# Framed Deformation and Modularity

$$R_{\emptyset,\mathrm{ord}}/\mathfrak{N} \xrightarrow{\sim} \mathbf{T}_{\emptyset}$$

*Author:*
Shrenik Shah

*Advisor:*
Prof. Richard Taylor

Submitted to the Harvard University Department of Mathematics in partial fulfillment of the requirements for the degree of A.B. in Mathematics

March 30, 2009

# Acknowledgements

I would like to thank Prof. Taylor for his warmth, dedication, and patience in advising this thesis. Although he was also advising an incredible number of graduate students, I always felt as if I was his only advisee because of his willingness to find time to answer my questions whenever I had them. Prof. Taylor answered my questions thoroughly regardless of whether they were trivial or deep, and as a result he was able to clear up my many, many misunderstandings about the material. Without a doubt, working with Prof. Taylor on my senior thesis has been the defining experience of my time as an undergraduate at Harvard.

I thank Prof. Ono for being a mentor, a teacher, and a friend. He taught me about modular forms and congruences with enthusiasm that I will never forget.

I also thank Profs. Conrad and Mazur for meeting with me to discuss material related to my thesis, as well as Stefan Patrikis for helping to explain Kisin's work on the Fontaine-Mazur conjecture.

I also would like to thank Profs. Harris, Vadhan, Kronheimer, McMullen, Elkies, Lam, Rabin, Valiant, and Mazur for their advice and guidance at various points during my time as an undergraduate. With their help, I have never felt unsupported here.

Finally, I would like to thank my family for their support and encouragement over the years.

# Contents

# Chapter 1

# Introduction

In 1637, Fermat posed the question of whether there were nonzero integer solutions to the equation

$$x^n + y^n = z^n$$

for $n \geq 3$, and claimed to have a marvelous proof that none existed. Number theory, which studies properties of the integers, has many simple questions whose answers require deep and difficult mathematics. Fermat's question was referred to as Fermat's Last Theorem (FLT) on the assumption that he did indeed know a proof, but many great mathematicians over the years tried and failed to solve the problem. While FLT in itself does not seem to reveal any deep properties of the integers, the approaches of various mathematicians to the problem have inspired many major developments in number theory.

Fermat did write down the solution to one case of the problem using a technique called "infinite descent." The idea was to show that if $(x, y, z)$ is a solution in positive integers to $x^4 + y^4 = z^4$, one could construct a solution with a smaller value of $z$. By repeating this procedure, one would obtain an infinite sequence of shrinking positive integers, which is impossible. Fermat's technique is used throughout mathematics as a fundamental method of argumentation.

Kummer invented the subject of algebraic number theory in order to prove additional cases of FLT. In particular, he devised "prime ideals" to study factorization in the ring $\mathbf{Z}[\zeta_n]$, where $\zeta_n$ is a primitive $n^{\text{th}}$ root of unity. This ring arises if one considers the factorization

$$y^n = x^n - z^n = \prod_{k=0}^{n-1}(x - \zeta_n^k z).$$

Kummer's criterion for whether his solution to FLT worked for a prime exponent $p$ was related to divisibility properties of a series of numbers, called Bernoulli numbers. Kummer's criterion was refined by Herbrand and Ribet [Rib76]. Ribet's result had significant implications for the modern area of Iwasawa theory.

Faltings proved a very general theorem called Mordell's conjecture, which implied that FLT has finitely many solutions in coprime integers for any particular $n$. This shows, moreover, that FLT can only have solutions for a set of exponents $n$ of "density 0," which informally means that these exponents are very sparsely distributed. His proof, in contrast to previous approaches, used the *geometry* of the curves $x^n + y^n = z^n$. In particular, the solutions to the "inhomogeneous" equation $X^n + Y^n = 1$, where $X = \frac{x}{z}$ and $Y = \frac{y}{z}$, looks like a sphere with a number $g$ of "handles" attached when viewed as a subset of the affine complex space $\mathbf{C}^2$. If the number $g$, called the genus, is at least 2, then Falting's proof shows that only finitely many integer points can lie on the curve.

However, the solution to Fermat's Last Theorem had to wait for the work of Wiles [Wil95] and Taylor-Wiles [TW95], whose work blended far more areas of number theory than any previous approach. As we will see, the work also introduces a brilliant mathematical argument that has already been used in the last decade to resolve many long-standing open problems and promises many more breakthroughs down the road.

## 1.1 Motivation

Wiles and Taylor-Wiles settled Fermat's Last Theorem in 1994. The path to the proof routed through several areas of number theory. Frey [Fre86, Fre89] showed that a nontrivial solution in integers to this equation would give rise to an elliptic curve that had peculiar properties. Serre [Ser87] then showed that if a special case of one of his conjectures, which he called the $\epsilon$-conjecture, were proven, then a conjecture of Shimura and Taniyama would imply Fermat's Last Theorem. Ribet [Rib90] proved the $\epsilon$-conjecture and showed, moreover, that only a special case of the Shimura-Taniyama conjecture – the *semistable* case – would be sufficient.

The Shimura-Taniyama conjecture relates *elliptic curves* over the rational numbers $\mathbf{Q}$, which are solution sets to equations of the form

$$y^2 = x^3 + Ax + B$$

for rational numbers $A$ and $B$, to *modular forms*, which are, loosely speaking, certain functions on the upper halfplane $\mathfrak{H}$ of the complex numbers satisfying transformation properties with respect to the action of $\mathrm{SL}_2(\mathbf{Z})$, the group of $2 \times 2$ matrices with determinant 1, on $\mathfrak{H}$. While it was long understood that modular forms could be seen as functions acting on a *moduli space* – a space that forms a geometric parametrization for an object – of elliptic curves, the Shimura-Taniyama conjecture predicts a surprising twist on the relationship between these two types of objects. In order to understand the relationship, we need to look at a third type of object – a Galois representation.

The field $\mathbf{Q}$, consisting of rational numbers, sits inside a number of larger fields, called *extensions*. We define the *algebraic closure* of $\mathbf{Q}$, $\overline{\mathbf{Q}}$, to be a field containing $\mathbf{Q}$ such that every element of $\overline{\mathbf{Q}}$ is the root of a polynomial with coefficients in $\mathbf{Q}$, and conversely, every polynomial of degree $n$ with coefficients in $\mathbf{Q}$ factors into $n$ linear factors over $\overline{\mathbf{Q}}$. One can define a group $G_{\mathbf{Q}}$, called the *absolute Galois group* whose members are automorphisms $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}$ that fix the subfield $\mathbf{Q}$. There is a natural topology on $G_{\mathbf{Q}}$, called the *Krull topology*, which expresses the "closeness" of these automorphisms. Since $G_{\mathbf{Q}}$ encloses a wealth of information about $\mathbf{Q}$ and its extensions, it is natural to try to understand its structure. In this vein, one can study *decomposition groups* $G_{\mathbf{Q}_\ell} \subset G_{\mathbf{Q}}$ corresponding to the completion of the ring $\mathbf{Z}$ at the prime $\ell$. This is a "local" piece of the group, and one can quite explicitly determine the structure of $G_{\mathbf{Q}_\ell}$. However, fully understanding the structure of $G_{\mathbf{Q}}$ directly appears to be intractable. Moreover, since $G_{\mathbf{Q}}$ is only determined up to conjugation by one of its elements, one would hope to study properties that are independent of this ambiguity.

In particular, one might hope to gain an understanding of the *representation theory* of $G_{\mathbf{Q}}$, which is the study of the ways in which $G_{\mathbf{Q}}$ can act on various objects, such as the vector spaces $\mathbf{C}^n$ or $\mathbf{F}_{p^k}^n$, where $\mathbf{F}_{p^k}$ denotes the finite field of $p^k$ elements. Where $G_{\mathbf{Q}}$ is acting on a free module $R^n$, we may express this as a continuous group homomorphism

$$G_{\mathbf{Q}} \to \mathrm{GL}_n(R).$$

Representations of $G_{\mathbf{Q}}$ on $\mathbf{C}^n$ and $\mathbf{F}_{p^k}^n$ have finite image in $\mathrm{GL}_n(\mathbf{C})$ and $\mathrm{GL}_n(\mathbf{F}_{p^k})$ (in the former case, this is for topological reasons). However, if one uses the ring of $p$-adic integers $\mathbf{Z}_p$ for $R$, one finds a wealth of interesting representations with infinite image.

Over $\mathbf{C}$, an elliptic curve $E$ is topologically shaped like a *torus*, the product $S^1 \times S^1$ of two circles. This can also be seen as a sphere with one handle attached, so an elliptic curve has genus 1. Since the circle $S^1$ has a natural addition via the embedding of $S^1$ as the complex numbers of unit modulus, one might expect that one can add points on $E$. In fact, an elliptic curve indeed has an addition law once a point has been selected as the identity. Looking at the torus, we see that there are $n^2$ points of order $n$ on the elliptic curve $E$. One can show that these points have coefficients in $\overline{\mathbf{Q}}$, and are permuted by the Galois group in a manner respecting their addition law. This gives rise to a representation

$$G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

For any prime $p$, one can consider the points of order dividing $p$, $p^2$, and so on to construct a continuous representation

$$G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p).$$

One obtains a family of Galois representations in this manner.

A far deeper theory of Deligne [Del71] and Deligne-Serre [DS74] constructs $p$-adic Galois representations associated to certain modular forms $f$. The Shimura-Taniyama conjecture predicts that the Galois representations associated to any elliptic curve are equivalent to Galois representations arising from modular forms. An elliptic curve with this property is called *modular* The work of Frey, Serre, and Ribet showed that a solution to the Fermat equation would produce an elliptic curve that *cannot* be modular.

## 1.2 The Work of Wiles and Taylor-Wiles

Wiles' approach to the conjecture was to show that if a $p$-adic representation $\rho$ satisfied certain conditions that all candidate modular representations satisfied, then $\rho$ would be equal to one of these representations. To any $p$-adic representation $\rho$, one can compose with the reduction map $\mathbf{Z}_p \to \mathbf{F}_p$ to obtain a *residual* representation

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p) \to \mathrm{GL}_2(\mathbf{F}_p).$$

Wiles instead started with a residual representation $\overline{\rho}$ already known to arise from a modular form, and showed that all suitable choices of $\rho$ that yield $\overline{\rho}$ upon reduction modulo $p$ were modular.

The idea behind this approach originates with a theory of Mazur [Maz89], introduced to study this very problem. In particular, Mazur viewed the sequence

$$\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p^2\mathbf{Z}, \mathbf{Z}/p^3\mathbf{Z}, \ldots$$

in the same manner as one might think of higher-order terms in a Taylor expansion. In particular, he saw elements of $\mathbf{Z}/p^k\mathbf{Z}$ reducing to an element of $\mathbf{Z}/p\mathbf{Z}$ as *deformations* of that element. While there was already existed an algebraic basis for this phenomenon, present in many other fields, Mazur turned this idea towards Galois representations in order to formalize the idea of looking at the geometric *deformation space* of a residual representation $\overline{\rho}$. He was interested in knowing the precise subspace of this deformation space corresponding to modular represention, and conjectured that certain minimal conditions were sufficient to carve out the subspace of modular deformations. Mazur's main innovation was to realize the deformation space as the *spectrum* of a ring $R$, which is a topological space that corresponds to the geometry of the ring. He transformed the question of whether representations are modular into a comparison of $R$ with a ring $\mathbf{T}$ whose spectrum describes the space of modular representations. In particular, an isomorphism of $R$ and $\mathbf{T}$, or even a "near-isomorphism," in a sense that will be made precise later, would prove that the $p$-adic representations parametrized by $R$ are modular.

The work of Wiles and Taylor-Wiles can be divided into three realms.

1. **Deformation theory**: Studying the size and structure of the deformation spaces of the rings $R$.

2. **Hecke algebras**: Studying the behavior of the rings $\mathbf{T}$.

3. **Commutative algebra**: Given certain data about the relationship between $R$ and $\mathbf{T}$, prove that these rings are (near-)isomorphic.

In addition to the global strategy, Wiles and Taylor-Wiles invented techniques in each of these areas that have been studied and refined thoroughly in the interim years.

## 1.3 The Aftermath

We can view the work of Wiles and Taylor-Wiles not as an end to an ancient problem but as a beginning of an entirely new approach to number theory, one that has proven successful not only in resolving the full Shimura-Taniyama conjecture, which was achieved by Breuil, Conrad, Diamond, and Taylor [BCDT01], but in groundbreaking work thereafter on the Fontaine-Mazur conjecture by Kisin [Kis], on the Serre conjectures by Khare and Wintenberger [KWa, KWb], and on the Sato-Tate conjecture by Clozel, Harris, Shepard-Barron, and Taylor [CHT08, Tay08, HSBT]. Our primary interest, however, will not be in studying the successful generalizations or applications of the work of Wiles and Taylor-Wiles. Rather, we will examine and demonstrate by example several improvements to Wiles' methods that have been transformative in enabling these applications.

In this vein, we mention some new improvements of Kisin [Kis], Diamond [Dia97], and Faltings [TW95, Appendix] to the Wiles and Taylor-Wiles methodology. Kisin developed a notion of *framed* deformation of Galois representations. While the spectra of Mazur's deformation rings $R$ correspond to distinct equivalence classes of representations, Kisin's rings correspond to representations. While the rings in Mazur's construction occasionally fails to exist, Kisin's rings exist in great generality. By *locally* framing at a prime $p$, one can apply deformation conditions at $p$ that may not otherwise have been possible. See Section 2.1.3 for an account of the history and development of Galois deformation theory.

The other major improvement we use is due to Faltings, Diamond, and Kisin. They reorganized the "patching criterion" of Taylor-Wiles, which is used in the final stages of the proof that $R$ and $\mathbf{T}$ are (near-)isomorphic. The patching criterion we present in Section 6 is a slight variant on Diamond's criterion, though it uses ideas of Kisin in order to accomodate framed deformation rings. The original goal of Diamond's reorganization of the patching criterion was to obtain Mazur's multiplicity one result [Maz78] as a corollary of the Taylor-Wiles argument rather than to assume it. The step which allows Diamond to conclude Mazur's theorem will, in our situation, tell us the precise Krull dimension of all of the deformation rings involved in our construction.

## 1.4 Our Goal

Our goal is primarily an expository one, but we do so via an original demonstration of existing techniques rather than a strict presentation of existing material. Kisin [Kis] proves a very general modularity lifting theorem using difficult techniques from $p$-adic Hodge theory and the theory of finite flat group schemes. We make no use of these techniques here, and work in a case where these methods can be bypassed. Kisin studies a local lifting ring, applying the aforementioned techniques to bound its dimension and to work around the possibility that it may not be an integral domain. We instead carry out an explicit analysis of this ring in a very special case, allowing us to bound its dimension and show that the ring is an integral domain. In doing so we make use of the explicit description of the local deformation ring in a crucial way. We use the same framed deformation techniques, including a modification of the definition of the Selmer group and the associated duality results, that Kisin employs. In summary, we illustrate one of Kisin's innovations in a context where the situation lines up well, allowing us to proceed without much of the general machinery. While the result itself is too specialized to find many applications, our methodology explicitly reveals the mechanics of local deformation theory as it feeds into the Wiles and Taylor-Wiles strategy.

The technical heart of our work is Section 3, which deals with *local* deformation theory, meaning that one looks at how deformations behave only at a subgroup $G_{\mathbf{Q}_p} \subset G_{\mathbf{Q}}$ corresponding to the prime $p$. We find ourselves in the situation for which Kisin developed framed deformation – the local deformation problems cannot be studied using Mazur's deformation rings. The global deformation theory is presented in Section 4, which adapts the argument presented in the survey article of Darmon, Diamond, and Taylor [DDT97] to the framed setting.

As our demonstration of the aforementioned techniques, we prove a theorem that roughly says the following.

**Main Theorem 1.** *Let $K/\mathbf{Q}_p$ be a finite extension with ring of integers $\mathfrak{O}_K$ and residue field $k$. Suppose that the continuous group homomorphism $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_K)$ satisfies the following conditions, as well as additional technical limitations on the conductor $N(\overline{\rho})$:*

1. *The residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$ is absolutely irreducible, odd, modular, and unramified outside a finite set of primes.*
2. *The restriction $\overline{\rho}|_{G_{\mathbf{Q}_p}}$ is trivial.*
3. *The restriction $\rho|_{G_{\mathbf{Q}_p}}$ is ordinary.*
4. *For all $\ell \neq p$, $\rho$ is minimally ramified at $\ell$.*
5. *The product $\epsilon \det \rho$ is tamely ramified at $p$.*

*Then $\rho$ is modular.*

The precise statement of this result is Theorem 6.1.

We note that we have only studied the "minimal case" of the modularity lifting problem. We expect that using additional methods from Kisin's paper [Kis], one could extend the results of Sections 5 and 6 to encompass the general case as well. We remark that due to work of Khare and Wintenberger [KWa, KWb], the first condition in the Main Theorem is a mild one.

## 1.5 The Strategy

In order to prove that deformations are modular, we will compare rings $R$ and $\mathbf{T}$. The ring $\mathbf{T}$ acts on a space $S$ of modular forms. In order to understand the relationship between $R, \mathbf{T}$, and $S$, we will need to build an entire family of rings $R_n$ and $\mathbf{T}_n$ acting on a family of $\mathbf{T}_n$-modules $S_n$. Every member of these families will have an action from a group ring $W(k)[\Delta_{Q_n}]$ such that $R_n/\mathfrak{a}_n R_n = R$ and $S_n/\mathfrak{a}_n S_n = S$, where $\mathfrak{a}_n$ is the *augmentation ideal* of $W(k)[\Delta_{Q_n}]$, which is generated by multiples of $g - 1$ for $g \in \Delta_{Q_n}$. The group $\Delta_{Q_n}$ is the product of $p$-groups of increasing size that are subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$ for choices of "auxilliary primes" $q$. All of these objects fit into the diagram

$$\begin{tikzcd}
A \arrow[dr, "\varphi_n"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& B \arrow[r, "\mu_n"] \arrow[d, "\psi_n"] & \mathrm{End}(S_n) \arrow[d, "\pi_n"] \\
& R \arrow[r] & \mathrm{End}(S)
\end{tikzcd},$$

where $A$ is a "limiting ring" $W(k)[[s_1, \ldots, s_r]]$ for the rings $W(k)[\Delta_{Q_n}]$ and $B$ is a ring of Krull dimension $r+1$ that can surject onto each of the $R_n$.

The main idea is that $W(k)[\Delta_{Q_n}]$ approximates the free ring $W(k)[[s_1, \ldots, s_r]]$ on a fixed number of generators as $n$ grows large, while $S_n$ is always free over $W(k)[\Delta_{Q_n}]$. By "sandwiching" a ring $R_n$ of Krull dimension at most $r$ as an intermediate ring for the action of $W(k)[[s_1, \ldots, s_r]]$ on the ring $S_n$, we find that $S_n$ should be a "nice" module over $R_n$. This conclusion comes from the theory of Cohen-Macaulay modules over a local ring. It is a simple algebraic maneuver to translate the conclusions one derives from the action of $R$ on $S$ into a comparison between $R$ and $\mathbf{T}$.

In order to fit all of the objects just described into this picture, we need to know that $S_n/\mathfrak{a}_n S_n = S$ and that the $S_n$ are free over $W(k)[\Delta_{Q_n}]$. This requires an understanding of the $\Delta_{Q_n}$-action as it factors through $R_n$. Moreover, the proof makes use of topological arguments regarding cohomology groups of modular curves. We also need to bound the dimension of the rings $R_n$. One can show using the above setup that $R_n$ cannot have Krull dimension less than $r+1$, so any argument that achieves the necessary bound has to *optimize* each relevant computation in order for the proof to succeed.

If one proceeds as in Wiles and Taylor-Wiles' proof of the minimal case, one finds quickly that the behavior at $p$ cannot be measured using their methodology. The Selmer group approach yields a contribution of 6 to the global Selmer group dimension, when one expects the contribution to be 4. This inconsistency is a result of singular behavior in the local deformation theory. As mentioned earlier, we use *explicit* local deformation theoretic techniques to replace the Selmer group calculation with a direct determination of the Krull dimension and other properties of the local ring. Then Kisin's [Kis] framed deformation theory allows one to neatly replace the local Selmer group at $p$ with the explicit computation in the argument, thereby obtaining the needed bound.

## 1.6 Local Geometry of Ordinary Liftings

Our secondary goal in this thesis is to expose particularly interesting geometry for a certain deformation problem that has not yet been studied explicitly. In particular, the residual representations we consider will be trivial when restricted to $G_{\mathbf{Q}_p}$. The local deformation theory is peculiar in our case. The restriction $\overline{\rho}|_{G_{\mathbf{Q}_p}}$ of the residual representation is ordinary, so we study ordinary liftings of $\overline{\rho}$. However, the residual representation does not determine a filtration of the underlying vector space $k^2$, so the filtration space for ordinary liftings $\rho$ already has the geometrically interesting structure of $\mathbf{P}^1_k$, the projective line over $k$. As a result, we find a *formal scheme* $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ fibered over $\mathbf{P}^1_k$ rather than a ring as the representing object for our deformation problem, in contrast to essentially every other 2-dimensional deformation problem imaginable.

This creates significant troubles when attempting to conduct the usual Taylor-Wiles argument, since one cannot expect a local ring $\mathbf{T}$ to be easily comparable to a formal scheme fibered over $\mathbf{P}^1_k$. The key step is to replace $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ by its image in the formal spectrum of the local lifting ring $\operatorname{Spf} R^{\mathrm{loc}}_p$. While the resulting ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ cannot solve the original deformation problem for all rings, we prove in Proposition 3.7 that when restricting the deformation to the subcategory of discrete valuation rings (DVR), it suffices. We use the explicit description of $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ to bound its Krull dimension in Proposition 3.8 and use a criterion of Taylor [Tay09], presented in Proposition 3.11, to build a local deformation problem out of $R^{\mathrm{loc}}_{p,\mathrm{ord}}$.

We point out that while the unusual behavior just described is unique to the residually trivial case in dimension 2, it exists when solving reducible deformation problems in many cases for higher dimensions. In these cases, depending on the condition being studied, the formal schemes that arise could be fibered over larger projective spaces or Grassmannians. Perhaps with more exotic deformation conditions, other spaces may arise. The key advantage we exploit in our local deformation computations is Fact 2.3, which provides us with a very convenient structure for the local lifting ring $R^{\mathrm{loc}}_p$. While in the cases where the residual representation is not trivial, one cannot apply Fact 2.3 directly, one still can reduce to the maximal quotient of $G_{\mathbf{Q}_p}$ such that $\ker\overline{\rho}$ becomes pro-$p$. This could potentially simplify the deformation problem. The explicit description of the ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ was crucial in our proofs of both Propositions 3.7 and 3.8.

The ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ may be used as the base ring for constructing global framing rings satisfying a universal property for DVRs. However, $\mathbf{T}$ is not a DVR, so the construction of a natural map $R \to \mathbf{T}$ is not entirely automatic. By using the fact that the ring $\mathbf{T}$ may be built (following a construction of Carayol [Car94]) out of a product of discrete valuation rings, we argue in Proposition 5.8 that the usual $R \to \mathbf{T}$ map can be constructed and is unique even though $\mathbf{T}$ is not in our category.

## 1.7 Structure

We have the following organization for the paper.

- Section 2 presents some background on representations, automorphic forms, and algebraic geometry.
- Section 3 constructs the ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ and proves its necessary properties.
- Section 4 constructs the ring $R_{\emptyset,\mathrm{ord}}$ and a family $R_{Q_n,\mathrm{ord}}$ of related rings and proves several of their key properties.

- Section 5 constructs $\mathbf{T}_\emptyset$ and the family $\{\mathbf{T}_{Q_n}\}$, and proves several key properties of these rings and their modules $S_\emptyset$ and $S_{Q_n}$.
- Section 6 uses the preceding objects and an abstract theorem in commutative algebra to prove the key isomorphism
$$R_\emptyset/\mathfrak{N} \xrightarrow{\sim} \mathbf{T}_\emptyset,$$
from which Theorem 6.1 follows.

We assume familiarily with basic algebra, number theory, and topology, but otherwise present all facts used in Section 2 or in the section where the fact is used. In particular, we assume no familiarity with modular forms or Galois representation theory.

# Chapter 2

# Preliminaries

As described in Section 1, the global structure of the proof of Theorem 6.1 will encompass three worlds: Galois representations, modular forms, and commutative algebra. In this section we state some of the results of interest to us in each of these areas, as well as provide definitions for the basic notions. We also provide in Section 2.1.3 a historic overview of deformation theory, which is the area in which we most substantially extend the arguments of Wiles and Taylor-Wiles for the proof of Theorem 6.1.

## 2.1 Galois Representations

As discussed in Section 1, Galois representation theory is our most promising avenue for discovering new structural information about the global Galois group $G_{\mathbf{Q}}$. We present some of the technical algebraic machinery we will need in order to study deformations of Galois representations in Sections 3 and 4.

### 2.1.1 Group Theory

We will need to know the possible behaviors for the residual representation $\overline{\rho}$. In fact, we will make use of group cohomology in order to relate the dimension of the space of possible liftings of $\overline{\rho}$ to properties of $\overline{\rho}$ itself. However, in order to compute with group cohomology, one needs to know the possibilities for a certain action, called the adjoint action, of $G_{\mathbf{Q}}$ induced by $\overline{\rho}$. For this we will require a full classification of the 2-dimensional projective representations of finite groups.

**Fact 2.1** ([Lan95]). *Let $H \subseteq \mathrm{PGL}_2(\overline{\mathbf{F}_p})$ be a finite subgroup. Then one of the following is true.*

- *The subgroup $H$ is conjugate to a subgroup of the upper triangular matrices.*
- *The subgroup $H$ is conjugate to $\mathrm{PSL}_2(\mathbf{F}_{p^r})$ or $\mathrm{PGL}_2(\mathbf{F}_{p^r})$ for some $r \geq 1$.*

- *The subgroup $H$ is isomorphic to $A_4, A_5, S_4$, or the dihedral group $D_{2r}$ of order $2r$ with $r \geq 2$, $p \nmid r$.*

*In the case that $H$ is isomorphic to $D_{2r}$ with $r \geq 2, p \nmid r$, we may explicitly describe the embedding of $H = \langle s, t : s^2 = t^r = 1, sts = t^{-1} \rangle$ as being conjugate to*

$$s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, t \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix},$$

*where $\zeta$ is a primitive $r^{th}$ root of unity, possibly after an extension of degree 2.*

*The only subgroups of $\mathrm{PGL}_2(\overline{\mathbf{F}}_5)$ isomorphic to $A_5$ are conjugate to $\mathrm{PSL}_2(\mathbf{F}_5)$.*

We will also make use of various methods from the area of group cohomology, including certain arithmetic duality theorems. We refer the reader to an article of Atiyah and Wall [CF86] for background on group cohomology, though we discuss arithmetic duality in Section 4.5. We will be interested only in the groups $H^0(G, M)$ and $H^1(G, M)$, where $G$ is a group and $M$ is a $G$-module. We define

$$\begin{aligned} H^0(G, M) &= M^G = \{m \in M : gm = m \text{ for all } g \in G\} \\ H^1(G, M) &= \frac{\{\varphi : G \to M | \varphi(g_1 g_2) = \varphi(g_1) + g_1 \varphi(g_2) \text{ for all } g_1, g_2 \in G\}}{\{\phi : g \mapsto gm - m | m \in M\}}. \end{aligned}$$

### 2.1.2 Algebraic Number Theory

The algebraic approach to number theory was initiated by Kummer in his approach to proving Fermat's Last Theorem. In this section we briefly describe the basic notions of algebraic number theory.

We define $G_K$ to be the absolute Galois group of a field $K$. If $K$ is a global field and $S$ a finite set of places of $K$, we write $G_{K,S}$ for the Galois group of the maximal extension unramified away from $S$. Throughout we will fix a choice of decomposition group $G_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}}$ for each prime $p$.

The decomposition group $G_{\mathbf{Q}_p}$ is naturally isomorphic to the absolute Galois group of $\mathbf{Q}_p$. We have subgroups $I_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}_p}$ and $P_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}_p}$ corresponding to the maximal unramified extension $\mathbf{Q}^{\mathrm{ur}}$ and maximal tamely ramified extension $\mathbf{Q}^{\mathrm{tr}}$. The group $P_{\mathbf{Q}_p}$ is a $p$-group. For the quotient $G_{\mathbf{Q}_p}/P_{\mathbf{Q}_p} = \mathrm{Gal}(\mathbf{Q}_p^{\mathrm{tr}}/\mathbf{Q}_p)$, we have a structure theorem, due to Iwasawa.

**Fact 2.2** ([NSW08, Theorems 7.5.2, 7.5.3])**.** *Let $\langle \mathrm{Frob}_p \rangle \cong \widehat{\mathbf{Z}}$ be the absolute Galois group of the residue field $\mathbf{F}_p$ of $\mathbf{Z}_p$. We have*

$$\widehat{\mathbf{Z}}^{(p)} = \prod_{\ell \neq p} \mathbf{Z}_\ell \cong I_{\mathbf{Q}_p}/P_{\mathbf{Q}_p}.$$

*Moreover, we have a split group extension*

$$0 \to \widehat{\mathbf{Z}}^{(p)} \to \mathrm{Gal}(\mathbf{Q}_p^{tr}/\mathbf{Q}_p) \to \langle \mathrm{Frob}_p \rangle \to 0$$

*where the action of* $\mathrm{Frob}_p$ *on* $\tau \in \widehat{\mathbf{Z}}^{(p)}$ *is*

$$(\mathrm{Frob}_p)\tau(\mathrm{Frob}_p)^{-1} = \tau^q.$$

The *cyclotomic character* $\epsilon_p : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is defined by taking the limit over $n$ of the quotient homomorphisms

$$G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}_{\zeta_{p^n}}/\mathbf{Q}) \cong (\mathbf{Z}/p^n\mathbf{Z})^\times.$$

We shorten $\epsilon_p$ to $\epsilon$ since we will use only the $p$-adic cyclotomic character.

There is a natural homomorphism $\tau_p : \mathbf{F}_p^\times \to \mathbf{Z}_p^\times$, sending each element $\alpha \in \mathbf{F}_p^\times$ to an element of $\mathbf{Z}_p^\times$ that lifts $\alpha$ and is also a $p-1^{\mathrm{st}}$ root of unity. This map is called the Teichmüller lift. We can construct a character $\omega_p : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ as the composition

$$\omega_p : G_{\mathbf{Q}} \xrightarrow{\epsilon_p} \mathbf{Z}_p^\times \to \mathbf{F}_p^\times \xrightarrow{\tau_p} \mathbf{Z}_p^\times,$$

where the second map is the reduction map modulo $p$. This will be used in constructing an explicit residually trivial determinant character for Theorem 6.1.

The exact structure of the groups $G_{\mathbf{Q}_p}$ is known for $p > 2$. We will only need here a result concerning the maximal pro-$p$ quotient of this absolute Galois group.

**Fact 2.3** ([NSW08, Theorem 7.5.11])**.** *If* $p > 2$*, then the group* $G_{\mathbf{Q}_p}(p)$ *is the free pro-p group on two generators.*

*Remark* 1. The generators of $G_{\mathbf{Q}_p}(p)$ can be taken to be a Frobenius lift $\sigma$ and an element $\tau \in I_{\mathbf{Q}_p}$ such that $\psi(\sigma) = 1$ and $\psi(\tau) = 1 - p$, where $\psi$ is the product of the cyclotomic character and the multiplicative inverse of the Teichmüller lift. In particular, given some choice of Frobenius lift $\sigma$, we replace it by $\sigma\tau_0^{-1}$ where $\psi(\sigma) = \psi(\tau_0)$ and $\tau_0 \in I_{\mathbf{Q}_p}$. This hypothesis will be used in Section 3.

We lastly mention that we use the notation $\mathrm{Frob}_p$ for the generator of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ that sends $x \mapsto x^p$. This map is called the arithmetic Frobenius automorphism. Due to certain conventions that we have chosen, we will often make use of the *geometric* Frobenius automorphism, which we denote by $\mathrm{Frob}_p^{-1}$ (as it is the inverse of the arithmetic Frobenius automorphism). We will also use $\mathrm{Frob}_p$ and $\mathrm{Frob}_p^{-1}$ to denote lifts of these elements to $G_{\mathbf{Q}_p}$ or $G_{\mathbf{Q}}$.

### 2.1.3 Deformation Theory

#### History

Mazur [Maz89] developed a deformation theory for Galois representations. Mazur was initially interested both in the geometry of the deformation spaces and in using deformation theory as an algebraic approach to determining which members of a family of $p$-adic Galois representations are modular. Motivated by a construction of Hida [Hid86], Mazur and

Wiles [MW86] constructed a ring $\mathbf{T}$ and universal modular representation $\rho^{\mathrm{mod}}$ parametrizing families of modular $p$-adic representations. Mazur sought a ring $R$ parametrizing all representations expected to be modular, so that one could prove modularity for this entire family via a single isomorphism $R \cong \mathbf{T}$.

Concretely, a $p$-adic Galois representation is a morphism

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_N(R)$$

for a ring $R$ such that for all but finitely many primes $r$, the image of $I_{\mathbf{Q}_r}$ is trivial. The representations $\rho$ and $\rho'$ are said to be strictly equivalent if $\rho = \alpha\rho\alpha^{-1}$ for $\alpha \in \mathbf{1}_2 + \mathbf{M}_2(\mathfrak{m}_R)$, where $\mathbf{1}_2$ is the $2 \times 2$ identity matrix and $\mathbf{M}_2(\mathfrak{a})$ denotes, for an ideal $\mathfrak{a} \subseteq R$, the ring of $2 \times 2$ matrices with coefficients in $\mathfrak{a}$. In the construction of Mazur and Wiles, maps $\mathbf{T} \to \mathfrak{O}_K$ correspond to strict equivalence classes of modular $p$-adic representations $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_K)$ lifting a fixed residual representation $\overline{\rho}$. Mazur [Maz89] compared $\mathbf{T}$ to a ring $R$ with the property that maps $R \to R'$ correspond to strict equivalence classes of representations $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R')$ lifting $\overline{\rho}$ that have additional properties, such as having a fixed determinant and being ordinary when restricted to $G_{\mathbf{Q}_p}$, that the modular representations parametrized by $\mathbf{T}$ shared. Moreover, the maps $\rho$ are all induced by projection from a single universal representation $\rho^{\mathrm{univ}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$.

Using the universal property of $R$, Mazur was able to show that there existed a natural surjective homomorphism $R \twoheadrightarrow \mathbf{T}$. In a very special case where the representation $\overline{\rho}$ is a fixed dihedral representation, Mazur was able to construct $R$ explicitly and show that the map $R \twoheadrightarrow \mathbf{T}$ is an isomorphism.

The main technical results in deformation theory are various existence theorems. Assuming that $\overline{\rho}$ is absolutely irreducible, universal deformation rings exist in a fairly general setting. However, for representations that are not absolutely irreducible, one needs to construct objects with weaker properties.

The constructions of universal deformation rings tend to be fairly abstract, so it is difficult to imagine how one would write the rings down explicitly. After Mazur's introduction of deformation theory, Boston and Mazur [Bos91, BM89] were able to solve deformation problems in certain specific cases explicitly. In many cases, such as the aforementioned scenario where $\overline{\rho}$ is dihedral, the deformation problem is *unobstructed*, meaning the ring $R$ is topologically freely generated. The more interesting cases are those where there are nontrivial relations on the ring $R$. In this case we say that $R$ is *obstructed*.

**Example 1** ([BU93, Theorem 7.6])**.** Boston and Ullom have shown that the residual Galois representation

$$G_{\mathbf{Q},\{3,7,\infty\}} \to \mathrm{GL}_2(\mathbf{F}_3)$$

associated to the 3-division points of the elliptic curve $X_0(49)$ has universal deformation ring

$$\mathbf{Z}_3[[t_1, t_2, t_3, t_4]]/((1+t_4)^3 - 1).$$

Mazur [Maz97] showed that the number of topological generators of $R$ can be measured using Galois cohomology. The Krull dimension can be bounded above and below in terms of cohomology groups. Wiles [Wil95] defined an analogue of the Selmer group of an elliptic curve for a family of deformation conditions and proved a duality theorem for these groups. This theorem was then used to bound the size of the deformation rings arising in the proof of Fermat's Last Theorem.

The main technical advance in the deformation theory of Galois representations after Wiles' work is Kisin's introduction of *framed* deformation rings [Kis], which hold information about a lifting of the representation at certain primes. Taylor [Tay08] made significant use of this technique in his work on the Sato-Tate conjecture, particularly to study modularity questions for liftings of representations that are not minimally ramified. Khare and Wintenberger [KWa, KWb] also made use of framed deformation in their work on the Serre conjectures. One can write down a Selmer group for framed deformation rings, and a generalization of Wiles' duality theorem holds in this setting. We briefly discuss framed deformation rings later in this section. We construct relevant framed deformation problems in Sections 4.2 and 4.3 and use duality on Selmer groups to bound the size of deformation rings in Sections 4.4 and 4.5.

### Overview

The deformation theory of $p$-adic representations is defined with respect to a profinite group $\Pi$, a complete Noetherian local ring $A$, and fixed base representation $\overline{\rho} : \Pi \to \mathrm{GL}_N(A)$. In practice, $A$ is frequently chosen to be a finite residue field $k$, and in this case $\overline{\rho}$ is referred to as the *residual* representation. A deformation of $\overline{\rho}$ to a ring $A'$ with respect to a homomorphism $f : A' \to A$ is simply a map $\rho : \Pi \to \mathrm{GL}_2(A')$ such that the composition of $\rho$ with the projection $\mathrm{GL}_2(A') \to \mathrm{GL}_2(A)$ induced by $f$ is $\overline{\rho}$. We phrase this in terms of a functor $D$ taking a suitable category of rings $A'$ to the set of possible deformations.

The goal of deformation theory is to have as "clean" a description as possible for all the liftings of $\overline{\rho}$. The ideal situation is that $D$ be *representable*, meaning that there exists an isomorphism $D \cong \mathrm{Hom}(A', \cdot)$ for some object $A'$ in the category under consideration. Thus the main technical issue within deformation theory is the question of representability of a given deformation functor.

Grothendieck [Gro95] proved an elegant necessary and sufficient criterion for representability, but this criterion is difficult to check in practice. Mazur [Maz89] proved the existence theorem using a refinement of Grothendieck's criterion obtained by Schlessinger [Sch68]. We remark that Lenstra and de Smit [dSL97] and Dickinson [Gou01, Appendix 1] have given proofs of existence for deformation rings for absolutely irreducible $\overline{\rho}$ directly from Grothendieck's criterion in the more general setting of rings that are not necessary noetherian.

Even in the case where a deformation functor $D$ is not representable, Schlessinger [Sch68] guarantees the existence of a "hull," which has the disadvantages that it satisfies a weaker condition and is not unique up to *unique* isomorphism. We refer the reader to Mazur's survey [Maz97] for the details, since in this paper we instead use the idea of Kisin [Kis] of changing the functor $D$ to be "framed" in order to avoid issues of non-representability.

### Setting

One works over the category $\mathbf{CLNRings}(\Lambda)$ of complete local Noetherian rings over a fixed coefficient-ring $\Lambda$ with finite residue field $k$. The morphisms in this category are *coefficient-ring homomorphisms*, which for a map $f : R \to R'$ means that $f^{-1}(\mathfrak{m}_{R'}) = \mathfrak{m}_R$ and $R/\mathfrak{m}_R \cong R'/\mathfrak{m}_{R'}$. In particular, all objects $\mathbf{CLNRings}(\Lambda)$ share the residue field $k$. By the universal property of the ring $W(k)$ of Witt vectors of $k$, there is a homomorphism $W(k) \to R$ for any complete local Noetherian coefficient ring $R$ with residue field $k$. For this reason, in practice, we will in fact set $\Lambda = W(k)$, and abbreviate $\mathbf{CLNRings}(W(k))$ to $\mathbf{CLNRings}(k)$. If we are in the "relative" setting described above, where the base representation is $\overline{\rho} : \Pi \to \mathrm{GL}_N(A)$ for $A \neq k$, then one also asks for every object to be equipped with an $A$-augmentation. This will not be necessary for our purposes – see Mazur's survey [Maz97] for a treatment at this level of generality.

**Definition 1.** Let $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$ be a representation. We define $D_{\overline{\rho}} : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ to be the functor

$$R \mapsto \{\text{strict equivalence classes of } \rho : \Pi \to \mathrm{GL}_2(R) : \rho \text{ lifts } \overline{\rho}\}.$$

If $D_{\overline{\rho}}$ is representable, we call the representing ring $R_{\overline{\rho}}$.

### Representability

The criteria for representability of functors make central use of the notion of a *Cartesian square*. Given a diagram

$$\begin{tikzcd} A \arrow[dr, "\alpha"] & & B \arrow[dl, "\beta"'] \\ & C & \end{tikzcd},$$

in a category $\mathcal{C}$, one defines the fiber product $A \times_C B$ to fill in the diagram

$$\begin{tikzcd} & A \times_C B \arrow[dl, "\pi_A"'] \arrow[dr, "\pi_B"] & \\ A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\ & C & \end{tikzcd} \tag{2.1}$$

and satisfy the universal property that for all objects $D$ with maps $D \to A$ and $D \to B$ making

$$\begin{tikzcd} & D \arrow[dl] \arrow[dr] & \\ A \arrow[dr] & & B \arrow[dl] \\ & C & \end{tikzcd}$$

commute, the maps factor through a unique map $D \to A \times_C B$. In the category of sets, fiber products exist and are given by $A \times_C B = \{(a,b) \in A \times B | \alpha(a) = \beta(b)\}$. We call (2.1) meeting this universal property a Cartesian square.

For a category $\mathcal{C}$, object $X \in \mathrm{Ob}(\mathcal{C})$, and Cartesian square (2.1) in $\mathcal{C}$, the functor $\mathrm{Hom}(X, \cdot) : \mathcal{C} \to \mathbf{Sets}$ provides a natural isomorphism

$$\mathrm{Hom}(X, A \times_C B) \cong \mathrm{Hom}(A) \times_{\mathrm{Hom}(X,C)} \mathrm{Hom}(X, B).$$

This provides a necessary condition for a functor $D$ to be representable. In particular, for all Cartesian squares of the form (2.1), we must have an isomorphism of sets

$$D(A \times_C B) \cong D(A) \times_{D(C)} D(B).$$

The category $\mathbf{CLNRings}(k)$ is not closed under fiber product, so one needs to work over the full subcategory $\mathbf{CLARings}(k)$ of local Artinian rings over $W(k)$ instead. If a functor defined on $\mathbf{CLARings}(k)$ is representable by an object in $\mathbf{CLNRings}(k)$, it is said to be *pro-representable*. If a functor $D$ is *continuous*, meaning that for all rings $R \in \mathbf{CLNRings}(k)$,

$$\lim_{n \to \infty} D(R/\mathfrak{m}_R^n) = D(R),$$

then it is representable over $\mathbf{CLNRings}(k)$ if and only if it is pro-representable over the subcategory $\mathbf{CLARings}(k)$. Mazur's survey [Maz97] shows that the deformation functors $D_{\overline{\rho}}$ are continuous.

Since we are requiring our representing ring $R$ to be Noetherian, the tangent space $\mathrm{Hom}_k(\mathfrak{m}_R/(\mathfrak{m}_R^2 + \mathfrak{m}_{W(k)}), k)$ will be finite-dimensional. In particular, $\mathrm{Hom}(R, k[\delta]/\delta^2)$ will be a finite-dimensional $k$-vector space. Thus, we expect the set $D(k[\delta]/\delta^2)$, which we think of as the tangent space of $D$, to be finite. In fact, these observations provide a necessary and sufficient criterion for representability.

**Fact 2.4** ([Gro95]). *Let $k$ be a finite field and let $D : \mathbf{CLARings}(k) \to \mathbf{Sets}$ be a functor such that such that $D(k)$ consists of a single element. Then $D$ is pro-representable if and only if $D$ preserves Cartesian squares and $D(k[\delta]/\delta^2)$ is finite.*

Schlessinger refines Grothendieck's result by requiring that only certain Cartesian squares be preserved. Call a mapping $A \to B$ of objects of $\mathbf{CLARings}(k)$ *small* if its kernel is a principal ideal annihilated by $\mathfrak{m}_A$.

**Fact 2.5** ([Sch68]). *Let $k$ and $D$ be as in Fact 2.4. Given a Cartesian square of the form in (2.1), we denote the induced map by $h : D(A \times_C B) \cong D(A) \times_{D(C)} D(B)$. Then $D$ is pro-representable if and only if $D$ satisfies the following conditions.*

*H1. If $A \to C$ is small, then $h$ is surjective.*

*H2. If $A \to C$ is the map $k[\delta]/\delta^2 \to k$, then $h$ is bijective.*

*H3. The tangent space $D(k[\delta]/\delta^2)$ is finite.*

*H4. If $A \to C$ and $B \to C$ are the same map and small, then $h$ is bijective.*

Note that if $\Pi$ is the free group on a countably infinite set of generators and $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$ is any representation, the space $D_{\overline{\rho}}(k[\delta]/\delta^2)$ is infinite dimensional. It is not known whether the Galois group $G_{\mathbf{Q},S}$ is topologically finitely generated (this is a conjecture of Shafarevich), so we must find an alternative hypothesis. Mazur [Maz89] bypasses this difficulty by instead using the *p-finiteness condition*, which is the statement that $\mathrm{Hom}(\Pi, \mathbf{Z}/p\mathbf{Z})$ is finite. This hypothesis holds by class field theory for the groups $G_{\mathbf{Q},S}$.

We now state Mazur's result on representability.

**Fact 2.6** ([Maz97])**.** *Let $\Pi$ be a profinite group satisfying the p-finiteness condition. Let $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$ be a residual representation.*

- *The functor $D_{\overline{\rho}}$ satisfies H1, H2, and H3 of Fact 2.5.*
- *If $\overline{\rho}$ is absolutely irreducible, then $D_{\overline{\rho}}$ is representable.*

### Deformation Conditions

Since the representations arising from modular forms satisfy additional properties, we would like to study deformations of $\overline{\rho}$ satisfying additional properties. Although $\overline{\rho}$ must satisfy the somewhat stringent hypothesis of being absolutely irreducible for $D_{\overline{\rho}}$ to be representable, it is somewhat less difficult to apply conditions to the functor $D_{\overline{\rho}}$.

Given a representable functor $D : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ such that $D(k)$ contains a single element, a functor $D' : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ is a *subfunctor* of $D$ if $D'(R) \subseteq D(R)$ for all $R \in \mathrm{Ob}(\mathbf{CLNRings}(k))$ and $D'(k) = D(k)$.

A subfunctor $D'$ of $D$ is called *relatively representable* if for all Cartesian diagrams of the form in (2.1) we have a commutative diagram

$$\begin{tikzcd} D'(A \times_C B) \arrow[r] \arrow[d, "\subseteq"] & D'(A) \times_{D'(C)} D'(B) \arrow[d, "\subseteq"] \\ D(A \times_C B) \arrow[r] & D(A) \times_{D(C)} D(B) \end{tikzcd}.$$

If $D$ is representable, then a relatively representable subfunctor $D'$ of $D$ is representable as well. We will state sufficient conditions for a collection $L$ of lifts of $\overline{\rho}$ to constitute a relatively representable subfunctor of $D_{\overline{\rho}}$. For a ring homomorphism $f : A \to B$, we use the notation $f_*\rho$ to denote the *projection* of $\rho : \Pi \to \mathrm{GL}_2(A)$ to a map $f_*\rho : \Pi \to \mathrm{GL}_2(B)$.

**Definition 2.** We define a deformation condition for $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$ to be a collection $E$ of lifts satisfying the following properties.

1. The collection $E$ is closed under strict equivalence and projection.
2. For every diagram of the form in (2.1) in $\mathbf{CLNRings}(k)$ and representation $\rho : \Pi \to \mathrm{GL}_2(A \times_C B)$ lifting $\overline{\rho}$, the representation $\rho$ is a member of $E$ if both $\pi_{A*}\rho$ and $\pi_{B*}\rho$ are members of $E$.

*Remark* 2. Mazur [Maz97] adds a third condition that Dickinson [Gou01] has proved is implied by the other two conditions. If both conditions hold, the second condition is automatically an equivalence, since $\pi_{A*}\rho$ and $\pi_{B*}\rho$ are projections.

The first condition of Definition 2 amounts to saying that $E$ defines a subfunctor $D_E$ of $D_{\overline{\rho}}$, and the second condition implies that $D_E$ is relatively representable. In particular, we have the following result.

**Fact 2.7.** *Suppose that $E$ is a deformation condition for $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$. Then the functor $D_E : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ defined by*

$$D_E : R \mapsto \{\text{strict equivalence classes of } \rho : \Pi \to \mathrm{GL}_2(R) | \rho \text{ is a member of } E\}$$

*is a relatively representable subfunctor of $D_{\overline{\rho}}$.*

As an example, requiring a lifting of $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$ to have a fixed determinant character $\psi : \Pi \to W(k)$ is a deformation condition.

### Deformations of Galois Representations

We note that Definition 2 has the interesting property that given a representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$, if we have a deformation condition $E_v$ for lifts of $\overline{\rho}|_{G_v}$ for each place $v$, even if these restrictions are reducible, they define a global deformation condition $\mathfrak{E} = \{E_v\}$ for $\overline{\rho}$ – namely, a lift of $\overline{\rho}$ is in $\mathfrak{E}$ if its restrictions to $G_v$ are in $E_v$ for all $v$.

Such a condition $\mathfrak{E}$ is called a global Galois deformation condition. We will use the notion of a global Galois deformation condition to enforce particular behaviors at each prime. For example, we will require our $p$-adic representations to be *ordinary* at the prime $p$, which means that the representation takes the form

$$\rho|_{G_{\mathbf{Q}_p}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

with $\chi_1$ unramified and $\chi_2$ ramified, following the convention of Mazur [Maz97]. Note that this is the *opposite* of the convention used in Wiles's paper [Wil95] and in the survey article of Darmon, Diamond, and Taylor [DDT97]. We call a residual representation ordinary if

$$\overline{\rho}|_{G_{\mathbf{Q}_p}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

with $\chi_1$ unramified, but with no condition on $\chi_2$. The purpose of Section 3 is to analyze the local deformation theory for this condition.

### Framed Deformations

The framed deformation theory of Kisin can be seen as an enhancement to the locality of this approach. When possible, one computes local deformation rings in order to determine the global behavior of a deformation problem. Unfortunately, the local deformation rings may not exist, as $\overline{\rho}$ may become reducible upon restriction to a decomposition group $G_{\mathbf{Q}_p}$. However, a framed deformation ring exists in all cases.

**Definition 3.** Let $\overline{\rho} : \Pi \to \mathrm{GL}_2(k)$. We define the framed deformation functor $D_{\overline{\rho}}^{\square}$ : **CLNRings** $\to$ **Sets** by

$$D_{\overline{\rho}}^{\square} : R \mapsto \{\rho : \Pi \to \mathrm{GL}_2(R) | \rho \text{ lifts } \overline{\rho}\}.$$

The following result can be deduced from Fact 2.5.

**Fact 2.8** ([Kis]). *Let $\Pi$ be a profinite group satisfying the $p$-finiteness condition. Let $\overline{\rho}$ : $\Pi \to \mathrm{GL}_2(k)$ be a residual representation. The functor $D_{\overline{\rho}}^{\square}$ is representable.*

In practice, we will think of the framing as occurring at just the prime $p$ in a manner described in Section 4.

## 2.2 Automorphic Forms

The second general area of number theory we will deal with is that of automorphic forms. The notion of an automorphic form generalizes each of the defining properties of a modular form, defined in Section 2.2.1, so that it may be defined for Lie groups $G$ other than $\mathrm{SL}_2(\mathbf{R})$, and with respect to discrete subgroups other than those contained in $\mathrm{SL}_2(\mathbf{R})$. We will only be interested in modular forms here, but it is important to note that by work of Langlands, one expects a correspondence between automorphic forms and certain types of representations in great generality. Ideas from this area were important in proving some of the results, such as Fact 2.14, that we assume here.

### 2.2.1 Modular Forms

Modular forms are studied in many guises in fields outside of number theory, such as combinatorics, algebraic geometry, and physics. Modular forms can be viewed as functions on moduli spaces of elliptic curves, and they were first approached in the 19th century in this context. We will be interested primarily in their behavior as a module for the Hecke algebra. In fact, we will be less interested in modular forms in the usual sense than in modular curves themselves. In particular, we will not work with the spaces $S_k(\Gamma, \mathbf{C})$, but with the cohomology of modular curves. However, we will present the theory in the classical setting, and then explain how to pass to the cohomology of modular curves.

#### Definition

We denote by $\Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$ the *modular group*, which is defined by

$$\mathrm{SL}_2(\mathbf{Z}) = \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}.$$

More generally, we define certain subgroups of $\mathrm{SL}_2(\mathbf{Z})$, such as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}, \text{ and}$$
$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

Any subgroup of $\mathrm{SL}_2(\mathbf{Z})$ containing $\Gamma(N)$ for some $N$ is called a *congruence subgroup*. For a congruence subgroup $\Gamma$, the minimal $N$ such that $\Gamma \supseteq \Gamma(N)$ is called the *level* of $\Gamma$ and is denoted $N_\Gamma$. We define the quotient $Y_\Gamma = \Gamma \backslash \mathfrak{H}$ and define $X_\Gamma$ to be the compactification obtained by adjoining *cusps*, which will be discussed shortly.

Given any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, we define the *factor of automorphy* $j(\gamma, z) = cz + d$. One defines a meromorphic function $f : \mathfrak{H} \to \mathbf{C}$ to be *weakly modular of weight* $k$ for $\Gamma$ if

$$f(\gamma\tau) = j(\gamma, \tau)^k f(\tau) \text{ for all } \gamma \in \Gamma.$$

Since $\Gamma(N)$ contains the element $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$, every congruence subgroup $\Gamma$ contains $\left(\begin{smallmatrix} 1 & t_\Gamma \\ 0 & 1 \end{smallmatrix}\right)$ for some minimal $t_\Gamma \in \mathbf{Z}_{>1}$. One calls $t_\Gamma$ the *width* of the cusp at $\infty$. If $f$ is weakly modular of any weight $k$ for $\Gamma$, then $f(\tau + t_\Gamma) = f(\tau)$. Thus one can expand $f$ as a power series

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^{\frac{n}{t_\Gamma}}$$

centered at $\infty$, where $q = \exp(2\pi i \tau)$. If, in fact,

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^{\frac{n}{t_\Gamma}},$$

then we say $f$ is holomorphic at infinity. From here on, we restrict our attention to subgroups $\Gamma$ containing $\Gamma_1(N)$ for some $N$. In this case, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, so $t_\Gamma = 1$, and every weakly modular function can be expanded as a power series

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

We define $a_n(f)$ to be the corresponding coefficient of the expansion of $f$ at infinity.

However, for a congruence subgroup $\Gamma$, $\infty$ is not the only point of $\mathfrak{H}$ where $f$ may have interesting limiting behavior. The point $\infty$ is equivalent via $\mathrm{SL}_2(\mathbf{Z})$ to the points of $\mathbf{Q}$. We call the $\Gamma$-equivalence classes of points in $\mathbf{Q} \cup \{\infty\}$ *cusps*. By applying $\gamma \in \Gamma$ to move a given cusp $\frac{a}{b} \in \mathbf{Q}$ to infinity, one can use the discussion of the preceding paragraph to define holomorphicity at any cusp.

We define a *modular form* $f$ of weight $k$ for $\Gamma$ to be a weakly modular form of weight $k$ such that $f$ is holomorphic on $\mathfrak{H}$ and holomorphic at the cusps. We define a modular form $f$ to be a *cusp form* if $a_0(f(\gamma\tau)) = 0$ for all choices of $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. In other words, a cusp form vanishes at every cusp.

We denote by $M_k(\Gamma, \mathbf{C})$ and $S_k(\Gamma, \mathbf{C})$ the spaces of modular forms and cusp forms, respectively. The product of a modular form of weight $k$ with a modular form of weight $k'$ is a modular form of weight $k + k'$, so one can define a graded ring of modular forms. In what follows, however, we will be primarily interested in modular forms of weight 2.

We can decompose

$$M_k(\Gamma, \mathbf{C}) = S_k(\Gamma, \mathbf{C}) \oplus E_k(\Gamma, \mathbf{C})$$

where the space $E_k(\Gamma, \mathbf{C})$ is spanned by a set of forms, called *Eisenstein series*, each of which are 1 at a single cusp and vanish at the others.

#### Petersson Inner Product

We define an inner product $\langle \cdot, \cdot \rangle_\Gamma : S_k(\Gamma, \mathbf{C}) \times S_k(\Gamma, \mathbf{C}) \to \mathbf{C}$ by

$$\langle f, g \rangle_\Gamma = \mathrm{Vol}(\Gamma)^{-1} \int_{Y_\Gamma} f(\tau)\overline{g(\tau)} y^{k-2} dx dy,$$

where

$$\mathrm{Vol}(\Gamma) = \int_{Y_\Gamma} \frac{dx dy}{y^2}.$$

### 2.2.2 Hecke Algebras

Our primary interest will be not in the spaces of modular forms themselves, but in their interaction with a natural algebra $\mathbf{T}_{\Gamma,\mathbf{Z}}$, called the *Hecke algebra*, that acts on a space of modular forms. We will see that the Hecke algebra can be used to build the ring $\mathbf{T}$ described in Section 2.1.3. It will be sufficient for our purposes to set $\Gamma = \Gamma_1(N)$. The books of Miyake [Miy89] and Diamond and Shurman [DS05] provide general treatments of the subject.

#### Hecke Operators

We begin by defining the Hecke operator $\langle d \rangle$. We first observe that there is a homomorphism $\varphi : \Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times$ defined by

$$\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N.$$

We have $\ker \varphi = \Gamma_1(N)$. For a function $f \in M_k(\Gamma_1(N), \mathbf{Z})$ and matrix $\gamma \in \Gamma_0(N)$, consider the definition

$$(\gamma f)(\tau) = j(\gamma, z)^{-k} f(\gamma\tau).$$

Since $f$ is a modular form for $\Gamma_1(N)$, $\gamma f = f$ for $\gamma \in \Gamma_1(N)$. On the other hand, for $\gamma' \in \Gamma_1(N)$, we have

$$\begin{aligned}(\gamma f)(\gamma'\tau) &= j(\gamma,z)^{-k} f(\gamma\gamma'\tau) = j(\gamma,z)^{-k} f(\gamma''\gamma\tau) \\ &= j(\gamma,z)^{-k} j(\gamma'',z)^k f(\gamma\tau) = j(\gamma'',z)^k (\gamma f)(\tau)\end{aligned}$$

for $\gamma'' \in \Gamma_1(N)$ by the normality of $\Gamma_1(N) \subseteq \Gamma_0(N)$. This defines an action of $(\mathbf{Z}/N\mathbf{Z})^\times$ on $(\mathbf{Z}/N\mathbf{Z})^\times$ that we denote by $\langle\cdot\rangle$.

Following Diamond and Shurman [DS05, Proposition 5.2.2], we will define the Hecke operators $T_p$ for primes $p$ via their action on the Fourier series of a modular form at $\infty$. Let $f(\tau) = \sum_{n\geq 0} a_n q^n$ be a weight $k$ modular form on $\Gamma_1(N)$. Then we have

$$(T_p f)(\tau) = \begin{cases} \sum_{n=0}^{\infty} \left(a_{np}(f) + p^{k-1} a_{\frac{n}{p}}(\langle p\rangle f)\right) q^n & \text{if } p \nmid N \\ \sum_{n=0}^{\infty} a_{np}(f) q^n & \text{otherwise.}\end{cases}$$

If $p|N$, we will frequently denote $T_p$ by the alternate symbol $U_p$ to emphasize the distinction.

We note that the operators $T_p$ and $\langle d\rangle$ commute. One can extend the definition of $T_n$ to $\mathbf{Z}$ by the definitions

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p\rangle T_{p^{r-2}} \quad \text{and} \quad T_n T_m = T_{nm}$$

where $(n,m) = 1$ and $p$ is prime. Then the $T_n$ and $\langle d\rangle$ commute for all $n$.

### Definition of the Hecke Algebra

For a congruence subgroup $\Gamma$, we define $\mathbf{T}_{\Gamma,\mathbf{Z}}$ to be the subring of $\mathrm{End}(S_2(\Gamma,\mathbf{Z}))$ generated by the Hecke operators $T_n$ and $\langle d\rangle$ for all $n$ and $d$. We define $\mathbf{T}_{\Gamma,R} = \mathbf{T}_{\Gamma,\mathbf{Z}} \otimes_{\mathbf{Z}} R$ for any ring $R$. We will frequently drop the $\Gamma$ from the notation for $\mathbf{T}_{\Gamma,R}$ when it is understood.

The Hecke operators are normal with respect to the Petersson inner product, so one can choose an orthogonal basis for $S_2(\Gamma,\mathbf{C})$ of simultaneous eigenforms for $\mathbf{T}_{\Gamma,\mathbf{C}}$. From the definitions, one finds that $a_1(T_n f) = a_n(f)$. If $f$ is an eigenform under all of the Hecke operators, then $a_n(f) = a_1(T_n f) = \lambda_n a_1(f)$, where $\lambda_n$ is the $T_n$-eigenvalue of $f$. Thus if $f$ is normalized to have $a_1(f) = 1$, then $a_n(f) = \lambda_n$ for all $n$. In particular, the multiplicativity relations for the $T_n$ apply to the $a_n$. In fact, Hecke defined the Hecke operators in order to explain the multiplicativity of the coefficients of modular forms such as $\Delta$.

We have the following statement regarding the generators of $\mathbf{T}_{\Gamma,\mathbf{Z}}$.

**Fact 2.9** ([DDT97, Lemma 4.1]). *The Hecke algebra $\mathbf{T}_{\mathbf{Z}}$ for a congruence subgroup $\Gamma$ of level $N$ is generated by either of the following:*

1. *$T_n$ for $n \geq 1$.*
2. *$T_p$ for primes $p$ and $\langle d\rangle$ for $d \in (\mathbf{Z}/N\mathbf{Z})^\times$.*

**Nebentypus**

The Hecke operators $\langle\cdot\rangle$ provide a decomposition of the space of modular forms on $\Gamma_1(N)$. In particular, we have

$$S_k(\Gamma_1(N), \mathbf{C}) = \bigoplus_{\psi} S_k(\Gamma_0(N), \psi, \mathbf{C})$$

where the functions in $S_k(\Gamma_0(N), \psi, \mathbf{C})$ satisfy

$$f(\gamma\tau) = \psi(d) j(\gamma, \tau)^k f(\gamma)$$

for all $\gamma \in \Gamma_0(N)$, and the summand is over all characters $\psi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$. We say that such an $f$ has *Nebentypus character* $\psi$. For $f \in S_k(\Gamma_0(N), \psi, \mathbf{C})$ can see that $\langle d \rangle f = \psi(d)$ directly from the definition.

**Atkin-Lehner Theory**

If we further decompose the spaces $S_k(\Gamma_0(N), \psi, \mathbf{C})$, we can find eigenforms under all the $T_p$ for $p \nmid N$. One notices that $S_k(\Gamma_0(N), \psi, \mathbf{C}) \subseteq S_k(\Gamma_0(M), \psi, \mathbf{C})$ if $N|M$. We would like to distinguish modular forms $f$ that are "old" in the sense that they come from a smaller level from those that are "new." Assume that $M = Np$. One can check that if $f(\tau) \in S_k(\Gamma_0(N), \psi, \mathbf{C})$, one also has $p^{k-1} f(p\tau) \in S_k(\Gamma_0(Np), \psi, \mathbf{C})$. Thus, there are two distinct ways of producing forms of higher level from a given form $f$ – inclusion and precomposition with multiplication. We call an eigenform created in this manner an *oldform* of level $N$, and call an eigenform in the orthogonal complement to the space of oldforms a *newform* of level $N$. These spaces are preserved by the action of the Hecke algebra.

The theory of Atkin and Lehner [AL70] precisely describes the decomposition of the space $S_k(\Gamma_1(N), \psi, \mathbf{C})$ into spaces of oldforms and newforms. Let $\mathbf{T}'_{\Gamma_1(N),\mathbf{Z}}$ be the subring of $\mathbf{T}_{\Gamma_1(N),\mathbf{Z}}$ generated by the $T_n$ for $(n, N) = 1$.

**Fact 2.10** ([DDT97, Theorem 1.22]). *We can decompose the space $S_k(\Gamma_1(N), \mathbf{C})$ into an orthogonal direct sum of subspaces $S_f$ defined by*

$$S_f = \left\{ g \in S_k(\Gamma_1(N), \mathbf{C}) | Tg = \lambda_f(T) g \text{ for } T \in \mathbf{T}'_{\Gamma_1(N),\mathbf{Z}} \right\},$$

*where $\lambda_f$ is defined by $\lambda_f(T) f = Tf$, and $f$ is a newform of level $N_f$. Moreover, $S_f$ has as a basis $f(d\tau)$ for all $d | \frac{N}{N_f}$.*

One can prove this using the following result.

**Fact 2.11** ([DS05, Theorem 5.7.1]). *If $f \in S_k(\Gamma_1(N), \mathbf{C})$ has $a_n(f) = 0$ for $(n, N) = 1$, then*

$$f = \sum_{\substack{p|N \\ p \text{ prime}}} f_p(p\tau)$$

*for $f_p \in S_k\left(\Gamma_1\left(\frac{N}{p}\right), \mathbf{C}\right)$.*

If we are working with a space $S_k(\Gamma_1(N), \mathbf{C})$ of modular forms, we will call an eigenform $f$ of the operators $T_n$ with $(n, N) = 1$ a newform (without specifying a level) if $f$ is a newform of any level $N_f|N$, and call $f$ an oldform if it arose from a space of smaller level using the method of precomposition just described. Every oldform in $S_k(\Gamma_1(N_f), \mathbf{C})$ is associated to some newform. One can reinterpret Fact 2.11 as saying that we can detect whether an eigenform is an oldform or newform simply by examining whether its first coefficient vanishes. Moreover, it is not difficult to see that a newform is invariant under the entire Hecke algebra. In particular, for a newform $f$, the difference $T_n f - a_n(f)f$ is a newform. On the other hand, it has a vanishing first coefficient, so it is also an oldform. Thus $T_n f = a_n(f)f$.

Using Atkin-Lehner theory, one finds that over an algebraically closed field, the Hecke algebra behaves particularly neatly.

**Fact 2.12** ([DDT97, Lemma 1.35]). *Let $\mathbf{F}$ be an algebraically closed field. Let $\{g_i\}$ be a complete set of newforms for $S_2(\Gamma_1(N), \mathbf{F})$, and let*

$$g = \sum_i g_i \left( \frac{N}{N_g} \tau \right).$$

*Then the map $T \mapsto Tg$ makes $S_2(\Gamma_1(N), \mathbf{F})$ into a rank 1 $\mathbf{T}_{\Gamma_1(N),\mathbf{F}}$-algebra.*

### Newforms

We state without proof some properties of coefficients of weight 2 newforms. Note that item (1) below is a deep result of Deligne.

**Fact 2.13** ([DDT97, Theorem 1.27]). *Let $f$ be a weight 2 newform of level $N_f$ and character $\psi$. Let the conductor of $\psi$ be denoted $N_\psi$.*

1. *If $p \nmid N_f$, then $|a_p| \leq 2\sqrt{p}$.*
2. *If $p$ exactly divides $N_f$ and $p \nmid N_\psi$, then $a_p^2 = \psi_0(p)$, where $\psi_0$ is the primitive character associated to $\psi$.*
3. *If $p|N_f$ and $p \nmid \frac{N_f}{N_\psi}$, then $|a_p| = \sqrt{p}$.*
4. *If $p^2|N_f$ and $p|\frac{N_f}{N_\psi}$, then $a_p = 0$.*

### Cohomology of Modular Curves

Using the action of the Hecke algebras on lattices, it is possible to define a Hecke action directly on the cohomology group $H^1(X_\Gamma, \mathbf{Z})$. The $\mathbf{Z}$-rank of this group is twice the rank of $S_2(\Gamma, \mathbf{Z})$. However, the action of complex conjugation on the underlying curve $X_\Gamma$ commutes with the Hecke algebra, so that we obtain Hecke modules $H^1(X_\Gamma, \mathbf{Z})^+$ and $H^1(X_\Gamma, \mathbf{Z})^-$ corresponding to the eigenspaces of this action. Moreover, the eigenforms in $H^1(X_\Gamma, \overline{\mathbf{Q}})^-$ give the same eigenvalues as the eigenforms in $S_2(\Gamma, \overline{\mathbf{Q}})$, and similarly for any other algebraically closed field.

While the $\mathbf{Z}$-structure of the spaces $S_2(\Gamma, \mathbf{Z})$ and $H^1(X_\Gamma, \mathbf{Z})^-$ are different, which complicates certain arithmetic geometry arguments, it will suffice for our purposes to work with $H^1(X_\Gamma, \mathbf{Z})^-$.

We make the following definitions. Since the normalization $a_1(f) = 1$ does not make sense in this context, we instead consider 1-dimensional subspaces, and define $a_n(f)$ for a $T_n$-eigenform $f$ to be the $T_n$-eigenvalue of $f$. Denoting the projectivization of the vector space $V$ by $\mathbf{P}V$, we say that $[f] \in \mathbf{P}H^1(X_1(N), \overline{\mathbf{Q}})^-$ is a newform of level $N_f$ if $[f]$ has the same eigenvalues as a newform in $S_2(\Gamma_1(N_f), \overline{\mathbf{Q}})$. (This allows us to apply the aforementioned results of the classical theory of modular forms.) We say that $[f]$ is a newform in $\mathbf{P}H^1(X_1(N), \overline{\mathbf{Q}})^-$ if it is a newform of any level $N_f$ dividing $N$.

### 2.2.3 Representations Attached to Modular Forms of Weight Two

Eichler and Shimura showed that weight 2 newforms give rise to $p$-adic Galois representations. To a newform $f$ of weight $k \geq 3$, Deligne [Del71] later was able to attach $p$-adic Galois representations using substantially more difficult methods. Deligne and Serre [DS74] next attached Galois representations to newforms of weight 1, but the image in this case is finite and can be embedded into $\mathbf{C}$. We will be interested, however, only in the representations arising from the Eichler-Shimura construction.

The coefficients $a_r$ of the modular form $f$ correspond to the traces of $\rho(\mathrm{Frob}_r^{-1})$ when $r \nmid N_f$, while the character (and weight, though this is fixed in our case) of $f$ corresponds to the determinant of $\rho(\mathrm{Frob}_r^{-1})$, multiplied by the cyclotomic character. We point out that our definition of $\rho_f$ corresponds to the tensor product of the representation $\rho'_f$ of the survey article of Darmon, Diamond, and Taylor [DDT97] with $(\det \rho'_f)^{-1}$. If $r$ divides the level $N_f$, the representation may be ramified at $r$. There is also a special consideration at the prime $p$.

In the following fact we collect a number of results concerning the representations $\rho_f$ in the weight 2 case. The survey article of Darmon, Diamond, and Taylor [DDT97] provides comments and references for the proofs of these statements.

**Fact 2.14** ([DDT97, Theorem 3.1]). *Let $f$ be a newform of weight 2, level $N_f$, and character $\psi_f$, and let $\rho_f$ be the $p$-adic representation associated to $f$. Moreover, let $K_f$ be the extension generated over the fraction field of $W(k)$ by the Hecke eigenvalues of $f$ and let $\mathfrak{O}_f$ be the ring of integers of $K_f$.*

*We use $\rho^{I_{\mathbf{Q}_r}}$ and $\rho_{I_{\mathbf{Q}_r}}$ to denote the $I_{\mathbf{Q}_p}$-invariants and coinvariants, respectively, of the underlying $G_{\mathbf{Q}}$-module of $\rho$. We have the following statements regarding the representation $\rho_f$.*

1. *For a prime $r \nmid N_f p$, the representation $\rho_f$ is unramified at $r$ and $\rho_f(\mathrm{Frob}_r^{-1})$ has characteristic polynomial*
$$X^2 - a_r X + r\psi_f(r).$$
2. *The character $\det(\rho_f)$ is the product of $\psi_f^{-1}$ with $\epsilon^{-1}$.*

3. *For a complex conjugation* $\mathbf{c}$, $\rho_f(\mathbf{c})$ *is conjugate to* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

4. *The representation* $\rho_f$ *is absolutely irreducible.*

5. *The prime to* $p$ *part of the conductor of the representation* $\rho_f$ *is the maximal divisor of* $N_f$ *prime to* $p$.

6. *Let* $r \neq p$ *where* $r$ *exactly divides* $N_f$, *and let* $\chi : G_{\mathbf{Q}_r} \twoheadrightarrow G_{\mathbf{F}_r} \to K_f$ *be an unramified character defined by* $\mathrm{Frob}_r^{-1} \mapsto a_r$. *If* $r$ *does not divide the conductor of* $\psi_f$, *then*

$$\rho_f|_{G_{\mathbf{Q}_r}} \sim \begin{pmatrix} \chi & * \\ 0 & \chi\epsilon^{-1} \end{pmatrix}.$$

   *If* $r$ *divides the conductor of* $\psi_f$, *then*

$$\rho_f|_{G_{\mathbf{Q}_r}} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1}\epsilon^{-1}\psi_f^{-1} \end{pmatrix}.$$

7. *Suppose that* $p > 2$. *If* $a_p$ *is a unit in* $\mathfrak{O}_f$, *then* $\rho_f|_{G_{\mathbf{Q}_p}}$ *is ordinary. If* $p||N_f$, *then* $\rho^{I_{\mathbf{Q}_p}}(\mathrm{Frob}_p^{-1}) = a_p$.

For a DVR $\mathfrak{O}_K$, we define $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_K)$ to be *modular* if there exists some newform $f$ such that $\rho \otimes_{\mathfrak{O}_K} \mathfrak{O}_f$ is equivalent to $\rho_f$, where $\mathfrak{O}_f$ is here the ring of integers of the field $K_f/K$ generated by the coefficients of $f$.

## 2.3 Algebra and Algebraic Geometry

In this section we briefly discuss certain objects and results from commutative algebra and algebraic geometry that we make use of in Sections 3 and 6. In particular, we discuss the dimension theory of modules and state some results that allow one to derive some consequences from "extremal" situations. We then discuss the definitions for the theory of formal schemes.

### 2.3.1 Cohen-Macaulay Rings and Modules

Recall that the Krull dimension of a ring $R$ is the length of the longest chain of prime ideals in $R$. The Krull dimension of an $R$-module $M$ is the dimension of $R/\operatorname{Ann}(M)$. One can also define dimension in a different way that extends to modules. This definition is a generalization of the notion of a system of parameters for the completion of an ideal at a smooth point.

In particular, for a complete noetherian ring $R$, one calls $R$ *regular* if $\mathfrak{m}$ can be generated by $\dim R$ elements. In this case, a set of $\dim R$ elements generating $R$ is called a *regular system of parameters*.

For a general complete local Noetherian ring $R$, we call elements $a_1, \ldots, a_n \in R$ a *regular sequence* if $(a_1, \ldots, a_n) \neq R$ and for each $k$, $x_{k+1}$ is a nonzerodivisor of $R/(x_1, \ldots, x_k)$. In the case where $R$ is a regular local ring, a regular system of parameters is a regular sequence, as one can show using the fact that regular local rings are integral domains. Any rearrangement of a regular sequence for a local ring is a regular sequence. We define the *depth* of $R$ to be the longest regular sequence for $R$.

We define a regular sequence for an $R$-module $M$ to be a sequence $a_1, \ldots, a_n \in R$ such that $(a_1, \ldots, a_n)M \neq M$ and $a_{k+1}$ is a nonzerodivisor for $M/(a_1, \ldots, a_k)M$. The length of the longest regular sequence for $M$ is called the *depth* of $M$. The notions of depth and dimension have a fundamental relationship.

**Fact 2.15** ([Eis95, Theorem A4.3])**.** *Let $M$ be a finitely generated module over a local ring $R$. Then*

$$\operatorname{depth}_R M \leq \dim_R M \leq \dim R.$$

Setting $R = M$ in Fact 2.15, we find that $\operatorname{depth} R \leq \dim R$. If equality holds, we say that $R$ is Cohen-Macaulay.

For a general module, in the case where equality holds in Fact 2.15, by which we mean $\operatorname{depth}_R M = \dim_R M = \dim R$, we call $M$ a Cohen-Macaulay $R$-module, in analogy with the definition of a Cohen-Macaulay ring. Even if $R$ is not Cohen-Macaulay, the module $M$ behaves well with respect to $R$. In particular, we have the following result.

**Fact 2.16** ([Eis95, Proposition 21.9])**.** *Suppose that $R$ is a local ring and that $M$ is a finitely generated $R$-module such that* $\operatorname{depth}_R M = \dim R$*. Then every element outside of the minimal primes of $R$ is a nonzerodivisor of $M$.*

We end by mentioning a basic fact that will be used in Section 6.

**Fact 2.17** ([Eis95, Theorem 10.8])**.** *Let $R$ be a ring and let $M$ be a finitely generated $R$-module. For any ideal $\mathfrak{a} \subseteq R$,*

$$\operatorname{Rad}(\operatorname{Ann}(M/\mathfrak{a}M)) = \operatorname{Rad}(\mathfrak{a} + \operatorname{Ann} M).$$

### 2.3.2 Formal Schemes

We will need to use formal schemes in Section 3 in order to parametrize a deformation space fibered over $\mathbf{P}^1_k$. We mention the definitions and basic constructions of formal schemes, though we will not need any results.

Following Hartshorne [Har77, Pg. 72-3], we briefly review the definitions for the category of schemes. A *ringed space* is a pair $(X, \mathcal{O}_X)$ of a topological space $X$ and a sheaf $\mathcal{O}_X$ of rings on $X$. A morphism of ringed spaces $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $f : X \to Y$ of topological spaces and a map $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$ of sheaves of rings on $Y$. A *locally ringed space* is a ringed space $(X, \mathcal{O}_X)$ such that the stalks of $\mathcal{O}_X$ are local rings. Morphisms of local ringed spaces must induce *local* homomorphisms $f^{\#}_x : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ on the stalks. A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ such that every point $x \in X$ has a neighborhood $U$

that is isomorphic to $\operatorname{Spec} R$ for a ring $R$, and a morphism of schemes is simply a morphism of locally ringed spaces.

Passing from schemes to formal schemes is the scheme-theoretic generalization of the process of completion of a ring $R$ at an ideal $\mathfrak{a}$ to produce a ring $\hat{R}$ that is complete with respect to the $\mathfrak{a}$-adic topology. Following Hartshorne [Har77, Pg. 194-5], we restrict our discussion to the noetherian case. Given a noetherian scheme $X$ and closed subscheme $Y$ defined by an ideal sheaf $\mathcal{I}$, one constructs the *formal completion* of $X$ along $Y$ to be the locally ringed space $(\hat{X}, \mathcal{O}_{\hat{X}})$ given by the topological space $Y$ and sheaf of rings

$$\mathcal{O}_{\hat{X}} = \varprojlim \mathcal{O}_X/\mathcal{I}^n.$$

In the case where $X = \operatorname{Spec} R$ is affine and the completion is with respect to the ideal $\mathfrak{a}$, one obtains a scheme $\operatorname{Spf} R$ which is called the *formal spectrum* of $R$.

A *formal scheme*, in analogy to a scheme, is a locally ringed space locally isomorphic to the formal completion of a noetherian scheme along a closed subscheme, and a morphism of formal schemes is a morphism of locally ringed spaces. The category of noetherian formal schemes is an enlargement of the category of schemes, as can be seen by setting $X = Y$ in the definition of the formal completion. Note that one cannot relate the dimension of the underlying topological space of a formal scheme to the local dimension at the stalks – the structure sheaf contains information about the infinitesimal deformations of the underlying scheme $Y$ that are hidden to the topological space.

# Chapter 3

# Explicit Deformation of Residually Trivial Representations of $G_{\mathbf{Q}_p}$

In this section we explicitly study ordinary deformations of residually trivial representations. Let $p$ be an odd prime. Our focus is on understanding ordinary deformations of the form $G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathfrak{O}_K)$, where $K/\mathbf{Q}_p$ is a finite extension. While the general deformation problem will be represented by a formal scheme $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$, we will construct an auxiliary ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ that solves this problem for the smaller category of discrete valuation rings. The main difficulty with solving the deformation problem is that the unramified subspaces of the possible ordinary liftings of $\overline{\rho}$ are not residually determined, since the residual representation is the identity. Thus our solution to the deformation problem will pass through the construction of a formal scheme $\mathfrak{X}^{\mathrm{filt}}$ representing the choice of filtration.

We begin by simplifying the deformation problem in Section 3.1, allowing us to explicitly solve the lifting problem with a determinant condition in Section 3.2. We define the deformation problem $D^{\mathrm{loc}}_{p,\mathrm{ord}}$ in Section 3.3 and explain the obstruction to its representability. In Sections 3.4 and 3.5 we construct the representing formal scheme $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$. In Sections 3.6, 3.7, and 3.8, we define $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ and prove its various properties.

Define $\overline{\rho}$ to be the trivial representation and define $\psi : G_{\mathbf{Q}_p} \to W(k)^\times$ to be the fixed determinant character $\epsilon_p^{-1}\omega_p$.

## 3.1 Factoring through $G_{\mathbf{Q}_p}(p)$

In order to simplify the deformation problem, we show that residually trivial representations out of $G_{\mathbf{Q}_p}$ factor through its maximal pro-$p$ quotient. In the following, let $R$ denote a complete local Noetherian ring with residue field $k$, a finite field of characteristic $p$, and maximal ideal $\mathfrak{m}$.

**Proposition 3.1.** *The group* $\ker(\mathrm{GL}_N(R) \to \mathrm{GL}_N(k))$ *is a pro-$p$ group.*

*Proof.* Since

$$\ker(\mathrm{GL}_N(R) \to \mathrm{GL}_N(k)) = \varprojlim_n \ker(\mathrm{GL}_N(R/\mathfrak{m}^n) \to \mathrm{GL}_N(k)),$$

it suffices to show that $\ker(\mathrm{GL}_N(R/\mathfrak{m}^n) \to \mathrm{GL}_N(k))$ is a $p$-group for all $n$.

We have $\ker(\mathrm{GL}_N(R) \to \mathrm{GL}_N(k)) = \mathbf{1}_N + \mathfrak{m}\mathbf{M}_N(R)$. We have

$$(\mathbf{1}_N + \mathfrak{m}\mathbf{M}_N(R))^{p^k} = \sum_{i=0}^{p^k} \mathfrak{m}^i \mathbf{M}_N(R)^i \binom{p^k}{i}.$$

Since $(p) \subseteq \mathfrak{m}$,

$$\mathfrak{m}^i \mathbf{M}_N(R)^i \binom{p^k}{i} \subseteq \mathfrak{m}^{i+v_p\left(\binom{p^k}{i}\right)} \mathbf{M}_N(R)^i,$$

where $v_p$ denotes the $p$-valuation. Kummer's criterion for the $p$-valuation of $\binom{p^k}{i}$ implies that $k - v_p(i) \leq v_p\left(\binom{p^k}{i}\right)$. Choose $k = 2n$. Then for $i = 1, \ldots, p^n - 1$, we have $n \leq v_p(\binom{p^k}{i})$. For $i \geq p^n$, the power on $\mathfrak{m}$ is at least $p^n \geq n$. Thus in $\mathrm{GL}_N(R/\mathfrak{m}^n)$,

$$(\mathbf{1}_n + \mathfrak{m}\mathbf{M}_N(R))^{p^k} = \sum_{i=0}^{p^k} \mathfrak{m}^i \mathbf{M}_N(R)^i \binom{p^k}{i} = \mathbf{1}_n,$$

corresponding to the $i = 0$ term. We note that $R/\mathfrak{m}^n$ is finite by the Noetherian hypothesis (since $\dim_{\mathbf{F}_p} \mathfrak{m}^\ell/\mathfrak{m}^{\ell+1} < \infty$ for each $\ell$), so $\mathrm{GL}_N(R/\mathfrak{m}^n)$ is finite. □

This implies that the image of a residually trivial morphism $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ is pro-$p$, giving the following corollary.

**Corollary 3.2.** *Any residually trivial representation $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ factors through $G_{\mathbf{Q}_p}(p)$.*

## 3.2 The Deformation Problem $D_p^{\mathrm{loc}}$

We define a functor

$$D_p^{\mathrm{loc}} : \mathbf{CLNRings}(k) \to \mathbf{Sets}$$

from the category of complete local Noetherian rings over $W(k)$ to the category of sets by the assignment

$$D_p^{\mathrm{loc}} : R \mapsto \left\{ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) \;\middle|\; \begin{array}{l} \rho \text{ satisfies} \\ \;\; 1.\ \rho \text{ lifts } \overline{\rho} \\ \;\; 2.\ \det \rho \equiv \psi \end{array} \right\}.$$

Note that $\det \rho$ takes values in $R$, while $\psi$ takes values in $W(k)$. We define $\det \rho \equiv \psi$ to mean that the diagram

$$\begin{tikzcd} G_{\mathbf{Q}_p} \arrow[r, "\rho"] \arrow[d, "\psi"] & \mathrm{GL}_2(R) \arrow[d, "\det"] \\ W(k)^\times \arrow[r] & R^\times \end{tikzcd}$$

commutes, where the bottom arrow comes from the $W(k)$-algebra structure of $R$.

Using Proposition 2.3, we may explicitly find a universal framed deformation ring for $D_p^{\mathrm{loc}}$. As prescribed in Remark 1, let $\sigma$ and $\tau$ denote lifts to $G_{\mathbf{Q}_p}$ of the two topological generators of the maximal pro-$p$ quotient $G_{\mathbf{Q}_p}(p)$, with $\sigma$ a lift of Frobenius and $\tau \in I_{G_{\mathbf{Q}_p}}$, such that $\psi(\sigma) = 1$ and $\psi(\tau) = 1 - p$.

**Proposition 3.3.** *The ring*

$$\begin{aligned} R_{p,0}^{\mathrm{loc}} = W(k)[[A_{11}, A_{12}, A_{21}, A_{22}, B_{11}, B_{12}, B_{21}, B_{22}]]/((1 + A_{11})(1 + A_{22}) - A_{12}A_{21} - \psi(\sigma), \\ (1 + B_{11})(1 + B_{22}) - B_{12}B_{21} - \psi(\tau)) \end{aligned}$$

*represents the functor $D_p^{\mathrm{loc}}$ by associating to a morphism $\varphi : R_{p,0}^{\mathrm{loc}} \to R$ the projetion along $\varphi$ of the representation $\rho_{p,0}^{\mathrm{loc}} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R_{p,0}^{\mathrm{loc}})$ given by*

$$\rho_{p,0}^{\mathrm{loc}}(\sigma) \mapsto \begin{pmatrix} 1 + A_{11} & A_{12} \\ A_{21} & 1 + A_{22} \end{pmatrix} \quad \text{and} \quad \rho_{p,0}^{\mathrm{loc}}(\tau) \mapsto \begin{pmatrix} 1 + B_{11} & B_{12} \\ B_{21} & 1 + B_{22} \end{pmatrix}.$$

*Note that in this definition, we are implicitly using the fact that $\rho_{p,0}^{\mathrm{loc}}$ factors through $G_{\mathbf{Q}_p}(p)$.*

*Proof.* We note that the homomorphism $\rho_{0,p}^{\mathrm{loc}}$ exists by the completeness of the ring $R_{p,0}^{\mathrm{loc}}$. Given a complete local noetherian ring $R$, observe that a morphism $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ is determined by the images of $\sigma$ and $\tau$. Consequently, there exists a unique morphism $\varphi : R_{p,0}^{\mathrm{loc}} \to R$ such that $\rho = \varphi_* \rho_{p,0}^{\mathrm{loc}}$, determined by sending $A_{ij}$ and $B_{ij}$ to the associated entries of the matrices for $\rho(\sigma)$ and $\rho(\tau)$. Note that since $\rho$ has determinant $\psi$, the map factors through the relations in $R_{p,0}^{\mathrm{loc}}$. Conversely, a morphism $\varphi$ determines a homomorphism by projection.

$\square$

**Proposition 3.4.** *The ring*

$$R_p^{\mathrm{loc}} = W(k)[[A_{12}, A_{21}, A_{22}, B_{12}, B_{21}, B_{22}]]$$

*and representation $\rho^{\mathrm{loc}} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R_p^{\mathrm{loc}})$ given by*

$$\rho_p^{\mathrm{loc}}(\sigma) = \begin{pmatrix} (\psi(\sigma) + A_{12}A_{21})(1 + A_{22})^{-1} & A_{12} \\ A_{21} & 1 + A_{22} \end{pmatrix}$$

*and*

$$\rho_p^{\mathrm{loc}}(\tau) = \begin{pmatrix} (\psi(\tau) + B_{12}B_{21})(1 + B_{22})^{-1} & B_{12} \\ B_{21} & 1 + B_{22} \end{pmatrix}$$

*represents the functor $D_p^{\mathrm{loc}}$.*

*Proof.* We claim that the map $R_p^{\mathrm{loc}} \to R_{p,0}^{\mathrm{loc}}$ sending $A_{ij} \mapsto A_{ij}$, $B_{ij} \mapsto B_{ij}$ is an isomorphism. Note that $A_{11}$ and $B_{11}$ are the images of the elements

$$(\psi(\sigma) + A_{12}A_{21})(1 + A_{22})^{-1} - 1 \quad \text{and} \quad (\psi(\tau) + B_{12}B_{21})(1 + B_{22})^{-1} - 1,$$

respectively, so that the map is surjective. Conversely, there are no relations among the six generators $A_{12}, A_{21}, A_{22}, B_{12}, B_{21}, B_{22}$ of $R_0^{\mathrm{loc}}$, so the map is both surjective and injective. $\square$

## 3.3 The Deformation Problem $D_{p,\mathrm{ord}}^{\mathrm{loc}}$

In this section we restrict to those deformations that are ordinary. We define a functor

$$D_{p,\mathrm{ord}}^{\mathrm{loc}} : \mathbf{CLNRings}(k) \to \mathbf{Sets}$$

by the assignment

$$D_{p,\mathrm{ord}}^{\mathrm{loc}} : R \mapsto \left\{ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) \;\middle|\; \begin{array}{l} \rho \text{ satisfies} \\ \;\; 1.\ \overline{\rho} \equiv \mathbf{1} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(k) \\ \;\; 2.\ \det \rho \equiv \psi \\ \;\; 3.\ \rho \sim \left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right) \text{ with } \chi_1 \text{ unramified} \end{array} \right\}.$$

Our hope would be to find an object of $\mathbf{CLNRings}(k)$ representing this functor. We remark that the third condition in the definition of $D_{p,\mathrm{ord}}^{\mathrm{loc}}$ together with the definition of $\psi$ forces the lifting to be ramified. In particular, any lifting $\rho$ has a 1-dimensional subspace fixed by $\rho|_{I_{\mathbf{Q}_p}}$.

Unfortunately, the deformation problem $D_{p,\mathrm{ord}}^{\mathrm{loc}}$ is not representable by a local ring $R$. To see why, consider the same problem with $G_{\mathbf{Q}_p}$ replaced (for simplicity) by $\mathbf{Z}_p = \overline{\langle \sigma \rangle}$, where $\bar{\cdot}$ here denotes the pro-$p$ completion. Define $R_\gamma = k[\gamma]/(\gamma^2)$, $R_\delta = k[\delta]/(\delta^2)$, and $R_{\gamma,\delta} = k[\gamma,\delta]/(\gamma,\delta)^2$. Define representations $\rho_\gamma : \mathbf{Z}_p \to \mathrm{GL}_2(R_\gamma)$ and $\rho_\delta : \mathbf{Z}_p \to \mathrm{GL}_2(R_\delta)$ by $\sigma \mapsto \left(\begin{smallmatrix} 1 & \gamma \\ 0 & 1 \end{smallmatrix}\right)$ and $\sigma \mapsto \left(\begin{smallmatrix} 1 & 0 \\ \delta & 1 \end{smallmatrix}\right)$, respectively. We have the diagram of rings

$$\begin{tikzcd} & R_{\gamma,\delta} \arrow[dl, "\pi_\gamma"'] \arrow[dr, "\pi_\delta"] & \\ R_\gamma \arrow[dr] & & R_\delta \arrow[dl] \\ & k & \end{tikzcd}$$

induced by the maps

$$\pi_\gamma : \gamma \mapsto \gamma, \delta \mapsto 0 \quad \text{and} \quad \pi_\delta : \delta \mapsto \delta, \gamma \mapsto 0.$$

While both $\rho_\gamma$ and $\rho_\delta$ are ordinary, the lifting $\rho_{\gamma,\delta} : \sigma \mapsto \left(\begin{smallmatrix} 1 & \gamma \\ \delta & 1 \end{smallmatrix}\right)$ is not. The obstruction is that while $\rho_\gamma$ and $\rho_\delta$ are both ordinary, as can be seen by conjugating the latter by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, the 1-dimensional unramified subspaces for these representations are residually distinct, so no residually trivial base change matrix could be used to align them.

In order to continue we will need to expand our category to one where we may find an object to represent $D^{\text{loc}}_{p,\text{ord}}$.

## 3.4 Choosing a Filtration

For any ordinary representation $\rho$, the 1-dimensional submodule $U$ fixed by $\rho|_{I_{\mathbf{Q}_p}}$ gives a filtration $0 \subseteq U \subseteq R^2$ that yields a complete flag $0 \subseteq \overline{U} \subseteq k^2$ for the residual vector space $k^2$. As noted in Section 3.3, two representations with distinct flags cannot be conjugated to each other by a residually trivial matrix. Thus we expect to need a family of local rings – one for each of the possible choices for the 1-dimensional subspace of $k^2$ – to represent $D^{\text{loc}}_{p,\text{ord}}$. These local rings will arise as the localizations of a formal scheme, so that a morphism from a complete local noetherian ring to this formal scheme is equivalent to a morphism out of one of these local rings. In order to do this, we need to first build a formal scheme whose points correspond to choices for the complete flag on $k^2$, which in turn corresponds to a choice of a 1-dimensional subspace of $k^2$.

Formally, we would like to represent the functor $D^{\text{filt}} : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ defined by

$$D^{\text{filt}} : R \mapsto \left\{ U \subseteq R^2 | U \cong R, 0 \neq \overline{U} \subseteq k^2 \right\}.$$

A 1-dimensional subspace of $k^2$ is spanned by a single vector, which we may take to be either $\left(\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right)$ for $x \in k$ or $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. We can view the latter as a special case of the set $\left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right)$, so that we may glue together the affine formal schemes $\operatorname{Spf} W(k)\langle x \rangle$ and $\operatorname{Spf} W(k)\langle y \rangle$, whose topologies are $\operatorname{Spec} k[x]$ and $\operatorname{Spec} k[y]$, respectively, in order to produce a formal scheme with spectrum $\mathbf{P}^1_k$. The notation $\langle \cdot \rangle$ is defined for a topological ring $R$ by

$$R\langle x \rangle = \left\{ \sum_{n=0}^{\infty} r_n x^n \middle| r_n \to 0 \right\}.$$

The gluing map is defined to send $\overline{k} \setminus 0 \subseteq \operatorname{Spec} k[x]$ to $\overline{k} \setminus 0 \subseteq \operatorname{Spec} k[y]$ via the map $\alpha \mapsto \alpha^{-1}$ on the level of topological spaces. This corresponds to the ring homomorphism defined by $x \mapsto y^{-1}$ taking the open subscheme $\operatorname{Spf} W(k)\langle x, x^{-1} \rangle$ of $\operatorname{Spf} W(k)\langle x \rangle$ isomorphically to the open subscheme $\operatorname{Spf} W(k)\langle y, y^{-1} \rangle$ of $\operatorname{Spf} W(k)\langle y \rangle$. Let $\mathfrak{X}^{\text{filt}}$ denote this formal scheme.

**Proposition 3.5.** *The formal scheme $\mathfrak{X}^{\text{filt}}$ represents the functor $D^{\text{filt}}$. Moreover, for any complete local noetherian ring $R$ with residue field $k_R$ a finite extension of $k$, we have*

$$\operatorname{Hom}(\operatorname{Spf} R, \mathfrak{X}^{\text{filt}}) \cong \left\{ U \subseteq R^2 | U \cong R, 0 \neq \overline{U} \subseteq k_R^2 \right\}.$$

*Proof.* A morphism $\varphi : \operatorname{Spf} R \to \mathfrak{X}^{\text{filt}}$ of formal schemes over $W(k)$ either sends the nontrivial point of $\operatorname{Spf} R$ to the point $(y) + (\pi) \subseteq W(k)\langle y\rangle$, where $\pi \in W(k)$ is a uniformizer, or to a point of $\operatorname{Spf} W(k)\langle x\rangle = \operatorname{Spec} k[x]$. By symmetry, we may suppose the latter without loss of generality. Let the image of the nontrivial point be $\alpha \in \overline{k}$, corresponding to the ideal $\mathfrak{p}_\alpha \in \operatorname{Spec} k[x]$. Then we are given a morphism of rings $\varphi^{\#}_{\mathfrak{m}+\mathfrak{p}_\alpha} : W(k)\langle x\rangle_{\mathfrak{m}+\widetilde{\mathfrak{p}}_\alpha} \to R$, where $\widetilde{\mathfrak{p}}_\alpha \subseteq W(k)\langle x\rangle$ is the ideal generated by an arbitrary lift of the generator of the principal ideal $\mathfrak{p}_\alpha$ to $W(k)\langle x\rangle$. To this morphism we associate the subspace spanned by $\left(\begin{smallmatrix} \varphi^{\#}_{\mathfrak{m}+\widetilde{\mathfrak{p}}_\alpha}(x) \\ 1 \end{smallmatrix}\right)$. The former case is treated in the same manner. This associates a unique filtration to $\varphi$ such that the residue is a complete flag.

We claim, conversely, that to any filtration with complete flag residue there exists a morphism $\varphi$. The filtration is determined by $U \subseteq R^2$ with $U \cong R$, so we can take $U = R\left(\begin{smallmatrix} \widetilde{\alpha} \\ \widetilde{\beta} \end{smallmatrix}\right)$ for $\widetilde{\alpha}, \widetilde{\beta} \in R$ reducing to $\alpha, \beta \in k_R$. One of $\alpha$ or $\beta$ is nonzero since $U$ is by assumption residually nontrivial. Without loss of generality, suppose that $\beta$ is nonzero. Then replacing $\left(\begin{smallmatrix} \widetilde{\alpha} \\ \widetilde{\beta} \end{smallmatrix}\right)$ with $\left(\begin{smallmatrix} \widetilde{\alpha}\widetilde{\beta}^{-1} \\ 1 \end{smallmatrix}\right)$ yields the same filtration. We may then define the ring homomorphism $W(k)\langle x\rangle_{\mathfrak{m}+\widetilde{\mathfrak{p}}_{\alpha\beta^{-1}}} \to R$ by mapping $x$ to a lift of $\alpha\beta^{-1} \in R$. This gives rise to a morphism of formal schemes, $\varphi : \operatorname{Spf} R \to \mathfrak{X}^{\text{filt}}$, completing the proof. $\square$

## 3.5 Representation by a Formal Scheme $\mathfrak{X}^{\text{loc}}_{p,\text{ord}}$

We seek a formal scheme $\mathfrak{X}^{\text{loc}}_{p,\text{ord}}$ representing the functor $D^{\text{loc}}_{p,\text{ord}}$. The idea behind the construction is to note that on each point of $\mathfrak{X}^{\text{filt}}$, we can explicitly write the condition for a representation with the corresponding residual filtration to be ordinary. Thus, by using a scheme fibered over $\mathfrak{X}^{\text{filt}}$, with fibers corresponding to the deformation problem for each choice of residual filtration, we may represent $D^{\text{loc}}_{p,\text{ord}}$.

Specifically, we fix the basis used in Section 3.4 to write $\rho(\sigma)$ as a $2 \times 2$ matrix over $R$ for each $\sigma \in G_{\mathbf{Q}_p}$. Written in the basis $\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} y \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ corresponding to the filtration for the ordinary representation, $\rho(\tau_0)$ for any $\tau_0 \in I_{\mathbf{Q}_p}$ should be of the form $\left(\begin{smallmatrix} 1 & w \\ 0 & \psi(\sigma) \end{smallmatrix}\right)$ for some $w \in \mathfrak{m}_R$. For general elements $\sigma_0 \in G_{\mathbf{Q}_p}$, we know that $\rho(\sigma_0)$ is of the form $\left(\begin{smallmatrix} (1+z_0)^{-1} & z_1 \\ 0 & (1+z_0)\psi(\sigma) \end{smallmatrix}\right)$ in this basis. Since the representation factors through $G_{\mathbf{Q}_p}(p)$, Proposition 2.3 and Remark 1 imply that the aforementioned condition for $\rho$ to be ordinary is equivalent to the requirement that

$$\begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \rho(\sigma) \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 + z_{11} & z_{12} \\ 0 & \psi(\sigma)(1 + z_{11})^{-1} \end{pmatrix} \tag{3.1}$$

and

$$\begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \rho(\tau) \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} \tag{3.2}$$

when the filtration is of the form $\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, and that

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} \rho(\sigma) \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} 1 + z'_{11} & z'_{12} \\ 0 & \psi(\sigma)(1 + z'_{11})^{-1} \end{pmatrix} \tag{3.3}$$

and

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} \rho(\tau) \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} 1 & w'_{12} \\ 0 & \psi(\tau) \end{pmatrix} \tag{3.4}$$

when the filtration is of the form $\left(\begin{smallmatrix} y \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$.

In order to glue these two charts together, we observe that by defining $x \mapsto y^{-1}$, we obtain

$$\begin{aligned}
&\begin{pmatrix} 1 + z_{11} & z_{12} \\ 0 & \psi(\sigma)(1 + z_{11})^{-1} \end{pmatrix} \\
&= \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 + z'_{11} & z'_{12} \\ 0 & \psi(\sigma)(1 + z'_{11})^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 + z'_{11} & -y\,(1 + z'_{11})^{-1}\,((\psi(\sigma) - 1) - 2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}) \\ 0 & (1 + z'_{11})^{-1} \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
\begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} &= \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 & w'_{12} \\ 0 & \psi(\tau) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -y\,((\psi(\tau) - 1) + yw'_{12}) \\ 0 & 1 - p \end{pmatrix}.
\end{aligned}$$

Thus, we construct $\mathfrak{X}^{\text{loc}}_{p,\text{ord}}$ by gluing the rings

$$\mathfrak{X}_1 = \operatorname{Spf} W(k)\,\langle x \rangle\,[[z_{11}, z_{12}, w_{12}]] \quad \text{and} \quad \mathfrak{X}_2 = \operatorname{Spf} W(k)\,\langle y \rangle\,[[z'_{11}, z'_{12}, w'_{12}]]$$

along the open subschemes

$$\operatorname{Spf} W(k)\,\langle x, x^{-1} \rangle\,[[z_{11}, z_{12}, w_{12}]] \quad \text{and} \quad \operatorname{Spf} W(k)\,\langle y, y^{-1} \rangle\,[[z'_{11}, z'_{12}, w'_{12}]]$$

via the map $\varphi : W(k)\,\langle x, x^{-1} \rangle\,[[z_{11}, z_{12}, w_{12}]] \to W(k)\,\langle y, y^{-1} \rangle\,[[z'_{11}, z'_{12}, w'_{12}]]$ defined by

$$\begin{aligned}
x &\mapsto y^{-1} \\
z_{11} &\mapsto z'_{11} \\
z_{12} &\mapsto -y\,(1 + z'_{11})^{-1}\left((\psi(\sigma) - 1) - 2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right) \\
w_{12} &\mapsto -y\,((\psi(\tau) - 1) + yw'_{12})\,.
\end{aligned}$$

**Proposition 3.6.** *The formal scheme $\mathfrak{X}$ represents the functor $D^{\text{loc}}_{p,\text{ord}}$. Moreover, for any complete local noetherian ring $R$ with residue field $k_R$ a finite extension of $k$, we have*

$$\operatorname{Hom}(\operatorname{Spf} R, \mathfrak{X}^{\text{loc}}_{p,\text{ord}}) \cong \left\{ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) \;\middle|\; \begin{array}{l} \rho \textit{ satisfies} \\ \;\; 1.\ \overline{\rho} \equiv \mathbf{1} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(k_R) \\ \;\; 2.\ \det \rho \equiv \psi \\ \;\; 3.\ \rho \sim \left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right) \textit{ with } \chi_1 \textit{ unramified} \end{array} \right\}.$$

*Proof.* Suppose we are given an ordinary, residually trivial representation $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ with determinant $\psi$. Recall from Corollary 3.2 that $\rho$ factors through a map $G_{\mathbf{Q}_p}(p) \to \mathrm{GL}_2(R)$, so it is defined by the images of the elements $\sigma$ and $\tau$ defined earlier. Since $\rho$ is ordinary, $\rho$ is upper triangular in some basis $\{\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right), \left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)\}$ of $R^2$, and the inertia group acts trivially on the space generated by $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$. As mentioned earlier the choice of subspace acted upon trivially by the inertia group is unique since the determinant condition forces a nontrivial action by inertia on the whole space. Since at least one of $a$ or $b$ is residually nontrivial (in $k_R$), we can rewrite $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ in the form $\left(\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right)$ (if $b$ is nontrivial) or $\left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right)$ (otherwise) by dividing both entries by the residually nontrivial element. If we replace $\left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ with $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ in the first case and $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ in the second, $\rho$ must still have the form $\left(\begin{smallmatrix} \chi & * \\ 0 & * \end{smallmatrix}\right)$ with $\chi$ unramified with respect to this basis. Note that aside from the choice of chart when both $a$ and $b$ are residually nontrivial, there is a unique choice of $x$ (or $y$) provided by this procedure. We finally define the morphism $\operatorname{Spf} R \to \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ by topologically sending the ideal of $R$ to the residual filtration, and on rings, defining the map using (3.1) and (3.2) or (3.3) and (3.4).

Conversely, given a map $\operatorname{Spf} R \to \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$, we define $\rho(\sigma)$ and $\rho(\tau)$ by filling in the images under the map (on rings) of the variables in the formulas

$$\rho(\sigma) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 + z_{11} & z_{12} \\ 0 & \psi(\sigma)(1 + z_{11})^{-1} \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

and

$$\rho(\tau) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

and similarly for $y$. This clearly reverses the construction in the previous paragraph, so we have the desired isomorphism.

□

## 3.6 Specializing to Discrete Valuation Rings

Since the representations of interest take values in an extension $K/\mathbf{Q}_p$, we may potentially be able to simplify our representing object for $D^{\mathrm{loc}}_{p,\mathrm{ord}}$ by specializing to the subcategory of discrete valuation rings.

We obtain our candidate ring to represent $D^{\mathrm{loc}}_{p,\mathrm{ord}}$ by considering the image $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ of the natural morphism $R^{\mathrm{loc}}_p \to \Gamma(\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}})$.

Since $\Gamma(\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}})$ is a subring of $W(k)\langle x \rangle [[z_{11}, z_{12}, w_{12}]]$, we can regard $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ as the image of the morphism $R^{\mathrm{loc}}_p \to W(k)\langle x \rangle [[z_{11}, z_{12}, w_{12}]]$ induced by the natural morphism. In particular, using the description of $R^{\mathrm{loc}}_p$ given in Proposition 3.4, and solving for $\rho(\sigma)$ and $\rho(\tau)$ in the formulas (3.1) and (3.2), we can identify $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ as the image of the morphism explicitly defined by

$$\begin{aligned}
A_{12} &\mapsto x(1+z_{11}) - x(1+z_{11})^{-1} - x^2 z_{12}\\
A_{21} &\mapsto z_{12}\\
A_{22} &\mapsto z_{11} - x z_{12}\\
B_{12} &\mapsto -px - x^2 w_{12}\\
B_{21} &\mapsto w_{12}\\
B_{22} &\mapsto -x w_{12}.
\end{aligned}$$

We can write $R^{\mathrm{loc}}_{p,\mathrm{ord}} = W(k)[[a_{12}, a_{21}, a_{22}, b_{12}, b_{21}, b_{22}]]/\mathfrak{b}$, where $\mathfrak{b}$ is the ideal of relations existing among the generators when $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ is identified with the image of the ring $R^{\mathrm{loc}}_{p}$ in $W(k)\langle x\rangle[[z_{11}, z_{12}, w_{12}]]$ via $A_{ij} \mapsto a_{ij}$ and $B_{ij} \mapsto b_{ij}$.

Our first observation is to note that

$$-b_{21}b_{12} + b_{22}p - b_{22}^2, \tag{3.5}$$

$$a_{12}(b_{21}^2 + b_{21}^2 a_{22} - b_{22}b_{21}a_{21}) + b_{22}(2a_{22}b_{21} + a_{22}^2 b_{21} - b_{22}a_{22}a_{21} - b_{22}a_{21}), \tag{3.6}$$

and

$$a_{12}(p-b_{22})((p-b_{22})+(p-b_{22})a_{22}-b_{12}a_{21})+b_{12}(2(p-b_{22})a_{22}+(p-b_{22})a_{22}^2-b_{12}b_{22}a_{21}-b_{12}a_{21}) \tag{3.7}$$

are relations in $R^{\mathrm{loc}}_{p,\mathrm{ord}}$, as can be verified by explicit computation. A fourth relation, not implied by these, is given by

$$\begin{aligned}
&- a_{12}a_{22}b_{21}b_{22} + b_{21}b_{12}a_{22}^2 - b_{12}b_{22}a_{21}a_{22} - a_{12}b_{21}b_{12}a_{21}\\
&+ pa_{12}a_{22}b_{21} - a_{12}b_{21}b_{22} + 2b_{21}b_{12}a_{22} - b_{12}b_{21}a_{21} + pa_{12}b_{21},
\end{aligned} \tag{3.8}$$

which can also be verified by explicit computation. We define $\mathfrak{b}_0$ to be the ideal generated by these four relations. We have $\mathfrak{b}_0 \subseteq \mathfrak{b}$, inducing a map $R^{\mathrm{loc}}_{p}/\mathfrak{b}_0 \to R^{\mathrm{loc}}_{p,\mathrm{ord}}$.

We need $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ to solve the deformation problem $D^{\mathrm{loc}}_{p,\mathrm{ord}}$ for discrete valuation rings. In order to prove that $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ solves this deformation problem, we will show that $R^{\mathrm{loc}}_{p}/\mathfrak{b}_0$ solves this deformation problem, and deduce the result using the natural map $R^{\mathrm{loc}}_{p}/\mathfrak{b}_0 \to R^{\mathrm{loc}}_{p,\mathrm{ord}}$.

**Proposition 3.7.** *When restricted to the category $\mathbf{DVR}(k)$ of discrete valuation rings over $W(k)$, the ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ represents the functor $D^{\mathrm{loc}}_{p,\mathrm{ord}}$. Moreover, for any discrete valuation ring $\mathfrak{O}_K$ with residue field $k_K$ that is a finite extension of $k$,*

$$\mathrm{Hom}(R^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{O}_K) \cong \left\{ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathfrak{O}_K) \;\middle|\; \begin{array}{l} \rho \textit{ satisfies} \\ \;1.\ \overline{\rho} \equiv \mathbf{1} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(k_K) \\ \;2.\ \det\rho \equiv \psi \\ \;3.\ \rho \sim \left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right) \textit{ with } \chi_1 \textit{ unramified} \end{array} \right\}.$$

Section 3.7 is devoted to the detailed verification of the computational steps of Proposition 3.7. We give an overview of the proof as follows.

Given $f : R^{\mathrm{loc}}_{p,\mathrm{ord}} \to \mathfrak{O}_K$ for $\mathfrak{O}_K$ with valuation $v_K$ and residue field $k_K$, we would like to fill in the dotted arrow in the commutative diagram

$$\begin{tikzcd} & \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}} \arrow[d] \\ \mathrm{Spf}\,\mathfrak{O}_K \arrow[ur, dashed, "\widetilde{f}^*"] \arrow[r, "f^*"] & \mathrm{Spf}\,R^{\mathrm{loc}}_{p,\mathrm{ord}} \end{tikzcd}$$

such that the diagram commutes. In particular, we desire a lift $\widetilde{f}^*$ of the morphism $f^* : \mathrm{Spf}\,R \to \mathrm{Spf}\,R^{\mathrm{loc}}_{p,\mathrm{ord}}$ induced by $f$. Note that since the map $f$ is determined by the lifting $\widetilde{f}^*$ (via the inclusion $R^{\mathrm{loc}}_{p,\mathrm{ord}} \hookrightarrow \Gamma(\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}})$), constructing a lifting for all $f$ shows that the functors $\mathrm{Hom}(\cdot, \mathrm{Spf}\,R^{\mathrm{loc}}_{p,\mathrm{ord}})$ and $\mathrm{Hom}(\cdot, \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}})$ are isomorphic on the category of DVRs $\mathfrak{O}_K$ with residue field $k_K$ a finite extension of $k$.

A map $\widetilde{f}^* : \mathrm{Spf}\,\mathfrak{O}_K \to \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ is a map of the underlying topological spaces $\mathrm{Spec}\,k \to \mathrm{Spec}\,k[x]$, together with a morphism of sheaves $\mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}} \to (\widetilde{f}^*)_* \mathcal{O}_{\mathrm{Spf}\,\mathfrak{O}_K}$.

Thus in order to construct a lifting, we first need to determine the morphism $\widetilde{f}^*$ as it acts on topological spaces. In particular, this corresponds to a choice of residual filtration for the representation. Algebraically, we can see from the morphism defined earlier in this section that if $-\frac{b_{22}}{b_{21}}$ is defined, it would provide the value of $x$, which determines the filtration. Alternatively, if $-\frac{b_{21}}{b_{22}}$ is defined, it would provide the value of $y$. Thus we can break into cases based on whether $v_K(f(b_{22}))$ is greater than, equal to, or less than $v_K(f(b_{21}))$, and in each of these, it is just a matter of explicit algebra to determine the lifting. However, it is possible that $f(b_{21}) = f(b_{22}) = 0$, in which case another approach must be taken.

In this case, we extract $x$ from $f(b_{12})$ by computing $-p^{-1} f(b_{12})$ if it is defined. If not, we may use $-pf(b_{12})^{-1}$ to define $y$. Again, one breaks into subcases depending on the valuations $v_K(p)$ and $v_K(f(b_{12}))$. Thus, through the explicit determination in each of a total of four cases/subcases carried out in Section 3.7, one proves Proposition 3.7. We remark that in this proof, we will not make use of (3.8).

## 3.7 Proof of Proposition 3.7

Before we check each of the cases, we will compute the composition $R^{\mathrm{loc}}_p \to R_1 \langle x^{-1} \rangle \to R_2$, where

$$R_1 = W(k)\langle x \rangle [[z_{11}, z_{12}, w_{12}]] \quad \text{and} \quad R_2 = W(k)\langle y \rangle [[z'_{11}, z'_{12}, w'_{12}]]$$

are the two rings whose formal spectra are glued to construct $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ and $R_1[x^{-1}] \to R_2$ is the gluing homomorphism $\varphi$.

In particular, we have

$$\begin{aligned}
a_{12} \mapsto & y^{-1}\left(\underbrace{z'_{11} + (1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right)}_{\text{image of } a_{22}} + \frac{z'_{11}}{1+z'_{11}}\right) \\
= & z'_{12} \\
a_{21} \mapsto & -y\,(1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right) \\
a_{22} \mapsto & z'_{11} - y^{-1}\underbrace{\left(-y\,(1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right)\right)}_{\text{image of } a_{21}} \\
= & z'_{11} + (1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right) \\
b_{12} \mapsto & -y^{-1}(p + y^{-1}\left(-y\left(p + yw'_{12}\right)\right)) = -y^{-1}(p - (p + yw'_{12})) = w'_{12} \\
b_{21} \mapsto & -y\left(p + yw'_{12}\right) \\
b_{22} \mapsto & -y^{-1}\underbrace{\left(-y\left(p + yw'_{12}\right)\right)}_{\text{image of } b_{21}} = p + yw'_{12}.
\end{aligned}$$

In all cases, we will proceed in the following manner. We pick a point of $\operatorname{Spec} k[x]$ (or $\operatorname{Spec} k[y]$) that corresponds to the residual image of $x$ (or $y$). Denote this point by $\mathfrak{p}_x$ (or $\mathfrak{p}_y$). We define the underlying map of topological spaces $\operatorname{Spec} k \to \operatorname{Spec} k[x]$ to send the point of $\operatorname{Spec} k$ to the ideal $\mathfrak{p}_x$ (or $\mathfrak{p}_y$). In the case analysis, we will construct an explicit ring homomorphism $g : \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{p}_x+\mathfrak{m}_1} \to \mathfrak{O}_K$, where $\mathfrak{m}_1 = (p, z_{11}, z_{12}, w_{12}) \subseteq R_1$, or in the case of $y$, $\mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{p}_y+\mathfrak{m}_2} \to \mathfrak{O}_K$, where $\mathfrak{m}_2 = (p, z'_{11}, z'_{12}, w'_{12}) \subseteq R_2$. Once this map has been defined, we define $\widetilde{f}^*$ by defining a map to the open subscheme $\operatorname{Spf} R_1$ (or $\operatorname{Spf} R_2$) and extending by zero to $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$.

More formally, for any open set $U \subseteq \operatorname{Spf} \mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$ containing $\mathfrak{p}_x \in \operatorname{Spec} k[x]$ (or $\mathfrak{p}_y$), we have a map

$$\mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}}(U) \to \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{m}_1+\mathfrak{p}_x} \quad \text{or} \quad \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}}(U) \to \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{m}_2+\mathfrak{p}_y}$$

by the universal property of the stalk. By composing this with our map

$$R_{1,\mathfrak{m}_1+\mathfrak{p}_x} = \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{m}_1+\mathfrak{p}_x} \to \mathfrak{O}_K \quad \text{or} \quad R_{2,\mathfrak{m}_2+\mathfrak{p}_y} = \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}, \mathfrak{m}_2+\mathfrak{p}_y} \to \mathfrak{O}_K$$

and extending by 0 on open sets not containing $\mathfrak{p}_x$ (or $\mathfrak{p}_y$), we obtain the map

$$\mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}} \to \widetilde{f}_* \mathcal{O}_{\operatorname{Spf} \mathfrak{O}_K}$$

of sheaves on $\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}}$.

Once the morphism $g$ is defined, it suffices to check that the diagram of rings

$$\begin{tikzcd}
 & R_{1,\mathfrak{m}_1+\mathfrak{p}_x} \arrow[dl, dashed, "g"] \\
\mathfrak{O}_K & R^{\mathrm{loc}}_{p,\mathrm{ord}} \arrow[l, "f"] \arrow[u, "h"]
\end{tikzcd} \tag{3.9}$$

commutes. Note that we denoted the inclusion $R^{\mathrm{loc}}_{p,\mathrm{ord}} \hookrightarrow R_{1,\mathfrak{m}_1+\mathfrak{p}_x}$ by $h$.

**Case 1:** $v_K(f(b_{21})) \le v_K(f(b_{22})) < \infty$ **or** $v_K(f(b_{21})) < v_K(f(b_{22})) = \infty$

We keep the above notation, and denote the maximal ideal of $\mathfrak{O}_K$ by $\mathfrak{m}_K$. Define $\alpha = -\frac{f(B_{22})}{f(B_{21})} \in \mathfrak{O}_K$, which has residue $\overline{\alpha} \in \mathfrak{O}_K/\mathfrak{m}_K$. Let $\mathfrak{p}_x \in k[x]$ be the prime corresponding to the point $\overline{\alpha}$. We will define a map $g : R_{1,\mathfrak{m}+\mathfrak{p}_x} \to \mathfrak{O}_K$ and check that (3.9) commutes.

We define $g$ via the natural map $W(k) \to \mathfrak{O}_K$ on the coefficient ring and by

$$\begin{aligned} g(x) &= -\frac{f(b_{22})}{f(b_{21})} \\ g(z_{11}) &= f(a_{22}) - \frac{f(b_{22})}{f(b_{21})} f(a_{21}) \\ g(z_{12}) &= f(a_{21}) \\ g(w_{12}) &= f(b_{21}) \end{aligned}$$

on the generators, using the valuation condition to define the image of $x$. We note that the images under $g \circ h$ of $W(k)$, $a_{21}$, $a_{22}$, $b_{21}$, and $b_{22}$ clearly match their images under $f$ by the definitions presented. It suffices to check the compatibility, then, for the images of $a_{12}$ and $b_{12}$.

We have $h(b_{12}) = -x(p + xw_{12}) \in R_{1,\mathfrak{m}+\mathfrak{p}_x}$. Observe that if $f(b_{21}) \neq 0$, which must be the case if either $v_K(f(b_{21})) \le v_K(f(b_{22})) < \infty$ or $v_K(f(b_{21})) < v_K(f(b_{22})) = \infty$, we have $f(b_{12}) = f(b_{21})^{-1}(f(b_{22})p - f(b_{22})^2) \in K$ by (3.5). Then

$$\begin{aligned} f(b_{12}) = f(b_{21})^{-1}(f(b_{22})p - f(b_{22})^2) &= -g(x)p + g(x)f(b_{21})\frac{f(b_{22})}{f(b_{21})} = -g(x)p + g(x)^2 g(w_{21}) \\ &= g(h(b_{12})), \end{aligned}$$

as needed.

Our next claim is that

$$f(b_{21})^2 + f(b_{21})^2 f(a_{22}) - f(b_{22})f(b_{21})f(a_{21}) \neq 0.$$

Suppose otherwise. Since $f(b_{21}) \neq 0$, $f(b_{21}) + f(b_{21})f(a_{22}) - f(b_{22})f(a_{21}) = 0$, or $f(b_{21}) = (1 + f(a_{22}))^{-1} f(b_{22})f(a_{21})$, which is absurd since $v_K(f(b_{22})) \ge v_K(f(b_{21}))$ and $v_K(a_{12}) > 0$.

We have

$$h(a_{12}) = x(1 + z_{11}) - x(1 + z_{11})^{-1} - x^2 z_{12} = x\left(z_{11} - xz_{12} + \frac{z_{11}}{1 + z_{11}}\right). \tag{3.10}$$

By (3.6) and the preceding claim,

$$\begin{aligned}
f(a_{12}) =& -\left(f(b_{21})^2 + f(b_{21})^2 f(a_{22}) - f(b_{22})f(b_{21})f(a_{21})\right)^{-1} f(b_{22}) \\
&\cdot \left(2f(a_{22})f(b_{21}) + f(a_{22})^2 f(b_{21}) - f(b_{22})f(a_{22})f(a_{21}) - f(b_{22})f(a_{21})\right) \\
=& g(x)\left(1 + f(a_{22}) - \frac{f(b_{22})}{f(b_{21})}f(a_{21})\right)^{-1} f(b_{21})^{-1} \\
&\cdot \left(2f(a_{22})f(b_{21}) + f(a_{22})^2 f(b_{21}) - f(b_{22})f(a_{22})f(a_{21}) - f(b_{22})f(a_{21})\right) \\
=& g(x)(1+g(z_{11}))^{-1}\left(f(a_{22}) + f(a_{22})\left(f(a_{22}) - \frac{f(b_{22})}{f(b_{21})}f(a_{21})\right)\right. \\
&\left. + f(a_{22}) - \frac{f(b_{22})}{f(b_{21})}f(a_{21})\right) \\
=& g(x)(1+g(z_{11}))^{-1}\left(f(a_{22}) + f(a_{22})g(z_{11}) + g(z_{11})\right) \\
=& g(x)\left(f(a_{22}) - \frac{f(b_{22})}{f(b_{21})}f(a_{21}) + \frac{f(b_{22})}{f(b_{21})}f(a_{21}) + \frac{g(z_{11})}{1+g(z_{11})}\right) \\
=& g(x)\left(g(z_{11}) + xg(z_{12}) + \frac{g(z_{11})}{1+g(z_{11})}\right) \\
=& g(h(a_{12})).
\end{aligned}$$

## Case 2: $v_K(f(C)) < v_K(f(w_{12}))$

In this case, we define

$$g : \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}},\mathfrak{m}+(y)} = R_{2,\mathfrak{m}+(y)} \to \mathfrak{O}_K,$$

setting $\mathfrak{p}_y = (y)$. We define $g$ via the natural map $W(k)$ on the coefficient field and by

$$\begin{aligned}
g(y) &= -\frac{f(b_{21})}{f(b_{22})} \\
g(z'_{11}) &= -\left(f(a_{22}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12})\right)\left(1 + f(a_{22}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12})\right)^{-1} \\
g(z'_{12}) &= f(a_{12}) \\
g(w'_{12}) &= f(b_{12})
\end{aligned}$$

on the generators, using the valuation condition to define the image of $y$.

We need to check that $g \circ h = f$, which is immediately true for the images of $W(k)$, $a_{12}$, and $b_{12}$. By (3.5), we have $-f(b_{21})f(b_{12}) = -pf(b_{22}) + f(b_{22})^2$. Note that $f(b_{22}) \neq 0$ by the inequality on the valuation, so we may rearrange to find

$$f(b_{22}) = -\frac{f(b_{21})}{f(b_{22})}f(b_{12}) + p = g(yw'_{12} + p) = g(h(b_{22})).$$

Since $g(h(b_{22})) = f(b_{22})$, we have

$$g(h(b_{21})) = g(-y(p+yw'_{12})) = -g(y)g(p+yw'_{12}) = \frac{f(b_{21})}{f(b_{22})}g(h(b_{22})) = f(b_{21})$$

as well. We are left to prove that the images of $a_{21}$ and $a_{22}$ are correct.

Rearranging the definition of $g$, we find

$$-\frac{f(b_{21})}{f(b_{22})}f(a_{12}) - f(a_{22}) = g(z'_{11})\left(1 + f(a_{22}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12})\right).$$

Collecting terms in $f(a_{22})$, we find

$$\begin{aligned}
-f(a_{22})(1+g(z'_{11})) =& g(z'_{11}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12})g(z'_{11}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12}) \\
f(a_{22}) =& -\left(g(z'_{11}) + \frac{f(b_{21})}{f(b_{22})}g(z'_{11})f(a_{12}) + \frac{f(b_{21})}{f(b_{22})}f(a_{12})\right)(1+g(z'_{11}))^{-1} \\
f(a_{22}) =& g(z'_{11}) + (1+g(z'_{11}))^{-1} \\
&\cdot\left(-2g(z'_{11}) - g(z'_{11})^2 - \frac{f(b_{21})}{f(b_{22})}f(a_{12}) - \frac{f(b_{21})}{f(b_{22})}g(z'_{11})f(a_{12})\right) \\
f(a_{22}) =& g(z'_{11}) + (1+g(z'_{11}))^{-1}\left(-2g(z'_{11}) - g(z'_{11})^2 + g(yz'_{12}) + g(yz'_{11}z'_{12})\right) \\
f(a_{22}) =& g(h(a_{22})).
\end{aligned}$$

By (3.6), we have

$$\begin{gathered}
f(a_{12})(f(b_{21})^2 + f(b_{21})^2 f(a_{22}) - f(b_{22})f(b_{21})f(a_{21})) = \\
-f(b_{22})(2f(a_{22})f(b_{21}) + f(a_{22})^2 f(b_{21}) - f(b_{22})f(a_{22})f(a_{21}) - f(b_{22})f(a_{21})),
\end{gathered}$$

which, separating out terms with $f(a_{21})$, rearranges to

$$\begin{gathered}
f(a_{21})\left(f(a_{12})f(b_{22})f(b_{21}) + f(b_{22})^2 f(a_{22}) + f(b_{22})^2\right) = \\
2f(b_{22})f(a_{22})f(b_{21}) + f(b_{22})f(a_{22})^2 f(b_{21}) + f(a_{12})f(b_{21})^2 + f(a_{12})f(b_{21})^2 f(a_{22}).
\end{gathered}$$

Noting that $f(b_{22})$ is invertible by the valuation condition, we have

$$\begin{gathered}
f(a_{21})\left(1 + f(a_{12})\frac{f(b_{21})}{f(b_{22})} + f(a_{22})\right) = \\
2f(a_{22})\frac{f(b_{21})}{f(b_{22})} + f(a_{22})^2\frac{f(b_{21})}{f(b_{22})} + f(a_{12})\frac{f(b_{21})^2}{f(b_{22})^2} + f(a_{12})f(a_{22})\frac{f(b_{21})^2}{f(b_{22})^2}.
\end{gathered}$$

We solve for $f(a_{21})$ in order to complete the proof of commutativity:

$$\begin{aligned}
f(a_{21}) =& -\frac{f(b_{21})}{f(b_{22})}\left(-2f(a_{22}) - f(a_{22})^2 - f(a_{12})\frac{f(b_{21})}{f(b_{22})} - f(a_{12})f(a_{22})\frac{f(b_{21})}{f(b_{22})}\right)\\
&\left(1 + f(a_{12})\frac{f(b_{21})}{f(b_{22})} + f(a_{22})\right)^{-1}\\
f(a_{21}) =& g(y)\left(-f(a_{22}) - f(a_{22})^2 - \left(f(a_{22}) + f(a_{12})\frac{f(b_{21})}{f(b_{22})}\right) + g(z'_{12})f(a_{22})g(y)\right)\\
&\left(1 + f(a_{12})\frac{f(b_{21})}{f(b_{22})} + f(a_{22})\right)^{-1}\\
f(a_{21}) =& g(y)\left(-f(a_{22}) - f(a_{22})^2 + g(z'_{12})f(a_{22})g(y)\right)\\
&\left(1 - g(z'_{12})g(y) + f(a_{22})\right)^{-1} + g(y)g(z'_{11})\\
f(a_{21}) =& -g(y)f(a_{22}) + g(y)g(z'_{11}).
\end{aligned}$$

Since we proved that $f(a_{22}) = g(h(a_{22}))$,

$$\begin{aligned}
f(a_{21}) &= -g(y)g(h(a_{22})) + g(yz'_{11}) \\
&= g\left(-y\left(z'_{11} + (1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right)\right) + yz'_{11}\right)\\
&= g\left(-y\,(1+z'_{11})^{-1}\left(-2z'_{11} - z'^2_{11} + yz'_{12} + yz'_{11}z'_{12}\right)\right)\\
&= g(h(a_{21})),
\end{aligned} \tag{3.11}$$

completing the proof of Case 2.

## Case 3: $f(b_{22}) = f(b_{21}) = 0$

If $f(b_{22}) = f(b_{21}) = 0$, relations (3.5) and (3.6) are automatically satisfied, so $f(a_{12})$, $f(a_{21})$, $f(a_{22})$, and $f(b_{12})$ are subject only to relations (3.7) and (3.8). In fact, we will just use the consequence

$$\begin{aligned}
&f(a_{12})p(p+pf(a_{22}) - f(b_{12})f(a_{21}))\\
&\quad = -f(b_{12})(2pf(a_{22}) + pf(a_{22})^2 - f(b_{12})f(a_{22})f(a_{21}) - f(b_{12})f(a_{21}))
\end{aligned} \tag{3.12}$$

of (3.7) in the proof of this case. Let the ramification index of $K/\mathbf{Q}_p$ be denoted $e$. The definition of the map $h$ suggests that to choose the image of $x$ in this case, one might use the definition $g(x) = p^{-1}f(b_{12})$ if the right hand side exists in $\mathfrak{O}_K$. Else, one can use $g(y) = pf(b_{12})^{-1}$ on the chart $\operatorname{Spf} R_2$. Thus, we break into two subcases.

**Subcase 3.1:** $v_K(f(b_{12})) \geq e$

We define $\mathfrak{p}_x$ using the residue of $p^{-1}f(b_{12})$ as in Case 1, and construct a map out of $R_{1,\mathfrak{m}+\mathbf{p}_x}$. We define $g$ via the natural map on the coefficient field $W(k)$, and by

$$\begin{aligned} g(x) &= -p^{-1}f(b_{12}) \\ g(z_{11}) &= f(a_{22}) - p^{-1}f(b_{12})f(a_{21}) \\ g(z_{12}) &= f(a_{21}) \\ g(w_{12}) &= f(b_{21}) = 0 \end{aligned}$$

on the generators.

By remarks at the beginning of the section, it suffices to check that $f = g \circ h$, which is immediately true for the images of $W(k)$, $a_{21}$, $a_{22}$, $b_{12}$, $b_{21}$, and $b_{22}$ (since $g(h(b_{22})) = p^{-1}f(b_{12})f(b_{21}) = 0$).

Thus it suffices to show that $g(h(a_{12})) = f(a_{12})$. By (3.12), we have

$$\begin{aligned} f(a_{12}) =& - p^{-1}f(b_{12})(2f(a_{22}) + f(a_{22})^2 - p^{-1}f(b_{12})f(a_{22})f(a_{21}) - p^{-1}f(b_{12})f(a_{21})) \\ &\cdot (1 + f(a_{22}) - p^{-1}f(b_{12})f(a_{21}))^{-1}. \\ =& g(x)(f(a_{22})\left(1 + f(a_{22}) - p^{-1}f(b_{12})f(a_{21})\right) + f(a_{22}) - p^{-1}f(b_{12})f(a_{21})) \\ &\cdot (1 + f(a_{22}) - p^{-1}f(b_{12})f(a_{21}))^{-1}. \\ =& g(x)\left(f(a_{22}) + g(z_{11})(1 + f(a_{22}) - p^{-1}f(b_{12})f(a_{21}))^{-1}\right) \\ =& g(x)\left(g(z_{11}) + p^{-1}f(b_{12})f(a_{21}) + g(z_{11})(1 + g(z_{11}))^{-1}\right) \\ =& g(x)\left(g(z_{11}) - g(x)g(z_{12}) + g(z_{11})(1 + g(z_{11}))^{-1}\right) \\ =& g(h(a_{12})), \end{aligned}$$

where the last equality follows from (3.10).

**Subcase 3.2:** $v_K(f(b_{12})) < e$

As in Case 2, we define a map

$$g : \mathcal{O}_{\mathfrak{X}^{\mathrm{loc}}_{p,\mathrm{ord}},\mathfrak{m}+(y)} = R_{2,\mathfrak{m}+(y)} \to \mathcal{O}_K.$$

We define $g$ by the natural map on the coefficient ring $W(k)$ and by

$$\begin{aligned} g(y) &= -pf(b_{12})^{-1} \\ g(z'_{11}) &= -\left(pf(b_{12})^{-1}f(a_{12}) + f(a_{22})\right)\left(1 + f(a_{22}) + pf(b_{12})^{-1}f(a_{12})\right)^{-1} \\ g(z'_{12}) &= f(a_{12}) \\ g(w'_{12}) &= f(b_{12}), \end{aligned}$$

where the definition of $g(y)$ is possible by the valuation condition.

It suffices to check that $f = g \circ h$, which is immediately true for the images of $W(k)$, $a_{12}$, $b_{12}$, $b_{21}$, and $b_{22}$. We are left to prove that $f(a_{21}) = g(h(a_{21}))$ and $f(a_{22}) = g(h(a_{22}))$.

Rearranging the definition of $g(z'_{11})$, we have

$$-pf(b_{12})^{-1}f(a_{12}) - f(a_{22}) = g(z'_{11})\left(1 + f(a_{22}) + pf(b_{12})^{-1}f(a_{12})\right).$$

Rearranging to group the terms with $f(a_{22})$ together, we find

$$\begin{aligned}
-f(a_{22})(g(z'_{11})+1) =& g(z'_{11}) + pf(b_{12})^{-1}g(z'_{11})f(a_{12}) + pf(b_{12})^{-1}f(a_{12})\\
f(a_{22}) =& -\left(g(z'_{11}) + pf(b_{12})^{-1}g(z'_{11})f(a_{12}) + pf(b_{12})^{-1}f(a_{12})\right)(g(z'_{11})+1)^{-1}\\
f(a_{22}) =& g(z'_{11}) + (1+g(z'_{11}))^{-1}\left(-2g(z'_{11}) - g(z'_{11})^2 - pf(b_{12})^{-1}f(a_{12})\right.\\
&\left.-pf(b_{12})^{-1}g(z'_{11})f(a_{12})\right)\\
f(a_{22}) =& g(z'_{11}) + (1+g(z'_{11}))^{-1}\left(-2g(z'_{11}) - g(z'_{11})^2 + g(yz'_{12}) + g(yz'_{11}z'_{12})\right)\\
f(a_{22}) =& g(h(a_{22})).
\end{aligned}$$

By (3.12), we have

$$\begin{aligned}
&f(a_{12})p(p+pf(a_{22}) - f(b_{12})f(a_{21}))\\
&\qquad = -f(b_{12})(2pf(a_{22}) + pf(a_{22})^2 - f(b_{12})f(a_{22})f(a_{21}) - f(b_{12})f(a_{21})).
\end{aligned}$$

Collecting terms in $f(a_{21})$, we have

$$\begin{aligned}
&-f(a_{21})f(b_{12})\left(pf(a_{12}) + f(b_{12})(1+f(a_{22}))\right)\\
&\qquad = -f(a_{12})p^2(1+f(a_{22})) - f(b_{12})(2pf(a_{22}) + pf(a_{22})^2).
\end{aligned}$$

Since $f(b_{12})$ is invertible by assumption, we have

$$\begin{aligned}
&f(a_{21})\left(1 + pf(b_{12})^{-1}f(a_{12}) + f(a_{22})\right) =\\
&\qquad f(a_{12})p^2f(b_{12})^{-2}(1+f(a_{22})) + pf(b_{12})^{-1}(2f(a_{22}) + f(a_{22})^2).
\end{aligned}$$

We now move $1 + pf(b_{12})^{-1}f(a_{12}) + f(a_{22})$ to the right and evaluate as follows.

$$\begin{aligned}
f(a_{21}) =& -pf(b_{12})^{-1}\left(-f(a_{12})pf(b_{12})^{-1}(1+f(a_{22})) - 2f(a_{22}) - f(a_{22})^2\right)\\
&\left(1 + f(a_{22}) + pf(b_{12})^{-1}f(a_{12})\right)^{-1}\\
f(a_{21}) =& -pf(b_{12})^{-1}\left(-f(a_{12})pf(b_{12})^{-1}f(a_{22}) - f(a_{22}) - f(a_{22})^2\right)\\
&\left(1 + f(a_{22}) + pf(b_{12})^{-1}f(a_{12})\right)^{-1} + g(y)g(z'_{11})\\
f(a_{21}) =& g(y)\left(g(z'_{12})g(y)f(a_{22}) - f(a_{22}) - f(a_{22})^2\right)(1 + f(a_{22}) - g(y)g(z'_{12}))^{-1} + g(y)g(z'_{11})\\
f(a_{21}) =& -f(a_{22})g(y) + g(y)g(z'_{11}).
\end{aligned}$$

Since we have shown already that $f(a_{22}) = g(h(a_{22}))$, the remainder of the computation proceeds exactly as in (3.11).

## 3.8 Additional Properties of $R^{\mathrm{loc}}_{p,\mathrm{ord}}$

We need to know additional facts concerning the ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$. The first is a bound on the Krull dimension, which will be necessary in producing a well-behaved family of deformation rings $R_Q$ that are essential to the argument of Section 6.

**Proposition 3.8.** *We have* $\dim R^{\mathrm{loc}}_{p,\mathrm{ord}} \leq 5$.

*Remark* 3. We will show in Corollary 6.4 that in fact $\dim R^{\mathrm{loc}}_{p,\mathrm{ord}} = 5$.

*Proof.* Note that for any ideal $\mathfrak{a}$ of a ring $R$, $\dim R \geq \dim R/\mathfrak{a}$, since the primes of $R$ are in order-preserving bijection with the primes of $R$ containing $\mathfrak{a}$. Let $\mathfrak{b}_1$ be the ideal generated by relations (3.5) and (3.6). If we show that $5 \geq \dim R^{\mathrm{loc}}_p/\mathfrak{b}_1$, then

$$5 \geq \dim R^{\mathrm{loc}}_p/\mathfrak{b}_1 \geq \dim R^{\mathrm{loc}}_p/\mathfrak{b}_0 \geq \dim R^{\mathrm{loc}}_p/\mathfrak{b} = R^{\mathrm{loc}}_{p,\mathrm{ord}}, \tag{3.13}$$

as desired.

Let $R_0 = W(k)[[B_{12}, B_{21}, B_{22}]]$, an integral domain of dimension 4 and, by Gauss's lemma, a UFD. Then the ideal $(-B_{21}B_{12} + B_{22}p - B_{22}^2)$ is prime by the following claim.

**Claim 3.9.** *The element*

$$-B_{21}B_{12} + B_{22}p - B_{22}^2$$

*is an irreducible element of* $W(k)[[B_{12}, B_{21}, B_{22}]]$.

*Proof.* Suppose that $-B_{21}B_{12} + B_{22}p - B_{22}^2 = fg$ for $f, g \in W(k)[[B_{12}, B_{21}, B_{22}]]$. Moreover, suppose that $f, g$ are not units. Consider both sides modulo $\mathfrak{m}_{R_0}^3$. Since $f, g \in \mathfrak{m}_{R_0}$, we can ignore all monomials of degree 2 or higher (in $p, B_{12}, B_{21}$, and $B_{22}$) in either $f$ or $g$, since these vanish in the product modulo $\mathfrak{m}_{R_0}^3$. Thus,

$$-B_{21}B_{12} + B_{22}p - B_{22}^2 = (\alpha p + \alpha_{12}B_{12} + \alpha_{21}B_{21} + \alpha_{22}B_{22})(\beta p + \beta_{12}B_{12} + \beta_{21}B_{21} + \beta_{22}B_{22}),$$

where the values of $\alpha, \beta$ are only important modulo $\mathfrak{m}$, and thus can be assumed to take values in the image of the Teichmüller lift of $k$, which we will identify with $k$. From the term $-B_{22}^2$ we may already deduce $\beta_{22} = -\alpha_{22}^{-1}$, and neither of these values vanish. Next note that $\alpha_{12}\beta_{12} = 0$ and $\alpha_{21}\beta_{21} = 0$, but if both $\alpha_{12}$ and $\alpha_{21}$ vanish or both $\beta_{12}$ and $\beta_{21}$ vanish then the term $-B_{21}B_{12}$ cannot possibly appear on the left. Thus we must either have $\alpha_{12} = \beta_{21} = 0$ or $\alpha_{21} = \beta_{12} = 0$. Since $B_{21}$ and $B_{12}$ are symmetric in both expressions, we can assume without loss of generality that $\alpha_{12} = \beta_{21} = 0$. Looking at the right hand side, we also have $\alpha\beta = 0$. Without loss of generality, we may assume $\beta = 0$, since we may otherwise switch the two factors. Finally note that $\alpha_{21}\beta_{12} = -1$, so $\beta_{12} = -\alpha_{21}^{-1}$ and $\alpha \cdot (-\alpha_{22}^{-1}) = 1$, so $\alpha = -\alpha_{22}$. Thus, we have

$$-B_{21}B_{12} + B_{22}p - B_{22}^2 = (-\alpha_{22}p + \alpha_{21}B_{21} + \alpha_{22}B_{22})(-\alpha_{21}^{-1}B_{12} - \alpha_{22}^{-1}B_{22}),$$

with neither $\alpha_{22}$ nor $\alpha_{21}$ equal to 0. Since the right hand side has a nontrivial $B_{12}B_{22}$ term not present on the left, this factorization is impossible, and $-B_{21}B_{12} + B_{22}p - B_{22}^2$ is irreducible as claimed.

□

Note that $-B_{21}B_{12} + B_{22}p - B_{22}^2$ strictly contains the prime ideal 0. Defining $R_1 = R_0/(-B_{21}B_{12} + B_{22}p - B_{22}^2)$, we must have $\dim R_1 < \dim R_0$, since any maximal chain of prime ideals in $R_0$ must begin with (0), which does not correspond to a prime ideal of $R_1$. In particular, $\dim R_1 \leq 3$, and by Claim 3.9, $R_1$ is an integral domain. (It is easy to see, in fact, that $\dim R_1 = 3$.)

Define $R_2 = R_1[[A_{12}, A_{21}, A_{22}]]$, also an integral domain, now satisfying $\dim R_2 \leq 5$. Define

$$R_3 = R_2/(A_{12}(B_{21}^2 + B_{21}^2 A_{22} - B_{22}B_{21}A_{21}) + B_{22}(2A_{22}B_{21} + A_{22}^2 B_{21} - B_{22}A_{22}A_{21} - B_{22}A_{21}).$$

Let

$$a = B_{21}^2 + B_{21}^2 A_{22} - B_{22}B_{21}A_{21}$$

and

$$b = B_{22}(2A_{22}B_{21} + A_{22}^2 B_{21} - B_{22}A_{22}A_{21} - B_{22}A_{21}),$$

so that $R_3 = R_2/(A_{12}a + b)$.

**Claim 3.10.** *The element $A_{12}a + b$ is nonzero in $R_2$.*

*Proof.* It suffices to show that $a$ is nonzero, since $b$ (which has no factor of $A_{12}$) cannot be equal to $-A_{12}a$ if it is nonzero. We can factor

$$a = B_{21}^2 + B_{21}^2 A_{22} - B_{22}B_{21}A_{21} = B_{21}\left(B_{21} + B_{21}A_{22} + B_{22}A_{21}\right). \tag{3.14}$$

Since

$$R_2 = W(k)[[A_{12}, A_{21}, A_{22}, B_{12}, B_{21}, B_{22}]]/(-B_{21}B_{12} + B_{22}p - B_{22}^2)$$

is an integral domain by Claim 3.9, it suffices to show that neither factor of (3.14) is contained in $(-B_{21}B_{12} + B_{22}p - B_{22}^2)$. But $B_{21} \in \mathfrak{m}_{R_2} \setminus \mathfrak{m}_{R_2}^2$, as is $B_{21} + B_{21}A_{22} + B_{22}A_{21}$, so neither of these can be a multiple of $-B_{21}B_{12} + B_{22}p - B_{22}^2 \in \mathfrak{m}_{R_2}^2$. $\square$

Since $R_2$ is an integral domain of dimension at most 6, and by Claim 3.10, $(A_{12}a + b)$ strictly contains the prime ideal (0), $\dim R_3 < \dim R_2 \leq 6$ by the same argument as used earlier. Thus $\dim R_3 \leq 5$, and since $R_3 = R_p^{\mathrm{loc}}/\mathfrak{b}_1$, we find $\dim R_{p,\mathrm{ord}}^{\mathrm{loc}} \leq 5$ by (3.13).

$\square$

The second property of $R_{p,\mathrm{ord}}^{\mathrm{loc}}$ we need is that maps out of $R_{p,\mathrm{ord}}^{\mathrm{loc}}$ satisfy a key property that holds for ordinary deformations. In particular, conjugation of a map $R_{p,\mathrm{ord}}^{\mathrm{loc}} \to R$ by a residually trivial element of $\mathrm{GL}_2(R)$ should yield another such map. A special case of this fact is that the ideal $\mathfrak{b}$ defined in Section 3.6 is invariant under the action of $\mathbf{1}_2 + \mathbf{M}_2(R_p^{\mathrm{loc}})$ given by conjugation of the underlying representation. We will prove the following result of Taylor [Tay09] showing that under some weak hypotheses that hold in the case of $R_{p,\mathrm{ord}}^{\mathrm{loc}}$, this special case implies the general statement that we need.

**Proposition 3.11** ([Tay09]). *Let $\rho_p^{\mathrm{loc}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(R_p^{\mathrm{loc}})$ be the universal lifting, and let $\mathfrak{a} \subset R_p^{\mathrm{loc}}$ be an ideal closed under the action of $\mathbf{1}_2+\mathbf{M}_2(R_p^{\mathrm{loc}})$ defined by sending $\alpha \in \mathbf{1}_2+\mathbf{M}_2(R_p^{\mathrm{loc}})$ to the morphism $A_{ij} \mapsto (\alpha A\alpha^{-1})_{ij}$, $B_{ij} \mapsto (\alpha B\alpha^{-1})_{ij}$. Moreover, assume that the ring $R_p^{\mathrm{loc}}/\mathfrak{a}$ is reduced and not equal to the residue field $k$. Then the functor $D_{\mathfrak{a}} : \mathbf{CLNRings} \to \mathbf{Sets}$ defined by*

$$D_{\mathfrak{a}} : R \mapsto \left\{r : R_p^{\mathrm{loc}} \to R | r(\mathfrak{a}) = (0)\right\}$$

*defines a local deformation condition at $p$.*

We will need to use the following result in the proof of Proposition 3.11.

**Lemma 3.12.** *Let $R$ be a reduced complete Noetherian local ring with residue field $k$, and assume $R \neq k$. Let $F \in R[[x]]$. If $F(x) = 0$ for all $x \in \mathfrak{m}_R$, then $F = 0$.*

*Proof.* Since $R$ is reduced, $R \hookrightarrow \oplus_{\mathfrak{p}} R/\mathfrak{p}$, where the direct sum is over all prime ideals of $R$. If $F$ vanishes on $\mathfrak{m}_R$, then it vanishes on $\mathfrak{m}_{R/\mathfrak{p}} = \mathfrak{m}_R/\mathfrak{p}$. Thus, if the lemma holds for integral domains, then it holds for all rings meeting the conditions of the lemma.

Write $F(x) = \sum_i F_i x^i$ with $F_i \in R$. If $F(x) = x^n G(x)$ with $n$ maximal, then for all nonzero elements $a \in \mathfrak{m}_R$, $a^n \neq 0$, so $G(a) = 0$. Moreover, letting $a_i \in \mathfrak{m}_R^i$ and letting $G = \sum_i G_i x^i$, we have $G(0) - G(a_i) = G(0) \in \mathfrak{m}_R^i$, so $G(0) \in \bigcap_i \mathfrak{m}_R^i = (0)$. Thus $G$ satisfies the same property that $F$ does, so we may assume that $F_0 \neq 0$.

Next choose $a \in \mathfrak{m}_R \setminus 0$ and consider

$$F_0^{-1}F(F_0 ax) = \sum_i F_i F_0^{i-1} x^i a^i = 1 + F_1 ax + F_2 F_0 a^2 x^2 + \dots.$$

We note that $F_0^{-1}F(F_0ax) = 0$ for all $x \in \mathfrak{m}_R$ – otherwise, multiplying by $F_0$ on both sides yields a contradiction (since $R$ is an integral domain and $F_0 \neq 0$). Let $G(x) = F_0^{-1}F(F_0ax) = \sum_i G_i x^i$. Then $G(x)$ satisfies $G_0 = 1$ and $G_i \in \mathfrak{m}_R$ for $i > 1$. In particular, $G(x)$ is the sum of a unit and an element of $\mathfrak{m}_R$ for all $x \in \mathfrak{m}_R$, a contradiction. $\square$

*Proof of Proposition 3.11.* The functor $D_{\mathfrak{a}}$ defines a relatively representable subfunctor of $D_p^{\mathrm{loc}}$ since it is representable by $\mathrm{Hom}(R_p^{\mathrm{loc}}/\mathfrak{a}, \cdot)$. Thus it suffices to prove that for a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ lifting $\overline{\rho}$ such that the natural map $r : R_p^{\mathrm{loc}} \to R$ satisfies $r(\mathfrak{a}) = 0$ and any $\alpha \in \mathbf{1}_2 + \mathbf{M}_2(R)$, the natural map $r_\alpha : R_p^{\mathrm{loc}} \to R$ associated to the representation $\alpha\rho\alpha^{-1} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ satisfies $r_\alpha(\mathfrak{a}) = 0$ as well.

Consider the map $\sigma : R_p^{\mathrm{loc}} \to R_p^{\mathrm{loc}}[[C_{11}, C_{12}, C_{21}, C_{22}]]$ induced by the representation

$$\begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix} \rho^{\mathrm{loc}} \begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix}^{-1} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R_p^{\mathrm{loc}}).$$

Then for all $a \in R_p^{\mathrm{loc}}$,

$$\sigma(a) \equiv \mathbf{1}_{R_p^{\mathrm{loc}}}(a) \bmod (C_{11}, C_{12}, C_{21}, C_{22}),$$

where $\mathbf{1}_{R_p^{\mathrm{loc}}}$ is the identity map.

For any ring $R$, let $\mathbf{C}_R = (c_{11}, c_{12}, c_{21}, c_{22}) \in \mathfrak{m}_R^4$. Then define

$$\mathrm{ev}_{\mathbf{C}_R} : R[[C_{11}, C_{12}, C_{21}, C_{22}]] \to R$$

to be the homomorphism $C_{ij} \mapsto c_{ij}$. In this language, we can rephrase the condition that $\mathfrak{a} \subset R_p^{\mathrm{loc}}$ be closed under the action of $\mathbf{1}_2 + \mathbf{M}_2(R_p^{\mathrm{loc}})$ as the statement that for all choices of $\mathbf{C}_{R_p^{\mathrm{loc}}}$, $\mathrm{ev}_{\mathbf{C}_{R_p^{\mathrm{loc}}}}(\sigma(\mathfrak{a})) \subseteq \mathfrak{a}$.

Suppose that $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ is such that the induced homomorphism $r : R_p^{\mathrm{loc}} \to R$ satisfies $r(\mathfrak{a}) = 0$, and let $\mathbf{C}_R = (c_{11}, c_{12}, c_{21}, c_{22}) \in \mathfrak{m}_R^4$. The representation

$$\begin{pmatrix} 1+c_{11} & c_{12} \\ c_{21} & 1+c_{22} \end{pmatrix} \rho \begin{pmatrix} 1+c_{11} & c_{12} \\ c_{21} & 1+c_{22} \end{pmatrix}^{-1}$$

induces a second homomorphism $r' : R_p^{\mathrm{loc}} \to R$. It suffices to show that $r'(\mathfrak{a}) = 0$.

**Claim 3.13.** *We have* $r' = \mathrm{ev}_{\mathbf{C}_R} \circ r \circ \sigma$.

*Proof.* Our claim is that $r'$ is the composition

$$R_p^{\mathrm{loc}} \xrightarrow{\sigma} R_p^{\mathrm{loc}}[[C_{11}, C_{12}, C_{21}, C_{22}]] \xrightarrow{r} R[[C_{11}, C_{12}, C_{21}, C_{22}]] \xrightarrow{\mathrm{ev}_{\mathbf{C}_R}} R.$$

The claim follows by noting that the sequence of homomorphisms corresponds to the following sequence of representations

$$\begin{aligned} \rho_p^{\mathrm{loc}} &\to \begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix} \rho_p^{\mathrm{loc}} \begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix}^{-1} \\ &\to \begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix} \rho \begin{pmatrix} 1+C_{11} & C_{12} \\ C_{21} & 1+C_{22} \end{pmatrix}^{-1} \\ &\to \begin{pmatrix} 1+c_{11} & c_{12} \\ c_{21} & 1+c_{22} \end{pmatrix} \rho \begin{pmatrix} 1+c_{11} & c_{12} \\ c_{21} & 1+c_{22} \end{pmatrix}^{-1} \end{aligned}$$

via projection.

□

If we prove that $\sigma(\mathfrak{a}) \subseteq \mathfrak{a}[[C_{11}, C_{12}, C_{21}, C_{22}]]$, then Claim 3.13 implies that $r'(\mathfrak{a}) = 0$.

So let $a \in \mathfrak{a}$, and consider the function $F = \sigma(a) \bmod \mathfrak{a} \in R_p^{\mathrm{loc}}/\mathfrak{a}[[C_{11}, C_{12}, C_{21}, C_{22}]]$. Recall that $\mathrm{ev}_{\mathbf{C}_{R_p^{\mathrm{loc}}}}(F) = 0 \bmod \mathfrak{a}$ for all $\mathbf{C}_{R_p^{\mathrm{loc}}} \in \mathfrak{m}_{R_p^{\mathrm{loc}}}^4$, so we also have $\mathrm{ev}_{\mathbf{C}_{R_p^{\mathrm{loc}}/\mathfrak{a}}}(F) = 0 \bmod \mathfrak{a}$ for all $\mathbf{C}_{R_p^{\mathrm{loc}}} \in \mathfrak{m}_{R_p^{\mathrm{loc}}/\mathfrak{a}}^4$.

For any $(c_{11}, c_{12}, c_{21}) \in \mathfrak{m}_{R_p^{\mathrm{loc}}/\mathfrak{a}}^3$, we substitute these values for $c_{11}, c_{12}, c_{21}$ to obtain $0 = F$ by Lemma 3.12, considered as an element of $R_p^{\mathrm{loc}}/\mathfrak{a}[[C_{22}]]$. Thus, writing $F = \sum_i F_i C_{22}$, all of the coefficients $F_i \in R_p^{\mathrm{loc}}/\mathfrak{a}[[C_{11}, C_{12}, C_{21}]]$ vanish for all choices of $(c_{11}, c_{12}, c_{21}) \in \mathfrak{m}_{R_p^{\mathrm{loc}}/\mathfrak{a}}^3$. Applying Lemma 3.12 repeatedly in this fashion, we find that $F$ vanishes.

□

**Proposition 3.14.** *The ideal $\mathfrak{b} \subseteq R_p^{\mathrm{loc}}$ satisfies the conditions of Proposition 3.11. In fact, the ideal $\mathfrak{b}$ is $\mathrm{GL}_2(R_p^{\mathrm{loc}})$-invariant.*

*Proof.* Since
$$R_{p,\mathrm{ord}}^{\mathrm{loc}} \hookrightarrow \Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}}) \hookrightarrow W(k)\langle x\rangle [[z_{11}, z_{12}, w_{12}]],$$
it is an integral domain. Since $R_{p,\mathrm{ord}}^{\mathrm{loc}}$ includes $W(k)$, it is not equal to its residue field. Thus, $R_{p,\mathrm{ord}}^{\mathrm{loc}} = R_p^{\mathrm{loc}}/\mathfrak{b}$ meets both of the supplementary hypotheses for Proposition 3.11.

Next, recall that $\mathfrak{b}$ is the kernel of the morphism $\psi : R_p^{\mathrm{loc}} \to \Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}})$. We will define an action of $\mathrm{GL}_2(R_p^{\mathrm{loc}})$ on $\Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}})$, and show that $\psi$ is equivariant under this action in the sense that for any element $\alpha \in \mathrm{GL}_2(R_p^{\mathrm{loc}})$ and element $r \in R_p^{\mathrm{loc}}$ we have $\varphi(r)^\alpha = \varphi(r^\alpha)$.

Since a morphism out of $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}$ corresponds to a representation that is ordinary, and the class of ordinary representations are closed under conjugation, there is already a natural action of $\mathrm{GL}_2(R_p^{\mathrm{loc}})$ on $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}$ that "automatically" agrees with the action on $R_p^{\mathrm{loc}}$. In particular, we defined $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}$ by gluing together the formal schemes $\mathfrak{X}_1 = \mathrm{Spf}\, W(k)\langle x\rangle [[z_{11}, z_{12}, w_{12}]]$ and $\mathfrak{X}_2 = \mathrm{Spf}\, W(k)\langle y\rangle [[z'_{11}, z'_{12}, w'_{12}]]$, so it suffices to define the morphism on these. The former corresponds to the representation given by (3.1) and (3.2) as
$$\rho(\sigma) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1+z_{11} & z_{12} \\ 0 & \psi(\sigma)(1+z_{11})^{-1} \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$
and
$$\rho(\tau) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$
and the latter can be written using (3.3) and (3.4) similarly. Thus, one can compute the conjugate $\alpha\rho\alpha^{-1}$ of this representation by $\alpha \in \mathrm{GL}_2(R_p^{\mathrm{loc}})$ by computing
$$(\alpha\rho\alpha^{-1})(\sigma) = \alpha\rho(\sigma)\alpha^{-1} = \alpha \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1+z_{11} & z_{12} \\ 0 & \psi(\sigma)(1+z_{11})^{-1} \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \alpha^{-1} \tag{3.15}$$
and
$$(\alpha\rho\alpha^{-1})(\tau) = \alpha\rho(\tau)\alpha^{-1} = \alpha \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^{-1} \alpha^{-1}, \tag{3.16}$$
where one uses the natural map $R_p^{\mathrm{loc}} \to \Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}})$ and inclusion $\Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}}) \hookrightarrow W(k)\langle x\rangle [[z_{11}, z_{12}, w_{12}]]$ to regard the entries of $\alpha$ as elements of the ring $W(k)\langle x\rangle [[z_{11}, z_{12}, w_{12}]]$. The image of $x$ is determined by taking the image of the basis $\left(\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ under left-multiplication by $\alpha$ and right-multiplying by another matrix $m$ to renormalize it to appear in the form $\left(\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. If we constrain $m$ to only scale the left column of the matrix $\alpha \left(\begin{smallmatrix} x & 1 \\ 1 & 0 \end{smallmatrix}\right)$, the conjugated matrices
$$m \begin{pmatrix} 1+z_{11} & z_{12} \\ 0 & \psi(\sigma)(1+z_{11})^{-1} \end{pmatrix} m^{-1} \quad \text{and} \quad m \begin{pmatrix} 1 & w_{12} \\ 0 & \psi(\tau) \end{pmatrix} m^{-1}$$

will be in the form necessary of an ordinary representation (since the underlying filtration of $R^2$ hasn't changed) and the choice of $m$ is unique by the same argument as used in the proof of Proposition 3.6.

It is clear from the definitions that the $\mathrm{GL}_2(R_p^{\mathrm{loc}})$-action is equivariant on the map $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}} \to \operatorname{Spf} R_p^{\mathrm{loc}}$, since both of these are identical to conjugation of the underlying representation. We note that the $\mathrm{GL}_2(R_p^{\mathrm{loc}})$ action on $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}$ yields an action of $\mathrm{GL}_2(R_p^{\mathrm{loc}})$ on $\Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}})$ as follows. An element $\alpha \in \mathrm{GL}_2(R_p^{\mathrm{loc}})$ acts as an invertible morphism $\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}} \to \mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}$, so in particular it must be an isomorphism on the topological spaces. Thus the map

$$\alpha^{\#} : \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}} \to \alpha_* \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}}$$

includes as part of its data a map

$$\Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}}) \to \Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}}).$$

In particular, we have an equivariant morphism of rings $R_p^{\mathrm{loc}} \to \Gamma(\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}, \mathcal{O}_{\mathfrak{X}_{p,\mathrm{ord}}^{\mathrm{loc}}})$.

Finally, for any $a \in \mathfrak{b}$, we have $\psi(a^\alpha) = \psi(a)^\alpha = 0^\alpha = 0$, so $\mathfrak{b}$ is closed under the $\mathrm{GL}_2(R_p^{\mathrm{loc}})$-action.

□

*Remark* 4. One can check computationally that $\mathfrak{b}_0 \subseteq \mathfrak{b}$ above is also $\mathrm{GL}_2(R_p^{\mathrm{loc}})$-invariant. The fourth relation (3.8) is essential for this fact.

The $\mathrm{GL}_2(R_p^{\mathrm{loc}})$-invariance in Proposition 3.14 is a consequence of the residual triviality of the representation $\overline{\rho}$. Otherwise, only matrices that preserve the residual filtration for the ordinary representation $\overline{\rho}$ could possibly leave $\mathfrak{b}$ invariant.

We define the functor $D_{p,\mathrm{ord}}^{\mathrm{loc}} = D_{\mathfrak{b}}$ in the language of Proposition 3.11. Combining Proposition 3.14 with Proposition 3.11 yields the following result.

**Corollary 3.15.** *Let $\overline{\rho}$ be the trivial representation on $G_{\mathbf{Q}_p}$, and let*

$$D_{\overline{\rho}} : \mathbf{CLNRings}(k) \to \mathbf{Sets}$$

*be defined by*

$$R \mapsto \{\textit{strict equivalence classes of representations } \rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R) | \rho \textit{ lifts } \overline{\rho}\}.$$

*The functor $D_{p,\mathrm{ord}}^{\mathrm{loc}}$ is a subfunctor of $D_{\overline{\rho}}$ and defines a local deformation condition.*

# Chapter 4

# Construction of a Family $\{R_{Q_n,\mathrm{ord}}\}$ of Global Deformation Rings

Let $k$ be a field of characteristic $p$, and fix an absolutely irreducible residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$ that is residually trivial when restricted to $G_{\mathbf{Q}_p}$. Let $T = N(\overline{\rho})$, and let $Q$ be a finite set of primes not dividing $Tp$. Assume that $T$ is squarefree. Recall from Section 3 the construction of a ring $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ representing the local deformation problem defined in Section 3.3 when restricted to the subcategory $\mathbf{DVR}(k)$. By applying results from Section 2.1.3, we will define rings representing the solutions to various global deformation problems.

Specifically, we construct rings $R_{Q,\mathrm{ord}}$ and $R^{\square}_{Q,\mathrm{ord}}$, where the latter is framed. These rings will be used in Section 6 to prove that lifts of $\overline{\rho}$ are modular. For the proof, we will need to know bounds on the Krull dimension of the rings $R_{Q,\mathrm{ord}}$ and $R^{\square}_{Q,\mathrm{ord}}$. For this purpose, it will nearly suffice to use the dimension of the tangent space as a crude bound on the number of variables adjoined to the coefficient ring. However, looking at $R^{\mathrm{loc}}_{p,\mathrm{ord}}$, one finds that the Krull dimension of the ring, which was bounded in Proposition 3.8 by 5, is substantially less than the bound of 7 given by a cohomological calculation. For this reason, while we will use cohomological methods for the places away from $p$, we will make use of the explicit local deformation theory in computing our final global bound. Moreover, we will work with the framed ring $R^{\square}_{Q,\mathrm{ord}}$ in order to make this computation possible, but in the end we will also conclude a bound for the Krull dimension of $R_{Q,\mathrm{ord}}$.

We will only consider lifts of $\overline{\rho}$ that are *minimally ramified*, which is a deformation-theoretic condition that we will define in Section 4.1. The definition corresponds exactly to the possible structures for the representations $\rho_f$ associated to modular forms $f$ of level $N_f$ such that for each $t \in T$, $t$ exactly divides $N_f$.

In Sections 4.2 and 4.3, we construct $R_{Q,\mathrm{ord}}$ and $R^{\square}_{Q,\mathrm{ord}}$. In Sections 4.4 and 4.5, we use cohomological techniques to prove bounds on the dimensions of $R_{Q,\mathrm{ord}}$ and $R^{\square}_{Q,\mathrm{ord}}$ in terms of properties of $\overline{\rho}$ at the primes in $Q$. In Section 4.7, we prove additional properties of the rings $R_{Q,\mathrm{ord}}$ and $R^{\square}_{Q,\mathrm{ord}}$ assuming certain properties of the primes in $Q$. In Section 4.8, we construct a family of sets of primes $Q_n$ meeting the conditions for the bound.

## 4.1 Minimal Ramification Conditions

Since $T = N(\overline{\rho})$ is squarefree, we may assume that by Fact 2.14 that for each $t|T$, $\overline{\rho}$ has either

$$\overline{\rho}|_{I_{\mathbf{Q}_t}} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \tag{4.1}$$

or

$$\overline{\rho}|_{I_{\mathbf{Q}_t}} \sim \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}. \tag{4.2}$$

Thus it suffices to define minimally ramified representations in these two cases. For convenience, we will also define a lifting at a prime $r$ at which $\overline{\rho}$ is unramified to be minimally ramified if $\rho$ is unramified.

In the case where $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.1), we will define $\rho$ lifting $\overline{\rho}$ to be minimally ramified if

$$\rho|_{I_{\mathbf{Q}_t}} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

In the case where $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.2), we will define $\rho$ lifting $\overline{\rho}$ to be minimally ramified if

$$\#\rho(I_{\mathbf{Q}_t}) = \#\overline{\rho}(I_{\mathbf{Q}_t}).$$

We prove that both of these are deformation conditions in the sense defined in Section 2.1.3.

**Proposition 4.1** ([Maz97, §29])**.** *Suppose that $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.1) and that $t \neq p$. Then the condition that $\rho$ be minimally ramified is a deformation condition.*

We begin by proving a lemma that we will use to simplify the statement of the condition.

**Lemma 4.2** ([Maz97, §29])**.** *Let $R$ be a complete noetherian local ring with residue field $k$, and let $V$ be a free $R$-module of rank 2. The following are equivalent.*

1. *The map $\eta : V \to V$ satisfies $(\eta - \mathbf{1}_2)^2 = 0$ and that $\eta$ does not descend to the identity in $V \otimes_R k$.*

2. *There is an $R$-basis of $V$ such that*

$$\eta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

*in this basis.*

*Proof.* The reverse implication is immediate, so we prove the forward implication. Define $\eta_0 = \eta - \mathbf{1}_2$. Then since $\eta_0^2 = 0$, we must have $\operatorname{im} \eta_0 \subseteq \operatorname{Ann}_{\eta_0}(V)$. In particular, we can decompose the map $\eta_0 : V \to V$ into the composition

$$V \to \eta_0(V) \hookrightarrow \operatorname{Ann}_{\eta_0}(V) \hookrightarrow V.$$

Since the composite map is nonzero upon tensoring with $k$, it factors through the inclusion $\mathrm{Ann}_{\eta_0}(V) \hookrightarrow V$, so there is some element $v_1 \in \mathrm{Ann}_{\eta_0}(V)$ with nontrivial residue modulo $k$. We use Nakayama's lemma to extend $v_1$ to the basis $\{v_1, v_2\}$. Then the map $\eta_0$ must take the form

$$\eta_0 = \begin{pmatrix} 0 & r_1 \\ 0 & r_2 \end{pmatrix}$$

in this basis. Moreover, since $\eta_0$ does not induce the 0 map on $V \otimes_R k$, one of $r_1, r_2$ must be invertible. Since $\eta_0^2 = 0$, we have $r_1 r_2 = 0$ and $r_2^2 = 0$, meaning that $r_1$ must be invertible and thus $r_2 = 0$. Replacing $x$ with $r_1 x$, we obtain

$$\eta_0 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

in this basis. Then $\eta_0 + \mathbf{1}_2 = \eta$ has the desired form. $\square$

*Proof of Proposition 4.1.* It is immediate from the definition that the property of being minimally ramified is preserved by changing $\rho$ within its strict equivalence class.

Suppose that $\rho : G_{\mathbf{Q}_t} \to \mathrm{GL}_2(R)$ is a minimally ramified lifting of $\overline{\rho}$. Observe that the subgroup of $\mathrm{GL}_2(R)$ of elements of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ is isomorphic to the additive group $R^+$ of $r$, which is a pro-$p$ group. Note that by Fact 2.2, the maximal pro-$p$ quotient of $I_{\mathbf{Q}_t}$ is $\mathbf{Z}_p$. In particular, any morphism $\rho : G_{\mathbf{Q}_t} \to \mathrm{GL}_2(R)$ for $t \neq R$ is determined by the image of a lift $\eta \in G_{\mathbf{Q}_t}$ of a generator of the quotient $\mathbf{Z}_p$. Moreover, $\eta$ must satisfy the conditions of Lemma 4.2, because if $\eta$ acts trivially on the residual vector space, then $\overline{\rho}$ was not ramified. By Lemma 4.1, we can choose a basis so that $\eta = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. It is then clear that projections of $\rho$ are minimal from the reverse implication of Lemma 4.2 and the observation that the image of $\eta$ under projection is, taking the image of the basis under $\eta$ for the basis of the image, also $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Given a diagram as in (2.1) and $\rho : G_{\mathbf{Q}_t} \to \mathrm{GL}_2(A \times_C B)$, suppose that the projections $\pi_{A*}\rho$ and $\pi_{B*}\rho$ are minimally ramified, and consider the matrix $\rho(\eta)$, where $\eta$ is chosen using Lemma 4.2 on $k$. Since the projections to $A$ and $B$ are minimally ramified, we have

$$(\pi_{A*}\rho(\eta) - \mathbf{1}_2)^2 = 0 \quad \text{and} \quad \pi_{B*}(\rho(\eta) - \mathbf{1}_2)^2 = 0.$$

Thus the equality holds for $A \times_C B$ as well. The residue of $\rho(\eta)$ in $\mathrm{GL}_2(k)$ is the same as that of its projections, so by Lemma 4.2, we find that $\rho$ is minimally ramified.

$\square$

**Proposition 4.3** ([Maz97, §29])**.** *Suppose that $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.2) and that $t \neq p$. Then the condition that $\rho$ be minimally ramified is a deformation condition.*

*Proof.* As in the proof of Proposition 4.1, it is immediate that being minimally ramified is preserved by changing $\rho$ within its strict equivalence class. Since projection cannot increase the size of $\rho(I_{\mathbf{Q}_t})$, minimal ramification is preserved under projection.

Given a diagram as in (2.1) and $\rho : G_{\mathbf{Q}_t} \to \mathrm{GL}_2(A \times_C B)$, suppose that the projections $\pi_{A*}\rho$ and $\pi_{B*}\rho$ are minimally ramified. It suffices to show that $\ker \rho = \ker \overline{\rho}$. But a matrix in $\mathrm{GL}_2(A \times_C B)$ is trivial if its projections are trivial, and $\ker \pi_{A*}\rho = \ker \pi_{B*}\rho = \ker \overline{\rho}$ by the minimal ramification condition, so $\ker \rho = \ker \overline{\rho}$.

$\square$

## 4.2 Unconstrained Deformation Rings

By Fact 2.6 and Propositions 4.1 and 4.3, there exists a ring $R_Q$ representing the functor $D_Q : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ defined by

$$D_Q : R \mapsto \left\{ \begin{array}{c|l} & \rho \text{ satisfies} \\ \text{strict equivalence classes of} & 1.\ \rho \text{ lifts } \overline{\rho} \\ \text{representations} & 2.\ \rho \text{ is minimally ramified at all primes} \\ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) & \qquad \ell \notin Q \cup \{p\} \\ & 3.\ \det \rho \equiv \psi \end{array} \right\}.$$

Note that while $G_{\mathbf{Q}}$ does not have the $p$-finiteness property, the restriction that $\rho$ be minimally ramified at $\ell \notin Q \cup \{p\}$ implies that the representation factors through the group $G_{\mathbf{Q},\{p\}\cup T \cup Q}$ – the Galois group of the maximal extension unramified outside $\{p\} \cup T \cup Q$ – which does has the $p$-finiteness property.

We may also define $R_Q^\square$ representing the framed version of this deformation problem. In particular, $R_Q^\square$ represents the functor $D_Q^\square : \mathbf{CLNRings}(k) \to \mathbf{Sets}$ defined by

$$D_Q^\square : R \mapsto \left\{ \begin{array}{c|l} \text{strict equivalence classes of} & \rho \text{ satisfies} \\ \text{pairs } (\rho, \alpha) \text{ where} & 1.\ \rho \text{ lifts } \overline{\rho} \\ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) \text{ is a} & 2.\ \rho \text{ is minimally ramified at all primes} \\ \text{representation and} & \qquad \ell \notin Q \cup \{p\} \\ \alpha \in \mathbf{1}_2 + \mathbf{M}_2(\mathfrak{m}_R) & 3.\ \det \rho \equiv \psi \end{array} \right\}.$$

We define $(\rho, \alpha)$ and $(\rho', \alpha')$ to belong to the same strict equivalence class if $\rho' = \beta\rho\beta^{-1}$ and $\alpha' = \beta\alpha$ for some $\beta \in \mathbf{1}_2 + \mathbf{M}_2(\mathfrak{m}_R)$. We assocate to the pair $(\rho, \alpha)$ the lifting $\alpha^{-1}\rho\alpha|_{G_{\mathbf{Q}_p}}$ of $\overline{\rho}$ to $G_{\mathbf{Q}_p}$. This association of a lifting to the strict equivalence class $(\rho, \alpha)$ allows us to regard the universal deformation ring $R_Q^\square$ as an $R_p^{\mathrm{loc}}$-algebra. We use the notation $[\rho, \alpha]$ to denote the strict equivalence class of framed deformations containing $(\rho, \alpha)$ as a member.

## 4.3 Deformation Rings with Constraints at $p$

We seek to solve the deformation problem $D_{Q,\mathrm{ord}} : \mathbf{DVR}(k) \to \mathbf{Sets}$ defined by

$$D_{Q,\mathrm{ord}} : R \mapsto \left\{ \begin{array}{c|l} & \rho \text{ satisfies} \\ \text{strict equivalence classes of} & 1.\ \rho \text{ lifts } \overline{\rho} \\ \text{representations} & 2.\ \rho \text{ is minimally ramified at all primes} \\ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) & \qquad \ell \notin Q \cup \{p\} \\ & 3.\ \det \rho \equiv \psi \\ & 4.\ \rho|_{G_{\mathbf{Q}_p}} \sim \left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right) \text{ with } \chi_1 \text{ unramified} \end{array} \right\},$$

where $\sim$ means that $\rho|_{G_{\mathbf{Q}_p}}$ can be conjugated by an element of $\mathrm{GL}_2(R)$ into the designated form. By Corollary 3.15, Fact 2.7, and the representability of $D_Q$, $D_{\mathrm{ord},Q}$ is representable by a ring $R_{\mathrm{ord},Q}$.

We finally seek to solve the deformation problem $D^{\square}_{\mathrm{ord},Q} : \mathbf{DVR}(k) \to \mathbf{Sets}$ defined by

$$D^{\square}_{Q,\mathrm{ord}} : R \mapsto \left\{ \begin{array}{c|l} & \rho \text{ satisfies} \\ \text{strict equivalence classes of} & 1.\ \rho \text{ lifts } \overline{\rho} \\ \text{pairs } (\rho, \alpha) \text{ where} & 2.\ \rho \text{ is minimally ramified at all primes} \\ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R) \text{ is a} & \qquad \ell \notin Q \cup \{p\} \\ \text{representation and} & 3.\ \det \rho \equiv \psi \\ \alpha \in \mathbf{1}_n + M_n(\mathfrak{m}_R) & 4.\ \rho|_{G_{\mathbf{Q}_p}} \sim \left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right) \text{ with } \chi_1 \text{ unramified} \end{array} \right\}.$$

While it follows from Corollary 3.15 that $D^{\square}_{Q,\mathrm{ord}}$ is representable by a ring $R^{\square}_{Q,\mathrm{ord}}$, one can construct the ring directly.

There is a natural map $R_p^{\mathrm{loc}} \to R_Q^{\square}$ given by restriction of $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ to $G_{\mathbf{Q}_p}$. We may then define the ring $R^{\square}_{Q,\mathrm{ord}} = R_Q^{\square} \widehat{\otimes}_{R_p^{\mathrm{loc}}} R^{\mathrm{loc}}_{p,\mathrm{ord}}$.

**Proposition 4.4.** *The ring $R^{\square}_{Q,\mathrm{ord}}$ represents the functor $D^{\square}_{Q,\mathrm{ord}}$.*

*Proof.* The completed tensor product fits into a diagram

$$\begin{tikzcd} & R_p^{\square} \arrow[dl] \arrow[dr] & \\ R_Q^{\square} \arrow[dr] & & R^{\mathrm{loc}}_{p,\mathrm{ord}} \arrow[dl] \\ & R_Q^{\square} \widehat{\otimes}_{R_p^{\square}} R^{\mathrm{loc}}_{p,\mathrm{ord}} & \end{tikzcd}$$

that satisfies the univeral property for a Cartesian square. In particular, a map from $R_Q^{\square} \widehat{\otimes}_{R_p^{\square}} R^{\mathrm{loc}}_{p,\mathrm{ord}}$ is in natural correspondence with a pair of maps from $R_Q^{\square}$ and $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ agreeing on $R_p^{\mathrm{loc}}$. But such data specifies exactly an extension of an ordinary representation

$\rho_0 : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$ to a global representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ satisfying the constraints of the deformation problem $D_Q^{\square}$. Conversely, a global representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ satisfying the constraints of $D_{Q,\mathrm{ord}}^{\square}$ yields by restriction the ordinary representation $\rho|_{G_{\mathbf{Q}_p}} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(R)$, so by the universal properties of the rings $R_{p,\mathrm{ord}}^{\mathrm{loc}}$ and $R_Q^{\square}$, the data of this pair of agreeing maps and thus a map from $R_{Q,\mathrm{ord}}^{\square} = R_Q^{\square} \widehat{\otimes}_{R_p^{\mathrm{loc}}} R_{p,\mathrm{ord}}^{\mathrm{loc}}$ exists and is unique.

□

## 4.4 Selmer Groups

In Section 2.1.3, we stated that certain kinds of subfunctors – those defining local deformation conditions – were relatively representable. We defined a global Galois deformation problem for $G_{\mathbf{Q}}$ to be a collection of local deformation problems for each place of $\mathbf{Q}$. In this section, we describe an algebraic analogue of a global deformation problem. Since we will be considering both archimedean and nonarchimedean places simultaneously, we use the notation $G_v$ and $I_v$ for the local absolute Galois group and its inertia subgroup, respectively.

To any deformation problem $D$, one can associate the tangent space $D(k[\delta])$, which is isomorphic to the tangent space of the ring $R$ representing $D$. In this manner, given a family of local deformation problems, one might consider trying to relate the local tangent spaces to the global tangent space. Observe that a local deformation condition defines a subspace of the unrestricted local deformation problem, and similarly for the global case. In an algebraic manner, one can define a deformation condition by specifying these subspaces.

Let $M$ be a finite, discrete, and continuous $G_{\mathbf{Q}}$-module. For example, one might use $M \cong k^2$ with $G_{\mathbf{Q}}$ acting via $\overline{\rho}$. One can define the local deformation conditions by choosing for each place $v$ a subgroup $L_v$ of the tangent space $H^1(G_v, M)$ of the full local deformation functor. To the data $\mathfrak{L} = \{L_v\}$, one can *algebraically* define the global Selmer group $H^1_{\mathfrak{L}}(G_{\mathbf{Q}}, M)$ by

$$H^1_{\mathfrak{L}}(G_{\mathbf{Q}}, M) = \left\{\xi \in H^1(G_{\mathbf{Q}}, M) | \operatorname{Res}_v(\xi) \in L_v \text{ for all places } v\right\},$$

where $\operatorname{Res}_v : H^1(G_{\mathbf{Q}}, M) \to H^1(G_v, M)$ is the restriction homomorphism.

Many key properties of the deformation rings $R_Q$ and $R_Q^{\square}$ can be derived through understanding of these Selmer groups. Unfortunately, the Selmer groups only provide an *upper bound* for the Krull dimension of these rings, so at places where the deformation problem is obstructed, one needs to handle the analysis specially. In our case, the only such place will be $p$. Following Clozel, Harris, and Taylor [CHT08], one may construct a variation on the cochain defining the Selmer groups as follows.

**Definition 4.** Let $\mathfrak{L} = \{L_v\}$ be a set of local conditions, and let $Q$ be the set of places other than $p$ where $L_v \neq H^1(G_v/I_v, \operatorname{ad}\overline{\rho}^{I_v})$. We define $H^i_{\mathfrak{L},p}(G_{\mathbf{Q}}, M)$ to be the cohomology of the cochain complex defined by

$$\begin{aligned}
C^0_{\mathfrak{L},p} &= C^0(G_{\mathbf{Q}}, M)\\
C^1_{\mathfrak{L},p} &= C^1(G_{\mathbf{Q}}, M) \oplus C^0(G_{\mathbf{Q}_p}, M)\\
C^2_{\mathfrak{L},p} &= C^2(G_{\mathbf{Q}}, M) \oplus C^1(G_{\mathbf{Q}_p}, M) \oplus \bigoplus_{q\in Q\cup\{p\}} C^1(G_q, M)/\widetilde{L}_q\\
C^i_{\mathfrak{L},p} &= C^i(G_{\mathbf{Q}}, M) \oplus \bigoplus_{q\in Q\cup\{p\}} C^{i-1}(G_q, M) \text{ for } i \geq 3
\end{aligned}$$

with the boundary map

$$\left(\xi, \eta_p, \{\nu_q\}_{q\in Q}\right) \mapsto (\partial\xi, \xi|_{G_{\mathbf{Q}_p}} - \partial\eta_p, \left\{\xi|_{G_{\mathbf{Q}_q}} - \partial\eta_q\right\}_{q\in Q}\Big)$$

and where $\widetilde{L}_q$ is the preimage of $L_q$ in $C^1(G_q, M)$.

We will be interested only in $H^1_{\mathfrak{L},p}(G_{\mathbf{Q}}, M)$, which can be defined as

$$\begin{aligned}
H^1_{\mathfrak{L},p}(G_{\mathbf{Q}}, M) &= \frac{Z^1_{\mathfrak{L},p}(G_{\mathbf{Q}}, M)}{B^1_{\mathfrak{L},p}(G_{\mathbf{Q}}, M)}\\
&= \frac{\left\{(\xi, \eta_p) \in Z^1(G_{\mathbf{Q}}, M) \oplus C^0(G_{\mathbf{Q}_p}, M) : \mathrm{Res}_p(\xi) = \partial\eta_p, \mathrm{Res}_q(\xi) \in \widetilde{L}_q \text{ for all } q \in Q\right\}}{\left\{(\partial\xi, \xi|_{G_{\mathbf{Q}_p}})\right\}_{\xi\in C^0(G_{\mathbf{Q}},M)}}.
\end{aligned} \tag{4.3}$$

We will be able to bound the size of $R^\square_Q$ via a careful study of Selmer groups.

In order to apply the results on Selmer groups to the remaining places, we first observe that $R^\square_Q$ is an algebra over $R^{\mathrm{loc}}_{p,\mathrm{ord}}$, so we may think of this local deformation ring as if it were a coefficient ring for our representation. With this in mind, we define the tangent space

$$t^\square_Q = \mathrm{Hom}_k(\mathfrak{m}_{R^\square_Q}/(\mathfrak{m}^2_{R^\square_Q}, \pi, \mathfrak{m}_{R^{\mathrm{loc}}_{p,\mathrm{ord}}}), k),$$

where $\pi$ is a uniformizer for $W(k)$, and we write the subscript $k$ to emphasize that these are $k$-vector space homomorphisms. Then $\dim_k t^\square_Q + \dim R^{\mathrm{loc}}_{p,\mathrm{ord}}$ is an upper bound for the Krull dimension of the ring $R^\square_Q$.

We will construct a deformation problem $\mathfrak{L}_Q = \{L_{v,Q}\}$ in order to measure $\dim_k t^\square_Q$ in terms of a Selmer group. Specifically, we set

$$L_{v,Q} = \begin{cases} H^1(G_v/I_v, \mathrm{ad}^0\,\overline{\rho}^{I_v}) & \text{if } v \notin Q \cup \{p\}\\ H^1(G_v, \mathrm{ad}^0\,\overline{\rho}) & \text{if } v \in Q \cup \{p\}\,. \end{cases} \tag{4.4}$$

With this definition, we may connect the tangent space to $H^1_{\mathfrak{L}_Q,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho})$.

The proof of the following Proposition 4.5 is no more than a long definition chase, but it illustrates three key ideas:

- There are many equivalent ways of writing down $t_Q^\square$.

- The proof of Subclaim 4.8 shows that the Selmer group restriction corresponding to the requirement of minimal ramification is identical to the restriction that forces a residually unramified representation to have an unramified lifting.

- The proof of Claims 4.7 and 4.7 illustrate that the notions of deformation and of framed deformation are perfectly compatible with the Selmer cohomology group definition. In view of the results of Section 4.5 showing that the Selmer cohomology group satisfies elegant duality relations, the definition of the framed deformation should hopefully appear less artificial.

**Proposition 4.5** ([CHT08, Proposition 2.2.9])**.** *We have a canonical isomorphism*

$$t_Q^\square \cong H^1_{\mathfrak{L}_Q,p}(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}).$$

*Proof.* We begin by identifying $t_Q^\square$ with a space of deformations of $\rho$.

**Claim 4.6.** *The space $t_Q^\square$ may be canonically identified with the subspace of framed deformations $[\rho, \alpha] \in D_Q^\square(k[\delta]/\delta^2)$ such that $\alpha^{-1}\rho\alpha|_{G_{\mathbf{Q}_p}}$ is the trivial lifting.*

*Proof.* Given a complete noetherian local ring $R$ with $W(k)$-algebra structure given by $\phi_R : W(k) \to R$ and an ideal $\mathfrak{a} \subseteq \mathfrak{m}_R$, we first show that there is an isomorphism

$$\operatorname{Hom}_k(\mathfrak{m}_R/(\mathfrak{m}_R^2, \pi, \mathfrak{a}), k) \cong \operatorname{Hom}_{W(k)}(R/\mathfrak{a}, k[\delta]/\delta^2).$$

First note that in a morphism $R/\mathfrak{a} \to k[\delta]/\delta^2$, any element of $\mathfrak{m}_R^2$ must map to $\delta^2 = 0$ in $k[\delta]/\delta^2$, while $\pi$ must map to 0 to respect the $W(k)$-algebra structure. Thus, we have a bijection

$$\operatorname{Hom}_k(R/(\mathfrak{m}_R^2, \pi, \mathfrak{a}), k) \to \operatorname{Hom}_{W(k)}(R/\mathfrak{a}, k[\delta]/\delta^2)$$

sending a map $\psi$ to itself. Next observe that since $R/(\mathfrak{m}_R^2, \pi, \mathfrak{a}) \cong k \oplus \mathfrak{m}_R/(\mathfrak{m}_R^2, \pi, \mathfrak{a})$, and the image of $k$ is forced by the $k$-algebra structure, a map in $\operatorname{Hom}_k(R/(\mathfrak{m}_R^2, \pi, \mathfrak{a}), k)$ is determined by its restriction to $\mathfrak{m}_R/(\mathfrak{m}_R^2, \pi, \mathfrak{a})$.

In particular,

$$\operatorname{Hom}_k(\mathfrak{m}_{R_Q^\square}/(\mathfrak{m}^2_{R_Q^\square}, \pi, \mathfrak{m}_{R^{\mathrm{loc}}_{p,\mathrm{ord}}}), k) \cong \operatorname{Hom}_{W(k)}(R_Q^\square/\mathfrak{m}_{R^{\mathrm{loc}}_{p,\mathrm{ord}}}, k[\delta]/\delta^2).$$

A map in $\operatorname{Hom}_{W(k)}(R_Q^\square, k[\delta]/\delta^2)$ is simply an element of $D_Q^\square(k[\delta]/\delta^2)$. Note that $R_Q^\square/\mathfrak{m}_{R^{\mathrm{loc}}_{p,\mathrm{ord}}} \cong R_Q^\square/\mathfrak{m}_{R_p^{\mathrm{loc}}}$, where $\mathfrak{m}_{R_p^{\mathrm{loc}}}$ is defined by the pushforward of the natural map $R_p^{\mathrm{loc}} \to R_Q^\square$. Then the composite map $R_p^{\mathrm{loc}} \to R_Q^\square/\mathfrak{m}_{R^{\mathrm{loc}}_{p,\mathrm{ord}}} \to k[\delta]/\delta^2$ is the quotient by $\mathfrak{m}_{R_p^{\mathrm{loc}}}$, so by the explicit bijection in Proposition 3.4, the lift $\alpha^{-1}\rho\alpha|_{G_{\mathbf{Q}_p}}$ is trivial (meaning equal to $\overline{\rho}|_{G_{\mathbf{Q}_p}}$).

$\square$

*Remark* 5. Mazur [Maz97] shows that one can also induce a natural $k$-vector space structure on $D_Q^\square(k[\delta]/\delta^2)$ that matches that of $t_Q^\square$ – this is not necessary for our purposes.

We next characterize a lifting of the form described in Claim 4.6 in terms of a cocycle.

**Claim 4.7.** *The space of framed liftings $(\rho, \alpha) \in D_Q^{\square}(k[\delta]/\delta^2)$ such that $\rho|_{G_{\mathbf{Q}_p}}$ is the trivial lifting may be canonically identified with $Z^1_{\mathfrak{L},p}(G_{\mathbf{Q}_p}, \mathrm{ad}^0 \overline{\rho})$.*

*Proof.* We follow closely an argument of Mazur [Maz97, Proposition 1, §21]. Observe that there exists a short exact sequence

$$0 \to \mathbf{1}_2 + \delta \,\mathrm{ad}\,\overline{\rho} \to \mathrm{GL}_2(k[\delta]/\delta^2) \to \mathrm{GL}_2(k) \to 0,$$

forgetting for now the $G_{\mathbf{Q}}$-action on $\mathrm{ad}\,\overline{\rho}$. We may replace the multiplicative group $\mathbf{1} + \delta \,\mathrm{ad}\,\overline{\rho}$ by the additive group $\mathrm{ad}\,\overline{\rho}$. The inclusion $\mathrm{GL}_2(k) \hookrightarrow \mathrm{GL}_2(k[\delta]/\delta^2)$ provides a splitting, so that

$$\mathrm{GL}_2(k[\delta]/\delta^2) \cong \mathrm{ad}\,\overline{\rho} \rtimes \mathrm{GL}_2(k)$$

via the conjugation action.

A framed lifting $(\rho, \alpha)$ of $\overline{\rho}$ is simply a morphism

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(k[\delta]/\delta^2) \cong \mathrm{ad}\,\overline{\rho} \rtimes \mathrm{GL}_2(k) \to \mathrm{GL}_2(k)$$

with composition $\overline{\rho}$. An example of such a morphism is the trivial lift $\rho_0$ of $\overline{\rho}$. For any other $\rho$ with this property, define $\xi_\rho \in \mathrm{ad}\,\overline{\rho}$ by $\rho = (1 + \xi_\rho)\rho_0$. We have $\xi_\rho \in Z^1(G_{\mathbf{Q}_p}, \mathrm{ad}\,\overline{\rho})$, since for $g, h \in G_{\mathbf{Q}}$ we have

$$\begin{aligned}
(1 + \xi_\rho(gh))\rho_0(gh) &= (1 + \xi_\rho(g))\rho_0(g)(1 + \xi_\rho(h))\rho_0(h) \\
\rho_0(gh) + \delta\xi_p(gh)\rho_0(gh) &= \rho_0(gh) + \delta(\xi_\rho(g)\rho_0(gh) + \rho_0(g)\xi_p(h)\rho_0(h)) \\
\xi_p(gh) &= \xi_p(g) + \rho_0(g)\xi_p(h)\rho_0(g)^{-1}.
\end{aligned}$$

Note, moreover, that for $m \in \mathrm{ad}\,\overline{\rho}$, $\det(\mathbf{1}_2 + \delta m) = 1 + \delta \,\mathrm{Tr}\, m$, so $\det \rho = \det \rho_0$ exactly when $\mathrm{Tr}(\xi_\rho) = 0$. The determinant condition then implies that $\xi_\rho$ lies in $Z^1(G_{\mathbf{Q}_p}, \mathrm{ad}^0 \overline{\rho})$.

By (4.3), at primes away from $pT$, it is tautological that $\rho$ meets the deformation conditions exactly when $\mathrm{Res}_q \xi_\rho \in \widetilde{L}_{q,Q}$. We have to check, however, that the notion of being minimally ramified at $t|T$ corresponds to the Selmer group conditions in (4.4).

**Subclaim 4.8.** *The restriction of a cocycle $\xi_\rho$ associated to a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(k[\delta]/\delta^2)$ to $G_{\mathbf{Q}_t}$ is an element of $H^1_{\mathfrak{L}_Q,p}(G_{\mathbf{F}_t}, \mathrm{ad}^0 \overline{\rho}^{I_{\mathbf{Q}_t}})$ if and only if $\rho$ is minimally ramified at $t$.*

*Proof.* Suppose that $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.1). By Lemma 4.2, we choose $\eta \in I_{\mathbf{Q}_t}$ such that $\overline{\rho}(\eta)$ and thus $\rho_0(\eta)$ has the form $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Suppose that $\rho$ is minimally ramified. By Lemma 4.2, we may suppose that $\rho(\eta) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) + \delta \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{M}_2(k)$ where $(\rho(\eta) - \mathbf{1}_2)^2 = 0$. Observe that

$$(\rho(\eta) - \mathbf{1}_2)^2 = \begin{pmatrix} a\delta & 1 + b\delta \\ c\delta & d\delta \end{pmatrix}^2 = \begin{pmatrix} c\delta & (a+d)\delta \\ 0 & c\delta \end{pmatrix},$$

which implies that $c=0$ and $a=-d$, so that $\rho(\eta)=\left(\begin{smallmatrix}1+a\delta & 1+b\delta\\ 0 & 1-a\delta\end{smallmatrix}\right)$. But

$$\begin{pmatrix}1+b\delta & 0\\ -a\delta & 1\end{pmatrix}\begin{pmatrix}1+a\delta & 1+b\delta\\ 0 & 1-a\delta\end{pmatrix}\begin{pmatrix}1+b\delta & 0\\ -a\delta & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$

so $\rho|_{I_{\mathbf{Q}_t}}$ is in the same strict equivalence class as $\rho_0|_{I_{\mathbf{Q}_t}}$. Conversely, if $\rho|_{I_{\mathbf{Q}_t}}$ is in the same strict equivalence class as $\rho_0|_{I_{\mathbf{Q}_t}}$, then $\rho$ is certainly minimally ramified by definition. We lastly need to know that changing the strict equivalence class of $\rho$ changes $\xi_\rho$ by a coboundary. This is proved in Claim 4.9.

Suppose that $\overline{\rho}|_{I_{\mathbf{Q}_t}}$ has the form in (4.2) and $\rho$ is a minimally ramified lifting. The quotient $G_{\mathbf{Q}_t}/\ker\overline{\rho}$ is cyclic, so choose a lift $\eta$ of the generator. We can write $\rho(\eta)=\left(\begin{smallmatrix}1 & 0\\ 0 & \alpha\end{smallmatrix}\right)+\delta\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ where $1\neq\alpha\in k$ and $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\mathbf{M}_2(k)$. We can use the change of basis

$$\begin{aligned}&\begin{pmatrix}1 & b(\alpha-1)^{-1}\delta\\ c(1-\alpha)^{-1}\delta & 1\end{pmatrix}^{-1}\begin{pmatrix}1+a\delta & b\delta\\ c\delta & \alpha+d\delta\end{pmatrix}\begin{pmatrix}1 & b(\alpha-1)^{-1}\delta\\ c(1-\alpha)^{-1}\delta & 1\end{pmatrix}\\ &=\begin{pmatrix}1+a\delta & 0\\ 0 & \alpha+d\delta\end{pmatrix}\end{aligned}$$

to write $\rho(\eta)$ in diagonal form. Note that $\#(G_{\mathbf{Q}_t}/\ker\overline{\rho})|p-1$, so we must have

$$\begin{aligned}\begin{pmatrix}1+a\delta & 0\\ 0 & \alpha+d\delta\end{pmatrix}^{p-1}&=\begin{pmatrix}1+(p-1)a\delta & 0\\ 0 & \alpha^{p-1}+(p-1)\alpha^{p-2}d\delta\end{pmatrix}\\ &=\begin{pmatrix}1+(p-1)a\delta & 0\\ 0 & 1+(p-1)\alpha^{p-2}d\delta\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{aligned}$$

and thus $a=d=0$. In particular, the cocycle $\xi_\rho$ has trivial restriction to $I_{\mathbf{Q}_t}$ and thus lies in $H^1_{\mathfrak{L}_Q,p}(G_{\mathbf{F}_t},\mathrm{ad}^0\overline{\rho}^{I_{\mathbf{Q}_t}})$.

Conversely, if $\xi_\rho$ lies in $H^1_{\mathfrak{L}_Q,p}(G_{\mathbf{F}_t},\mathrm{ad}^0\overline{\rho}^{I_{\mathbf{Q}_t}})$, it is trivial on $I_{\mathbf{Q}_t}$, and thus $\rho|_{I_{\mathbf{Q}_t}}=\rho_0|_{I_{\mathbf{Q}_t}}$. But $\rho_0$ is the trivial lifting of $\overline{\rho}$ and thus minimally ramified.

□

Finally, writing $\alpha=1-\delta a$, the triviality of $\mathrm{Res}_p\,\alpha^{-1}\rho\alpha$ means that

$$(1+\delta a)(1+\delta\xi_\rho)\rho_0|_{G_{\mathbf{Q}_p}}(1-\delta a)=\rho_0|_{G_{\mathbf{Q}_p}}.$$

Rearranging (and suppressing the restriction to $G_{\mathbf{Q}_p}$), this implies

$$(1+\delta(a+\xi_\rho))(\rho_0+\delta\rho_0 a)=(\rho_0+\delta(a\rho_0+\xi_\rho\rho_0-\rho_0 a))=\rho_0$$

and thus $\xi_\rho=\rho a\rho^{-1}-a$, which is exactly the statement that $\xi_\rho=\partial a$. Thus $(\xi_\rho,a)\in Z^1_{\mathfrak{L},p}(G_{\mathbf{Q}_p},\mathrm{ad}^0\overline{\rho})$, and conversely.

□

To finish the proof, we need only check that the equivalence relation corresponds to the space of coboundaries.

**Claim 4.9.** *Two framed liftings $(\rho, \alpha)$ and $(\rho', \alpha')$ are equivalent exactly when they differ by an element of $B^1_{\mathfrak{L},p}(G_{\mathbf{Q}_p}, \mathrm{ad}^0 \overline{\rho})$.*

*Proof.* Using the definitions of Claim 4.7, one needs $\beta = \mathbf{1}_2 + \delta b$ such that $\rho' = \beta\rho\beta^{-1}$ and $\alpha' = \beta\alpha$. Thus $\xi_{\rho'} = \xi_\rho + b - \rho_0 b \rho_0$ and $m' = m + b$ by a computation identical to that in Claim 4.7.

□

□

## 4.5 Arithmetic Duality Theorems

In this section we state without proof some cohomological results from [Mil06] and [CHT08]. These result come from the world of arithmetic duality. For $G_{\mathbf{Q}}$-modules, we define the $G_{\mathbf{Q}}$-module $\mathrm{Hom}(M, N)$ via the map $\psi \overset{g}{\mapsto} g \circ \psi \circ g^{-1}$ for all $g \in G_{\mathbf{Q}_p}$. For a finite $G_{\mathbf{Q}}$-module $M$, we define its dual

$$M^* = \mathrm{Hom}(M, \mu_n(\overline{\mathbf{Q}})),$$

where $\mu_n(\overline{\mathbf{Q}})$ is the subgroup of $n^{\text{th}}$ roots of unity $\overline{\mathbf{Q}}$ with induced $G_{\mathbf{Q}}$-action and $nM = 0$.

There are a number of results of Tate relating modules to their duals.

**Fact 4.10** ([Mil06, §1.2])**.** *Let $v$ be a place of $\mathbf{Q}$ and let $M$ be a finite $G_{\mathbf{Q}}$-module. Then*

1. *The group $H^r(G_v, M)$ is finite for all $r$.*
2. *If $v \nmid \infty$, then $H^r(G_v, M) = 0$ for $r > 2$, and we have the local Euler characteristic formula*
$$\chi(G_v, M) = \frac{\#H^0(G_v, M)\#H^2(G_v, M)}{\#H^1(G_v, M)} = \#(M \otimes \mathbf{Z}_v)^{-1}.$$
3. *If $v \nmid \infty$, there is a perfect pairing*
$$H^i(G_v, M) \times H^{2-i}(G_v, M^*) \to H^2(G_v, \mu_n(\overline{\mathbf{Q}})).$$

We would like a second interpretation of the notion of duality in the case of $\mathrm{ad}^0 \overline{\rho}$ to aid in the explicit computation of its cohomology. The cyclotomic character $\epsilon : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ gives rise to the $G_{\mathbf{Q}}$-module $\mathbf{Z}_p(1)$, which as an abelian group is isomorphic to $\mathbf{Z}_p$, but has an action of $G_{\mathbf{Q}}$-multiplication via $\epsilon$. Given a finite module $M$, one defines its twist $M(1)$ by the formula $M(1) = M \otimes \mathbf{Z}_p(1)$. We can relate the twist $\mathrm{ad}^0 \overline{\rho}(1)$ to the dual $(\mathrm{ad}^0 \overline{\rho})^*$.

**Proposition 4.11.** *We have the isomorphism* $\mathrm{ad}^0 \overline{\rho}(1) \cong (\mathrm{ad}^0 \overline{\rho})^*$.

*Proof.* Consider the perfect pairing

$$\mathrm{ad}^0\,\overline{\rho} \times \mathrm{ad}^0\,\overline{\rho}(1) \to k(1)$$

sending $(x, y) \mapsto \mathrm{Tr}(xy)$. Note that for $g \in G_{\mathbf{Q}}$,

$$(x^g, y^g) \mapsto \mathrm{Tr}(gxg^{-1}\epsilon(g)gyg^{-1}) = \epsilon(g)\,\mathrm{Tr}(xy),$$

so the pairing is $G_{\mathbf{Q}}$-equivariant. Thus we have the isomorphism

$$\mathrm{ad}^0\,\overline{\rho}(1) \cong \mathrm{Hom}_k(\mathrm{ad}^0\,\overline{\rho}, k)(1).$$

Observe that

$$\mathrm{Hom}_k(\mathrm{ad}^0\,\overline{\rho}, k)(1) \cong \mathrm{Hom}_{\mathbf{F}_p}(\mathrm{ad}^0\,\overline{\rho}, \mathbf{F}_p)(1),$$

where the isomorphism sends $\psi \mapsto \mathrm{Tr}_{k/\mathbf{F}_p} \circ \psi$. But since $\mathbf{F}_p(1) \cong \mu_p(\overline{\mathbf{Q}})$, we have

$$\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{ad}^0\,\overline{\rho}, \mathbf{F}_p)(1) \cong (\mathrm{ad}^0\,\overline{\rho})^*,$$

as desired. □

The main result in arithmetic duality that we will need is a result of Wiles [Wil95]. Since we are using Selmer groups for framed deformations, we will use a slightly modified form of the result.

**Fact 4.12** ([CHT08, Lemma 2.3.4]). *Let $\mathfrak{L}$ be a set of conditions that is unramified outside a finite set. We have the equality*

$$\begin{aligned}\dim_k H^1_{\mathfrak{L},p}(G_{\mathbf{Q}_p}, \mathrm{ad}^0\,\overline{\rho}) = {} & \dim_k H^0(G_{\mathbf{Q}_p}, \mathrm{ad}^0\,\overline{\rho}) - \dim_k H^0(G_{\mathbf{Q}_p}, \mathrm{ad}^0\,\overline{\rho}(1)) \\ & + \dim_k H^1_{\mathfrak{L}^\perp,p}(G_{\mathbf{Q}_p}, \mathrm{ad}^0\,\overline{\rho}(1)) + \sum_{v \neq p}(\dim_k L_v - \dim_k H^0(G_v, \mathrm{ad}^0\,\overline{\rho})),\end{aligned}$$

*where*

$$H^1_{\mathfrak{L}^\perp,p}(G_{\mathbf{Q}_p}, \mathrm{ad}^0\,\overline{\rho}(1)) = \ker\left(H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) \to \bigoplus_{v \neq p} H^1(G_v, \mathrm{ad}^0\,\overline{\rho}(1))/L_v^\perp\right)$$

*and $L_v^\perp$ is the annihilator of $L_v$ under the pairing*

$$H^1(G_v, \mathrm{ad}^0\,\overline{\rho}) \times H^1(G_v, \mathrm{ad}^0\,\overline{\rho}(1)) \to k(1).$$

We remark that the primary ingredient of the proof of Fact 4.12 is an application of the Poitou-Tate exact sequence.

## 4.6 Computations of Local and Global Galois Cohomology Groups

In this section, we apply Fact 4.12 to compute $\dim_k H^1_{\mathfrak{L}_Q,p}$, where $\mathfrak{L}_Q$ is the set of conditions defined in (4.4).

**Proposition 4.13.** *We have* $\dim_k H^0(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}) = 0$ *and* $\dim_k H^0(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}(1)) = 0$.

*Proof.* An element of $\operatorname{ad}^0 \overline{\rho}^{G_{\mathbf{Q}}}$ is a $G_{\mathbf{Q}}$-equivariant homomorphism $M_{\overline{\rho}} \to M_{\overline{\rho}}$, which must be scalar multiplication by Schur's lemma. But $\operatorname{ad}^0 \overline{\rho}$ consists only of traceless matrices, so in fact we must have $\dim_k H^0(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}) = 0$.

Similarly, a nonzero element of $(\operatorname{ad}^0 \overline{\rho}(1))^{G_{\mathbf{Q}}}$ is a $G_{\mathbf{Q}}$-equivariant homomorphism $M_{\overline{\rho}} \to M_{\overline{\rho}(1)}$, which implies that $M_{\overline{\rho}} \cong M_{\overline{\rho}(1)}$ by Schur's lemma. Thus $\det \overline{\rho} = \det \overline{\rho} \cdot \epsilon^2$, so every element of $k$ must square to 1. This implies that $p = 3$, which we excluded.

□

**Proposition 4.14** ([DDT97, Pg. 61])**.** *Let $\mathfrak{L}$ be any set of local conditions for a finite $G_{\mathbf{Q}}$-module $M$. For nonarchimedean places $v$ such that $L_v = H^1(G_v/I_v, M^{I_v})$,*

$$\dim_k L_v = \dim_k H^0(G_v, \operatorname{ad}^0 \overline{\rho}).$$

*Proof.* Let $\operatorname{Frob}_v$ be a choice of Frobenius element in $G_v$. Then

$$0 \to H^0(G_v, M) \to M^{I_v} \stackrel{\operatorname{Frob}_v - 1}{\to} M^{I_v} \to H^1(G_v/I_v, M^{I_v}) \to 0,$$

is exact, where the first map is the inclusion $M^{G_v} \hookrightarrow M^{I_v}$ and the third is the map $m \mapsto \psi_m$, where $\psi_m(\operatorname{Frob}_v) = m$. Since the middle terms have the same order, $\dim_k H^0(G_v, M) = H^1(G_v/I_v, M^{I_v})$.

□

**Proposition 4.15.** *Let $v = \infty$ denote the real infinite place of $\mathbf{Q}$. Then* $\dim_k L_\infty = 0$ *and* $\dim_k H^0(G_\infty, \operatorname{ad}^0 \overline{\rho}) = 1$.

*Proof.* The first statement can be verified explicitly as follows. The kernel of the map $\operatorname{ad}^0 \overline{\rho} \twoheadrightarrow B^1(G_\infty, \operatorname{ad}^0 \overline{\rho})$ defined by $m \mapsto (\sigma \mapsto \sigma \cdot m - m)$ is the 1-dimensional subspace of diagonal matrices, so $\dim_k B^1(G_\infty, \operatorname{ad}^0 \overline{\rho}) = 2$. Setting $G_\infty = \{1, c\}$, note that a cocycle $\psi$ sends 1 to 0, and that $\psi(c \cdot c) = 0 = c \cdot \psi(c) + \psi(c)$, so that $\psi(c)$ lies in the $-1$ eigenspace, which has dimension 2. Thus $2 = \dim_k Z^1(G_\infty, \operatorname{ad}^0 \overline{\rho})$ and the result follows.

The second statement is immediate since $\overline{\rho}$ is odd. □

**Proposition 4.16.** *For $q \in Q$, we have*

$$\dim_k L_{Q,q} - \dim_k H^0(G_{\mathbf{Q}_q}, \operatorname{ad}^0 \overline{\rho}) = \dim_k H^0(G_{\mathbf{Q}_q}, \operatorname{ad}^0 \overline{\rho}(1))$$

*Proof.* By the local Euler characteristic formula (Fact 4.10),

$$\begin{aligned}\dim_k L_{Q,q} - \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}) &= \dim_k H^1(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}) - \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}) \\ &= \dim_k H^2(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}),\end{aligned}$$

since $\mathrm{ad}^0\,\overline{\rho} \otimes \mathbf{Z}_q = 0$. Since by Fact 4.10 and Proposition 4.11, there is a perfect pairing

$$H^2(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}) \times H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}(1)) \to H^2(G_{\mathbf{Q}_q}, \mu_n(\overline{\mathbf{Q}})),$$

we must have $\dim_k H^2(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}) = \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}(1))$. □

Combining Propositions 4.13, 4.14, 4.15, and 4.16 with Fact 4.12 and Proposition 4.5, we can bound the size of $R^{\square}_{Q,\mathrm{ord}}$.

**Corollary 4.17.** *The ring $R^{\square}_{Q,\mathrm{ord}}$ has tangent space dimension as an $R^{\mathrm{loc}}_{p,\mathrm{ord}}$-algebra given by the formula*

$$\dim_k t^{\square}_Q = \dim_k H^1_{\mathfrak{L}^{\perp}_Q,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) + \sum_{q\in Q} \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}(1)) - 1.$$

From Proposition 3.8, we find the following result.

**Corollary 4.18.** *The ring $R^{\square}_{Q,\mathrm{ord}}$ satisfies the bound*

$$\dim R^{\square}_{Q,\mathrm{ord}} \leq \dim_k H^1_{\mathfrak{L}^{\perp}_Q,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) + \sum_{q\in Q} \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}(1)) + 4.$$

We finally relate $\dim R^{\square}_{Q,\mathrm{ord}}$ to $\dim R_{Q,\mathrm{ord}}$, since the latter will be important in Section 6.

**Proposition 4.19.** *The choice of a member $\rho_{Q,\mathrm{ord}}$ of the equivalence class of the universal deformation $[\rho_{Q,\mathrm{ord}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(R_{Q,\mathrm{ord}})]$ induces an isomorphism*

$$R_{Q,\mathrm{ord}}[[c_1, c_2, c_3]] \to R^{\square}_{Q,\mathrm{ord}}.$$

*Proof.* By Schur's lemma, since $\overline{\rho}$ is irreducible, the module of elements of the form $\mathbf{1}_2 + \left(\begin{smallmatrix} c_1 & c_2 \\ c_3 & 0 \end{smallmatrix}\right)$ acts faithfully on liftings of $[\rho_{Q,\mathrm{ord}}]$ by conjugation. Conversely, conjugating a lifting within its strict equivalence class, which corresponds to conjugation by a matrix of the form $\left(\begin{smallmatrix} 1+c_1' & c_2' \\ c_3' & 1+c_4' \end{smallmatrix}\right)$, is equivalent to conjugation by $\left(\begin{smallmatrix} (1+c_1')(1+c_4')^{-1} & c_2'(1+c_4')^{-1} \\ c_3'(1+c_4')^{-1} & 1 \end{smallmatrix}\right)$. Thus, the pair $(\rho_{Q,\mathrm{ord}}, \mathbf{1}_2 + \left(\begin{smallmatrix} 1+c_1 & c_2 \\ c_3 & 1 \end{smallmatrix}\right))$ is a univeral framed deformation of $\overline{\rho}$, so the rings $R_{Q,\mathrm{ord}}[[c_1, c_2, c_3]]$ and $R^{\square}_{Q,\mathrm{ord}}$ are isomorphic.

□

Combining Proposition 4.19 with Corollary 4.18, we obtain the following.

**Corollary 4.20.** *The ring $R_{Q,\mathrm{ord}}$ satisfies the bound*

$$\dim R_{Q,\mathrm{ord}} \leq \dim_k H^1_{\mathfrak{L}^{\perp}_Q,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) + \sum_{q\in Q} \dim_k H^0(G_{\mathbf{Q}_q}, \mathrm{ad}^0\,\overline{\rho}(1)) + 1.$$

## 4.7 Definition and Properties of the Sets of Primes $Q$

In this section we define conditions on the sets of primes $Q$ to guarantee tameness of the rings $R_{Q_n,\mathrm{ord}}$. In particular, we will choose conditions that allow us to relate $R_{Q_n,\mathrm{ord}}$ with the ring $R_{\emptyset,\mathrm{ord}}$ and that force the restriction $\rho|_{G_{\mathbf{Q}_q}}$ to decompose into the direct sum of characters.

We assume without loss of generality that $\overline{\rho}(\sigma)$ has $k$-rational eigenvalues for all $\sigma$ – if not, one can extend $k$ by degree 2 without shrinking the space of deformations. All primes in $Q$ will satisfy the following properties.

- We have $q \equiv 1 \bmod p$.
- The restriction $\overline{\rho}|_{G_{\mathbf{Q}_q}}$ is unramified.
- The matrix $\overline{\rho}(\mathrm{Frob}_q^{-1})$ has distinct eigenvalues, which we call $\alpha_q$ and $\beta_q$.
- The character $\psi$ is unramified at $q$.

For $q$ meeting these properties, the univeral lifting $\rho^{\square}_{Q,\mathrm{ord}}$ has a particularly nice form when restricted to $G_{\mathbf{Q}_q}$.

**Proposition 4.21** ([DDT97, Lemma 2.44])**.** *For all $q \in Q$,*

$$\rho^{\square}_{Q,\mathrm{ord}}|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \xi & 0 \\ 0 & \psi\xi^{-1} \end{pmatrix}$$

*for a character $\xi$ with $\overline{\xi}(Frob_q^{-1}) = \alpha_q$, and similarly for $\rho_{Q,\mathrm{ord}}$.*

Before proving Proposition 4.21, we will prove a consequence of Hensel's lemma that will be important here and elsewhere.

**Lemma 4.22.** *Let $R$ be a complete Noetherian local ring with residue field $k$. Suppose $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right) \in \mathbf{M}_2(k)$ is a diagonal matrix with $\alpha, \beta$ distinct and nonzero, and suppose that $\left(\begin{smallmatrix} A & C_1 \\ C_2 & B \end{smallmatrix}\right)$ lifts this matrix to $\mathbf{M}_2(R)$. Then $\left(\begin{smallmatrix} A & C_1 \\ C_2 & B \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} \widetilde{\alpha} & 0 \\ 0 & \widetilde{\beta} \end{smallmatrix}\right)$, where $\widetilde{\alpha}$ and $\widetilde{\beta}$ lift $\alpha$ and $\beta$, respectively.*

*Proof.* By Hensel's lemma, there exist roots to the equations $x^2C_1 + x(A-B) - C_2 = 0$ and $y^2C_2 + y(B-A) - C_1$ that are close to 0, and thus in $\mathfrak{m}_R$ (here we are using the fact that $\overline{A-B} = \alpha - \beta \neq 0$). In particular, we have

$$\begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix}^{-1} \begin{pmatrix} A & C_1 \\ C_2 & B \end{pmatrix} \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix} = \begin{pmatrix} \widetilde{\alpha} & 0 \\ 0 & \widetilde{\beta} \end{pmatrix}$$

where $\widetilde{\alpha}$ and $\widetilde{\beta}$ reduce to $\alpha$ and $\beta$.

□

We will also prove another lemma that will find use here and elsewhere.

**Lemma 4.23.** *Let $R$ be a complete Noetherian local ring with residue field $k$. Suppose that $\rho : G_{\mathbf{Q}_q} \to \mathrm{GL}_2(R)$ has the property that $\overline{\rho}$ is unramified and that in some basis $\{\mathbf{e}_1, \mathbf{e}_2\}$, $\rho(\mathrm{Frob}_q^{-1}) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha \neq \beta$ for some choice of $\mathrm{Frob}_q^{-1}$. Then in this basis, $\rho$ is diagonal.*

*Proof.* We need only show that $\rho(\sigma)$ is diagonal for $\sigma \in I_{\mathbf{Q}_q}$. Let $\rho(\sigma) = \mathbf{1}_2 + \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Since $\overline{\rho}$ is unramified, Proposition 3.1 implies that $\rho$ is tamely ramified. By Fact 2.2, $\rho(\mathrm{Frob}_q^{-1})^{-1}\rho(\sigma)\rho(\mathrm{Frob}_q^{-1}) = \rho(\sigma)^q$. In particular,

$$\mathbf{1}_2 + \begin{pmatrix} a & b\frac{\widetilde{\beta}_q}{\widetilde{\alpha}_q} \\ c\frac{\widetilde{\alpha}_q}{\widetilde{\beta}_q} & d \end{pmatrix} = \sum_{i=0}^{q} \binom{q}{i} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^i .$$

Subtracting $\mathbf{1}_2 + q\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ from both sides,

$$\begin{pmatrix} a & b\left(\frac{\widetilde{\beta}_q}{\widetilde{\alpha}_q} - q\right) \\ c\left(\frac{\widetilde{\alpha}_q}{\widetilde{\beta}_q} - q\right) & d \end{pmatrix} = \sum_{i=2}^{q} \binom{q}{i} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^i .$$

The upper right diagonal entry of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^i$ for $i \geq 2$ lies in $b\mathfrak{m}_R$, and the lower left entry lies in $c\mathfrak{m}_R$. On the left, $\frac{\widetilde{\alpha}_q}{\widetilde{\beta}_q} - q$ and $\frac{\widetilde{\beta}_q}{\widetilde{\alpha}_q} - q$ are invertible, so the ideal generated by the upper right and lower left entries is $(b, c)$. Thus $(b, c) \subseteq \mathfrak{m}_R(b, c)$, which implies $b = c = 0$ by Nakayama's lemma.

□

*Proof of Proposition 4.21.* Let $\rho = \rho_{Q,\mathrm{ord}}$ or $\rho^{\square}_{Q,\mathrm{ord}}$, and similarly let $R = R_{Q,\mathrm{ord}}$ or $R^{\square}_{Q,\mathrm{ord}}$. Choose a basis where $\overline{\rho}(\mathrm{Frob}_q^{-1}) = \begin{pmatrix} \alpha_q & 0 \\ 0 & \beta_q \end{pmatrix}$, so that $\rho(\mathrm{Frob}_q^{-1}) = \left(\begin{smallmatrix} A & C_1 \\ C_2 & B \end{smallmatrix}\right)$ where $A$ and $B$ reduce to $\alpha_q$ and $\beta_q$ (fixing a particular $\mathrm{Frob}_q^{-1} \in G_{\mathbf{Q}_p}$). Using Lemma 4.22, perform a change of basis so that $\rho(\mathrm{Frob}_q^{-1}) = \begin{pmatrix} \widetilde{\alpha}_q & 0 \\ 0 & \widetilde{\beta}_q \end{pmatrix}$ where $\widetilde{\alpha}_q$ and $\widetilde{\beta}_q$ reduce to $\alpha_q$ and $\beta_q$.

By Lemma 4.23, $\rho$ is diagonal. Let $\xi$ be the character in the upper right corner. Then the form $\begin{pmatrix} \xi & 0 \\ 0 & \psi\xi^{-1} \end{pmatrix}$ is implied by the determinant condition.

□

Following [DDT97], we define $\Delta_q$ to be the maximal quotient of $(\mathbf{Z}/q\mathbf{Z})^\times$ of $p$-power order, and define $\Delta_Q = \prod_{q \in Q} \Delta_q$. For each $q$ there exists a map

$$\chi_q : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q}) \cong (\mathbf{Z}/q\mathbf{Z})^\times \twoheadrightarrow \Delta_q,$$

and we define $\chi_Q : G_{\mathbf{Q}} \to \Delta_Q$ to be the product of these maps.

Let $\mathfrak{a}_Q$ be the augmentation ideal of $W(k)[\Delta_Q]$. We have an isomorphism

$$W(k)[[\{S_q\}_{q \in Q}]]/((1 + S_q)^{\#\Delta_q} - 1)_{q \in Q} \cong W(k)[\Delta_Q],$$

obtained by mapping each $S_q$ to $g_q - 1$, $g$ a generator of $\Delta_q$.

Let the characters obtained in Proposition 4.21 be denoted $\xi_{q,Q} : G_{\mathbf{Q}_q} \to R_{Q,\mathrm{ord}}^{\times}$ and $\xi_{q,Q}^{\square} : G_{\mathbf{Q}_q} \to R_{Q,\mathrm{ord}}^{\square\times}$. Since $\rho_{Q,\mathrm{ord}}$ and $\rho_{Q,\mathrm{ord}}^{\square}$ are tamely ramified, the restrictions $\xi_{q,Q}|_{I_{\mathbf{Q}_q}}$ and $\xi_{q,Q}^{\square}|_{I_{\mathbf{Q}_q}}$ factor through $\chi_q$.

Since a character of $G_{\mathbf{Q}}$ is determined by its restriction to inertia groups at all prime, if there exist maps $\xi_Q : G_{\mathbf{Q}} \to R_{Q,\mathrm{ord}}^{\times}$ and $\xi_Q^{\square} : G_{\mathbf{Q}_q} \to R_{Q,\mathrm{ord}}^{\square,\times}$ whose restrictions to $I_{\mathbf{G}_q}$ are equal to the corresponding restrictions of $\xi_{q,Q}$ and $\xi_{q,Q}^{\square}$, respectively, and which are unramified elsewhere, then the maps are unique. (Every nontrivial extension of $\mathbf{Q}$ is ramified at some prime $p$.) On the other hand, since these characters are tamely ramified at all $q \in Q$, they must factor through $G_{\mathbf{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbf{Q}(\zeta_Q)/\mathbf{Q}) \cong \Delta_Q$, so we can construct these maps explicitly using the definitions of the maps $\xi_{q,Q}$ or $\xi_{q,Q}^{\square}$.

We define maps $\pi_Q : W(k)[\Delta_Q] \to R_{Q,\mathrm{ord}}$ and $\pi_Q^{\square} : W(k)[\Delta_Q] \to R_{Q,\mathrm{ord}}^{\square}$ by sending an element of $\Delta_Q$ to its image under $\xi_Q^{-2}$ or $\xi_Q^{\square-2}$, respectively (which is defined since these maps factor through $\chi_Q$, as noted earlier).

**Proposition 4.24** ([DDT97, Corollary 2.45])**.** *The natural maps*

$$R_{Q,\mathrm{ord}} \to R_{\emptyset,\mathrm{ord}} \quad \textit{and} \quad R_{Q,\mathrm{ord}}^{\square} \to R_{\emptyset,\mathrm{ord}}^{\square}$$

*have kernels given by the pushforwards of $\mathfrak{a}_Q$ under $\pi_{Q,\mathrm{ord}}$ and $\pi_{Q,\mathrm{ord}}^{\square}$, respectively.*

*Proof.* As in the proof of Proposition 4.21, we let $\pi : W(k)[\Delta_Q] \to R \to R_{\emptyset}$ and $\rho$ denote the objects in either of the two cases. It suffices to show that the composite map $G_{\mathbf{Q}} \xrightarrow{\rho} \mathrm{GL}_2(R) \to \mathrm{GL}_2(R/\mathfrak{a}_Q)$ is unramified at $q \in Q$ and that if $\mathfrak{a} \subset R$ is another ideal with this property, then $\mathfrak{a}_Q \subseteq \mathfrak{a}$. But the identifications of the images of the elements of $\Delta_Q$ with 1, together with the explicit description of $\rho|_{G_{\mathbf{Q}_q}}$ in Proposition 4.21, imply that the first of these claims hold, since they show that $\rho|_{I_{\mathbf{Q}_q}}$ is trivial (using the fact that $\psi$ is unramified away from $p$). Conversely, if $\mathfrak{a}$ had this property, it must identify $\xi(\sigma) = 1$ for all $\sigma \in \rho|_{I_{\mathbf{Q}_q}}$. But $\mathfrak{a}_Q$ is generated by $\xi(\sigma) - 1$ for $\sigma \in \rho|_{I_{\mathbf{Q}_q}}$, so $\mathfrak{a}_Q \subseteq \mathfrak{a}$.

□

We next compute certain local cohomology groups for $q \in Q$, taking advantage of the simple structure of $\overline{\rho}(\mathrm{Frob}_q)$.

**Proposition 4.25** ([DDT97, Lemma 2.46])**.** *We have*

$$\dim_k H^0(G_{\mathbf{F}_q}, \mathrm{ad}^0 \overline{\rho}) = \dim_k H^0(G_{\mathbf{F}_q}, \mathrm{ad}^0 \overline{\rho}(1)) = 1$$

*and*

$$\dim_k H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0 \overline{\rho}) = \dim_k H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0 \overline{\rho}(1)) = 1.$$

*Proof.* Note that the actions of $G_{\mathbf{F_q}}$ on $\mathrm{ad}^0 \overline{\rho}$ and $\mathrm{ad}^0 \overline{\rho}(1)$ are the same, so it suffices to consider just $\mathrm{ad}^0 \overline{\rho}$. It is clear that $\dim_k H^0(G_{\mathbf{F}_q}, \mathrm{ad}^0 \overline{\rho}) = 1$ since $\begin{pmatrix} \alpha_q & 0 \\ 0 & \beta_q \end{pmatrix}$ commutes only with the subspace generated by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{ad}^0 \overline{\rho}$.

For $H^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho})$, note that a cocycle is determined exactly by the image of Frobenius, so $\dim_k Z^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho}) = 3$. Since $\operatorname{ad}^0 \overline{\rho} \twoheadrightarrow B^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho})$ via $m \mapsto (\sigma \mapsto \sigma \cdot m - m)$, it suffices to compute the dimension of the kernel of this map. But the kernel is just $(\operatorname{ad}^0 \overline{\rho})^{\operatorname{Frob}_q}$, which as mentioned earlier has dimension 1. Thus, $\dim_k H^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho}) = 1$. $\square$

We next determine a condition under which $R_{Q,\mathrm{ord}}$ has Krull dimension at most $\#Q$.

**Proposition 4.26** ([DDT97, Lemma 2.46])**.** *Suppose that*

$$H^1_{\mathfrak{L}_\emptyset^\perp, p}(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}(1)) \cong \bigoplus_{q \in Q} H^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho}(1))$$

*via the map* $\xi \mapsto (\operatorname{Res}_{G_{\mathbf{F}_q}} \xi)_{q \in Q}$. *Then* $\dim R^\square_{Q,\mathrm{ord}} \leq \#Q + 4$ *and* $\dim R_{Q,\mathrm{ord}} \leq \#Q + 1$.

*Proof.* Note first that by Proposition 4.25, $\sum_{q \in Q} \dim_k H^0(G_{\mathbf{Q}_q}, \operatorname{ad}^0 \overline{\rho}(1)) = \#Q$. Thus, both bounds will follow from Corollaries 4.18 and 4.20 if we show that $H^1_{\mathfrak{L}_Q^\perp, p}(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}(1)) = 0$.

By definition,

$$H^1_{\mathfrak{L}_Q^\perp, p}(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}(1)) = \ker\left( H^1(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}) \to \bigoplus_{v \neq p} H^1(G_v, \operatorname{ad}^0 \overline{\rho}(1))/L_{v,Q} \right).$$

But using the restriction homomorphism on components in $Q$ and the 0 map elsewhere, we have a composite map

$$H^1(G_{\mathbf{Q}}, \operatorname{ad}^0 \overline{\rho}) \to \bigoplus_{v \neq p} H^1(G_v, \operatorname{ad}^0 \overline{\rho}(1))/L_{v,Q} \to \bigoplus_{q \in Q} H^1(G_{\mathbf{F}_q}, \operatorname{ad}^0 \overline{\rho}(1))$$

that is an isomorphism, so the kernel of the first map must vanish, as needed.

$\square$

## 4.8 Construction of Appropriate Sets of Primes $Q_n$

In this section, we prove the existence of a family of sets $Q_n$ with the properties described in Section 4.7. Moreover, these sets will be chosen to optimize the Krull dimensions of the rings $R_{Q,\mathrm{ord}}$. We will choose the sets $Q_n$ to meet the conditions of Proposition 4.26.

**Proposition 4.27** ([DDT97, Theorem 2.49])**.** *There exists an integer $r \geq 0$ such that for every $n$ we can construct a set $Q_n$ with the following properties.*

1. *For each $q \in Q_n$, $q \equiv 1 \bmod p^n$.*
2. *For each $q \in Q_n$, $\overline{\rho}$ is unramified at $q$ and $\overline{\rho}(\operatorname{Frob}_q)$ has distinct $k$-rational eigenvalues.*
3. *We have $\#Q_n = r$.*

*4. The set $Q_n$ contains no primes where $\psi$ is ramified.*

*5. We have the bounds* $\dim R_{Q_n,\mathrm{ord}} \le \#Q + 1$ *and* $\dim R^{\square}_{Q_n,\mathrm{ord}} \le \#Q + 4$.

*Proof.* Let $r = \dim_k H^1_{\mathfrak{L}_\emptyset,p}(\mathbf{Q}, \mathrm{ad}^0\,\overline{\rho}(1))$. By Proposition 4.26 and Proposition 4.25, it suffices to find a set $Q_n$ such that the following hold.

1. For each $q \in Q_n$, $q \equiv 1 \bmod p^n$.

2. For each $q \in Q_n$, $\overline{\rho}$ is unramified on $G_{\mathbf{Q}_q}$ and $\overline{\rho}(\mathrm{Frob}_q^{-1})$ has distinct $k$-rational eigenvalues.

3. The character $\psi$ is unramified at each $q \in Q_n$.

4. We have the isomorphism

$$H^1_{\mathfrak{L}_\emptyset^\perp,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) \cong \bigoplus_{q\in Q} H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0\,\overline{\rho}(1)).$$

Moreover, since the $H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0\,\overline{\rho}(1))$ are one-dimensional, an inclusion

$$H^1_{\mathfrak{L}_\emptyset^\perp,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)) \hookrightarrow \bigoplus_{q\in Q} H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0\,\overline{\rho}(1))$$

will suffice, as we can remove factors until the map is an isomorphism. Thus, it suffices to show that for every $[\xi] \in H^1_{\mathfrak{L}_\emptyset^\perp,p}(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1))$, there exists a prime $q$ such that the following hold.

1. We have $q \equiv 1 \bmod p^n$.

2. The representation $\overline{\rho}$ is unramified on $G_{\mathbf{Q}_p}$ and $\overline{\rho}(\mathrm{Frob}_q)$ has distinct $k$-rational eigenvalues.

3. The character $\psi$ is unramified at $q$.

4. The image of $[\xi]$ in $H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0\,\overline{\rho}(1))$ is nontrivial.

**Claim 4.28.** *We claim, in fact, that it suffices to show that there exists $\sigma \in G_{\mathbf{Q}_p}$ with the following properties.*

*1. We have* $\sigma|_{\mathbf{Q}(\zeta_{p^n})} = 1$.

*2. The action of* $\overline{\rho}(\sigma)$ *on* $\mathrm{ad}^0\,\overline{\rho}$ *has an eigenvalue other than 1.*

*3. We have* $\xi(\sigma) \notin (\sigma - 1)\,\mathrm{ad}^0\,\overline{\rho}(1) = B^1(\widehat{\langle\sigma\rangle}, \mathrm{ad}^0\,\overline{\rho}(1))$, *where* $\widehat{\cdot}$ *denotes the profinite completion.*

*Proof.* We show that each of the earlier conditions hold.

1. By the Čebotarev density theorem, Frobenius elements are dense in $G_{\mathbf{Q}_p}$. If $\mathrm{Frob}_q^{-1}$ is sufficiently close to $\sigma$, so that they have the same action on $\mathbf{Q}(\zeta_{p^n})$, then $\epsilon^{-1}(\mathrm{Frob}_q^{-1}) = q = 1 \bmod p^n$.

2. Suppose that $\overline{\rho}(\sigma)$ has an eigenvalue other than 1. First note that we may choose a basis so that either $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$. In the first case, we can write the matrix for the action on the ordered basis $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ as
$$\begin{pmatrix} 1 & \frac{2}{\alpha} & -\frac{1}{\alpha} \\ 0 & 1 & -\frac{1}{\alpha^2} \\ 0 & 0 & 1 \end{pmatrix},$$
so there are no eigenvalues other than 1. In the second case, the eigenvalues are $1, \frac{\alpha}{\beta}$, and $\frac{\beta}{\alpha}$, so $\beta \neq \alpha$ exactly when the matrix has an eigenvalue other than 1.

3. By the Čebotarev density theorem, we can avoid the finite set of primes where $\psi$ is ramified.

4. For a sufficiently close approximation $\mathrm{Frob}_q^{-1}$ to $\sigma$, the third condition implies that the image of $[\xi]$ in $H^1(G_{\mathbf{F}_q}, \mathrm{ad}^0\,\overline{\rho}(1))$ must be nontrivial.

$\square$

We next define a family of fields $F_m$ for $m \geq 0$ by letting $F_m$ be the kernel of the representation $\mathrm{ad}^0\,\overline{\rho}|_{G_{\mathbf{Q}(\zeta_{p^m})}}$. In other words, if $F$ is the fixed field of the representation $\mathrm{ad}^0\,\overline{\rho}$, then $F_m$ is the compositum $F \cdot \mathbf{Q}(\zeta_{p^m})$.

**Claim 4.29.** *The image $\xi(G_{F_n}) \subseteq \mathrm{ad}^0\,\overline{\rho}(1)$ is nontrivial.*

*Proof.* Consider the inflation homomorphism
$$H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \mathrm{ad}^0\,\overline{\rho}(1)) \to H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1)),$$
noting that $G_{F_n}$ acts trivially on $\mathrm{ad}^0\,\overline{\rho}(1)$ since $F_n \subseteq \mathbf{Q}(\zeta_p)$. If $\xi(G_{F_n})$ is trivial, then $\xi$ pulls back to a nontrivial element of $H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \mathrm{ad}^0\,\overline{\rho}(1))$ since it is nontrivial as an element of $H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\,\overline{\rho}(1))$. Thus, it suffices to show that $H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \mathrm{ad}^0\,\overline{\rho}(1)) = 0$.

Consider the inflation-restriction exact sequence
$$\begin{aligned} 0 &\to H^1(\mathrm{Gal}(F_0/\mathbf{Q}), (\mathrm{ad}^0\,\overline{\rho}(1))^{G_{F_0}}) \to H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \mathrm{ad}^0\,\overline{\rho}(1)) \\ &\to H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0\,\overline{\rho}(1))^{\mathrm{Gal}(F_0/\mathbf{Q})} = H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0\,\overline{\rho}(1))^{G_{\mathbf{Q}}}, \end{aligned}$$
where the action of $g \in \mathrm{Gal}(F_0/\mathbf{Q})$ sends $\eta \mapsto (h \mapsto g^{-1}\eta(ghg^{-1}))$. Since $\mathrm{Gal}(F_1/F_0)$ has order dividing $p-1$ and thus prime to $p$, the restriction map
$$H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0\,\overline{\rho}(1)) \to H^1(\mathrm{Gal}(F_n/F_1), \mathrm{ad}^0\,\overline{\rho}(1))$$

is an isomorphism, as one can see using the fact that the restriction-corestriction sequence

$$H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0 \overline{\rho}(1)) \to H^1(\mathrm{Gal}(F_n/F_1), \mathrm{ad}^0 \overline{\rho}(1)) \to H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0 \overline{\rho}(1))$$

is an isomorphism. Note that the action of $G_{\mathbf{Q}}$-conjugation is trivial on $\mathrm{Gal}(F_n/F_1)$ since it factors through the abelianization of $G_{\mathbf{Q}}$. Since $\mathrm{Gal}(F_n/F_1) \cong \mathbf{Z}/p^{n-1}\mathbf{Z}$ is cyclic, and the cocycle relation holds, the map is determined by the image of a generator $h$. Then for $\varphi \in H^1(\mathrm{Gal}(F_n/F_1), \mathrm{ad}^0 \overline{\rho}(1))^{G_{\mathbf{Q}}}$ defined by $\varphi(h) = m$, $\varphi$ is $G_{\mathbf{Q}}$-invariant if for $g \in G_{\mathbf{Q}}$, $g^{-1}\varphi(ghg^{-1}) = g^{-1}\varphi(h) = g^{-1}m = m$, meaning that $m$ is $G_{\mathbf{Q}}$-invariant. Conversely, such a choice of $m$ defines a cocycle. In particular, we have

$$H^1(\mathrm{Gal}(F_n/F_1), \mathrm{ad}^0 \overline{\rho}(1))^{G_{\mathbf{Q}}} \cong \mathrm{Hom}(\mathrm{Gal}(F_n/F_1), (\mathrm{ad}^0 \overline{\rho}(1))^{G_{\mathbf{Q}}}).$$

Finally, observe that $(\mathrm{ad}^0 \overline{\rho}(1))^{G_{\mathbf{Q}}} = 0$ by Proposition 4.13.

Next, consider $H^1(\mathrm{Gal}(F_0/\mathbf{Q}), (\mathrm{ad}^0 \overline{\rho}(1))^{G_{F_0}})$. Note that $(\mathrm{ad}^0 \overline{\rho}(1))^{G_{F_0}}$ is trivial unless $F_0$ contains $\mathbf{Q}(\zeta_p)$, since otherwise some element of $G_{F_0}$ acts on $\mathrm{ad}^0 \overline{\rho}(1)$ nontrivially by multiplication by the cyclotomic character $\epsilon$. If $p \nmid \mathrm{Gal}(F_0, \mathbf{Q})$, then $H^1(\mathrm{Gal}(F_0/\mathbf{Q}), (\mathrm{ad}^0 \overline{\rho}(1))^{G_{F_0}})$ vanishes since it injects into the cohomology with respect to a Sylow $p$-subgroup. Thus we are reduced to the case where $p | \# \mathrm{Gal}(F_0/\mathbf{Q})$ and has $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ as a quotient. Note also that $\mathrm{Gal}(F_0/\mathbf{Q})$ is the projective image of $\overline{\rho}$ (since the kernel of the action on $\mathrm{ad}\, \overline{\rho}$ is given by the scalar matrices in $\mathrm{GL}_2(k)$). We will show that these conditions are impossible to meet, completing the proof.

Fact 2.1 classifies all possibilities for $\mathrm{Gal}(F_0/\mathbf{Q})$. Since we have assumed $p > 3$, the condition that $p | \# \mathrm{Gal}(F_0/\mathbf{Q})$ leaves us with the cases $D_{2r}$, $A_5$, $\mathrm{PSL}(\mathbf{F}_{p^r})$, $\mathrm{PGL}(\mathbf{F}_{p^r})$, and subgroups of the upper triangular matrices. Since $\mathrm{PSL}(\mathbf{F}_{p^r})$ is simple for $p > 3$ and the only nontrivial proper normal subgroup of $\mathrm{PGL}(\mathbf{F}_{p^r})$ is of index 2, these cases are ruled out since $\mathrm{Gal}(F_0/\mathbf{Q})$ must have a quotient of order $p - 1$. The group $A_5$ is ruled out for the same reason, as it is simple, and $D_{2r}$ since $p \nmid r$ in the statement of the proposition. If $\mathrm{Gal}(F_0/\mathbf{Q})$ is conjugate to a subgroup of the upper triangular matrices, then $\overline{\rho}$ is not absolutely irreducible.

□

**Claim 4.30.** *The restriction $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_{p^n})}}$ is absolutely irreducible.*

*Proof.* We first show that $\overline{\rho}|_{G_L}$ is absolutely irreducible, where $L = \mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$. Note that $\mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ has discriminant $p$, so that the extension is ramified only at $p$. Since $\overline{\rho}$ is unramified at $p$, the image $\overline{\rho}(G_{\mathbf{Q}})$ is the same as $\overline{\rho}(G_L)$, so $\overline{\rho}|_{G_L}$ is absolutely irreducible.

Now suppose that $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_{p^n})}}$ is not absolutely irreducible. We consider the cases described in Fact 2.1 for the image $\mathrm{Gal}(F_0/\mathbf{Q})$.

- Since $\overline{\rho}$ is absolutely irreducible, we can exclude the case where $\mathrm{Gal}(F_0/\mathbf{Q})$ is conjugate to a subgroup of the upper triangular matrices.

- In the case of $\mathrm{PSL}_2(\mathbf{F}_{p^r})$, since this group is simple, if $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_{p^n})}}$ is not absolutely irreducible, then $F_0 \subseteq \mathbf{Q}(\zeta_{p^n})$, which means that $\mathrm{Gal}(F_0/\mathbf{Q})$ is abelian, contradicting hypothesis. In the case of $\mathrm{PGL}_2(\mathbf{F}_{p^r})$, the subgroup can only be a conjugate of $\mathrm{PSL}_2(\mathbf{F}_{p^r})$ or trivial, but the first still makes $\overline{\rho}$ absolutely irreducible and the second is impossible for the same reason as for $\mathrm{PSL}_2(\mathbf{F}_{p^r})$.

- Since $A_5$ is simple, we may apply the same argument as earlier. The explicit representation of $D_{2r}$ in Fact 2.1 shows that if the subgroup of $\mathrm{Gal}(F_0/\mathbf{Q})$ yields a $\overline{\rho}$ that is no longer absolutely irreducible, the subgroup must be contained in $\langle t\rangle$. But then $\rho|_{G_L}$ is already reducible, since the associated subgroup is $\langle t\rangle$, which has diagonal image. In the $A_4$ and $S_4$ cases, $\overline{\rho}(G_{\mathbf{Q}(\zeta_{p^n})})$ must be nontrivial by the preceding argument since $A_4$ and $S_4$ are nonabelian. The smallest nontrivial normal subgroup in either case is the Klein four group, which falls under the dihedral case in the enumeration in Fact 2.1, and is thus irreducible by the explicit enumeration of dihedral subgroups in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$.

$\square$

Now consider the image $\xi(G_{F_n})$. Since $\mathrm{Gal}(F_0/\mathbf{Q}) = G_{\mathbf{Q}}/G_{F_0}$ acts on $\mathrm{ad}^0\,\overline{\rho}$, so does $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n})) = G_{\mathbf{Q}(\zeta_{p^n})}/(G_{F_0}\cap G_{\mathbf{Q}(\zeta_{p^n})})$. Moreover, $\xi(G_{F_n})$ is preserved by the conjugation action by $G_{\mathbf{Q}(\zeta_{p^n})}$ since for $\tau \in G_{F_n}$ and $\sigma \in G_{\mathbf{Q}(\zeta_{p^n})}$, we have

$$\xi(\sigma\tau\sigma^{-1}) = \xi(\sigma)+\sigma\cdot\xi(\tau\sigma^{-1}) = \xi(\sigma)+\sigma\cdot\xi(\tau)+\sigma\tau\cdot\xi(\sigma^{-1}) = \xi(\sigma)+\sigma\cdot\xi(\tau)+\sigma\cdot\xi(\sigma^{-1}) = \sigma\cdot\xi(\tau)$$

by the cocycle relation and the fact that $\tau$ acts trivially on $\mathrm{ad}^0\,\overline{\rho}$, and $\sigma\tau\sigma^{-1} \in G_{F_n}$ by the normality of the extension $F_n$. The image $\xi(G_{F_n})$ is also closed under addition, since for $\tau_1, \tau_2 \in \xi(G_{F_n})$,

$$\xi(\tau_1) + \xi(\tau_2) = \tau_2 \cdot \xi(\tau_1) + \xi(\tau_2) = \xi(\tau_2\tau_1),$$

and $\tau_2\tau_1 \in G_{F_n}$. Thus $\xi(G_{F_n})$ is a $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$-submodule of $\mathrm{ad}^0\,\overline{\rho}$.

**Claim 4.31.** *There exists an element $g \in \mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$ with order not dividing $p$ that fixes a nonzero element of $\xi(G_{F_n})$.*

*Proof.* First note that the map $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n})) \to \mathrm{GL}_2(k)$ is absolutely irreducible by Claim 4.30. By Fact 2.1, we are reduced to three cases for the image. We further remark that if we prove the statement for the case where $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$ has image $H$, then the statement holds for any group $G$ containing $H$.

- By absolute irreducibility, we can exclude the case where $\mathrm{Gal}(F_0/\mathbf{Q}(\zeta_{p^n}))$ is conjugate to a subgroup of the upper triangular matrices.

- By the preceding remark, we need only consider the case of $\mathrm{PSL}_2(\mathbf{F}_{p^r})$. Note that $\mathrm{ad}^0\,\overline{\rho}$ is a simple module under the action of $\mathrm{PSL}_2(\mathbf{F}_{p^r})$, so $\psi(G_{F_n}) = \mathrm{ad}^0\,\overline{\rho}$ in this case. Since $p > 3$, the matrix $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{smallmatrix}\right)$ for $\alpha \in \mathbf{F}_{p^r}$ such that $\alpha \neq \alpha^{-1}$ fixes the nonzero element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Note that this element has order dividing $p-1$.

- By the preceding remark, it suffices to consider the cases of $D_4$ and $D_{2r}$ where $r$ is odd, since $A_4, S_4$, and $A_5$ contain the Klein four group as a subgroup. Using the explicit description of $D_4$ in Fact 2.1, we find that $\mathrm{ad}^0\,\overline{\rho}$ decomposes into 1-dimensional irreducible submodules

$$\mathrm{ad}^0\,\overline{\rho} \cong \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix} \oplus \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix}, a, b, c \in k,$$

and it is easy to find a nontrivial element for each of the three submodules that preserves the space. In fact, each of the elements of $D_4$ act as $\pm 1$ on any particular 1-dimensional irreducible submodule, and there are three nontrivial elements, so one of them must act trivially. All of these elements have order 2.

In the case of $D_{2r}$ for $r$ odd, we have the decomposition

$$\mathrm{ad}^0\,\overline{\rho} \cong \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \oplus \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, a, b, c \in k$$

into $D_{2r}$-submodules. We claim that the submodule of matrices of the form $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ is irreducible. If not, there is a 1-dimensional irreducible submodule given by the multiples of some element $\left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right)$. Acting by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, we see that $d\left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & \beta \\ \alpha & 0 \end{smallmatrix}\right)$ for $d \in k$, meaning that if, say, $\alpha \neq 0$, then $\alpha = d\beta = d^2\alpha$, or $d^2 = 1$. Thus either $\alpha = -\beta$ or $\alpha = \beta$. Acting by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_r \end{smallmatrix}\right)$, we find that neither of these 1-dimensional subspaces are preserved. Thus the given decomposition is the irreducible decomposition of $\mathrm{ad}^0\,\overline{\rho}$. We find that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_r \end{smallmatrix}\right)$ preserves the first irreducible component and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ fixes $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ in the second. Since $p \nmid \#D_{2r}$, the order of $g$ does not divide $p$.

$\square$

We will next show that $\xi(G_{F_n}) \not\subseteq (g-1)\,\mathrm{ad}^0\,\overline{\rho}(1)$. For this we need the following.

**Claim 4.32.** *The representation of* $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$ *on* $\mathrm{ad}^0\,\overline{\rho}(1)$ *is semisimple.*

*Proof.* Using Fact 2.1, we are reduced to three cases as before, and the case where the image of $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$ is conjugate to a subgroup of the upper triangular matrices is eliminated by the fact that the representation is absolutely irreducible. The action of $\mathrm{PGL}_2(\mathbf{F}_{p^r})$ or $\mathrm{PSL}_2(\mathbf{F}_{p^r})$ on $\mathrm{ad}^0\,\overline{\rho}$, so we are reduced to $D_{2r}$, $A_4$, $S_4$, and $A_5$. Maschke's theorem and the assumption $p > 3$ reduces us to $A_5$ and $p = 5$. But Fact 2.1 shows that the image $A_5$ is conjugate to $\mathrm{PSL}_2(\mathbf{F}_5)$, a case just worked out.

$\square$

We have $\xi(G_{F_n}) \not\subseteq (g-1)\xi(G_{F_n})$ since the existence of an element of $\xi(G_{F_n})$ fixed by $g$ implies that the linear operator $g-1$ has an image in $\psi(G_{F_n})$ of positive codimension. Since $\mathrm{ad}^0\,\overline{\rho} = \xi(G_{F_n}) \oplus M$ for some $\mathrm{Gal}(F_n/\mathbf{Q}(\zeta_{p^n}))$-module $M$ by Claim 4.32, we must have $\xi(G_{F_n}) \not\subseteq (g-1)\,\mathrm{ad}^0\,\overline{\rho}(1)$ as well.

Lifting $g$ to an element $\sigma_0 \in G_{\mathbf{Q}(\zeta_{p^n})}$, we claim we can chose an element $\tau \in G_{F_n}$ such that $\sigma = \tau\sigma_0$ satisfies the requisite properties stated in Claim 4.28. Observe that any such $\sigma$ fixes

$\mathbf{Q}(\zeta_{p^n})$, so $\sigma$ satisfies the first property. Since $\xi(G_{F_n}) \not\subseteq (g-1)\,\mathrm{ad}^0\,\overline{\rho}(1) = (\sigma - 1)\,\mathrm{ad}^0\,\overline{\rho}(1)$, we can pick $\tau$ such that

$$\xi(\tau\sigma_0) = \xi(\tau) + \tau \cdot \xi(\sigma_0) = \xi(\tau) + \xi(\sigma_0) \notin (\sigma - 1)\,\mathrm{ad}^0\,\overline{\rho}(1),$$

so $\sigma$ satisfies the third property. Finally, observe that after conjugation, $\overline{\rho}(\sigma)$ is of the form $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$, since the eigenvalues of $\rho$ are assumed $k$-rational. Observe that $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)^m = \left(\begin{smallmatrix} \alpha^m & m\alpha^{m-1} \\ 0 & \alpha^m \end{smallmatrix}\right)$. For this to vanish, since $\alpha^{m-1}$ is nonzero, we must have $p|m$. Since $g$ has order not dividing $p$, $\overline{\rho}$ cannot have the form $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$. We can also rule out the case where $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha = \beta$ since $g \notin G_{F_n}$ and thus acts nontrivially on $\mathrm{ad}^0\,\overline{\rho}$. Thus $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha \neq \beta$, completing the proof of the proposition.

$\square$

# Chapter 5

# Families of Hecke Algebras Acting on Weight Two Cusp Forms

In Sections 3 and 4, we constructed a ring $R_{\emptyset,\mathrm{ord}}$ such that when restricted to $\mathbf{DVR}(k)$, $\mathrm{Hom}(R_{\emptyset,\mathrm{ord}}, \cdot)$ parametrizes liftings that we expect to be modular. In order to show that all of the deformations of a residual representation $\overline{\rho}$ meeting the conditions defined in Section 4 are modular, we must compare the ring $R_{\emptyset,\mathrm{ord}}$ to a ring $\mathbf{T}_\emptyset$ that has the property that when the functor $\mathrm{Hom}(\mathbf{T}_\emptyset, \cdot)$ is restricted to the subcategory $\mathbf{DVR}(k)$, it parametrizes *modular* liftings of $\overline{\rho}$. Moreover, $\mathbf{T}_\emptyset$ acts on a space $S_\emptyset$ of modular forms that give rise to these modular representations.

In order to perform this comparison, we will need to build and relate families of rings $\{R_{Q_n,\mathrm{ord}}\}$ and $\{\mathbf{T}_{Q_n}\}$ that are endowed with actions from $p$-groups $\Delta_{Q_n}$ of increasing size. The family $\{\mathbf{T}_{Q_n}\}$ acts on a family $\{S_{Q_n}\}$ of spaces of modular forms. Moreover, the quotient of the rings $R_{Q_n,\mathrm{ord}}$ and spaces $S_{Q_n}$ by the action of $\Delta_{Q_n}$ should collapse them to $R_{\emptyset,\mathrm{ord}}$ and $S_\emptyset$. We constructed rings $R_{Q_n,\mathrm{ord}}$, bounded their tangent space dimensions, and checked that $R_{Q_n,\mathrm{ord}}/\mathfrak{a}_{Q_n} R_{Q_n,\mathrm{ord}} = R_{\emptyset,\mathrm{ord}}$ in Section 4. In this section, we will construct the family $\{\mathbf{T}_{Q_n}\}$ and analyze its properties.

We will need to have two views of the Hecke algebras $\mathbf{T}_{Q_n}$. Following Carayol [Car94], the first, presented in Section 5.1, will be as a subring of a product $\widetilde{\mathbf{T}}_{Q_n}$ of rings of integers associated to certain newforms $f$. With this definition, it will be automatic to define a universal modular Galois representation $\widetilde{\rho}^{\mathrm{mod}}_{Q_n} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\widetilde{\mathbf{T}}_{Q_n})$. From this we will construct a representation valued in $\mathbf{T}_{Q_n}$. We will next view $\mathbf{T}_{Q_n}$ as a localization of the usual Hecke algebra acting on the cohomology of modular curves. We will prove an isomorphism between the two possible constructions of $\mathbf{T}_{Q_n}$ in Section 5.2.

We will construct surjective morphisms $R_{\emptyset,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_\emptyset$ and $R_{Q_n,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_{Q_n}$ in Section 5.3. Moreover, we will find that the natural action of $\Delta_{Q_n}$ on $\mathbf{T}_{Q_n}$ coming from the diamond operators $\langle d \rangle$ agrees with the action induced via the $R_{Q_n,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_{Q_n}$ morphism in Section 5.4. Both this compatibility and the isomorphism between the two definitions of $\mathbf{T}_{Q_n}$ will make use of the deep structure theorems for the representations $\rho_f$ presented in Fact 2.14.

We will finally prove in Section 5.5 an analogue of Proposition 4.24 for the cohomology groups of modular curves, viewed as $\mathbf{T}_{Q_n}$ and $\mathbf{T}_\emptyset$-modules. This will be the last ingredient necessary for the Taylor-Wiles argument presented in Section 6.

## 5.1 Definition of the Rings $\mathbf{T}_{\mathfrak{F}}$ and Associated Representations $\rho_{\mathfrak{F}}^{\mathrm{mod}}$

We will construct the ring $\mathbf{T}_{\mathfrak{F}}$ in a general setting. Let $T$ denote the product of primes where $\overline{\rho}$ is ramified. As before, let $p > 3$ denote a prime and $\psi : G_{\mathbf{Q}} \to W(k)$ a fixed character that is unramified outside a finite set of primes. We define $\psi'$ via $\psi = \epsilon^{-1}\psi'$, so that $\psi'$ is the character of the newforms $f$ whose representations have the correct determinant. We assume that $T$ is squarefree and that for all primes $t|T$, $p \nmid t-1$.

Let $N$ be a positive integer such that $pT|N$ and let $H^1(X_1(N), W(k))^-$ be the negative eigenspace of the induced action on $H^1(X_1(N), W(k))$ of the complex conjugation $z \mapsto -\overline{z}$ on $X_1(N)$. We have a Hecke algebra $\mathbf{T}_{\Gamma_1(N),W(k)}$ acting on $H^1(X_1(N), W(k))^-$.

Denote by $F(k)$ the fraction field of $W(k)$. For a newform $f \in \mathbf{P}H^1(X_1(N), \overline{F(k)})^-$, we denote by $K_f$ the finite extension of $F(k)$ generated by its eigenvalues under the Hecke algebra $\mathbf{T}_{\Gamma_1(N_f),W(k)}$, where $N_f$ denotes the level of $f$. Recall from Section 2.2.2 that we consider $f$ to be a newform for $\Gamma$ if its Hecke eigenvalues are identical to those of a newform of level $N_f$. Denote by $\mathfrak{O}_f$ the ring of integers of $K_f$ and by $k_f$ its residue field. Denote by $\psi_f$ the Nebentypus character of $f$.

Denote the Galois representation attached to a newform $f$ by $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_f)$. Given a family $\mathfrak{F} = \{f_i\}$ of newforms in $\mathbf{P}H^1(X_1(N), \overline{F(k)})$ such that $\rho_{f_i}$ lifts (a conjugate of) $\overline{\rho}$ for each $i$, we may construct a Galois representation

$$\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}} : G_{\mathbf{Q}} \to \prod_i \mathrm{GL}_2(\mathfrak{O}_{f_i}) \cong \mathrm{GL}_2\left(\prod_i \mathfrak{O}_{f_i}\right).$$

We define $\widetilde{\mathbf{T}}_{\mathfrak{F}} = \prod_i \mathfrak{O}_{f_i}$ and $\mathbf{T}_{\mathfrak{F}}$ to be the $W(k)$-subalgebra of $\widetilde{\mathbf{T}}_{\mathfrak{F}}$ generated by elements of the form $T_r = (a_r(f_i)) \in \widetilde{\mathbf{T}}_{\mathfrak{F}}$ for $r \nmid N$. We also add the element $U_p = (a_p(f_i)) \in \widetilde{\mathbf{T}}_{\mathfrak{F}}$.

**Proposition 5.1** ([DDT97, Lemma 3.27]). *We may conjugate $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\widetilde{\mathbf{T}}_{\mathfrak{F}})$ to yield a representation*

$$\rho_{\mathfrak{F}}^{\mathrm{mod}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{F}}).$$

*Proof.* Fix a complex conjugation $\mathbf{c}$, and conjugate $\overline{\rho}$ so that $\overline{\rho}(\mathbf{c}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Conjugate each factor of $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}$ so that it reduces to $\overline{\rho}$ modulo every maximal ideal. By applying 4.22 to each factor of $\widetilde{\mathbf{T}}_{\mathfrak{F}}$, we may choose a basis $(\mathbf{e}_+, \mathbf{e}_-)$ such that $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c}) = \left(\begin{smallmatrix} \widetilde{1} & 0 \\ 0 & \widetilde{-1} \end{smallmatrix}\right)$, where $\widetilde{1}$ lifts $1 \in k$ and $\widetilde{-1}$ lifts $-1 \in k$. Note that $\widetilde{1}$ must square to 1 in each factor $\mathcal{O}_{f_i}$ and lift 1, so it is 1, and similarly, $\widetilde{-1} = -1$. Thus $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Next recall that by Fact 2.14, $T_r = \operatorname{Tr} \rho_{f_i}(\mathrm{Frob}_r^{-1})$ for primes $r \nmid N_\Gamma$. Each of the $\rho_{f_i}$ is continuous, so $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}$ is continuous. Thus the Čebotarev density theorem implies that $\operatorname{Tr} \widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}$

takes values in $\mathbf{T}_{\mathfrak{F}}$. Let $g \in G_{\mathbf{Q}}$, and write $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(g) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c}g) = \left(\begin{smallmatrix} a & b \\ -c & -d \end{smallmatrix}\right)$, so since $p \neq 2$, both

$$a = \frac{\mathrm{Tr}\,\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(g) + \mathrm{Tr}\,\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c}g)}{2} \quad \text{and} \quad d = \frac{\mathrm{Tr}\,\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(g) - \mathrm{Tr}\,\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c}g)}{2}$$

lie in $\mathbf{T}_{\mathfrak{F}}$.

Since $\overline{\rho}$ is irreducible, there is some $\sigma \in G_{\mathbf{Q}}$ so that $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} * & b \\ * & * \end{smallmatrix}\right)$ where $b \neq 0$. Let $\widetilde{b}$ denote the lift of $b$. If we rescale $\mathbf{e}_+$, $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\mathbf{c})$ does not change, so the preceding argument still implies that the diagonal entries are in $\mathbf{T}_{\mathfrak{F}}$. Thus, if we replace $\mathbf{e}_+$ with $\widetilde{b}^{-1}\mathbf{e}_+$, we have $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\sigma) = \left(\begin{smallmatrix} a & 1 \\ c & d \end{smallmatrix}\right)$. For any $g \in G_{\mathbf{Q}}$, writing $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(g) = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$, we have

$$\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\sigma g) = \begin{pmatrix} a'a + c' & ab' + d' \\ ca' + dc' & cb' + dd' \end{pmatrix},$$

so using the fact that $a, a' \in \mathbf{T}_{\mathfrak{F}}$ just proved, $c' \in \mathbf{T}_{\mathfrak{F}}$.

Finally, we use the absolute irreducibility of $\overline{\rho}$ to choose $\tau \in G_{\mathbf{Q}}$ so that $\overline{\rho}(\tau) = \left(\begin{smallmatrix} * & * \\ c & * \end{smallmatrix}\right)$ where $c \neq 0$. Then $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\tau) = \left(\begin{smallmatrix} a & b \\ c_0 & d \end{smallmatrix}\right)$ where $c_0 \in \mathbf{T}_{\mathfrak{F}}^{\times}$ by the preceding paragraph. In particular, for any $g \in G_{\mathbf{Q}}$, writing $g = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$, we have

$$\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}(\tau g) = \begin{pmatrix} a'a + bc' & ab' + bd' \\ c_0a' + dc' & c_0b' + dd' \end{pmatrix},$$

so $b' \in \mathbf{T}_{\mathfrak{F}}$ since $d, d' \in \mathbf{T}_{\mathfrak{F}}$ as proved earlier and $c_0 \in \mathbf{T}_{\mathfrak{F}}^{\times}$. Thus, when written in this basis, $\widetilde{\rho}_{\mathfrak{F}}^{\mathrm{mod}}$ is a representation

$$\rho_{\mathfrak{F}}^{\mathrm{mod}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{F}}).$$

□

## 5.2 Definition and Properties of the Families $\{\mathbf{T}_{Q_n}\}$ and $\{S_{Q_n}\}$

Let $Q_n$ be as in Section 4 and define $q_n = \prod_{q \in Q_n} q$. We define $\mathbf{T}_{Q_n} = \mathbf{T}_{\mathfrak{F}_n}$, where $\mathfrak{F}_n$ is the collection of newforms

$$\mathfrak{F}_n = \left\{ f \in \mathbf{P}H^1(X_1(pq_nT), \overline{F(k)})^- \;\middle|\; \begin{array}{l} \rho_f \text{ satisfies} \\ \quad 1.\ \overline{\rho}_f \cong \overline{\rho} \otimes_k k_f \\ \quad 2.\ U_q(f) \equiv \alpha_q \bmod p \\ \quad 3.\ \det \rho_f|_{(\mathbf{Z}/pT\mathbf{Z})^\times} \equiv \psi|_{(\mathbf{Z}/pT\mathbf{Z})^\times} \end{array} \right\}. \tag{5.1}$$

Define $\rho_{Q_n}^{\mathrm{mod}}$ to be the representation given by Proposition 5.1. Note that the third condition in (5.1) allows $\rho_f$ to have a nontrivial character on $(\mathbf{Z}/q_n\mathbf{Z})^\times$.

We similarly define $\mathbf{T}_\emptyset = \mathbf{T}_{\mathfrak{F}_\emptyset}$, where $\mathfrak{F}_\emptyset$ is the collection of newforms

$$\mathfrak{F}_\emptyset = \left\{ f \in \mathbf{P}H^1(X_1(pT), \overline{F(k)})^- \;\middle|\; \begin{array}{l} \rho_f \text{ satisfies} \\ \quad 1.\ \overline{\rho}_f \cong \overline{\rho} \otimes_k k_f \\ \quad 2.\ \det \rho_f \equiv \psi \end{array} \right\}. \tag{5.2}$$

Define $\rho_\emptyset^{\mathrm{mod}}$ to be the representation given by Proposition 5.1.

We will relate $\mathbf{T}_{Q_n}$ and $\mathbf{T}_\emptyset$ to Hecke algebras acting on spaces of modular forms. From Section 2.2.2, we recall that we may construct the Hecke algebra $\mathbf{T}_{Q_n,\mathbf{Z}}$ acting on $H^1(X_1(pq_nT), \mathbf{Z})^-$ as the subring of $\mathrm{End}(H^1(X_1(pq_nT), \mathbf{Z})^-)$ generated by the Hecke operators $T_m$ for $m \geq 1$ and $\langle d \rangle$ for $d \in (\mathbf{Z}/pq_nT\mathbf{Z})^\times$. We construct $\mathbf{T}_{\emptyset,\mathbf{Z}} \subseteq \mathrm{End}(H^1(\Gamma_1(pT), \mathbf{Z})^-)$ in the same manner. Tensoring with $W(k)$, we obtain Hecke algebras

$$\mathbf{T}_{Q_n,W(k)} \subseteq \mathrm{End}(H^1(X_1(pq_nT), W(k))^-) \quad \text{and} \quad \mathbf{T}_{\emptyset,W(k)} \subseteq \mathrm{End}(H^1(X_1(pT), W(k))^-).$$

We will construct maximal ideals $\mathfrak{m}_{Q_n}$ and $\mathfrak{m}_\emptyset$ of $\mathbf{T}_{Q_n,W(k)}$ and $\mathbf{T}_{\emptyset,W(k)}$ such that $\mathbf{T}_{Q_n}$ and $\mathbf{T}_\emptyset$ are isomorphic to the localizations of $\mathbf{T}_{Q_n,W(k)}$ and $\mathbf{T}_{\emptyset,W(k)}$ at these maximal ideals. Via these isomorphisms, $\mathbf{T}_{Q_n}$ acts on the space

$$S_{Q_n} = H^1(X_1(pq_nT), W(k))^-_{\mathfrak{m}_{Q_n}}$$

and $\mathbf{T}_\emptyset$ acts on

$$S_\emptyset = H^1(X_1(pT), W(k))^-_{\mathfrak{m}_\emptyset}.$$

**Proposition 5.2.** *There exists a maximal ideal $\mathfrak{m}_{Q_n} \subseteq \mathbf{T}_{Q_n,W(k)}$ such that*

$$\mathbf{T}_{\mathfrak{m}_{Q_n}} \cong \mathbf{T}_{Q_n},$$

*where $R_\mathfrak{a}$ denotes the completion of the ring $R$ at $\mathfrak{a}$. Moreover, this isomorphism sends the Hecke operator $T_n \in \mathbf{T}_{\mathfrak{m}_{Q_n}}$ to the tuple $T_n$ of coefficients $(a_n(f_i))_{f_i \in \mathfrak{F}}$ in $\mathbf{T}_{Q_n}$. Similarly, there exists a maximal ideal $\mathfrak{m}_\emptyset \subseteq \mathbf{T}_{\emptyset,W(k)}$ such that*

$$\mathbf{T}_\emptyset \cong \mathbf{T}_{\mathfrak{m}_\emptyset},$$

*and which preserves the Hecke operators in this fashion.*

We begin by proving a lemma describing the structure of the Hecke algebras $\mathbf{T}_{Q_n,W(k)}$ and $\mathbf{T}_{\emptyset,W(k)}$. This is similar to a fact proved in the survey article of Darmon, Diamond, and Taylor [DDT97, Lemma 4.4], but we drop the hypothesis that $K$ contain the coefficients of the newform $f$ while assuming that the level is squarefree.

**Lemma 5.3.** *Suppose that $N$ is squarefree. Let $\mathbf{T}_{N,\mathbf{Z}}$ denote the Hecke algebra associated to $H^1(X_1(N), \mathbf{Z})^-$, and denote $\mathbf{T}_{N,R} = \mathbf{T}_{N,\mathbf{Z}} \otimes R$ for a ring $R$. We have a product decomposition*

$$\mathbf{T}_{N,F(k)} = \prod_{[f]} K_f[\{u_q\}_{\frac{N}{N_f}}]/(u_q^2 - a_p u_q + q\psi_f(q))_{q|\frac{N}{N_f}}, \tag{5.3}$$

*where $[f]$ ranges over $G_{F(k)}$-equivalence classes of newforms in $\mathbf{P}H^1(X_1(N), \overline{F(k)})^-$.*

*Proof.* Given a newform $f$, we define $S_f$ to be the $F(k)$-vector space with basis

$$\left\{ f(m\tau) : m \,\middle|\, \frac{N}{N_f} \right\},$$

so that

$$\dim_{F(k)} S_f = \sigma_0\left(\frac{N}{N_f}\right). \tag{5.4}$$

We claim we obtain a surjective map

$$\mathbf{T}_{N,F(k)} \to K_f[\{u_q\}_{q|\frac{N}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{N}{N_f}}$$

by sending $T_n$ to $a_n(f)$ for $(n, \frac{N}{N_f}) = 1$ and $U_q$ for $q|\frac{N}{N_f}$ to $u_q$. The surjectivity is automatic from the definition of $K_f$, so we need only to check that $U_q$ satisfies the given characteristic polynomial.

Note that $U_q$ acts on the space generated by $f(\tau)$ and $f(q\tau)$ by Fact 2.10, and $U_q$ differs from the operator $T_q$ of the Hecke algebra acting on $H^1(X_1(N_f), \overline{\mathbf{Q}}_p)^-$ by the term

$$\sum_{n=0}^{\infty} q a_{\frac{n}{q}}(\langle q\rangle\, f)\underline{q}^n = q\psi_f(q)\sum_{n=0}^{\infty} a_n(f)\underline{q}^{nq} = q\psi_f(q) f(q\tau),$$

where we have used $\underline{q} = \exp(2\pi i\tau)$ to distinguish this from the prime $q$. Also note that $U_q$ acts on $f(q\tau)$ by sending it to

$$\sum_{n=0}^{\infty} a_{nq}(f(q\tau))\underline{q}^n = \sum_{n=0}^{\infty} a_n(f(\tau))\underline{q}^n = f(\tau).$$

Thus the matrix of $U_q$ acting on $f$ is

$$\begin{pmatrix} a_q & 1 \\ -q\psi_f(q) & 0 \end{pmatrix},$$

which has characteristic polynomial $u_q^2 - a_q u_q + q\psi_f(q)$.

Moreover, for any $G_{F(k)}$-conjugate $g$, we just compose the map just constructed with the automorphism taking $f$ to $g$, which acts both on the coefficient field $K_f$ and the coefficients of the polynomial $u_q^2 - a_q u_q + q\psi_f(q)$, so we obtain a map into the same image ring. We also note that $[K_f : F(k)]$ is the number of $G_{F(k)}$-conjugates of $f$.

We define

$$\mathbf{T}_{F(k),f} \subseteq \mathrm{End}(S_f)$$

to be the image of $\mathbf{T}_{N,F(k)}$. The argument above shows that

$$K_f[\{u_q\}_{q|\frac{N}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{N}{N_f}} \cong \mathbf{T}_{F(k),f}.$$

We observe that the map

$$\mathbf{T}_{Q_n,F(k)} \to \prod_{[f]} \mathbf{T}_{F(k),f}$$

is injective, since the action of $\mathbf{T}_{F(k)}$ is faithful, and if an element of $\mathbf{T}_{F(k)}$ annihilates $f$, it annihilates all of the $G_{F(k)}$-conjugates of $f$ as well.

We finally observe that

$$\begin{aligned}
\dim_{F(k)} \mathbf{T}_{N,F(k)} &= \dim_{\overline{F(k)}} \mathbf{T}_{N,\overline{F(k)}} = \dim_{\overline{F(k)}} H^1(X_1(N), \overline{F(k)})^- = \sum_f \dim_{F(k)} S_f \\
&= [K_f : F(k)] \sum_{[f]} \dim_{F(k)} S_f = [K_f : F(k)] \sum_{[f]} \sigma_0 \left(\frac{N}{N_f}\right) \\
&= \dim_{F(k)} \prod_{[f]} \mathbf{T}_{F(k),f}
\end{aligned}$$

by Fact 2.12 for the second equality, Fact 2.10, the discussion in Section 2.2.2 comparing the space $H^1(\cdot,\cdot)^-$ with the space $S_2(\cdot,\cdot)$ together with Fact 2.10 for the third, the earlier remark regarding the number of $G_{F(k)}$-conjugates of $f$ for the fourth, the equation (5.4) for the fifth, and the observation that

$$2^{\#\{u_q\}_{q|\frac{N}{N_f}}} = \sigma_0\left(\frac{N}{N_f}\right)$$

for squarefree $N$ for the sixth. Thus we obtain the isomorphism (5.3).

□

We define the ideals

$$\begin{aligned}
\mathfrak{m}_{Q_n} = \big(\pi, &\left\{T_r - \operatorname{Tr}\overline{\rho}(\mathrm{Frob}_r^{-1})\right\}_{r\nmid pq_nT}, \\
&\left\{\langle r\rangle - \psi'(r)\right\}_{r\nmid pq_nT}, U_p - 1, \left\{U_t - \operatorname{Tr}\overline{\rho}^{I_p}(\mathrm{Frob}_t^{-1})\right\}_{t|T}, \left\{U_q - \alpha_q\right\}_{q\in Q_n}\big)
\end{aligned} \tag{5.5}$$

and

$$\begin{aligned}
\mathfrak{m}_{\emptyset} = \big(\pi, &\left\{T_r - \operatorname{Tr}\overline{\rho}(\mathrm{Frob}_r^{-1})\right\}_{r\nmid pq_nT}, \\
&\left\{\langle r\rangle - \psi'(r)\right\}_{r\nmid pq_nT}, U_p - 1, \left\{U_t - \operatorname{Tr}\overline{\rho}^{I_p}(\mathrm{Frob}_t^{-1})\right\}_{t|T}\big).
\end{aligned} \tag{5.6}$$

Also observe that we write $\alpha_q$ to mean an arbitrary lift of $\alpha_q \in k$ and similarly for $\operatorname{Tr}\overline{\rho}(\mathrm{Frob}_r^{-1})$ and $\operatorname{Tr}\overline{\rho}^{I_p}(\mathrm{Frob}_t^{-1})$. Since $\pi \in \mathfrak{m}_{Q_n}$ and $\pi \in \mathfrak{m}_\emptyset$ the choice of lift does not change $\mathfrak{m}_{Q_n}$ or $\mathfrak{m}_\emptyset$.

**Corollary 5.4.** *We have a product decomposition*

$$(\mathbf{T}_{Q_n,F(k)})_{\mathfrak{m}_{Q_n}} = \prod_{[f]} \left(K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}}\right)_{\mathfrak{m}_{Q_n}}, \tag{5.7}$$

*where $[f]$ ranges over $G_{F(k)}$-equivalence classes of newforms in $\mathbf{P}H^1(X_1(pq_nT), \overline{F(k)})^-_{\mathfrak{m}_{Q_n}}$.*

*Similarly, we have*

$$(\mathbf{T}_{\emptyset,F(k)})_{\mathfrak{m}_\emptyset} = \prod_{[f]} K_f, \tag{5.8}$$

*where $[f]$ ranges over $G_{F(k)}$-equivalence classes of newforms in $\mathbf{P}H^1(X_1(pT), \overline{F(k)})^-_{\mathfrak{m}_\emptyset}$.*

*Proof.* Notice that any functions $f$ such that $\rho_f$ lifts $\overline{\rho}$ have $T$ dividing the level since $\rho$ is ramified at primes dividing $T$. Similarly, $f$ has $p$ dividing the level since the condition $U_p - 1$ forces the representation $f$ to be ordinary. Lemma 5.3 then shows that (5.8) holds. Equation (5.7) follows immediately from Lemma 5.3, though we remark that the same argument shows that the $q$ can be taken to be elements of $Q_n$.

□

*Proof of Proposition 5.2.* By Corollary 5.4, we have

$$\mathbf{T}_{\mathfrak{m}_{Q_n}} = (\mathbf{T}_{Q_n,W(k)})_{\mathfrak{m}_{Q_n}} \hookrightarrow \prod_{[f]} \left( K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}} \right)_{\mathfrak{m}_{Q_n}}$$

and

$$\mathbf{T}_{\mathfrak{m}_\emptyset} = (\mathbf{T}_{\emptyset,W(k)})_{\mathfrak{m}_\emptyset} \hookrightarrow \prod_{[f]} K_f.$$

We can allow redundant choices of $f$ to obtain injections

$$\mathbf{T}_{\mathfrak{m}_{Q_n}} \hookrightarrow \prod_{f} \left( K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}} \right)_{\mathfrak{m}_{Q_n}}$$

and

$$\mathbf{T}_{\mathfrak{m}_\emptyset} \hookrightarrow \prod_{f} K_f.$$

We aim to simplify the expressions $\left( K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}} \right)_{\mathfrak{m}_{Q_n}}$. We break into cases.

- The newform $f$ has $q \nmid N_f$: By Fact 2.14, item (1), $\rho_f$ is unramified at $q$ and the characteristic polynomial of $\rho_f(\mathrm{Frob}_q^{-1})$ is $X^2 - a_q X + q\psi_f(q)$. In particular, the roots of this polynomial are residually $\alpha_q, \beta_q$ where $\alpha_q \neq \beta_q$. Note that this characteristic polynomial is also the characteristic polynomial $u_q^2 - a_q u_q + q\psi_f(q)$ of $U_q$. By Hensel's lemma, this quadratic factors as $(X - \widetilde{\alpha}_q)(X - \widetilde{\beta}_q)$ where $\widetilde{\alpha}_q$ reduces to $\alpha_q$ and $\widetilde{\beta}_q$ reduces to $\beta_q$ modulo $p$. In particular, we obtain the isomorphism

$$K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}} \cong K_f \oplus K_f$$

  where in the first factor $K_f$, $U_q = \widetilde{\alpha}_q$, and in the second, $U_q = \widetilde{\beta}_q$. Since $U_q - \alpha_q \in \mathfrak{m}_{Q_n}$, the second factor disappears upon localization.

- The newform $f$ has $q|N_f$ but $q \nmid N_{\psi_f}$: Fact 2.14, item (6) shows that

$$\rho|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \chi & * \\ 0 & \chi\epsilon^{-1} \end{pmatrix}$$

  for some character $\chi$, but $\epsilon^{-1}(\mathrm{Frob}_q^{-1}) = q \equiv 1 \bmod p$, so $\overline{\rho}_f|_{G_{\mathbf{Q}_q}}(\mathrm{Frob}_q^{-1})$ does not have distinct eigenvalues. Thus $\rho_f$ cannot lift $\overline{\rho}$, so we exclude this case.

- The newform $f$ has $q|N_f$ and $q|N_{\psi_f}$: Fact 2.14, item (6) shows that

$$\rho|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1}\epsilon^{-1}\psi_f^{-1} \end{pmatrix} = \chi_1 \oplus \chi_2,$$

  where $\chi$ is an unramified character satisfying $\chi(\mathrm{Frob}_q^{-1}) = a_q$. Note that $\epsilon(q) \equiv 1 \bmod p$, so

$$\chi_2|_{I_{G_{\mathbf{Q}_q}}} = \chi^{-1}\epsilon^{-1}\psi_f^{-1}|_{I_{G_{\mathbf{Q}_q}}} = \psi_f^{-1}|_{G_{\mathbf{Q}_q}}$$

  is ramified, since $q|N_{\psi_f}$. Thus, since $U_q(f)$ is the eigenvalue of $\mathrm{Frob}_q^{-1}$ on the unramified subspace, $U_q - \alpha_q \in \mathfrak{m}_{Q_n}$, and the roots of the reduction of the characteristic polynomial $u_q^2 - a_q u_q + q\psi_f(q)$ modulo $\pi$ are in $k$ by assumption, the ring $K_f[\{u_q\}_{q|\frac{pq_nT}{N_f}}]/(u_q^2 - a_q u_q + q\psi_f(q))_{q|\frac{pq_nT}{N_f}}$ collapses to $K_f$ after localization.

Thus we have

$$\mathbf{T}_{\mathfrak{m}_{Q_n}} \hookrightarrow \prod_f K_f \quad \text{and} \quad \mathbf{T}_{\mathfrak{m}_\emptyset} \hookrightarrow \prod_f K_f.$$

Since $\mathbf{T}_{\mathfrak{m}_{Q_n}}$ and $\mathbf{T}_{\mathfrak{Q}_\mathfrak{n}}$ are finite $W(k)$-algebras,

$$\mathbf{T}_{\mathfrak{m}_{Q_n}} \hookrightarrow \mathfrak{O}_f$$

and

$$\mathbf{T}_{\mathfrak{m}_\emptyset} \hookrightarrow \prod_f \mathfrak{O}_f.$$

It follows from the definitions that the image of $T_n \in \mathbf{T}_{\mathfrak{m}_{Q_n}}$ or $\mathbf{T}_{\mathfrak{m}_\emptyset}$ matches the element $T_n \in \mathbf{T}_{Q_n}$ or $\mathbf{T}_\emptyset$ for $n$ not dividing $pT$ or $pq_nT$, respectively. Similarly, the image of $U_p$ is the same in both cases. To see that these rings are isomorphic, it suffices to show that these elements generate the image of $\mathbf{T}_{\mathfrak{m}_{Q_n}}$ and $\mathbf{T}_{\mathfrak{m}_\emptyset}$ in $\prod_f \mathfrak{O}_f$.

Recall from Proposition 5.1 that the representations $\widetilde{\rho}_{Q_n}^{\mathrm{mod}}$ and $\widetilde{\rho}_\emptyset^{\mathrm{mod}}$ can be conjugated so they are valued in $\mathbf{T}_{Q_n}$ and $\mathbf{T}_\emptyset$, respectively. We show that each of the Hecke operators generating $\mathbf{T}_{\mathfrak{m}_{Q_n}}$ or $\mathbf{T}_{\mathfrak{m}_\emptyset}$ is contained in $\mathbf{T}_{Q_n}$ or $\mathbf{T}_\emptyset$, respectively.

- The diamond operators $\langle d \rangle$: Since $\langle r \rangle = r^{-1} \det \rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_r^{-1})$ is contained in $\mathbf{T}_{Q_n}$ and similarly for $\mathbf{T}_\emptyset$ for all prime $r$ not dividing the level, the Dirichlet theorem on primes in an arithmetic progression implies that all $\langle d \rangle$ are in $\mathbf{T}_{Q_n}$ and $\mathbf{T}_\emptyset$.

- The operators $T_r$ for $r$ not dividing the level: We find $T_r = \operatorname{Tr}\rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_r^{-1}) \in \mathbf{T}_{Q_n}$ and similarly for $\mathbf{T}_\emptyset$.

- The operators $U_t$ for $t|T$: We break further into two subcases.

  - The representation $\overline{\rho}$ is ramified as in (4.1): We have

  $$\overline{\rho}|_{G_{\mathbf{Q}_t}} \sim \begin{pmatrix} \chi & * \\ 0 & \chi\epsilon^{-1} \end{pmatrix}$$

  where $\chi(\mathrm{Frob}_t^{-1}) = a_t$. Recall the hypothesis that $t \nmid p-1$. This implies that $\chi(\mathrm{Frob}_t^{-1}) \neq \epsilon^{-1}(\mathrm{Frob}_t^{-1})\chi(\mathrm{Frob}_t^{-1})$. In particular, the characteristic polynomial of $\rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_t^{-1})$ splits over $k$ with distinct roots, so by Hensel's lemma, the roots of the characteristic polynomial of $\rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_t^{-1})$ or $\rho_\emptyset^{\mathrm{mod}}(\mathrm{Frob}_t^{-1})$ lie in $\mathbf{T}_{Q_n}$ or $\mathbf{T}_\emptyset$, respectively. But the root corresponding to the unramified character $\chi(\mathrm{Frob}_t^{-1})$ is the image of $U_t$ from $\mathbf{T}_{\mathfrak{m}_{Q_n}}$ or $\mathbf{T}_{\mathfrak{m}_\emptyset}$, by definition.

  - The representation $\overline{\rho}$ is ramified as in (4.2): We have

  $$\overline{\rho}|_{G_{\mathbf{Q}_t}} \sim \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$$

  with $\chi_1$ unramified and $\chi_2$ ramified. Thus we can choose a geometric Frobenius lift $\mathrm{Frob}_t^{-1}$ such that $\chi_1(\mathrm{Frob}_t^{-1}) \neq \chi_2(\mathrm{Frob}_t^{-1})$. In particular, since by assumption the eigenvalues of the matrix $\rho(\mathrm{Frob}_t^{-1})$ are in $k$, the characteristic polynomial splits over $k$ and has distinct roots. We apply the same argument as in the preceding case to see that $U_t$ lies in $\mathbf{T}_{Q_n}$ or $\mathbf{T}_\emptyset$.

- The operators $U_q$ for $q \in Q_n$: We apply the argument in the previous two cases, recalling that the characteristic polynomial of $\overline{\rho}(\mathrm{Frob}_q^{-1})$ has distinct roots $\alpha_q, \beta_q$ in $k$.

Thus in fact $\mathbf{T}_{Q_n} \cong \mathbf{T}_{\mathfrak{m}_{Q_n}}$ and $\mathbf{T}_\emptyset \cong \mathbf{T}_{\mathfrak{m}_\emptyset}$.

□

We conclude that certain diamond operators are trivial as elements of $\mathbf{T}_{Q_n}$.

**Corollary 5.5.** *The morphism*

$$(\mathbf{Z}/q_n\mathbf{Z})^\times \to \mathbf{T}_{Q_n}^\times \subseteq \mathrm{End}(H^1(\Gamma_1(pq_nT), W(k))^-_{\mathfrak{m}_{Q_n}})$$

*defined by restricting the map* $(\mathbf{Z}/pq_nT\mathbf{Z})^\times \overset{d\mapsto\langle d\rangle}{\to} \mathbf{T}_{Q_n}^\times$ *to the subgroup* $(\mathbf{Z}/q_n\mathbf{Z})^\times$ *factors through the quotient homomorphism*

$$(\mathbf{Z}/q_n\mathbf{Z})^\times \twoheadrightarrow \Delta_{Q_n}.$$

*Proof.* Let $H = \ker\left((\mathbf{Z}/q_n\mathbf{Z})^\times \twoheadrightarrow \Delta_{Q_n}\right)$. We need to show that for $d \in H$, we have $\langle d \rangle = 1$. We first note that $\langle d \rangle - 1 \in \mathfrak{m}_{Q_n}$ for all $d \in (\mathbf{Z}/q_n\mathbf{Z})^\times$, since the residual representation is unramified at primes in $Q_n$. Thus

$$\sum_{d \in H} \langle d \rangle \notin \mathfrak{m}_{Q_n},$$

since $\#H$ is prime to $p$. For $d' \in H$, we have

$$(\langle d' \rangle - 1) \sum_{d \in H} \langle d \rangle = 0,$$

which implies $\langle d \rangle' - 1 = 0$ by the invertibility of $\sum_{d \in H} \langle d \rangle$.

□

We will use $\eta_{Q_n} : \Delta_{Q_n} \to \mathbf{T}_{Q_n}^\times$ to denote the homomorphism obtained from Corollary 5.5.

Suppose that $\mathfrak{O}'_K \subseteq \mathfrak{O}_K$ is the subring of a DVR with residue field that is finite over $k$ obtained by taking elements that reduce to $k$ under reduction by the maximal ideal $\mathfrak{m}_K$. We will say that a map $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K)$ is modular if the composition $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K) \hookrightarrow \mathrm{GL}_2(\mathfrak{O}_K)$ is modular.

**Proposition 5.6.** *Suppose that $\mathfrak{O}'_K \subseteq \mathfrak{O}_K$ as before. Then*

$$\mathrm{Hom}_{W(k)}(\mathbf{T}_\emptyset, \mathfrak{O}'_K) \cong \left\{ \begin{array}{c|l} & \rho \textit{ satisfies} \\ \textit{strict equivalence classes of} & \;1.\ \rho \textit{ lifts } \overline{\rho} \\ \textit{representations} & \;2.\ \rho \textit{ is minimally ramified for } \ell \neq p \\ \rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathfrak{O}'_K) & \;3.\ \det \rho \equiv \psi \\ & \;4.\ \rho \textit{ is modular} \end{array} \right\}. \tag{5.9}$$

*Proof.* We begin by studying morphisms out of $\mathbf{T}_\emptyset$.

**Claim 5.7.** *Suppose that $\mathfrak{O}'_K \subseteq \mathfrak{O}_K$ as before. Then a map in $\mathrm{Hom}_{W(k)}(\mathbf{T}_\emptyset, \mathfrak{O}_K)$ sends $T_n \mapsto a_n(f)$ for some unique newform $f \in H^1(X_1(pT), W(k))^-$ and all $n$.*

*Proof.* Recall that $\mathbf{T}_\emptyset \cong \mathbf{T}_{\mathfrak{m}_\emptyset}$. Given a $W(k)$-homomorphism $\mathbf{T}_{\mathfrak{m}_\emptyset} \to \mathfrak{O}'_K$ in our category, the coefficient ring $W(k)$ must be preserved, so the intersection of the kernel with the coefficient ring is $(0)$.

We compose with the injection $\mathfrak{O}'_K \hookrightarrow K$ and localize $\mathbf{T}_{\mathfrak{m}_\emptyset}$ by adjoining an inverse to the uniformizer of $W(k)$ to obtain a homomorphism

$$\mathbf{T}_{\mathfrak{m}_\emptyset, K} = \mathbf{T}_{\mathfrak{m}_\emptyset} \otimes K \to K.$$

Let the maximal ideal $\mathfrak{p} \subseteq \mathbf{T}_{\mathfrak{m}_\emptyset, K}$ be the kernel of this homomorphism. The ring $\mathbf{T}_{\mathfrak{m}_\emptyset, K}$ acts faithfully on $H^1(X_1(pT), W(k))^-_{\mathfrak{m}_\emptyset} \otimes K = H^1(X_1(pT), K)^-_{\mathfrak{m}_\emptyset}$, so the localization $H^1(X_1(pT), K)^-_{\mathfrak{p}}$ is nonzero.

Take any eigenform $f \in H^1(X_1(pT), K)^-_{\mathfrak{p}}$, and let $(\mathbf{T}_{\mathfrak{m}_\emptyset,K})_{\mathfrak{p}} f$ be the space it generates. Observe that the determinant condition forces $p$ to divide the level of $f$ and the the inclusion of the $U_t - a_t$ terms in $\mathfrak{m}_\emptyset$ implies that the primes $t|T$ divide the level of $f$ as well. Thus $N_f = pT$.

We denote again by $\mathfrak{p}$ the maximal ideal of $(\mathbf{T}_{\mathfrak{m}_\emptyset,K})_{\mathfrak{p}}$. We must have $\mathfrak{p}f \neq (\mathbf{T}_{\mathfrak{m}_\emptyset,K})_{\mathfrak{f}} g$, else $f = 0$ by Nakayama's lemma. Note that the image of each $T_r \in \mathbf{T}_{\mathfrak{m}_\emptyset,K}$ for $r \nmid pT$ under the homomorphism $\mathbf{T}_{\mathfrak{m}_\emptyset,K} \to K$ is some element $a_r \in K$. Then $T_r - a_r$ maps to 0, so it is an element of $\mathfrak{p}$. On the other hand, $f$ is an eigenform for $r$, so $(T_r - a_r)f \in Kf$. Since $\mathfrak{p} \cap K = (0)$, we must have $T_r f = a_r f$. In particular, $a_r = a_r(g)$ for all primes $r$ not dividing $pT$. By multiplicativity, if we define $a_n$ to be the image of $T_n$ where $(n, pT) = 1$, we have $a_n = a_n(f)$, as needed. By the discussion in Section 2.2.2, since $N_f = pT$, this implies that $f$ is an eigenfunction for the full Hecke algebra.

$\square$

Given a morphism $r : \mathbf{T}_\emptyset \to \mathfrak{O}'_K$, we obtain a representation $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K)$ by composition of $\rho^{\mathrm{mod}}_\emptyset$ with the projection $\mathrm{GL}_2(\mathbf{T}_\emptyset) \to \mathrm{GL}_2(\mathfrak{O}'_K)$. Form the composition $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K) \hookrightarrow \mathrm{GL}_2(\mathfrak{O}_K)$. Since the traces of $\rho^{\mathrm{mod}}_\emptyset(\mathrm{Frob}_r^{-1})$ are $T_r$ for all $r \nmid pT$, and by the Čebotarev density theorem, the elements $\mathrm{Frob}_r^{-1}$ with $r \nmid pT$ are dense in $G_{\mathbf{Q}}$, we find from Claim 5.7 that $\mathrm{Tr}\,\rho$ agrees with $\mathrm{Tr}\,\rho_f$ on $G_{\mathbf{Q}}$ for the newform $f$ associated to $r$. Since $\rho_f$ is absolutely irreducible by Fact 2.14, the representations are equivalent. We next claim that $\rho$ has the properties described in (5.9). Property (1) follows from the isomorphism $\mathbf{T}_\emptyset \cong \mathbf{T}_{\mathfrak{m}_\emptyset}$ and properties (4) and (5) follow from the definition of $\mathbf{T}_\emptyset$ and $\rho^{\mathrm{mod}}_\emptyset$. Fact 2.14 immediately implies property (2). Moreover, Fact 2.14, item (6) also implies property (3), since the two possible forms for $\rho_f|_{I_{\mathbf{Q}_t}}$ for $t|T$ are exactly the two types of minimal ramification cases defined in Section 4.1.

Conversely, given a modular representation $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K)$, again form the composition $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K) \to \mathrm{GL}_2(\mathfrak{O}_K)$. From the definition of a modular representation, we are given an newform $f$ of level dividing $pT$ with representation $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_f)$ and character $\psi_f = \psi$ lifting $\overline{\rho}$, where $\mathfrak{O}_f$ is the ring of integers of the field $K_f/K$ generated over $K$ by the coefficients of $f$. We use the morphism $\lambda_f : \mathbf{T}_\emptyset \to \mathfrak{O}_K$ defined by projection of $\mathbf{T}_\emptyset \subseteq \widetilde{\mathbf{T}}_\emptyset$ to the factor corresponding to $f$ and embedding into the new ring $\mathfrak{O}_f$, which may be larger than the ring $\mathfrak{O}_f$ generated over $W(k)$ by the coefficients of $f$. Note that a factor corresponding to $f$ exists, as one sees by comparing (5.9) with (5.2). The representation coming from composing $\lambda_f$ with $\rho^{\mathrm{mod}}_\emptyset$ has the same traces at $T_r$ as $\rho_f$ for $r \nmid pT$. By the Čebotarev density theorem, the representations have the same traces everywhere. Since $\rho_f$ is absolutely irreducible by Fact 2.14, it is then equivalent to $\rho \otimes_{\mathfrak{O}_K} \mathfrak{O}_f$.

$\square$

## 5.3 Relating the Families $\{R_{Q_n,\mathrm{ord}}\}$ and $\{\mathbf{T}_{Q_n}\}$

We have the following result.

**Proposition 5.8.** *There exists a natural surjective morphism*

$$R_{Q_n,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_{Q_n}$$

*induced by the universal property of the ring* $R_{Q_n,\mathrm{ord}}$.

*Proof.* We begin by defining a character $D : G_{\mathbf{Q}} \to \mathbf{T}_{Q_n}^{\times}$ via the composition

$$G_{\mathbf{Q}} \twoheadrightarrow \Delta_{Q_n} \xrightarrow{d \mapsto d^{-\frac{1}{2}}} \Delta_{Q_n} \xrightarrow{\eta_{Q_n}} \mathbf{T}_{Q_n}^{\times},$$

where the second map is defined because $\#\Delta_{Q_n}$ is odd.

Define

$$\rho'_{Q_n} = \rho_{Q_n}^{\mathrm{mod}} \otimes D : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{T}_{Q_n}).$$

Note that each form $f \in \mathfrak{F}_n$ has $p||N(\rho)$, since $p$ divides the conductor of $\psi$. Since $U_p - 1 \in \mathfrak{m}_{Q_n}$, we must have $a_p(f) \equiv 1 \bmod \pi$, where $\pi$ is a uniformizer for $W(k)$. In particular, $a_p$ is a unit in $W(k)$. By Fact 2.14, item (7), we find that $\rho_f$ is ordinary. Thus $\rho'_{Q_n}$ is ordinary as well.

Next observe that by Fact 2.14, the determinant of $\rho_f$ is $\psi_f(r)r$ at $\mathrm{Frob}_r^{-1}$ for $r \nmid N_f p$. Thus $\rho_{Q_n}^{\mathrm{mod}}$ has determinant $\epsilon^{-1}\langle r \rangle$ at $\mathrm{Frob}_r^{-1}$. By the Čebotarev density theorem, $\rho_{Q_n}^{\mathrm{mod}}$ has determinant character $\epsilon^{-1}\langle \cdot \rangle$. Thus $\rho'_{Q_n}$ has determinant $\psi$. In particular, the ambiguity of determinant character in (5.1) is eliminated. Since $\overline{\rho}'_{Q_n} = \overline{\rho}$, we obtain a unique morphism

$$R_{Q_n} \to \mathbf{T}_{Q_n} \tag{5.10}$$

from the universal property.

Note that $\mathbf{T}_{Q_n}$ is generated by the elements $T_r$ for $r \nmid pq_nT$ by definition. But these elements are the images of $\mathrm{Tr}\,\rho'_{Q_n}(\mathrm{Frob}_r^{-1})$. Thus the map (5.10) is surjective.

We next check that the morphism $R_{Q_n} \to \mathbf{T}_{Q_n}$ factors through the local ring $R_{p,\mathrm{ord}}^{\mathrm{loc}}$. For each $f \in \mathfrak{F}_n$, we have a projection $\pi_f : \widetilde{\mathbf{T}}_{Q_n} \to \mathfrak{O}_f$, giving us maps

$$R_p^{\mathrm{loc}} \to R_{Q_n} \twoheadrightarrow \mathbf{T}_{Q_n} \hookrightarrow \widetilde{\mathbf{T}}_{Q_n} \to \mathfrak{O}_f. \tag{5.11}$$

The representation $\rho_{Q_n}^{\mathrm{mod}}$ pushes forward along the homomorphisms $\mathbf{T}_{Q_n} \hookrightarrow \widetilde{\mathbf{T}}_{Q_n} \to \mathfrak{O}_f$ to $\rho_f$, which by the preceding discussion is ordinary. However, we cannot yet conclude that the composition in (5.11) must vanish on $\mathfrak{b} \subseteq R_p^{\mathrm{loc}}$. The ring $\mathfrak{O}_f$ might not even be an object of $\mathbf{DVR}(k)$, since the residue field $k_f$ may potentially be an extension of $k$. Thus we need the following claim.

**Claim 5.9.** *The representation $\rho_f$ can be conjugated such that the image lies in the subgroup $\mathrm{GL}_2(\mathfrak{O}'_f) \subseteq \mathrm{GL}_2(\mathfrak{O}_f)$, where $\mathfrak{O}'_f$ consists of elements of $\mathfrak{O}_f$ whose residue in $k_f$ lies in the subfield $k$.*

*Proof.* By hypothesis, we have $\overline{\rho} \otimes_k k_f \cong \overline{\rho}_f$, so we may write $\overline{\rho}_f$ in a basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ over $k_f$ such that $\overline{\rho}_f = \overline{\rho}$. If we extend $\{\mathbf{e}_1, \mathbf{e}_2\}$ to a basis $\{\widetilde{\mathbf{e}}_1, \widetilde{\mathbf{e}}_2\}$ of $\mathfrak{O}_K^2$, then $\rho_f$ in this basis lifts entries of $k$, and thus has image valued in $\mathrm{GL}_2(\mathfrak{O}'_f)$.

∎

By Claim 5.9, we can replace $\rho_f$ with an equivalent representation that lies in our category, so the composition in (5.11) indeed vanishes on $\mathfrak{b} \subseteq R_p^{\mathrm{loc}}$. Since this is true of each $f \in \mathfrak{F}_n$, the composition

$$R_p^{\mathrm{loc}} \to R_{Q_n} \twoheadrightarrow \mathbf{T}_{Q_n} \hookrightarrow \widetilde{\mathbf{T}}_{Q_n}$$

also vanishes on $\mathfrak{b}$, so in fact the map factors through $R_{Q_n,\mathrm{ord}}$, giving us homomorphisms

$$R_{Q_n} \twoheadrightarrow R_{Q_n,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_{Q_n} \hookrightarrow \widetilde{\mathbf{T}}_{Q_n}.$$

$\square$

## 5.4 Compatibility of $W(k)[\Delta_{Q_n}]$-algebra Structures on $R_{Q_n,\mathrm{ord}}$ and $\mathbf{T}_{Q_n}$

We recall that $R_{Q_n,\mathrm{ord}}$ is a $W(k)[\Delta_{Q_n}]$-algebra via the map $\pi_{Q_n,\mathrm{ord}}$, and similarly for $R^{\square}_{Q_n,\mathrm{ord}}$. Proposition 5.8 then makes $\mathbf{T}_{Q_n}$ into a $W(k)[\Delta_{Q_n}]$-algebra.

We have a second natural $W(k)[\Delta_{Q_n}]$-algebra structure on $\mathbf{T}_{Q_n}$, which is defined using the morphism

$$\eta_{Q_n} : \Delta_Q \overset{d \mapsto \langle d \rangle}{\to} \mathbf{T}_{Q_n}^{\times}$$

obtained from Corollary 5.5.

We will show, in fact, that both of these $W(k)[\Delta_{Q_n}]$-algebra structures on $\mathbf{T}_{Q_n}$ coincide. The main idea behind the argument is to use Fact 2.14 to constrain the structure of each component of the representation $\rho_{Q_n}^{\mathrm{mod}\prime}$ until it meets the conditions described in Claim 5.11. Then $\rho_{Q_n}^{\mathrm{mod}\prime}$ has exactly the same structure as $\rho_{Q_n}$, so it is easy to check that the actions line up correctly.

**Proposition 5.10.** *The maps*

$$\Delta_{Q_n} \overset{\pi_{Q_n,\mathrm{ord}}}{\to} R_{Q_n,\mathrm{ord}}^{\times} \twoheadrightarrow \mathbf{T}_{Q_n}^{\times}$$

*and*

$$\Delta_{Q_n} \overset{\eta_{Q_n}}{\to} \mathbf{T}_{Q_n}^{\times}$$

*are the same.*

*Proof.* Recall from Section 5.1 that $\rho^{\mathrm{mod}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{T}_{Q_n})$ is constructed from representations $\rho_f$ associated to newforms $f \in H^1(X_1(pq_nT), W(k))^-$ such that $\overline{\rho}_f = \overline{\rho}$ and such that the character of $f$ is $\psi'$. Let $\mathfrak{F}_n$ denote the set of such forms $f$. We begin by showing that the representations $\rho_f$ are well-behaved upon restriction to $G_{\mathbf{Q}_q}$ for $q \in Q_n$.

**Claim 5.11.** *For every $f \in \mathfrak{F}_n$ and $q \in Q_n$, we have*

$$\rho_f|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix},$$

*satisfying the following.*

1. *The character* $\chi_1$ *is unramified and satisfies* $\chi_1(\mathrm{Frob}_q^{-1}) \equiv \alpha_q \bmod p$.

2. *The character* $\chi_2$ *satisfies* $\chi_2|_{I_{\mathbf{Q}_q}} = \psi'_f$.

*Proof.* We break into three cases. Let $N_f$ denote the level of $f$ and $N_{\psi_f}$ denote the conductor of $\psi_f$.

- The newform $f$ has $q \nmid N_f$: By Fact 2.14, item (1), $\rho_f$ is unramified at $q$ and the characteristic polynomial of $\rho_f(\mathrm{Frob}_q^{-1})$ is $X^2 - a_qX + q\psi_f(q)$. Using Lemmas 4.22 and 4.23, we can write $\rho_f|_{G_{\mathbf{Q}_q}} \sim \left(\begin{smallmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{smallmatrix}\right)$, where $\chi_1(\mathrm{Frob}_q^{-1}) \equiv \alpha_q \bmod p$. Note that the conductor of $N_{\psi_f}$ cannot have $q$ as a divisor, so $\psi'_f$ is trivial on $\Delta_q$. Thus $\chi_2|_{I_{\mathbf{Q}_q}} = \psi_f'^{-1}$, as both are trivial.

- We can exclude this case by the argument in Proposition 5.2.

- The newform $f$ has $q|N_f$ and $q|N_{\psi_f}$: Fact 2.14, item (6) shows that

  $$\rho|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1}\epsilon^{-1}\psi_f'^{-1} \end{pmatrix},$$

  where $\chi$ is an unramified character satisfying $\chi(\mathrm{Frob}_q^{-1}) = a_q$. Note that $\epsilon^{-1}(\mathrm{Frob}_q^{-1}) \equiv 1 \bmod p$, so

  $$\chi_2|_{I_{G_{\mathbf{Q}_q}}} = \chi^{-1}\epsilon^{-1}\psi_f'^{-1}|_{I_{G_{\mathbf{Q}_q}}} = \psi_f'^{-1}|_{I_{\mathbf{Q}_q}}$$

  is ramified, since $q|N_{\psi_f}$. Finally, note that $\chi(\mathrm{Frob}_q^{-1}) \equiv \alpha_q \bmod p$ is forced by the fact that $U_q - \alpha_q \in \mathfrak{m}_{Q_n}$ (so that $\alpha_q$ is the reduction of the *unramified* character).

$\square$

From the definition of the diamond operators in $\mathbf{T}_{Q_n}$ as tuples $(\psi_f(d))_{f \in H^1(X_1(pq_nT), W(k)^-_{\mathfrak{m}_{Q_n}})}$, we obtain the following corollary. The proof is more subtle than one might expect, because the change of basis provided by applying Claim 5.11 to each form $f \in \mathfrak{F}_n$ may take values in the ring $\widetilde{\mathbf{T}}_{Q_n}$ of Section 5.1.

**Corollary 5.12.** *We have*

$$\rho_{Q_n}^{mod}|_{G_{\mathbf{Q}_q}} \sim \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$$

*satisfying the following.*

1. *The character* $\chi_1$ *is unramified and satisfies* $\chi_1(\mathrm{Frob}_q^{-1}) \equiv \alpha_q \bmod p$.

2. *The character* $\chi_2$ *satisfies* $\chi_2|_{I_{\mathbf{Q}_q}} = \langle \cdot \rangle$.

*Note that* $\sim$ *indicates* $\mathrm{GL}_2(\mathbf{T}_{Q_n})$*-conjugation.*

*Proof.* It is immediate from Claim 5.11 that $\rho_{Q_n}^{\mathrm{mod}}|_{G_{\mathbf{Q}_q}}$ takes the form $\left(\begin{smallmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{smallmatrix}\right)$ when written in some basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ valued in $\widetilde{\mathbf{T}}_{Q_n}$. In particular, it does not follow that the characters $\chi_1$ and $\chi_2$ are $\mathbf{T}_{Q_n}$-valued. However, we can prove that it suffices to conjugate by an element of $\mathrm{GL}_2(\mathbf{T}_{Q_n})$.

First note that the determinant and trace of $\rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_q^{-1})$ are $\mathbf{T}_{Q_n}$-valued. By Lemma 4.22, we can choose an element of $\mathrm{GL}_2(\mathbf{T}_{Q_n})$ to conjugate $\rho_{Q_n}^{\mathrm{mod}}(\mathrm{Frob}_q^{-1})$ into the form $\left(\begin{smallmatrix} \widetilde{\alpha}_q & 0 \\ 0 & \widetilde{\beta}_q \end{smallmatrix}\right)$, where $\widetilde{\alpha}_q$ lifts $\alpha_q$ and $\widetilde{\beta}_q$ lifts $\beta_q$. Lemma 4.23 shows that $\rho_{Q_n}^{\mathrm{mod}} = \left(\begin{smallmatrix} \chi_1' & 0 \\ 0 & \chi_2' \end{smallmatrix}\right)$ when written in this basis. Since we know already that $\rho_{Q_n}^{\mathrm{mod}} = \chi_1 \oplus \chi_2$, and $\chi_1 \neq \chi_2$ (since they differ on $\mathrm{Frob}_q^{-1}$), we must have $\chi_1' = \chi_1$ and $\chi_2' = \chi_2$ or $\chi_2' = \chi_1$ and $\chi_1' = \chi_2$. In the latter case, we can conjugate by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which is $\mathbf{T}_{Q_n}$-valued. The characters $\chi_1$ and $\chi_2$ are thus $\mathbf{T}_{Q_n}$-valued and satisfy the conditions of the claim.

□

By Corollary 5.12, we find that

$$\rho_{Q_n}^{\mathrm{mod}} \otimes D \sim \begin{pmatrix} \chi_\alpha & 0 \\ 0 & \chi_\beta \end{pmatrix}$$

where $\overline{\chi}_\alpha = \alpha_q$, $\overline{\chi}_\beta = \beta_q$,

$$\chi_\alpha|_{I_{\mathbf{Q}_q}} = \langle\cdot\rangle^{-\frac{1}{2}}, \quad \text{and} \quad \chi_\beta|_{I_{\mathbf{Q}_q}} = \langle\cdot\rangle^{\frac{1}{2}}.$$

Recall from Proposition 4.21 that

$$\rho_{Q_n} \sim \begin{pmatrix} \xi & 0 \\ 0 & \psi\xi^{-1} \end{pmatrix}$$

where $\overline{\xi}(\mathrm{Frob}_q^{-1}) = \alpha_q$ and $\overline{\psi}(\mathrm{Frob}_q^{-1})\overline{\xi}(\mathrm{Frob}_q^{-1})^{-1} = \beta_q$. Recall also that the morphism $\pi_{Q_n} : \Delta_{Q_n} \to R_{Q_n,\mathrm{ord}}$ is defined via the map $\xi_{Q_n}^{-2} = \xi^{-2}$. Let $f : R_{Q_n,\mathrm{ord}} \to \mathbf{T}_{Q_n}$ be the morphism defined in Proposition 5.8. Then $f(\xi) = \chi_\alpha$ and $f(\psi\xi^{-1}) = \chi_\beta$. Thus, for $d \in \Delta_q$, we have

$$f(\pi_{Q_n}(d)) = \chi_\alpha(d)^{-2} = (\langle\cdot\rangle^{-\frac{1}{2}})^{-2} = \langle\cdot\rangle,$$

which is exactly the map $\eta_{Q_n}$.

□

## 5.5 Relationship of $S_{Q_n}$ with $S_\emptyset$

By Proposition 5.8, the spaces $S_{Q_n}$ and $S_\emptyset$ have the structure of $R_{Q_n,\mathrm{ord}}$-module and $R_{\emptyset,\mathrm{ord}}$-module, respectively. Using the clean description of the action of $\Delta_{Q_n}$ defined in Section 5.4 via the map $\eta_{Q_n}$, we will be able to see transparently the augmentation ideal $\mathfrak{a}_{Q_n}$ as it acts on $S_{Q_n}$. With this in hand, we will be able to prove the following analogue of the statement

$$R_{Q_n,\mathrm{ord}}/\mathfrak{a}_{Q_n}R_{Q_n,\mathrm{ord}} = R_{\emptyset,\mathrm{ord}}$$

of Proposition 4.24.

**Proposition 5.13.** *For each $n$, we have*

$$S_{Q_n}/\mathfrak{a}_{Q_n}S_{Q_n} = S_\emptyset.$$

Using the interpretation of modular forms in $M_2(\Gamma)$ as elements of the cohomology group $H^1(Y_\Gamma, \mathbf{Z})$, we will be able to use topological arguments to prove the needed result for the larger spaces of modular forms under consideration. We will then pass to the completion, which will eliminate any extra modular forms not contained in $S_{Q_n}$ and $S_\emptyset$.

We define the group $\Gamma_{Q_n}$ to be the preimage of the product of the maximal subgroup of $(\mathbf{Z}/q_n\mathbf{Z})^\times$ of order prime to $p$ and the trivial subgroup of $(\mathbf{Z}/pT\mathbf{Z})^\times$ under the morphism

$$\Gamma_0(pq_nT) \to (\mathbf{Z}/pq_nT\mathbf{Z})^\times \cong (\mathbf{Z}/q_n\mathbf{Z})^\times \times (\mathbf{Z}/pT\mathbf{Z})^\times$$

induced by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \bmod q_n$. We define $\Gamma_{Q_n-} = \Gamma_0(q_n) \cap \Gamma_1(pT)$. Note that $\Gamma_{Q_n}$ is a normal subgroup of $\Gamma_{Q_n-}$.

**Lemma 5.14** ([TW95, Proposition 1])**.** *Let $Y_{Q_n} = Y(\Gamma_{Q_n})$ and $Y_{Q_n-} = Y(\Gamma_{Q_n-})$. Then $H^1(Y_{Q_n}, W(k))^-$ is a free $W(k)[\Delta_{Q_n}]$-module of $W(k)[\Delta_{Q_n}]$-rank equal to the $W(k)$-rank of $H^1(Y_{Q_n-}, W(k))^-$. Moreover,*

$$H^1(Y_{Q_n}, W(k))^-_{\Delta_{Q_n}} = H^1(Y_{Q_n-}, W(k))^-. \tag{5.12}$$

*Proof.* We will begin by proving a property of the groups $\Gamma_{Q_n}$ and $\Gamma_{Q_n-}$ that will allow us to identify the topological cohomology of $Y_{Q_n}$ and $Y_{Q_n-}$ with the group cohomology of $\Gamma_{Q_n}$ and $\Gamma_{Q_n-}$.

**Claim 5.15.** *The groups $\Gamma_{Q_n}$ and $\Gamma_{Q_n-}$ are free and act freely on the upper half plane $\mathfrak{H}$.*

*Proof.* For the second assertion, it suffices to show that $\Gamma_{Q_n}$ and $\Gamma_{Q_n-}$ have no nontrivial elements of finite order. By the explicit enumeration of matrices of $\mathrm{SL}_2(\mathbf{Z})$ of finite order in Diamond and Shurman's text [DS05, Proposition 2.3.3], we find that it suffices to have no matrices of trace $-2, -1, 0$, or $1$. Since $p > 3$, the congruence conditions on $\Gamma_{Q_n}$ and $\Gamma_{Q_n-}$ rule out all matrices with these traces.

Let $\Gamma = \Gamma_{Q_n}$ or $\Gamma_{Q_n-}$. The action of $\Gamma$ on $\mathfrak{H}$ is properly discontinuous since this is true for the action of $\mathrm{SL}_2(\mathbf{Z})$ as well. Since $Y_\Gamma$ is the quotient of $\mathfrak{H}$ by a free and properly discontinuous action by the group $\Gamma$, the group $\Gamma$ is isomorphic to $\pi_1(Y_\Gamma)$. Since the fundamental group of a genus $g$ Riemann surface with at least one point removed is free, we obtain the first assertion.

□

**Claim 5.16.** *We have*

$$H^1(Y_{Q_n}, W(k)) \cong H^1(\Gamma_{Q_n}, W(k)).$$

*The complex conjugation action on $H^1(Y_{Q_n}, W(k))$ corresponds to $\mathbf{c} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$-conjugation on elements of $H^1(\Gamma_{Q_n}, W(k))$.*

*Proof.* Since the action of $\Gamma_{Q_n}$ on $W(k)$ is trivial,

$$H^1(\Gamma_{Q_n}, W(k)) = \mathrm{Hom}(\Gamma_{Q_n}, W(k)) = \mathrm{Hom}(\Gamma_{Q_n}^{\mathrm{ab}}, W(k)),$$

and an element of $\mathrm{Hom}(\Gamma_{Q_n}^{\mathrm{ab}}, W(k))$ is simply a choice of element of $W(k)$ for each of the free generators of $\Gamma_{Q_n}$. Via the identification of $\Gamma_{Q_n}$ with $\pi_1(Y_{\Gamma_{Q_n}})$, we obtain

$$\mathrm{Hom}(\Gamma_{Q_n}^{\mathrm{ab}}, W(k)) \cong \mathrm{Hom}(\pi_1(Y_{\Gamma_{Q_n}})^{\mathrm{ab}}, W(k)) \cong H^1(Y_{\Gamma_{Q_n}}, W(k)),$$

since an element of $H^1(Y_{\Gamma_{Q_n}}, W(k))$ may be defined by choosing an element of $W(k)$ for each of the free generators of $\pi_1(Y_{\Gamma_{Q_n}})^{\mathrm{ab}}$.

For second assertion, recall the definition of the isomorphism $\Gamma_{Q_n} \cong \pi_1(Y_{\Gamma_{Q_n}})$. In particular, $\Gamma_{Q_n}$ acts as the group of deck transformations on the universal cover $\mathfrak{H}$. Fixing a basepoint $y_0$ of $Y_{\Gamma_{Q_n}}$ and a lift $x_0$ of $y_0$ to $\mathfrak{H}$, we associate to $\sigma \in \Gamma_{Q_n}$ the image of the path from $y_0$ to $\sigma(y_0)$. Note that this path is unique up to homotopy equivalence since $\mathfrak{H}$ is simply connected.

The definition of the complex conjugation action on $\mathfrak{H}$ is by the action $w \mapsto -\overline{w}$. We choose the basepoint $x_0 = 2i \in \mathfrak{H}$ to define the isomorphism, since then the image $y_0 \in Y_{\Gamma_{Q_n}}$ is *fixed* under the conjugation action, and we obtain an involution on the *basepointed* homotopy group $\pi_1(Y_{\Gamma_{Q_n}}, y_0)$. Conjugation by $\mathbf{c}$ sends

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}.$$

Under the action $w \mapsto -\overline{w}$ on images of the basepoint $x_0$, we have

$$\frac{az+b}{cz+d} = \frac{a(2i)+b}{c(2i)+d} \mapsto -\frac{a(-2i)+d}{c(-2i)+d} = \frac{az-d}{-cz+d}.$$

In particular, the conjugation action of $\mathbf{c}$ on the group $\Gamma_{Q_n}$ matches the action of complex conjugation as a map $\pi_1(Y_{\Gamma_{Q_n}}, y_0) \to \pi_1(Y_{\Gamma_{Q_n}}, y_0)$, as needed.

□

**Claim 5.17.** *We have*

$$H^1(\Gamma_{Q_n}, W(k)) \cong H^1(\Gamma_{Q_n-}, W(k)[\Delta_Q])$$

*where the action of* $\Gamma_{Q_n-}$ *on* $\Delta_Q$ *is by right multiplication after factoring through the quotient homomorphism* $\Gamma_{Q_n-}/\Gamma_{Q_n} \cong \Delta_{Q_n}$.

*The complex conjugation action on* $H^1(\Gamma_{Q_n-}, W(k)[\Delta_Q])$ *corresponds to* $\mathbf{c}$*-conjugation with trivial action on* $\Delta_{Q_n}$.

*Proof.* By Shapiro's lemma, it suffices to check that $W(k)[\Delta_{Q_n}] \cong \mathrm{Ind}_{\Gamma_{Q_n}}^{\Gamma_{Q_n-}} W(k)$. Recall that as a set, $\mathrm{Ind}_{\Gamma_{Q_n}}^{\Gamma_{Q_n-}} W(k)$ is simply the set of morphisms of sets $\varphi : G \to W(k)$ such that $\varphi(hg) = h\varphi(g)$ for all $h$. Thus a choice of $\varphi$ corresponds exactly to a choice of $\varphi(g_i) \in W(k)$

for each of a set of representatives $\{g_i\}$ for the cosets of $H$ in $G$. By identifying a coset with the corresponding element of $\Delta_{Q_n}$, we obtain an isomorphism $W(k)[\Delta_{Q_n}] \cong \mathrm{Ind}_{\Gamma_{Q_n}}^{\Gamma_{Q_n-}} W(k)$ of *sets*. The $G$-action is defined by $(g\varphi)(g') = \varphi(g'g)$, as needed.

The second assertion is immediate from the proof of Claim 5.16 together with the observation that $\mathbf{c}$-conjugation preserves the $\Gamma_{Q_n}$-cosets in $\Gamma_{Q_n-}$.

□

By the cocycle relation, a cocycle in $Z^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])$ is determined by the images of a set of generators of $\Gamma_{Q_n-}$. Since $\Gamma_{Q_n-}$ is free, say on $m$ generators, a cocycle is exactly determined by the images of the $m$ generators. Thus,

$$Z^1(\Gamma_{Q_n}, W(k)[\Delta_{Q_n}]) \cong W(k)[\Delta_{Q_n}]^m.$$

Next recall from Claim 5.17 that $\mathbf{c}$ acts trivially on $\Delta_{Q_n}$. Thus

$$\mathbf{c}\sigma\mathbf{c}m - m = \mathbf{c}(\sigma m) - m = \sigma m - m,$$

so the action of conjugation on a coboundary is trivial. In particular, $B^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}]) \subseteq Z^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])^+$. So

$$H^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])^- = Z^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])^-$$

is a direct summand of the free module $Z^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])$ and thus projective. Since $W(k)[\Delta_{Q_n}]$ is local, $H^1(\Gamma_{Q_n-}, W(k)[\Delta_{Q_n}])^-$ is then a free $W(k)[\Delta_{Q_n}]$-module.

If we tensor with the field of fractions $F(k)$ of $W(k)$, we obtain

$$H^1(Y_{Q_n}, F(k))_{\Delta_{Q_n}} \cong H^1(Y_{Q_n-}, F(k))$$

since $\Delta_{Q_n}$ is the group of deck transformations of the covering $Y_{Q_n} \to Y_{Q_n-}$. Since complex conjugation commutes with the $\Delta_{Q_n}$-action, we have

$$H^1(Y_{Q_n}, F(k))^-_{\Delta_{Q_n}} \cong H^1(Y_{Q_n-}, F(k))^-$$

as well. Since

$$\begin{aligned} H^1(Y_{Q_n}, W(k))^-_{\Delta_{Q_n}} \otimes_{W(k)} F(k) &= H^1(Y_{Q_n}, F(k))^-_{\Delta_{Q_n}} \cong H^1(Y_{Q_n-}, F(k))^- \\ &= H^1(Y_{Q_n-}, W(k))^- \otimes_{W(k)} F(k), \end{aligned}$$

the $W(k)$ rank of $H^1(Y_{Q_n}, W(k))^-_{\Delta_{Q_n}}$ must be the $W(k)$-rank of $H^1(Y_{Q_n-}, W(k))^-$, as both of these modules are free. In particular, the $W(k)[\Delta_{Q_n}]$-rank of $H^1(Y_{Q_n}, W(k))^-$ is the $W(k)$-rank of $H^1(Y_{Q_n-}, W(k))^-$. The equation (5.12) follows. □

*Proof of Proposition 5.13.* By Lemma 5.14, we have

$$H^1(Y_{Q_n}, W(k))^-_{\Delta_{Q_n}} = H^1(Y_{Q_n-}, W(k))^-.$$

The Hecke algebra $\mathbf{T}_{Q_n}$ acts on $H^1(Y_{Q_n-}, W(k))^-$ by restriction. Localizing both sides at $\mathfrak{m}_{Q_n}$ and noting that $\overline{\rho}$ is irreducible, so that the Galois representations corresponding to Eisenstein series are eliminated by localization, we find that

$$\begin{aligned}(H^1(X_{Q_n}, W(k))^-_{\mathfrak{m}_{Q_n}})_{\Delta_{Q_n}} &= (H^1(Y_{Q_n}, W(k))^-_{\mathfrak{m}_{Q_n}})_{\Delta_{Q_n}} \\ &= H^1(Y_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}} = H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}}.\end{aligned}$$

We finally need to show that

$$(H^1(X_{Q_n}, W(k))^-_{\mathfrak{m}_{Q_n}})_{\Delta_{Q_n}} = H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}} = H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_{Q_n}},$$

where $X_\emptyset$ is the compact Riemann surface assocated to $\Gamma_1(pT)$. We divide the proof into two stages.

**Claim 5.18.** *We have an isomorphism*

$$\left(\bigotimes_{q\in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}\right)_{\mathfrak{m}_{Q_n}} \cong H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}}. \tag{5.13}$$

*Proof.* We define the injection

$$i : \bigotimes_{q\in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-} \hookrightarrow H^1(X_{Q_n-}, W(k))^-$$

to send

$$(x_V)_{V\in 2^{Q_n}} \mapsto \sum_{V\subseteq Q_n} \iota_V(x_V),$$

where $\iota_V$ is the map on $H^1(X_\emptyset, W(k))$ corresponding to the map

$$f(\tau) \mapsto f\left(\tau \prod_{q\in W} q\right)$$

on modular forms and the choice of whether $q \in V \in 2^{Q_n}$ or not indicates a choice of the first or second factor of $H^1(X_\emptyset, W(k))^{\oplus 2}$ corresponding to the prime $q$.

An application of a lemma of Ihara [Iha75] due to Ribet [Rib84] implies that the map $i \otimes k$ is injective, and thus the image of this map is a *direct summand* of $H^1(X_{Q_n-}, W(k))$. In particular, we have the decomposition

$$H^1(X_{Q_n-}, W(k))^- = i\left(\bigotimes_{q\in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}\right) \oplus M.$$

We note that the eigenforms in $M$ must have $q$ dividing the level since

$$i\left(\bigotimes_{q\in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2}\right)$$

is the subspace of the old subspace of $H^1(X_{Q_n-}, W(k))$ coming from level $pT$. The observation in the proof of Claim 5.11 that there are no newforms $f$ with $q$ in the level and trivial character at $q$ such that $\rho_f$ lifts $\overline{\rho}$ implies that $M$ goes to 0 under localization at $\mathfrak{m}_{Q_n}$. As a consequence, we obtain the isomorphism in (5.13).

$\square$

**Claim 5.19.** *We have the isomorphism*

$$H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} \cong H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}}. \tag{5.14}$$

*Proof.* We will apply successive localizations to certain modules at $\mathfrak{m}_\emptyset$ and then $\mathfrak{m}_{Q_n}$. Note that $\mathfrak{m}_{Q_n}$ is generated by adding the operators $U_q - \alpha_q$ to $\mathfrak{m}_\emptyset$.

We consider the map

$$\nu : H^1(X_\emptyset, W(k))^- \to \bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}$$

defined by

$$\nu : x \mapsto \bigotimes_{q \in Q_n} (U_q - \widetilde{\beta}_q)(x, 0) \in \bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-},$$

where $\widetilde{\beta}_q \in \mathbf{T}_{Q_n}$ is the root of the quadratic

$$u_q^2 - T_q u_q + q \langle q \rangle$$

lifting $\beta_q$. Define $\widetilde{\alpha}_q$ similarly. In particular, $U_q - \widetilde{\alpha}_q$ annihilates the image of $\nu$ in each component. We localize at $\mathfrak{m}_\emptyset$ to obtain

$$\nu : H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} \to \bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}_{\mathfrak{m}_\emptyset}.$$

The space $\bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}_{\mathfrak{m}_\emptyset}$ decomposes into a product of eigenspaces under the $U_q$ as

$$\bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}_{\mathfrak{m}_\emptyset} = \bigoplus_{V \subseteq Q_n} \left( H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} \right)_{(U_q - \chi_V(q))_{q \in Q_n}}, \tag{5.15}$$

where

$$\chi_V(q) = \begin{cases} \alpha_q & \text{if } q \in V \\ \beta_q & \text{otherwise.} \end{cases}$$

Since the image of $\nu$ is annihilated by the operators $U_q - \alpha_q$, $\nu$ extends to a morphism

$$H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} \to \left( \bigotimes_{q \in Q_n} H^1(X_\emptyset, W(k))^{\oplus 2,-}_{\mathfrak{m}_\emptyset} \right)_{\mathfrak{m}_{Q_n}},$$

but (5.15) shows that after localization at $\mathfrak{m}_{Q_n}$, only one of the $2^{\#Q_n}$ factors on the right hand side remains. In particular, our map becomes

$$H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} \to H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_{Q_n}}, \tag{5.16}$$

which is an isomorphism since the restriction of $\nu$ to any component was an isomorphism.

Since the right hand side of (5.16) was just seen to be the left hand side of (5.13), we obtain

$$\begin{aligned} H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_\emptyset} &\cong H^1(X_\emptyset, W(k))^-_{\mathfrak{m}_{Q_n}} \\ &\cong H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}}, \end{aligned}$$

as needed.

□

Finally, combining the isomorphism in (5.14) with

$$(H^1(X_{Q_n}, W(k))^-_{\mathfrak{m}_{Q_n}})_{\Delta_{Q_n}} = H^1(X_{Q_n-}, W(k))^-_{\mathfrak{m}_{Q_n}},$$

we obtain

$$H^1(X_\emptyset, W(k))_{\mathfrak{m}_\emptyset} \cong (H^1(X_{Q_n}, W(k))^-_{\mathfrak{m}_{Q_n}})_{\Delta_{Q_n}}.$$

□

# Chapter 6

# Taylor-Wiles and Modularity

In this section we aim to prove that representations of the absolute Galois group of $\mathbf{Q}$ meeting certain conditions are modular. We follow the argument of Wiles [Wil95] and Taylor-Wiles [TW95], using modifications of Diamond [Dia97] and Kisin [Kis] to bypass reducibility issues with the local deformation problem on the decomposition subgroup $G_{\mathbf{Q}_p}$.

Recall that the main idea of our argument is to find an isomorphism between a deformation functor that associates to a DVR $\mathfrak{O}_K$ the set of representations into $\mathrm{GL}_2(\mathfrak{O}_K)$ meeting the aforementioned conditions and a functor returning a related set of modular representations by passing to their representing objects.

We state our main theorem precisely in Section 6.1 and provide an overview of the scenario created by preceding chapters in Section 6.2. We prove Theorem 6.1 assuming three intermediate results in Section 6.3. The remaining sections are devoted to the proofs of these intermediate results.

## 6.1 Statement of the Main Theorem

Our goal is to prove that $p$-adic representations of $G_{\mathbf{Q}}$ that are residually trivial when restricted to $G_{\mathbf{Q}_p}$ are modular. As mentioned in Section 2, we define a $p$-adic representation to be unramified outside of a finite set of primes. Recall from Section 2.1.2 the definitions of the cyclotomic character $\epsilon_p$ and the character $\omega_p$ that we constructed from the Teichmüller lift. Then we aim to prove the following theorem.

**Theorem 6.1.** *Let $p > 3$ be prime. Let $K/\mathbf{Q}_p$ be a finite extension with ring of integers $\mathfrak{O}_K$ and residue field $k$. Suppose that the continuous group homomorphism $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_K)$ satisfies the following conditions.*

1. *The residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$ is absolutely irreducible, odd, and modular.*

2. *The restriction $\overline{\rho}|_{G_{\mathbf{Q}_p}}$ is trivial.*

3. *The restriction $\rho|_{G_{\mathbf{Q}_p}}$ is ordinary.*

4. *For all $\ell \neq p$, $\rho$ is minimally ramified over $\overline{\rho}$. Moreover, the prime-to-p part of the conductor $N(\overline{\rho})$ is a squarefree number $T$ such that for all $t|T$, $p \nmid t-1$.*

5. *The product $\epsilon \det \rho$ is tamely ramified at $p$.*

*Then $\rho$ is modular.*

*Remark* 6. The conditions of Theorem 6.1 imply that

$$\det \rho = \epsilon_p^{-1}\omega_p\chi,$$

where $\chi$ is an odd character, unramified outside a finite set of primes, at most tamely ramified everywhere, such that $\chi|_{G_{\mathbf{Q}_p}}$ is trivial.

In particular, since $\det \rho$ is residually trivial and $\epsilon \det \rho$ is a character $\psi : (\mathbf{Z}/pT\mathbf{Z})^\times \to \mathfrak{O}_K^\times$, the character $\psi\omega_p^{-1}$ is residually trivial on $G_{\mathbf{Q}_p}$. Since $(\mathbf{Z}/pT\mathbf{Z})^\times$ has order prime to $p$ by the hypotheses of Theorem 6.1 and $1+\mathfrak{O}_K \subseteq \mathfrak{O}_K^\times$ is pro-$p$, $\psi\omega_p^{-1}$ is trivial on $G_{\mathbf{Q}_p}$. In particular, $\psi\omega_p^{-1}$ is a character $\chi : (\mathbf{Z}/T\mathbf{Z})^\times \to \mathfrak{O}_K^\times$ with the aforementioned properties.

## 6.2 Morphisms

In this section we recall the relationships between all of the objects that will appear in the Taylor-Wiles argument. These objects come from the two worlds of Galois theory and modular forms. Section 4 defined the objects coming from the former world and Section 5 defined those coming from the latter.

The ring $R_{\emptyset,\mathrm{ord}}$ is defined by setting $Q = \emptyset$ in the definitions from Section 4.3. We defined the ring $\mathbf{T}_\emptyset$ and the $\mathbf{T}_\emptyset$-module $S_\emptyset$ in Section 5.2. We obtain from Proposition 5.8 a natural surjective morphism

$$R_{\emptyset,\mathrm{ord}} \twoheadrightarrow T_\emptyset,$$

making $S_\emptyset$ into an $R_{\emptyset,\mathrm{ord}}$-module.

For each $n$, we have an identical arrangement for the rings $R_{Q_n,\mathrm{ord}}$ and $\mathbf{T}_{Q_n}$, which act on the module $S_{Q_n}$. In this case, we have the additional structure of an action $W(k)[\Delta_Q] \to R_{Q_n,\mathrm{ord}}$. Proposition 4.24 showed that $R_{Q_n,\mathrm{ord}}/\mathfrak{a}_Q R_{Q_n,\mathrm{ord}} = R_{\emptyset,\mathrm{ord}}$. Recall that while we defined a second action $W(K)[\Delta_Q] \to \mathbf{T}_{Q_n}$ with the property that $S_{Q_n}/\mathfrak{a}_Q S_{Q_n} = S_\emptyset$, we proved in Proposition 5.10 that the action induced from the composition $W(k)[\Delta_Q] \to R_{Q_n,\mathrm{ord}} \to \mathbf{T}_{Q_n}$ is the same action.

Following Kisin [Kis], we will need to apply framing to this entire situation. In particular, we set

$$\mathbf{T}_{Q_n}^\square = \mathbf{T}_{Q_n} \otimes_{R_{Q_n,\mathrm{ord}}} R_{Q_n,\mathrm{ord}}^\square \quad \text{and} \quad S_{Q_n}^\square = S_{Q_n} \otimes_{R_{Q_n,\mathrm{ord}}} R_{Q_n,\mathrm{ord}}^\square.$$

Then $R_{Q_n,\mathrm{ord}}^\square \twoheadrightarrow \mathbf{T}_{Q_n}^\square$, since tensoring preserves surjectivity. Moreover, by Proposition 4.19 $R_{Q_n,\mathrm{ord}}^\square \cong R_{Q_n,\mathrm{ord}}[[c_1, c_2, c_3]]$, so we have

$$R_{Q_n,\mathrm{ord}}^\square/(\mathfrak{a}_Q, c_1, c_2, c_3)R_{Q_n,\mathrm{ord}}^\square = R_{\emptyset,\mathrm{ord}} \quad \text{and} \quad S_{Q_n}^\square/(\mathfrak{a}_Q, c_1, c_2, c_3)S_{Q_n}^\square = S_\emptyset. \tag{6.1}$$

We finally recall from Section 4.8 the isomorphism

$$W(k)[[\{s_q\}_{q\in Q_n}]]/((1+s_q)^{\#\Delta_q}-1)_{q\in Q_n} \cong W(k)[\Delta_{Q_n}],$$

where $\mathfrak{a}_Q = (g-1)_{g\in\Delta_Q} \subseteq W(k)[\Delta_Q]$ corresponds to $\{s_q\}_{q\in Q}$. Thus, rather than thinking of $R_{Q_n,\mathrm{ord}}$ and $R^{\square}_{Q_n,\mathrm{ord}}$ as $W(k)[\Delta_Q]$-algebras, we may instead regard these as $W(k)[[\{s_q\}_{q\in Q_n}]]$-algebras. Moreover, (6.1) becomes

$$R^{\square}_{Q_n,\mathrm{ord}}/(\{s_q\}_{q\in Q_n}, c_1, c_2, c_3)R^{\square}_{Q_n,\mathrm{ord}} = R_{\emptyset,\mathrm{ord}}$$

and

$$S^{\square}_{Q_n,\mathrm{ord}}/(\{s_q\}_{q\in Q_n}, c_1, c_2, c_3)S^{\square}_{Q_n,\mathrm{ord}} = S_{\emptyset,\mathrm{ord}}.$$

## 6.3 Overview of the Taylor-Wiles Argument

In the situation described in Section 6.2, we will be able to prove a relationship between the ring $R_{\emptyset,\mathrm{ord}}$ and the ring $\mathbf{T}_{\emptyset}$. In order to do so, we will prove a general fact in commutative algebra, which is a slight modification of a result of Diamond [Dia97].

**Proposition 6.2.** *Let $k$ be a finite field. Let $A = W(k)[[s_1,\ldots,s_t]]$ and let $\mathfrak{a} = (s_1,\ldots,s_t)$. Let $B$ be a complete local Noetherian integral domain and $W(k)$-algebra of Krull dimension $\leq t+1$. Let $R$ be a local $W(k)$-algebra, and let $S$ be a nonzero $R$-module, finite over $W(k)$. Suppose that for each $n$ there are maps $\varphi_n : A \to B$ and $\psi_n : B \to R$, as well as $B$-modules $S_n$ with $B$-module homomorphisms $\pi_n : S_n \to S$, such that the following three conditions hold.*

1. *The maps $\psi_n$ are surjective and the composition $\psi_n(\varphi_n(\mathfrak{a})) = 0$.*
2. *The maps $\pi_n$ induce $B$-module isomorphisms $\pi_n : S_n/\varphi(\mathfrak{a})S_n \xrightarrow{\sim} S$.*
3. *The module $S_n$ is free over $A/\mathfrak{a}^n A$.*

*Then* $\operatorname{Supp}_R S = \operatorname{Spec} R$ *and* $\dim B = t+1$.

The main idea behind the proof is to notice that although the objects with parameter $n$ do not form a directed system of which one might take a limit, one can use the compactness of the objects to find some subsequence where the limit is in fact defined. The objects in the limit are rather well-behaved, and the results of Section 2.3.1 will allow us to deduce consequences for the objects involved.

*Remark* 7. The main difference between Proposition 6.2 and Diamond's result [Dia97, Theorem 2.1] is that Diamond uses the stronger hypothesis that $B$ is smooth and, accordingly, obtains much stronger conclusions using the theory of regular local rings. In particular, while Proposition 6.3 will suffice to prove Theorem 6.1 via the weakened isomorphism in Proposition 6.5, Diamond's result implies an isomorphism of the form $R \cong \mathbf{T}$.

Initially, the proofs of both results are almost identical. However, where Diamond applies the Auslander-Buchsbaum-Serre theorem using the fact $B$ is regular, thereby allowing one to conclude from the Auslander-Buchsbaum formula that the projective dimension of $S_\infty$ is zero, we instead use the Krull dimension of $B$ to prove a weaker statement about the support of $S_\infty$ and then $S$.

By applying Proposition 6.2 to the setting described in Section 6.2, we will prove the following result.

**Proposition 6.3.** *Under the hypotheses of Theorem 6.1, we have*

$$\mathrm{Supp}_{R_{\emptyset,\mathrm{ord}}}(S_\emptyset) = \mathrm{Spec}(R_{\emptyset,\mathrm{ord}}).$$

We will also obtain the following result.

**Corollary 6.4.** *The inequality* $\dim R^{\mathrm{loc}}_{p,\mathrm{ord}} \leq 5$ *in Proposition 3.8 is an equality.*

Using Proposition 6.3, we will deduce the following result.

**Proposition 6.5.** *Assume the hypotheses of Theorem 6.1. Let $\mathfrak{N}$ be the nilradical of the ring $R_{\emptyset,\mathrm{ord}}$. We have the isomorphism*

$$R_{\emptyset,\mathrm{ord}}/\mathfrak{N} \cong \mathbf{T}_\emptyset.$$

From Proposition 6.5, Theorem 6.1 follows almost immediately.

*Proof of Theorem 6.1.* Suppose we are given a representation $\rho$ meeting the conditions of Theorem 6.1. Note that for a DVR $\mathfrak{O}_K$ with residue field $k_K$ that is finite over $k$, a morphism $R_{\emptyset,\mathrm{ord}} \to \mathfrak{O}_K$ factors through $R_{\emptyset,\mathrm{ord}}/\mathfrak{N}$ since the image is an integral domain. Proposition 6.5 implies that $R_{\emptyset,\mathrm{ord}}/\mathfrak{N} \cong \mathbf{T}_\emptyset$.

There is a minor obstruction to concluding Theorem 6.1. In particular, if the residue field $k_K$ is a nontrivial extension of $k$, the universal property of $R_{\emptyset,\mathrm{ord}}$ does not guarantee that we obtain exactly the set of strict equivalence classes of representations meeting the conditions of the theorem, since $\mathfrak{O}_K$ is not in the category $\mathbf{CLNRings}(k)$. There are two ways we can solve this issue. The first is to assume that $\mathfrak{O}_K$ has residue field $k$, which is not a loss of generality since we can always tensor $\overline{\rho}$ with an extension $k'$ of $k$. However, this may seem to be a disappointing solution, since the representations $\rho$ are in fact equivalent to representations into complete local noetherian rings with residue field $k$, as seen in Claim 5.9. We will provide an alternative approach.

Observe that the statements of Propositions 3.5, 3.6, and 3.7 allowed for discrete valuation rings with residue field a finite extension of $k$. By examining the proof of Proposition 3.7, one finds that since Proposition 3.6 applies to any object of $\mathbf{CLNRings}(k)$, Proposition 3.7 applies to subrings of DVRs $\mathfrak{O}'_K \subseteq \mathfrak{O}_K$ with the property that the inverse of any element of $\mathfrak{O}'_K \cap \mathfrak{O}_K^\times$ is also in $\mathfrak{O}'_K$, which is certainly true of the rings arising in Claim 5.9. In particular, the proof can be applied using the valuation $v_K$ from the DVR. We did not use the fact that the maximal ideal of a DVR is principal – we needed only that the ring is an integral domain. We also note that the statement of Proposition 5.6 applies to those rings arising in Claim 5.9 as well.

Thus, given a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}_K)$ lifting $\overline{\rho} \otimes k_K$ meeting the conditions of Theorem 6.1, we consider the representation $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathfrak{O}'_K)$ as in Claim 5.9. Then the above discussion shows that the map in $\mathrm{Hom}(R_\emptyset, \mathfrak{O}'_K)$ corresponding to $\rho'$ factors through $R_{\emptyset,\mathrm{ord}}$ and through the quotient by $\mathfrak{N}$. Then the isomorphism in Proposition 6.5 provides a corresponding morphism $\mathbf{T}_\emptyset \to \mathfrak{O}'_K$, proving that $\rho'$ and thus $\rho$ is modular by Proposition 5.6.

$\square$

## 6.4 Proof of Proposition 6.2

Letting $d = \dim S$, fix a lift $b_1, \ldots, b_d$ to $S$ of a $k$-basis for $S/(\pi)$, where $\pi$ is a uniformizer for $W(k)$. For each $n$, define $b_{1,n}, \ldots, b_{d,n}$ to be a lift of $b_1, \ldots, b_d$ to $S_n$. By Nakayama's lemma, $b_{1,n}, \ldots, b_{d,n}$ generate $S_n$ over $A/\mathfrak{a}^n A$. Since $S_n$ is free over $A/\mathfrak{a}^n A$, $b_{1,n}, \ldots, b_{d,n}$ form a basis for $S_n$ as an $A/\mathfrak{a}^n A$-module. Using $b_{1,n}, \ldots, b_{d,n}$ as a basis, we identify $\mathrm{End}(S_n)$ with $\mathbf{M}_d(A/\mathfrak{a}^n A)$. We use $b_1, \ldots, b_d$ to identify $\mathrm{End}(S)$ with $\mathbf{M}_d(W(k))$. We denote the morphism $B \to \mathbf{M}_d(A/\mathfrak{a}^n A)$ by $\mu_n$.

For each $n$, we can fit the various objects in the proposition into the commutative diagram

$$\begin{tikzcd}
A \arrow[dr, "\varphi_n"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& B \arrow[r, "\mu_n"] \arrow[d, "\psi_n"] & \mathbf{M}_d(A/\mathfrak{a}^n A) \arrow[d, "\pi_n"] \\
& R \arrow[r] & \mathbf{M}_d(W(k))
\end{tikzcd}$$

where the map $A \to M_d(A/\mathfrak{a}^n A)$ sends $a \mapsto a\mathbf{1}_d$ and the $W(k)$-algebra homomorphism $A \to R$ sends $s_i \mapsto 0$ for all $i$. Note that the commutativity of the triangle

$$\begin{tikzcd}
A \arrow[r, "\varphi_n"] \arrow[dr] & B \arrow[d, "\psi_n"] \\
& R
\end{tikzcd}$$

is condition (3) of the proposition and the commutativity of the triangle

$$\begin{tikzcd}
A \arrow[d, "\varphi_n"] \arrow[dr] & \\
B \arrow[r, "\mu_n"] & M_d(A/\mathfrak{a}^n A)
\end{tikzcd}$$

is the statement that the $A$-module structure of $S_n$ is inherited through $B$ (and so the composite map is $A$-multiplication). Finally, the commutativity of the square

$$\begin{tikzcd} B \arrow[r, "\mu_n"] \arrow[d, "\psi_n"] & \mathbf{M}_d(A/\mathfrak{a}^n A) \arrow[d, "\pi_n"] \\ R \arrow[r] & \mathbf{M}_d(W(k)) \end{tikzcd},$$

follows from condition (2) of the proposition and the $\pi_n$-compatibility of the definitions of the bases for $\mathrm{End}(S_n)$ and $\mathrm{End}(S)$.

We will take a limit of this structure in the following way. Let $e$ be the tangent space dimension of $B$, so that there is a set of $e$ elements $x_1, \ldots, x_e \in B$ that topologically generate $B$ over $W(k)$. For each $i \in \{1, \ldots, e\}$ and $n \geq 1$, we define $\nu_n(x_i) \in \mathbf{M}_d(A)$ to be an arbitrary lift of $\mu_n(x_i)$. The product $B^t \times R^e \times \mathbf{M}_d(A)^e$ is compact and first-countable since it is a finite product of spaces with these properties. In particular, it is a sequentially compact space, so the sequence

$$\{(\varphi_n(s_1), \ldots, \varphi_n(s_t), \psi_n(x_1), \ldots, \psi_n(x_e), \nu_n(x_1), \ldots, \nu_n(x_e))\}_{n \geq 1}$$

has a subsequence converging to a limit

$$(\varphi_\infty(s_1), \ldots, \varphi_\infty(s_t), \psi_\infty(x_1), \ldots, \psi_\infty(x_e), \nu_\infty(x_1), \ldots, \nu_\infty(x_e)). \tag{6.2}$$

**Claim 6.6.** *The values in the tuple (6.2) define homomorphisms*

$$\varphi_\infty : A \to B, \psi_\infty : B \twoheadrightarrow R \quad \textit{and} \quad \nu_\infty : B \to \mathbf{M}_d(A)$$

*fitting into the commutative diagram*

$$\begin{tikzcd} A \arrow[dr, "\varphi_\infty"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & B \arrow[r, "\nu_\infty"] \arrow[d, two heads, "\psi_\infty"] & \mathbf{M}_d(A) \arrow[d, "\pi_\infty"] \\ & R \arrow[r] & \mathbf{M}_d(W(k)) \end{tikzcd}. \tag{6.3}$$

*Define $S_\infty \cong A^d$ with $B$-module structure defined using $\nu_\infty$, and define $\pi_\infty$ to be the quotient by $\mathfrak{a}$. Then the properties stated in the proposition hold in the limit, as follows.*

1. *We have $\psi_\infty(\varphi_\infty(\mathfrak{a})) = 0$.*

2. *There is an isomorphism of $B$-modules $\pi_\infty : S_\infty/\varphi(\mathfrak{a})S_\infty \xrightarrow{\sim} S$.*

*Proof.* It is immediate that (6.2) defines a homomorphism $\varphi_\infty : A \to B$. We next need to check that if the variables $x_1, \dots, x_e$ are subject to the relation $R(x_1, \dots, x_e)$ in $B$, then $\psi_\infty(R(x_1, \dots, x_e))$. Note that $\psi_n(R(x_1, \dots, x_e))$ for each $n$. Since addition and multiplication are continuous, this must be true in the limit. Moreover, since each of the $\psi_n$ are surjective, the map $\psi_\infty$ is as well. In particular, for $r \in R$, the limit of the sequence of preimages of $r$ under $\psi_{n_i}$ maps to $r$ under $\psi_\infty$, where $\{n_i\}$ is the set of indices for the convergent subsequence.

To prove that $\nu_\infty(x_1), \dots, \nu_\infty(x_e)$ defines a homomorphism, it suffices to show that for all $m$, the $\nu_\infty(\cdot)$ define a homomorphism

$$\nu_{\infty,m} : B \to \mathbf{M}_d(A/\mathfrak{a}^m A),$$

since this implies both that the commutators $\nu_\infty(x_i)\nu_\infty(x_j) - \nu_\infty(x_j)\nu_\infty(x_i)$ must lie in $\mathfrak{a}^m$ for all $m$ and thus vanish and that the relations in $B$ map to elements of $\mathfrak{a}^m$ for all $m$ and thus vanish as well. For sufficiently large $i$, the projection of $\nu_{n_i}$ to $\mathbf{M}_d(A/\mathfrak{a}^m A)$ must agree with both $\mu_m$ and $\nu_{\infty,m}$. But $\mu_m$ is a homomorphism, so $\nu_{\infty,m}$ is a homomorphism as well.

The commutativity of (6.3) follows from the commutativity of the diagrams for each $n$. By continuity, the composition $\psi_\infty(\varphi_\infty(\mathfrak{a}))$ vanishes in the limit. The isomorphism $\pi_\infty : S_\infty/\varphi(\mathfrak{a})S_\infty \xrightarrow{\sim} S$ is automatic from the definition of $S_\infty$.

□

Since $S_\infty$ is free over $A$, the elements

$$p, \varphi_\infty(s_1), \dots, \varphi_\infty(s_t)$$

define an $S_\infty$-regular sequence with respect to the $B$-module structure of $S_\infty$. In particular, we obtain the inequality

$$\operatorname{depth}_B S_\infty \geq t + 1.$$

On the other hand, by Fact 2.15, we have $\operatorname{depth}_B S_\infty \leq \dim B \leq t + 1$. In particular, we find $\operatorname{depth}_B S_\infty = \dim B = t + 1$.

In this situation, Fact 2.16 implies that every element not contained in a minimal prime of $B$ is a non-zero-divisor of $S_\infty$. Since $B$ is an integral domain by hypothesis, we find that $(0) \in \operatorname{Supp}_B S_\infty$. Moreover, the support is closed in $\operatorname{Spec} B$, so in fact $\operatorname{Supp}_B S_\infty = \operatorname{Spec} B$. By Fact 2.17,

$$\operatorname{Rad}(\operatorname{Ann}_B S) = \operatorname{Rad}(\operatorname{Ann}_B S_\infty/\varphi_\infty(\mathfrak{a})S_\infty) = \operatorname{Rad}(\varphi_\infty(\mathfrak{a}) + \operatorname{Ann}_B S_\infty) = \operatorname{Rad}(\varphi_\infty(\mathfrak{a})). \quad (6.4)$$

In particular, since prime ideals are radical, any prime of $B$ containing $\varphi(\mathfrak{a})$ also contains $\operatorname{Rad}(\operatorname{Ann}_B S)$ and thus $\operatorname{Ann}_B S$. Since the primes in $\operatorname{Supp}_{B/\varphi_\infty(\mathfrak{a})B} S$ are exactly those primes containing $\operatorname{Ann}_B S$, we have

$$\operatorname{Supp}_{B/\varphi_\infty(\mathfrak{a})B} S = \operatorname{Spec} B/\varphi_\infty(\mathfrak{a})B. \quad (6.5)$$

We note that the morphism $\psi_\infty : B \twoheadrightarrow R$ is surjective and factors through $B/\varphi_\infty(\mathfrak{a})B$ by Claim 6.6. On the other hand, the kernel of the morphism $\pi_\infty \circ \nu_\infty$ is contained in

$\mathrm{Rad}(\varphi_\infty(\mathfrak{a}))$, since this is the morphism that makes $S$ into a $B$-module and we know that $\mathrm{Ann}_B S \subseteq \mathrm{Rad}(\varphi_\infty(\mathfrak{a}))$ from (6.4). Thus, by commutativity of (6.3), the kernel $\mathfrak{b}$ of $\psi_\infty : B \twoheadrightarrow R$ satisfies

$$\varphi_\infty(\mathfrak{a}) \subseteq \mathfrak{b} \subseteq \mathrm{Rad}(\varphi_\infty(\mathfrak{a})).$$

We thus find $\operatorname{Spec} B/\varphi_\infty(\mathfrak{a})B = \operatorname{Spec} B/\mathfrak{b} \cong \operatorname{Spec} R$.

The primes in $\mathrm{Supp}_R S$ are the primes containing $\mathrm{Ann}_R S$. For a prime $\mathfrak{p} \in \operatorname{Spec} B/\mathfrak{b} \cong \operatorname{Spec} R$, which corresponds to a prime $\mathfrak{p}_B$ of $B$ containing $\mathfrak{b}$, $\mathfrak{p}_B$ contains $\mathrm{Ann}_B S$ exactly when it contains $\mathrm{Rad}(\mathrm{Ann}_B S) = \mathrm{Rad}(\varphi_\infty(\mathfrak{a}))$ and thus $\varphi_\infty(\mathfrak{a})$ by (6.4). In particular, the primes in $\mathrm{Supp}_R S$ correspond exactly to the primes of $\operatorname{Spec} B/\varphi_\infty(\mathfrak{a})B$. Then (6.5) gives us

$$\mathrm{Supp}_R S \cong \mathrm{Supp}_{B/\mathfrak{b}B} S = \operatorname{Spec} B/\varphi_\infty(\mathfrak{a})B \cong \operatorname{Spec} R$$

and thus $\mathrm{Supp}_R S = \operatorname{Spec} R$.

## 6.5 Proof of Proposition 6.3 and Corollary 6.4

Define $d = \#Q_n - 1$ and $e = \dim_{W(k)} S_\emptyset$. By Corollary 4.17 and Proposition 4.27, there exists a surjective homomorphism

$$\psi_n : R^{\mathrm{loc}}_{p,\mathrm{ord}}[[x_1, \dots, x_d]] \twoheadrightarrow R^{\square}_{Q_n,\mathrm{ord}} \twoheadrightarrow R_{\emptyset,\mathrm{ord}} \tag{6.6}$$

for all $n$, where the second surjection is the composition of the maps $R^{\square}_{Q_n,\mathrm{ord}} \twoheadrightarrow R_{Q_n,\mathrm{ord}}$ and $R_{Q_n,\mathrm{ord}} \twoheadrightarrow R_{\mathrm{ord},\emptyset}$ from Propositions 4.19 and 4.24. Define $B = R^{\mathrm{loc}}_{p,\mathrm{ord}}[[x_1, \dots, x_d]]$ and $R = R_{\emptyset,\mathrm{ord}}$.

For each $n$, we define $\varphi_n$ to be any homomorphism

$$\varphi_n : W(k)[[\{s_q\}_{q \in Q_n}, c_1, c_2, c_3]] \to R^{\mathrm{loc}}_{p,\mathrm{ord}}[[x_1, \dots, x_d]]$$

such that the diagram

$$\begin{tikzcd}
W(k)[[\{s_q\}_{q \in Q_n}, c_1, c_2, c_3]] \arrow[r, "\varphi_n"] \arrow[d, "\iota"] & R^{\mathrm{loc}}_{p,\mathrm{ord}}[[x_1, \dots, x_d]] \arrow[d, two heads, "\psi_n"] \\
W(k)[\Delta_{Q_n}] \arrow[r, "\xi_n"] & R^{\square}_{Q_n,\mathrm{ord}}
\end{tikzcd}$$

commutes, where $\iota$ sends the framing variables $c_1, c_2, c_3$ to 0. This can be done by choosing a lift of $\xi_n(\iota(s_q))$ along $\psi_n$ for each $q \in Q_n$. We define $A = W(k)[[\{s_q\}_{q \in Q_n}, c_1, c_2, c_3]]$.

We define the $B$-module $S'_n = S_{Q_n}$ via the composite map

$$R^{\mathrm{loc}}_{p,\mathrm{ord}}[[x_1, \dots, x_d]] \to R^{\square}_{Q_n,\mathrm{ord}} \to \mathbf{T}_{Q_n} \to \mathrm{End}(S_{Q_n}).$$

We then set $S_n = S'_n/\varphi(\mathfrak{a})^n S'_n$.

Finally, we set $R = R_{\emptyset,\mathrm{ord}}$ and define the $R$-module $S = S_\emptyset$ via the composite homomorphism

$$R_{\emptyset,\mathrm{ord}} \to \mathbf{T}_\emptyset \to \mathrm{End}(S_\emptyset).$$

We define the maps $\pi_n : S_n \to S$ using Proposition 5.13.

We will show that these assignments satisfy the conditions of Proposition 6.2. The bound on the Krull dimension of $B$ is implied by Proposition 3.8. That $B$ is an integral domain follows from the fact that $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ is a subring of the integral domain $W(k)\langle x\rangle[[z_{11}, z_{12}, w_{12}]]$. Since $R^{\mathrm{loc}}_{p,\mathrm{ord}}$ is Noetherian, $B$ is as well. The property (1) is automatic from the definitions since $\varphi_n(\mathfrak{a})$ vanishes under the homomorphism in (6.6). The property (2) follows from Proposition 5.13.

For property (3), we note from Lemma 5.14 that $S'_n$ is free over $W(k)[[\Delta_Q]]$. Observe that the kernel of the homomorphism $A \to W(k)[[\Delta_Q]]$, which is $((1+s_q)^{\Delta_q} - q)_{q\in Q_n}$, is contained in $\mathfrak{a}^{p^n}$ and thus $\mathfrak{a}^{p^n}$. It follows that $S_n = S'_n/\mathfrak{a}^n S'_n$ is free over $A/\mathfrak{a}^n A$. Proposition 6.3 follows.

By Proposition 6.2, we find that

$$\mathrm{Supp}_{R_{\emptyset,\mathrm{ord}}} S_\emptyset = \mathrm{Spec}\, R_{\emptyset,\mathrm{ord}}.$$

and $\dim B = \#Q_n + 4$. Thus,

$$\dim R^{\mathrm{loc}}_{p,\mathrm{ord}} = \dim B - d = (\#Q_n + 4) - (\#Q_n - 1) = 5,$$

proving Corollary 6.4.

## 6.6 Proof of Proposition 6.5

By Proposition 6.3, we have morphisms

$$R_{\emptyset,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_\emptyset \to \mathrm{End}(S_\emptyset).$$

Since

$$\mathbf{T}_\emptyset \hookrightarrow \widetilde{\mathbf{T}}_\emptyset = \prod_f \mathfrak{O}_f,$$

the ring $\mathbf{T}_\emptyset$ is reduced. Thus the kernel of the surjection $R_{\emptyset,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_\emptyset$ contains the nilradical $\mathfrak{N}$ of $R_{\emptyset,\mathrm{ord}}$.

Since $\mathrm{Supp}_{R_{\emptyset,\mathrm{ord}}} S_\emptyset = \mathrm{Spec}\, R_{\emptyset,\mathrm{ord}}$, any element of $R_{\emptyset,\mathrm{ord}}$ that annihilates $S_\emptyset$ must be contained in every prime of $R_{\emptyset,\mathrm{ord}}$. Thus we must have $\mathrm{Ann}_{R_{\emptyset,\mathrm{ord}}} S_\emptyset \subseteq \mathfrak{N}$. On the other hand, any element of $R_{\emptyset,\mathrm{ord}}$ that does not annihilate $S_\emptyset$ must map to a nonzero element of $\mathbf{T}_\emptyset$, so

$$\ker(R_{\emptyset,\mathrm{ord}} \twoheadrightarrow \mathbf{T}_\emptyset) \subseteq \mathrm{Ann}_{R_{\emptyset,\mathrm{ord}}} S_\emptyset \subseteq \mathfrak{N}.$$

In particular, we obtain an isomorphism

$$R_{\emptyset,\mathrm{ord}}/\mathfrak{N} \xrightarrow{\sim} \mathbf{T}_\emptyset.$$

# Bibliography


[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BM89] N. Boston and B. Mazur, *Explicit universal deformations of Galois representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 1–21.

[Bos91] N. Boston, *Explicit deformation of Galois representations*, Invent. Math. **103** (1991), no. 1, 181–196.

[BU93] N. Boston and S. V. Ullom, *Representations related to CM elliptic curves*, Math. Proc. Cambridge Philos. Soc. **113** (1993), no. 1, 71–85.

[Car94] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, $p$-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math., vol. 165, Amer. Math. Soc., Providence, RI, 1994, pp. 213–237.

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[CHT08] L. Clozel, M. Harris, and R. Taylor, *Automorphy for some* $l$*-adic lifts of automorphic mod* $l$ *Galois representations*, preprint (2008).

[DDT97] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140.

[Del71] P. Deligne, *Formes modulaires et représentations* $\ell$*-adiques*, Springer-Verlag, New York, Berlin, Heidelberg, 1971, pp. 139–172. Lecture Notes in Math., Vol. 179.

[Dia97] F. Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. **128** (1997), no. 2, 379–391.

[DS74] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975).

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[dSL97] B. de Smit and H. W. Lenstra, Jr., *Explicit construction of universal deformation rings*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 313–326.

[Eis95] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[Fre86] G. Frey, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), no. 1, iv+40.

[Fre89] ______, *Links between solutions of $A - B = C$ and elliptic curves*, Number theory (Ulm, 1987), Lecture Notes in Math., vol. 1380, Springer, New York, 1989, pp. 31–62.

[Gou01] F. Q. Gouvêa, *Deformations of Galois representations*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, Appendix 1 by Mark Dickinson, Appendix 2 by Tom Weston and Appendix 3 by Matthew Emerton, pp. 233–406.

[Gro95] A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules*, Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, pp. Exp. No. 195, 369–390.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hid86] H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 2, 231–273.

[HSBT] M. Harris, N. Shepherd-Barron, and R. Taylor, *A family of calabi-yau varieties and potential automorphy*, Ann. Math., *to appear*.

[Iha75] Yasutaka Ihara, *On modular curves over finite fields*, Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973), Oxford Univ. Press, Bombay, 1975, pp. 161–202.

[Kis] M. Kisin, *Moduli of finite flat group schemes and modularity*, Ann. Math., *to appear*.

[KWa] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, preprint.

[KWb] ———, *Serre's modularity conjecture (II)*, preprint.

[Lan95] S. Lang, *Introduction to modular forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 222, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Maz89] ———, *Deforming Galois representations*, Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 385–437.

[Maz97] ———, *An introduction to the deformation theory of Galois representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 243–311.

[Mil06] J. S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[Miy89] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

[MW86] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Math. **59** (1986), no. 2, 231–264.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[Rib76] K. A. Ribet, *A modular construction of unramified p-extensions of*$Q(\mu_p)$, Invent. Math. **34** (1976), no. 3, 151–162.

[Rib84] Kenneth A. Ribet, *Congruence relations between modular forms*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983) (Warsaw), PWN, 1984, pp. 503–514.

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[Sch68] M. Schlessinger, *Functors of Artin rings*, Trans. Amer. Math. Soc. **130** (1968), 208–222.

[Ser87] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[Tay08] R. Taylor, *Automorphy for some $\ell$-adic lifts of automorphic mod $\ell$ Galois representations II*, preprint (2008).

[Tay09] ———, *personal communication.*

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.