha}$. Then, for any $q \in \mathfrak{Q}$, $q \neq q_0$, $\mathrm{inv}_q(f_\ell \cup \Phi_q) = \alpha$ if and only if $\mathrm{inv}_\ell(g_\ell \cup (\Phi_q - \Phi_{q_0})) = 0$, which happens on a set of density $\frac{1}{\#\mathbf{k}}\,\mathrm{dens}(\mathfrak{L})$ by Proposition 4.7.

Proposition 4.17. *Let X_i be sets of primes. Then,*

$$\overline{\mathrm{dens}}\left(\bigcup_{i=1}^{M} X_i\right) \geq \left(\sum_{i=1}^{M} \underline{\mathrm{dens}}(X_i)\right) - \sum_{1\leq i<j\leq M} \overline{\mathrm{dens}}(X_i \cap X_j).$$

Proof. Let $\epsilon > 0$ be given. Set $b_i = \underline{\mathrm{dens}}(X_i)$ and $y = \overline{\mathrm{dens}}(\bigcup_{i=1}^{M} X_i)$. For large x,

$$\begin{aligned} (y+\epsilon)\pi(x) &\geq \#\left(\left(\bigcup_{i=1}^{M} X_i\right) \cap [1,x]\right), \\ \#\left(X_i \cap [1,x]\right) &\geq (b_i - \epsilon)\pi(x), \text{ and} \\ (\overline{\mathrm{dens}}(X_i \cap X_j) + \epsilon)\pi(x) &\geq \#\left(X_i \cap X_j\right) \cap [1,x]. \end{aligned}$$

From inclusion-exclusion, we have for all x

$$\begin{aligned} \#\left(\left(\bigcup_{i=1}^{M} X_i\right) \cap [1,x]\right) \geq &\left(\sum_{i=1}^{M} \#\left(X_i \cap [1,x]\right)\right) \\ &- \left(\sum_{1\leq i<j\leq M} \#\left(\left(X_i \cap X_j\right) \cap [1,x]\right)\right), \end{aligned}$$

so for large x

$$(y+\epsilon)\pi(x) \geq \left(\sum_{i=1}^{M} (b_i - \epsilon)\right)\pi(x) - \left(\sum_{1\leq i<j\leq M} \left(\overline{\mathrm{dens}}\left(X_i \cap X_j\right) + \epsilon\right)\right)\pi(x),$$

and the result follows. □

Theorem 4.18. *Let $\alpha \in \mathbf{Z}/p\mathbf{Z}$. There are at most $\sqrt{2\#\mathbf{k}}$ primes q_i such that $\underline{\mathrm{dens}}(\mathfrak{L}_{q_i,\alpha}) \geq \frac{\sqrt{2\#\mathbf{k}}\,\mathrm{dens}(\mathfrak{L})}{\#\mathbf{k}}$.*

Proof. Suppose there are $M \geq \sqrt{2\#\mathbf{k}} + 1$ such q_i, namely $q_1, \ldots, q_M$. Proposition 4.17 implies

$$\overline{\text{dens}}\left(\bigcup_{i=1}^{M} \mathfrak{L}_{q_i,\alpha}\right) \geq \left(\sum_{i=1}^{M} \frac{\sqrt{2\#\mathbf{k}}\,\text{dens}(\mathfrak{L})}{\#\mathbf{k}}\right) - \left(\sum_{1\leq i<j\leq M} \overline{\text{dens}}(\mathfrak{L}_{q_i,\alpha} \cap \mathfrak{L}_{q_j,\alpha})\right).$$

Proposition 4.16 and the fact that $\mathfrak{L}_{q_i,\alpha} \subseteq \mathfrak{L}$ imply

$$\text{dens}(\mathfrak{L}) \geq \overline{\text{dens}}\left(\bigcup_{i=1}^{M} \mathfrak{L}_{q_i,\alpha}\right) \geq \binom{M}{1} \frac{\sqrt{2\#\mathbf{k}}\,\text{dens}(\mathfrak{L})}{\#\mathbf{k}} - \binom{M}{2} \frac{\text{dens}(\mathfrak{L})}{\#\mathbf{k}}. \tag{4.4}$$

The right hand side of Equation (4.4) is a quadratic in M that is maximized at $M = \sqrt{2\#\mathbf{k}} + \frac{1}{2}$. At $M = \sqrt{2\#\mathbf{k}} + \frac{1}{2} - \frac{1}{2} = \sqrt{2\#\mathbf{k}}$, the inequality becomes $\text{dens}(\mathfrak{L}) \geq \left(1 + \frac{1}{\sqrt{2\#\mathbf{k}}}\right)\text{dens}(\mathfrak{L})$. This would lead to a contradiction if $\sqrt{2\#\mathbf{k}}$ were an integer. As quadratics are symmetric about their extrema, we get the same inequality for $M = \sqrt{2\#\mathbf{k}} + \frac{1}{2} + \frac{1}{2} = \sqrt{2\#\mathbf{k}} + 1$. Plugging the integer in the interval $[\sqrt{2\#\mathbf{k}}, \sqrt{2\#\mathbf{k}} + 1]$ into Equation (4.4) gives a contradiction. □

Note. In analogy to the comments after Theorem 4.15, the second part of Theorem B′ follows from this result.

BIBLIOGRAPHY

[1] A.O.L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[2] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[3] F. Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997.

[4] F. Diamond and R. Taylor. Nonoptimal levels of mod l modular representations. *Invent. Math.*, 115(3):435–46, 1994.

[5] M. Emerton, R. Pollack, and T. Weston. Variation of Iwasawa invariants in Hida families. *Invent. Math.*, 163(3):523–580, 2006.

[6] T. Gee. Companion forms over totally real fields. II. *Duke Math. J.*, 136(2):275–284, 2007.

[7] F. Gouvêa. Deformations of Galois representations. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 233–406. Amer. Math. Soc., Providence, RI, 2001. Appendix 1 by Mark Dickinson, Appendix 2 by Tom Weston and Appendix 3 by Matthew Emerton.

[8] S. Hamblen and R. Ramakrishna. Deformations of certain reducible Galois representations. II. *Amer. J. Math.*, 130(4):913–944, 2008.

[9] H. Hida. Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85(3):545–613, 1986.

[10] H. Hida. Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup. (4)*, 19(2):231–273, 1986.

[11] C. Khare and R. Ramakrishna. Finiteness of Selmer groups and deformation rings. *Invent. Math.*, 154(1):179–198, 2003.

[12] C. Khare and J.-P. Wintenberger. On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. *Ann. of Math. (2)*, 169(1):229–253, 2009.

[13] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[14] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[15] M. Kisin. Moduli of finite flat group schemes, and modularity. *Ann. of Math. (2)*, 170(3):1085–1180, 2009.

[16] J.C. Lagarias and A.M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[17] B. Lundell and R. Ramakrishna. New parts of hecke rings. *Math. Res. Lett.*, 18(1):59–73, 2011.

[18] B. Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'IHES*, 47:33–186, 1977.

[19] B. Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[20] J.S. Milne. *Arithmetic duality theorems.* BookSurge, LLC, Charleston, SC, second edition, 2006.

[21] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields.* Springer, Berlin, 2000.

[22] A. Pande. Deformations of Galois representations and the theorems of Sato-Tate, Lang-Trotter and others, 2009.

[23] R. Ramakrishna. Lifting Galois representations. *Invent. Math.*, 138(3):537–562, 1999.

[24] R. Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. *Ann. of Math. (2)*, 156(1):115–154, 2002.

[25] K. Ribet. Congruence relations between modular forms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 503–514, Warsaw, 1984. PWN.

[26] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[27] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[28] W. Stein. The Modular Forms Database. *http://modular.math.washington.edu/Tables*, 2004.

[29] R. Taylor. On icosahedral Artin representations. II. *Amer. J. Math.*, 125(3):549–566, 2003.

[30] L.C. Washington. Galois cohomology. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 101–120. Springer, New York, 1997.

[31] G. Wiese. *Galois Representations*. 2008. Available online `http://www.uni-due.de/~hx0037/`.

[32] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.