Deformations of Induced Galois Representations

S. Cho & V. Vatsal

November 1, 2000

1   Introduction

The object of this article is to study the behavior of certain deformation problems and Hecke rings under base change to a real quadratic field. These questions were the subject of conjectures by Doi, Hida, Ishii (see [DHI98] and [Hid98]); in this paper, we will show that Conjecture 2.2 of [Hid98] holds under a suitable hypothesis, and that the isomorphism predicted by Conjecture 3.8 of [DHI98] holds up to a pseudo-null cokernel. The deformations studied in this paper are also interesting in light of the recent work by Skinner and Wiles (see [SW97] and [SW99]) on the deformation of reducible Galois representations. Namely, the ring R_+^{ord} studied in [Hid98] and [DHI98] turns out to be closely related to a pseudo-deformation ring; the explication of this connection is crucial to our results. Furthermore, the central conjecture of [Hid98] turns out to be related to a certain class number condition, which is exactly analogous to the condition that appears in [SW97]. Finally, we would like to point out that the deformations considered here give rise to a number of interesting examples. Specifically, we are able to exhibit Λ-adic representations whose traces generate a nontrivial extension of Λ, and with the property that the specializations to certain arithmetic points of weight one are actually *ramified* over $\mathrm{Spec}(\Lambda)$. This is in contrast to the well-known theorem of Hida, which asserts that arithmetic points of weight $k \geq 2$ are smooth over $\mathrm{Spec}(\Lambda)$.

To state the results more precisely, we consider a real quadratic extension $F = \mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, with $D > 0$. Write σ for a generator of the group $\Delta = \mathrm{Gal}\,(F/\mathbb{Q})$. We fix a prime $p > 2$, with $(D, p) = 1$, such that $p = \mathfrak{p}\mathfrak{p}^\sigma$ in F with $\mathfrak{p} \neq \mathfrak{p}^\sigma$. Let F_p denote the maximal algebraic extension of F unramified outside p and infinity. Let $H = \mathrm{Gal}\,(F_p/F)$, and let $G = \mathrm{Gal}\,(F_p/\mathbb{Q})$.

Now consider a character

$$\overline{\varphi} : H \to \mathbb{F}^\times$$

unramified outside $\mathfrak{p}$, where $\mathbb{F}$ is a finite field of characteristic p. Then let

$$\overline{\rho} = \mathrm{Ind}_{\mathbb{Q}}^{F}\overline{\varphi} : G \to GL_2(\mathbb{F})$$

be the induction of $\overline{\varphi}$ from H to G. We assume that $\bar{\rho}$ is absolutely irreducible. Observe that our hypotheses imply that $\overline{\rho}$ is *ordinary* in the sense that

$$\rho|_{D_\mathfrak{p}} = \begin{pmatrix} \overline{\varphi} & * \\ 0 & \overline{\varphi}^\sigma \end{pmatrix}$$

where $\overline{\varphi}^\sigma$ is unramified for the decomposition group $D_\mathfrak{p}$ at $\mathfrak{p}$. Furthermore, we will assume that

$$\overline{\varphi}^2|_{I_\mathfrak{p}} \neq 1,$$

for the inertia group $I_\mathfrak{p}$ at $\mathfrak{p}$.

Let $\mathcal{O}$ denote the ring of integers of a finite extension $K/\mathbb{Q}_p$. We assume that $\mathcal{O}$ contains the ring of Witt vectors for $\mathbb{F}$. Let π denote a uniformizing element of $\mathcal{O}$, and let $k = \mathcal{O}/\pi$ denote the residue field. Let $CNL_\mathcal{O}$ be the category of complete, noetherian, local $\mathcal{O}$-algebras with residue field k, and let $SETS$ be the category of sets. We consider a deformation functor $\mathcal{F}_G^{\mathrm{ord}} : CNL_\mathcal{O} \to SETS$ given by strict equivalence classes of deformations $\tilde{\rho} : G \to GL_2(A)$ of $\overline{\rho}$, that are ordinary at $\mathfrak{p}$. It is by now a standard matter to show, using Schlesinger's criteria, that the functor $\mathcal{F}_G^{\mathrm{ord}}$ is representable; taking this for granted, we write R^{ord} for the universal deformation ring. Thus R^{ord} is a complete Noetherian local $\mathcal{O}$-algebra with residue field k.

Let $\chi_F : G/H \cong \{\pm 1\}$ be the nontrivial character of $\Delta = G/H$. Since $\overline{\rho} \otimes \chi_F \cong \overline{\rho}$, we see that

$$\rho \mapsto \rho \otimes \chi_F$$

induces an automorphism of the deformation functor and hence, an automorphism

$$\tau : R^{ord} \to R^{ord}$$

with $\tau^2 = 1$. Write R_+^{ord} for the subring of R^{ord} fixed by τ. Then R_+^{ord} and R are naturally algebras over $\Lambda = \mathcal{O}[[T]]$, and it is known by works of Hida and Taylor-Wiles that R^{ord}, and hence R_+^{ord}, are reduced and free of finite rank over Λ. See [Hid85], [Wil95] and [TW95]. To apply the result of Taylor-Wiles, we observe that it follows from our assumption that $\overline{\varphi}^2$ is nontrivial on inertia that $\overline{\rho}$ is not induced from the quadratic subfield of $\mathbb{Q}(\zeta_p)$.

Now let ϵ denote a fundamental unit of the quadratic field F. We may view ϵ as an element of $\mathbb{C}_p$ via the completion of F at the prime $\mathfrak{p}$, where $\mathbb{C}_p$ denotes the completion of an algebraic closure of $\mathbb{Q}_p$ at a prime lying over $\mathfrak{p}$. If $\log_p$ denotes the p-adic logarithm function on $\mathbb{C}_p$, we set $<\epsilon> = (1 + T)^{\log_p(\epsilon)/\log_p(1+p)}$. Let I_χ denote the ideal of R^{ord} generated by elements of the form $a - \tau(a)$. Then we have the following conjecture of Hida ([Hid98], Conjecture. 2.2):

Conjecture 1.1 *If $\mathcal{O}$ is sufficiently large, we have $R^{ord} = R_+^{ord}[\sqrt{<\epsilon> - 1}]$. The ideal I_χ is principal, generated by $\sqrt{<\epsilon> - 1}$.*

In this paper, we will show that this conjecture is equivalent to certain hypotheses on class numbers. To state this more precisely, let Cl_F denote the p-Sylow subgroup of the ideal class group of F. Then we will prove

Theorem A. *Each of the following statements is a necessary condition for the validity of Conjecture 1.1 :*

1. *$\mathrm{rank}_\Lambda(R^{ord}) = \#\mathrm{Cl}_F$, or*

2. *the subgroup $S \subset \dim_k(H^1(\mathrm{Gal}\,(F_p/F), \overline{\varphi}/\overline{\varphi}^\sigma)$ consisting of cocycles unramified outside $\mathfrak{p}$ is a one-dimensional k-space.*

Furthermore, statement 1 above is even sufficient for Conjecture 1.1

Condition 2 above is the exact analogue of the condition (ii) in Theorem 1.2 of the work by Skinner and Wiles (see [SW97]), on deformation of reducible Galois representations. Indeed, Skinner and Wiles show that their condition (ii) implies that certain deformation rings coming from reducible representations are complete intersections. This property is faithfully echoed in our Theorem 2.1 below. It seems rather likely that one could prove the sufficiency of the second statement by generalizing the results of [SW97] to real quadratic fields, but we have not pursued this.

On the other hand, the present situation was studied from a different point of view by Doi, Hida, and Ishii, in the fundamental work [DHI98]. The main consideration here is that of congruence relations between Hilbert modular forms, and their reflection in certain twisted adjoint L-values. Crucial to this study is the understanding of congruences between forms that arise via base-change from $\mathbb{Q}$, and forms that are intrinsic to F.

Thus, let $\mathfrak{m}$ denote the maximal ideal of the Hecke ring p-adic Hecke algebra $h_\mathbb{Q} = h_\mathbb{Q}(Dp^\infty)$ of level Dp^∞, determined by the representation $\rho = \mathrm{Ind}_\mathbb{Q}^F(\varphi) : G \to GL_2(\mathcal{O})$, for the Teichmuller lift φ of $\overline{\varphi}$. Such a maximal ideal exists because (as was known to Hecke) the representation ρ corresponds to a theta series of weight one on $\Gamma_1(Dp)$.

Now consider the Hecke ring $h_F = h_F(p^\infty)$ arising from Hilbert modular forms of level p^∞ for the field F. Then Doi, Hida, and Ishii have constructed a base-change morphism

$$\beta : h_F \to h_\mathbb{Q}.$$

Let $\mathfrak{n}$ denote the inverse image of $\mathfrak{m}$ under this base-change map. Then we have the following conjecture (see [DHI98], Conjecture. 3.8):

Conjecture 1.2 *Suppose $\overline{\varphi}$ is everywhere unramified, so that $\det(\rho) = \chi_F$. Then, passing to the completions at $\mathfrak{m}$ and $\mathfrak{n}$ gives an isomorphism*

$$\beta : h_{F,\mathfrak{n}} \cong h_{\mathbb{Q},\mathfrak{m}}^w,$$

where $h_{\mathbb{Q},\mathfrak{m}}^w$ is the fixed part of $h_{\mathbb{Q},\mathfrak{m}}$ under the action of the Atkin-Lehner involution w.

In view of the isomorphism theorems between Hecke rings and deformation rings, one can translate the above conjecture into a statement about deformation rings. In this setting the conjecture predicts that the fixed part of R^{ord} under the involution τ is generated by the image of h_F. In view of the well-known properties of modular representations, this may be restating as requiring that R_+^{ord} be generated by the traces $\text{Tr}\,(\varrho(\text{Frob}(\mathfrak{q})))$, for primes $\mathfrak{q}$ of F, where $\varrho : G \to GL_2(R^{ord})$ denotes the universal representation.

In this paper, we will prove that the analog of Conjecture 1.2 holds up to pseudo-isomorphism:

Theorem B *Suppose that $\overline{\varphi}$ satisfies $\overline{\varphi}^2|_{I_\mathfrak{p}} \neq 1$. Then there is a natural morphism*

$$\beta : h_F \to R_+^{ord} \subset R^{ord} \cong h_{\mathbb{Q},\mathfrak{m}}.$$

The ring $\beta(h_F)$ has finite index in R_+^{ord}.

The proof of this theorem is based on the interpretation of R_+^{ord} in terms of deformation theory. However we cannot simply appeal to Mazur's deformation theory to complete this plan. Rather, we are forced to consider the more general notions of pseudo-representations and pseudo-deformations, as introduced by Wiles and Skinner (see [Wil88] and [SW99]). The reason for this may be described as follows. The Taylor-Wiles theorem, applied to the residual representation $\overline{\rho}$, tells us that R^{ord} is isomorphic to the Hecke ring $h_{\mathbb{Q},\mathfrak{m}}$. It is therefore natural to seek an interpretation of R_+^{ord} in terms of the restriction (base-change) of $\overline{\rho}$ to $\text{Gal}\,(F_p/F)$. But, since $\overline{\rho}$ is an induced representation, it is clear that $\overline{\rho}$ becomes reducible when restricted to $\text{Gal}\,(F_p/F)$. As is well-known, reducible representations do not have a good deformation theory, because the associated functor is not representable. Skinner and Wiles observed that one still has a good pseudo-deformation functor, and it is their approach that we will follow in this paper.

Finally, we would like to warn the reader that we will make free use of the theorems of Taylor and Wiles [TW95], [Wil95] in this paper. These celebrated theorems identify certain deformation rings as familiar Hecke algebras, and one can therefore obtain information about the deformation side by invoking Hida's extensive study of the Hecke theory. As a reference for Hida's theory, we refer the reader to [Hid85] and [Hid93]. Note however that the results of [Hid85] assume $p \geq 5$ for technical reasons, although it is well-known to the experts that the the restriction can be eliminated. The basic argument is given in [Hid93], Chapter 7, where simpler proofs are given for many of the theorems in [Hid85]. In this paper we will assume the validity of Hida's theory for $p = 3$.

The authors would like to thank H. Hida and A. Wiles for their help and guidance. Some of the results in this paper are drawn from the first named author's Ph. D. thesis, written at UCLA under the direction of Hida. By a curious coincidence, a related line of

investigation was suggested to the second author by Wiles, but that project subsequently took a somewhat different direction. The second author would also like to thank Skinner and Wiles for sharing the results of their joint work; their study of pseudo-deformations provided some of the crucial ideas needed for the proof of Theorem B. Finally, we would like to thank the referee for numerous comments towards the improvement of this work, and for pointing out an error in the original version of the manuscript. The responsibility for any remaining errors is solely that of the authors.

2 A Sufficient Condition

In this section, we prove a necessary and sufficient condition for the validity of Conjecture 1.1, as given in Theorem A of the introduction.

Theorem 2.1 *The following statements hold:*

1. *We have $Rank_\Lambda(R_+^{ord}) \geq \#\mathrm{Cl}_F$. If the equality holds for the rank, the ring R_+^{ord} is a complete intersection.*

2. *If the ring R_+^{ord} is a Gorenstein ring, then the ideal I_χ is principal, generated by an element $\mathfrak{D} \in R^{ord}$ with $\mathfrak{D}^2 \in R_+^{ord}$. The element $\mathfrak{D}$ generates a free R_+^{ord}-module, and $R^{ord} = R_+^{ord}[\mathfrak{D}]$ is free of rank 2 over R_+^{ord}.*

3. *If the rank condition in part 1 above is satisfied, then $(\mathfrak{D}^2) = (< \epsilon > - 1)$ and $R^{ord} = R_+^{ord}[\sqrt{< \epsilon > - 1}]$, if $\mathcal{O}$ is sufficiently large.*

4. *If $\mathrm{rank}_\Lambda(R_+^{ord})$ is strictly greater than $\#\mathrm{Cl}_F$, then $I_\chi \cap R_+^{ord}$ is strictly larger than $(< \epsilon > - 1)$. The conjecture 1.1 does not hold in this case.*

We will break up the proof of the theorem into a series of steps. To begin with, consider the functor $\mathcal{F}_H : CNL_\mathcal{O} \to SETS$ defined by

$$\mathcal{F}_H(A) = \{\tilde{\varphi} : H \to A^\times | \tilde{\varphi} \text{ is unramified outside } \mathfrak{p} \text{ and } \tilde{\varphi} \equiv \overline{\varphi} \pmod{\mathfrak{m}_A}\}.$$

Let N be the maximal abelian p-extension of F unramified outside $\mathfrak{p}$. Then N/F is finite, since F is real quadratic. Let $H_\mathfrak{p}$ denote the finite group $\mathrm{Gal}(N/F)$. Then $\mathcal{F}_H(A)$ is represented by $(\mathcal{O}[H_\mathfrak{p}], \Phi)$ where $\Phi(h) = \varphi(h)h$ in $\mathcal{O}[H_\mathfrak{p}]$. Here we have identified the group element $h \in H_\mathfrak{p}$ with the corresponding element of the group ring, and we have written $\varphi(h) \in \mathcal{O}^\times$ for the Teichmuller lift of $\overline{\varphi}(h) \in k^\times$. With these notations, $\mathrm{Ind}_\mathbb{Q}^F(\Phi)$ is an element of $\mathcal{F}_G(\mathcal{O}[H_\mathfrak{p}])$. Thus, there exists a unique morphism $\alpha : R^{ord} \to \mathcal{O}[H_\mathfrak{p}]$ such that $\alpha \circ \varrho$ is equivalent to $\mathrm{Ind}_\mathbb{Q}^F(\Phi)$, where (R^{ord}, ϱ) is the universal couple for $\mathcal{F}_G$. As we have remarked, the character χ acts on $\mathcal{F}_G^{\mathrm{ord}}$ by $\rho \mapsto \rho \otimes \chi$. Then we have the following simple lemma:

5

Lemma 2.2 *The morphism $\iota : \mathcal{F}_H(A) \to \mathcal{F}_G(A)^\tau$ given by $\xi \mapsto \mathrm{Ind}_\mathbb{Q}^F(\xi)$ is an isomorphism, where $\mathcal{F}_G(A)^\tau$ is the part of $\mathcal{F}_G(A)$ fixed by τ.*

Proof. Let $\tilde{\rho}$ denote an element of $\mathcal{F}_G(A)^\tau$. Then we have $\tilde{\rho} \cong \tilde{\rho} \otimes \chi$. According to a lemma of Doi, Hida, and Ishii ([DHI98], Lemma 3.2) the isomorphism $\tilde{\rho} \otimes \chi \cong \tilde{\rho}$ holds if and only if $\tilde{\rho}$ is of the form $\mathrm{Ind}_\mathbb{Q}^F(\xi)$ for some φ. Thus the map ι is surjective. The injectivity is an easy exercise, and may safely be left to the reader.

Corollary 2.3 *There is an isomorphism $R^{ord}/I_\chi \cong \mathcal{O}[H_\mathfrak{p}]$. The ideal $I_\chi \cap \Lambda$ of Λ is principal, generated by $\langle \epsilon \rangle - 1$.*

Proof. The first assertion follows from the preceding lemma, and the observation that R^{ord}/I_χ is the maximal quotient of R^{ord} on which τ acts trivially. Now let Cl_F denote the p-Sylow subgroup of the class group of F. Then the second statement follows from the short exact sequence of class-field theory

$$0 \to U_\mathfrak{p}^1/\langle \epsilon \rangle \to H_\mathfrak{p} \to \mathrm{Cl}_F \to 0,$$

where $U_\mathfrak{p}^1$ denotes the the pro-p part part of the unit group in the integer ring in $F_\mathfrak{p}$. Here we have used the facts that the action of Λ is via the determinant, and that $\det(\mathrm{Ind}_\mathbb{Q}^F(\Phi)) = \chi_F \cdot N_\mathbb{Q}^F(\Phi)$ restricts to a faithful character of $U_\mathfrak{p}^1/< \epsilon >$.

We can now prove the first statement in Theorem 2.1. We contend first that there is a *surjection*

$$R_+^{ord}/TR_+^{ord} \to \mathcal{O}[\mathrm{Cl}_F]. \tag{1}$$

This may be seen as follows. Corollary 2.3 gives an exact sequence

$$0 \to I_\chi \to R^{ord} \to \mathcal{O}[H_\mathfrak{p}] \to 0.$$

The ideal I_χ is invariant under the action of τ, so that we get an induced action of τ on $\mathcal{O}[H_\mathfrak{p}]$. One verifies that this induced action coincides with the obvious $\mathrm{Ind}_\mathbb{Q}^F(\Phi) \mapsto \mathrm{Ind}_\mathbb{Q}^F(\Phi) \otimes \chi$. But, by the lemma of Doi, Hida and Ishii cited previously, one has $\mathrm{Ind}_\mathbb{Q}^F(\Phi) \cong \mathrm{Ind}_\mathbb{Q}^F(\Phi) \otimes \chi$. Thus $H^0(\tau, \mathcal{O}[H_\mathfrak{p}]) = \mathcal{O}[H_\mathfrak{p}]$. Furthermore, we have $H^0(\tau, R^{ord}) = R_+^{ord}$ by definition, and $H^1(\tau, I_\chi) = 0$ since I_χ is p-profinite and τ has order 2 (recall that $p \neq 2$). We therefore obtain a surjection

$$R_+^{ord} = H^0(\tau, R^{ord}) \to H^0(\tau, \mathcal{O}[H_\mathfrak{p}]) = \mathcal{O}[H_\mathfrak{p}].$$

Reduce both sides modulo T. Since the tensor product is right-exact, the resulting map is still a surjection. The left-hand side is simply R_+^{ord}/TR_+^{ord}. Since $\mathcal{O}[H_\mathfrak{p}]$ represents the

functor $\mathcal{F}_H$, we see that the quotient modulo T represents the subfunctor whose points give a trivial deformation of the determinant. It is clear that this subfunctor is represented by $\mathcal{O}[\mathrm{Cl}_F]$. Thus we get a surjection $R_+^{ord}/TR_+^{ord} \to \mathcal{O}[\mathrm{Cl}_F]$.

Now suppose that $\mathrm{rank}_\Lambda(R_+^{ord}) \leq \#\mathrm{Cl}_F$. Since $\mathcal{O}[\mathrm{Cl}_F]$ already has rank equal to $\#\mathrm{Cl}_F$, we must have an equality of ranks in (1), and, consequently, an isomorphism $R_+^{ord}/TR_+^{ord} = \mathcal{O}[\mathrm{Cl}_F]$. It is clear that $\mathcal{O}[\mathrm{Cl}_F]$ is a complete intersection. Furthermore, it follows from the work of Taylor and Wiles that T is not a zero-divisor in R_+^{ord}. Indeed, the theorems of [TW95] and [Wil95] show that R^{ord} is isomorphic to a certain p-adic Hecke algebra $\mathbf{T}$ of level Dp^∞, which was shown by Hida to be free over Λ. The ring R_+^{ord} being a direct summand of R^{ord}, it follows that R_+^{ord} is a projective, hence free, Λ-module as well. Applying Theorem 21.2 (ii), of [Mat90], we conclude that R_+^{ord} is a complete intersection. This proves the first part of Theorem 2.1.

We now consider the second statement of the theorem. For an element $x \in R^{ord}$, we define $\mathrm{Tr}\,(x) = \mathrm{Tr}_{R_+^{ord}}^{R^{ord}}(x) = x + \tau(x)$. This definition makes sense even though R^{ord} is not known to be free over R_+^{ord} (which is necessary to give a definition using linear algebra). We would also like to point out another simple consequence of the Taylor-Wiles isomorphism, namely, that R^{ord} is finitely generated over R_+^{ord}, since both rings are finite, flat Λ-modules. This will be useful in the sequel.

Lemma 2.4 *The linear map $R^{ord} \to \mathrm{Hom}_{R_+^{ord}}(R^{ord}, R_+^{ord})$ given by $a \mapsto \xi_a : b \mapsto \mathrm{Tr}\,(ab)$ is injective. The induced pairing $R^{ord} \times R^{ord} \to R_+^{ord}$ is nondegenerate.*

Proof. Since the Hecke ring $\mathbf{T}$ is known to be reduced (see [Hid93], Chapter 7), we may apply the Taylor-Wiles theorems as above to conclude that that the ring $R^{ord} \cong \mathbf{T}$ is reduced. Now consider the total ring of fractions L of R_+. Since the set of zero-divisors of R_+^{ord} is the union of the minimal prime ideals, we see that L has the property that every prime ideal is maximal. Since L is reduced, it follows from [Mat90], Theorem 8.15 that L is in fact a product of fields (this could also be checked by hand). In particular, any L-module M is projective. Let $L = \prod L_i$, where each L_i is a field. Let $K = R^{ord} \otimes L$. Then we have a corresponding decomposition $K = \prod K_i$, where $K_i = K \otimes_L L_i$.

We contend that each K_i is free of rank 2 over L_i, satisfying $K_i = L_i \oplus X_i \cdot L_i$ where $\tau(X_i) = -X_i$. To see this, observe first that each K_i is a reduced Artin algebra over the field L_i, since R^{ord} is reduced and finitely generated over R_+^{ord}. This implies that K_i is a product of fields, and, in fact, that either $K_i = L_i \oplus L_i$, or K_i is a quadratic extension of L_i. In any case, K is a product of fields, and τ acts on each component K_i. Let K' be any direct factor of K, and write P for the kernel of the composite map $R^{ord} \to K \to K'$. Composing with the universal deformation, we get a representation ρ' of $\mathrm{Gal}\,(F_p/F)$ into $GL_2(R^{ord}/P)$. Since R^{ord} is a finitely generated module over R_+^{ord}, we see that P is a minimal prime ideal of R^{ord}. Since Hida's Λ-adic Hecke rings are equidimensional, of dimension 2, we conclude from the Taylor-Wiles isomorphism that R^{ord}/P has Krull dimension 2. On the other hand,

we have seen above that the maximal quotient of R^{ord} on which τ acts trivially is isomorphic to $\mathcal{O}[H_{\mathfrak{p}}]$, which has Krull dimension 1. It follows that τ acts nontrivially on the image of $R^{ord}/P \subset K' \subset K$. Thus we see that τ either induces a nontrivial automorphism of K' (if $K' = K_i$ for some i), or interchanges K' with another component K'' (if $K_i = K' \oplus K''$, for some i). In any case, we have $K_i = L_i \oplus X_i \cdot L_i$, where $\tau(X_i) = -X_i$, as asserted.

In view of these remarks, one sees that if $x \in K$, then $x + \tau(x) \in L$ is the trace of the L-linear mapping induced by multiplication by x. The lemma follows since K is reduced.

We now return to the proof of part 2 of the theorem. It is known, again as a consequence of the results of Wiles and Taylor, that the ring R^{ord} is a Gorenstein Λ-algebra. Furthermore, we are assuming that R^{ord}_+ is Gorenstein as well. Thus we have $\mathrm{Hom}_\Lambda(R^{ord}_+, \Lambda) \cong R^{ord}_+$, and this leads to

$$\mathrm{Hom}_{R^{ord}_+}(R^{ord}, R^{ord}_+) \cong \mathrm{Hom}_{R^{ord}_+}(R^{ord}, \mathrm{Hom}_\Lambda(R^{ord}_+, \Lambda)) \cong \mathrm{Hom}_\Lambda(R^{ord}, \Lambda) \cong R^{ord}. \quad (2)$$

Here the penultimate isomorphism is induced by $f \mapsto \{r \mapsto (f(r))(1)\}$.

In view of the preceding lemma, the rule

$$\theta(a) : x \mapsto \mathrm{Tr}\,(ax)$$

induces an inclusion $\theta : R^{ord} \hookrightarrow \mathrm{Hom}_{R^{ord}_+}(R^{ord}, R^{ord}_+)$. Fix an isomorphism

$$\mathrm{Hom}_{R^{ord}_+}(R^{ord}, R^{ord}_+) \cong R^{ord}.$$

Then the R^{ord}-module $\Theta = R^{ord}/(\theta(R^{ord}))$ is independent of this choice, and we have $\Theta \cong R^{ord}/\mathfrak{D}R^{ord}$, for some $\mathfrak{D} \in R^{ord}$. The element $\mathfrak{D}$ is called a different of R^{ord}/R^{ord}_+. It is determined up to units in $R^{ord\times}$.

Observe that $\mathfrak{D}$ is not a zero-divisor in R^{ord}. To prove this, consider $x \in R^{ord}$ such that $x \cdot \mathfrak{D} = 0$. Then, for arbitrary $a \in R^{ord}$, the definition of $\mathfrak{D}$ shows that there exists $f_a \in \mathrm{Hom}_{R^{ord}_+}(R^{ord}, R^{ord}_+)$ such that $\theta(a) = \mathfrak{D} \cdot f_a$. Hence we have $\mathrm{Tr}\,(ax) = (\mathfrak{D} \cdot f_a)(x) = f_a(\mathfrak{D}x) = f_a(0) = 0$. Since the trace is non-degenerate, it follows that $x = 0$. Thus $\mathfrak{D}^{-1}$ exists in the total ring of fractions of R^{ord}. We will exploit this fact below.

We will now show that we may choose $\mathfrak{D}$ so that $\tau(\mathfrak{D}) = -\mathfrak{D}$. Let us temporarily *assume* that there is a different $\mathfrak{D}$ which is a non-unit. Assuming this, we may then argue as follows. By definition of the different, $D = \mathfrak{D}^{-1}R^{ord} \subset K$ is the set of $x \in K$ with $\mathrm{Tr}\,(xR^{ord}) \subset R^{ord}_+$. Let $D^+ = D \cap L$. Then if $x \in D^+$, we have $2x = \mathrm{Tr}\,(x) \in R^{ord}_+$, so that $x \in R^{ord}_+$ (as $p \neq 2$). It follows that $D^+ = R^{ord}_+ \subset R \subset K$. Since we have assumed that $\mathfrak{D}$ is a non-unit, we see that $R^{ord} \subsetneq D$, which means that R^{ord} is a *proper* R^{ord}-submodule of D. On the other hand, D is free of rank one over R^{ord}, which implies that $R^{ord} \subset \mathfrak{m}D$, for the maximal ideal $\mathfrak{m}$ of R^{ord} (because $\mathfrak{m}X$ contains all proper R^{ord}-submodules of X, for any X free of rank 1). In particular, we get $D^+ = R^{ord}_+ \subset R^{ord} \subset \mathfrak{m}D$. It follows from Nakayama's Lemma (since

$p \neq 2$) that there exists $x \in D^- = D \cap K^{\tau=-1}$ such that x generates D as a B-module, as required.

Thus, we have reduced our contention to showing that the different $\mathfrak{D}$ is a non-unit. This does *not* seem to be evident, owing to the facts that R^{ord} is not known to be flat over R^{ord}_+, and our trace map is defined in an *ad hoc* way so that the formation of the different does not obviously commute with passage to fibers over the ramified points. We are forced therefore to invoke the analysis of §3 below, which uses entirely different methods, and which gives some control of the local properties at the points of interest. Thus we let P_{ord} denote the height one prime ideal of R^{ord} corresponding to the weight-one representation $\rho = \mathrm{Ind}^F_{\mathbb{Q}}(\varphi)$, for the Teichmuller lift φ of $\overline{\varphi}$. Let $P^+_{ord} = P_{ord} \cap R^{ord}_+$. Then P_{ord} is a fixed point for the action of τ, and we want to show that the localization of $\mathfrak{D}$ at P_{ord} is a non-unit.

Let us simply write $S = (R^{ord}_+)_{P^+_{ord}}$ for the localization of R^{ord}_+ at the prime P^+_{ord}. Then, according to Lemma 3.9 below, S is a discrete valuation ring. It follows from this that the localization $R^{ord} \otimes S$ of R^{ord} at P^+_{ord} is free, of rank 2. Furthermore, S is a Gorenstein ring by [Mat90], Thm. 18.2. Finally, S is a flat R^{ord}_+-algebra, so we have

$$\left(\mathrm{Hom}\,_{R^{ord}_+}(X, Y) \right) \otimes S = \mathrm{Hom}\,_S \left(X \otimes S, Y \otimes S \right),$$

for any two finitely generated R^{ord}_+-modules X and Y. In particular, we get

$$\mathrm{Hom}\,_S(R^{ord} \otimes S, S) = \mathrm{Hom}\,_{R^{ord}_+}(R^{ord}, R^{ord}_+) \otimes S \equiv R^{ord} \otimes S. \tag{3}$$

One then has a local different $\mathfrak{D}^{loc}$ corresponding to the flat extension of rings $S \to R^{ord} \otimes S$. One checks, using the flatness, that the trace pairing on R^{ord} (as defined above) gives the standard trace on the free S-module $R^{ord} \otimes S$. It is clear from this and (3) that formation of the different commutes with localization, which means that $\mathfrak{D}$ and $\mathfrak{D}^{loc}$, are associate in $(R^{ord})_{P^+_{ord}}$. On the other hand, we know from Corollary 3.12, that $(R^{ord})_{P_{ord}}$ is ramified over $(R^{ord}_+)_{P^+_{ord}}$, with ramification index 2. A standard calculation as in number theory shows that the local different $\mathfrak{D}^{loc}$ is a non-unit, and in fact lies in P_{ord}. Thus $\mathfrak{D}$ is a non-unit, as we have asserted.

In summary, we have shown that we may choose a different $\mathfrak{D}$ for R^{ord} over R^{ord}_+ such that $\tau(\mathfrak{D}) = -\mathfrak{D}$. Now let $x \in R^{ord}$ satisfy $\tau(x) = -x$. Then we have $\mathrm{Tr}\,(x/\mathfrak{D}) \in R^{ord}_+$. But $x/\mathfrak{D}$ is fixed by τ, so that we get $2x/\mathfrak{D} \in R^{ord}_+$. Since 2 is a unit, we get $x = a\mathfrak{D}$, for some $a \in R^{ord}_+$. This proves that that $R^{ord} = R^{ord}_+ \oplus \mathfrak{D} R^{ord}_+$, and that $R^{ord} = R^{ord}_+[\mathfrak{D}]$, as claimed. It is also clear from this that $I_\chi = \mathfrak{D} R^{ord}$ is principal. This completes the proof of item 2 in the theorem.

To verify statement 3, we must prove that $(\mathfrak{D})^2$ is associate to $<\epsilon> - 1$, under the hypothesis that $\mathrm{rank}_\Lambda(R^{ord}_+) = h = \#\mathrm{Cl}_F$. It follows easily from part 2 above that $I_\chi \cap R^{ord}_+$ is principal, generated by $\mathfrak{D}^2$. It suffices therefore to show that $I_\chi \cap R^{ord}_+$ is also generated by $<\epsilon> - 1$. Note here that since $I_\chi \cap \Lambda = (<\epsilon> - 1)$, we have $<\epsilon> - 1 \in I_\chi$.

9

Thus let n denote the cardinality of the finite group $\Gamma/<\epsilon>$. Then the algebra $\Lambda/(<\epsilon>-1)$ is a finite flat $\mathcal{O}$-algebra of rank n, and $R_+^{ord}/(<\epsilon>-1)$ has $\mathcal{O}$-rank nh. On the other hand, we have seen already that there are surjections $R_+^{ord}/(<\epsilon>-1) \to R_+^{ord}/(I_\chi \cap R_+^{ord}) \to \mathcal{O}[H_\mathfrak{p}]$. Since $\mathcal{O}[H_\mathfrak{p}]$ also has $\mathcal{O}$-rank nh, we find that $I_\chi \cap R_+^{ord}$ is generated by $<\epsilon>-1$.

It remains to prove the final assertion of our theorem. So suppose that $\mathrm{rank}_\Lambda(R_+^{ord}) > h$. Then $R_+^{ord}/(<\epsilon>-1)R_+^{ord}$ has $\mathcal{O}$-rank strictly larger than nh. In particular,

$$R_+^{ord}/(<\epsilon>-1)R_+^{ord} \to \mathcal{O}[H_\mathfrak{p}] = R_+^{ord}/(I_\chi \cap R_+^{ord})$$

must have nontrivial kernel. This implies that $I_\chi \cap R_+^{ord}$ is strictly larger than $(<\epsilon>-1)$. Thus Conjecture 1.1 cannot be valid in this case.

3   Deformations and pseudo-deformations

In this section we will give representation-theoretic descriptions of the rings R^{ord} and R_+^{ord}, and thereby calculate their cotangent spaces at certain prime ideals corresponding to dihedral representations. In terms of the Hecke algebra, these primes ideals correspond to modular forms of weight one.

These tangent space calculations are the key to our proof of Theorem B in the introduction. While the calculations for R^{ord} follow quite closely the ideas in [Wil95], where the prime ideals corresponding to certain modular forms of weight $k \geq 2$ are considered, the case of R_+^{ord} is quite different. As we have already remarked, we are interested in dihedral representations which become *reducible* upon restriction to $\mathrm{Gal}(F_p/F)$, so that we are forced to consider pseudo-representations, as introduced in [Wil88], as well as the pseudo-deformations of [SW99]. Even in the case of R^{ord}, we see a significant difference arising in the present instance: while the cotangent spaces of prime ideals that arise from modular forms of weight $k \geq 2$ are generally finite, our weight one form gives rise to a prime whose cotangent space is *infinite*.

The basic plan of attack is as follows. We will introduce a certain pseudo-deformation ring R^{ps}, which admits a map

$$R^{ps} \to R_+^{ord} \to R^{ord}.$$

The image of R^{ps} inside $R^{ord} \cong h_{\mathbb{Q},\mathfrak{m}}$ is precisely the image of the base-change Hecke ring h_F constructed from Hilbert modular forms over F. To compare R_+^{ord} and h_F, it therefore suffices to compare R^{ps} and R_+^{ord}. We achieve this by computing the tangent spaces, and showing that the map $R^{ps} \to R_+^{ord}$ becomes an isomorphism upon passing to the completion at height one prime ideals.

Deformations

Let $\rho' : \mathrm{Gal}\,(F_p/\mathbb{Q}) \rightarrow GL_2(\mathcal{O})$ be any ordinary deformation of $\overline{\rho}$, such that ρ' becomes *reducible* on the subgroup $H = \mathrm{Gal}\,(F_p/F)$. It follows from the considerations of the previous section that

$$\rho' = \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi),$$

where $\xi : H_{\mathfrak{p}} \rightarrow \mathcal{O}^{\times}$ is some abelian character. Then ρ' is induced by a unique homomorphism $R^{ord} \rightarrow \mathcal{O}$, and we will write P_{ord} to denote the corresponding prime ideal of R^{ord}. Note of course that both P_{ord}, as well as the homomorphism $R^{ord} \rightarrow \mathcal{O}$ depend on ρ' and ξ; for simplicity we will suppress this from the notation. Let K denote the field of fractions of $\mathcal{O}$. Then our goal is to prove

Theorem 3.1 *The vector space $M = P_{ord}/P_{ord}^2 \otimes K$ has dimension 1, and the localization of R^{ord} at P_{ord} is a discrete valuation ring.*

Proof. Consider the rank-4 representation $\mathrm{Ad}(\rho')$. Then an easy exercise in linear algebra shows that we have

$$\mathrm{Ad}(\rho') = 1 \oplus \chi_F \oplus \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi/\xi^{\sigma}), \tag{4}$$

where χ_F denotes the Kronecker character of the quadratic extension $F/\mathbb{Q}$. Observe here that, since φ is ramified only at $\mathfrak{p}$ and $\varphi^2|_{I_{\mathfrak{p}}} \neq 1$, we have $\frac{\xi}{\xi^{\sigma}} \neq \frac{\xi^{\sigma}}{\xi}$, so that the representation $\mathrm{Ind}_{\mathbb{Q}}^{F}(\frac{\xi}{\xi^{\sigma}})$ is irreducible.

We may realize $\mathrm{Ad}(\rho)$ by letting ρ act by conjugation on 2×2 matrices as follows:

$$\mathrm{Ad}(\rho) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \oplus \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix} \oplus \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \tag{5}$$

where each of the three summands in (4) is realized on matrices of the form indicated in the corresponding component of (5).

Now consider the subspace $V^{ord} \subset V = M_2(\mathcal{O}) = \mathrm{Ad}(\rho)$ consisting of matrices of the form $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$. Then we consider a Selmer group

$$\mathrm{Sel}(\mathbb{Q}, V) \subset H^1(\mathrm{Gal}\,(F_p/\mathbb{Q}), V \otimes K/\mathcal{O})$$

defined by local condition at $\mathfrak{p}$ as follows: we require that

$$\mathrm{Sel}(\mathbb{Q}, V) = \ker \left\{ H^1(\mathrm{Gal}\,(F_p/\mathbb{Q}), V \otimes K/\mathcal{O}) \rightarrow H^1(I_{\mathfrak{p}}, (V/V^{ord}) \otimes K/\mathcal{O}) \right\}. \tag{6}$$

Observe that we have $V^{ord} = V_1^{ord} \oplus V_2^{ord}$, where V_1^{ord} is the subspace $\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}$, and V_2^{ord} is the subspace $\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$. Then, with the notations of (4), we find that $V_1^{ord} \subset 1 \oplus \chi_F$, and that $V_2^{ord} \subset \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi/\xi^{\sigma})$. Thus we find that

$$\mathrm{Sel}(\mathbb{Q}, V) = \mathrm{Sel}(\mathbb{Q}, 1 \oplus \chi_F) \oplus \mathrm{Sel}(\mathbb{Q}, \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi/\xi^{\sigma}))$$

breaks up as a direct sum of two pieces, with local conditions given by the subspaces V_1^{ord} and V_2^{ord} respectively.

We first compute $\text{Sel}(\mathbb{Q}, 1 \oplus \chi_F)$. The inflation-restriction sequence gives

$$H^1(\text{Gal}\,(F_p/\mathbb{Q}), (1 \oplus \chi_F) \otimes K/\mathcal{O}) = \text{Hom}\,(\text{Gal}\,(F_p/\mathbb{Q}), K/\mathcal{O}) \oplus \text{Hom}\,(\text{Gal}\,(F_p/\mathbb{Q}), K/\mathcal{O})^{\chi_F}. \tag{7}$$

Now let F_p^{ab} denote the maximal pro-p-abelian extension of F that is unramified outside p. Let $L \subset F_p^{ab}$ denote the Hilbert class-field, and let h denote the degree of L/F. Then the definition of V_1^{ord} shows that $\text{Sel}(\mathbb{Q}, 1 \oplus \chi_F)$ is finite, of order equal $\#(\mathcal{O}/\eta)$, where

$$\eta = h \cdot \frac{\log_p(<\epsilon>)}{\log_p(1+p)} \in \mathcal{O}^\times. \tag{8}$$

This comes from a simple analysis of the ramification conditions, together with the description, coming from class field theory:

$$\text{Gal}\,(F_p^{ab}/H) = (U_{\mathfrak{p}}^1 \times U_{\mathfrak{p}^\sigma}^1)/ <\epsilon>.$$

Here $U_{\mathfrak{p}}^1$ denotes the pro-p-part of the units in the ring of integers in the completion of F at $\mathfrak{p}$. The definition of $U_{\mathfrak{p}^\sigma}^1$ is analogous.

On the other hand, the group $\text{Sel}(\mathbb{Q}, \text{Ind}_{\mathbb{Q}}^F(\xi/\xi^\sigma))$ is infinite, and in fact has $\mathcal{O}$-corank 1. To see this, observe that the $\mathcal{O}$-corank of $\text{Sel}(\mathbb{Q}, \text{Ind}_{\mathbb{Q}}^F(\xi/\xi^\sigma))$ is equal to the K-dimension of $\text{Sel}(\mathbb{Q}, \text{Ind}_{\mathbb{Q}}^F(\xi/\xi^\sigma)_K)$, where this time we take coefficients in the field K, rather than in the divisible module $K/\mathcal{O}$. But we may easily compute $\text{Sel}(\mathbb{Q}, \text{Ind}_{\mathbb{Q}}^F(\xi/\xi^\sigma)_K)$. Indeed, the inflation-restriction sequence gives

$$H^1(\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q}), K^2) \to H^1(\text{Gal}\,(F_p/\mathbb{Q}), \text{Ind}_{\mathbb{Q}}^F(\varphi/\varphi^\sigma)_K)$$
$$\to \text{Hom}\,(\text{Gal}\,(F_p/F(\xi/\xi^\sigma)), K^2)^{\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q})} \to H^2(\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q}), K^2), \quad (9)$$

where $F(\xi/\xi^\sigma)$ is the splitting field of the character ξ/ξ^σ, and $\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q})$ acts via the representation $\text{Ind}_{\mathbb{Q}}^F(\xi/\xi^\sigma)$. We remark that the degree of $F(\xi/\xi^\sigma)/\mathbb{Q}$ may be divisible by p. But, even so, we know that each of the terms $H^i(F(\xi/\xi^\sigma)/F, K^2)$ is killed by $\#(\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q}))$, and so must vanish, since we have taken coefficients in a field of characteristic zero. Thus we get an isomorphism

$$H^1(\text{Gal}\,(F_p/\mathbb{Q}), \text{Ind}_{\mathbb{Q}}^F(\varphi/\varphi^\sigma)_K) \cong \text{Hom}\,(\text{Gal}\,(F_p/F(\xi/\xi^\sigma)), K^2)^{\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q})}.$$

Observe also that we may identify

$$\text{Hom}\,(\text{Gal}\,(F_p/F(\xi/\xi^\sigma)), K^2)^{\text{Gal}\,(F(\xi/\xi^\sigma)/\mathbb{Q})} = \text{Hom}\,(\text{Gal}\,(F_p/F(\xi/\xi^\sigma)), K)^{\xi/\xi^\sigma}.$$

Now, unwinding the ramification conditions at $I_{\mathfrak{p}}$, and the action of $\operatorname{Gal}(F(\xi/\xi^\sigma)/\mathbb{Q})$, we find that

$$\operatorname{Sel}(\mathbb{Q}, \operatorname{Ind}_{\mathbb{Q}}^{F}(\varphi/\varphi^\sigma)_K) \subset \operatorname{Hom}(\operatorname{Gal}(F_p/F(\xi/\xi^\sigma)), K)^{\xi/\xi^\sigma}$$

consists of homomorphisms that are unramified at all primes of $F(\xi/\xi^\sigma)$ away from the prime $\mathfrak{p}$ of F. Any such homomorphism must factor through the Galois group G' of the maximal pro-p-abelian extension N of $F(\xi/\xi^\sigma)$ that is unramified outside $\mathfrak{p}$. But, from class-field theory, we know that

$$\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}^1 / U(F(\xi/\xi^\sigma)) \subset G'$$

with finite index, where $U(F(\xi/\xi^\sigma))$ denotes the image of the group of global units. But the character ξ is nontrivial at precisely one infinite place of F (since ρ' is odd) so that the character ξ/ξ^σ is totally odd. Dirichlet's unit theorem now implies that the ξ/ξ^σ-eigenspace inside the global units is trivial. Thus we get

$$\operatorname{Hom}(G', K)^{\xi/\xi^\sigma} = \operatorname{Hom}(((\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}^1) \otimes K)^{\xi/\xi^\sigma}, K),$$

and one checks easily that $((\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}^1) \otimes K)^{\xi/\xi^\sigma}$ has dimension one, as required.

Now, according to an argument of Wiles (see [Wil95], Proposition 1.2), we have

$$\operatorname{Sel}(\mathbb{Q}, \operatorname{Ad}(\rho)) = \operatorname{Hom}(P_{ord}/P_{ord}^2, K/\mathcal{O}).$$

Since the former has $\mathcal{O}$-corank one by what we have already proven, it follows that the prime ideal P_{ord} of R^{ord} at P_{ord} is locally principal, in the sense that P_{ord} is principal in the localization of R^{ord} at P_{ord}. To complete the proof of the first statement in our theorem, it therefore remains to prove that P_{ord} has height one. To do this, we recall the Λ-adic Hecke ring $h_{\mathbb{Q},\mathfrak{m}}$ of level Dp^∞, as defined in the introduction. As we have already remarked, there is a deformation ρ_h of $\overline{\rho}$, with values in $h_{\mathbb{Q},\mathfrak{m}}$. Since ρ' is associated to a p-ordinary modular form, we see that the morphism $R^{ord} \to \mathcal{O}$ induced by ρ' factors through the morphism $R^{ord} \to h_{\mathbb{Q},\mathfrak{m}}$. Let P_h denote the corresponding prime ideal of $h_{\mathbb{Q},\mathfrak{m}}$. Since $h_{\mathbb{Q},\mathfrak{m}}$ is a finite, flat Λ-algebra, we find that P_h has height one. This implies that P_{ord} has height ≥ 1. Since P_{ord} is locally generated by a single element, we conclude from [Mat90], Theorem 11.2 that the localization of R^{ord} at P_{ord} is a discrete valuation ring (see Remark 3.5 below).

Remark 3.2 Having proven that P_{ord} is locally principal, it is natural to ask for an explicit generator. In the case of prime ideals associated to modular forms of weight $k \geq 2$, Hida has shown that the corresponding prime ideals are unramified over Λ, and are locally generated by elements of the form $\omega_k = (1+T)^k - 1$. According to the Taylor-Wiles theorem, we have $R^{ord} \cong h_{\mathbb{Q},\mathfrak{m}}$, so that the corresponding primes of R^{ord} are also unramified over Λ. However, the prime ideal P_{ord} considered above is associated to a prime of weight one, and it turns out

to be *ramified* over Λ. This may be most conveniently seen as follows. The representation $\rho' = \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi)$ satisfies $\rho' = \rho' \otimes \chi$, and so is fixed by the involution τ. It follows that P_{ord} is ramified over R_+^{ord}, and that the ramification index of P_{ord} over Λ is even.

Now let $\mathscr{F}$ denote any Λ-adic family of representations that specializes to ρ in weight one. It follows from the theorem above that $\mathscr{F}$ is unique, since there is only one component of $\mathrm{Spec}(R^{ord})$ passing through the point P_{ord}. Furthermore, since P_{ord} is ramified over Λ, it follows that the representation $\mathscr{F}$ cannot be realized over Λ. Equivalently, the coefficients of the associated Λ-adic form generate a nontrivial extension of Λ. We summarize these observations in the following

Corollary 3.3 *The prime ideal P_{ord} has even ramification index $2n$ over Λ, where $n \geq 1$. There exists a unique Λ-adic family of representations specializing to ρ in weight one. The traces of this Λ-adic representation generate a nontrivial extension of Λ.*

Remark 3.4 We will show in the next subsection that P_{ord} has ramification index exactly two over Λ.

Remark 3.5 Let R denote any commutative ring, and $I \subset R$ any prime ideal. We will often encounter the situation that I, while not principal as an ideal of R, becomes principal in the localization R_I of R at I. In this case, we shall say that I is locally principal. It is clear in this case that I has height at most 1. If I has height 1, then R_I is a discrete valuation ring. This was already used above.

We now give a necessary condition for Conjecture 1.1 to hold, in terms of the Zariski tangent spaces at the closed points $\mathfrak{m}$ and $\mathfrak{m}_+$ of the rings R^{ord} and R_+^{ord} respectively. Indeed, writing k for the residue field of $\mathcal{O}$, it is known that

$$\mathrm{Sel}(\mathbb{Q}, \mathrm{Ad}(\overline{\rho})) = \mathrm{Hom}\left(\mathfrak{m}/(p, \mathfrak{m}^2), k\right),$$

where

$$\mathrm{Sel}(\mathbb{Q}, \mathrm{Ad}(\overline{\rho})) \subset H^1(F_p/\mathbb{Q}, \mathrm{Ad}(\overline{\rho}))$$

consists of the cocycles that lie in the kernel of the natural morphism to $H^1(I_{\mathfrak{p}}, \mathrm{Ad}(\overline{\rho})/V_p^{\mathrm{ord}})$. Here V_p^{ord} denotes the k-space of matrices $\left(\begin{smallmatrix} * & 0 \\ 0 & 0 \end{smallmatrix}\right)$. There is a natural map $\mathfrak{m}_+ \to \mathfrak{m}$, and this induces a map $\mathfrak{m}_+ \to \mathfrak{m}/(p, \mathfrak{m}^2)$. Furthermore, there is an induced action of the involution τ on the k-vector space $\mathfrak{m}/(p, \mathfrak{m}^2)$, and it is clear that the image of $\mathfrak{m}_+$ is contained in the subspace of invariants under τ. We can compute the action of τ precisely, using the identification $H^1(\mathrm{Gal}\,(F_p/\mathbb{Q}), \mathrm{Ad}(\overline{\rho})) = \mathrm{Hom}\left(\mathfrak{m}/(p, \mathfrak{m}^2), k\right)$. In view of the lemma of Doi, Hida and Ishii already cited, the k-dimension of the fixed space of τ is given by the k-dimension of the maximal subspace of $\mathfrak{m}/(p, \mathfrak{m}^2)$ on which Galois acts via an induced representation. One sees easily that this dimension is given by the p-rank of the ideal class-group $H_{\mathfrak{p}}$. We

remind the reader that $H_{\mathfrak{p}} = \mathrm{Gal}\,(N/F)$, where N/F is the maximal pro-p-abelian extension of F that is unramified outside $\mathfrak{p}$.

On the other hand, we can compute the dimension of the Selmer group precisely, using the analogue of (4). Letting N' denote the maximal abelian pro-p-extension of $F(\overline{\varphi}/\overline{\varphi}^{\sigma})$ that is unramified away from $\mathfrak{p}$, we find that

$$\dim_k(\mathrm{Sel}(\mathbb{Q}, \mathrm{Ad}(\overline{\rho}))) = \dim_k(H_{\mathfrak{p}}) \otimes k + \dim_k(\mathrm{Hom}\,(\mathrm{Gal}\,(N'/F(\overline{\varphi}/\overline{\varphi}^{\sigma})), k))^{\overline{\varphi}/\overline{\varphi}^{\sigma}}.$$

Thus the image of $\mathfrak{m}_+$ has cokernel of dimension at least equal to the p-rank of the group $\mathrm{Gal}\,(N'/F(\overline{\varphi}/\overline{\varphi}^{\sigma}))^{\varphi/\varphi^{\sigma}}$. On the other hand, it is clear that R^{ord} is of the form $R_+^{ord}[x]$ if and only if the image of $\mathfrak{m}_+$ has codimension ≤ 1. It follows that Conjecture 1.1 cannot hold if $\mathrm{Gal}\,(N'/F(\overline{\varphi}/\overline{\varphi}^{\sigma}))^{\overline{\varphi}/\overline{\varphi}^{\sigma}}$ has k-dimension greater than 1. We summarize this observation in the following

Proposition 3.6 *Conjecture 1.1 cannot hold if* $\mathrm{Gal}\,(N/F(\overline{\varphi}/\overline{\varphi}^{\sigma}))^{\overline{\varphi}/\overline{\varphi}^{\sigma}}$ *has k-dimension greater than 1. In particular, Conjecture 1.1 cannot hold if the $\overline{\varphi}/\overline{\varphi}^{\sigma}$-part of the p-Sylow subgroup of the ideal class group of $F(\overline{\varphi}/\overline{\varphi}^{\sigma})$ is not cyclic.*

Finally, we record a consequence of Theorem 3.1 that will be useful in our analysis of pseudo-deformations in the next section.

Corollary 3.7 *Let $h \to \begin{pmatrix} a(h) & b(h) \\ c(h) & d(h) \end{pmatrix} \in GL_2(R^{ord})$ be a realization of the universal deformation by matrices. There exist elements g, h of $\mathrm{Gal}\,(F_p/F)$ such that each of $b(g)$ and $c(h)$ has order 1 at the discrete valuation associated to P_{ord}.*

Proof. This follows directly from the explicit description of the K-space $P_{ord}/(T, P_{ord}^2)$ in terms of the Selmer group $\mathrm{Sel}(\mathbb{Q}, \mathrm{Ad}(\rho)) = \mathrm{Sel}(\mathbb{Q}, 1 \oplus \chi_F) \oplus \mathrm{Sel}(\mathbb{Q}, \mathrm{Ind}_{\mathbb{Q}}^F(\frac{\xi}{\xi^{\sigma}}))$. Indeed, we showed that the group $\mathrm{Sel}(\mathbb{Q}, \mathrm{Ind}_{\mathbb{Q}}^F(\varphi/\varphi^{\sigma}))$ has $\mathcal{O}$-corank 1. Since the representation $\mathrm{Ind}_{\mathbb{Q}}^F(\varphi/\varphi^{\sigma})$ is concentrated on the off-diagonal elements in (5), and $\mathrm{Ind}_{\mathbb{Q}}^F(\varphi/\varphi^{\sigma})$ is irreducible, the assertion of the lemma is immediate.

Pseudo-deformations

In this section we will prove that the ideal $P_{ord}^+ = P_{ord} \cap R_+^{ord}$ is unramified over Λ. We apply this result to prove Theorem B of the introduction. The key idea is to relate R_+^{ord} to a certain pseudo-deformation ring.

Recall therefore (see [Wil88], pp 563-564 for details) that a pseudo-representation ρ of a group H into a ring $(A, \mathfrak{m}) \in \mathrm{CNL}_{\mathcal{O}}$ consists of functions $a, d : H \to A$ and a function $x : H \times H \to \mathfrak{m}_A$ satisfying the following rules:

1. $a(\sigma\tau) = a(\sigma)a(\tau) + x(\sigma, \tau),$

2. $d(\sigma\tau) = d(\sigma)d(\tau) + x(\tau, \sigma)$

3. $x(\sigma, \tau)x(\alpha, \beta) = x(\sigma, \beta)x(\alpha, \tau),$

4. $x(\sigma\tau, \alpha\beta) = a(\sigma)a(\beta)x(\tau, \alpha) + a(\beta)d(\tau)x(\sigma, \alpha) + a(\sigma)d(\alpha)x(\tau, \beta) + d(\tau)d(\alpha)x(\sigma, \beta),$

5. $a(1) = d(1) = 1$, and

6. $x(\sigma, g) = x(g, \sigma) = 0$ if $g = 1$, or g is some fixed choice c of complex conjugation.

The *trace* and *determinant* of ρ are the functions $\mathrm{Tr}\,(\rho)(\sigma) = a(\sigma) + d(\sigma)$, and $\det(\rho)(\sigma) = a(\sigma)d(\sigma) - x(\sigma, \sigma)$. Now let $\rho : G \to GL_2(A)$ be a representation. Suppose that $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then, writing $\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$, the functions $a(\sigma), d(\sigma)$ and $x(\sigma, \tau) = b(\sigma)c(\tau)$ define a pseudo-representation. The trace and determinant of this pseudo-representation coincide with the usual trace and determinant of ρ.

Now let $\overline{\rho}^{ps}$ denote the k-valued pseudo-representation of $H = \mathrm{Gal}\,(F_p/F)$ corresponding to the representation $\begin{pmatrix} \overline{\varphi} & 0 \\ 0 & \overline{\varphi}^\sigma \end{pmatrix}$. Then a *pseudo-deformation* of $\overline{\rho}^{ps}$ is a pair $(A, \tilde{\rho})$ consisting of a complete Noetherian local $\mathcal{O}$-algebra A with residue field k, and a pseudo-representation $\tilde{\rho}$ of H into A such that $\rho \equiv \overline{\rho}^{ps} \pmod{\mathfrak{m}_A}$. Equivalently, we require that $a \equiv \overline{\varphi} \pmod{\mathfrak{m}_A}$, and $d \equiv \overline{\varphi}^\sigma \pmod{\mathfrak{m}_A}$. For more on pseudo-representations we refer the reader to [Wil88] and [Hid93]. Meanwhile, the work [SW99] is the definitive reference for pseudo-deformations.

Recall our assumption that $\mathrm{Ind}_{\mathbb{Q}}^F(\varphi)$ was an ordinary representation. Specifically, we assumed that $p = \mathfrak{p}\mathfrak{p}^\sigma$ in F, and that the restriction of $\mathrm{Ind}_{\mathbb{Q}}^F(\varphi)$ to a given decomposition group D_p at p was upper-triangular, with a one-dimensional unramified quotient. As before, we will write $\mathfrak{p}$ for the prime of F singled out by this choice of D_p. With these notations, we will say that a pseudo-deformation $\tilde{\rho} = (A, \tilde{\rho})$ is *ordinary* at the prime $\mathfrak{p}|p$ if $x(h', h) = 0$ for $h \in D_\mathfrak{p}$, and $d(h) = 1$ if $h \in I_\mathfrak{p}$.

Consider now the functor that assigns to an $A \in \mathrm{CNL}_\mathcal{O}$ the set of ordinary pseudo-deformations $(A, \tilde{\rho})$ of $\overline{\rho}^{ps}$ to A satisfying the further condition that

$$\mathrm{Tr}\,(\tilde{\rho}(h)) = \mathrm{Tr}\,(\tilde{\rho}(h^\sigma)) \tag{10}$$

for $h \in \mathrm{Gal}\,(F_p/F)$. Here h^σ denotes the image of h under conjugation by any element of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ which induces the nontrivial automorphism of $F/\mathbb{Q}$. It is straightforward to check, using Schlesinger's criteria, that this functor is representable. Write R^{ps} and ρ^{ps} for the universal pseudo-deformation ring and universal pseudo-deformation respectively. Note that there is a natural morphism $\Lambda \to R^{ps}$, induced by the determinant.

Lemma 3.8 *The pseudo-deformation ring R^{ps} is topologically generated over Λ by elements of the form $\mathrm{Tr}\,(\rho^{ps}(h))$, for $h \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$. The pseudo-deformation ρ^{ps} satisfies the following additional properties:*

- $x(h, h') = 0$ for h in $D_{\mathfrak{p}^\sigma}$, and

- $a(h) = 1$ for $h \in I_{\mathfrak{p}^\sigma}$.

Proof. The first statement is well-known (see, for instance, [Wil88], page 564). The rest of the lemma is a consequence of the fact that $D_{\mathfrak{p}}$ (resp. $I_{\mathfrak{p}}$) and $D_{\mathfrak{p}^\sigma}$ (resp. $I_{\mathfrak{p}^\sigma}$) are interchanged by the action of $\mathrm{Gal}\,(F/\mathbb{Q})$, and that the functions a and d are multiplicative on $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$. The details are left to the reader.

To proceed further, observe that the universal deformation $\varrho : \mathrm{Gal}\,(F_p/\mathbb{Q}) \to GL_2(R^{ord})$ of $\overline{\rho}$ gives rise to an ordinary pseudo-deformation ρ_+ of $\overline{\rho}$, with invariant traces as above. Furthermore, it is clear that this ρ_+ actually takes values in the smaller ring R^{ord}_+. It is the relationship between ρ_+ and the universal pseudo-deformation that is the focus of this section.

First we study the local properties of of R^{ord}_+ and R^{ps} in the neighbourhood of a point corresponding to a dihedral representation. Thus fix a representation $\rho' = \mathrm{Ind}^F_{\mathbb{Q}}(\xi)$ as in the previous subsection, and let P_{ord} denote the corresponding prime ideal of R^{ord}. We will write P^+_{ord} for the ideal $P_{ord} \cap R^{ord}_+$ of R^{ord}_+. As always, we will let K denote the fraction field of $\mathcal{O}$.

Lemma 3.9 *The localization of R^{ord}_+ at the ideal P^+_{ord} is a discrete valuation ring. The image of ρ_+ in $R^{ord}_+/(P^+_{ord})^2 \otimes K \cong K[\epsilon]/\epsilon^2$ is nontrivial (i.e, not equal to the K-valued pseudorepresentation ρ').*

Proof. Consider the localization S of R^{ord}_+ at P^+_{ord}, and the corresponding localization $S \otimes R^{ord}$ of R^{ord}. Since P_{ord} is the unique prime of R^{ord} over P^+_{ord}, we see that $S \otimes R^{ord}$ is a local ring, so that $S \otimes R^{ord}$ coincides with the localization of R^{ord} at P_{ord}. We know already that the localization of R^{ord} at the prime P_{ord} is a discrete valuation ring. In particular, $S \otimes R^{ord}$ is an integrally closed domain. It follows that S is also an integral domain. Now let x be any element of the fraction field of S, such that x is integral over S. Then x is integral over $S \otimes R^{ord}$, and we get $x \in S \otimes R^{ord}$. Write $x = r/s$, where $r \in R^{ord}$ and $s \in R^{ord}_+$ lies in the complement of P^+_{ord}. Since x is in the fraction field of S, we find that x is fixed by τ. But the denominator s lies in R^{ord}_+, and so is fixed by τ as well. A simple argument shows that we may take $r \in R^{ord}_+$, and that S is integrally closed. Thus S must be a discrete valuation ring.

To verify that pseudo-deformation into $R^{ord}_+/(P^+_{ord})^2 \otimes K$ is nontrivial, we will use the explicit description coming from Lemma 3.7. Writing a, d, x for the coefficients of the pseudo-deformation into R^{ord}_+, we know that there is a factorization $x(g, h) = b(g) \cdot c(h)$, for functions b, c with values in the larger ring R^{ord}. As we have already remarked, there exist g, h such that the elements $b(g)$ and $c(h)$ have order one at discrete valuation associated to the ideal P_{ord}. Since P_{ord} is ramified over P^+_{ord} with ramification index two, it follows from this that there is a pair (g, h) such that the element $x(g, h) = b(g) \cdot c(h)$ has order one at P^+_{ord}. The lemma is now immediate, since such an element $x(g, h)$ is nonzero in $P^+_{ord}/(P^+_{ord})^2 \otimes K$.

Now let P_{ps} denote the prime ideal of R^{ps} associated to the pseudo-deformation coming from the $\mathcal{O}$-valued representation $\rho' = \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi)$. The following result is the first theorem of this section; it leads to a complete description of the local structure of the ring R^{ord} in a neighborhood of the point P_{ord}.

Theorem 3.10 *The localization of R^{ps} at the prime ideal P_{ps} is a discrete valuation ring. The ideal P_{ps} is unramified over the corresponding prime of Λ.*

Proof. We begin with the first statement. For this it suffices to show that P_{ps} is locally principal. Note that by the universal property of R^{ps}, there is a natural morphism

$$\alpha : R^{ps} \to R_{+}^{ord}$$

such that $P_{\mathrm{ps}} = \alpha^{-1}(P_{ord}^{+})$. Let $I = \ker(\alpha)$. Then $I \subset P_{\mathrm{ps}}$, and we will show first that $\alpha(P_{\mathrm{ps}}) = P_{\mathrm{ps}}/I$ is locally principal in R^{ps}/I. To see this, observe that there is a well defined function

$$v : P_{\mathrm{ps}} :\to \mathbb{Z} \cup \infty$$

defined by $v(x) = \mathrm{val}(\alpha(x))$, where "val" is the discrete valuation defined by P_{ord}^{+}. To prove that P_{ps} is principal modulo I, it suffices to show that there exists an $x \in P_{\mathrm{ps}}$ such that $v(x) = 1$. Indeed, since R^{ps} and R_{+}^{ord} have the same residue ring $\mathcal{O}$ at P_{ps} and P_{ord}^{+}, it will then follow that the map $\alpha(R^{ps}) \hookrightarrow R_{+}^{ord}$ induces an isomorphism on completing at P_{ps}/I and P_{ord}^{+}.

Now suppose on the other hand that every $x \in P_{\mathrm{ps}}$ satisfies $v(x) \geq 2$. Then we get

$$\alpha(P_{\mathrm{ps}}) \subset (P_{ord}^{+})^{2}, \tag{11}$$

at least upon localization at P_{ord}^{+}. Writing K for the fraction field of $\mathcal{O}$, we have seen above that $M_{+} = P_{ord}^{+}/(P_{ord}^{+})^{2} \otimes K$ is a 1-dimensional K-space, and since R^{ps} is generated by the traces of the universal pseudo-deformation, it follows from (11) that the natural pseudo-deformation of ρ' into

$$(R_{+}^{ord}/{P_{ord}^{+}}^{2}) \otimes K$$

is constant. But this contradicts the conclusion of Lemma 3.9.

We have therefore proven that P_{ps} is locally principal modulo I. To complete the proof that P_{ps} is locally principal, we simply observe that I is contained in the nilradical of R^{ps}. Indeed, given an arbitrary prime ideal Q of R^{ps}, with residue ring T, we can find a genuine representation $\check{\rho}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ with values in the fraction field of T which induces the pseudo-deformation ρ^{ps} (mod Q) (see [Wil88], pp. 564-565). If $\check{\rho}$ is reducible, there may be several such representations, so we make a choice by specifying that $\check{\rho}$ be the unique semisimple representation with the given traces.

Now, since the trace of ρ^{ps} is invariant under the action of $\mathrm{Gal}(F/\mathbb{Q})$, we see that there exists an extension of $\check{\rho}$ to a representation $\check{\rho}'$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, defined over some extension

T' of T. The extension may not be unique, but that will not be relevant here. We need only to observe that $\check{\rho}'$ is ordinary (since ρ^{ps} is so) and that $\check{\rho}'$ is a deformation of $\overline{\rho}$. To verify this latter point, one can simply observe that the traces of $\check{\rho}'$ agree with those of $\overline{\rho}^{ps}$ on $\mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$, so that the reduction of $\check{\rho}'$ modulo the maximal ideal of T' coincides with $\overline{\varphi} \oplus \overline{\varphi}^{\sigma}$ up to semisimplification. Since $\check{\rho}'$ extends to a representation of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, and $\overline{\varphi}$ and $\overline{\varphi}^{\sigma}$ are interchanged by $\mathrm{Gal}\,(F/\mathbb{Q})$, we see that the reduction of $\check{\rho}'$ must equal to $\overline{\varphi} \oplus \overline{\varphi}^{\sigma}$ on $\mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$. But $\overline{\rho}$ is the unique extension of $\overline{\varphi} \oplus \overline{\varphi}^{\sigma}$ to a representation of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$.

By the universal property of R^{ord}, there is a homomorphism $R^{ord} \to T'$ inducing $\check{\rho}'$. Unwinding the definitions, one finds that the map $R^{ps} \to R^{ps}/Q = T \to T'$ may be factored as

$$R^{ps} \xrightarrow{\alpha} R^{ord}_+ \to R^{ord} \to T'.$$

Since $Q = \ker\left\{R^{ps} \to T\right\} = \ker\left\{R^{ps} \to T'\right\}$, it follows from this that there must exist a prime ideal of R^{ord}, and hence of R^{ord}_+, lying over Q. Let Q_+ denote a prime ideal of R^{ord}_+ such that $\alpha^{-1}(Q_+) = Q$. Since $I = \alpha^{-1}(0) \subset \alpha^{-1}(Q_+) = Q$, it follows that I is contained in every prime ideal Q of R^{ps}, and hence lies in the nilradical of R^{ps}. We may now conclude, by Nakayama's Lemma, that P_{ps} is locally principal. Since the localization of R^{ps} at P_{ps} has Krull dimension at least one, it must be a discrete valuation ring. This completes the proof of the first statement in the theorem.

We have now to prove that P_{ps} is unramified over Λ. To achieve this, it suffices to show that the $\mathcal{O}$-module $P_{\mathrm{ps}}/(T_{\zeta}, P_{\mathrm{ps}}^2)$ is finite. Here $T_{\zeta} = T - (\zeta - 1)$, for $\zeta \in \mu_{p^{\infty}}$, is such that the weight one prime ideal $P_{ord} \cap \Lambda$ is generated by T_{ζ}. Equivalently, if we write K for the fraction field of $\mathcal{O}$, then it suffices to show that $M = P_{\mathrm{ps}}/(T_{\zeta}, P_{\mathrm{ps}}^2) \otimes K = 0$. We will prove the latter statement by contradiction. Indeed, if it were false, then there would exist a nonconstant deformation $\tilde{\rho}^{\mathrm{ps}}$ of ρ' into the ring of dual numbers $K[\epsilon]/\epsilon^2$, such that $\tilde{\rho}^{\mathrm{ps}} = \rho'$ (mod ϵ). Furthermore, since $T_{\zeta} \mapsto 0$ in M, we see that $\det(\tilde{\rho}^{\mathrm{ps}}) = \det(\rho')$.

Write $\tilde{a}, \tilde{d}$, and $\tilde{x}$ for the coefficients a, d and x of the pseudo-representation $\tilde{\rho}^{\mathrm{ps}}$. It follows from the fact that $\tilde{\rho}^{\mathrm{ps}}$ is ordinary that the function $\tilde{x}$ is trivial on $I_{\mathfrak{p}} \times I_{\mathfrak{p}}$, and also on $I_{\mathfrak{p}^{\sigma}} \times I_{\mathfrak{p}^{\sigma}}$. Thus the functions $\tilde{a}$ and $\tilde{d}$ define multiplicative characters $I_{\mathfrak{p}^{\sigma}}, I_{\mathfrak{p}} \to \mathcal{O}^{\times}$. Since $\det(\tilde{\rho}^{\mathrm{ps}}) = \det(\rho')$, and one of the functions $\tilde{a}$ or $\tilde{d}$ is unramified, we may conclude that the pseudo-deformation $\tilde{\rho}^{\mathrm{ps}}$ is constant on the inertia groups $I_{\mathfrak{p}}$ and $I_{\mathfrak{p}^{\sigma}}$.

Now let F' denote the splitting field of the representation $\rho' = \mathrm{Ind}_{\mathbb{Q}}^{F}(\xi)$, and let $H' = \mathrm{Gal}\,(\overline{\mathbb{Q}}/F')$. It follows from the defining properties of a pseudo-deformation that the function $\tilde{x}$ defines a bilinear homomorphism

$$H' \times H' \to K.$$

Furthermore, it follows from the fact that $\tilde{\rho}^{\mathrm{ps}}$ is nonconstant that the homomorphism defined by $\tilde{x}$ is nonzero (see the proof of Lemma 3.9). Now let F'_{∞} denote the maximal abelian pro-p-extension of F' that is unramified away from primes lying over p, and let

$H'_\infty = \mathrm{Gal}\,(\overline{\mathbb{Q}}/F'_\infty)$. It is clear that the function $\tilde{x}$ is trivial on $H'_\infty \times H'_\infty$. Thus there are characters

$$\varphi', \psi' : H'_\infty \to K[\epsilon]/\epsilon^2$$

such that the pseudo-representation defined by $\tilde{\rho}^{\mathrm{ps}}$ coincides with that defined by $\varphi' \oplus \psi'$. By relabeling, if necessary, we may assume that $\tilde{a} = \varphi'$ and $\tilde{d} = \psi'$ on H'_∞.

Now let $g \in I_{\mathfrak{p}^\sigma}$ and $h \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/F'_\infty)$. Then we can compute

$$\tilde{a}(ghg^{-1}) = \tilde{a}(g)\tilde{a}(hg^{-1}) + \tilde{x}(g, hg^{-1}) = \tilde{a}(g)\tilde{a}(hg^{-1}) = \tilde{a}(g)(\tilde{a}(h)\tilde{a}(g^{-1}) + \tilde{x}(h, g^{-1}))$$
$$= \tilde{a}(g)\tilde{a}(h)\tilde{a}(g^{-1}), \quad (12)$$

where we have used the fact that $\tilde{x}(g, *) = 0$ for $g \in I_{\mathfrak{p}^\sigma}$ (ordinariness) and that $\tilde{x}(h, g^{-1}) = 0$ (the functional $\tilde{x}(*, g^{-1})$ kills $\mathrm{Gal}\,(\overline{\mathbb{Q}}/F'_\infty)$ by definition). Finally, since our deformation is constant on inertia groups, we find that $\tilde{a}(g^{-1}) = \tilde{a}(g)^{-1}$, so that $a(ghg^{-1}) = \tilde{a}(h)$, for $g \in I_{\mathfrak{p}}$ and $h \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/F'_\infty)$. A very similar computation shows that $a(ghg^{-1}) = a(h)$, for $g \in I_{\mathfrak{p}}$ and $h \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/F'_\infty)$. One can also make analogous computations upon replacing the function $\tilde{a}$ by $\tilde{d}$.

Let F'' denote the maximal everywhere unramified subextension of N_∞/F'. Then F'' is finite over F'. Observe now that $\mathrm{Gal}\,(N_\infty/F'')$ is abelian, and can be expressed as the surjective image of a product of inertia groups. We may conclude from the considerations above that $\mathrm{Gal}\,(F'_\infty/F'')$ acts trivially on the characters $\varphi' = \tilde{a}$ and $\psi' = \tilde{d}$ of H'_∞. Thus if N_∞ denotes the splitting field (over H'_∞) of $\varphi' \oplus \psi'$, then it follows that N_∞ is an *abelian* extension of F''. Furthermore, one verifies directly that the restriction of $\tilde{\rho}^{\mathrm{ps}}$ to $\mathrm{Gal}\,(F_p/F'')$ actually factors through the abelian quotient $\mathrm{Gal}\,(N_\infty/F'')$, in the sense that the coefficient functions are well-defined on this quotient. Then one checks that the function $\tilde{x}(g, h)$ is symmetric in g and h (by abelianness: $a(gh) = a(hg)$ and $d(gh) = d(gh)$.) Since $\tilde{\rho}^{\mathrm{ps}}$ is ordinary, it follows that x vanishes identically on $\mathrm{Gal}\,(N_\infty/F'')$. Finally, since our pseudo-deformation is constant on inertia groups, we see that it must become constant upon base-change to the finite extension F''. This contradicts the fact that $\tilde{x}$ defines a nonzero bilinear map $H' \times H' \to K$, and completes the proof of the theorem.

We can now prove Theorem B of the introduction. Before commencing the proof, we remark that we have followed the conventions given in [DHI98] for normalizing the Hecke operators and Frobenius elements. Of course, this choice of convention does not affect the argument. With this in mind, our Theorem B follows directly from the following

Theorem 3.11 *Let $\alpha(R^{ps}) \subset R_+^{ord}$ denote the image of R^{ps} under the natural morphism. Then*

- $\alpha(R^{ps})$ *coincides with the closed subring of R_+^{ord} topologically generated over Λ by the trace elements* $\mathrm{Tr}\,(\rho^{ps}(h))$, *for $h \in (\mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$;*

- *The ring $\alpha(R^{ps})$ is in the image of the Hecke ring h_F of Hilbert modular forms over F under the base change map β, and*

- *The ring $\alpha(R^{ps})$ has finite index in R^{ord}_+.*

Proof. The first assertion is immediate, as R^{ps} is topologically generated over Λ by the trace elements indicated (see Lemma 3.8). As for the second, we note simply that the ring h_F is generated over Λ by Hecke operators $T_{\mathfrak{q}}$, for all $\mathfrak{q}$. By the Tchebotarev density theorem, and the first assertion already proven, we find that R^{ps} is topologically generated by elements $\mathrm{Tr}\,(\rho^{\mathrm{ps}}(\mathrm{Frob}(\mathfrak{q})))$, for $\mathfrak{q} \nmid Dp$. On the other hand, we know that $\mathrm{Tr}\,(\varrho(\mathrm{Frob}(\mathfrak{q})))$ is the image of $\beta(T_{\mathfrak{q}})$ under the base change map. Thus, $\alpha(R^{ps})$ coincides with the subring topologically generated over Λ by the elements $\beta(T_{\mathfrak{q}})$, which is contained in $\beta(h_F)$.

To verify the remaining assertion, let Q_+ denote a prime ideal of R^{ord}_+, and let Q denote the corresponding prime of $S = \alpha(R^{ps})$. Then we shall show that the map of $\mathrm{Spec}(R^{ord}_+) \to \mathrm{Spec}(R^{ps})$ is unramified at Q_+. More precisely, we will show that the map of completions

$$S_Q \to (R^{ord}_+)_{Q_+} \tag{13}$$

is an isomorphism. To achieve this, select a prime ideal Q_{ord} of R^{ord} lying over Q_+, and let ρ_Q denote the specialization of the universal deformation ρ^{ord} to Q_{ord}. We will first consider the case where ρ_Q is *irreducible* on the subgroup $\mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$. Now consider the fibre ring

$$T = R^{ord} \otimes S_Q/Q.$$

Then there is a natural deformation ρ_T of ρ into T, obtained by reducing the universal deformation. By definition of T, we have $\mathrm{Tr}\,(\rho_T(h)) = \mathrm{Tr}\,(\rho_Q(h))$, for $h \in H = \mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$. Since ρ_Q is assumed irreducible on H, it we may argue as in [Maz89], Proposition 4, to conclude that the deformation ρ_T is constant on H. It follows easily from this that ρ_T is constant, equal to ρ_Q, on $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$. This implies then that the morphism $\mathrm{Spec}(R^{ord}) \to \mathrm{Spec}(S)$ is unramified at Q_{ord}.

On the other hand, since R^{ord}_+ is the fixed subring of an involution τ, it is clear that the map $\mathrm{Spec}(R^{ord}) \to \mathrm{Spec}(R^{ord}_+)$ is unramified away from the fixed points of τ. But a prime ideal of R^{ord} is fixed by τ if and only if the corresponding representation is dihedral, and reducible on the subgroup H. Since our ρ_Q was assumed irreducible on H, it follows that $\mathrm{Spec}(R^{ord}) \to \mathrm{Spec}(R^{ord}_+)$ is unramified at Q. This implies that $\mathrm{Spec}(R^{ord}_+) \to \mathrm{Spec}(S)$ is unramified at Q_+. Since it is obvious that R^{ord}_+ and S have the same residue ring, we obtain (13) when ρ_Q is irreducible on H.

To treat the case of a prime Q where ρ_Q is dihedral, we note that such primes can be described exactly. Namely, such a prime ideal is either maximal, or has residue characteristic zero, and is such that $\rho_Q = \mathrm{Ind}_{\mathbb{Q}}^F(\varphi\xi)$, for some unramified character ψ of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/F)$ of p-power order. To obtain (13) in this latter case, we can use Theorem 3.1. Indeed, we have

shown that $R^{ps}_{P_{\mathrm{ps}}}$ and $(R^{ord}_+)_{P^+_{ord}}$ are both discrete valuation rings, and in the course of proving Theorem 3.10, we checked that there existed an element $x \in R^{ps}$ such that $\alpha(x)$ had valuation 1 at P^+_{ord}. This proves the map (13) is unramified at P^+_{ord}.

To summarize, we have shown that the map (13) is an isomorphism for any nonmaximal prime ideal Q_+ of R^{ord}_+. It follows now that $\alpha(R^{ps})$ has finite index in R^{ord}_+, since the cokernel is supported at the the closed point.

Corollary 3.12 *The prime ideals P_{ord} of R^{ord} and P^+_{ord} of R^{ord}_+ are both locally principal. The ideal P^+_{ord} is unramified over Λ, and P_{ord} is ramified over P^+_{ord} with ramification index two.*

Proof. This follows from Lemma 3.9, Theorem 3.1, Theorem 3.10, and the isomorphism (13).

References

[DHI98] K. Doi, H. Hida, and H. Ishii, *Discriminants of Hecke fields and the twisted adjoint L-values for GL(2)*, Inv. Math (1998).

[Hid85] H. Hida, *Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85** (1985), 545–613.

[Hid93] H. Hida, *Elementary theory of p-adic L-functions and Eisenstein series*, Cambridge University Press, 1993.

[Hid98] H. Hida, *Global quadratic units and Hecke algebras*, Documenta Math. **3** (1998), 273–285.

[Mat90] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1990.

[Maz89] B. Mazur, *Deforming galois representations*, Galois groups over **Q** (Y. Ihara, ed.), MSRI Publications, 1989, pp. 385–437.

[SW97] C. Skinner and A. Wiles, *Ordinary forms and Galois representations*, Proc. Nat. Acad. Sci **94** (1997), 10520–10527.

[SW99] C. Skinner and A. Wiles, *Deforming reducible Galois representations*, preprint.

[TW95] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math **142** (1995), 265–280.

[Wil88] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

[Wil95]   A. Wiles, *Modular elliptic curves and Fermat's last theorem.*, Ann. Math. **141** (1995), 443–551.