View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Harvard University - DASH

DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD

Modularity of Certain Potentially Barsotti-Tate Galois Representations

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters.

Citation	Conrad, Brian, Fred Diamond, and Richard L. Taylor. 1999. Modularity of certain potentially Barsotti-Tate Galois representations. Journal of the American Mathematical Society 12: 521-567.
Published Version	doi:10.1090/S0894-0347-99-00287-8
Accessed	February 18, 2015 6:21:16 AM EST
Citable Link	http://nrs.harvard.edu/urn-3:HUL.InstRepos:3579185
Terms of Use	This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

(Article begins on next page)

JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0894-0347(XX)0000-0

MODULARITY OF CERTAIN POTENTIALLY BARSOTTI-TATE GALOIS REPRESENTATIONS

BRIAN CONRAD, FRED DIAMOND, AND RICHARD TAYLOR

Introduction

Conjectures of Langlands, Fontaine and Mazur [22] predict that certain Galois representations

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell)$$

(where ℓ denotes a fixed prime) should arise from modular forms. This applies in particular to representations defined by the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the ℓ-adic Tate module of an elliptic curve defined over $\mathbf{Q}$, and so implies the Shimura-Taniyama-Weil conjecture.

Wiles' breakthrough in [46], completed by [45] and extended in [12], provided results of the form

$$\overline{\rho} \text{ modular } \Rightarrow \rho \text{ modular}$$

where $\overline{\rho}$ is the reduction of ρ. These results were subject to hypotheses on the local behavior of ρ at ℓ, i.e., the restriction of ρ to a decomposition group at ℓ, and to irreducibility hypotheses on $\overline{\rho}$. In this paper, we build on the methods of [46], [45] and [12] and relax the hypotheses on local behavior. In particular, we treat certain ℓ-adic representations which are not semistable at ℓ, but potentially semistable.

We do this using results of [6], generalizing a theorem of Ramakrishna [32] (see Fontaine-Mazur [22, §13] for a slightly different point of view). The results in [6] show that certain "potentially Barsotti-Tate" deformation problems are smooth, allowing us to define certain universal deformations for $\overline{\rho}$ with the necessary Galois-theoretic properties to apply Wiles' method. To carry out the proof that these deformations are indeed realized in the cohomology of modular curves (i.e., that the universal deformation rings are Hecke algebras), we need to identify the corresponding cohomology groups and prove they have the modular-theoretic properties needed to apply Wiles' method. As in [15] and [12], the identification is made by matching local behavior of automorphic representations and Galois representations via the local Langlands correspondence (together with Fontaine's theory at the prime ℓ). We work directly with cohomology of modular curves instead of

Received by the editors March 21, 1998 and, in revised form, Sept 1, 1998.
1991 *Mathematics Subject Classification.* Primary 11F80; Secondary 11G18.
Key words and phrases. Hecke algebra, Galois representation, modular curves.
B.C. was supported by an N.S.F. Postdoctoral Fellowship, and would like to thank The Institute for Advanced Study for its hospitality. F.D. was at M.I.T. during part of the research and received support from an A.M.S. Centennial Fellowship, and for another part was visiting Université de Paris-Sud supported by the C.N.R.S. R.T. was supported by a grant from the N.S.F. All of the authors are grateful to Centre Émile Borel at the Institut Henri Poincaré for its hospitality at the p-adic semester.

©1997 American Mathematical Society

using the Jacquet-Langlands correspondence, and we use the simplification of [46] provided by [13] and Fujiwara [23] independently.

The main technical restriction in this paper is that we only treat representations which arise from ℓ-divisible groups over certain *tamely* ramified extensions of $\mathbf{Q}_\ell$. We do obtain sufficiently strong results here to give the following application:

Theorem *If E is an elliptic curve over $\mathbf{Q}$ with conductor not divisible by 27, then E is modular.*

Note that the hypothesis on the conductor of E is satisfied if and only if E acquires semistable reduction over a tamely ramified extension of $\mathbf{Q}_3$.

Notation We fix an odd prime ℓ and algebraic closures $\overline{\mathbf{Q}}$, $\overline{\mathbf{R}} = \mathbf{C}$, and $\overline{\mathbf{Q}}_p$ for all p. Choose embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and $\overline{\mathbf{Q}}_p$ for all p, so we realize the Galois group $G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ as a decomposition group inside of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let I_p denote the inertia subgroup, $\mathrm{Frob}_p \in G_p/I_p$ the arithmetic Frobenius element, and W_p the Weil subgroup of G_p (i.e., the preimage of the subgroup of $G_p/I_p \simeq \widehat{\mathbf{Z}}$ generated by Frob_p). We define $\overline{\mathbf{F}}_p$ to be the residue field of the valuation ring of $\overline{\mathbf{Q}}_p$, and regard this as 'the' algebraic closure of $\mathbf{F}_p$. The order p^n subfield of $\overline{\mathbf{F}}_p$ is denoted $\mathbf{F}_{p^n}$.

For any field F of characteristic distinct from ℓ and having a fixed choice of separable closure F_s, with $G_F = \mathrm{Gal}(F_s/F)$ the resulting Galois group, define $\epsilon : G_F \to \mathbf{Z}_\ell^\times$ to be the ℓ-adic cyclotomic character. We let $\omega = \epsilon \bmod \ell$ and let $\tilde{\omega} : G_F \to \mathbf{Z}_\ell^\times$ denote its Teichmüller lift. For any $\mathbf{Z}_\ell[G_F]$-module V, define $V(n) = V \otimes_{\mathbf{Z}_\ell} \epsilon^n$ for all $n \in \mathbf{Z}$. For a representation ρ of G_F and L/F a subextension of F_s/F, let $\rho|_L$ denote the restriction $\rho|_{G_L}$.

We will let $\eta_{p,n}$ denote the character $I_p \to W(\mathbf{F}_{p^n})^\times$ obtained from the inverse of the reciprocity map $F^\times \to G_F^{\mathrm{ab}}$ of local class field theory, where F is the field of fractions of $W(\mathbf{F}_{p^n})$. We write η_n for $\eta_{\ell,n}$, ϵ_n for η_n^{-1}, $\omega_n : I_\ell \to \mathbf{F}_{\ell^n}^\times$ for the reduction mod ℓ of ϵ_n and $\tilde{\omega}_n$ for the Teichmüller lift of ω_n. Thus $\epsilon_1 = \epsilon$, $\omega_1 = \omega$, and $\tilde{\omega}_n$ satisfies

$$\sigma(\ell^{1/(\ell^n-1)}) = \tilde{\omega}_n(\sigma)\ell^{1/(\ell^n-1)},$$

where $\ell^{1/(\ell^n-1)}$ denotes any (ℓ^n-1)th root of ℓ in $\overline{\mathbf{Q}}_\ell$ [36, §1.5, Prop 3].

1. Deformation Algebras

1.1. **Potentially Barsotti-Tate representations.** Fix a finite extension K of $\mathbf{Q}_\ell$ in $\overline{\mathbf{Q}}_\ell$ with valuation ring $\mathcal{O}$ and residue field k. Let E be a characteristic 0 field complete with respect to a discrete valuation, with valuation ring $\mathcal{O}_E$ and residue field perfect of characteristic ℓ. Consider a continuous representation

$$\rho : G_E \to \mathrm{GL}(M),$$

where M is a vector space of finite dimension d over K. By a continuity and compactness argument, there exists an $\mathcal{O}$-lattice L in M which is stable under the action of G_E.

Since all choices of L are commensurable, an argument using the method of scheme-theoretic closure (see [33, §2.2-2.3]) shows that if there exists an ℓ-divisible group $\Gamma_{/\mathcal{O}_E}$ with generic fiber representation L (as a $\mathbf{Z}_\ell[G_E]$-module), then for any choice of L such a Γ exists. In this case, we say that ρ is *Barsotti-Tate* (over E). It is straightfoward to check that for K'/K a finite extension, ρ is Barsotti-Tate if and only if $\rho \otimes_K K'$ is Barsotti-Tate. We say that ρ is *potentially Barsotti-Tate* if

there exists a finite extension E'/E such that $\rho|_{G_{E'}}$ is Barsotti-Tate, in which case we say *ρ becomes Barsotti-Tate over E'*.

We remark that if E' denotes the completion of the maximal unramified extension E^{un} of E, so $G_{E'}$ is identified with the inertia group of E (because the valuation ring of E^{un} is a henselian discrete valuation ring with algebraically closed residue field), then ρ is Barsotti-Tate if and only if $\rho|_{I_E} = \rho|_{G_{E'}}$ is Barsotti-Tate. To see this, fix a lattice L stable under ρ and let ρ denote the representation of G_E on L. Applying [1, Ch 6, Prop. D4(b)] to each torsion level, if $\rho|_{I_E}$ is Barsotti-Tate (over E') then there exists an ℓ-divisible group Γ over the (perhaps non-complete) valuation ring of E^{un} with generic fiber $\rho|_{I_E}$. Using [44, Thm 4] and étale descent at each torsion level, this descends to an ℓ-divisible group over $\mathcal{O}_E$ with generic fiber ρ, so ρ is Barsotti-Tate. The same theorem [44, Thm 4] shows that when ρ is Barsotti-Tate and we fix a choice of G_E-stable lattice L, the corresponding ℓ-divisible group $\Gamma_{/\mathcal{O}_E}$ is canonically unique and admits a unique action of $\mathcal{O}$ extending that on the generic fiber.

Let $\rho : G_E \to \mathrm{Aut}_{\mathcal{O}}(L)$ be a potentially Barsotti-Tate representation, with L a finite free $\mathcal{O}$-module of rank d (so $\rho \otimes_{\mathcal{O}} K$ is potentially Barsotti-Tate). Suppose that the residue field of E is finite (i.e., E is a finite extension of $\mathbf{Q}_\ell$). In Appendix B, we review (following ideas of Fontaine) how to attach to ρ a continuous representation

$$WD(\rho) : W_E \to \mathrm{GL}(D),$$

where W_E is the Weil group of E (i.e., the subgroup of G_E which maps to an integral power of Frobenius in the Galois group of the residue field) and D is a vector space over $\overline{\mathbf{Q}}_\ell$ of dimension d. A discussion of various properties of this construction (e.g., behavior with respect to tensor products) is given in Appendix B. For example, if ρ has cyclotomic determinant, then $WD(\rho)$ has unramified determinant sending Frob_E to $|k_E|$, the size of the residue field of E.

1.2. **Types of local deformations.** Fix a continuous two-dimensional representation

$$\overline{\rho} : G_\ell \to \mathrm{GL}(V)$$

over k such that $\mathrm{End}_{k[G_\ell]} V = k$. One then has a universal deformation ring $R_{V,\mathcal{O}}$ for $\overline{\rho}$ (see Appendix A).

An *ℓ-type* is an equivalence class of two-dimensional representations

$$\tau : I_\ell \to \mathrm{GL}(D)$$

over $\overline{\mathbf{Q}}_\ell$ with open kernel. For each ℓ-type τ, we shall define a certain quotient $R^D_{V,\mathcal{O}}$ of the complete local Noetherian $\mathcal{O}$-algebra $R_{V,\mathcal{O}}$. This quotient will be a 'Zariski closure of certain characteristic 0 points'.

A deformation ρ of V to the the ring of integers $\mathcal{O}'$ of a finite extension of K in $\overline{\mathbf{Q}}_\ell$, is said to be *of type τ* if

(1) ρ is Barsotti-Tate over F for any finite extension F of $\mathbf{Q}_\ell$ such that $\tau|_{I_F}$ is trivial;
(2) the restriction of $WD(\rho)$ to I_ℓ is equivalent to τ;
(3) the character $\epsilon^{-1} \det \rho$ is the Teichmüller lift of the prime-to-ℓ order character $\omega^{-1} \det \overline{\rho} : G_\ell \to \overline{\mathbf{F}}_\ell^\times$.

We say that a prime ideal $\mathfrak{p}$ of $R_{V,\mathcal{O}}$ is *of type τ* if there exists a finite extension K' of K (with valuation ring $\mathcal{O}'$) and a (necessarily local) $\mathcal{O}$-algebra homomorphism $R_{V,\mathcal{O}} \to \mathcal{O}'$ with kernel $\mathfrak{p}$ such that the corresponding deformation is of type τ. If $\mathfrak{p}$ is

of type τ, then so is the deformation corresponding to any $\mathcal{O}$-algebra homomorphism with kernel $\mathfrak{p}$ and values in some $\mathcal{O}'$ as above.

If there do not exist any prime ideals $\mathfrak{p}$ of type τ, we define $R^D_{V,\mathcal{O}} = 0$. Otherwise, define $R^D_{V,\mathcal{O}}$ to be the quotient of $R_{V,\mathcal{O}}$ by the intersection of all $\mathfrak{p}$ of type τ. We say that a deformation of $\overline{\rho}$ to R is *weakly of type* τ if the associated local $\mathcal{O}$-algebra map $R_{V,\mathcal{O}} \to R$ factors through the quotient $R^D_{V,\mathcal{O}}$. We say that τ is *acceptable* for $\overline{\rho}$ if $R^D_{V,\mathcal{O}} \neq 0$ and if there is a surjective local $\mathcal{O}$-algebra map $\mathcal{O}[\![X]\!] \twoheadrightarrow R^D_{V,\mathcal{O}}$. More concretely, if $\mathfrak{m}^D$ denotes the maximal ideal of $R^D_{V,\mathcal{O}}$, then the surjectivity condition is equivalent to $\dim_k \mathfrak{m}^D/(\lambda, (\mathfrak{m}^D)^2) \leq 1$.

It is straightforward to check (cf. [9, Lemma 2.38]) that the above notions are well-behaved with respect to extension of the field K. In particular, if K' is a finite extension of K with valuation ring $\mathcal{O}'$ and residue field k', then $\mathcal{O}' \otimes_{\mathcal{O}} R^D_{V,\mathcal{O}}$ is naturally isomorphic to $R^D_{V\otimes_k k',\mathcal{O}'}$ and τ is acceptable for $\overline{\rho}$ if and only if τ is acceptable for $\overline{\rho} \otimes_k k'$.

We make the following conjectures, although they are considerably stronger than the results that will actually be important in the sequel. What is important for the sequel is only the question of which ℓ-types are acceptable for a given $\overline{\rho}|_{G_\ell}$.

Conjecture 1.2.1. *A deformation $\rho : G_\ell \to \mathrm{GL}(M)$ of $\overline{\rho}$ to $\mathcal{O}'$ is weakly of type τ if and only if it is of type τ.*

Conjecture 1.2.2. *Suppose that $\tau = \tilde{\omega}^i \oplus \tilde{\omega}^j$. Then $R^D_{V,\mathcal{O}} \neq (0)$ if and only if $\overline{\rho}|_{I_\ell} \otimes_k \overline{k}$ is of one of the following three forms:*

- $\begin{pmatrix} \omega^{1+i} & * \\ 0 & \omega^j \end{pmatrix}$ *and in the case $j \equiv i \bmod \ell - 1$, $*$ is peu-ramifié (in the sense of Serre [40]),*
- $\begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^i \end{pmatrix}$ *and in the case $j \equiv i \bmod \ell - 1$, $*$ is peu-ramifié,*
- $\omega_2^{1+\{j-i\}+(\ell+1)i} \oplus \omega_2^{\ell-\{j-i\}+(\ell+1)j}$*, where $\{a\}$ denotes the unique integer in the range from 0 to $\ell - 2$ congruent to a modulo $\ell - 1$.*

In the first two of these three cases $R^D_{V,\mathcal{O}} \cong \mathcal{O}[\![X]\!]$ and so τ is acceptable for $\overline{\rho}$. In the last case, if $j \equiv i \bmod \ell - 1$, then $R^D_{V,\mathcal{O}} \cong \mathcal{O}[\![X]\!]$ and so τ is acceptable for $\overline{\rho}$.

Conjecture 1.2.3. *Suppose that $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{\ell m}$ where $m \in \mathbf{Z}/(\ell^2 - 1)\mathbf{Z}$ and $m = i + (\ell+1)j$ with $i = 1, \ldots, \ell$ and $j \in \mathbf{Z}/(\ell-1)\mathbf{Z}$. Then $R^D_{V,\mathcal{O}} \neq (0)$ if and only if $\overline{\rho}|_{I_\ell} \otimes_k \overline{k}$ is of one of the following four forms:*

- $\begin{pmatrix} \omega^{i+j} & * \\ 0 & \omega^{1+j} \end{pmatrix}$ *and in the case $i = 2$, $*$ is peu-ramifié,*
- $\begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^{i+j} \end{pmatrix}$ *and in the case $i = \ell - 1$, $*$ is peu-ramifié,*
- $\omega_2^{1+m} \oplus \omega_2^{\ell(1+m)}$,
- $\omega_2^{\ell+m} \oplus \omega_2^{1+\ell m}$,

In all these cases $R^D_{V,\mathcal{O}} \cong \mathcal{O}[\![X]\!]$ and so τ is acceptable for $\overline{\rho}$.

It will be convenient to say that a type τ is *strongly acceptable* for $\overline{\rho}|_{G_\ell}$ if it is acceptable and if one of the following is true:

- $\overline{\rho}|_{I_\ell} \cong \begin{pmatrix} \omega^m & * \\ 0 & \omega^n \end{pmatrix}$ for some $m, n \in \mathbf{Z}/(\ell-1)\mathbf{Z}$ (and in the case $m \equiv n+1 \bmod \ell-1$, $*$ is peu-ramifié), and τ is equivalent to $\tilde{\omega}^{m-1} \oplus \tilde{\omega}^n$ or $\tilde{\omega}_2^{\{m-n\}+1+(n-1)(\ell+1)} \oplus \tilde{\omega}_2^{\ell(\{m-n\}+1)+(n-1)(\ell+1)}$.
- $\overline{\rho}|_{I_\ell} \otimes_k \overline{k} \cong \omega_2^{1+m} \oplus \omega_2^{\ell(1+m)}$ for some $m \in \mathbf{Z}/(\ell^2-1)\mathbf{Z}$, and $\tau \cong \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{\ell m}$

Note that in particular we are conjecturing that we can suppress the assumption of acceptability in the definition of strong acceptability. In section 2 we shall explain what we know about these conjectures.

1.3. **Global Galois representations.** Fix a finite extension K of $\mathbf{Q}_\ell$ in $\overline{\mathbf{Q}}_\ell$ with valuation ring $\mathcal{O}$, uniformizer λ and residue field k, and a continuous global two-dimensional (over k) Galois representation

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}(V).$$

We shall suppose $\overline{\rho}$ satisfies the following hypotheses.

- The determinant of $\overline{\rho}(c)$ is -1, where c denotes a complex conjugation.
- The restriction of $\overline{\rho}$ to $\mathbf{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$ is absolutely irreducible.
- The conductor of $\overline{\rho}$ (see [40]) divides the conductor of all of its twists by $\overline{k}^\times$-valued characters.
- The centralizer of $\overline{\rho}(G_\ell)$ consists only of scalar matrices.

We remark that the third condition is simply for convenience and will be removed as an assumption from all our main theorems by an easy twisting argument. Let S be a finite set of rational primes which does not contain ℓ, and let $\tau : I_\ell \to \mathrm{GL}(D)$ be an ℓ-type which is strongly acceptable for $\overline{\rho}|_{G_\ell}$.

We will say that a deformation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(M)$ of $\overline{\rho}$ to an object R of $\mathcal{C}_{\mathcal{O}}^*$ (see Appendix A) is of type (S, τ) if the following hold:

- $\rho|_{G_\ell}$ is weakly of type τ.
- If $p \notin S \cup \{\ell\}$ and the order of $\overline{\rho}(I_p)$ is not ℓ, then $\rho(I_p) \xrightarrow{\sim} \overline{\rho}(I_p)$.
- If $p \notin S \cup \{\ell\}$ and the order of $\overline{\rho}(I_p)$ is ℓ, then M/M^{I_p} is free of rank one over R.
- $\epsilon^{-1} \det \rho$ has finite order prime to ℓ.

One checks that the subsets of deformations of type (S, τ) satisfy the representability criterion in Appendix A. Note that when $p \notin S \cup \{\ell\}$, $\overline{\rho}(I_p)$ has order ℓ, and the fourth condition above holds, then $\rho|_{I_p}$ is tame with $\det \rho|_{I_p}$ trivial, so if $g \in I_p^t$ is a topological generator, then a lift $\rho(g)$ of $\overline{\rho}(g)$ fixes a basis vector if and only if $\mathrm{tr}\rho(g) = 1 + \det(\rho(g))$ (which is equivalent to $(\rho(g)-1)^2 = 0$ in the present setting). We let $R_{V,\mathcal{O}}^{S,D}$ denote the universal type (S, τ) deformation ring. We write simply $R_{V,\mathcal{O}}$ and $R_{V,\mathcal{O}}^D$ for the deformation rings associated to $\overline{\rho}|_{G_\ell}$. Then $R_{V,\mathcal{O}}$, $R_{V,\mathcal{O}}^D$ and $R_{V,\mathcal{O}}^{S,D}$ are complete local Noetherian $\mathcal{O}$-algebras with residue field k, well-behaved with respect to finite extension of K.

1.4. **Galois cohomology.** We will let $\mathrm{ad}^0 V$ denote the representation of $G_{\mathbf{Q}}$ on the trace zero endomorphisms of V. The trace pairing gives rise to a Galois equivariant perfect pairing

$$\mathrm{ad}^0 V \otimes_k (\mathrm{ad}^0 V)(1) \to k(1).$$

If $\mathfrak{m}$ denotes the maximal ideal of $R_{V,\mathcal{O}}^D$, then there is a natural injective map from the k-dual of $\mathfrak{m}/(\lambda, \mathfrak{m}^2)$ to $H^1(\mathbf{Q}_\ell, \mathrm{ad}^0 V)$. Using the trace pairing and a k-linear

analogue of local Poitou-Tate duality we get a surjective map $H^1(\mathbf{Q}_\ell, (\mathrm{ad}^0 V)(1)) \to \mathfrak{m}/(\lambda, \mathfrak{m}^2)$. We will denote the kernel of this map by $H^1_D(\mathbf{Q}_\ell, \mathrm{ad}^0 V(1))$. We will let $H^1_{S,D}(\mathbf{Q}, (\mathrm{ad}^0 V)(1))$ denote those classes in $H^1(\mathbf{Q}, (\mathrm{ad}^0 V)(1))$ which localize trivially at all primes in S, to an element of $H^1_D(\mathbf{Q}_\ell, (\mathrm{ad}^0 V)(1))$ at ℓ, and to an element of $H^1(\mathbf{F}_p, ((\mathrm{ad}^0 V)(1))^{I_p})$ at all primes $p \notin S \cup \{\ell\}$.

Observe that for $p \notin S \cup \{\ell\}$ with $\overline{\rho}(I_p)$ not of order ℓ, the condition $\rho(I_p) \xrightarrow{\sim} \overline{\rho}(I_p)$ for a deformation ρ of $\overline{\rho}$ to $k[\epsilon]$ with $\det \rho = \det \overline{\rho}$ is *equivalent* to the splitting of the extension as a $k[I_p]$-module. To see this, let ρ be such a deformation of $\overline{\rho}$, so $\rho(g) = (1 + \epsilon c(g))\overline{\rho}(g)$ for $g \in I_p$, with the cocycle c representing an element of $H^1(I_p, \mathrm{ad}^0 \overline{\rho})$. We need to check that the cohomology class of c is zero. Suppose that $g, h \in I_p$ and $\overline{\rho}(h) = 1$. By our hypothesis on ρ, we have $c(h) = 0$, and since $c(gh) = \overline{\rho}(g)c(h)\overline{\rho}(g)^{-1} + c(g)$, it follows that $c(gh) = c(g)$. Thus, we can view c as representing an element of $H^1(\overline{\rho}(I_p), \mathrm{ad}^0 \overline{\rho})$, and we must show that this element is zero. By restriction-inflation, $H^1(\overline{\rho}(I_p), \mathrm{ad}^0 \overline{\rho}) \cong H^1(G, (\mathrm{ad}^0 \overline{\rho})^{I_p^{\mathrm{w}}})$, where I_p^{w} is wild inertia at p and $G = \overline{\rho}(I_p)/\overline{\rho}(I_p^{\mathrm{w}})$. Since G is a finite discrete quotient of the tame inertia group at p, G is a cyclic group. Let $G(\ell)$ denote the ℓ-Sylow subgroup and $I_p^{(\ell)}$ the kernel of the map from I_p onto its maximal ℓ-primary quotient. By restriction-inflation we can identify c with an element of $H^1(G(\ell), (\mathrm{ad}^0 \overline{\rho})^{I_p^{(\ell)}})$. Since $G(\ell)$ is a finite cyclic group, the size of this H^1 cohomology group is the same as the size of the analogous H^0 group, which is $H^0(I_p, \mathrm{ad}^0 \overline{\rho})$.

Without loss of generality, we may assume $H^0(I_p, \mathrm{ad}^0 \overline{\rho}) \neq 0$ (so $G(\ell) \neq 0$ also). After making a finite extension of scalars on k (which we may do), $\overline{\rho}|_{I_p}$ is reducible and is a non-trivial extension of χ by itself, where $\chi : I_p \to k^\times$ is some continuous character. If χ is non-trivial, then the conductor $N(\overline{\rho})$ of $\overline{\rho}$ is divisible by p^2. But if we twist $\overline{\rho}$ by a global character $G_{\mathbf{Q}} \to k^\times$ whose restriction to I_p is χ^{-1} and which is unramified at all other primes, then this twist of $\overline{\rho}$ has conductor which has the same prime-to-p part as $N(\overline{\rho})$ but has p-part equal to p. By our hypothesis on the minimality of the conductor of $\overline{\rho}$, this is a contradiction. Thus, the above character χ must be trivial, so $\overline{\rho}$ is a non-trivial extension of 1 by 1. Since $\ell \neq p$, this forces $\overline{\rho}$ to be tame at p. The pro-cyclicity of tame inertia then forces $\overline{\rho}(I_p)$ to have order ℓ, contrary to hypothesis. Therefore, the original deformation ρ as a $k[I_p]$-module extension class of $\overline{\rho}$ by $\overline{\rho}$ must be the trivial extension, as desired. A similar argument (ending with the same analysis of $H^0(I_p, \mathrm{ad}^0 \overline{\rho})$) proves the analogue for $(\mathcal{O}/\lambda^n)[\epsilon]$-deformations of type (S, τ) of a fixed $\mathcal{O}/\lambda^n$-deformation of $\overline{\rho}$ of type (S, τ) (this is needed in the proof of Lemma 1.4.2 below). With this noted, the usual calculations give rise to the following lemma (see for example section 2 of [9], especially Corollary 2.43).

Lemma 1.4.1. *Suppose that τ is acceptable for $\overline{\rho}|_{G_\ell}$. Then $R^{S,D}_{V,\mathcal{O}}$ can be topologically generated as an $\mathcal{O}$-algebra by*

$$\dim_k H^1_{S,D}(\mathbf{Q}, (\mathrm{ad}^0 V)(1)) + \sum_{p \in S} \dim_k H^0(\mathbf{Q}_p, (\mathrm{ad}^0 V)(1))$$

elements.

The proof of this lemma makes essential use of the assumption that τ is acceptable for $\overline{\rho}|_{G_\ell}$. More precisely, the acceptability hypothesis enables the local contribution at ℓ to 'exactly cancel' the local contribution (of $\dim H^0(\mathbf{R}, \mathrm{ad}^0 \overline{\rho}) = 1$) at ∞.

Now suppose that we are given a deformation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(M)$ of $\overline{\rho}$ of type (S, τ) to $\mathcal{O}$. Let $\theta^{S,D} : R^{S,D}_{V,\mathcal{O}} \to \mathcal{O}$, $\theta^D : R^D_{V,\mathcal{O}} \to \mathcal{O}$ and $\theta : R_{V,\mathcal{O}} \to \mathcal{O}$ denote the corresponding homomorphisms. We let $\mathrm{ad}\, M$ and $\mathrm{ad}^0 M$ denote the representations of $G_{\mathbf{Q}}$ on the endomorphisms and trace-zero endomorphisms of M respectively. Let $H^1_D(\mathbf{Q}_\ell, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})$ denote the image of

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}}(\ker\theta^D/(\ker\theta^D)^2, K/\mathcal{O}) \quad &\longrightarrow \quad \mathrm{Hom}_{\mathcal{O}}(\ker\theta/(\ker\theta)^2, K/\mathcal{O}) \\ &\cong H^1(\mathbf{Q}_\ell, \mathrm{ad}\, M \otimes_{\mathcal{O}} K/\mathcal{O}). \end{aligned}$$

It is easy to see that the image is in fact contained in

$$H^1(\mathbf{Q}_\ell, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O}) \subset H^1(\mathbf{Q}_\ell, \mathrm{ad}\, M \otimes_{\mathcal{O}} K/\mathcal{O}).$$

We let $H^1_{S,D}(\mathbf{Q}, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})$ denote the set of elements of $H^1(\mathbf{Q}, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})$ which localise at ℓ to an element of $H^1_D(\mathbf{Q}_\ell, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})$ and at each prime $p \notin S \cup \{\ell\}$ to an element of $H^1(\mathbf{F}_p, (\mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})^{I_p})$. Note that for any particular $x \in H^1(\mathbf{Q}, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})$, the conditions at the $p \notin S \cup \{\ell\}$ are automatically satisfied for all but finitely many p. Therefore, we can argue by passage to the direct limit from the torsion cases, using the usual calculations to get the following lemma (see for example section 2 of [9]).

Lemma 1.4.2. *In the above situation we have an isomorphism of $\mathcal{O}$-modules*

$$\mathrm{Hom}_{\mathcal{O}}(\ker\theta^{S,D}/(\ker\theta^{S,D})^2, K/\mathcal{O}) \cong H^1_{S,D}(\mathbf{Q}, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O}).$$

This isomorphism is compatible with change in S.

Corollary 1.4.3. *Suppose that $p \notin S \cup \{\ell\}$, let $S' = S \cup \{p\}$ and let $\theta^{S',D}$ denote the composite $R^{S',D}_{V,\mathcal{O}} \to R^{S,D}_{V,\mathcal{O}} \to \mathcal{O}$. Then*

$$\begin{aligned} &\mathrm{length}_{\mathcal{O}}(\ker\theta^{S',D})/(\ker\theta^{S',D})^2 \\ &\quad \leq \mathrm{length}_{\mathcal{O}}(\ker\theta^{S,D})/(\ker\theta^{S,D})^2 + \mathrm{length}_{\mathcal{O}}(\mathrm{ad}^0 M)(1)^{I_p}/(\mathrm{Frob}_p - 1)(\mathrm{ad}^0 M)(1)^{I_p}. \end{aligned}$$

In this corollary, the lengths involved could a priori be infinite, so the inequality is understood to imply that if the right side is finite, then so is the left side. In order to see that the second term on the right (which might be infinite) has the same cardinality as $H^1(I_p, \mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O})^{G_p}$ (which is what arises in the calculation), we just need to observe that $\mathrm{ad}^0 M(1)$ is (via the trace pairing) Cartier dual to $\mathrm{ad}^0 M \otimes_{\mathcal{O}} K/\mathcal{O}$ and for any finite discrete G_p-module X with prime-to-p-power order n and Cartier dual X^*, the G_p/I_p-equivariant pairing (via cup product)

$$H^1(I_p, X) \times H^0(I_p, X^*) \to H^1(I_p, \mu_n) = H^1(I_p, \mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})(-1)$$

is a perfect pairing. This follows from [37, Ch I, §3.5, Prop 17, Rem 4] and the *proof* of [37, Ch II, §5, Thm 1].

2. Local Calculations

In this section, we study local deformation problems. Consider a continuous two-dimensional representation $\overline{\rho} : G_\ell \to \mathrm{GL}(V)$ over k. Choose a subfield $F \subseteq \overline{\mathbf{Q}}_\ell$ with finite degree over $\mathbf{Q}_\ell$ and with absolute ramification index $e = e(F) \leq \ell - 1$. We write A for the valuation ring of F, and I_F for the inertia subgroup of G_F.

A finite discrete G_ℓ-module $\rho : G_\ell \to \mathrm{Aut}(M)$ is called *A-flat* if there exists a finite flat commutative group scheme $\mathcal{G}$ over A and a G_F-module isomorphism $\rho|_{G_F} \simeq \mathcal{G}(\overline{\mathbf{Q}}_\ell)$. In this case, all subrepresentations and quotient representations are

also A-flat. If instead ρ is an inverse limit of finite discrete G_ℓ-modules, we say that ρ is A-*flat* if all finite discrete quotients of ρ are A-flat.

2.1. **A-ordinary deformations.** Assume that $\overline{\rho}$ is reducible and $\mathrm{End}_{k[G_\ell]} V = k$, so $\overline{\rho}$ is isomorphic to a non-semisimple representation

$$\overline{\rho} \simeq \begin{matrix} \psi_a\omega^m & * \\ 0 & \psi_b\omega^n \end{matrix}$$

for some $a, b \in k^\times$, $m, n \in \mathbf{Z}/(\ell-1)$ with $a \neq b$ or $m \neq n$ (where $\psi_x : G_\ell \to k^\times$ is the unique continuous unramified character sending Frob_ℓ to $x \in k^\times$). If $m \neq n+1$ or $a \neq b$, then $\dim_k H^1(G_\ell, (\psi_b\omega^n)^{-1}\psi_a\omega^m) = 1$, so the non-split condition implies that $\overline{\rho}$ is determined up to $k[G_\ell]$-module isomorphism by the specification (and ordering) of its diagonal characters. See the discussion above [6, Thm 2.4.4] for more details on this. In the case $m = n+1$, we assume $*$ is peu ramifié. This condition is automatically satisfied if $a \neq b$, and it is satisfied for a unique isomorphism class of representations in the case $a = b$.

In this section, we let F denote the unramified extension of $\mathbf{Q}_\ell(\mu_\ell)$ of degree $|k^\times|$ (so both diagonal characters of $\overline{\rho}$ are trivial on G_F). We say that a deformation M of $\overline{\rho}$ to an object R of $\mathcal{C}_{\mathcal{O}}^*$ is A-*ordinary* if its determinant is $\epsilon\eta$, with η the Teichmüller lift of $(\det\overline{\rho})\omega^{-1} : G_\ell \to k^\times$, and there is an exact sequence of $R[G_\ell]$-modules

$$0 \to M^{(-1)} \to M \to M^{(0)} \to 0$$

with $M^{(-1)}$ and $M^{(0)}$ free of rank one over R, and I_F acting via ϵ on $M^{(-1)}$ and trivially on $M^{(0)}$. (Note that the G_ℓ actions on $M^{(-1)}/\mathfrak{m}_R$ and $M^{(0)}/\mathfrak{m}_R$ are necessarily via $\psi_a\omega^m$ and $\psi_b\omega^n$ respectively.) Using the criterion in Appendix A, one checks that there is a universal A-ordinary deformation of $\overline{\rho}$, where in the case $m = n+1$ we also require that the twist of our deformations by $\tilde{\omega}^{-n}$ is $\mathbf{Z}_\ell$-flat. We let $R_{V,\mathcal{O}}^{A-\mathrm{ord}}$ denote the universal A-ordinary deformation ring, canonically a quotient of $R_{V,\mathcal{O}}$.

We shall now define a subspace of $H^1(G_\ell, \mathrm{ad}^0 V)$ denoted $H^1_{A-\mathrm{ord}}(G_\ell, \mathrm{ad}^0 V)$. Let $W^{(0)}$ denote the subspace of $\mathrm{ad}^0 V$ consisting of those trace-zero endomorphisms preserving the filtration

$$0 \to V^{(-1)} \to V \to V^{(0)} \to 0$$

(i.e., $W^{(0)}$ consists of matrices with lower left entry vanishing), and let $W^{(-1)} = \mathrm{Hom}_k(V^{(0)}, V^{(-1)}) \subset W^{(0)}$ (i.e., the matrices vanishing outside of the upper right entry). There are thus canonical exact sequences

$$0 \longrightarrow W^{(0)} \longrightarrow \mathrm{ad}^0 V \longrightarrow \mathrm{Hom}_k(V^{(-1)}, V^{(0)}) \longrightarrow 0, \quad \text{and}$$

$$0 \longrightarrow W^{(-1)} \longrightarrow W^{(0)} \longrightarrow \mathrm{Hom}_k(V^{(-1)}, V^{(-1)}) \longrightarrow 0.$$

We define a subspace C_1 of $H^1(I_\ell, W^{(-1)})$ as follows: If $m \neq n+1$, we let $C_1 = H^1(I_\ell, W^{(-1)})$. If $m = n+1$, then $W^{(-1)} \cong k(1)$ as $k[I_\ell]$-modules and we define C_1 to be the kernel of the map

$$H^1(I_\ell, W^{(-1)}) \cong H^1(I_\ell, k(1)) \cong (\mathbf{Q}_\ell^{\mathrm{un}})^\times \otimes k \to k,$$

where the second isomorphism is the Kummer map and the last homomorphism is induced by the valuation on $\mathbf{Q}_\ell^{\mathrm{un}}$. Let C_2 denote the image of C_1 in $H^1(I_\ell, W^{(0)})$, let C_3 denote the preimage of C_2 in $H^1(G_\ell, W^{(0)})$, and finally, let $H^1_{A-\mathrm{ord}}(G_\ell, \mathrm{ad}^0 V)$ be the image of C_3 under the natural inclusion.

Theorem 2.1.1. *There is a surjective homomorphism of $\mathcal{O}$-algebras*

$$\mathcal{O}[\![T]\!] \to R_{V,\mathcal{O}}^{A-\mathrm{ord}}.$$

Proof. Letting $\mathfrak{m}$ denote the maximal ideal $R_{V,\mathcal{O}}^{A-\mathrm{ord}}$, it suffices to prove $\mathfrak{m}/(\lambda,\mathfrak{m}^2)$ is at most one-dimensional over k. This is done by checking that the image of $\mathrm{Hom}_k(\mathfrak{m}/(\lambda,\mathfrak{m}^2),k)$ in $H^1(G_\ell,\mathrm{ad}\,V)$ is contained in $H^1_{A-\mathrm{ord}}(G_\ell,\mathrm{ad}^0\,V)$, and then computing the dimension of this subspace. See the *proof* of [46, Prop 1.9(*iii*)] for the case $m \neq n+1$ (recall that $\overline{\rho}(G_\ell)$ has trivial centralizer) and see [9, 2.4] for the case $m = n+1$. ∎

Now suppose that $\rho : G_\ell \to \mathrm{GL}_2(\mathcal{O}')$ is a deformation of $\overline{\rho}$ of type τ, with $\tau = \tilde{\omega}^i \oplus \tilde{\omega}^j$ for some i and j. In this case there is an ℓ-divisible group Γ over A with an action of $\mathcal{O}'$ such that $\rho|_{G_F}$ is isomorphic to the representation defined by the action of $\mathcal{O}'[G_F]$ on the Tate module of Γ:

$$M = \mathrm{proj\,lim}\,\Gamma[\ell^n](\overline{\mathbf{Q}}_\ell).$$

The canonical connected-étale sequence for Γ gives rise to an exact sequence

$$0 \to M^0 \to M \to M^{\text{ét}} \to 0$$

of free $\mathcal{O}'$-modules with an action of G_F.

Lemma 2.1.2. *The $\mathcal{O}'$-modules M^0 and $M^{\text{ét}}$ are each free of rank one, and I_F acts via ϵ on M^0.*

Proof. First observe that it suffices to prove that $M^{\text{ét}} \neq 0$, for I_F acts trivially on $M^{\text{ét}}$ and $\det \rho|_{I_F} = \epsilon$.

Suppose now that $M^{\text{ét}} = 0$, so $\Gamma[\ell]$ is connected. Since $V \cong M/\lambda M$ has a nonzero element fixed by G_F, the same is true of

$$(M/\ell M)[\lambda] \subset \Gamma[\ell](\overline{\mathbf{Q}}_\ell).$$

Therefore there is a nontrivial map

$$\mu_{\ell,F} = (\mathbf{Z}/\ell\mathbf{Z})_{/F} \to \Gamma[\ell]_{/F} \to \Gamma[\ell].$$

Since $\Gamma[\ell]$ is connected and $e = \ell - 1$, the schematic closure of the image is isomorphic to $\mu_{\ell,A}$. It follows that the Cartier dual of $\Gamma[\ell]$ is not connected.

Now let Γ^D denote the dual ℓ-divisible group, and M^D its Tate module. As $\mathcal{O}'[G_F]$-modules, we have

$$M^D \cong \mathrm{Hom}_{\mathbf{Z}_\ell}(M,\mathbf{Z}_\ell(1)) \cong \mathrm{Hom}_{\mathcal{O}'}(M,\mathcal{O}'(1))$$

(the first isomorphism is canonical, the second depends on a choice of generator for the different of $\mathcal{O}'$). We have just proved that $\Gamma^D[\ell]$ is not connected, so $M^{D,\text{ét}} \neq 0$. The lemma follows on observing that the first paragraph of the proof now applies to M^D, showing that I_F acts via ϵ on $M^{D,0} \neq 0$.

∎

We can now deduce the following from Theorem 2.1.1.

Corollary 2.1.3. *Suppose that $\overline{\rho}$ is reducible with $\mathrm{End}_{k[G_\ell]}V = k$. If $\overline{\rho}$ admits a lifting of type $\tau : I_\ell \to \mathrm{GL}(D)$ (i.e., if $R^D_{V,\mathcal{O}} \neq 0$) with $\tau \cong \tilde{\omega}^i \oplus \tilde{\omega}^j$, then τ is acceptable for $\overline{\rho}$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $R_{V,\mathcal{O}}$ of type τ, so $\mathfrak{p}$ is the kernel of a homomorphism $R_{V,\mathcal{O}} \to \mathcal{O}'$ such that the associated deformation to $\mathcal{O}'$ is of type τ. The lemma (along with [16, Prop 8.2] in case $m = n+1$) shows this deformation is A-ordinary, so the map $R_{V,\mathcal{O}} \to \mathcal{O}'$ factors through $R_{V,\mathcal{O}}^{A-\mathrm{ord}}$. Therefore the kernel of the map

$$R_{V,\mathcal{O}} \to R_{V,\mathcal{O}}^{A-\mathrm{ord}}$$

is contained in the intersection of all prime ideals $\mathfrak{p}$ of type τ. It follows that $R_{V,\mathcal{O}}^{D}$ is a quotient of $R_{V,\mathcal{O}}^{A-\mathrm{ord}}$, hence a quotient of $\mathcal{O}[\![T]\!]$.

■

2.2. **A-flat deformations.** Now we return to the case of arbitrary F with $e \leq \ell-1$. We no longer assume that $\overline{\rho}$ is reducible. We assume that V is A-flat, with $\mathcal{G}$ connected and having connected dual. Under these conditions, $\mathcal{G}$ is the unique finite flat A-group scheme with generic fiber isomorphic (as a G_F-module) to $\overline{\rho}|_{G_F}$, with $\mathcal{G}$ determined up to unique isomorphism (see [6, §2.1] for details; the connectedness conditions ensure uniqueness when $e = \ell - 1$).

Let M denote the (contravariant) Dieudonné module of the closed fiber of $\mathcal{G}$. We assume that the canonical sequence of groups

$$0 \to M/VM \xrightarrow{F} M = M/\ell M \to M/FM \to 0$$

is *exact*, where F and V denote the Frobenius and Verschiebung operators respectively. This exactness condition is automatically satisfied when $\mathcal{G} \simeq \Gamma[\ell]$ for $\Gamma_{/A}$ an ℓ-divisible group, and so is an extremely natural condition; also, it is needed in the results we will require from [6] below.

We now give the complete list of isomorphism classes of representations $\overline{\rho}$ satisfying the above conditions. (See Corollary 2.2.3 and Theorem 2.4.4 of [6].) The irreducible $\overline{\rho}$ which arise are absolutely irreducible and are exactly those continuous $\overline{\rho} : G_\ell \to \mathrm{GL}_2(k)$ satisfying $\overline{\rho}|_{I_\ell} \otimes_k \bar{k} \simeq \omega_2^m \oplus \omega_2^{\ell m}$, with $em \equiv e \bmod \ell^2 - 1$. The reducible $\overline{\rho}$ which arise can be written as non-semisimple representations

$$\overline{\rho} \simeq \begin{matrix} \psi_a\omega^m & * \\ 0 & \psi_b\omega^n \end{matrix}$$

for $a, b \in k^\times$, $m, n \in \mathbf{Z}/(\ell-1)$. The precise possibilities are as follows. There must exist an integer j satisfying $1 \leq j \leq e-1$, $en \equiv j \bmod \ell - 1$, $e | j(\ell+1)$ and $m = n + 1 - j(\ell+1)/e \bmod \ell - 1$. These conditions imply $e \not| (\ell-1)$, $m \neq n$, and for $\ell \equiv -1 \bmod 4$ they also imply $m \neq n+1$. For $\ell \equiv -1 \bmod 4$, the unique (up to isomorphism) non-split extensions of $\psi_b\omega^n$ by $\psi_a\omega^m$ for $a, b \in k^\times$ and n and m as above are exactly the $\overline{\rho}$ which arise. For $\ell \equiv 1 \bmod 4$, we get the same list, except that the cases with $m = n+1$ (which occur precisely when $e = (\ell+1)/2$, $n = (\ell-1)/2$) and $a = b$ are given by the unramified k-twists the (unique up to isomorphism) non-split $\mathbf{F}_\ell$-representation of the form

$$\omega^{(\ell-1)/2} \otimes \begin{matrix} \omega & * \\ 0 & 1 \end{matrix}$$

for which $*$ is peu-ramifié.

The property of being A-flat is closed under taking submodules, quotients and finite products, and since $\mathrm{End}_{k[G_\ell]} V = k$ for the representations listed above, there is an associated universal A-flat deformation ring $R_{V,\mathcal{O}}^{A-\mathrm{flat}}$ which is a quotient of $R_{V,\mathcal{O}}$. Consider also the fixed determinant character $\chi : G_\ell \to \mathcal{O}^\times$ of the form $\epsilon\eta$,

with η the Teichmüller lift of $(\det \overline{\rho})\omega^{-1} : G_\ell \to k^\times$. There is a universal deformation of $\overline{\rho}$ which is A-flat with determinant χ, and the universal deformation ring is naturally a quotient of $R_{V,\mathcal{O}}^{A-\mathrm{flat}}$ which we denote $R_{V,\mathcal{O}}^{A-\mathrm{flat},\chi}$. The main deformation-theoretic result we need in the local theory is provided by Theorems 4.1.1 and 4.1.2 of [6].

Theorem 2.2.1. *There are $\mathcal{O}$-algebra isomorphisms*

$$R_{V,\mathcal{O}}^{A-\mathrm{flat}} \simeq \mathcal{O}[\![T_1, T_2]\!] \quad \textit{and} \quad R_{V,\mathcal{O}}^{A-\mathrm{flat},\chi} \simeq \mathcal{O}[\![T]\!].$$

Corollary 2.2.2. *If $\overline{\rho}$ admits a lifting of type $\tau : I_\ell \to \mathrm{GL}(D)$ (i.e., if $R_{V,\mathcal{O}}^{D} \neq 0$) and τ is trivial on the inertia group of F, then τ is acceptable for $\overline{\rho}$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $R_{V,\mathcal{O}}$ of type τ, so $\mathfrak{p}$ is the kernel of a homomorphism $R_{V,\mathcal{O}} \to \mathcal{O}'$ such that the associated deformation to $\mathcal{O}'$ is of type τ. Replacing $\mathcal{O}$ by $\mathcal{O}'$ without loss of generality, the determinant χ of this deformation is $\mathcal{O}^\times$-valued, so our map $R_{V,\mathcal{O}} \to \mathcal{O}$ factors through $R_{V,\mathcal{O}}^{A-\mathrm{flat},\chi}$. Therefore the kernel of the map

$$R_{V,\mathcal{O}} \to R_{V,\mathcal{O}}^{A-\mathrm{flat},\chi}$$

is contained in the intersection of all prime ideals $\mathfrak{p}$ of type τ. It follows that $R_{V,\mathcal{O}}^{D}$ is a quotient of $R_{V,\mathcal{O}}^{A-\mathrm{flat},\chi}$, which, by the preceding theorem, is isomorphic to $\mathcal{O}[\![T]\!]$. ∎

2.3. **Twisted A-flat deformations.** We now consider a variant of the A-flat deformation problem. We still fix a finite extension $F/\mathbf{Q}_\ell$ with $e(F) \leq \ell - 1$ and study certain deformations of a given $\overline{\rho} : G_\ell \to \mathrm{GL}_2(k)$. However, instead of requiring $\overline{\rho}|_{G_F}$ to arise as the generic fiber of a finite flat A-group scheme, we fix a (ramified) quadratic character ψ on G_F and require that $\overline{\rho}|_{G_F} \otimes \psi$ is the generic fiber of a finite flat A-group scheme. Moreover, we impose the same connectedness/unipotence conditions and the same exactness hypothesis on Dieudonné modules as above, and we study those deformations of $\overline{\rho}$ whose ψ-twist is A-flat (in the same sense as above). In contrast to the (untwisted) A-flat setting, the case $e|(\ell - 1)$ can now occur, and we shall actually restrict our attention to this case. In §4.2 of [6], it is explained how the methods of [6] carry over to this setting. In particular, under the above hypotheses, $\mathrm{End}_{k[G_\ell]} V = k$, so there is a universal deformation ring $R_{V,\mathcal{O}}$ for $\overline{\rho}$. The property of the ψ-twist being A-flat is preserved under taking submodules, quotients and finite products, so there is an associated quotient of $R_{V,\mathcal{O}}$, which we denote $R_{V,\mathcal{O}}^{A-\psi\otimes\mathrm{flat}}$. We can also consider the quotient $R_{V,\mathcal{O}}^{A-\psi\otimes\mathrm{flat},\chi}$ representing such deformations with fixed determinant $\chi = \epsilon\eta$. Theorem 4.2.1 of [6] then gives:

Theorem 2.3.1. *Under the above hypotheses, there are $\mathcal{O}$-algebra isomorphisms*

$$R_{V,\mathcal{O}}^{A-\psi\otimes\mathrm{flat}} \simeq \mathcal{O}[\![T_1, T_2]\!] \quad \textit{and} \quad R_{V,\mathcal{O}}^{A-\psi\otimes\mathrm{flat},\chi} \simeq \mathcal{O}[\![T]\!].$$

Corollary 2.3.2. *Suppose that $e(F)|(\ell - 1)$, ψ is a quadratic character of G_F and $\tau\otimes\psi$ is trivial on the inertia group of F. If $\overline{\rho}$ admits a lifting of type $\tau : I_\ell \to \mathrm{GL}(D)$ (i.e., if $R_{V,\mathcal{O}}^{D}(\overline{\rho}) \neq 0$) and $\overline{\rho} \otimes \psi$ is A-flat and satisfies the above connectedness, unipotence and Dieudonné module hypotheses, then τ is acceptable for $\overline{\rho}$.*

3. Some Representations of Finite Groups

3.1. **Representations of $\mathrm{GL}_2(\mathbf{F}_p)$.** Let us recall the classification of irreducible finite-dimensional representations of $\mathrm{GL}_2(\mathbf{F}_p)$ over an algebraically closed field F of characteristic zero. Any such representation is isomorphic to one of the following, where we have fixed an embedding $i : \mathbf{F}_{p^2} \to M_2(\mathbf{F}_p)$ corresponding to a choice of $\mathbf{F}_p$-basis of $\mathbf{F}_{p^2}$.

- For any character $\chi : \mathbf{F}_p^\times \to F^\times$, the representation $\chi \circ \det$.
- For any character $\chi : \mathbf{F}_p^\times \to F^\times$, the representation $\mathrm{sp}_\chi = \mathrm{sp} \otimes (\chi \circ \det)$, where sp is the representation of $\mathrm{GL}_2(\mathbf{F}_p)$ on the space of functions $\mathbf{P}^1(\mathbf{F}_p) \to F$ with average value zero (with $g \in \mathrm{GL}_2(\mathbf{F}_p)$ acting on a function through the usual action of g^{-1} on $\mathbf{P}^1(\mathbf{F}_p)$).
- For any pair of characters $\chi_1 \neq \chi_2 : \mathbf{F}_p^\times \to F^\times$, the representation $I(\chi_1, \chi_2)$ on the space of functions $f : \mathrm{GL}_2(\mathbf{F}_p) \to F$ which satisfy

$$f\left(\begin{matrix} a_1 & b \\ 0 & a_2 \end{matrix} g\right) = \chi_1(a_1)\chi_2(a_2) f(g),$$

  where $g \in \mathrm{GL}_2(\mathbf{F}_p)$ acts on f through right multiplication of g on $\mathrm{GL}_2(\mathbf{F}_p)$. This representation is isomorphic to the representation induced from the following character on the subgroup of upper-triangular matrices in $\mathrm{GL}_2(\mathbf{F}_p)$:

$$\begin{matrix} a_1 & b \\ 0 & a_2 \end{matrix} \mapsto \chi_1(a_1)\chi_2(a_2).$$

- For any character $\chi : \mathbf{F}_{p^2}^\times \to F^\times$ with $\chi \neq \chi^p$, a representation $\Theta(\chi)$ of dimension $p-1$ which is characterized by

$$\Theta(\chi) \otimes \mathrm{sp} \simeq \mathrm{Ind}_{\mathbf{F}_{p^2}^\times}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi.$$

The only isomorphisms between these representations are $I(\chi_1, \chi_2) \cong I(\chi_2, \chi_1)$ and $\Theta(\chi) \cong \Theta(\chi^p)$. For convenience, we include the character table of $\mathrm{GL}_2(\mathbf{F}_p)$:

Conjugacy class of:	Representation			
	$\chi \circ \det$	sp_χ	$I(\chi_1, \chi_2)$	$\Theta(\chi)$
$\begin{matrix} a & 0 \\ 0 & a \end{matrix}$	$\chi(a)^2$	$p\chi(a)^2$	$(p+1)\chi_1(a)\chi_2(a)$	$(p-1)\chi(a)$
$\begin{matrix} a & 1 \\ 0 & a \end{matrix}$	$\chi(a)^2$	0	$\chi_1(a)\chi_2(a)$	$-\chi(a)$
$\begin{matrix} a & 0 \\ 0 & b \end{matrix} \notin \mathbf{F}_p^\times$	$\chi(ab)$	$\chi(ab)$	$\chi_1(a)\chi_2(b) + \chi_1(b)\chi_2(a)$	0
$i(c) \notin \mathbf{F}_p^\times$	$\chi(c^{p+1})$	$-\chi(c^{p+1})$	0	$-\chi(c) - \chi(c^p)$

We recall also the classification of absolutely irreducible finite-dimensional representations of $\mathrm{GL}_2(\mathbf{F}_\ell)$ in characteristic ℓ. We will let σ_n denote the natural representation of $\mathrm{GL}_2(\mathbf{F}_\ell)$ on $\mathrm{Symm}^n(\mathbf{F}_\ell^2)$ for each $n \in \mathbf{Z}_{\geq 0}$. The semsimplicity of σ_n follows from that of σ_1, and for $n \leq \ell - 1$ the representation σ_n is absolutely irreducible (cf. [8, Example 17.17]). For $m \in \mathbf{Z}/(\ell-1)\mathbf{Z}$ and $0 \leq n \leq \ell - 1$, we will let

$\sigma_{n,m}$ denote $\sigma_n \otimes \det^m$. These representations $\sigma_{n,m}$ are mutually non-isomorphic and exhaust the isomorphism classes of absolutely irreducible finite-dimensional representations of $\mathrm{GL}_2(\mathbf{F}_\ell)$ in characteristic ℓ. The Brauer character of $\sigma_{n,m}$ is given by:

$$\begin{array}{lll} \begin{matrix} a & 0 \\ 0 & a \end{matrix} & \mapsto & (n+1)\tilde{a}^{2m+n}, \\ \\ \begin{matrix} a & 0 \\ 0 & b \end{matrix} \quad \notin \mathbf{F}_\ell^\times & \mapsto & \tilde{a}^m\tilde{b}^m(\tilde{a}^{n+1}-\tilde{b}^{n+1})/(\tilde{a}-\tilde{b}), \\ \\ i(c) \notin \mathbf{F}_\ell^\times & \mapsto & \tilde{c}^{m(\ell+1)}(\tilde{c}^{(n+1)\ell}-\tilde{c}^{n+1})/(\tilde{c}^\ell-\tilde{c}), \end{array}$$

where $\tilde{}$ indicates Teichmüller lift. In fact, since the $\sigma_{n,m}$ are defined over $\mathbf{F}_\ell$, any irreducible finite-dimensional representation of $\mathrm{GL}_2(\mathbf{F}_\ell)$ over a field k of characteristic ℓ is isomorphic to some $\sigma_{n,m} \otimes_{\mathbf{F}_\ell} k$ and so is absolutely irreducible. Using Brauer characters, one finds:

Lemma 3.1.1. *Let L be a finite free $\mathcal{O}$-module with an action of $\mathrm{GL}_2(\mathbf{F}_\ell)$ such that $V = L \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell$ is irreducible.*

(1) *If $V \cong \chi \circ \det$ with $\chi(a) = \tilde{a}^m$, then $L \otimes_{\mathcal{O}} k \cong \sigma_{0,m}$.*
(2) *If $V \cong \mathrm{sp}_\chi$ with $\chi(a) = \tilde{a}^m$, then $L \otimes_{\mathcal{O}} k \cong \sigma_{\ell-1,m}$.*
(3) *If $V \cong I(\chi_1, \chi_2)$ with $\chi_i(a) = \tilde{a}^{m_i}$ (for distinct $m_i \in \mathbf{Z}/(\ell-1)\mathbf{Z}$), then $L \otimes_{\mathcal{O}} k$ has two Jordan-Hölder subquotients: $\sigma_{\{m_1-m_2\},m_2}$ and $\sigma_{\{m_2-m_1\},m_1}$; where $0 < \{m\} < \ell-1$ and $\{m\} \equiv m \bmod \ell-1$.*
(4) *If $V \cong \Theta(\chi)$ with $\chi(c) = \tilde{c}^{i+(\ell+1)j}$ where $1 \le i \le \ell$ and $j \in \mathbf{Z}/(\ell-1)\mathbf{Z}$, then $L \otimes_{\mathcal{O}} k$ has one or two Jordan-Hölder subquotients: $\sigma_{i-2,1+j}$ and $\sigma_{\ell-1-i,i+j}$. Both occur unless $i = 1$ (when only the second one occurs) or $i = \ell$ (when only the first occurs), and in either of these exceptional cases $L \otimes_{\mathcal{O}} k \cong \sigma_{\ell-2,,1+j}$.*

3.2. **Representations of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$.** We shall also need to consider certain representations of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ for $n > 1$ which generalize the representations $\Theta(\chi)$ for $n = 1$. Let σ denote Frob_p on $A = W(\mathbf{F}_{p^2})$, choose an isomorphism

$$M_2(\mathbf{Z}_p) \cong \mathrm{End}_{\mathbf{Z}_p} A = A \oplus A\sigma,$$

and let ϖ_n denote the projection $\mathrm{GL}(A) \to G = \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Let $m = [n/2] \ge 1$ and define subgroups $N \subset H$ of G as follows:

$$\begin{aligned} N &= \varpi_n\left(\{\, x + y\sigma \mid x \in 1 + p^n A, y \in p^{n-m}A \,\}\right) \\ H &= \varpi_n\left(\{\, x + y\sigma \mid x \in A^\times, y \in p^m A \,\}\right). \end{aligned}$$

Thus $[N : 1] = p^{2m}$ and $[G : H] = \phi(p^{2m})$. Note that N is normal in H and H contains the center of G.

Again let F denote an algebraically closed field of characteristic 0. Suppose that $\chi : A^\times \to F^\times$ is a character of conductor p^n. We assume also that $\chi/(\chi \circ \sigma)$ has conductor p^n (or equivalently, no twist of χ by a character factoring through the norm $A^\times \to \mathbf{Z}_p^\times$ has conductor less than p^n; see [24, §3.2]). Since the quotient group $\mathbf{F}_{p^2}/\mathbf{F}_p$ is of order p, this latter condition implies that for any $x \in A^\times$ with $x \not\equiv x^\sigma \bmod pA$, $(\chi/\chi \circ \sigma)(1 + p^{n-1}x) \ne 1$. If n is even, we define a character β_χ of

H/N by $\beta_\chi(x+y\sigma) = \chi(x)$. If n is odd, we let β_χ denote the unique p-dimensional representation of H/N whose character satisfies

$$\operatorname{tr}\beta_\chi(x+y\sigma) = \begin{cases} p\chi(x), & \text{if } y \equiv 0 \bmod p^{m+1}A = p^{n-m}A \text{ and } x \equiv x^\sigma \bmod pA; \\ -\chi(x), & \text{if } y \equiv 0 \bmod p^{m+1}A = p^{n-m}A \text{ and } x \not\equiv x^\sigma \bmod pA; \\ 0, & \text{if } x+y\sigma \text{ is not conjugate to an element as above.} \end{cases}$$

Note that since the above class function satisfies $\langle \operatorname{tr}\beta_\chi, \operatorname{tr}\beta_\chi\rangle_{H/N} = 1$, the existence of such a representation can be proved using Brauer's criterion [38, §11.1], and it is absolutely irreducible. Regarding β_χ as a representation of H, let $\Theta(\chi)$ denote the $\phi(p^n)$-dimensional representation $\operatorname{Ind}_H^G \beta_\chi$. The isomorphism class of $\Theta(\chi)$ is independent of the choice of isomorphism $M_2(\mathbf{Z}_p) \cong \operatorname{End}_{\mathbf{Z}_p} A$, since any two such isomorphisms differ by conjugation by an element of $\mathrm{GL}_2(\mathbf{Z}_p)$. So far, the only conductor hypothesis we have used is that χ has conductor dividing p^n.

Lemma 3.2.1. *Suppose that $n \geq 1$ and χ_1 and χ_2 are a pair of characters of $A^\times \to \overline{\mathbf{Q}}_\ell^\times$ as above. Suppose that L_i for $i = 1, 2$, is a free $\mathcal{O}$-module with an action of $G = \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ such that $L_i \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell$ is isomorphic to $\Theta(\chi_i)$. Let B denote the subgroup of G consisting of matrices which mod p are upper triangular, and let $C = A^\times \cap B = \{x \in A^\times | x \equiv x^\sigma \bmod p\}$.*

1. *The restrictions $\Theta(\chi_i)|_B$ are irreducible,*
2. *$\Theta(\chi_1) \simeq \Theta(\chi_2) \Leftrightarrow \chi_2 \in \{\chi_1, \chi_1 \circ \sigma\}$,*
3. *$\Theta(\chi_1)|_B \simeq \Theta(\chi_2)|_B \Leftrightarrow \chi_2|_C \in \{\chi_1|_C, \chi_1 \circ \sigma|_C\}$,*
4. *if $p(p-1)$ is not divisible by ℓ, then $L_i \otimes_{\mathcal{O}} k$ is absolutely irreducible,*
5. *if $\chi_1 \equiv \chi_2 \bmod \lambda$, then $L_1 \otimes_{\mathcal{O}} k$ and $L_2 \otimes_{\mathcal{O}} k$ have isomorphic semisimplifications.*

Proof. The second assertion is proved by computing $\langle \Theta(\chi_1), \Theta(\chi_2)\rangle_G$ and showing that this equals 1 if $\chi_2 = \chi_1$ or if $\chi_2 = \chi_1 \circ \sigma$, and equals 0 otherwise. This uses the hypotheses on conductors, as we now explain. Using Frobenius reciprocity twice and [38, §7.3], we get

$$\langle \Theta(\chi_1), \Theta(\chi_2)\rangle_G = \sum_{g \in X} \langle \beta_{\chi_1}^g, \beta_{\chi_2}\rangle_{H_g},$$

where X is a set of double coset representatives for $H\backslash G/H$, $H_g = H \cap gHg^{-1}$, and $\beta_{\chi_1}^g(z) = \beta_{\chi_1}(g^{-1}zg)$. Note that 1 and σ represent two distinct double cosets, and $H\sigma = \sigma H$, so $H_\sigma = H$. By computing conjugacy classes in H/N and treating separately the cases where n is even or odd, we compute that

$$\langle \beta_{\chi_1}, \beta_{\chi_2}\rangle_H = \langle \beta_{\chi_1}, \beta_{\chi_2}\rangle_{H/N} = \langle \chi_1, \chi_2\rangle_{A^\times}.$$

Since $\beta_\chi^\sigma = \beta_{\chi\circ\sigma}$ and $\chi \neq \chi \circ \sigma$ for our characters $\chi = \chi_i$, the sum of the terms for $g = 1$ and $g = \sigma$ is 1 if $\chi_2 \in \{\chi_1, \chi_1 \circ \sigma\}$, and is 0 otherwise.

For $g \in X$ not equivalent to 1 or σ, we claim that $\langle \beta_{\chi_1}, \beta_{\chi_2}\rangle_{H_g} = 0$. It suffices to construct $h \in H \cap gNg^{-1}$ of the form $h = 1 + p^{n-1}(t - t^\sigma) + p^{n-m}s\sigma$ for $t \in A^\times$ with $t \not\equiv t^\sigma \bmod pA$ and $s \in A$, because then on the subgroup of H_g generated by h, $\beta_{\chi_1}^g$ is a direct sum of copies of the trivial representation (since $g^{-1}hg \in N$) and β_{χ_2} is a direct sum of copies of a *non-trivial* character (the number of copies being 1 when n is even and p when n is odd). This non-triviality follows from the fact that on the subgroup in H/N generated by h, β_{χ_2} is a direct sum of copies of the 1-dimensional representation which sends h to

$$\chi_2(1 + p^{n-1}(t - t^\sigma)) = (\chi_2/\chi_2 \circ \sigma)(1 + p^{n-1}t) \neq 1.$$

Since σ and H normalize N, we may multiply g on the right by σ or an element of H without changing gNg^{-1}, and hence without loss of generality.

To construct h, we write $g = x + y\sigma$ and first multiply by σ if necessary so that x is not divisible by p and then multiply by $x^{-1} \in H$ to get a representative of the form $g = 1 + p^r u\sigma$, with $u \not\equiv 0 \bmod pA$ and $r < m$. Note that for $r = 0$, the invertibility of $1+u\sigma$ forces $uu^\sigma \not\equiv 1 \bmod p\mathbf{Z}_p$, because $\det(x+y\sigma) = \mathrm{N}x - \mathrm{N}y$ for all $x, y \in A$, where $\mathrm{N} : A \to \mathbf{Z}_p$ is the norm map. Now define $h = g(1+p^{n-r-1}v\sigma)g^{-1}$, where $v \in A^\times$ is chosen so that $uv^\sigma \not\equiv vu^\sigma \bmod pA$ (in which case we can take $t = uv^\sigma$ when $r \neq 0$ and $t = uv^\sigma/(1-uu^\sigma)$ if $r = 0$). For the first and third assertions, after changing the isomorphism $M_2(\mathbf{Z}_p) \cong \mathrm{End}_{\mathbf{Z}_p}(A)$ we can suppose that $\sigma \in B$. Thus, for $g \in B$, $g \in H \cap B$ if and only if $g \in H$ and $g \in (H \cap B)\sigma$ if and only if $g \in H\sigma$. In particular, if $g \notin (H \cap B) \cup (H \cap B)\sigma$ then we can construct the h as above and this also lies in B since $h \equiv 1 \bmod p$. Since $G = BH$,

$$\Theta(\chi)|_B \cong \mathrm{Ind}_{H\cap B}^B(\beta_\chi|_{H\cap B}).$$

We can now run through the exact same calculation as before with B and $H \cap B$ replacing G and H respectively. This settles the first and third assertions (note that $\chi_1|_C \neq \chi_1 \circ \sigma|_C$ because $\chi_1/\chi_1 \circ \sigma$ has conductor p^n and $n \geq 2$).

If ℓ doesn't divide $p(p-1)$, so $\#B$ is not divisible by ℓ, then the reductions $L_i \otimes_{\mathcal{O}} k$ are also absolutely irreducible by [38, §15.5]. The last assertion follows since the two representations have the same Brauer character.

■

3.3. **Duality.** Let K, $\mathcal{O}$, λ and k be as above, and let $\mathcal{O}'$ denote the valuation ring of $K' = K(\lambda')$, where $\lambda'^2 = \lambda$. Suppose that V is a K-vector space with an action of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ such that $V \otimes_K \overline{\mathbf{Q}}_\ell$ is one of the representations considered above, i.e., that $n = 1$ and V is absolutely irreducible, or that $n > 1$ and $V \otimes_K \overline{\mathbf{Q}}_\ell$ is isomorphic to $\Theta(\chi)$ for some character $\chi : A^\times \to \overline{\mathbf{Q}}_\ell^\times$ with conductor p^n such that $\chi/\chi \circ \sigma$ also has conductor p^n. In each case, there is a nondegenerate pairing $(\ ,\ )$ on V such that

$$(gu, gv) = \psi(\det g)(u, v),$$

where $\psi : (\mathbf{Z}/p^n\mathbf{Z})^\times \to K^\times$ is the central character of the representation (note that ψ necessarily takes values in K since V is absolutely irreducible). Equivalently, we have an isomorphism of representation spaces $V \simeq V^* \otimes (\psi \circ \det)$ in all cases. For $n = 1$, this is clear from the character table, and for $\Theta(\chi)$ with $n > 1$, this follows from the analogous assertion for β_χ. More precisely, using the fact that $\det(x + y\sigma) = xx^\sigma \in \mathbf{Z}_p^\times$ for $x + y\sigma \in H$ with $y \equiv 0 \bmod p^{m+1}A$ for odd n, one checks that $\beta_\chi \cong \beta^*_{\chi\circ\sigma} \otimes (\psi \circ \det)|H$, where $\psi = \chi|_{(\mathbf{Z}/p^n\mathbf{Z})^\times}$ (and then induct up to G, using that $\Theta(\chi) = \Theta(\chi \circ \sigma)$).

We will need the following lemma.

Lemma 3.3.1. *Suppose G is a finite group which acts absolutely irreducibly on a finite dimensional K-vector space V. Let $(\ ,\ )$ be a non-degenerate pairing on V such that $(gu, gv) = \psi(g)(u, v)$ for some character $\psi : G \to K^\times$. Let $V' = V \otimes_K K(\lambda^{1/2})$. Then there is a G-invariant $\mathcal{O}'$-lattice $L' \subset V'$ which is self-dual for $(\ ,\ )$.*

Proof. First note that by Schur's lemma, the pairing is symmetric or alternating. Choose a G-invariant lattice L_1 in V which contains its dual lattice $L_1^\perp$. Then $(\ ,\ )$ induces a perfect pairing $L_1/L_1^\perp \times L_1/L_1^\perp \to K/\mathcal{O}$. Let X be a maximal isotropic G-submodule of $L_1/L_1^\perp$ and replace L_1 by L_2, the preimage of $X^\perp$. Using the

maximality of X, one sees that $L_2 \supset L_2^\perp \supset \lambda L_2$. It is then easy to check that $L' = L_2^\perp \oplus \lambda^{1/2} L_2$ will suffice.

■

4. Galois representations for modular forms.

4.1. ℓ-adic representations associated to modular forms. Now let us recall some facts about the ℓ-adic representations attached to certain automorphic representations of $\mathrm{GL}_2(\mathbf{A})$, where $\mathbf{A}$ denotes the adele ring of $\mathbf{Q}$. Recall that we have fixed embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and into $\overline{\mathbf{Q}}_p$ for all p. Suppose that $\pi \cong \otimes_v' \pi_v$ is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbf{A})$ such that π_∞ is a lowest discrete series representation of $\mathrm{GL}_2(\mathbf{C})$ with trivial central character. Recall that the set of such representations π is in one-to-one correspondence with the set of weight two newforms. The theory of Eichler and Shimura associates a continuous irreducible two-dimensional representation

$$\rho_\pi : G_{\mathbf{Q}} \to \mathrm{GL}(V_\pi)$$

over $\overline{\mathbf{Q}}_\ell$ to π which is characterized as follows: For any prime $p \neq \ell$ such that π_p is unramified, ρ_π is unramified at p and $\rho_\pi(\mathrm{Frob}_p)$ has characteristic polynomial

$$X^2 - t_p X + p s_p,$$

where t_p denotes the eigenvalue of the Hecke operator

$$T_p = \left[\mathrm{GL}_2(\mathbf{Z}_p) \quad \begin{matrix} p & 0 \\ 0 & 1 \end{matrix} \quad \mathrm{GL}_2(\mathbf{Z}_p)\right]$$

on $\pi_p^{\mathrm{GL}_2(\mathbf{Z}_p)}$, and s_p denotes that of

$$S_p = \left[\mathrm{GL}_2(\mathbf{Z}_p) \quad \begin{matrix} p & 0 \\ 0 & p \end{matrix} \quad \mathrm{GL}_2(\mathbf{Z}_p)\right].$$

Let $S(\pi)$ denote the set of primes p such that π_p is ramified, and let S be any finite set of primes. Then the set of t_p for $p \notin S \cup S(\pi)$ generate a number field over which π is defined, and ρ_π is defined over the closure of this field inside of $\overline{\mathbf{Q}}_\ell$ (some finite extension of $\mathbf{Q}_\ell$). If π and π' are such that the corresponding eigenvalues t_p and t_p' coincide for all $p \notin S \cup S(\pi) \cup S(\pi')$, then in fact $\pi = \pi'$. For any automorphism σ in G_ℓ, there is an automorphic representation denoted π^σ such that $\rho_\pi^\sigma \simeq \rho_{\pi^\sigma}$.

For any prime p, the local Langlands correspondence associates to π_p a certain continuous semi-simple two-dimensional representation $WD(\pi_p) : W_p \to \mathrm{GL}(D_{\pi_p})$ over $\overline{\mathbf{Q}}$ with discrete topology. Our convention here is that $WD(\pi_p)$ is the restriction to W_p of $\sigma(\pi_p) \otimes |\ |^{-1}$, where $\sigma(\pi_p)$ is as in [3] and we have identified $\mathbf{Q}_p^\times$ with W_p^{ab} by the Artin map (which, with our conventions, sends p to a preimage of $\mathrm{Frob}_p \in W_p/I_p$). Thus $\Pi \mapsto WD(\Pi)$ establishes a bijection between (a) isomorphism classes of irreducible admissible infinite-dimensional representations of $\mathrm{GL}_2(\mathbf{Q}_p)$ defined over $\overline{\mathbf{Q}}$, and (b) isomorphism classes of continuous semi-simple representations $W_p \to \mathrm{GL}_2(\overline{\mathbf{Q}})$. The bijection has the following properties:

- If χ is a continuous character $\mathbf{Q}_p^\times \to \overline{\mathbf{Q}}^\times$, then $WD(\Pi \otimes \chi \circ \det) \cong WD(\Pi) \otimes \chi$.
- The determinant of $WD(\Pi)$ is $\epsilon \chi_\Pi$, where χ_Π is the central character of Π.

A theorem of Carayol ([3, Thm. A], generalizing results of Langlands and Deligne) shows that

$$\overline{\mathbf{Q}}_\ell \otimes_{\overline{\mathbf{Q}}} WD(\pi_p) \cong (\rho_\pi|_{W_p})^{\mathrm{ss}}$$

for $p \neq \ell$. If π_ℓ is not special, then $\rho_\pi|_{G_\ell}$ is Barsotti-Tate over any finite extension F of $\mathbf{Q}_\ell$ such that $WD(\pi_\ell)|_{I_F}$ is trivial and

$$\overline{\mathbf{Q}}_\ell \otimes_{\overline{\mathbf{Q}}} WD(\pi_\ell) \cong WD(\rho_\pi|_{G_\ell}).$$

For a proof of this last isomorphism, see Appendix B (note also that the isomorphism of representations follows from the main theorem of [34]).

4.2. **The local Langlands correspondence.** We shall need to recall some properties of the correspondence $\Pi \leftrightarrow WD(\Pi)$. Before doing so, we define, for each $n \geq 0$, open subgroups

$$U_0(p^n) \supset U_\ell(p^n) \supset U_1(p^n) \supset U(p^n)$$

of $\mathrm{GL}_2(\mathbf{Z}_p)$ as follows. We set

- $U_0(p^n) = \varpi_n^{-1} \left\{ \begin{matrix} * & * \\ 0 & * \end{matrix} \right\}$;
- $U_\ell(p^n) = \varpi_n^{-1} \left\{ \begin{matrix} * & * \\ 0 & a \end{matrix} \mid a \in (\mathbf{Z}/p^n\mathbf{Z})^\times \text{ has } \ell\text{-power order} \right\}$;
- $U_1(p^n) = \varpi_n^{-1} \left\{ \begin{matrix} * & * \\ 0 & 1 \end{matrix} \right\}$;
- $U(p^n) = \ker \varpi_n$;

where ϖ_n denote the natural projection $\mathrm{GL}_2(\mathbf{Z}_p) \to \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. For $V = U_0(p^n)$, $U_\ell(p^n)$ or $U_1(p^n)$ with $n \geq 1$, we let U_p denote the Hecke operator $V \left(\begin{matrix} p & 0 \\ 0 & 1 \end{matrix} \right) V$ on Π^V. If V and V' are two such subgroups with $V' \subset V$, then the operators denoted U_p are compatible with the natural inclusion $\Pi^V \to \Pi^{V'}$.

Lemma 4.2.1. *There is an integer $c = c(\Pi) \geq 0$ such that*

$$\dim \Pi^{U_1(p^m)} = \max\{0, m - c + 1\}$$

for all $m \geq 0$.

(1) *If $c = 0$ and $n > 0$, then the characteristic polynomial of U_p on $\Pi^{U_0(p^n)} = \Pi^{U_1(p^n)}$ is $X^{n-1}(X^2 - t_pX + ps_p)$, where t_p (respectively, s_p) is the eigenvalue of T_p (respectively, S_p) on $\pi_p^{\mathrm{GL}_2(\mathbf{Z}_p)}$.*

(2) *If $c > 0$ and $n > 0$, then the characteristic polynomial of U_p on $\Pi^{U_1(p^{c+n})}$ is $X^n(X - u_p)$, where u_p is the eigenvalue of U_p on $\Pi^{U_1(p^c)}$.*

With the above notation, we have the following well-known properties of the correspondence $\Pi \leftrightarrow WD(\Pi)$.

Lemma 4.2.2. (1) *Suppose that $c = 0$. Then $WD(\Pi)$ is unramified and the characteristic polynomial of Frob_p on $WD(\Pi)$ is $X^2 - t_pX + ps_p$.*

(2) *Suppose that $c = 1$. Let χ denote the character of $\mathbf{Z}_p^\times$ defined by the action of $\mathbf{F}_p^\times \cong U_0(p)/U_1(p)$ on $\Pi^{U_1(p)}$. Then $WD(\Pi)|_{I_p} \cong 1 \oplus \chi \circ \eta_{p,1}$. If χ is trivial, then $WD(\Pi) \cong \xi \oplus \xi|\ |^{-1}$ where ξ is unramified and $\xi(\mathrm{Frob}_p) = u_p$. If χ is not trivial, then Frob_p acts via u_p on $WD(\Pi)^{I_p}$.*

(3) *Suppose that $c > 1$. Then c is the conductor of $WD(\Pi)$. Moreover $u_p \neq 0$ if and only if $WD(\Pi)^{I_p} \neq 0$, in which case* Frob_p *acts via u_p on $WD(\Pi)^{I_p}$.*

Note that the only case where $c(\Pi)$ is not the conductor of $WD(\Pi)$ is when $c(\Pi) = 1$ and the central character of Π is unramified. We refer to such Π as unramified special representations. We let $e(\Pi) = 1$ if $WD(\Pi)$ is unramified special, and $e(\Pi) = \dim WD(\Pi)^{I_p}$ otherwise. In general, if π is an automorphic representation as above and $p \neq \ell$, then $\dim \rho_\pi^{I_p} = e(\pi_p)$.

Corollary 4.2.3. *The characteristic polynomial of U_p on $\pi_p^{U_1(p^{c(\pi_p)+e(\pi_p)})}$ is of the form $xf(x)$ where $f(x)$ has degree $e(\pi)$ and roots which are ℓ-adic units.*

We also have the following relationship between $WD(\Pi)$ and the action of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{Z}_p)/U(p^n)$ on $\Pi^{U(p^n)}$.

Lemma 4.2.4. (1) *Suppose that $\chi : \mathbf{F}_p^\times \to \overline{\mathbf{Q}}^\times$. If $\langle \mathrm{sp}_\chi \oplus \chi \circ \det, \Pi^{U(p)} \rangle_{\mathrm{GL}_2(\mathbf{F}_p)} \neq 0$, then $WD(\Pi)|_{I_p} \cong \chi \circ \eta_{p,1} \oplus \chi \circ \eta_{p,1}$. Conversely if $WD(\Pi)|_{I_p} \cong \chi \circ \eta_{p,1} \oplus \chi \circ \eta_{p,1}$, then either $\Pi^{U(p)} \cong \mathrm{sp}_\chi \oplus \chi \circ \det$ and Π is the twist of an unramified representation, or $\Pi^{U(p)} \cong \mathrm{sp}_\chi$ and Π is special.*

(2) *Suppose that $\chi_1 \neq \chi_2 : \mathbf{F}_p^\times \to \overline{\mathbf{Q}}^\times$. If $\langle I(\chi_1, \chi_2), \Pi^{U(p)} \rangle_{\mathrm{GL}_2(\mathbf{F}_p)} \neq 0$, then $WD(\Pi)|_{I_p} \cong (\chi_1 \circ \eta_{p,1}) \oplus (\chi_2 \circ \eta_{p,1})$. Conversely if $WD(\Pi)|_{I_p} \cong (\chi_1 \circ \eta_{p,1}) \oplus (\chi_2 \circ \eta_{p,1})$, then $\Pi^{U(p)} \cong I(\chi_1, \chi_2)$.*

(3) *Suppose that $\chi : A^\times = W(\mathbf{F}_{p^2})^\times \to \overline{\mathbf{Q}}^\times$ is as in §3.2 with conductor $p^n A$. If $\langle \Theta(\chi), \Pi^{U(p^n)} \rangle_{\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})} \neq 0$, then $WD(\Pi)|_{I_p} \cong (\chi \circ \eta_{p,2}) \oplus (\chi \circ \mathrm{Frob}_p \circ \eta_{p,2})$. Conversely if $WD(\Pi)|_{I_p} \cong (\chi \circ \eta_{p,2}) \oplus (\chi \circ \mathrm{Frob}_p \circ \eta_{p,2})$, then $\Pi^{U(p^n)} \cong \Theta(\chi)$.*

These assertions follow from explicit descriptions of the local Langlands correspondence. The first two parts can already be deduced from the properties listed above, together with the classification of representations of $\mathrm{GL}_2(\mathbf{F}_p)$. For the third part, see [24, §3].

5. Hecke Algebras and Modules

5.1. **Definition of Hecke algebras.** We use the notation of §1.3. In particular,

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}(V)$$

is absolutely irreducible, τ is an ℓ-type strongly acceptable for $\overline{\rho}|_{G_\ell}$ and S is a finite set of primes not containing ℓ. We suppose from now on that $\overline{\rho}$ is *modular*, meaning there exist an automorphic representation as in §4 and a finite extension K' of K such that $\rho_\pi \cong \overline{\mathbf{Q}}_\ell \otimes_{\mathcal{O}'} \rho$ for some deformation ρ of $\overline{\rho}$ to $\mathcal{O}'$. We let $\mathcal{N}_S$ denote the set of π such that this holds for some ρ of type (S, τ). We shall write R_S for the universal deformation ring of type (S, τ), and ρ_S for the universal deformation.

Let $S(\overline{\rho})$ denote the set of primes p such that $p = \ell$ or $\overline{\rho}$ is ramified at p. Let $T(\overline{\rho})$ denote the set of primes p such that $p \equiv -1 \bmod \ell$, $\overline{\rho}|_{G_p}$ is irreducible and $\overline{\rho}|_{I_p}$ is reducible. We let $\tilde{\mathbf{T}}_S$ denote the polynomial algebra over $\mathcal{O}$ generated by the variables T_p and S_p for $p \notin S \cup S(\overline{\rho})$. We define the Hecke algebra $\mathbf{T}_S$ as the image of the $\mathcal{O}$-algebra homomorphism

$$\tilde{\mathbf{T}}_S \to \prod_{\pi \in \mathcal{N}_S} \overline{\mathbf{Q}}_\ell,$$

sending $T_p \mapsto t_p$ and $S_p \mapsto s_p$ in each component. We let I_S denote the kernel of $\tilde{\mathbf{T}}_S \to \mathbf{T}_S$. We also let $\tilde{\mathbf{T}}'_S$ denote the polynomial algebra over $\tilde{\mathbf{T}}_S$ generated by the variables U_p for $p \in S$, and let I'_S denote the ideal generated by I_S and the set of U_p for $p \in S$.

For each prime p we will define open subgroups $V_{S,p}$, normal in $U_{S,p} \subset \mathrm{GL}_2(\mathbf{Z}_p)$, an element $w_{S,p} \in \mathrm{GL}_2(\mathbf{Q}_p)$ and a finite-dimensional irreducible representation $\sigma_{S,p}$ of $U_{S,p}/V_{S,p}$ over $\overline{\mathbf{Q}}$. For $p \neq \ell$, let c_p denote the conductor of $\overline{\rho}|_{G_p}$ and $e_p = \dim_k \overline{\rho}^{I_p}$. If $p \in T(\overline{\rho})$, then c_p is even and we can choose a character $\chi_p : W(\mathbf{F}_{p^2})^\times \to \overline{\mathbf{Q}}^\times$ of order prime to ℓ whose reduction $\overline{\chi}_p$ satisfies

$$\overline{\rho}|_{I_p} \otimes_k \overline{\mathbf{F}}_\ell \cong \overline{\chi}_p \circ \eta_{p,2} \oplus \overline{\chi}_p \circ \mathrm{Frob}_p \circ \eta_{p,2}.$$

- If $p \notin S \cup T(\overline{\rho}) \cup \{\ell\}$ then $U_{S,p} = V_{S,p} = U_\ell(p^{c_p})$, $w_{S,p} = \begin{matrix} 0 & -1 \\ p^{c_p} & 0 \end{matrix}$ and $\sigma_{S,p} = 1$.
- If $p \in S - T(\overline{\rho})$ then $U_{S,p} = V_{S,p} = U_\ell(p^{c_p+e_p})$, $w_{S,p} = \begin{matrix} 0 & -1 \\ p^{c_p+e_p} & 0 \end{matrix}$ and $\sigma_{S,p} = 1$.
- If $p \in T(\overline{\rho}) - S$ then $U_{S,p} = \mathrm{GL}_2(\mathbf{Z}_p)$, $V_{S,p} = U(p^{c_p/2})$, $w_{S,p} = 1$ and $\sigma_{S,p} = \Theta(\chi_p)$.
- If $p \in T(\overline{\rho}) \cap S$ then $U_{S,p} = U_0(p)$, $V_{S,p} = U(p^{c_p/2})$, $w_{S,p} = 1$ and $\sigma_{S,p} = \Theta(\chi_p)|_{U_{S,p}/V_{S,p}}$.
- If $p = \ell$, then $U_{S,p} = GL_2(\mathbf{Z}_\ell)$, $V_{S,p} = U(\ell)$, $w_{S,p} = 1$ and $\sigma_{S,p}$ is

$$\begin{cases} \chi \circ \det, & \text{if } \tau \cong \chi \circ \omega_1 \oplus \chi \circ \omega_1 \text{ for some } \chi : \mathbf{F}_\ell^\times \to \overline{\mathbf{Q}}^\times; \\ I(\chi_1, \chi_2), & \text{if } \tau \cong \chi_1 \circ \omega_1 \oplus \chi_2 \circ \omega_1 \text{ with } \chi_1 \neq \chi_2 : \mathbf{F}_\ell^\times \to \overline{\mathbf{Q}}^\times; \\ \Theta(\chi), & \text{if } \tau \cong \chi \circ \omega_2 \oplus \chi^\ell \circ \omega_2 \text{ with } \chi \neq \chi^\ell : \mathbf{F}_{\ell^2}^\times \to \overline{\mathbf{Q}}^\times. \end{cases}$$

We will set $U_S = \prod_p U_{S,p}$, and $V_S = \prod_p V_{S,p}$, $w_S = \prod_p w_{S,p}$ and $\sigma_S = \otimes_p \sigma_{S,p}$. We have defined w_S for later use. The point of the definitions of U_S and σ_S is the following lemma.

Lemma 5.1.1. *Suppose that $\rho_\pi \cong \overline{\mathbf{Q}}_\ell \otimes_{\mathcal{O}'} \rho$ for some deformation ρ of $\overline{\rho}$ to the ring of integers $\mathcal{O}'$ of a finite extension K' of K. Then $\pi \in \mathcal{N}_S$ if and only if*

$$\mathrm{Hom}_{U_S}(\sigma_S, \pi^\infty) \neq (0).$$

In that case, the eigenvalues of U_p on $\mathrm{Hom}_{U_S}(\sigma_S, \pi^\infty)$ for each $p \in S$ are either 0 or ℓ-adic units, and the subspace on which $U_p = 0$ for all $p \in S$ is 1-dimensional.

Proof. This follows from the results recalled in the preceding section together with the analysis of possible lifts of $\overline{\rho}|_{G_p}$ for $p \neq \ell$ (see [4] and [15]). In particular that analysis shows that $c(\pi_p) + e(\pi_p) = c_p + e_p$. Moreover if $p \notin T(\overline{\rho})$, $c_p = c(\pi_p)$ and $\det \rho|_{I_p}$ has order prime to ℓ, then $\rho|_{I_p}$ satisfies the local condition at p in the definition of type (S, τ). On the other hand, if $p \in T(\overline{\rho})$, then $\pi_p^{U(p^{c_p/2})}$ as a module for $\mathrm{GL}_2(\mathbf{Z}_p)$ is isomorphic to $\Theta(\chi_p\psi_p)$ for some character ψ_p of ℓ-power order. Note that in that case $\Theta(\chi_p\psi_p)|_{U_0(p)} \cong \Theta(\chi_p)|_{U_0(p)}$.

■

Corollary 5.1.2. *The set $\mathcal{N}_S$ is finite, $\mathbf{T}_S$ is finitely generated as an $\mathcal{O}$-module and the natural map*

$$\mathbf{T}_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell \to \prod_{\pi \in \mathcal{N}_S} \overline{\mathbf{Q}}_\ell$$

is an isomorphism.

Proof. By the lemma, $\mathcal{N}_S$ is finite, from which it follows that $\mathbf{T}_S$ is finitely generated over $\mathcal{O}$. For $\pi \in \mathcal{N}_S$ and $p \notin S \cup S(\pi)$, let $t_p(\pi)$ denote the eigenvalue of T_p on $\pi_p^{\mathrm{GL}_2(\mathbf{Z}_p)}$. Choose any $\pi \in \mathcal{N}_S$. For each $\pi' \in \mathcal{N}_S$ distinct from π, choose a prime $p(\pi') \notin S \cup S(\pi) \cup S(\pi')$ with $t_{p(\pi')}(\pi) \neq t_{p(\pi')}(\pi')$. The element

$$\prod_{\pi' \neq \pi} (T_{p(\pi')} \otimes 1 - 1 \otimes t_{p(\pi')}(\pi')) \in \mathbf{T}_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell$$

maps to 0 in all components except for the πth one, where it has non-zero image. This proves surjectivity. It now suffices to show $\dim_K \mathbf{T}_S \otimes_{\mathcal{O}} K \leq |\mathcal{N}_S|$. Let $K_\pi \subseteq \overline{\mathbf{Q}}_\ell$ denote the subfield of finite degree over $\mathbf{Q}_\ell$ which is generated by the $t_p(\pi)$'s for $p \notin S \cup S(\pi)$. Under the natural action of $G_K \subseteq G_\ell$ on the coefficient field $\overline{\mathbf{Q}}_\ell$, $\mathcal{N}_S$ is stable. For $\sigma \in G_K$, $\rho_{\pi^\sigma} = \rho_\pi^\sigma \simeq \rho_\pi$ if and only if σ fixes K_π, so the orbit of π under the action of G_K has size equal to $[K_\pi : K]$. Thus, if we sum over a set X of representatives for the G_K-orbits in $\mathcal{N}_S$,

$$|\mathcal{N}_S| = \sum_{\pi \in X} [K_\pi : K].$$

But the image of $\mathbf{T}_S \otimes_{\mathcal{O}} K$ in the πth factor $\overline{\mathbf{Q}}_\ell$ is K_π, and using the G_K-action we see that any element of $\mathbf{T}_S \otimes_{\mathcal{O}} K$ is determined by its image in the K_π's for $\pi \in X$. Thus, $\dim_K \mathbf{T}_S \otimes_{\mathcal{O}} K \leq |\mathcal{N}_S|$.

■

5.2. **The universal modular deformation.** For each π in $\mathcal{N}_S$, the universal property of the deformation ring R_S provides an $\mathcal{O}$-algebra homomorphism $R_S \to \overline{\mathbf{Q}}_\ell$ so that ρ_π is the extension of scalars of the universal deformation. The map

$$R_S \to \prod_{\pi \in \mathcal{N}_S} \overline{\mathbf{Q}}_\ell$$

has image $\mathbf{T}_S$ since R_S is topologically generated by traces. We let ϕ_S denote the resulting surjective $\mathcal{O}$-algebra homomorphism

$$R_S \to \mathbf{T}_S.$$

Note that whenever $S \subset S'$, we have a natural commutative diagram of $\mathcal{O}$-algebra homomorphisms

$$\begin{array}{ccccc} \tilde{\mathbf{T}}_{S'} & \to & \mathbf{T}_{S'} & \leftarrow & R_{S'} \\ \downarrow & & \downarrow & & \downarrow \\ \tilde{\mathbf{T}}_S & \to & \mathbf{T}_S & \leftarrow & R_S, \end{array}$$

with all maps surjective except $\tilde{\mathbf{T}}_{S'} \to \tilde{\mathbf{T}}_S$ which is injective.

5.3. **Definition of Hecke modules.** It is convenient to fix an auxiliary prime $r \notin S(\overline{\rho})$ such that no lift of $\overline{\rho}$ can be ramified at r (see Lemma 2 of [15]). Thus we have $\mathcal{N}_S = \mathcal{N}_{S\cup\{r\}}$, so $\mathbf{T}_{S\cup\{r\}} \cong \mathbf{T}_S$. We also assume the field K is sufficiently large that it contains all quadratic extensions of some field K_0 such that

- $\overline{\rho}$ is defined over k_0;
- $\sigma_{\emptyset,p} \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_\ell$ is defined over K_0 for each $p \in T(\overline{\rho}) \cup \{\ell\}$.

For each $p \in T(\overline{\rho})\cup\{\ell\}$, we fix a lattice M_p as in Lemma 3.3.1 for $\sigma_{\emptyset,p}$ and a pairing $(\ ,\ )_p$ inducing an isomorphism

$$M_p \to \mathrm{Hom}_{\mathcal{O}}(M_p, \mathcal{O}(\chi_p))$$

of $\mathcal{O}U_{\emptyset,p}$-modules, where $\chi_p = \psi_p \circ \det$, ψ_p being the central character of $\sigma_{\emptyset,p}$. Letting M_S denote the model $\otimes_{p\notin S} M_p$ over $\mathcal{O}$ for σ_S, we have a pairing $(\ ,\ )_S$ on M_S which induces an isomorphism

$$M_S \to \mathrm{Hom}_{\mathcal{O}}(M_S, \mathcal{O}(\chi_S))$$

of $\mathcal{O}U_S$-modules, where $\chi_S = \psi_S \circ \det$, where $\psi_S = \otimes_{p\in S}\psi_p$.

If U is an open compact subgroup of $\mathrm{GL}_2(\mathbf{A}^\infty)$ then we will let Y_U denote the modular curve

$$\mathrm{GL}_2(\mathbf{Q})\backslash((\mathrm{GL}_2(\mathbf{A}^\infty)/U) \times (\mathbf{C}-\mathbf{R})) \cong \mathrm{GL}_2(\mathbf{Q})\backslash \mathrm{GL}_2(\mathbf{A})/UU_\infty,$$

where $U_\infty = O_2(\mathbf{R})\mathbf{R}^\times$. We let X_U denote its compactification obtained by adjoining cusps. Recall that X_U is not necessarily connected (its connected components are in bijection with $\hat{\mathbf{Z}}^\times/\det U$), and that X_U has a model over $\mathbf{Q}$. Our convention for the definition of this model is that $Y_U(\overline{\mathbf{Q}})$ is in canonical bijection with the set of equivalence classes of pairs (E,α), where E is an elliptic curve over $\overline{\mathbf{Q}}$ and $\alpha : \mathbf{A}\times\mathbf{A} \xrightarrow{\sim} (\mathrm{proj\,lim}_n E[n]) \otimes_{\hat{\mathbf{Z}}} \mathbf{A}$. We consider $(E_1,\alpha_1) \sim (E_2,\alpha_2)$ if there is an isogeny $\phi : E_1 \to E_2$ such that $\phi\circ\alpha_1 = \alpha_2 \circ u$ for some $u \in U$. The point $\mathrm{GL}_2(\mathbf{Q})\cdot(xU,\tau)$ corresponds to the elliptic curve $\mathbf{C}/\Lambda_\tau$ where $\Lambda_\tau = \mathbf{Z}\tau \oplus \mathbf{Z}$ and α is defined by composing x with the isomorphism obtained using $(\tau,1)$ as a basis over $\hat{\mathbf{Z}}$ for $\mathrm{proj\,lim}_n E[n]$.

We obtain an admissible $\mathrm{GL}_2(\mathbf{A}^\infty)$-module

$$\mathcal{H} = \operatorname*{inj\,lim}_U H^1(X_U, \overline{\mathbf{Q}})$$

where the limit is with respect to the natural maps on cohomology induced by $X_V \to X_U$ whenever $V \subset U$. Then $\mathcal{H}$ decomposes as $\oplus_\pi(B_\pi^+ \oplus B_\pi^-)$ where each $B_\pi^\pm$ is a model for π. We recover each $H^1(X_U,\overline{\mathbf{Q}})$ from $\mathcal{H}$ as the subspace $\mathcal{H}^U$ of U-invariants.

We let $X_S = X_{V_S}$ and consider $H^1(X_S,\mathcal{O})$. We have natural compatible actions on it of $\tilde{\mathbf{T}}'_S$, and $G_S = U_S/V_S$. If r is in S, then we define L_S to be the $\mathbf{T}_S$-module

$$\mathrm{Hom}_{\mathcal{O}[G_S]}(M_S, H^1(X_S,\mathcal{O}))[I'_S].$$

(If I is an ideal in a ring R and M is an R-module, we write $M[I]$ for the largest submodule of M whose annihilator contains I.) If r is not in S, then we set $L_S = L_{S\cup\{r\}}$.

Lemma 5.3.1. *The $(\mathbf{T}_S \otimes_{\mathcal{O}} K)$-module $L_S \otimes_{\mathcal{O}} K$ is free of rank two.*

Proof. We may assume r is in S and replace K by $\overline{\mathbf{Q}}_\ell$. Writing $H^1(X_S, \overline{\mathbf{Q}}_\ell)$ as $(\mathcal{H} \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_\ell)^{V_S}$ and decomposing $\mathcal{H}$, we obtain an isomorphism of $\mathbf{T}_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell$-modules

$$L_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell \cong \bigoplus (B'_\pi \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_\ell)[I_S]$$

where B'_π is the subspace of $\mathrm{Hom}_{U_S}(\sigma_S, B_\pi^+ \oplus B_\pi^-)$ killed by U_p for all p in S. By Lemma 5.1.1, this space is two-dimensional whenever π is in $\mathcal{N}_S$. The lemma follows, since for p not in $S \cup S(\overline{\rho})$, the operators T_p and S_p act on B'_π as t_p and s_p, respectively.

■

There is also a natural action of $G_{\mathbf{Q}}$ on L_S compatible with that of $\mathbf{T}_S$. This can be defined, for example, via the isomorphism of $\mathrm{Hom}_{\mathbf{Z}_\ell}(H^1(X_S, \mathbf{Z}_\ell), \mathbf{Z}_\ell)$ with the ℓ-adic Tate module of the Jacobian of X_S. Each $\pi \in \mathcal{N}_S$ gives rise to a homomorphism $\theta_{\pi,S} : \mathbf{T}_S \to \overline{\mathbf{Q}}_\ell$ sending $T_p \mapsto t_p$ and $S_p \mapsto s_p$. The resulting representation of $G_{\mathbf{Q}}$ on $L_S \otimes_{\mathbf{T}_S} \overline{\mathbf{Q}}_\ell(1)$ is isomorphic to ρ_π, and we therefore have the following lemma:

Lemma 5.3.2. *There is an isomorphism*

$$L_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell(1) \cong \bigoplus_{\pi \in \mathcal{N}_S} V_\pi$$

of representations of $G_{\mathbf{Q}}$ over $\mathbf{T}_S \otimes_{\mathcal{O}} \overline{\mathbf{Q}}_\ell \cong \bigoplus_{\pi \in \mathcal{N}_S} \overline{\mathbf{Q}}_\ell$.

5.4. **The main results.** Recall that we are assuming $\overline{\rho}$ is as in §1.3 and that it is modular. We defined $\mathcal{N}_S$ and $\mathbf{T}_S$ in §5.1, ϕ_S in §5.2 and L_S in §5.3. We have not yet shown that these objects are non-trivial. We shall deduce the following lemma from related results in the literature in section 6.

Proposition 5.4.1. *With the above notation and hypotheses, $\mathcal{N}_S \neq \emptyset$.*

Our main result is the following theorem; we give the proof in the rest of this section, subject to some propositions which are proved in §6.

Theorem 5.4.2. *With the above hypotheses and notation, the following hold:*

(1) *ϕ_S is an isomorphism;*
(2) *$\mathbf{T}_S$ is a complete intersection;*
(3) *L_S is free over $\mathbf{T}_S$.*

5.5. **Reduction to the case $S = \emptyset$.** Following Wiles [46], we shall deduce the result for arbitrary S from the result for $S = \emptyset$.

For each $p \notin S \cup \{\ell\}$, we define an element $\mu_p \in \mathbf{T}_S$ as follows:

- If $e_p = 2$, then $\mu_p = (p-1)(T_p^2 - S_p(1+p)^2)$.
- If $e_p = 1$ and $\det \overline{\rho}$ is unramified at p, then $\mu_p = p^2 - 1$.
- If $e_p = 1$ and $\det \overline{\rho}$ is ramified at p, then $\mu_p = p - 1$.
- If $e_p = 0$ and $p \in T(\overline{\rho})$ then $\mu_p = p + 1$.
- If $e_p = 0$ and $p \notin T(\overline{\rho})$ then $\mu_p = 1$.

If Σ is a finite set of primes disjoint from $S \cup \{\ell\}$, we let $\mu_\Sigma = \prod_{p \in \Sigma} \mu_p$.

The key proposition we prove in §6 for the induction step is the following:

Proposition 5.5.1. (1) *There exists a pairing $\langle\ ,\ \rangle_S$ on L_S which induces an isomorphism*

$$L_S \to \mathrm{Hom}_{\mathcal{O}}(L_S, \mathcal{O})$$

of $\mathbf{T}_S$-modules.

(2) *If $S \subset S'$ and $\ell \notin S'$, then there exists a $\mathbf{T}_{S'}$-module homomorphism*

$$i_S^{S'} : L_S \to L_{S'}$$

such that $i_{S,S'} \otimes_{\mathcal{O}} k$ is injective and

$$j_{S'}^S i_S^{S'} L_S = \mu_{S'-S} L_S$$

where $j_{S'}^S$ is the adjoint of of $i_S^{S'}$ with respect to the pairings $\langle\ ,\ \rangle_S$ and $\langle\ ,\ \rangle_{S'}$.

Fix for the moment an element π of $\mathcal{N}_\emptyset$. Note that if part 1 or 2 of Theorem 5.4.2 holds for some K such that $\mathbf{T}_S$ is defined, then it holds for all such K, and similarly for part 3 provided L_S is defined. We may therefore assume that K contains the eigenvalues t_p and s_p for all $p \notin S(\overline{\rho})$. Let $\mathfrak{p}_S$ denote the kernel of $\theta_{\pi,S}$ and J_S the annihilator of $\mathfrak{p}_S$ in $\mathbf{T}_S$. Define

$$C_{S,\theta} = L_S/(L_S[\mathfrak{p}_S] + L_S[J_S]).$$

This is isomorphic to the cokernel of the map

$$L[\mathfrak{p}_S] \to \mathrm{Hom}_{\mathcal{O}}(L[\mathfrak{p}_S], \mathcal{O})$$

defined by the restriction of $\langle\ ,\ \rangle_S$. Thus $C_{S,\theta}$ has finite length over $\mathcal{O}$, and by Proposition 5.5.1 we have

$$\mathrm{length}_{\mathcal{O}} C_{S\cup\{p\},\theta} = \mathrm{length}_{\mathcal{O}} C_{S,\theta} + 2 \cdot \mathrm{length}_{\mathcal{O}}(\mathcal{O}/\theta_{\pi,S}(\mu_p)).$$

Since $\theta_{\pi,S}(\mu_p)$ is a unit times the determinant of $\mathrm{Frob}_p - 1$ on $\mathrm{ad}^0 V_\pi(1)^{I_p}$, we can combine this with Theorem 2.4 of [13] and Corollary 1.4.3 to conclude that Theorem 5.4.2 for all S follows from the special case $S = \emptyset$.

5.6. **The case of $S = \emptyset$.** We now turn to the proof of Theorem 5.4.2 in the case $S = \emptyset$. We will use the improvement on the method of Taylor and Wiles ([45]) found by Diamond ([13]) and Fujiwara ([23]). We keep the above hypotheses and notation, but only consider finite sets S of primes with the following properties. If $p \in S$ then

- $p \notin S(\overline{\rho})$,
- $p \equiv 1 \bmod \ell$,
- $\overline{\rho}(\mathrm{Frob}_p)$ has distinct eigenvalues $\alpha_{1,p}$ and $\alpha_{2,p}$.

One checks as in Lemma 2.44 of [9], that for each $p \in S$, the restriction to G_p of the universal deformation ρ_S is equivalent to $\chi_{1,p}^S \oplus \chi_{2,p}^S$ for some characters

$$\chi_{i,p}^S : G_p \to R_S^\times,$$

where the reduction of $\chi_{i,p}^S$ mod the maximal ideal of R_S is unramified and sends Frob_p to $\alpha_{i,p}$ for $i = 1, 2$. The restrictions $\chi_{i,p}^S|_{I_p}$ are of the form $\xi_{i,p}^S \circ \omega_{p,1}$ where $\omega_{p,1}$ denotes the mod p cyclotomic character $I_p \to (\mathbf{Z}/p\mathbf{Z})^\times$. We let $\Delta_S = \prod_{p\in S} \Delta_p$ where Δ_p denotes the ℓ-Sylow subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$. We regard R_S as an $\mathcal{O}[\Delta_S]$-algebra by mapping

$$\xi_{1,p}^S : \Delta_p \to R_S^\times$$

for each $p \in S$. This makes L_S an $\mathcal{O}[\Delta_S]$-module. We let $\mathfrak{a}_S$ denote the augmentation ideal of $\mathcal{O}[\Delta_S]$. The last key result whose proof we postpone until §6 is the following proposition:

Proposition 5.6.1. *The $\mathcal{O}[\Delta_S]$-module L_S is free. The map $\pi_{\emptyset,S} : L_S \to L_\emptyset$ induces an isomorphism*

$$L_S/\mathfrak{a}_S L_S \xrightarrow{\sim} L_\emptyset.$$

We also need the following lemma, which is proved exactly as Theorem 2.49 of [9] using Lemma 1.4.1.

Lemma 5.6.2. *There exists an integer $r \geq 0$ such that for any integer $n > 0$, there exists a finite set of primes S_n disjoint from $S(\overline{\rho})$ such that*

(1) *if $p \in S_n$ then $p \equiv 1 \bmod \ell^n$;*
(2) *if $p \in S_n$ then $\overline{\rho}(\mathrm{Frob}_p)$ has distinct eigenvalues;*
(3) *$\#S_n = r$;*
(4) *R_{S_n} can be topologically generated by r elements as an $\mathcal{O}$-algebra.*

We can then apply Theorem 2.1 of [13] to complete the proof of Theorem 5.4.2 in the case $S = \emptyset$. (See the proof of Theorem 3.1 of [13].)

6. Cohomology of modular curves

In this section we will give the proofs of Propositions 5.4.1, 5.5.1 and 5.6.1. We maintain the notation of the preceding section. In particular, we consider a representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$ which is irreducible and modular. Recall that $\tilde{\mathbf{T}}_S$ is the polynomial algebra generated by the operators T_p and S_p for p not in $S \cup S(\overline{\rho})$. We define $\mathfrak{m}_S$ to be the kernel of the map $\tilde{\mathbf{T}}_S \to k$ defined by $T_p \mapsto \mathrm{tr}(\overline{\rho}(\mathrm{Frob}_p))$, $S_p \mapsto p^{-1}\det(\overline{\rho}(\mathrm{Frob}_p))$. We consider also the polynomial algebra $\tilde{\mathbf{T}}'_S$ over $\tilde{\mathbf{T}}_S$ generated by the operators U_p for $p \in S$, and the maximal ideal $\mathfrak{m}'_S$ generated by $\mathfrak{m}_S$ and the operators U_p for $p \in S$. Recall that since $\overline{\rho}$ is irreducible, the maximal ideals $\mathfrak{m}_S$ and $\mathfrak{m}'_S$ are not Eisenstein. (We say a maximal ideal $\mathfrak{m}$ of $\tilde{\mathbf{T}}_S$ or $\tilde{\mathbf{T}}'_S$ is Eisenstein if there exists an integer $N > 0$ such that $T_p - 2 \in \mathfrak{m}$ and $S_p - 1 \in \mathfrak{m}$ for all $p \in S \cup S(\overline{\rho})$ with $p \equiv 1 \bmod N$; see [14, Proposition 2], for example.)

For $n \geq 0$, we let L_n denote the $\mathrm{SL}_2(\mathbf{Z})$-module $\mathrm{Symm}^n \mathbf{Z}^2$. Recall that if $\Gamma_1(N) \subset \Gamma \subset \Gamma_0(N)$ for some $N \geq 1$ and $S \cup S(\overline{\rho})$ contains the set of prime divisors of N, then there is a natural action of $\tilde{\mathbf{T}}_S$ on $H^1(\Gamma, L_n \otimes M)$ for any $\mathcal{O}$-module M. (See for example, [43, Chapter 8].)

6.1. Preliminary Lemmas.

The following is a consequence of the results of Ribet and others (see [11, Corollary 1.2]).

Theorem 6.1.1. *Suppose that $0 \leq n \leq \ell - 1$ and $\overline{\rho}|_{I_\ell}$ is of the form*

- $\begin{pmatrix} \omega^{n+1} & * \\ 0 & 1 \end{pmatrix}$ *with $*$ peu ramifié if $n = 0$, or*
- $\begin{pmatrix} \omega_2^{n+1} & 0 \\ 0 & \omega_2^{(n+1)\ell} \end{pmatrix}$.

Let N be any integer divisible by the conductor of ρ, let Γ denote the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ such that $d \bmod N$ has ℓ-power order and let S be a set of primes such that $S \cup S(\overline{\rho})$ contains the set of prime divisors of N. Then $\mathfrak{m}_S$ contains the annihilator of $H^1(\Gamma, L_n \otimes K)$, hence is in the support of $H^1(\Gamma, L_n \otimes \mathcal{O})$ and $H^1(\Gamma, L_n \otimes k)$.

Suppose that V is an open compact subgroup of $\mathrm{GL}_2(\mathbf{A}^\infty)$. We assume that V is of the form $\prod_p V_p$ with $V_p \subset \mathrm{GL}_2(\mathbf{Z}_p)$ and that $V_r \subset U_1(r^2)$ for some fixed prime r as in §5.3. Suppose that Σ is a finite set of primes, and that for each p in Σ we are given a finitely generated $\mathcal{O}$-module M_p with a left action of V_p which is continuous for the discrete topology on V_p. We can then associate to the V-module $M = \otimes_p M_p$ a locally constant sheaf

$$\mathcal{F}_M = \mathrm{GL}_2(\mathbf{Q})\backslash(\mathrm{GL}_2(\mathbf{A}) \times M^{\mathrm{op}})/VU_\infty$$

on Y_V. If r is in S, then we let $Y_S = Y_{U_S}$ and $\mathcal{F}_S = \mathcal{F}_{\check{M}_S}$, where $\check{M}_S$ denotes the U_S-module $\mathrm{Hom}_{\mathcal{O}}(M_S, \mathcal{O})$. (See §5.1 and §5.3 for the definitions of U_S and M_S.) If r is not in S, then we let $Y_S = Y_{S\cup\{r\}}$ and $\mathcal{F}_S = \mathcal{F}_{S\cup\{r\}}$.

If for all $p \notin S \cup S(\overline{p})$ we have $V_p = \mathrm{GL}_2(\mathbf{Z}_p)$ and V_p acts trivially on M, then there is a natural action of $\tilde{\mathbf{T}}_S$ on the cohomology groups

$$H^1_c(Y_V, \mathcal{F}_M) \quad \text{and} \quad H^1(Y_V, \mathcal{F}_M).$$

Standard arguments yield the following useful technical result.

Lemma 6.1.2. *Suppose V, M and S are as above and let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $\tilde{\mathbf{T}}_S$ with finite residue field.*

(1) *The map $H^1_c(Y_V, \mathcal{F}_M)_{\mathfrak{m}} \to H^1(Y_V, \mathcal{F}_M)_{\mathfrak{m}}$ is an isomorphism.*

(2) *If M is free over $\mathcal{O}$, then the natural map*

$$H^1(Y_V, \mathcal{F}_M)_{\mathfrak{m}} \otimes_{\mathcal{O}} k \to H^1(Y_V, \mathcal{F}_{M\otimes_{\mathcal{O}} k})_{\mathfrak{m}}$$

is an isomorphism.

(3) *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of $\mathcal{O}[V]$-modules, then the sequence*

$$0 \to H^1(Y_V, \mathcal{F}_{M'})_{\mathfrak{m}} \to H^1(Y_V, \mathcal{F}_M)_{\mathfrak{m}} \to H^1(Y_V, \mathcal{F}_{M''})_{\mathfrak{m}} \to 0$$

is exact.

(4) *If $V' \subset V$ and satisfies the hypotheses above for S, then*

$$H^1(Y_V, \mathcal{F}_M)_{\mathfrak{m}} \to H^1(Y_{V'}, \mathcal{F}_M)^V_{\mathfrak{m}}$$

is an isomorphism.

(5) *If V acts trivially on M, then*

$$H^1(X_V, \mathcal{O})_{\mathfrak{m}} \otimes_{\mathcal{O}} M \to H^1(Y_V, \mathcal{F}_M)_{\mathfrak{m}}$$

is an isomorphism.

If in addition we have $U_1(p^n) \subset V_p \subset U_0(p^n)$ for some $n > 0$ and V_p acts trivially on M for all $p \in S$, then this action extends naturally to an action of $\tilde{\mathbf{T}}'_S$. Furthermore, the lemma holds for $\mathfrak{m} = \mathfrak{m}'_S$. In particular, $\tilde{\mathbf{T}}'_{S\cup\{r\}}$ acts on

$$H^1_c(Y_S, \mathcal{F}_S) \quad \text{and} \quad H^1(Y_S, \mathcal{F}_S)$$

and the lemma yields natural isomorphisms

$$H^1_c(Y_S, \mathcal{F}_S)_{\mathfrak{m}} \to H^1(Y_S, \mathcal{F}_S)_{\mathfrak{m}} \to \mathrm{Hom}_{G_S}(M_S, H^1(X_S, \mathcal{O}))_{\mathfrak{m}}$$

where $\mathfrak{m} = \mathfrak{m}'_{S\cup\{r\}}$. One can also check that the natural map

$$L_S = \mathrm{Hom}_{G_S}(M_S, H^1(X_S, \mathcal{O}))[I'_{S\cup\{r\}}] \to \mathrm{Hom}_{G_S}(M_S, H^1(X_S, \mathcal{O}))_{\mathfrak{m}}$$

is an isomorphism, so we conclude:

Lemma 6.1.3. *There are natural isomorphisms of $\tilde{\mathbf{T}}'_{S\cup\{r\}}$-modules*

$$H^1_c(Y_S,\mathcal{F}_S)_{\mathfrak{m}} \cong H^1(Y_S,\mathcal{F}_S)_{\mathfrak{m}} \cong L_S$$

identifying $\mathbf{T}_S = \mathbf{T}_{S\cup\{r\}}$ with the localization at $\mathfrak{m}$ of the image of $\tilde{\mathbf{T}}'_{S\cup\{r\}}$ in $\mathrm{End}_{\mathcal{O}} H^1(Y_S,\mathcal{F}_S)$ *(or* $\mathrm{End}_{\mathcal{O}} H^1_c(Y_S,\mathcal{F}_S)$ *).*

6.2. **Proof of Proposition 5.4.1.** Suppose for the moment that $0 \le n \le \ell-1$ and $\overline{\rho}|_{I_\ell}$ is of the form

- $\begin{pmatrix} \omega^{n+1} & * \\ 0 & 1 \end{pmatrix}$ with $*$ peu ramifié if $n=0$, or
- $\begin{pmatrix} \omega_2^{n+1} & 0 \\ 0 & \omega_2^{(n+1)\ell} \end{pmatrix}$.

Setting $S = T(\overline{\rho}) \cup \{r\}$, we find that the group $\Gamma = \mathrm{SL}_2(\mathbf{Z}) \cap U_S$ satisfies the hypotheses of Theorem 6.1.1. Furthermore

$$H^1(Y_S,\mathcal{F}_M) \cong H^1(\Gamma, L_n \otimes k)$$

as a $\tilde{\mathbf{T}}'_S$-module where M is the module for $U_{S,\ell} = \mathrm{GL}_2(\mathbf{Z}_\ell)$ defined by the action of $\mathrm{GL}_2(\mathbf{F}_\ell)$ on $\mathrm{Hom}(L_n,k)$. Therefore $\mathfrak{m}_S$ is in the support of $H^1(Y_S,\mathcal{F}_M)$. On examining the list of possible τ which can be considered strongly acceptable for $\overline{\rho}$ (see the definition after Conjecture 1.2.3), we see from Lemma 3.1.1 that M is a constituent of $\mathrm{Hom}_{\mathcal{O}}(M_S,k)$. It follows from Lemma 6.1.2 that $\mathfrak{m}_S$ is in the support of $H^1(Y_S,\mathcal{F}_S)$, so L_S is non-zero and $\mathcal{N}_S$ is non-empty. Moreover by twisting by a power of the Teichmüller character, we see that this holds without the assumption on $\overline{\rho}|_{I_\ell}$ imposed in Theorem 6.1.1.

Now choose an automorphic representation π in $\mathcal{N}_S$. Then for each $p \in T(\overline{\rho})$, $\rho_\pi|_{I_p}$ is necessarily of the form

$$\chi'_p \circ \eta_{p,2} \oplus \chi'_p \circ \mathrm{Frob}_p \circ \eta_{p,2}$$

for some character χ'_p of $W(\mathbf{F}_{p^2})$ such that $\overline{\chi}'_p = \overline{\chi}_p$. Suppose now that $\mathcal{O}$ is sufficiently large that each representation $\Theta(\chi'_p)$ has a model M'_p over $\mathcal{O}$, and set

$$M'_{\{r\}} = M_\ell \otimes_{\mathcal{O}} \bigotimes_{p\in T(\overline{\rho})} M'_p.$$

It follows from Lemma 6.1.2 and the last part of Lemma 4.2.4 that

$$\mathrm{Hom}_{\mathcal{O}[G_{\{r\}}]}(M'_{\{r\}}, H^1(X_{\{r\}},\mathcal{O}))_{\mathfrak{m}_S} \cong H^1(Y_\emptyset, \mathcal{F}_{M'_{\{r\}}})_{\mathfrak{m}_S} \neq 0.$$

Finally, since $M'_{\{r\}} \otimes_{\mathcal{O}} k \cong M_{\{r\}} \otimes k$ by Lemma 3.2.1, we conclude from Lemma 6.1.2 that $\mathfrak{m}_S$ is in the support of

$$H^1(Y_{\{r\}},\mathcal{F}_{\{r\}}) = H^1(Y_\emptyset,\mathcal{F}_\emptyset),$$

hence $\mathcal{N}_\emptyset$ is not empty.

6.3. **Proof of Proposition 5.5.1.** We first define the pairings $\langle\ ,\ \rangle_S$ on L_S inducing isomorphisms

$$L_S \to \mathrm{Hom}_{\mathcal{O}}(L_S,\mathcal{O})$$

of $\mathbf{T}_S$-modules. We may assume $r \in S$. We let W_S denote the involution of Y_S defined by $g \mapsto (\det g)^{-1} g w_S$, where w_S was defined in §5.1. There is a natural isomorphism of sheaves

$$W_S^* \mathcal{F}_S \to \mathcal{F}_S(\chi_S) = \mathcal{F}_S \otimes_{\mathcal{O}} \mathcal{F}_{\chi_S \circ \det},$$

where $\chi_S = \sigma_S|_{\mathbf{A}^\times \cap U_S}$. (Recall that $\mathcal{F}_S$ is associated to $\check{M}_S = \mathrm{Hom}_{\mathcal{O}}(M_S, \mathcal{O})$.) The U_S-equivariant perfect pairing chosen in §5.3 gives rise to one on $\check{M}_S$ which defines an isomorphism of sheaves $\mathcal{F}_S(\chi_S) \to \mathcal{F}_{M_S}$. We thus obtain an isomorphism

$$H^1_c(Y_S, \mathcal{F}_S) \xrightarrow{\sim} H^1_c(Y_S, W_S^* \mathcal{F}_S) \xrightarrow{\sim} H^1_c(Y_S, \mathcal{F}_{M_S}).$$

The cup product gives rise to a pairing

$$H^1_c(Y_S, \mathcal{F}_{M_S}) \times H^1(Y_S, \mathcal{F}_S) \to H^2_c(X_S, \mathcal{O}) \cong \mathcal{O},$$

which defines an isomorphism

$$H^1_c(Y_S, \mathcal{F}_{M_S}) \to \mathrm{Hom}_{\mathcal{O}}(H^1(Y_S, \mathcal{F}_S), \mathcal{O}).$$

We thus obtain an isomorphism

$$H^1_c(Y_S, \mathcal{F}_S) \to \mathrm{Hom}_{\mathcal{O}}(H^1(Y_S, \mathcal{F}_S), \mathcal{O}),$$

which one can check is $\tilde{\mathbf{T}}'_S$-linear. Localizing at $\mathfrak{m}$ and applying Lemma 6.1.3, we obtain the desired isomorphism

$$L_S \to \mathrm{Hom}_{\mathcal{O}}(L_S, \mathcal{O})$$

of $\tilde{\mathbf{T}}_S$-modules, arising from an alternating pairing $\langle\ ,\ \rangle_S$ on L_S.

Now we suppose p is a prime not in $S \cup \{\ell\}$ and we define a homomorphism

$$i_S^{S'} : L_S \to L_{S'}$$

of $\mathbf{T}_{S'}$-modules where $S' = S \cup \{p\}$. We use the identity map if $p = r$, and then we can can assume $r \in S$. We let $\beta_{p^n} = \begin{smallmatrix} p^{-n} & 0 \\ 0 & 1 \end{smallmatrix}_p$. Let $\tilde{\mathbf{T}}_S^{(p)}$ denote the polynomial algebra over $\mathcal{O}$ generated by the variables T_q and S_q for $q \notin S' \cup S(\overline{\rho})$ and U_q for $q \in S$. We regard $\tilde{\mathbf{T}}_S^{(p)}$ as a subalgebra of both $\tilde{\mathbf{T}}'_S$ and $\tilde{\mathbf{T}}'_{S'}$, and let $\mathfrak{m}_S^{(p)} = \mathfrak{m}'_S \cap \tilde{\mathbf{T}}_S^{(p)} = \mathfrak{m}'_{S'} \cap \tilde{\mathbf{T}}_S^{(p)}$.

If $0 \le n \le e_p$, then $g \mapsto g\beta_{p^n}$ defines a map $Y_{S'} \to Y_S$ and $\beta_{p^n}^* \mathcal{F}_S$ is canonically isomorphic to $\mathcal{F}_{S'}$. We also use β_{p^n} to denote the induced $\tilde{\mathbf{T}}_S^{(p)}$-linear map on cohomology

$$H^1(Y_S, \mathcal{F}_S) \to H^1(Y_{S'}, \mathcal{F}_{S'}).$$

Now consider the map

$$i_S^{S'} : H^1(Y_S, \mathcal{F}_S)_{\mathfrak{m}_S^{(p)}} \to H^1(Y_{S'}, \mathcal{F}_{S'})_{\mathfrak{m}_S^{(p)}}$$

defined by

- $x \mapsto p\beta_1 x - \beta_p T_p x + \beta_{p^2} S_p x$, if $e_p = 2$;
- $x \mapsto p\beta_1 x - \beta_p U_p x$, if $e_p = 1$;
- $x \mapsto \beta_1 x$, if $e_p = 0$.

Using Lemma 6.1.2 we can identify $H^1(Y_S, \mathcal{F}_S)_{\mathfrak{m}_S^{(p)}}$ with the $\mathbf{T}_{S'}$-module L_S. One then checks that the image of $i_S^{S'}$ is in $H^1(Y_{S'}, \mathcal{F}_{S'})_{\mathfrak{m}_S^{(p)}}[U_p]$, which can be identified with the $\mathbf{T}_{S'}$-module $L_{S'}$. We thus obtain the desired map $i_S^{S'} : L_S \to L_{S'}$.

These are compatible for varying p in the sense that $i_{S\cup\{p\}}^{S'} \circ i_S^{S\cup\{p\}} = i_{S\cup\{q\}}^{S'} \circ i_S^{S\cup\{q\}}$ if $S' = S \cup \{p, q\}$ for distinct primes $p, q \notin S \cup \{\ell\}$. We can therefore inductively define $i_S^{S'} : L_S \to L_{S'}$ if $S \subset S'$ and $\ell \notin S'$.

To complete the proof of the proposition, we can assume $S' = S \cup \{p\}$. First consider the calculation of $j^S_{S'} i^{S'}_S$. The assertion holds for $p = r$ since μ_r is a unit in $\mathbf{T}_S$. We can then assume $r \in S$.

In the case $e_p = 2$, one finds that the adjoint of β_{p^n} is the trace map

$$H^1_c(Y_{S'}, \mathcal{F}_{S'}) \to H^1_c(Y_S, \mathcal{F}_S)$$

with respect to $\beta_{p^{2-n}}$, which we denote $\beta^t_{p^{2-n}}$. After localizing at $\mathfrak{m}_S^{(p)}$, we can compute the composites $\beta^t_{p^m}\beta_{p^n}$ on $H^1(X_S, \mathcal{O})$, for example. Finally, we are reduced to the calculation of

$$d(p, -T_p, S_p) \begin{pmatrix} T_p^2 - (p+1)S_p & pT_p & p(p+1) \\ pT_p & p(p+1) & pS_p^{-1}T_p \\ p(p+1) & pS_p^{-1}T_p & S_p^{-2}(T_p^2 - (p+1)S_p) \end{pmatrix} \begin{pmatrix} p \\ -T_p \\ S_p \end{pmatrix}$$

where d is the prime-to-ℓ part of $\phi(p^2)$. The result is $-d\mu_p$.

The case of $e_p = 1$ is similar, except that one gets $-pU_p(p^2 - U_p^* U_p)$ where $U_p^* = V_{S,p} \begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}_p V_{S,p}$. One then uses that

$$U_p^* U_p = \begin{cases} 1, & \text{if } \pi_p \text{ is unramified special,} \\ p, & \text{if } \pi_p \text{ is principal series with } e_p = 1. \end{cases}$$

Note that this also shows that U_p is an automorphism of L_S.

In the case $e_p = 0$, one gets $j^S_{S'} i^{S'}_S = p + 1$ if $p \in T(\overline{\rho})$ and $j^S_{S'} i^{S'}_S = 1$ if $p \notin T(\overline{\rho})$.

We now turn to the proof that $L_S \otimes_{\mathcal{O}} k \to L_{S'} \otimes_{\mathcal{O}} k$ is injective. Again we may assume $r \in S$ and $S' = S \cup \{p\}$ for some $p \notin S \cup \{\ell\}$.

First we treat the case $e_p = 0$. There is nothing to prove if $p \notin T(\overline{\rho})$, and if p is in $T(\overline{\rho})$ then the assertion is immediate from Lemma 6.1.2.

The remaining cases of Proposition 5.5.1 follow from Lemma 6.1.2 and the lemma below, the first part of which is essentially due to Ihara [27] and the second to Wiles [46]. For the following lemma, we let $V_1(N) = \prod_q U_1(q^{v_q(N)})$, $V_0(N) = \prod_q U_0(q^{v_q(N)})$ and $V(N) = \prod_q U(q^{v_q(N)})$. We also let $V_{1,0}(N, N')$ denote $V_1(N) \cap V_0(N')$ and $V_1(N, N')$ denote $V_1(N) \cap V(N')$. We also use β_p to denote the map $H^1(X_V, \mathcal{F}_M) \to H^1(X_{V'}, \mathcal{F}_M)$ induced on cohomology (by the matrix β_p) whenever $\beta_p V' \beta_p^{-1} \subset V$ and V_p acts trivially on M.

Lemma 6.3.1. *Suppose that D and N are relatively prime positive integers with $N > 3$ and p not dividing $ND\ell$. Let $\mathfrak{m} = \mathfrak{m}_\Sigma$ where Σ is a finite set of primes containing those dividing $NDp\ell$. Suppose that M is a $k[\mathrm{GL}_2(\mathbf{Z}/D\mathbf{Z})]$-module, finite-dimensional over k.*

(1) *The map*

$$H^1(X_{V_1(N)}, \mathcal{F}_M)^2_{\mathfrak{m}} \xrightarrow{1 \oplus \beta_p} H^1(X_{V_1(Np)}, \mathcal{F}_M)_{\mathfrak{m}}$$

is injective.

(2) *If $s \geq 1$ then*

$$0 \to H^1(X_{V_1(Np^{s-1})}, \mathcal{F}_M)_{\mathfrak{m}} \xrightarrow{(-\beta_p, 1)} H^1(X_{V_1(Np^s)}, \mathcal{F}_M)^2_{\mathfrak{m}} \xrightarrow{1 \oplus \beta_p} H^1(X_{V_1(Np^{s+1})}, \mathcal{F}_M)_{\mathfrak{m}}$$

is exact.

Proof. We first explain the proof of the second part. Let $V = \beta_p^{-1} V_1(Np^s)\beta_p$ and $L = H^1(X_{V_1(N,p^s)}, \mathcal{F}_M)_{\mathfrak{m}}$. Then using Lemma 6.1.2, we see that we are required to check the exactness of

$$(0) \longrightarrow L^{V_1(Np^{s-1})} \longrightarrow L^V \oplus L^{V_1(Np^s)} \longrightarrow L^{V \cap V_1(Np^s)},$$

where the nontrivial maps are given by $x \mapsto (-x, x)$ and $(x, y) \mapsto x + y$. Thus it suffices to check that $V_1(Np^{s-1})$ is generated by $V_1(Np^s)$ and V, which is a straightforward calculation.

We now turn to the proof of the first part of the lemma. By Lemma 6.1.2, it suffices to show that if (x, y) is in the kernel of

$$H^1(X_{V_1(N)}, \mathcal{F}_M)^2 \stackrel{1 \oplus \beta_p}{\longrightarrow} H^1(X_{V_{1,0}(N,p)}, \mathcal{F}_M)$$

then x restricts to zero in $H^1(X_V, \mathcal{F}_M)$ for some open subgroup $V \subset V_1(N)$. However we can rewrite this map as

$$H^1(\Gamma_1(N), M)^2 \longrightarrow H^1(\Gamma_1(N) \cap \Gamma_0(p), M)$$

with the map induced by $1 \oplus \mu$ where $\mu = \begin{matrix} p & 0 \\ 0 & 1 \end{matrix} \in \mathrm{GL}_2(\mathbf{Z}[1/p])$. Thus it suffices to show that if (x, y) is in the kernel, then there is a congruence subgroup $\Gamma \subset \Gamma_1(N)$ with $\mathrm{Res}\, x = 0$ in $H^1(\Gamma, M)$. Let $\Delta \subset \mathrm{SL}_2(\mathbf{Z}[1/p])$ denote the subgroup of elements congruent to $\begin{matrix} 1 & * \\ 0 & 1 \end{matrix}$ modulo N. Then Δ is the amalgam of $\Gamma_1(N)$ and $\mu^{-1}\Gamma_1(N)\mu$ over $\Gamma_1(N) \cap \Gamma_0(p)$ (see Serre [39, II.1.4]). Thus we have an exact sequence

$$H^1(\Delta, M) \to H^1(\Gamma_1(N), M) \oplus H^1(\mu^{-1}\Gamma_1(N)\mu, M) \to H^1(\Gamma_1(N) \cap \Gamma_0(p), M).$$

(See [39, II.2.8].) Thus it suffices to show that if $x \in H^1(\Delta, \overline{\sigma})$ there is a congruence subgroup $\Delta' \subset \Delta$ with $0 = \mathrm{Res}\, x \in H^1(\Delta', M)$. We may choose a subgroup Δ' of finite index in Δ such that $\mathrm{Res}\, x = 0$, and since Δ has the congruence subgroup property [35], Δ' will be a congruence subgroup.

■

6.4. **Proof of Proposition 5.6.1.** For the rest of the section, S will denote a fixed set of primes as in §5.6. We let s denote the cardinality of S. Recall that r is a fixed prime such that no lift of $\overline{\rho}$ can be ramified at r. It is convenient to choose another such prime r' and a character $\psi : (\mathbf{Z}/r'\mathbf{Z})^\times \to \mathcal{O}^\times$ of order greater than 2. For each prime p, we define open subgroups $V_{1,p} \subset V_{0,p} \subset \mathrm{GL}_2(\mathbf{Z}_p)$ as follows:

- $V_{1,p} = V_{0,p} = U_{\{r\},p}$ if $p \notin S \cup \{r'\}$, where $U_{\{r,r'\},p}$ was defined in §5.1;
- $V_{1,p} = U_1(p)$ and $V_{0,p} = U_\ell(p)$ if $p \in S$;
- $V_{1,p} = V_{0,p} = U_0(r'^2)$ if $p = r'$.

We then set $V_1 = \prod_p V_{1,p}$ and $V_0 = \prod_p V_{0,p}$, so $V_1 \subset V_0 \subset U_{\{\emptyset\}}$. We identify $U_S'/U_{0,S}'$ with $\Delta_S = \prod_{p \in S} \Delta_p$, where Δ_p denotes the ℓ-Sylow subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$. Recall that we defined a representation $\sigma_\emptyset$ of $U_\emptyset$ in §5.1. Now we let $\sigma = \sigma_\emptyset \otimes \psi_{r'}^{-2}$ where $\psi_{r'}$ is the character of $U_0(r'^2) \to (\mathbf{Z}/r'\mathbf{Z})^\times$ gotten by composing with ψ. If χ is a Dirichlet character and π is an automorphic representation, we write simply $\pi \cdot \chi$ for $\pi \otimes (\chi_{\mathbf{A}} \circ \det)$ where $\chi_{\mathbf{A}}$ is the character of $\mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}^\times$ corresponding to χ.

The analogue of Lemma 5.1.1 for V_1 and V_0 is the following:

Lemma 6.4.1. *Suppose that $\rho_{\pi\cdot\psi} \cong \overline{\mathbf{Q}}_\ell \otimes_{\mathcal{O}'} \rho$ for some deformation ρ of $\overline{\rho}$ to the ring of integers $\mathcal{O}'$ of a finite extension K' of K.*

(1) *The space $\mathrm{Hom}_{V_0}(\sigma, \pi^\infty)$ is non-zero if and only if $\pi\cdot\psi \in \mathcal{N}_\emptyset$. In that case the dimension is $3\cdot 2^s$.*

(2) *The space $\mathrm{Hom}_{V_1}(\sigma, \pi^\infty)$ is non-zero if and only if the following hold:*
   - *$\pi\cdot\psi\chi$ is in $\mathcal{N}_S$ for some character χ unramified outside S;*
   - *$c(\pi_p) \le 1$ for all $p \in S$.*

   In that case the character χ is unique, and the space has dimension $3\cdot 2^{s-d}$ where d is the number of primes dividing the conductor of χ.

Proof. For part 1, we note that if $p \in S$, $c(\pi_p) \le 1$ and π_p has unramified central character, then $\rho_{\pi\cdot\psi^{-1}}$ is unramified at p (using the above description of the universal deformation, or the analysis of local lifts in [15]). So if $\mathrm{Hom}_{V_0}(\sigma, \pi^\infty)$ is not zero, then $c(\pi_p) = 0$ for each $p \in S$ and it follows that $\mathrm{Hom}_{U_{\{r,r'\}}}(\sigma_{\{r,r'\}}, (\pi\cdot\psi)^\infty)$ is not zero. Therefore $\pi\cdot\psi \in \mathcal{N}_{\{r,r'\}} = \mathcal{N}_\emptyset$. To compute the dimension if $\pi\cdot\psi \in \mathcal{N}_\emptyset$, one uses the lemmas in §4 to check that

$$\dim \mathrm{Hom}_{V_{0,p}}(\sigma_p, \pi_p) = \begin{cases} 3, & \text{if } p = r \\ 2, & \text{if } p \in S \\ 1, & \text{otherwise.} \end{cases}$$

For part 2, we note that if $p \in S$, then the central character χ_{π_p} of π_p has ℓ-power order. We may therefore choose a finite order character χ of $\mathbf{A}^\times$ so that $\chi_p^2 = \chi_{\pi_p}^{-1}$. If $\mathrm{Hom}_{V_1}(\sigma, \pi^\infty)$ is not zero, then neither is $\mathrm{Hom}_{U_{S\cup\{r,r'\}}}(\sigma_{S\cup\{r,r'\}}, (\pi\cdot\psi\chi)^\infty)$, so $\pi\cdot\psi\chi$ is in $\mathcal{N}_{S\cup\{r,r'\}} = \mathcal{N}_S$. The uniqueness of χ is clear and the dimension calculation is similar to the one above.

■

Choose a model M for σ over $\mathcal{O}$. For $i = 0, 1$, we let $L_i = H^1(Y_{V_i}, \mathcal{F}_{\check{M}})_{\mathfrak{m}}$ where $\check{M} = \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O})$ and $\mathfrak{m}$ is the kernel of the map

$$\begin{array}{rcl} \tilde{\mathbf{T}}_{S\cup\{r,r'\}} & \to & k \\ T_p & \mapsto & \psi(p)^{-1}\,\mathrm{tr}(\overline{\rho}(\mathrm{Frob}_p)) \\ S_p & \mapsto & \psi(p)^{-2}p^{-1}\det(\overline{\rho}(\mathrm{Frob}_p)). \end{array}$$

Lemma 6.1.2 lets us identify L_i with $\mathrm{Hom}_{\mathcal{O}[V_i]}(M, H^1(X_V, \mathcal{O}))_{\mathfrak{m}}$ for $V \subset V_1 \cap \ker\sigma$.

Lemma 6.4.2. *The $\mathcal{O}$-rank of L_0 is $3\cdot 2^s \#\mathcal{N}_\emptyset$. The $\mathcal{O}$-rank of L_1 is $3\cdot 2^s \#\mathcal{N}_S$.*

Proof. The first assertion follows from Lemma 6.4.1 and the argument of 5.3.1. Simliarly one finds

$$\mathrm{rank}_{\mathcal{O}} L_1 = \sum_{\pi' \in \mathcal{N}'_S} \dim(\mathrm{Hom}_{V_1}(\sigma, \pi'^\infty)),$$

where $\mathcal{N}'_S$ is the set of automorphic representations as in part 2 of Lemma 6.4.1. Note that if $\pi \in \mathcal{N}_S$, then for each p in S, $\rho_\pi|_{I_p}$ is equivalent to a representation of the form $\xi_p \oplus \xi_p^{-1}$ where ξ has ℓ-power order. It follows that there are 2^d twists of π in $\mathcal{N}'_S$, where d is the number of primes in S such that ξ_p is ramified.

■

There is also a natural action Δ_S on L_1 compatible with that of $\mathbf{T}_{S\cup\{r,r'\}}$; in fact, the action Δ_p factors through the homomorphism

$$\prod_{p\in S}(\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{T}^\times_{S\cup\{r,r'\}}$$

sending q^{-1} to the image of S_q for each prime $q\notin S$ such that $q\equiv 1 \bmod N(\overline{\rho})r^2\ell$. The key lemma for the proof of Proposition 5.6.1 is the following:

Lemma 6.4.3. *The $\mathcal{O}[\Delta_S]$-module L_1 is free of rank equal to the $\mathcal{O}$-rank of L_0.*

Proof. Since L_0 is isomorphic to $L_1^{\Delta_S}$, it suffices to prove L_1 is free over $\mathcal{O}[\Delta_S]$. Since L_1 is an $\mathcal{O}[\Delta_S]$-module summand of $H^1(Y_{V_1},\mathcal{F}_{\check{M}})$, it suffices to prove that $H^1(Y_{V_1},\mathcal{F}_{\check{M}})$ is free. Letting $\Gamma_i=\mathrm{GL}_2(\mathbf{Q})\cap V_i$, we have

$$H^1(Y_{V_1},\mathcal{F}_{\check{M}})\cong H^1(\Gamma_1,\check{M})$$

as a module for $\Delta_S\cong\Gamma_0/\Gamma_1$. Since Γ_1 and Γ_2 are fundamental groups of connected non-compact Riemann surfaces, they are free groups, so $H^i(\Gamma_1,A)=H^i(\Gamma_1,A)=0$ for $i>1$ and any Γ_0-module A. Note also that this holds for $i=0$ and $A=\check{M}\otimes_{\mathcal{O}}k$ since $\overline{\psi}^2$ is non-trivial. Therefore $H^1(\Gamma_1,\check{M})$ is torsion-free over $\mathcal{O}$, and it suffices to prove that $H^i(\Delta_S,H^1(\Gamma_1,\check{M}))=0$ for $i>0$ (see [2, VI.8.10], for example), and this is immediate from the Hochschild-Serre spectral sequence.

■

We now complete the proof of Proposition 5.6.1. First note that the image of $\mathfrak{a}_S$ in $R^{\emptyset,D}_{V,\mathcal{O}}$ is trivial, so we have a surjective map $\mathbf{T}_S/\mathfrak{a}_S\mathbf{T}_S\to\mathbf{T}_\emptyset$. By Corollary 5.1.2, this map is an isomorphism after tensoring over $\mathcal{O}$ with $\overline{\mathbf{Q}}_\ell$, hence after tensoring with K. It follows that the rank of $\mathbf{T}_S[\mathfrak{a}_S]$ is the same as that of $\mathbf{T}_\emptyset$. Setting $\mathfrak{b}_S=\mathrm{Ann}_{\mathcal{O}[\Delta_S]}\mathfrak{a}_S$, we also see that the rank of $\mathbf{T}_S[\mathfrak{b}_S]$ is the same as that of the kernel of $\mathbf{T}_S\to\mathbf{T}_\emptyset$. Since

$$i^S_\emptyset(L_\emptyset)\subset L_S[\mathfrak{a}_S]$$

and $i^S_\emptyset$ is injective with torsion-free cokernel (by Lemma 5.5.1), we conclude that equality holds. Similarly we find that $L_S[\mathfrak{b}_S]=\ker j^\emptyset_S$. Furthermore, using the surjectivity of $j^S_\emptyset$ and the formula for $j^\emptyset_S i^S_\emptyset$, we conclude that

$$L_S/(L_S[\mathfrak{b}_S]+L_S[\mathfrak{a}_S])\xrightarrow{\sim}L_\emptyset/\#\Delta_S(L_\emptyset).$$

The first assertion of Proposition 5.6.1 now follows from Theorem 3 of [13], and the second follows from surjectivity and comparison of ranks.

7. Applications

7.1. **Basic Results.** Combining Theorem 5.4.2 with [12, Thm 5.3], we obtain the following result.

Theorem 7.1.1. *Let K denote a finite extension of $\mathbf{Q}_\ell$ and k its residue field. Suppose that $\rho:G_{\mathbf{Q}}\to\mathrm{GL}_2(K)$ is a continuous odd representation ramified at only finitely many primes. Assume its reduction, $\overline{\rho}:G_{\mathbf{Q}}\to\mathrm{GL}_2(k)$ is irreducible and modular. Suppose also that $\ell\neq 2$, that $\overline{\rho}|_{\mathbf{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})}$ is absolutely irreducible, and that at least one of the following holds:*

- *the centralizer of $\overline{\rho}(G_\ell)$ consists only of scalars, ρ is potentially Barsotti-Tate and the type of $WD(\rho)$ is strongly acceptable for $\overline{\rho}|_{G_\ell}$,*

- *there are characters χ_1 and χ_2 of G_ℓ such that $\chi_1|_{I_\ell}$ and $\chi_2|_{I_\ell}$ have finite order, $\overline{\chi}_1\overline{\epsilon} \neq \overline{\chi}_2$ and*

$$\rho|_{G_\ell} \simeq \begin{matrix} \chi_1\epsilon & * \\ 0 & \chi_2 \end{matrix} .$$

Then ρ is modular.

Using the theorem, we will obtain the following strengthening of [12, Thm 5.4]:

Theorem 7.1.2. *Let $E_{/\mathbf{Q}}$ be an elliptic curve whose conductor is not divisible by 27. Then E is modular.*

Let us first recall some basic facts about an elliptic curve E over a finite extension F of $\mathbf{Q}_\ell$. If $j(E) \notin \mathcal{O}_F$, then E acquires multiplicative reduction over a quadratic extension of F. If $j(E) \in \mathcal{O}_F$, then E acquires good reduction over a finite Galois extension F'/F with ramification degree dividing 6 if $\ell \geq 5$, dividing 12 if $\ell = 3$, and dividing 24 if $\ell = 2$. In the case of potentially good reduction, the j-invariant of the reduction of the Néron model of E over $\mathcal{O}_{F'}$ is the reduction of $j(E)$. In particular, the notions of potentially good ordinary and potentially supersingular reduction are well-defined and can be detected from $j(E) \in F$.

Let $\rho_{E,\ell}$ denote the representation of G_F on the Tate module of E, and assume that E acquires good reduction over the finite extension F'/F. Then $\rho_{E,\ell} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ is potentially Barsotti-Tate; in fact, this representation becomes Barsotti-Tate over F' and the representations $WD(\rho_{E,\ell})$ and $\rho_{E,\ell'}|_{W_F}$ for $\ell' \neq \ell$ are defined over $\overline{\mathbf{Q}}$ (viewed as a subfield of $\overline{\mathbf{Q}}_\ell$, $\overline{\mathbf{Q}}_{\ell'}$) and are semisimple and isomorphic over this common subfield of definition (for a proof, see Proposition B.4.2).

We need the following lemma:

Lemma 7.1.3. *Let ℓ be a prime and E an elliptic curve over $\mathbf{Q}_\ell$. Let $\rho = \rho_{E,\ell} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.*

(1) *If E has potentially multiplicative reduction, then*

$$\rho \sim \begin{matrix} \epsilon\chi & * \\ 0 & \chi \end{matrix}$$

for some quadratic character χ.

(2) *If E has potentially good ordinary reduction, then*

$$\rho \simeq \begin{matrix} \epsilon\tilde{\omega}^j\chi & * \\ 0 & \tilde{\omega}^{-j}\chi^{-1} \end{matrix}$$

for some character χ such that $\chi|_{I_\ell}$ is trivial if $\ell \geq 3$, and quadratic if $\ell = 2$.

(3) *If E has potentially supersingular reduction, then ρ is irreducible.*

Proof. First, we consider the case in which E is potentially ordinary. Let F be a Galois extension of $\mathbf{Q}_\ell$ over which E acquires good ordinary reduction. The ℓ-power torsion geometric points of the closed fiber of the Néron model of $E_{/F}$ give rise to an unramified quotient of $\rho|_F$, so $\rho|_{I_F}$ is of the form

$$\begin{matrix} \epsilon & * \\ 0 & 1 \end{matrix} .$$

Let v generate the line on which I_F acts via ϵ. Since I_F is normal in G_ℓ, we see that I_F acts via ϵ on $\rho(g)v$ for any $g \in G_\ell$, so ρ is reducible. Moreover the representation has the form

$$\begin{matrix} \chi_1\epsilon & * \\ 0 & \chi_2 \end{matrix}$$

with $\chi_1|_{I_F} = \chi_2|_{I_F}$ trivial. Since $\chi_1|_{I_\ell}$ and $\chi_2|_{I_\ell}$ have order dividing the number of roots of unity in $\mathbf{Z}_\ell^\times$, they are of the required form.

The case of potentially multiplicative reduction is similar; split multiplicative reduction is attained over a quadratic extension and the Tate model yields an trivial quotient in the split case.

There remains the case in which E is potentially supersingular. We will prove that if E has potentially good reduction and ρ is reducible, then E is potentially ordinary. Let F be a finite extension of $\mathbf{Q}_\ell$ such that $E_{/F}$ has good reduction. Since ρ is reducible, we must have

$$\rho_{E,\ell}|_{G_F} \sim \begin{matrix} \chi_1 & * \\ 0 & \chi_2 \end{matrix} .$$

The representation $\rho_{E,\ell}$ arises from the Tate module of an ℓ-divisible group Γ over $\mathcal{O}_F$, so the same is true of χ_1 and χ_2 by [33, Prop 2.3.1]. Clearly, the ℓ-divisible group over $\mathcal{O}_F$ corresponding to each χ_i has dimension 0 or 1, so it follows from [33, Thm 4.2.1] that each $\chi_i|_{I_F}$ is either trivial or $\epsilon|_{I_F}$. Since $\chi_1\chi_2 = \epsilon$, it follows that one of the characters is unramified. By Tate's full faithfulness theorem [44, Thm 4], Γ has non-trivial connected and étale parts, so $E_{/F}$ has ordinary reduction.

■

7.2. **Modularity Results.** We now prove the following weaker version of Theorem 7.1.2:

Theorem 7.2.1. *Let $E_{/\mathbf{Q}}$ be an elliptic curve such that $\overline{\rho}_{E,3}|_{\mathbf{Q}(\sqrt{-3})}$ is absolutely irreducible. If the conductor of E is not divisible by 27, then E is modular.*

Proof. Recall that the modularity of $\overline{\rho} = \overline{\rho}_{E,3}$ follows from results of Langlands and Tunnell. If E has a quadratic twist with semistable reduction over $\mathbf{Q}_3$, then E is modular by Theorem 5.4 of [12], so suppose this is not the case. Since we assume the conductor of E is not divisible by 27 (so the 'wild' part of the conductor at 3 is trivial), Lemma 7.1.3 shows that E acquires good supersingular reduction over any extension L of $\mathbf{Q}_3$ with $e(L) = 4$, but not over any extension with $e(L) = 2$. It follows from § B.2 and Proposition B.4.2 that $\tau = WD(\rho)|_{I_3}$ has the form $\tilde{\omega}_2^2 \oplus \tilde{\omega}_2^6$, where $\rho = \rho_{E,3}$.

We now claim that the centralizer of $\overline{\rho}|_{G_3}$ consists only of scalars and that $WD(\rho)|_{I_3}$ is strongly acceptable for $\overline{\rho}$. Let F be a ramified quadratic extension of $\mathbf{Q}_3$ and consider the twist E' of $E_{/F}$ by any ramified quadratic character ψ of G_F. Considering $\rho_{E',\ell'}$ for any $\ell' \neq 3$, we see that E' has good reduction, which is supersingular since $j_{E'} = j_E$. Therefore $\overline{\rho}|_{G_F} \otimes \psi$ arises from a local-local finite flat group scheme over $\mathcal{O}_F$ and so satisfies the hypotheses in §2.3. The claim concerning the centralizer follows, and τ is acceptable by Theorem 2.3.2. To conclude strong acceptability, we need to know that if $\overline{\rho}|_{G_3} \simeq E[3](\overline{\mathbf{Q}}_3)$ is reducible, then the splitting field is peu ramifié. One can compute this splitting field to be $\mathbf{Q}_3(\sqrt{-3}, \Delta^{1/3})$, which is peu ramifié because $3|v_3(\Delta)$, or one can see the peu ramifié property by using [6, Thm 4.2.2].

■

We shall use Wiles' argument switching to $\ell = 5$, where we have:

Theorem 7.2.2. *Let $E_{/\mathbf{Q}}$ be an elliptic curve such that $\overline{\rho}_{E,5}|_{\mathbf{Q}(\sqrt{5})}$ is absolutely irreducible. If $\overline{\rho}_{E,5}$ is modular, then E is modular.*

Proof. Theorem 5.3 of [12] applies if E has a twist with semistable reduction or, in view of Lemma 7.1.3, potentially ordinary reduction at 5. We will show that Theorem 7.1.1 applies even if E has potentially supersingular reduction (but has no twist with good reduction). Making a quadratic twist if necessary, we can assume E acquires good reduction over a field F with $e(F) = 3$. Note then (by § B.2 and Proposition B.4.2) that $\tau = WD(\rho)$ must be of the form $\tilde{\omega}_2^8 \oplus \tilde{\omega}_2^{16}$, where $\rho = \rho_{E,5}$. Applying the results of §2.2, we conclude that the centralizer of $\overline{\rho}$ consists only of scalars and τ is acceptable for $\overline{\rho}$. Moreover, the list of possibilities in §2.2 shows that $\overline{\rho}|_{I_5}$ is isomorphic (over the algebraic closure of $\mathbf{F}_5$ in the first case below) to one of the following:

- $\omega_2^m \oplus \omega_2^{5m}$ for some $m \equiv 1 \bmod 8$;
- $\begin{pmatrix} \omega^{1-m} & * \\ 0 & \omega^m \end{pmatrix}$ for some $m \in \{2, 3\}$, with $*$ peu ramifié if $m = 2$.

Appealing to Theorem 5.3 of [5], we can rule out the possibility that (over the algebraic closure of $\mathbf{F}_5$) $\overline{\rho}|_{I_5} \cong \omega_2 \oplus \omega_2^5$, and conclude that τ is strongly acceptable for $\overline{\rho}$.

■

To remove the irreducibility hypothesis in Theorem 7.2.1, we need the following lemma. We are grateful to Elkies for providing part of the proof (for details of Elkies' calculation, see the appendix of [17]).

Lemma 7.2.3. *Suppose that $E_{/\mathbf{Q}}$ is an elliptic curve such that neither $\overline{\rho}_{E,5}|_{\mathbf{Q}(\sqrt{5})}$ nor $\overline{\rho}_{E,3}|_{\mathbf{Q}(\sqrt{-3})}$ is absolutely irreducible. Then $j_E \in \{0, (11/2)^3, 5(29)^3/2^5\}$, and E is modular.*

Proof. We divide the proof into four cases, according to whether the representations $\overline{\rho}_{E,3}$ and $\overline{\rho}_{E,5}$ are reducible.

Suppose first that both $\overline{\rho}_{E,3}$ and $\overline{\rho}_{E,5}$ are reducible. Then E gives rise to rational points on $X_0(15)$, and as noted in [46], such points are accounted for by elliptic curves with conductor 50 (and $j = 5(29)^3/2^5$), known to be modular.

Now suppose that one of the representations, say $\overline{\rho}_{E,p}$, is irreducible, but its restriction to G_F is *not* absolutely irreducible, where F is the appropriate quadratic extension of $\mathbf{Q}$. In the case of $p = 3$, we see (taking into account complex conjugation) that the projective image of $\overline{\rho}_{E,3}$ in $\mathrm{PGL}_2(\mathbf{F}_3) \cong S_4$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. It follows that the image of $\overline{\rho}_{E,3}$ has order 8 and that $\overline{\rho}_{E,3}|_K$ is in fact reducible for some quadratic extension K of $\mathbf{Q}$. In the case of $p = 5$, we see (again using complex conjugation) that $\overline{\rho}_{E,5}|_{\mathbf{Q}(\sqrt{5})}$ is reducible and the image of $\overline{\rho}_{E,5}$ has order 16.

Consider the case in which the other of the two representations $\overline{\rho}_{E,q}$ is reducible. The case of $p = 3$, $q = 5$ is discussed in the final remark of [46], and the details are given in [12, Lemma 5.5]. In that case one finds that E is isomorphic (over $\overline{\mathbf{Q}}$) to a modular elliptic curve of conductor 338, with $j = (11/2)^3$. We need to analyze the situation with the roles of 3 and 5 interchanged. For clarity, we repeat the argument of [12, Lemma 5.5] with two arbitrary distinct odd primes p and q, and then specialize to the cases $(p, q) = (3, 5), (5, 3)$.

Thus, our elliptic curve $E_{/\mathbf{Q}}$ satisfies the properties that there is subgroup of order q defined over $\mathbf{Q}$ and $E[p](\overline{\mathbf{Q}})$ contains two lines which are interchanged by the action of $G_{\mathbf{Q}}$. We will now exhibit all such $E_{/\mathbf{Q}}$ as $\mathbf{Q}$-rational points on a suitable curve and will thereby check directly that all such $E_{/\mathbf{Q}}$ are modular. Define the curve $Y_{/\mathbf{Q}}$ to be the quotient of the smooth connected affine curve $Y(pq)_{/\mathbf{Q}}$ (in the sense of [28, §3.1]) by the subgroup of elements

$$g = \begin{matrix} a & b \\ c & d \end{matrix} \in \mathrm{GL}_2(\mathbf{Z}/pq\mathbf{Z})$$

for which $c \equiv 0 \bmod p$, and $a \equiv d \equiv 0 \bmod q$ or $b \equiv c \equiv 0 \bmod q$. This is the coarse moduli scheme attached to the functor "isomorphism classes of elliptic curves E over S with a cyclic order q subgroup C and an unordered pair of cyclic order p subgroups $\{L_1, L_2\}$ such that the natural map of S-group schemes $L_1 \times_S L_2 \to E[p]$ is an isomorphism," for variable $\mathbf{Q}$-schemes S.

The complex manifold associated to the base change $Y_{/\mathbf{C}}$ is a smooth connected open Riemann surface which is naturally identified with the quotient of the upper half plane in $\mathbf{C}$ by the action of the group of elements $g \in \mathrm{SL}_2(\mathbf{Z})$ whose image in $\mathrm{GL}_2(\mathbf{Z}/pq\mathbf{Z})$ satisfies the above congruences. The elements of $Y(\mathbf{Q})$ correspond to $\mathbf{Q}$-isomorphism classes of triples $(E, C, \{L_1, L_2\})$ with $E_{/\mathbf{Q}}$ an elliptic curve, C a $G_{\mathbf{Q}}$-stable subgroup of $E[q](\overline{\mathbf{Q}})$ with order q, and $\{L_1, L_2\}$ a non-ordered set of distinct lines in $E[p](\overline{\mathbf{Q}})$ such that the set $\{L_1, L_2\}$ is stable under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on lines in $E[p](\overline{\mathbf{Q}})$.

In order to determine the $\mathbf{Q}$-rational points on Y, we first identify it with another curve. Let $Y_0(N)_{/\mathbf{Q}}$ denote the smooth geometrically connected curve which is the coarse moduli scheme for the functor "isomorphism classes of elliptic curves E over S with a cyclic subgroup C of order N" for variable $\mathbf{Q}$-schemes S. If $d|N$ and $(d, N/d) = 1$, then there is a natural involution $W_d : Y_0(N) \to Y_0(N)$ which on geometric points is given by sending (E, C) to $(E/C[d], (E[d] + C)/C[d])$. This is compatible with the involution $W_d : Y_0(d) \to Y_0(d)$ via the natural projection $Y_0(N) \to Y_0(d)$ (we should really write $W_{d,N}$ for accuracy). We also note that if $e|(N/d)$ and $(e, N/de) = 1$, then the operators W_d and W_e commute, with composite W_{de}.

There is a natural map $Y_0(p^2q) \to Y$ arising from the map

$$(E, C) \to (E/C[p], C[pq]/C[p], \{C[p^2]/C[p], E[p]/C[p]\})$$

on 'points'. This is visibly W_{p^2}-invariant, so we get a natural map of smooth geometrically connected curves $Y_0(p^2q)/W_{p^2} \to Y$. One can check that the map is an isomorphism by noting that the resulting map on complex points is a bijection.

We will study $\mathbf{Q}$-rational points on $Y_0(p^2q)/W_{p^2}$, and even its 'compactification' $X_0(p^2q)/W_{p^2}$, with W_{p^2} acting on the smooth connected proper curve $X_0(p^2q)_{/\mathbf{Q}}$ in the unique way extending the above action on $Y_0(p^2q)$. For $p = 3$, $q = 5$, one finds that $X_0(45)/W_9$ is an elliptic curve of conductor 15, and has at most four rational points, all accounted for by modular elliptic curves with $j = (11/2)^3$. For $p = 5$, $q = 3$, the resulting curve $X = X_0(75)/W_{25}$ is a curve of genus 3 whose rational points were determined by Elkies as follows. The quotient $E_0 = X/W_3$ has genus one and exactly one rational cusp. Elkies found an explicit Weierstrass equation for E_0 and concluded it is isomorphic to the elliptic curve of conductor 15 denoted 15-A3(B) $[1, 1, 1, -5, 2]$ in the tables of Cremona [7]. This curve has rank 0 and a torsion subgroup of order 8. One need only look in the fibers of $X \to E_0$ over

the 7 non-cuspidal points in $E_0(\mathbf{Q})$ in order to find the rational points on Y. By writing the function field $\mathbf{Q}(X)$ as $\mathbf{Q}(E_0)[T]/(T^2 - f)$ for an explicit $f \in \mathbf{Q}(E_0)$, Elkies computed that the value of f at 6 of the points in $E_0(\mathbf{Q})$ is a non-square in $\mathbf{Q}$, and also that there is a single point in the geometric fiber on X over the remaining point. From this it follows that there is a unique non-cuspidal point in $X(\mathbf{Q})$; since it is fixed by W_3, it must arise from an elliptic curve over $\mathbf{Q}$ with complex multiplication. One can also check that $j = 0$ for such a curve.

Finally we rule out the possibility that both $\overline{\rho}_{E,3}$ and $\overline{\rho}_{E,5}$ are irreducible. First suppose that E has potentially multiplicative or potentially good ordinary reduction at 5. In that case Lemma 7.1.3 shows that $\overline{\rho}_{E,5}|_{G_5}$ is reducible, so its semisimplification is isomorphic to $\omega\overline{\chi} \oplus \overline{\chi}^{-1}$ for some character $\overline{\chi}$. On the other hand, since $\overline{\rho}_{E,5}$ is induced from $G_{\mathbf{Q}(\sqrt{5})}$, the ratio of the above characters on G_5 must be the quadratic character trivial on $G_{\mathbf{Q}_5(\sqrt{5})}$. This gives $\omega\overline{\chi}^2 = \omega^2$, contradicting the fact that ω is not a square. We can therefore assume that E has potentially supersingular reduction at 5. If E has a quadratic twist with good supersingular reduction, then the order of $\overline{\rho}_{E,5}(I_5)$ is divisible by 24, contradicting that $\overline{\rho}_{E,5}(G_{\mathbf{Q}})$ has order 16. Otherwise, the order of $\overline{\rho}_{E,3}(I_5)$ (which a priori divides 6) is divisible by 3, contradicting that $\overline{\rho}_{E,3}(G_{\mathbf{Q}})$ has order 8.

■

We now complete the proof of Theorem 7.1.2. According to Theorem 7.2.1, we may suppose that $\overline{\rho}_{E,3}|_{\mathbf{Q}(\sqrt{-3})}$ is not absolutely irreducible. By Lemma 7.2.3, we may assume $\overline{\rho}_{E,5}|_{\mathbf{Q}(\sqrt{5})}$ is absolutely irreducible. Wiles' argument using the Hilbert Irreducibility Theorem shows that there is an elliptic curve E' over $\mathbf{Q}$ such that

- $\overline{\rho}_{E',5} \sim \overline{\rho}_{E,5}$;
- $\overline{\rho}_{E',3}|_{\mathbf{Q}(\sqrt{-3})}$ is absolutely irreducible.

Since $\overline{\rho}_{E',5} \sim \overline{\rho}_{E,5}$, the conductor of E' is not divisible by 27. Therefore E' is modular by Theorem 7.2.1, so $\overline{\rho}_{E,5} \sim \overline{\rho}_{E',5}$ is modular. Therefore E is modular by Theorem 7.2.2.

Finally, we record the following strengthening of Theorem 7.2.2, immediate from Theorem 7.1.2:

Theorem 7.2.4. *Let $E_{/\mathbf{Q}}$ be an elliptic curve. If $\overline{\rho}_{E,5}$ is modular or $\overline{\rho}_{E,5}|_{\mathbf{Q}(\sqrt{5})}$ is not absolutely irreducible, then E is modular.*

Appendix A. Deformation theory

We recall some general facts from the deformation theory of representations of profinite groups. The basic results are due to Mazur [30], with improvements by Ramakrishna [32], Faltings, deSmit and Lenstra [10].

Let G be a profinite group, and let $\mathcal{O}$ be a local Noetherian ring with residue field k. We give k the discrete topology. Suppose that V is a finite-dimensional discrete k-vector space with a continuous action of G. We assume that $\mathrm{End}_{k[G]} V = k$, and we consider deformations of the representation

$$G \longrightarrow \mathrm{End}_k V$$

to certain $\mathcal{O}$-algebras.

We let $\mathcal{C}_{\mathcal{O}}^*$ denote the category of local topological $\mathcal{O}$-algebras A such that the natural map

$$A \to \operatorname*{proj\,lim}_{\mathfrak{a} \in \mathcal{U}_A} A/\mathfrak{a}$$

is a topological isomorphism, where $\mathcal{U}_A$ is the set of open ideals $\mathfrak{a} \neq A$ such that $A/\mathfrak{a}$ is Artinian. The basic theory of such rings is developed in [26, Exp. VII$_B$] (where they are called pseudocompact). For example, $\mathcal{C}_{\mathcal{O}}^*$ is stable under formation of inverse limits and quotients by closed ideals. Also, if A is an object of $\mathcal{C}_{\mathcal{O}}^*$, then $\mathcal{U}_A$ above is simply the set of open ideals. We let $\mathfrak{m}_A$ denote the maximal ideal of A and k_A the residue field. Note that we do not assume that $k_A = k$. (In the applications, $\mathcal{O}$ will be a complete discrete valuation ring, and A will be a complete local Noetherian $\mathcal{O}$-algebra.)

Definition A *deformation* of V to A (an object of $\mathcal{C}_{\mathcal{O}}^*$) is an isomorphism class of $A[G]$-modules D such that D is free of finite rank over A, $k_A \otimes_A D$ is isomorphic to $k_A \otimes_k V$ as a $k_A[G]$-module, and $G \to \mathrm{End}_A(D)$ is continuous.

We let $F_V(A)$ denote the set of deformations of V to A. If $A \to B$ is a morphism in $\mathcal{C}_{\mathcal{O}}^*$, then extension of scalars defines a map $F_V(A) \to F_V(B)$, allowing us to regard F_V as a functor from $\mathcal{C}_{\mathcal{O}}^*$ to the category of sets. According to Theorem 7.1 of [10], F_V is representable on the full subcategory of $\mathcal{C}_{\mathcal{O}}^*$ whose objects have residue field k. The proof actually shows that F_V is representable on $\mathcal{C}_{\mathcal{O}}^*$ by an object $R_{V,\mathcal{O}}$ with residue field k. We call $R_{V,\mathcal{O}}$ *the universal* $\mathcal{O}$*-deformation ring of* V, and the canonical element of $F_V(R_{V,\mathcal{O}})$ is called *the universal* $\mathcal{O}$*-deformation of* V.

If $R_{V,\mathcal{O}}$ is Noetherian, then it represents F_V on the category $\mathcal{C}_{\mathcal{O}}$ of complete local Noetherian $\mathcal{O}$-algebras, because $\mathcal{C}_{\mathcal{O}}$ is a full subcategory of $\mathcal{C}_{\mathcal{O}}^*$ (as shown by the proof of Proposition 2.4 of [10]). This holds, for instance, if G is topologically finitely generated.

A.1. **Change of rings.** Suppose we are given another local Noetherian ring $\mathcal{O}'$ with maximal ideal $\mathfrak{m}'$ and residue field k', and a local map $\mathcal{O} \to \mathcal{O}'$. Let $V' = V \otimes_k k'$ and note that $\mathrm{End}_{k[G]} V = k$ if and only if $\mathrm{End}_{k'[G]} V' = k'$. For an object B in $\mathcal{C}_{\mathcal{O}'}^*$, we can identify $F_V(B)$ with $F_{V'}(B)$, so we have a canonical bijection

$$\mathrm{Hom}_{\mathcal{C}_{\mathcal{O}}^*}(R_{V,\mathcal{O}}, B) \to \mathrm{Hom}_{\mathcal{C}_{\mathcal{O}'}^*}(R_{V',\mathcal{O}'}, B).$$

For an object A of $\mathcal{C}_{\mathcal{O}}^*$ *with residue field* k, consider

$$\mathcal{O}' \widehat{\otimes}_{\mathcal{O}} A = \operatorname*{proj\,lim}_{n>0, \mathfrak{a} \in \mathcal{U}_A} (\mathcal{O}'/(\mathfrak{m}')^n) \otimes_{\mathcal{O}} (A/\mathfrak{a}).$$

Each ring $(\mathcal{O}'/(\mathfrak{m}')^n) \otimes_{\mathcal{O}} (A/\mathfrak{a})$ is a local Artinian ring with residue field k' because A has residue field k. Thus by Exp. VII$_B$, 0.2 of [26], $\mathcal{O}' \widehat{\otimes}_{\mathcal{O}} A$ is an object of $\mathcal{C}_{\mathcal{O}'}^*$. The natural map $A \to \mathcal{O}' \widehat{\otimes}_{\mathcal{O}} A$ is continuous, and for any object B of $\mathcal{C}_{\mathcal{O}}^*$, it induces a bijection

$$\mathrm{Hom}_{\mathcal{C}_{\mathcal{O}'}^*}(\mathcal{O}' \widehat{\otimes}_{\mathcal{O}} A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}_{\mathcal{O}}^*}(A, B).$$

It follows that $\mathcal{O}' \widehat{\otimes}_{\mathcal{O}} R_{V,\mathcal{O}}$ is the universal $\mathcal{O}'$-deformation ring of V'. Furthermore, the universal deformation is obtained by extending scalars from $R_{V,\mathcal{O}}$. Analogous statements are also true for the construction in the next section.

A.2. **Restricted deformations.** Suppose that for each A in $\mathcal{C}^*_{\mathcal{O}}$, we are given a subset $S_V(A)$ of $F_V(A)$. We then have the following necessary and sufficient condition for S_V to be a functor represented by $R_{V,\mathcal{O}}/I$ for some closed ideal I of $R_{V,\mathcal{O}}$: for all $A \in \mathcal{C}^*_{\mathcal{O}}$ and $D \in F_V(A)$, we have:

(1) $D \in S_V(A)$ if and only if $D/\mathfrak{a} \in S_V(A/\mathfrak{a})$ for all $\mathfrak{a} \in \mathcal{U}_A$;
(2) if $\mathfrak{a}, \mathfrak{b} \in \mathcal{U}_A$, $D/\mathfrak{a} \in S_V(A/\mathfrak{a})$ and $D/\mathfrak{b} \in S_V(A/\mathfrak{b})$, then

$$D/(\mathfrak{a} \cap \mathfrak{b}) \in S_V(A/(\mathfrak{a} \cap \mathfrak{b}));$$

(3) if $A \to A'$ is an inclusion of Artinian rings in $\mathcal{C}^*_{\mathcal{O}}$, then $D \in S_V(A)$ if and only if $D \otimes_A A' \in S_V(A')$.

The necessity of (1), (2) and (3) is easily verified. The sufficiency is proved exactly as in Proposition 6.1 of [10].

Suppose we are given a local Noetherian $\mathcal{O}$-algebra $\mathcal{O}'$ as in §A.1. Suppose that S_V is a restriction on deformations represented by $R_{\mathcal{O},V}/I$ for some closed ideal I, and that $S_{V'}(B) = S_V(B)$ for $B \in \mathcal{C}^*_{\mathcal{O}'}$. Then $S_{V'}$ is represented by $\mathcal{O}'\widehat{\otimes}_{\mathcal{O}} R_{\mathcal{O},V}/I$, which is naturally isomorphic to the quotient of $R_{\mathcal{O}',V'}$ by the closure of the ideal generated by the image of I.

Example A.2.1. This example is based on an observation of Ramakrishna [32]. Suppose that k has positive characteristic and P is a property of finite discrete G-modules which is preserved under taking submodules, quotients and finite products. Suppose there is a finite subfield k_0 of k such that $V = k \otimes_{k_0} V_0$ for some $k_0[G]$-module V_0. For $D \in F_V(A) = F_{V_0}(A)$, we let $A_{D,0}$ denote the the image of $R_{V_0,W(k_0)} \to A$. We let D_0 denote the corresponding element of $F_{V_0}(A_{D,0})$. (Given the quotient topology, $A_{D,0}$ is an object of $\mathcal{C}^*_{W(k_0)}$ with residue field k_0. Since the map $A_{D,0} \to A$ is continuous, both spaces are Hausdorff and $A_{D,0}$ is compact, the topology is the same as the subspace topology. This means that the set of $\mathfrak{a} \cap A_{D,0}$ for $\mathfrak{a} \in \mathcal{U}_A$ is a base of open ideals in $A_{D,0}$.)

Define $S^P_V(A)$ as the set of D such that $D_0/\mathfrak{a}$ has property P for all $\mathfrak{a}$ in $\mathcal{U}_{A_{D,0}}$. One checks that S^P_V is independent of the choice of k_0 and satisfies (1), (2) and (3). If A itself is finite, then $S^P_V(A)$ is simply the set of D having property P. Note also that given $\mathcal{O} \to \mathcal{O}'$ as in §A.1, we have $S^P_V(B) = S^P_{V'}(B)$ for B in $\mathcal{C}^*_{\mathcal{O}'}$.

Appendix B. Potentially Barsotti-Tate representations

B.1. **Definition of $WD(\rho)$.** Let K and E be finite extensions of $\mathbf{Q}_\ell$ inside of $\overline{\mathbf{Q}}_\ell$, and let $\rho : G_E \to \mathrm{GL}(M)$ be a continuous representation on a d-dimensional vector space M over K. We denote the valuation rings of K and E by $\mathcal{O}$ and $\mathcal{O}_E$ respectively. Under certain hypotheses on ρ, we will define a continuous representation of the Weil group

$$WD(\rho) : W_E \to \mathrm{GL}(D)$$

on a d-dimensional $\overline{\mathbf{Q}}_\ell$-vector space D and will investigate several properties. Also, in case ρ is potentially Barsotti-Tate, we will give a more explicit description of this construction. This explicit description will be used to prove several 'independence of ℓ' properties in the context of elliptic curves and Jacobians of modular curves. Throughout this appendix, the oddness of ℓ is never needed.

In [20], the notions of *semistable*, *crystalline*, *potentially semistable*, and *potentially crystalline* are defined for continuous representations of the Galois group of a

characteristic 0 local field with perfect residue field of characteristic ℓ (on a finite-dimensional $\mathbf{Q}_\ell$-vector space). There are a number of rings $(B_{\mathrm{st}}, B_{\mathrm{cris}}, \dots)$ that are used there as well. We use these concepts below, and refer to [20] and the references therein for complete proofs of the basic facts we need. Although our primary interest is in the case of potentially Barsotti-Tate representations, the greater generality of potentially semistable representations is convenient for making the initial definition of the WD functor and establishing some properties (e.g., behavior with respect to tensor product constructions, which can destroy the potentially Barsotti-Tate property).

Consider ρ as above. Assume ρ is potentially semistable [20, 5.6.1, 5.6.8], which is to say that for some finite extension F/E, $\rho|_{G_F}$ is semistable (this depends only on the underlying $\mathbf{Q}_\ell[G_E]$-module of ρ). For example, since Barsotti-Tate representations are crystalline [21, Thm 6.2], hence semistable, we can take any ρ which is potentially Barsotti-Tate. This includes any finite order representation. By the very definition of semistability, the $\mathbf{Q}_\ell$-vector space

$$D_{\mathrm{st},F}(M) = (B_{\mathrm{st}} \otimes_{\mathbf{Q}_\ell} M)^{G_F}$$

is a vector space over the maximal unramified subextension F_0 of F (via action on B_{st}) of dimension equal to the $\mathbf{Q}_\ell$-dimension of M. By functoriality, $D_{\mathrm{st},F}(M)$ is a module over $F_0 \otimes_{\mathbf{Q}_\ell} K$, and in fact is *free* of rank d. To see this, it suffices to check that after applying the faithfully flat extension of scalars $B_{\mathrm{st}} \otimes_{F_0}$ we get a free rank d module over $B_{\mathrm{st}} \otimes_{\mathbf{Q}_\ell} K$. But this follows from [20, 5.6.7(*iii*), 5.6.8(*ii*)] (and the semistability of ρ over F).

From the definitions, $D_{\mathrm{st},F}(M)$ is equipped with a bijective endomorphism ϕ which is semilinear with respect to the arithmetic Frobenius automorphism of F_0 and linear with respect to K. Also, if F/E is Galois then there is a canonical action of $\mathrm{Gal}(F/E)$ which is semilinear with respect to F_0 and linear with respect to K and which commutes with ϕ. There are additional structures (filtration on $F \otimes_{F_0} D_{\mathrm{st},F}(M)$ and a monodromy operator) which we ignore. If F'/F is a finite extension, then $\rho|_{G_{F'}}$ is semistable and there is a natural isomorphism

$$F'_0 \otimes_{F_0} D_{\mathrm{st},F}(M) \to D_{\mathrm{st},F'}(M)$$

of $F'_0 \otimes_{\mathbf{Q}_\ell} K$-modules which respects the action of $\mathrm{Gal}(F'/E)$ if F' and F are Galois over E.

Suppose F/E is Galois, so $D_{\mathrm{st},F}(M)$ is an $(F_0 \otimes_{\mathbf{Q}_\ell} K)[\mathrm{Gal}(F/E)]$-module with an automorphism ϕ which acts semilinearly with respect to the F_0-action and linearly with respect to the $K[\mathrm{Gal}(F/E)]$-action. We define an $F_0 \otimes_{\mathbf{Q}_\ell} K$-linear action of W_E as follows. For any $g \in W_E$, we let g act on $D_{\mathrm{st},F}(M)$ as the product of the commuting operators given by the action of the image of g in $\mathrm{Gal}(F/E)$ and ϕ^{-n}, where the image of g in $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ is the nth power of absolute Frobenius (*not* the nth power of the Frobenius relative to the residue field of E). Note that the action of $I_F \subseteq W_E$ is trivial, so W_E acts continuously on $D_{\mathrm{st},F}(M)$. Thus, $D_{\mathrm{st},F}(M)$ is a free module of rank d over $F_0 \otimes_{\mathbf{Q}_\ell} K$ equipped with a continuous *linear* action of W_E that commutes with ϕ. Define

$$WD_K(\rho) = D_{\mathrm{st},F}(M) \otimes_{F_0 \otimes_{\mathbf{Q}_\ell} K} \overline{\mathbf{Q}}_\ell.$$

Clearly $WD_K(\rho)$ is of dimension d over $\overline{\mathbf{Q}}_\ell$ and the action of K on ρ induces the action of $K \subseteq \overline{\mathbf{Q}}_\ell$ on $WD_K(\rho)$. When there is no risk of confusion, we write $WD(\rho)$ in place of $WD_K(\rho)$.

B.2. **Properties of $WD(\rho)$.** If E'/E is a finite extension, then $WD(\rho|_{G_{E'}}) \simeq WD(\rho)|_{W_{E'}}$ It follows trivially from the definitions (and properties of the functor $D_{\mathrm{st},F}$) that the representation $WD(\rho)$ admits as a field of definition any common finite extension of F_0 and K inside of $\overline{\mathbf{Q}}_\ell$ and that it is (up to isomorphism) independent of the choice of F. Moreover, if K'/K is a finite extension (so $\rho \otimes_K K'$ is potentially semistable if and only if ρ is), then for potentially semistable ρ we have a canonical isomorphism $WD_{K'}(\rho \otimes_K K') \simeq WD_K(\rho)$ as $\overline{\mathbf{Q}}_\ell[W_E]$-modules. Consider continuous representations of G_E on finite-dimensional $\overline{\mathbf{Q}}_\ell$-vector spaces (it is automatic that there is a field of definition of *finite* degree over $\overline{\mathbf{Q}}_\ell$). There is an obvious notion of *potential semistability* for these representations, and we have a well-defined functor WD on the category of such potentially semistable representations on $\overline{\mathbf{Q}}_\ell$-vector spaces.

By using [20, 1.5, 5.1.2], the functor WD_K on potentially semistable $K[G_E]$-modules is exact and is naturally of formation compatible with tensor products (and hence exterior products). The tensor product compatibility means that for ρ_1, ρ_2 two semistable representations of G_E on finite-dimensional K-vector spaces, there is a canonical map

$$WD(\rho_1) \otimes_{\overline{\mathbf{Q}}_\ell} WD(\rho_2) \to WD(\rho_1 \otimes_K \rho_2)$$

of $\overline{\mathbf{Q}}_\ell[W_E]$-modules which is an isomorphism. Strictly speaking, [20] only considers cases with $K = \mathbf{Q}_\ell$, but since the $\mathbf{Q}_\ell[G_E]$-module ρ_0 underlying ρ gives rise to a natural isomorphism

$$WD_{\mathbf{Q}_\ell}(\rho_0) \otimes_{K \otimes_{\mathbf{Q}_\ell} \overline{\mathbf{Q}}_\ell} \overline{\mathbf{Q}}_\ell \cong WD_K(\rho),$$

we readily get the tensor product compatibility for $WD = WD_K$. In the same manner, we get compatibility with the Hom functor (and WD is even a functor between tensor categories).

We mention two explicit examples. First, $WD(\epsilon)$ is a 1-dimensional unramified representation of W_E over $\overline{\mathbf{Q}}_\ell$, given by the character that sends arithmetic Frobenius to $|k_E|$, where k_E is the residue field of E. For a proof, one is reduced to the case $E = K = \mathbf{Q}_\ell$, where (by [20, 5.5.1, 5.6.3]) it comes down to the assertion that $D_{\mathrm{cris}}(\epsilon)$ is 1-dimensional over $\mathbf{Q}_\ell$ with ϕ acting as multiplication by $1/\ell$. But $B_{\mathrm{cris}}^{G_\ell} = \mathbf{Q}_\ell$ and there exists a non-zero $t \in B_{\mathrm{cris}}$ on which G_ℓ acts as the cyclotomic character and $\phi(t) = \ell t$, so $D_{\mathrm{cris}}(\epsilon) = \mathbf{Q}_\ell \cdot 1/t$ has ϕ acting as desired.

The second example is when ρ has finite order (e.g., a finite order character with values in $K^\times$). In this case, we claim that $WD(\rho) \simeq \rho|_{W_E} \otimes_K \overline{\mathbf{Q}}_\ell$. This is an immediate consequence of the definitions, as we now explain. Take F/E to be the splitting field of ρ, so $\rho|_{G_F}$ is trivial (and hence crystalline). Since $B_{\mathrm{cris}}^{G_F} = F_0$ (the maximal unramified subextension of F), on which the action of ϕ corresponds to the lifting of absolute Frobenius, we see that $D_{\mathrm{st},F}(\rho) = F_0 \otimes_{\mathbf{Q}_\ell} \rho$ with $g \in W_E$ acting as $1 \otimes \rho(g)$. Thus, $WD_K(\rho)$ is naturally isomorphic to $\rho|_{W_E} \otimes_K \overline{\mathbf{Q}}_\ell$.

B.3. **The Potentially Barsotti-Tate Case.** We give an alternate definition of WD in the potentially Barsotti-Tate case. This formulation, to be given in terms of Dieudonné modules, will be the means by which we establish the desired results for representations coming from elliptic curves and modular forms.

Let ρ as above be potentially Barsotti-Tate, fix a finite Galois extension F/E (with residue field k_F) over which ρ becomes Barsotti-Tate, and fix a stable $\mathcal{O}$-lattice L for ρ. This gives us an ℓ-divisible group $\Gamma_{/\mathcal{O}_F}$ and by [44, Thm 4] there is

a unique action of $\mathcal{O}$ on Γ compatible with the $\mathcal{O}$-action on the generic fiber. The generic fiber descent data for $\rho|_{G_F}$ down to ρ gives rise (via contravariance of Spec and Tate's full faithfulness theorem [44, Thm 4]) to a right action of $\mathrm{Gal}(F/E)$ on Γ over the right action on $\mathrm{Spec}(\mathcal{O}_F)$. This commutes with the $\mathcal{O}$-action on Γ. We get induced actions on the closed fiber $\Gamma_{/k_F}$.

Let ϕ_E denote the k_E-Frobenius endomorphism of the closed fiber, so this commutes with the other actions we just defined. Now suppose that g is in W_E, $g \mapsto \sigma \in \mathrm{Gal}(F/\mathbf{Q}_\ell)$ and $g \mapsto \mathrm{Frob}_E^n$ in W_E/I_E. Working in the category of ℓ-divisible groups 'up to isogeny', we can define the action of g on $\Gamma_{/k_F}$ to be $\sigma\phi_E^{-n}$, and thereby give $\Gamma_{/k_F}$ the structure of a 'right-module' over $K[W_E]$.

Let $D(\Gamma)$ denote the (contravariant) Dieudonné module of $\Gamma_{/k_F}$, as defined in [18, III, 1.2]. Since the Dieudonné functor is contravariant, it converts right actions into left actions. Thus, $D(\Gamma)$ is a free $W(k_F)$-module of rank $d \cdot [K : \mathbf{Q}_\ell]$ such that $D(\Gamma) \otimes_{\mathcal{O}} K$ is a left module over $K[W_E]$. Define $D'(\Gamma) = \mathrm{Hom}_{W(k_F)}(D(\Gamma), W(k_F))$, and define the Frob_ℓ-semilinear endomorphism ϕ' of $D'(\Gamma)[1/\ell]$ to be the 'semilinear transpose' of ϕ^{-1} (i.e., $\phi'(f) = \sigma \circ f \circ \phi^{-1}$, with σ the absolute Frobenius endomorphism of $W(k_F)$). Define a *left* semilinear action of $\mathrm{Gal}(F/E)$ on $D'(\Gamma)$ by $g(f) = \overline{g} \circ f \circ g^{-1}$, where $\overline{g}$ denotes the automorphism of $W(k_F)$ induced by g and where we have used the previously defined semilinear left action of $\mathrm{Gal}(F/E)$ on $D(\Gamma)$. This commutes with ϕ' on $D'(\Gamma)[1/\ell]$. We define a $W(k_F)$-*linear* action of W_E in the usual manner (using powers of ϕ' to 'cancel' the semilinearity of the action of $\mathrm{Gal}(F/E)$). Also, we let $\mathcal{O}$ act through its action on $D(\Gamma)$. We define

$$WD'(\rho) = D'(\Gamma) \otimes_{W(k_F) \otimes_{\mathbf{Z}_\ell} \mathcal{O}} \overline{\mathbf{Q}}_\ell$$

as a $\overline{\mathbf{Q}}_\ell[W_E]$-module.

This is our desired 'concrete' definition of $WD(\rho)$ in the potentially Barsotti-Tate case (as the following Proposition will justify). Note that the Dieudonné module of the dual ℓ-divisible group of Γ has underlying $W(k_F)$-module $D'(\Gamma)$ and Frobenius endomorphism $\ell\phi'$.

Due to the compatibility of the Dieudonné module functor with respect to base change (e.g., Frobenius automorphisms of the base field), we can recover the Frobenius morphism of $D(\Gamma)$ from the semilinear absolute Frobenius morphism of Γ and we can likewise define a *semilinear* left action of $\mathrm{Gal}(F/E)$ on $D(\Gamma)$ by using the 'generic fiber descent data'. Putting these together gives an alternate formulation of the *linear* W_E-action on D in terms of suitable composites of semilinear actions (of ϕ and $\mathrm{Gal}(F/E)$).

Proposition B.3.1. *For potentially Barsotti-Tate ρ as above, $WD'(\rho) \simeq WD(\rho)$ as $\overline{\mathbf{Q}}_\ell[W_E]$-modules.*

Proof. Let $\rho' = \mathrm{Hom}_{\mathbf{Q}_\ell}(\rho, \mathbf{Q}_\ell)$. Via ρ, this is a $K[G_E]$-module. In [21, 6.6], there is defined a natural isomorphism

$$\eta_\Gamma : D(\Gamma)[1/\ell] \to D_{\mathrm{cris}}(\rho'|_{G_F}) = D_{\mathrm{st},F}(\rho')$$

as 'filtered modules'. In particular, this map respects the $W(k_F) \otimes_{\mathbf{Z}_\ell} \mathcal{O}$-module structures, as well as the absolute Frobenius maps on each side. Because the functor $D_{\mathrm{st},F}$ commutes with formation of duals, we are reduced to checking that this identification η_Γ respects the left W_E-actions. Looking back at how the linear W_E-actions have been defined in terms of the absolute Frobenius maps and semilinear

Galois actions on each side, it remains to show that the semilinear left actions of $\mathrm{Gal}(F/E)$ on $D(\Gamma)$ and $D_{\mathrm{cris}}(\rho'|_{G_F})$ are compatible via η_Γ.

Choose any $g \in \mathrm{Gal}(F/E)$. We have an $\mathcal{O}_F$-linear isomorphism $\Gamma \simeq \Gamma_g$ to the base change by g, satisfying the usual cocycle condition as we vary g. The induced isomorphism on the closed fiber, when combined with the base change compatibility of the Dieudonné module functor, gives rise to the semilinear action of g on $D(\Gamma)$. Now using the functoriality of the map η_Γ with respect to a *variable* ℓ-divisible group over a *fixed* base $\mathcal{O}_F$, all we have to do is prove that this map is also functorial with respect to base change of a *fixed* ℓ-divisible group Γ.

More precisely, consider an extension of scalars by a local extension $\mathcal{O}_{F'}$ of $\mathcal{O}_F$ (e.g., an automorphism σ of $\mathcal{O}_F$) and choose an embedding of algebraic closures $\overline{F} \to \overline{F}'$ over $F \to F'$ (e.g., an element of G_E over $\sigma \in \mathrm{Gal}(F/E)$). This gives rise to a continuous group map $G_{F'} \to G_F$ and a natural map $B_{\mathrm{cris}}(F) \to B_{\mathrm{cris}}(F')$ [19, 4.2.5(*d*)]. There is a 'base change diagram' which we need to commute. Namely, if $\Gamma' = \Gamma \times_{\mathcal{O}_F} \mathcal{O}_{F'}$ (so $V_\ell(\Gamma) = V_\ell(\Gamma')$ compatibly with $G_{F'} \to G_F$), then we have natural maps $D(\Gamma) \to D(\Gamma')$ and

$$\mathrm{Hom}_{\mathbf{Q}_\ell[G_F]}(V_\ell(\Gamma), B_{\mathrm{cris}}(F)) \to \mathrm{Hom}_{\mathbf{Q}_\ell[G_{F'}]}(V_\ell(\Gamma'), B_{\mathrm{cris}}(F')).$$

We want these to be compatible with the maps η_Γ and $\eta_{\Gamma'}$.

In view of the definition of the η maps, this finally reduces to the claim that the isomorphism [21, 6.4] is of formation compatible with such a base change $\mathcal{O}_F \to \mathcal{O}_{F'}$. But this is a consequence of the definitions (cf. [18, III, 6.2] in the case of ℓ-divisible groups, and note that the 'base change' compatibility of this is a consequence of how the Dieudonné module functor is *defined*).

■

B.4. **Independence of λ.** Let A be an abelian variety over a field k. Suppose that (in contrast to previous notation) $K \subset \overline{\mathbf{Q}}$ is a number field with ring of integers $\mathcal{O}$ and we are given an embedding

$$K \to \mathrm{End}_k^0 A = \mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbf{Q}$$

(we use here endomorphisms in the 'invert isogenies' category). If λ' is a prime of $\mathcal{O}$ lying over a prime ℓ' in $\mathbf{Z}$ distinct from the characteristic of k, we let $\rho_{A,\lambda'}$ denote the representation of G_k over $K_{\lambda'}$ defined by the Galois action on the λ'-adic Tate module $V_{\lambda'}(A)$ of A, which is

$$(\varprojlim A(k_s)[\lambda'^n]) \otimes \mathbf{Q}$$

if the full integer ring acts on A and more generally is defined as the factor of the ℓ'-adic Tate module corresponding to the factor ring $K_{\lambda'}$ of the ring $K \otimes_{\mathbf{Q}} \mathbf{Q}_{\ell'}$ (which acts on the usual ℓ'-adic Tate module $V_{\ell'}(A)$). The dimension of $\rho_{A,\lambda'}$ over $K_{\lambda'}$ is independent of λ' (equivalently, $V_{\ell'}(A)$ is free as a $K \otimes_{\mathbf{Q}} \mathbf{Q}_{\ell'}$-module), and so this dimension is equal to $2 \dim A/[K : \mathbf{Q}]$. Moreover, for any $f \in \mathrm{End}_k^0(A)$ which commutes with the action of K, the $K_{\lambda'}$-linear action of f on $V_{\lambda'}(A)$ has characteristic polynomial in $K[T]$ which is independent of the choice of prime λ' of $\mathcal{O}$. For proofs of these facts, see [42, Prop 11.9]. The proof of [31, §19, Thm 4] for Tate modules (and characteristic polynomials over $\mathbf{Q}_{\ell'}$) carries over verbatim to the case of Dieudonné modules when k is perfect of positive characteristic (with characteristic polynomials computed over the fraction field of $W(k)$).

Thus, in case k has positive characteristic ℓ and is perfect, the same arguments (with some minor modifications, due to the replacement of $\mathbf{Q}_{\ell'}$ by the fraction field

of $W(k)$ with k not necessarily equal to $\mathbf{F}_\ell$) carry over to give analogous results for the 'up to isogeny' Dieudonné module $D(A) = D(A[\ell^\infty])[1/\ell]$. More precisely, if F_0 denotes the fraction field of $W(k)$, then $D(A)$ is a free module over $K \otimes_{\mathbf{Q}} F_0$ and for any $f \in \mathrm{End}_k^0(A)$ which commutes with the action of K, the $K \otimes_{\mathbf{Q}} F_0$-linear endomorphism of $D(A)$ induced by f has characteristic polynomial in $K[T]$. Also, this polynomial is equal to the characteristic polynomial computed above on the ℓ'-adic Tate modules of A for $\ell' \neq \ell$. Of course, the same conclusions apply to the 'dual' Dieudonné module, since dualizing a linear map does not affect its characteristic polynomial.

Now suppose that $k = E$ is a finite extension of $\mathbf{Q}_\ell$ and that A has potentially good reduction. Let F be a finite Galois extension of E over which A has good reduction, and let $\mathcal{A}$ denote the Néron model of A over $\mathcal{O}_F$. We obtain commuting actions (in the 'invert isogenies' category) of K and $\mathrm{Gal}(F/E)$ exactly as in the case of ℓ-divisible groups (using the Néron mapping property instead of Tate's theorem), with $\mathrm{Gal}(F/E)$ acting on the right. Now change this Galois action, by letting $g \in \mathrm{Gal}(F/E)$ instead act as g^{-1} under the right action. This gives a left action of $K[\mathrm{Gal}(F/E)]$ on $\mathcal{A}_{/k_F}$ over the natural action of $\mathrm{Gal}(F/E)$ on k_F, composed with inversion in the Galois group. Again using powers of the absolute Frobenius morphism to 'cancel' out the semilinearity, we obtain a map of $\mathbf{Q}$-algebras

$$\theta : K[W_E] \to \mathrm{End}_{k_F}^0 \mathcal{A}_{/k_F} = (\mathrm{End}_{k_F} \mathcal{A}_{/k_F}) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

Note that $\theta|_{W_F}$ is unramified and sends Frob_F to the k_F-Frobenius endomorphism of $\mathcal{A}_{/k_F}$.

For $\ell' \neq \ell$, $V_{\ell'}(\mathcal{A}_{/k_F})$ is a module over $(K \otimes_{\mathbf{Q}} \mathbf{Q}_{\ell'})[W_E]$ using θ. Also, we use θ to make $D'(\mathcal{A}_{/k_F}[\ell^\infty])[1/\ell]$ a module over $(W(k_F) \otimes_{\mathbf{Z}_\ell} K)[W_E]$. We recall the following well-known result. Since we do not know a reference, we give a proof.

Lemma B.4.1. *For $\ell' \neq \ell$, there is an isomorphism of $(K \otimes_{\mathbf{Q}} \mathbf{Q}_{\ell'})[W_E]$-modules $V_{\ell'}(A) \cong V_{\ell'}(\mathcal{A}_{/k_F})$. Likewise, there is an isomorphism of $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_\ell)[W_E]$-modules $WD_{\mathbf{Q}_\ell}(V_\ell(A)) \cong D'(\mathcal{A}_{/k_F}[\ell^\infty])[1/\ell] \otimes_{W(k_F)} \overline{\mathbf{Q}}_\ell$.*

Proof. The ℓ-adic case is exactly our 'concrete' formulation of the definition of WD in the potentially Barsotti-Tate case (as a little checking will show). Now consider $\ell' \neq \ell$. There is an obvious isomorphism of the underlying groups of ℓ'-power torsion geometric points on A and $\mathcal{A}_{/k_F}$. Consider more specifically the 'reduction' morphism

$$r : A(\overline{\mathbf{Q}}_\ell) = \mathcal{A}(\overline{\mathbf{Z}}_\ell) \to \mathcal{A}(\overline{\mathbf{F}}_\ell)$$

(an isomorphism on ℓ'-power torsion). From the generic fiber descent data for $A_{/F}$ down to $A_{/E}$, we get (via the Néron property) a semilinear right action of $g \in \mathrm{Gal}(F/E)$ on $\mathcal{A}_{/\mathcal{O}_F}$, denoted by $[g]$. We also have the canonical absolute Frobenius morphism ϕ on $\mathcal{A} \times_{\mathcal{O}_F} k_F$.

For any $g \in W_E$ and any point $y \in \mathcal{A}(\overline{\mathbf{F}}_\ell)$, $[g^{-1}] \circ \phi^m \circ y$ is another such point, where g induces the mth power of absolute Frobenius on $\overline{\mathbf{F}}_\ell$. What we need to check is that for such g and m,

$$[g^{-1}] \circ \phi^m \circ r(x) = r(x \circ g)$$

for all $x \in A(\overline{\mathbf{Q}}_\ell)$. The point is that under the identification

$$A(\overline{\mathbf{Q}}_\ell) = \mathrm{Hom}_{\mathrm{Spec}(E)}(\mathrm{Spec}(\overline{\mathbf{Q}}_\ell), A) = \mathrm{Hom}_{\mathrm{Spec}(\mathcal{O}_F)}(\mathrm{Spec}(\overline{\mathbf{Z}}_\ell), \mathcal{A}) = \mathcal{A}(\overline{\mathbf{Z}}_\ell),$$

the translation of the usual action of G_E on $A(\overline{\mathbf{Q}}_\ell)$ into an action on $\mathcal{A}(\overline{\mathbf{Z}}_\ell)$ requires use of the generic fiber descent data isomorphisms (extended to $\mathcal{A}$ via the Néron property). It is easy to check that for $y \in \mathcal{A}(\overline{\mathbf{Z}}_\ell)$ and $g \in G_E$, $[g^{-1}] \circ y \circ g \in \mathcal{A}(\overline{\mathbf{Z}}_\ell)$ is the image of y under the action of G_E on $A(\overline{\mathbf{Q}}_\ell)$.

For any such y, with $g \in W_E$ inducing the mth power of absolute Frobenius on $\overline{\mathbf{F}}_\ell$, we need to show that

$$[g^{-1}] \circ \phi^m \circ r(y) = r([g^{-1}] \circ y \circ g),$$

where we regard r as a function on $\mathcal{A}(\overline{\mathbf{Z}}_\ell)$. This clearly reduces us to showing that for any map of $\mathcal{O}_F$-schemes $y : \mathrm{Spec}(\overline{\mathbf{Z}}_\ell) \to \mathcal{A}$ with reduction $\overline{y} : \mathrm{Spec}(\overline{\mathbf{F}}_\ell) \to \mathcal{A}_{/k_F}$ over k_F, and any $\mathcal{O}_E$-automorphism g of $\overline{\mathbf{Z}}_\ell$ inducing the mth power of absolute Frobenius on $\overline{\mathbf{F}}_\ell$, $\phi^m \circ \overline{y}$ is equal to the reduction of the semilinear map $y \circ g$. But the reduction of $y \circ g$ is $\overline{y} \circ \mathrm{Frob}_\ell^m$, so by the 'universal commutativity' of absolute Frobenius on $\mathbf{F}_\ell$-schemes, we're done.

■

Proposition B.4.2. *Let $A_{/E}$ be an abelian variety with potentially good reduction, $K \subseteq \overline{\mathbf{Q}}$ of finite degree over $\mathbf{Q}$, and $\theta : K \to \mathrm{End}_E^0(A)$ a $\mathbf{Q}$-algebra map. For $\ell' \neq \ell$, the representations $WD_{\mathbf{Q}_\ell}(\rho_{A,\ell})$ and $\rho_{A,\ell'}|_{W_E} \otimes_K \overline{\mathbf{Q}}_{\ell'}$ are semisimple and arise as the base changes of a common semisimple $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})[W_E]$-module (necessarily finite and free over $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}$). Also, for any λ in K dividing ℓ, $\rho_{A,\lambda}$ is Barsotti-Tate over any finite extension F/E such that $WD_{K_\lambda}(\rho_{A,\lambda})$ is unramified over F.*

Proof. Let F/E be a finite Galois extension over which A acquires good reduction. By Lemma B.4.1, we need to compare the $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_\ell)[W_E]$-module

$$D'(\mathcal{A}_{/k_F}[\ell^\infty])[1/\ell] \otimes_{W(k_F)} \overline{\mathbf{Q}}_\ell$$

and the $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_{\ell'})[W_E]$-module $V_{\ell'}(\mathcal{A}_{/k_F}) \otimes_{\mathbf{Q}_{\ell'}} \overline{\mathbf{Q}}_{\ell'}$. By our earlier observations, these are free modules over $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_\ell$ and $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_{\ell'}$ respectively, and for each $g \in W_E$, the characteristic polynomial of g (over $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_\ell$ and $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_{\ell'}$ respectively) under all of these representations is the same common polynomial $P_g \in K[T]$ (vastly more general comparison theorems for characteristic polynomials in étale and crystalline cohomology, at least for $K = \mathbf{Q}$, follow from [29, Thm 2(2)]).

To see the semisimplicity in all cases, we first claim that it suffices to check semisimplicity as W_F-representations. Indeed, if L is any field of characteristic 0 and G is any group with H a finite index subgroup, an $L[G]$-module with finite L-dimension which is semisimple as an $L[H]$-module is necessarily semisimple as an $L[G]$-module. To prove this, we just need to show that for $L[G]$-modules V and W with finite L-dimension, the natural map $\mathrm{Ext}^1_{L[G]}(V,W) \to \mathrm{Ext}^1_{L[H]}(V,W)$ is injective. But if we replace H by a finite index subgroup which is normal in G, this is indentified with the restriction map

$$H^1(G, V^* \otimes_L W) \to H^1(H, V^* \otimes_L W),$$

which is injective because $H^1(G/H, V^* \otimes_L W)$ is an L-vector space killed by $[G : H]$.

Viewing our W_E-representation spaces as W_F-representation spaces, all are unramified and we just need to check that the action of $\theta(\mathrm{Frob}_F)$ on $\mathcal{A}_{/k_F}$ is annihilated (in the 'up to isogeny' category) by a separable polynomial over K, or even over $\mathbf{Q}$. Since $\theta(\mathrm{Frob}_F)$ is the action of the k_F-Frobenius morphism on the abelian variety $\mathcal{A}_{/k_F}$, the 'semisimplicity' here is due to Weil. Here is the proof, for which

we may assume $K = \mathbf{Q}$. Let $\prod P_i^{e_i} \in \mathbf{Q}[T]$ be the characteristic polynomial P_{Frob_F}, with P_i irreducible. For $\ell' \neq \ell$, $\prod P_i^{e_i}(\theta(\mathrm{Frob}_F))$ kills $V_{\ell'}(\mathcal{A}_{/k_F})$, so it is the zero endomorphism of $\mathcal{A}_{/k_F}$. Each simple abelian subvariety of $\mathcal{A}_{/k_F}$ is preserved under the k_F-Frobenius morphism $\theta(\mathrm{Frob}_F)$, so $\prod P_i(\theta(\mathrm{Frob}_F))$ kills each such subvariety (by simplicity and the fact that $K = \mathbf{Q}$). Since $\mathcal{A}_{/k_F}$ is isogenous to a product of such subvarieties, $\prod P_i(\theta(\mathrm{Frob}_F)) = 0$ in $\mathrm{End}^0_{k_F}(\mathcal{A}_{/k_F})$.

Now we check that our semisimple W_E-representation spaces are base changes of semisimple $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})[W_E]$-modules, necessarily finite and free over $K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}$. The resulting $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})[W_E]$-modules are all isomorphic, as one sees by comparing characteristic polynomials of all $g \in W_E$ (which lie in $K[T]$). This readily yields the last part of the Proposition as well, since when $WD_{K_\lambda}(\rho_{A,\lambda})$ is unramified over some finite extension F/E, then the same clearly holds for all primes of K over ℓ (by a consideration of semisimplicity and characteristic polynomials), so for any $\ell' \neq \ell$, $V_{\ell'}(A)$ is unramified over F; by the Néron-Ogg-Shafarevich criterion, $A_{/F}$ then has good reduction.

Consider an extension L/K of characteristic 0 fields with K algebraically closed (e.g., $K = \overline{\mathbf{Q}}$, $L = \overline{\mathbf{Q}}_\ell$ or $\overline{\mathbf{Q}}_{\ell'}$), G a finitely generated group (such as W_E/I_F), and V a semisimple $L[G]$-module with finite L-dimension. Assume that all $g \in G$ act with characteristic polynomial in $K[T]$. The above setup is just a 'finite product' of this setting, replacing K and L by K^n and L^n for some $n \geq 1$ and replacing V by $V \otimes_K K^n$ where we use n field automorphisms $K \cong K$ to define $K \to K^n$. We claim that there exists a (necessarily unique up to isomorphism) semisimple $K[G]$-module V_0 with finite K-dimension such that all $g \in G$ have the same characteristic polynomials on V_0 as on V (which implies that $V_0 \otimes_K L \cong V$ as $L[G]$-modules and so finishes the proof). Since G is finitely generated, if we pick a basis of V over L then there exists a finitely generated extension field K'/K inside of L and a $K'[G]$-module V' with finite K'-dimension such that $V' \otimes_{K'} L \cong V$ as $L[G]$-modules. In fact, we can even find a finite type K-subalgebra $R' \subseteq K'$ and an $R'[G]$-module M' which is finite and free as an R'-module such that $M' \otimes_{R'} L \cong V$. Each $g \in G$ has characteristic polynomial on M' equal to the characteristic polynomial of g on V, which lies in $K[T]$. By the Nullstellensatz there exists a K-algebra map $R' \to K$, so if we define $V_0 = (M' \otimes_{R'} K)^{\mathrm{ss}}$, we're done.

■

Note that by a theorem of Grothendieck [25, Exp. IX, Cor 5.10], $\rho_{A,\ell}$ becomes Barsotti-Tate over F if and only if A acquires good reduction over F (for a simpler exposition of the proof of Grothendieck's theorem if one assumes potentially good reduction, see the proof of [5, Thm 5.3]).

Corollary B.4.3. *Suppose that f is a weight two newform with coefficients in a number field K. Let $\pi \cong \otimes'_v \pi_v$ denote the corresponding automorphic representation. For each prime λ of K, let*

$$\rho_{\pi,\lambda} : G_{\mathbf{Q}} \to \mathrm{GL}_2(K_\lambda)$$

denote the associated Galois representation. If $\lambda|\ell$ and π_ℓ is not special, then $\rho_{\pi,\lambda}|_{G_\ell}$ is Barsotti-Tate over any extension of $\mathbf{Q}_\ell$ such that $WD(\pi_\ell)|_{I_F}$ is trivial (such an F exists). Also, for any embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_\ell$ inducing the place λ on $K \subseteq \overline{\mathbf{Q}}$ (and so inducing an embedding $K_\lambda \to \overline{\mathbf{Q}}_\ell$ as K-algebras), there is a $\overline{\mathbf{Q}}_\ell[W_\ell]$-module isomorphism

$$\overline{\mathbf{Q}}_\ell \otimes_{\overline{\mathbf{Q}}} WD(\pi_\ell) \cong WD(\rho_{\pi,\lambda}|_{G_\ell}).$$

Proof. If $K_0 \subseteq K$ denotes the subfield generated by the q-expansion coefficients of f and λ lies over λ_0 in K_0, then $\rho_{\pi,\lambda} \simeq K_\lambda \otimes_{K_{0\lambda_0}} \rho_{\pi,\lambda_0}$, so we may suppose $K = K_0$. In this case, the Eichler-Shimura construction provides an abelian variety $A_f = A_{/\mathbf{Q}}$ with an action of an order in $\mathcal{O}$ so that $\rho_{A,\lambda} \cong \rho_{\pi,\lambda}$ for all primes λ and $\dim A = [K : \mathbf{Q}]$. Choose any $\ell' \neq \ell$ and pick a K-algebra map $\overline{\mathbf{Q}} \to K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}$. Define $\sigma_\ell = (K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}) \otimes_{\overline{\mathbf{Q}}} WD(\pi_\ell)$. By [3, Thm A],

$$\rho_{A,\ell'}|_{W_\ell} \otimes_{\mathbf{Q}_{\ell'}} \overline{\mathbf{Q}}_{\ell'} \cong \sigma_\ell \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_{\ell'}$$

as $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_{\ell'})[W_\ell]$-modules. We want to construct a $(K \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_\ell)[W_\ell]$-module isomorphism

$$WD_{\mathbf{Q}_\ell}(\rho_{A,\ell}|_{G_\ell}) \cong \sigma_\ell \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_\ell.$$

But this is immediate from Proposition B.4.2.

■

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Spring-Verlag, 1987.

[2] K. Brown, Cohomology of Groups, Springer-Verlag, 1982.

[3] H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Éc. Norm. Sup. **19** (1986), 409–468.

[4] H. Carayol, *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785–801.

[5] B. Conrad, *Finite group schemes over bases with low ramification*, to appear in Compositio Mathematica.

[6] B. Conrad, *Ramified deformation problems*, to appear in Duke Math. Journal.

[7] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge Univ. Press, 1992.

[8] C. Curtis, I. Reiner, Methods of Representation Theory, Volume 1, Wiley & Sons, New York, 1981.

[9] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*, in Current Developments in Mathematics, 1995, International Press, 1996, pp. 1–154.

[10] B. de Smit, H. Lenstra, *Explicit construction of universal deformation rings*, in Modular Forms and Fermat's Last Theorem (Boston, 1995), Springer-Verlag, 1997, pp. 313–326.

[11] F. Diamond, *The refined conjecture of Serre*, in Elliptic Curves, Modular Forms and Fermat's Last Theorem (Hong Kong, 1993), International Press, 1995, pp. 22–37.

[12] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144** (1996), 137–166.

[13] F. Diamond, *The Taylor-Wiles construction and multiplicity one*, Inv. Math. **128** (1997), 379–391.

[14] F. Diamond, R. Taylor, *Non-optimal levels for mod ℓ modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Inv. Math. **115** (1994), 435–462.

[15] F. Diamond, R. Taylor, *Lifting modular mod ℓ representations*, Duke Math. J. **74** (1994), 253–269.

[16] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Inv. Math. **109** (1992), 563–594.

[17] N. Elkies, *Elliptic and modular curves over finite fields, and related computational issues*, to appear in Computational Perspectives on Number Theory (J. Teitelbaum, ed.).

[18] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque **47-48**, Société mathématique de France, Paris, 1977.

[19] J.-M. Fontaine, *Le corps des périodes p-adiques* in Périodes p-adiques Astérisque **223**, 59–111.

[20] J.-M. Fontaine, *Représentations p-adiques semi-stables*, in Périodes p-adiques, Astérisque **223**, 113–184.

[21] J.-M. Fontaine, *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Annals of Mathematics, **115** (1982), 529–577.

[22] J.-M. Fontaine, B. Mazur, *Geometric Galois representations*, in Elliptic Curves, Modular Forms and Fermat's Last Theorem (Hong Kong, 1993), International Press, 1995, pp. 41–78.
[23] K. Fujiwara, *Deformation rings and Hecke algebras in the totally real case*, preprint.
[24] P. Gérardin, *Facteurs locaux des algèbres simples de rang 4. I*, in Groupes Réductifs et Formes Automorphes, I (Paris, 1976–77) Univ. Paris VII, 1978, pp. 37–77.
[25] A. Grothendieck, Groupes de Monodromie en Géométrie Algébrique (SGA 7), Lecture Notes in Math. **288**, Springer-Verlag, 1972.
[26] A. Grothendieck, Schémas en Groupes (SGA3), Lecture notes in Math. **151**, Springer-Verlag, 1970.
[27] Y. Ihara, On modular curves over finite fields, Discrete Subgroups of Lie Groups and Applications to Moduli (Bombay, 1973), Oxford Univ. Press, 1975, pp. 161–202.
[28] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Princeton Univ. Press, 1985.
[29] N. Katz, W. Messing, *Some consequences of the Riemann Hypothesis for varieties over finite fields*, Inv. Math. **23** (1974), 73–77.
[30] B. Mazur, *Deforming Galois representations*, in Galois Groups over $\mathbf{Q}$ (MSRI, 1987) Springer-Verlag, 1989, pp. 385–437.
[31] D. Mumford, Abelian Varieties, Oxford University Press, 1970.
[32] R. Ramakrishna, *On a variation of Mazur's deformation functor*, Comp. Math. **87** (1993), 269–286.
[33] M. Raynaud, *Schémas en groupes de type* $(p, p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.
[34] T. Saito, *Modular forms and p-adic Hodge theory*, Inv. Math. **129** (1997), 607–620.
[35] J.-P. Serre, *Le problème des groupes de congruence pour* SL_2, Ann. Math. **92** (1970), 489–527.
[36] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259–331.
[37] J.-P. Serre, Cohomologie Galoisienne, Springer-Verlag, 1973.
[38] J.-P. Serre, Linear Representations of Finite Groups, Springer-Verlag, 1977.
[39] J.-P. Serre, Trees, Springer-Verlag, 1980.
[40] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.
[41] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics **88** (1968), 492–517.
[42] G. Shimura, *Algebraic number fields and symplectic discontinuous groups*, Ann. Math. **86** (1967), 503–592.
[43] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton Univ. Press, 1971.
[44] J. Tate, *p-divisible groups* in Proceedings of a Conference on Local Fields (Dreibergen, 1966), Springer, 1967, pp. 158-183.
[45] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.
[46] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.