Canad. J. Math. Vol. **63** (2), 2011 pp. 277–297
doi:10.4153/CJM-2010-084-3

Locally Indecomposable Galois Representations

Eknath Ghate and Vinayak Vatsal

Abstract. In a previous paper the authors showed that, under some technical conditions, the local Galois representations attached to the members of a non-CM family of ordinary cusp forms are indecomposable for all except possibly finitely many members of the family. In this paper we use deformation theoretic methods to give examples of non-CM families for which every classical member of weight at least two has a locally indecomposable Galois representation.

1 Introduction

Let ρ_f be the global two dimensional p-adic Galois representation attached to a p-ordinary cuspidal eigenform f of weight at least two. The local representation obtained by restricting ρ_f to the decomposition subgroup at p is reducible. A natural question is whether this representation is semi-simple. If f has complex multiplication, this is known to be the case. The non-CM case is much more mysterious. For weight two forms corresponding to rational elliptic curves without CM, the local representation is not semi-simple or is indecomposable [Ser89]. In this paper we shall give the first non-trivial explicit examples of non-CM forms of weight larger than two for which ρ_f is locally indecomposable.

To achieve this it is convenient to work in a broader context. Recall that every classical p-ordinary form f of weight at least two lives in a unique family of p-ordinary forms in the sense of [Hid86]. Such an f is referred to as an arithmetic member of the family to distinguish it from the non-classical p-adic members of the family, as well as from the classical members of weight one. It is well known that the arithmetic members of a family either all have CM or are all of non-CM type. In an earlier paper [GV04], the authors showed that in the non-CM case all but finitely many of the arithmetic members have an indecomposable local representation. (This result was proved under some technical conditions: p is odd, and the residual representation is p-distinguished and absolutely irreducible when restricted to $\mathbb{Q}(\sqrt{p^*})$ with $p^* = (-1)^{(p-1)/2} \cdot p$). However, the possibility that there might be a finite number of arithmetic members of the family, including possibly f, for which the local representation is semi-simple remained. Indeed, it turns out that deciding whether the local representation is indecomposable for a particular form f can be a rather delicate matter.

Received by the editors August 5, 2008.
Published electronically December 29, 2010.
AMS subject classification: **11F80**.

In this paper we will show that for the first few cusp forms f of level one, *every* arithmetic member of the corresponding p-adic family, including f, has an indecomposable local representation for all, except possibly one or two, small ordinary primes p. More precisely, let Δ_k be the unique normalized cusp form of level 1 and weight $k \in \{12, 16, 18, 20, 22, 26\}$. We shall say that an ordinary prime p is a full companion prime for f if the image of the corresponding residual representation contains SL_2, and the associated local residual representation is semi-simple. Then we prove the following.

Theorem 1.1 *Let $f = \Delta_k$ be as above and let p be an ordinary prime for f. Assume that p is not a full companion prime for f. Then every member of the p-adic family attached to f has an indecomposable local Galois representation.*

Each of the six cusp forms above has only at most one or two ordinary primes $p < 10,000$ that are full companion primes. Thus the theorem gives rise to several explicit examples of locally indecomposable modular Galois representations (for which see the main text). These examples may be regarded as further evidence towards the general tendency of ordinary modular Galois representations to be locally semi-simple exactly when the underlying form has CM. For illustrative purposes we mention one example here. For the Ramanujan Delta function $\Delta = \Delta_{12}$, there are no full companion primes in the above range and we obtain the following.

Corollary 1.2 *The local Galois representation attached to ρ_Δ is indecomposable for every ordinary prime $p < 10,000$.*

1.1 Sketch of the Proof

The proof of Theorem 1.1 is quite different from the methods used in [GV04]. There we studied the "large" Λ-adic representation attached to a family and showed that this representation is locally indecomposable exactly when the family is of non-CM type (under technical conditions similar to those mentioned above, see [GV04, Theorem 3]). The result for individual arithmetic members of the family then followed by a descent argument, which naturally introduced a finite error into the final result.

The present approach uses instead the deformation theoretic methods introduced by Mazur in his foundational paper [Maz89]. Briefly, the idea is as follows. Fix a cuspidal eigenform f of arbitrary level and weight $k \geq 2$. Let $\bar{\rho} = \bar{\rho}_f$ be the mod p residual representation attached to f, and assume it is absolutely irreducible. Let $R = R_{\bar{\rho}}$ be the universal deformation ring of $\bar{\rho}$. If $k > 2$, then Weston [Wes04] has shown that for all but finitely many primes p (in fact for all $p \geq k + 1$ for the six cusp forms above) the deformation problem attached to $\bar{\rho}$ is unobstructed (see also Yamagami [Yam04]), and so R is a power series ring in three variables over the Witt vectors of the residue field.

Now assume in addition that f is of level 1, and therefore not of CM type. Suppose also that p is ordinary for f so that the residual representation $\bar{\rho}$ is locally reducible. For most such p the representation $\bar{\rho}$ tends to be locally indecomposable. In such

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

cases there is nothing to prove, since if f is p-distinguished (automatic in level 1 if p is odd), then all characteristic 0 deformations of $\bar{\rho}$ are also locally indecomposable [Gha05, Proposition 6].

However, there are primes p for which $\bar{\rho}$ is locally semi-simple or split; the existence of such primes p is closely related to the existence of a mod p companion form for f in the sense of Serre, Gross [Gro90], Coleman, and Voloch. Assume then that $\bar{\rho}$ is locally split (and p-distinguished). Since f is a non-CM form, one still expects ρ_f to be locally indecomposable. To show this we consider instead all deformations of $\bar{\rho}$ that are ordinary and locally split. These are parametrized by a quotient of the universal deformation ring R, which we denote by R^{split}, and we are reduced to showing that this ring is "small". In particular if the reduced tangent space $t(R^{\text{split}})$ of R^{split} vanishes, then there is a paucity of characteristic 0 points of R^{split}. A case by case inspection of these points sometimes allows one to conclude that R^{split} has no arithmetic points (corresponding to classical cuspidal eigenforms of weight 2 or more), thereby achieving our goal.

The computation of $t(R^{\text{split}})$ is in general a delicate matter. It is related to an explicit problem in class field theory. Let S be the set consisting of the primes p and ∞, and let G_S be the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside S. If W_0 is the representation of G_S defined via the usual conjugation action of $\bar{\rho}$ on the two by two trace zero matrices over the residue field, then the first cohomology group $\mathrm{H}^1(G_S, W_0)$ is known to have dimension 2 in the cases of interest. Let K denote the inertia field in the finite Galois extension cut out by $\bar{\rho}$. It turns out that $t(R^{\text{split}}) = 0$ if certain $\mathbb{Z}/p$-extensions of K coming from certain classes in $\mathrm{H}^1(G_S, W_0)$ are linearly disjoint from the usual cyclotomic $\mathbb{Z}/p$-extension of K, after completion.

For the six cusp forms above, the primes for which $\bar{\rho}$ is locally semi-simple can be classified into three types depending on the image of the global residual representation $\bar{\rho}$ in $\mathrm{GL}_2(\mathbb{F}_p)$. Either this image is dihedral, or it is full (*i.e.,* it contains $\mathrm{SL}_2(\mathbb{F}_p)$), or it triangular (*i.e.,* the global representation is reducible).

In the (two) cases where the image of $\bar{\rho}$ is dihedral, we solve the class field theory problem mentioned above. In fact the argument simplifies somewhat, since it turns out one has to show that the cyclotomic $\mathbb{Z}/p$-extension of K is disjoint from only one of the $\mathbb{Z}/p$-extensions of K coming from $\mathrm{H}^1(G_S, W_0)$, after completion. The cases where $\bar{\rho}$ has full image are more difficult and are not treated completely in this paper. Even in the smallest example the number field K has degree about 10^6, making explicit arguments intractable. This explains the occasional primes in the range $p < 10{,}000$ that we presently exclude in Theorem 1.1. Finally, in the cases where the residual representation is reducible, an application of a result of Ribet [Rib76] shows directly that the local representation attached to ρ_f is indecomposable.

2 Galois Representations

We start by recalling the basic objects we shall be studying. Let f be a primitive elliptic modular cuspidal eigenform of level 1 and weight $k \geq 2$. We remind the reader that such a form f is necessarily not of CM type. Let p be a prime, and let $\wp$ be a prime of $\overline{\mathbb{Q}}$ lying over p that is ordinary for f. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let K be the number field generated by the Hecke eigenvalues of f. Let $\rho = \rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\wp)$ be the

$\wp$-adic representation attached to f by Eichler, Shimura, and Deligne.

2.1 Ordinary Representations

Let G_p be a decomposition subgroup at $\wp$. By a result of Mazur and Wiles [MW86] and Wiles [Wil88], the ordinariness assumption implies that the restriction of ρ to G_p is reducible. More concretely, it has the shape

$$\rho|_{G_p} \sim \begin{pmatrix} \delta & \nu \\ 0 & \epsilon \end{pmatrix},$$

where δ, $\epsilon\colon G_p \to K_\wp^\times$ are characters, with ϵ unramified. More explicitly, if $\lambda(\alpha)\colon G_p \to K_\wp^\times$ denotes the unramified character of G_p that maps the Frobenius at p to $\alpha \in K_\wp^\times$, then $\epsilon = \lambda(\alpha_p)$, where α_p is the unique p-adic unit root of $x^2 - a_p x + p^{k-1}$, with a_p the p-th Fourier coefficient of f. Thus $\delta = \lambda(\alpha_p)^{-1} \cdot \nu^{k-1}$, where $\nu\colon G_\mathbb{Q} \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character.

The function $\nu\colon G_p \to K_\wp$ is a continuous map. The goal of this paper is to give examples of forms f as above for which ν cannot be made zero even after a change of basis. Put another way, we would like to show that the class of the cocycle $c = \epsilon^{-1} \cdot \nu$ in $\mathrm{H}^1(G_p, K_\wp(\delta\epsilon^{-1}))$ is non-zero. To do this, we will frequently work over the inertia subgroup $I_p \subset G_p$ at $\wp$. This is because the local representation $\rho|_{G_p}$ splits if and only if the representation $\rho|_{I_p}$ splits. Indeed the restriction map

$$\mathrm{H}^1(G_p, K_\wp(\delta\epsilon^{-1})) \to \mathrm{H}^1(I_p, K_\wp(\delta\epsilon^{-1}))$$

is injective: its kernel is $\mathrm{H}^1(G_p/I_p, K_\wp(\delta\epsilon^{-1})^{I_p}) = 0$, since $\delta \neq \epsilon$ on I_p.

We need to recall some terminology. If the reductions $\bar{\delta}$ and $\bar{\epsilon}$ of δ and ϵ are distinct on G_p, one says that f (or more precisely the residual representation attached to f) is p-distinguished. This condition is automatic in our setting if p is an odd prime. Indeed let ω be the mod p cyclotomic character. Then $\bar{\delta}|_{I_p} = \omega^{k-1} \neq 1$, since k is even (f has level 1) and $\bar{\epsilon}|_{I_p} = 1$.

2.2 Residual Representation

Let $\mathbb{F}$ denote the residue field of the ring of integers of $K_\wp$, and let $\bar{\rho}\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F})$ be the residual representation attached to ρ. Its isomorphism class is only determined up to semi-simplification.

Even though ρ is expected not to be locally split, it is possible for the residual representation $\bar{\rho}$ to be locally split or semi-simple. It is this phenomenon that makes the question studied in this paper interesting. For the six cusp forms f above, the primes for which this happens are listed in the following table, according to the image of the global residual representation $\bar{\rho}$ in $\mathrm{GL}_2(\mathbb{F}_p)$.

f	Non ordinary primes ($< 10^6$)	Dihedral	Full ($< 10^4$)	Reducible
Δ	2, 3, 5, 7, 2411	23		2, 3, 5, 7, 691
Δ_{16}	2, 3, 5, 7, 11, 13, 59, 15271, 18744	31	397	2, 3, 5, 7, 11, 3617
Δ_{18}	2, 3, 5, 7, 11, 13		271	2, 3, 5, 7, 11, 13, 43867
Δ_{20}	2, 3, 5, 7, 11, 13, 17, 3371, 64709		139, 379	2, 3, 5, 7, 11, 13, 283, 617
Δ_{22}	2, 3, 5, 7, 13, 17, 19			2, 3, 5, 7, 13, 17, 131, 593
Δ_{26}	2, 3, 5, 7, 11, 13, 17, 19, 23		107	2, 3, 5, 7, 11, 17, 19, 657931

Table 1. Primes for which $\bar{\rho}$ is locally split

The third column contains all such primes for which the image of $\bar{\rho}$ is dihedral, and is taken from Serre [Ser73]. There are only two cases, and for both the image is isomorphic to S_3. The fourth column contains such primes $< 10,000$ for which the image of $\bar{\rho}$ is full, *i.e.,* contains $\mathrm{SL}_2(\mathbb{F}_p)$. That these are the only primes up to $3,500$ is mentioned at the end of Gross' paper [Gro90] on companion forms and is due to Atkin and Elkies. C. Citro has recently checked that these are the only such primes up to $10,000$. The last column contains such primes for which $\bar{\rho}$ is reducible, and is again taken from [Ser73]. Finally, the second column describes all the non-ordinary primes for f less than a million, as compiled by Gouvêa in [Gou97]. Note that only one or two of the "reducible" primes are ordinary.

3 Deformation Theory

3.1 Universal Locally Split Deformation Ring

This ring will play a key role in what follows. We establish its existence in this section using ideas introduced by Mazur in [Maz89]. See also [Oht06].

We work somewhat generally. Let p be a prime and let $\mathbb{F}$ be a finite field of characteristic p. Let $S = \{p, \infty\}$, and let G_S be the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside S. Let $\bar{\rho}\colon G_S \to \mathrm{GL}_2(\mathbb{F})$ be any Galois representation, such that

$$\bar{\rho}|_{I_p} \sim \begin{pmatrix} \bar{\delta} & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.1}$$

where $\bar{\delta}\colon I_p \to \mathbb{F}^\times$ is a character with $\bar{\delta} \neq 1$. In particular the representation $\bar{\rho}$ is p-distinguished.

Let $\mathcal{O} = W(\mathbb{F})$. Let $\mathcal{CLN}(\mathcal{O})$ be the category whose objects are complete local noetherian $\mathcal{O}$-algebras with residue field $\mathbb{F}$ and morphisms are local homomorphisms that induce the identity map on $\mathbb{F}$. Let R be an object of this category and let $\rho\colon G_S \to \mathrm{GL}_2(R)$ be a continuous homomorphism whose composition with the residue map $R \to \mathbb{F}$ induces the homomorphism $\bar{\rho}$. Two such homomorphisms ρ_1 and ρ_2 are said to be strictly equivalent if there is a matrix $M \in \mathrm{GL}_2(R)$ that reduces to the identity under the residue map $R \to \mathbb{F}$ such that $\rho_2(g) = M \cdot \rho_1(g) \cdot M^{-1}$ for all $g \in G_S$. A deformation of $\bar{\rho}$ to $\mathrm{GL}_2(R)$ is a strict equivalence class of such representations $\rho\colon G_S \to \mathrm{GL}_2(R)$.

Let $\mathcal{SETS}$ be the category of sets. Consider the functor

$$D_{\bar{\rho}}\colon \mathcal{CLN}(\mathcal{O}) \to \mathcal{SETS}$$

defined by $D_{\bar{\rho}}(R) = \{\text{deformations of } \bar{\rho} \text{ to } \mathrm{GL}_2(R)\}$.

Assume that the scalar matrices are exactly the matricies in $\mathrm{M}_2(\mathbb{F})$ that commute with the image of $\bar{\rho}$, *i.e.,* $\mathrm{End}(\bar{\rho}) = \mathbb{F}$. This happens for instance if $\bar{\rho}$ is absolutely irreducible. This assumption also holds in the case when $\bar{\rho}$ is reducible and has the shape (6.1) below. In any case, under this assumption it is known that the functor $D_{\bar{\rho}}$ is representable. That is, there is a ring $R_{\bar{\rho}} \in \mathcal{CLN}(\mathcal{O})$ such that $D_{\bar{\rho}}(R) = \mathrm{Hom}(R_{\bar{\rho}}, R)$ for all $R \in \mathcal{CLN}(\mathcal{O})$. More concretely, there is a universal deformation to $\mathrm{GL}_2(R_{\bar{\rho}})$ such that every deformation to $\mathrm{GL}_2(R)$ is obtained by composing with a map $R_{\bar{\rho}} \to R$.

Now consider deformations $\rho\colon G_S \to \mathrm{GL}_2(R)$ of $\bar{\rho}$, which in addition are p-split, namely,

$$\rho|_{I_p} \sim \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix},$$

where $\delta\colon I_p \to R^\times$ is a character whose reduction is $\bar{\delta}$. In particular $\delta \neq 1$. More precisely, let $M_\rho = R^2$ be a model for ρ. Then ρ is said to be p-split if the sub-module $M^{I_p} \subset M_\rho$ is free of rank 1 over R, and has a free of rank 1 over R complement M' that is I_p-stable with I_p-action given by δ. Notice that if ρ is p-split, then all the members of the strict equivalence class of ρ are also p-split. Now consider the finer deformation functor

$$D_{\bar{\rho}}^{\mathrm{split}}\colon \mathcal{CLN}(\mathcal{O}) \to \mathcal{SETS}$$

defined by $D_{\bar{\rho}}^{\mathrm{split}}(R) = \{p\text{-split deformations of } \bar{\rho} \text{ to } \mathrm{GL}_2(R)\}$. Thus $D_{\bar{\rho}}^{\mathrm{split}} \subset D_{\bar{\rho}}$ is a sub-functor of the usual deformation functor.

Proposition 3.1 *The functor $D_{\bar{\rho}}^{\mathrm{split}}$ is also representable.*

Proof Consider the full sub-category $\mathcal{LA}(\mathcal{O})$ of $\mathcal{CLN}(\mathcal{O})$ whose objects are local artinian $\mathcal{O}$-algebras with residue field $\mathbb{F}$. Recall that a local artinian algebra is automatically complete and noetherian. Let $F_{\bar{\rho}}$ and $F_{\bar{\rho}}^{\mathrm{split}}$ respectively be the deformation functors corresponding to the two deformation problems above restricted to this smaller sub-category. It is a fact that $D_{\bar{\rho}}^{\mathrm{split}}$ is representable if and only if $F_{\bar{\rho}}^{\mathrm{split}}$ is pro-representable, that is, there is a ring $R_{\bar{\rho}}^{\mathrm{split}} \in \mathcal{CLN}(\mathcal{O})$ such that $F_{\bar{\rho}}^{\mathrm{split}}(R) = \mathrm{Hom}(R_{\bar{\rho}}^{\mathrm{split}}, R)$ for all $R \in \mathcal{LA}(\mathcal{O})$. So it suffices to show that $F_{\bar{\rho}}^{\mathrm{split}}$ is pro-representable. Now a similar statement applies to the representable functor $D_{\bar{\rho}}$

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

so the functor $F_{\bar\rho}$ is known to be pro-representable. In particular $F_{\bar\rho}$ satisfies Schlessinger's conditions (H1) through (H4). We must show that $F_{\bar\rho}^{\mathrm{split}}$ also satisfies these conditions.

Since $F_{\bar\rho}^{\mathrm{split}} \subset F_{\bar\rho}$ is a sub-functor, it suffices to show that $F_{\bar\rho}^{\mathrm{split}}$ satisfies condition (H1). The other conditions then follow. Let us recall this condition. Let $R_3 = R_1 \times_{R_0} R_2$ be a fiber product in the category $\mathcal{LA}(\mathcal{O})$ and let

$$(*)\ : F_{\bar\rho}^{\mathrm{split}}(R_3) \longrightarrow F_{\bar\rho}^{\mathrm{split}}(R_1) \times_{F_{\bar\rho}^{\mathrm{split}}(R_0)} F_{\bar\rho}^{\mathrm{split}}(R_2)$$

be the induced map on the level of sets. Then (H1) says that

> if $R_2 \to R_0$ is small (*i.e.*, surjective with kernel a principal ideal annihilated by the maximal ideal of R_2), then the map $(*)$ is surjective.

We shall show that $(*)$ is surjective, where $R_2 \to R_0$ is any (not necessarily small) surjective map. We first prove the following lemma.

Lemma 3.2 *Assume $R_2 \to R_0$ is surjective. Let $\rho_i : G_S \to \mathrm{GL}_2(R_i)$ for $i = 1, 2$ be homomorphisms whose compositions with the maps $R_i \to R_0$ for $i = 1, 2$ induce the same homomorphism to $\mathrm{GL}_2(R_0)$. Let $\rho_3 : G_S \to \mathrm{GL}_2(R_3)$ be the induced homomorphism to the fiber product. Then, if ρ_i is p-split for $i = 0, 1, 2$, then so is ρ_3.*

Proof Let v_i, v_i' be a basis for M_{ρ_i} for $i = 0, 1, 2$, with I_p-acting trivially on v_i and by δ_i on v_i'. Since the map $R_2 \to R_0$ is surjective, we may in fact assume that both v_1 and v_2 map to v_0 under the maps $R_1 \to R_0$ and $R_2 \to R_0$ respectively. Indeed choose v_0 to be the image of v_1 under $R_1 \to R_0$. Then the image of an arbitrary I_p-invariant vector in R_2 under $R_2 \to R_0$ must differ from v_0 by a unit in R_0. Modifying v_2 by an appropriate scalar (using the surjectivity of $R_2 \to R_0$) we may assume that v_2 does indeed map to v_1. A similar argument applies to the complementary basis vectors, v_1', v_2' and v_0'. Let v_3 and v_3' be the vectors in $M_{\rho_3} = R_3^2$ whose components in the fiber product $R_3 = R_1 \times_{R_0} R_2$ are constructed out of the components of the pairs of vectors (v_1, v_2) and (v_1', v_2') respectively. Clearly v_3, v_3' is a basis of R_3^2 with the desired properties. ■

To finish the proof of the proposition, let ρ_1 and ρ_2 be deformations to $\mathrm{GL}_2(R_1)$ and $\mathrm{GL}_2(R_2)$ respectively that yield strictly equivalent homomorphisms to $\mathrm{GL}_2(R_0)$, say differing by an element $\bar M \in \mathrm{GL}_2(R_0)$. Since $R_2 \to R_0$ is surjective, we may conjugate ρ_2 by a pre-image M of $\bar M$ in $\mathrm{GL}_2(R_2)$, and then ρ_1 and $M\rho_2M^{-1}$ induce the *same* homomorphism to $\mathrm{GL}_2(R_0)$. Since ρ_2 is p-split, so is $M\rho_2M^{-1}$. Hence their fiber product $\rho_1 \times M\rho_2M^{-1}$ is also p-split, by the above lemma. Clearly this homomorphism maps to (ρ_1, ρ_2) under the map $(*)$. This proves that $(*)$ is surjective. ■

For ease of notation write $R = R_{\bar\rho}$ for the universal deformation ring attached to $\bar\rho$. We also let $R^{\mathrm{ord}} = R_{\bar\rho}^{\mathrm{ord}}$ denote the universal deformation ring that parametrizes deformations of $\bar\rho$ which are ordinary at p. The existence of this ring was shown by Mazur. Finally we let $R^{\mathrm{split}} = R_{\bar\rho}^{\mathrm{split}}$ denote the universal deformation ring that parametrizes deformation that are ordinary at p, and split on I_p, *i.e.*, the ring that represents the sub-functor $D_{\bar\rho}^{\mathrm{split}}$ above. We have surjections $R \twoheadrightarrow R^{\mathrm{ord}} \twoheadrightarrow R^{\mathrm{split}}$.

3.2 Locally Split Tangent Space

Keep the notation of the last sub-section. In particular $\bar{\rho}\colon G_S \to \mathrm{GL}_2(\mathbb{F})$ is a fixed residual representation that is locally split.

For any algebra $A \in \mathcal{CLN}(\mathcal{O})$ with residue field $\mathbb{F}$, let

$$t(A) = \mathrm{Hom}(\mathfrak{m}_A/(p, \mathfrak{m}_A^2), \mathbb{F})$$

denote the (reduced) tangent space of A.

Let $W = \mathrm{Ad}(\bar{\rho})$ be $\mathrm{M}_2(\mathbb{F})$ with the conjugation action of G_S via $\bar{\rho}$. For the universal deformation ring R, we identify the $\mathbb{F}$-vector space $t(R)$ with deformations of $\bar{\rho}$ to the dual numbers $\mathbb{F}[\varepsilon]/(\varepsilon^2)$. All such deformations are in bijection with $\mathrm{H}^1(G_S, W)$. More explicitly we have a linear isomorphism

$$\mathrm{H}^1(G_S, W) \xrightarrow{\sim} t(R) \tag{3.2}$$

given by assigning to the class of the cocycle $U : G_S \to W$ the strict equivalence class of the homomorphism $\rho_U : G_S \to \mathrm{GL}_2(\mathbb{F}[\varepsilon]/(\varepsilon^2))$ defined by $\rho_U(g) = \bar{\rho}(g) \cdot 1 + U(g)\bar{\rho}(g) \cdot \varepsilon$.

Recall that $\bar{\rho}$ is locally split. Let $t(R^{\mathrm{split}}) \subset t(R)$ denote the tangent space of the universal locally split ring R^{split}. This vector space can be identified with a certain Selmer group. Fix a basis in which $\bar{\rho}$ has the shape (3.1). An easy computation shows that under the identification (3.2), the class of the cocycle

$$U(g) = \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}$$

corresponds to an ordinary locally split deformation if and only if the classes of the cocycles b_g in $\mathrm{H}^1(I_p, \mathbb{F}(\bar{\delta}))$, c_g in $\mathrm{H}^1(I_p, \mathbb{F}(\bar{\delta}^{-1}))$, and d_g in $\mathrm{H}^1(I_p, \mathbb{F}(\bar{\delta}))$, obtained by restricting g to I_p, all vanish. In other words:

$$t(R^{\mathrm{split}}) = \ker\big(\mathrm{H}^1(G_S, W) \to \mathrm{H}^1(I_p, W/W_1)\big), \tag{3.3}$$

where $W_1 \subset W$ is defined, in this basis, by $W_1 = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)\right\}$.

We now proceed to compute the "locally split" Selmer group in (3.3) in various cases.

4 Dihedral Case

Let p be an odd prime and assume that $p \equiv 3 \bmod 4$. Let $K_0 = \mathbb{Q}(\sqrt{-p})$ be an imaginary quadratic field and let $G_{K_0} = \mathrm{Gal}(\overline{\mathbb{Q}}/K_0)$. Let C_{K_0} denote the class group of K_0 and let h_{K_0} be the class number of K_0. Note that $p \nmid h_{K_0}$. Let $\mathbb{F}$ be a finite field of characteristic p and let $\bar{\chi} : C_{K_0} \to \mathbb{F}^\times$ be a character of order h_{K_0}. If H is the Hilbert class field of K_0, then $\bar{\chi}$ may also be thought of as a character of $\mathrm{Gal}(H/K_0)$. Let τ be a generator of $\mathrm{Gal}(K_0/\mathbb{Q})$ and write τ also for a fixed lift to $G_{\mathbb{Q}}$. Let $\bar{\chi}^\tau$ denote the conjugate character.

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

The basic object of study in this section is the residual representation

$$\bar{\rho} = \mathrm{Ind}_{G_{K_0}}^{G_{\mathbb{Q}}}(\bar{\chi}).$$

We fix a basis e_1, e_2 (which we shall refer to as "the global basis" of $\bar{\rho}$) for which we have

$$\bar{\rho} \sim \begin{cases} \begin{pmatrix} \bar{\chi} & 0 \\ 0 & \bar{\chi}^{\tau} \end{pmatrix} & \text{on } G_{K_0}, \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{for } \tau \in G_{\mathbb{Q}} \setminus G_{K_0}. \end{cases} \tag{4.1}$$

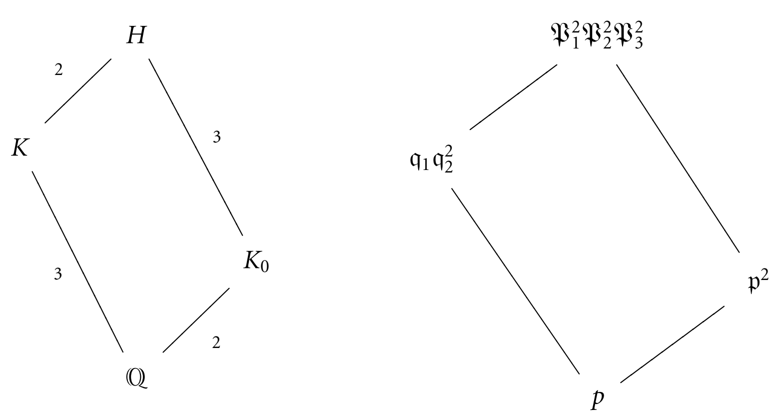
Let $W(\mathbb{F})$ denote the Witt vectors of $\mathbb{F}$ and let $\chi \colon C_{K_0} \to W(\mathbb{F})^{\times}$ denote the Techimüller lift of $\bar{\chi}$. Set $\rho = \mathrm{Ind}_{G_{K_0}}^{G_{\mathbb{Q}}}(\chi)$. If χ is non-trivial, then the theta series

$$f_1 = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) q^{N(\mathfrak{a})},$$

where the sum is over all integral ideals $\mathfrak{a}$ of K_0 is well known to be a cuspidal eigenform of weight 1, level p and character χ_{-p}, where χ_{-p} is the quadratic character of K_0. Further if ρ_{f_1} is the Deligne–Serre Galois representation attached to f_1, then $\rho_{f_1} \sim \rho$.

Now let f be one of the "first six" cusp forms of level 1 and assume p is ordinary for f. It sometimes happens that the weight 1 member of the corresponding p-adic family is the form f_1. This happens in particular for the two pairs $f = \Delta$ and $p = 23$, and $f = \Delta_{16}$ and $p = 31$. Since the residual representation is an invariant of the family, in these cases we have $\bar{\rho}_f \sim \bar{\rho}_{f_1} \sim \bar{\rho}$. As we shall see below this representation is locally split. We wish to show that the locally split tangent space $t(R^{\mathrm{split}})$ vanishes in these two cases.

The field H cut out by $\bar{\rho}$ has Galois group isomorphic to S_3 in these cases. (Such S_3-cases were studied in considerable detail in [BM89].) In fact H is the Galois closure of the cubic field $K = \mathbb{Q}(\alpha)$, with α a root of $q(x) = x^3 \mp x + 1$, of discriminant -23 and -31, respectively. The lattice of fields cut out by $\bar{\rho}$ is given in the diagram on the left below.



If β and γ denote the other roots of $q(x)$, then τ fixes α and switches β and γ, so $\mathrm{Gal}(H/K) = \langle\tau\rangle$. All the number fields above have class number 1 except for K_0, and $h_{K_0} = 3$.

The diagram on the right describes the prime decomposition of p in the various number fields above. It turns out that the residue degree $f(\mathfrak{P}_i/p) = 1$ for all $\mathfrak{P}_i|p$. The discriminant of K is $-p = (\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2$, and this factorization corresponds exactly to the three primes of H lying over p. If $\mathfrak{P}_1 = (\beta-\gamma)$, then the decomposition subgroup $G(\mathfrak{P}_1/p)$ and the inertia subgroup $I(\mathfrak{P}_1/p)$ are both equal to $\mathrm{Gal}(H/K)$. In particular K is the fixed field of inertia. The arithmetic of this field plays a vital role in what follows.

Now $\bar{\rho}|_{G_{\mathfrak{p}}}$ is trivial, since $G_{\mathfrak{p}} = G_{\mathfrak{P}_1} \subset G_H$. So $\bar{\rho}|_{G_p}$ factors through the decomposition subgroup $G(\mathfrak{p}/p)$ of K_0. Since $G(\mathfrak{p}/p) = \mathrm{Gal}(K_0/\mathbb{Q})$, and τ has eigenvalues 1 and -1, evidently $\bar{\rho}|_{G_p} \sim \chi_{-p} \oplus 1$. Thus $\bar{\rho}$ is ordinary and locally split. (A similar argument shows that $\rho|_{G_p} \sim \chi_{-p} \oplus 1$ is also ordinary and locally split.) Fix a basis f_1, f_2 for which $\bar{\rho}$ has the following shape:

$$\bar{\rho}|_{G_p} \sim \begin{pmatrix} \chi_{-p} & 0 \\ 0 & 1 \end{pmatrix}.$$

We refer to this basis as "the local basis" of $\bar{\rho}$. We wish to compute the Selmer group (3.3) in this basis.

4.1 Selmer Group Computations

To proceed further we note that the group $\mathrm{H}^1(G_S, W)$ decomposes. Indeed since $\bar{\rho}$ is dihedral, we have

$$W = 1 \oplus \chi_{-p} \oplus \bar{\rho} \tag{4.2}$$

as a G_S-module (the two-dimensional term above is $\mathrm{Ind}_{G_{K_0}}^{G_{\mathbb{Q}}}(\bar{\chi}^\tau/\bar{\chi}) = \bar{\rho}$, since $\bar{\chi}^\tau/\bar{\chi} = \bar{\chi}$). Using the global basis in which $\bar{\rho}$ has the shape (4.1), the decomposition (4.2) of W is given explicitly by

$$W = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right\} \oplus \left\{ \begin{pmatrix} d & 0 \\ 0 & -d \end{pmatrix} \right\} \oplus \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \right\}.$$

This yields the decomposition

$$\mathrm{H}^1(G_S, W) = \mathrm{H}^1(G_S, \mathbb{F}) \oplus \mathrm{H}^1(G_S, \mathbb{F}(\chi_{-p})) \oplus \mathrm{H}^1(G_S, \bar{\rho}).$$

Thus a class $\sigma \in \mathrm{H}^1(G_S, W)$ may be thought of as a tuple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ with respect to the decomposition above.

Now, in the local basis f_1, f_2 we have $W_1 = \{ \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right) \}$. Since τ flips e_1 and e_2, up to a scalar we have $f_1 = e_1 - e_2$ and $f_2 = e_1 + e_2$. It follows that

$$W_1 = \left\{ \begin{pmatrix} a & -a \\ -a & a \end{pmatrix} \right\}$$

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

in the global basis e_1, e_2. Comparing this with (4.2), we see $W_1 \subset 1 \oplus \bar{\rho}$.

Let $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ be a Selmer class. Since W_1 does not meet the line $\mathbb{F}(\chi_{-p})$ in (4.2), we see that σ_2 lies in the kernel of the map

$$\mathrm{H}^1(G_S, \chi_{-p}) \to \mathrm{H}^1(I_p, \chi_{-p}).$$

The inflation-restriction sequence allows one to work over K_0, and one sees immediately that this map is injective, since h_{K_0} is prime to p. One concludes that σ is a Selmer class if and only if (σ_1, σ_3) lies in the kernel of the map

$$\mathrm{H}^1(G_S, \mathbb{F}) \oplus \mathrm{H}^1(G_S, \bar{\rho}) \longrightarrow \mathrm{H}^1(I_p, (1 \oplus \bar{\rho})/W_1). \tag{4.3}$$

Since W_1 is transverse to the global subspaces 1 and $\bar{\rho}$ of W, computing the kernel of this map is somewhat subtle. To simplify things, define the auxiliary maps induced by restriction and projection:

$$\begin{aligned} r&\colon \mathrm{H}^1(G_S, \mathbb{F}) \to \mathrm{H}^1(I_p, \mathbb{F}) \\ s&\colon \mathrm{H}^1(G_S, \bar{\rho}) \to \mathrm{H}^1(I_p, \bar{\rho}) \to \mathrm{H}^1(I_p, \mathbb{F}) \\ t&\colon \mathrm{H}^1(G_S, \bar{\rho}) \to \mathrm{H}^1(I_p, \bar{\rho}) \to \mathrm{H}^1(I_p, \mathbb{F}(\chi_{-p})). \end{aligned}$$

Then we have the following.

Lemma 4.1 (σ_1, σ_3) *lies in the kernel of the map* (4.3) *if and only if*

$$r(\sigma_1) + s(\sigma_3) = 0 \quad \textit{and} \quad t(\sigma_3) = 0.$$

Proof Note (σ_1, σ_3) is in the kernel if there is an element $\bar{X} \in (1 \oplus \bar{\rho})/W_1$ such that $\sigma_1(i) + \sigma_3(i) = i \cdot \bar{X} - \bar{X}$ for all $i \in I_p$. (We are abusing notation slightly and letting σ_1 and σ_3 also stand for cocycles in the classes they denote.) Say $X = \left(\begin{smallmatrix} a & b \\ c & a \end{smallmatrix}\right) \in 1 \oplus \bar{\rho}$. We may write X as

$$a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{b+c}{2} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{b-c}{2} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now $i \in I_{\mathfrak{p}}$ fixes the last three matrices, whereas $\tau \in I_p \setminus I_{\mathfrak{p}}$ preserves the first two and acts as -1 on the last. Hence we see that $i \cdot X - X$ vanishes for $i \in I_{\mathfrak{p}}$, and equals $\left(\begin{smallmatrix} 0 & c-b \\ b-c & 0 \end{smallmatrix}\right)$ for $i \in I_p \setminus I_{\mathfrak{p}}$. Thus, thinking of the cocycles as taking values in W, we get

$$\sigma_1(i) + \sigma_3(i) = \begin{pmatrix} a_i & -a_i \\ -a_i & a_i \end{pmatrix} \in W_1,$$

if $i \in I_{\mathfrak{p}}$, plus possibly $\left(\begin{smallmatrix} 0 & c-b \\ b-c & 0 \end{smallmatrix}\right)$ if $i \in I_p \setminus I_{\mathfrak{p}}$.

Now $r(\sigma_1)(i) = a_i$, for all $i \in I_p$, since it is given by the entry that occurs on the diagonal of $\sigma_1(i)$. Also $s(\sigma_3)(i) = -a_i$, for all $i \in I_p$, since it is the average of the off diagonal entries of $\sigma_3(i)$. Thus $r(\sigma_1) + s(\sigma_3) = 0$. Similarly $t(\sigma_3)(i) = 0$, for $i \in I_{\mathfrak{p}}$, and equals $2c - 2b$ for $i \in I_p \setminus I_{\mathfrak{p}}$, since it is given by half the difference of the off diagonal entries of $\sigma_3(i)$. In particular $t(\sigma_3)$ is the coboundary $i \mapsto i \cdot (b-c) - (b-c)$, and so vanishes in cohomology. ∎

In view of the lemma above we see that (σ_1, σ_3) does not lie in the kernel of (4.3) if $r(\sigma_1) \neq -s(\sigma_3)$. We show that the last condition always holds unless (σ_1, σ_3) is trivial. First note the following fact.

Lemma 4.2 *The maps r and s are injective.*

Proof The injectivity of r is standard. The injectivity of s was proved by Greenberg [Gre91] in the case $f = \Delta$ and $p = 23$, which he studied in great detail in the context of the Iwasawa theory of motives. We recall his argument briefly and explain how it can be adapted to the case $f = \Delta_{16}$ and $p = 31$ as well. A short computation shows that the Galois group of the maximal abelian extension of H unramified outside S is $\mathbb{Z}_p^4 \times T$, where $T = \mathbb{Z}/11$ in the first case and $T = \mathbb{Z}/15 \times \mathbb{Z}/3$ in the second case. So the maximal p-quotient of this field has Galois group $(\mathbb{Z}/p)^4$ in both cases. One checks that under the natural action of $\mathrm{Gal}(H/\mathbb{Q})$ on this space each of the irreducible representations 1, χ_{-p}, and $\bar{\rho}$ occur with multiplicity one. In particular, $\dim \mathrm{H}^1(G_S, \bar{\rho}) = 1$. So, in both cases, to show s is injective it suffices to show s is non-zero. Let $\mathfrak{P}$ be any prime of H lying over p. Let $U_{\mathfrak{P}}$ be the local units at $\mathfrak{P}$ and $\tilde{U}_{\mathfrak{P}} = U_{\mathfrak{P}}/U_{\mathfrak{P}}^p$. Set

$$U = \prod_{\mathfrak{P}|p} U_{\mathfrak{P}} \quad \text{and} \quad \tilde{U} = \prod_{\mathfrak{P}|p} \tilde{U}_{\mathfrak{P}}.$$

Let E denote the global units of H and let $\tilde{E}$ denote the image of E in $\tilde{U}$. The decomposition subgroup $G(\mathfrak{P}/p) = \mathbb{Z}/2$ acts on each $\tilde{U}_{\mathfrak{P}}$, and the trivial and non-trivial isotypic components each have dimension 1. Let $\tilde{U}_0$ be the product over $\mathfrak{P}$ of the trivial components and likewise let $\tilde{U}_1$ be the product of the non-trivial components. Both of these are modules for $\mathrm{Gal}(H/\mathbb{Q})$. In [Gre91] it is shown that

$$s = 0 \iff \tilde{U}_0^{\bar{\rho}} = \tilde{E}, \tag{4.4}$$

where the super-script $\bar{\rho}$ denotes the $\bar{\rho}$-isotypic component. The argument is general and also applies to the case $f = \Delta_{16}$ and $p = 31$. An explicit computation with the units of H shows that (4.4) does not happen in either case. Indeed assuming the contrary we get for each $\mathfrak{P}$, the map $\tilde{E} \hookrightarrow \tilde{U} \twoheadrightarrow \tilde{U}_{\mathfrak{P}}$ followed by projection to the non-trivial eigenspace of $\tilde{U}_{\mathfrak{P}}$ under the action of $G(\mathfrak{P}/p)$, is the zero map. But with notation as before, $u := \beta/\gamma \in E$ satisfies $\tau(u) = u^{-1}$, so u gives rise to an element in the non-trivial eigenspace of $\tilde{U}_{\mathfrak{P}_1}$. Writing u as $1 + \pi_1/\gamma$ with $\pi_1 := \beta - \gamma$ a uniformizer of $\mathfrak{P}_1$, we see $u \in U_{\mathfrak{P}_1}^1$, the principal units in $U_{\mathfrak{P}_1}$. But clearly $u \notin (U_{\mathfrak{P}_1}^1)^p = U_{\mathfrak{P}_1}^3$. This lemma follows in both cases. ■

By the lemma we see that $r(\sigma_1) \neq -s(\sigma_3)$ if exactly one of σ_1 or σ_3 is trivial. Since $\mathrm{H}^1(G_S, \mathbb{F})$ and $\mathrm{H}^1(G_S, \bar{\rho})$ are both one-dimensional, we may as well assume that σ_1 and σ_3 are (non-zero) basis elements of these spaces.

Now any basis element of $\mathrm{H}^1(G_S, \mathbb{F})$ cuts out the cyclotomic $\mathbb{Z}/p$-extension of $\mathbb{Q}$, and the image of this element under r cuts out the cyclotomic $\mathbb{Z}/p$-extension of $\mathbb{Q}_p$. A basis element of $\mathrm{H}^1(G_S, \bar{\rho})$ cuts out a (p, p)-extension M of H. Let M_1 and M_2 denote the sub $\mathbb{Z}/p$-extensions of M on which $I(\mathfrak{P}_1/p)$ acts non-trivially and trivially respectively. Thus M_2 descends to a $\mathbb{Z}/p$-extension of the fixed field K of $I(\mathfrak{P}_1/p)$.

On completion of M_2 one gets another $\mathbb{Z}/p$-extension of $\mathbb{Q}_p = K_{\mathfrak{q}_1}$, and this corresponds to the image of the basis element under the map s.

Thus to show that the Selmer group vanishes it is enough to show that these two $\mathbb{Z}/p$-extensions of $\mathbb{Q}_p$ coming from r and s are linearly disjoint. This is proved in [Gre91] in the case $f = \Delta$ and $p = 23$, where it is left to the reader as an interesting exercise in class field theory. Since we found the hints there somewhat difficult to reproduce, we provide an alternative argument here, which also works in the case of $f = \Delta_{16}$ and $p = 31$.

Proposition 4.3 *The two $\mathbb{Z}/p$-extensions of $\mathbb{Q}_p$ coming from r and s are disjoint.*

Proof Let us rephrase the proposition. For simplicity, we sometimes write $\mathfrak{P}$ for $\mathfrak{P}_1$ and $\mathfrak{q}$ for $\mathfrak{q}_1$. Recall K is the fixed field of the inertia subgroup $I(\mathfrak{P}/p)$. If L_1 is the cyclotomic $\mathbb{Z}/p$-extension of K and L_2 is the $\mathbb{Z}/p$-extension of K obtained from M_2 by descent, we must show that L_1 and L_2 have distinct completions. To this end let $L = L_1L_2$ be the compositum. It is enough to show that $[L_{\mathfrak{P}} : K_{\mathfrak{q}}] = p^2$.

Write $K_{\mathfrak{q}}^{(p)}$ for the maximal abelian extension of $K_{\mathfrak{q}} = \mathbb{Q}_p$ of exponent p. By local class field theory one has $\mathrm{Gal}(K_{\mathfrak{q}}^{(p)}/K_{\mathfrak{q}}) = K_{\mathfrak{q}}^{\times}/(K_{\mathfrak{q}}^{\times})^p \xrightarrow{\sim} (\mathbb{Z}/p)^2$.

Now $\mathrm{Gal}(L/K) = (\mathbb{Z}/p)^2$. We have the natural maps:

$$\mathrm{Gal}(K_{\mathfrak{q}}^{(p)}/K_{\mathfrak{q}}) \twoheadrightarrow \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{q}}) \hookrightarrow \mathrm{Gal}(L/K).$$

Thus it suffices to show that the composite map is surjective.

To do this we need to make things explicit. On the local side, let $\pi \in K$ be a uniformizer for $K_{\mathfrak{q}} = \mathbb{Q}_p$. Then $\mathrm{Gal}(K_{\mathfrak{q}}^{(p)}/K_{\mathfrak{q}})$ has basis given by (the Artin symbols of) π, $1+\pi$. Since we are working modulo p-th powers, it is legitimate and more convenient to work with the basis π^{1-p}, $1+\pi$.

On the global side, one can check that L is the maximal p-quotient of the ray class field of K of modulus p^2. Write $\mathcal{O}$ for the ring of integers of K. Then by global class field theory $\mathrm{Gal}(L/K) = (\mathcal{O}/p^2\mathcal{O})^{\times}$ modulo units and p-th powers. Since $p = \mathfrak{q}_1\mathfrak{q}_2^2$ in K, we have

$$(\mathcal{O}/p^2\mathcal{O})^{\times} = \frac{1+\mathfrak{q}_1}{1+\mathfrak{q}_1^2} \times \frac{1+\mathfrak{q}_2}{1+\mathfrak{q}_2^4}$$

modulo p-th powers. Further, since $(1+\mathfrak{q}_2)^p = 1+\mathfrak{q}_2^3$, we may identify $\mathrm{Gal}(L/K)$ with

$$X = \frac{1+\mathfrak{q}_1}{1+\mathfrak{q}_2^2} \times \frac{1+\mathfrak{q}_2}{1+\mathfrak{q}_2^3} \text{ modulo units and } p\text{-th powers.}$$

Working adèlically, π^{1-p} is to be thought of as the element

$$(1, 1, \dots, 1, \pi^{1-p}, 1, 1, \dots, 1) \in K^{\times}\backslash\mathbb{A}_K^{\times},$$

which is equivalent to the element

$$(\pi^{p-1}, \pi^{p-1}, \dots, \pi^{p-1}, 1, \pi^{p-1}, \pi^{p-1}, \dots, \pi^{p-1}).$$

So under the above map π^{1-p} maps to the class of $(1, \pi^{p-1})$ in X. Similarly the second basis element $1+\pi$ maps to the class of $(1+\pi, 1)$ in X. We need to show that these two elements generate X. Clearly the second element generates the first factor, so we are reduced to showing that π^{p-1} generates $(1+\mathfrak{q}_2)/(1+\mathfrak{q}_2^3)$ modulo units and p-th powers. We note that this is quite possible, since $(1+\mathfrak{q}_2)/(1+\mathfrak{q}_2^3) \xrightarrow{\sim} (\mathbb{Z}/p)^2$ and the unit rank of K is 1. In fact the root α of $x^3 \mp x + 1$ is a fundamental unit of K. We show $(1+\mathfrak{q}_2)/(1+\mathfrak{q}_2^3)$ is generated by π^{p-1} and α^{p-1}. Indeed we have the following exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & \ker \arrow[r] \arrow[d] & \langle \pi^{p-1}, \alpha^{p-1} \rangle \arrow[r] \arrow[d] & \frac{1+\mathfrak{q}_2}{1+\mathfrak{q}_2^2} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \frac{1+\mathfrak{q}_2^2}{1+\mathfrak{q}_2^3} \arrow[r] & \frac{1+\mathfrak{q}_2}{1+\mathfrak{q}_2^3} \arrow[r] & \frac{1+\mathfrak{q}_2}{1+\mathfrak{q}_2^2} \arrow[r] & 0,
\end{tikzcd}$$

where the vertical arrows are inclusions. By the snake lemma, the middle inclusion is a surjection if the first inclusion is a surjection. This in turn follows if the kernel in the first exact sequence is non-zero (because the dimension of $(1+\mathfrak{q}_2^2)/(1+\mathfrak{q}_2^3)$ is 1). But now a brief check using Pari-gp shows that there exist a, b such that $(\pi^{p-1})^a(\alpha^{p-1})^b \equiv 1 \mod \mathfrak{q}_2^2$, but $\not\equiv 1 \mod \mathfrak{q}_2^3$. For the reader's convenience, we list these values explicitly, when π is taken to be $-3\alpha^2 \pm 4$. They are $a = 13$, $b = 1$ in the -23 case, and $a = 19$, $b = 23$ in the -31 case. ■

In view of the proposition, the kernel of (4.3) is trivial. Hence the Selmer group in (3.3) vanishes, *i.e.*, $t(R^{\text{split}}) = 0$. We can now prove the following.

Theorem 4.4 *Let $f = \Delta$ and $p = 23$, or $f = \Delta_{16}$ and $p = 31$. Then no arithmetic member of the $\wp$-ordinary Hida family passing through f has locally split Galois representation.*

Proof We claim that $R^{\text{split}} \cong \mathbb{Z}_p$ in both cases. Recall $\rho = \mathrm{Ind}_{G_{K_0}}^{G_{\mathbb{Q}}}(\chi)$, the representation arising from the form of weight 1 in the corresponding family, is locally split, and so gives rise to a characteristic 0 point of R^{split}. Since χ is cubic in both cases, ρ actually has a model over $\mathbb{Z}_p$ (even over $\mathbb{Z}$), since the traces of ρ take values in $\mathbb{Z}$. So there is a natural map $R^{\text{split}} \twoheadrightarrow \mathbb{Z}_p$. We show that this map is injective. Since $t(R^{\text{split}}) = 0$, by Nakayama's lemma, the maximal ideal $\mathfrak{m}$ of R^{split} must be the principal ideal $\mathfrak{m} = pR^{\text{split}}$. Now say x lies in the kernel. Then $x \in \mathfrak{m}$, and so $x = px_1$ for some $x_1 \in R^{\text{split}}$. If x_1 were a unit, then p would be in the kernel, which is not the case. So $x_1 \in \mathfrak{m}$, and $x_1 = px_2$ for some $x_2 \in R^{\text{split}}$. Continuing this way we see that, for each $n \geq 1$ we can write $x = p^n x_n$ for some $x_n \in R^{\text{split}}$, *i.e.*, $x \in \bigcap_{n=1}^{\infty} \mathfrak{m}^n$. But R^{split} is a noetherian local ring, so this intersection vanishes by the Krull intersection theorem, and $x = 0$. Thus the above map is injective, proving the claim. Since $R^{\text{split}} = \mathbb{Z}_p$, we see that in particular there are no additional characteristic 0 points of R^{split} other than the weight one point mentioned above, and we are done. ■

Remark 4.5 After the above arguments were written down the authors realized that there is an alternative and simpler method to show that the split Selmer group vanishes. This uses the map t instead of the maps r and s. We have chosen to preserve the argument concerning the maps r and s since similar arguments are likely to be necessary to treat the "full case", which we turn to next.

This argument goes as follows. By (4.4) we have $s = 0 \iff \tilde{U}_0^{\bar{\rho}} = \tilde{E}$. Reasoning identical to that used in [Gre91] to show that (4.4) holds can be similarly used to show that

$$t = 0 \iff \tilde{U}_1^{\bar{\rho}} = \tilde{E}. \tag{4.5}$$

Now $\tilde{E} \subset \tilde{U}^{\bar{\rho}}$ and $\tilde{U} = \tilde{U}_0 \oplus \tilde{U}_1 = (\tilde{U}_0^{\bar{\rho}} \oplus 1) \oplus (\tilde{U}_1^{\bar{\rho}} \oplus \chi_{-p})$. It would therefore appear that the equivalences (4.4) and (4.5) are mutually exclusive, so that $s \neq 0$ forces $t = 0$, rendering any use of the map t towards the vanishing of split Selmer useless. However this is not the case, since $\tilde{E}$ can be transverse to the two spaces $\tilde{U}_0^{\bar{\rho}}$ and $\tilde{U}_1^{\bar{\rho}}$. In fact we claim $t \neq 0$. To see this, note that otherwise by (4.5) we would get for each prime $\mathfrak{P}$ of H, the map $\tilde{E} \hookrightarrow \tilde{U} \twoheadrightarrow \tilde{U}_{\mathfrak{P}}$ followed by projection to the trivial eigenspace of $\tilde{U}_{\mathfrak{P}}$ under the action of the decomposition subgroup $G(\mathfrak{P}/p)$, is the zero map. But this is not true. Let $u' = \alpha^{22}$, where α is the root of $x^3 - x + 1 = 0$ fixed by τ. Then by definition α lies in the trivial eigenspace for the action of $G(\mathfrak{P}_1/p) = \langle \tau \rangle$ with $\mathfrak{P}_1 = (\beta - \gamma)$. On the other hand a computation shows that $u' \in (1 + \mathfrak{P}_1^2) \setminus (1 + \mathfrak{P}_1^3)$. Indeed, using Pari-gp one checks that in the cubic field K the $\mathfrak{q}_1$-adic valuation of $\alpha^{22} - 1$ is equal to 1, and so it has $\mathfrak{P}_1$-adic valuation equal to 2 (since $\mathfrak{q}_1 = \mathfrak{P}_1^2$ in H). Here $\mathfrak{q}_1$ is the prime of the cubic field K lying under $\mathfrak{P}_1$. Thus u' does not lie in $(1 + \mathfrak{P}_1)^p$, which, via the logarithm map, is $1 + \mathfrak{P}_1^3$, and so is non-zero modulo p-th powers. This u' is a global unit that projects non-trivially to the trivial eigenspace of $\tilde{U}_{\mathfrak{P}_1}$. Thus $t \neq 0$.

The non-vanishing of t implies that t is injective. This can be used to show that the split Selmer group vanishes (without using Proposition 4.3). Indeed by Lemma 4.1 if (σ_1, σ_3) is in the kernel of (4.3), then $t(\sigma_3) = 0$. By the injectivity of t we see that $\sigma_3 = 0$. But then the condition $r(\sigma_1) + s(\sigma_3) = 0$ forces $\sigma_1 = 0$ by the injectivity of r, and (σ_1, σ_3) is the trivial class. It is not clear that the analogues of the map t in the "full case" continue to be injective, in which case one would be forced to study the analogues of the maps r and s in this setting regardless.

5 Full Case

We now turn to the case where the image of $\bar{\rho} \colon G_S \to \mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.

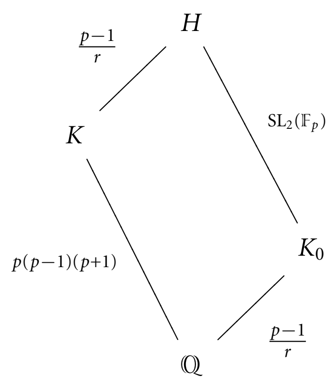
We choose notation in close analogy with the dihedral case above. Let $\mathbb{Q}(\zeta_p)$ denote the p-th cyclotomic field and let $K_0 \subset \mathbb{Q}(\zeta_p)$ be the field cut out by $\det \bar{\rho} = \omega^{k-1}$. Thus if r is the gcd of $k-1$ and $p-1$, then $K_0/\mathbb{Q}$ has degree $(p-1)/r$. Let H be the field cut out by $\bar{\rho}$. It turns out that H/K_0 is an unramified extension with $\mathrm{Gal}(H/K_0) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_p)$. Thus H is a non-abelian replacement for the Hilbert class field of K_0 that appeared in the dihedral setting.

Assume that $\bar{\rho}$ is locally split. The explicit description of the characters δ and ϵ in Section 2.1 shows that

$$\bar{\rho}|_{G_p} \sim \begin{pmatrix} \lambda(\bar{a}_p)^{-1}\omega^{k-1} & 0 \\ 0 & \lambda(\bar{a}_p) \end{pmatrix} \quad \text{and} \quad \bar{\rho}|_{I_p} \sim \begin{pmatrix} \omega^{k-1} & 0 \\ 0 & 1 \end{pmatrix},$$

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

where $\bar{a}_p \in \mathbb{F}_p$ is the mod p reduction of the p-th Fourier coefficient a_p of f. Let K denote the fixed field of the inertia subgroup $I(\mathfrak{P}_1/p)$, where $\mathfrak{P}_1$ is the prime of H induced by the prime $\wp$ of $\bar{\mathbb{Q}}$. Note H/K also has degree $(p-1)/r$. The information above is summarized in the following diagram:



The way in which p decomposes in the fields above is more involved. We have $p = \mathfrak{p}^{(p-1)/r}$ in K_0. If $\mathfrak{P}$ is any prime of H lying over p, then the ramification index $e(\mathfrak{P}/p) = (p-1)/r$ and the residue degree $f(\mathfrak{P}/p)$ is equal to the order of $\bar{a}_p$ in $\mathbb{F}_p^\times$, given by the following table.

f	p	$\bar{a}_p$	$f(\mathfrak{P}/p)$
Δ_{16}	397	367	33
Δ_{18}	271	168	270
Δ_{20}	139	132	138
Δ_{20}	379	42	378
Δ_{26}	107	106	2

Thus p decomposes as $p = \mathfrak{P}_1^{(p-1)/r} \cdots \mathfrak{P}_g^{(p-1)/r}$ in H, where $g = p(p-1)(p+1)/f(\mathfrak{P}/p)$. Of key importance is the prime decomposition of p in K. The number of primes of K lying over p is in bijection with the double coset space $I(\mathfrak{P}_1/p)\backslash G/G(\mathfrak{P}_1/p)$, where $G = \mathrm{Gal}(H/\mathbb{Q})$, and $G(\mathfrak{P}_1/p)$ and $I(\mathfrak{P}_1/p)$ are the decomposition and inertia subgroup of the prime $\mathfrak{P}_1$ of H lying over p. A lengthy but elementary computation of this double coset space in the "smallest" case $f = \Delta_{26}$, and $p = 107$ shows that

$$p = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_{(p-1)/2} \cdot \mathfrak{q}_{(p+1)/2}^{p-1}\, \mathfrak{q}_{(p+3)/2}^{p-1} \cdots \mathfrak{q}_{(p^2+2p-3)/2}^{p-1} \cdot \mathfrak{q}_{(p^2+2p-1)/2}^{p-1}$$

in K, with $f(\mathfrak{q}_i/p) = 2$ for each $\mathfrak{q}_i | p$ except for the last prime, which has $f(\mathfrak{q}_{(p^2+2p-1)/2}/p) = 1$.

We wish to compute the Selmer group in (3.3). While we have not been able to carry out the computation for any example, we now sketch how the computation might

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

proceed under some assumptions. Recall that $W = \mathrm{Ad}(\bar\rho) = 1 \oplus W_0$, where W_0 denotes the trace zero matrices. Thus, we wish to compute the kernel of the map

$$\mathrm{H}^1(G_S, \mathbb{F}) \oplus \mathrm{H}^1(G_S, W_0) \longrightarrow \mathrm{H}^1(I_p, W/W_1).$$

As an I_p-module $W_0 = \mathbb{F} \oplus \mathbb{F}(\omega^{k-1}) \oplus \mathbb{F}(\omega^{1-k})$. In analogy with the dihedral case, consider the maps, induced by restriction and projection:

$$\begin{aligned} r&\colon \mathrm{H}^1(G_S, \mathbb{F}) \to \mathrm{H}^1(I_p, \mathbb{F}),\\ s&\colon \mathrm{H}^1(G_S, W_0) \to \mathrm{H}^1(I_p, W_0) \to \mathrm{H}^1(I_p, \mathbb{F}),\\ t&\colon \mathrm{H}^1(G_S, W_0) \to \mathrm{H}^1(I_p, W_0) \to \mathrm{H}^1(I_p, \mathbb{F}(\omega^{k-1})),\\ u&\colon \mathrm{H}^1(G_S, W_0) \to \mathrm{H}^1(I_p, W_0) \to \mathrm{H}^1(I_p, \mathbb{F}(\omega^{1-k})).\end{aligned}$$

Again an explicit computation shows that the class $\sigma = (\sigma_1, \sigma_3)$ is Selmer if and only if $r(\sigma_1) = -s(\sigma_3)$ and $t(\sigma_3) = 0 = u(\sigma_3)$.

The map r is the same as before and is injective. Thus if either t or u is injective (cf. Remark 4.5), or more generally if $\ker(t) \cap \ker(u) = 0$, then the split tangent space vanishes. So we may assume that $\ker(t) \cap \ker(u) \neq 0$. If s is not injective on this space, the corresponding elements $(0, \sigma_3)$ would be in the split tangent space, and our method would fail. So we might hope that the following holds:

(i) The map s is injective on $\ker(t) \cap \ker(u)$.

Assuming this we proceed to compute the locally split tangent space.

Lemma 5.1 *$\dim \mathrm{H}^1(G_S, W_0) = 2$ and $\mathrm{H}^2(G_S, W_0) = 0$ for all $p \geq k+1$.*

Proof By Weston [Wes04], the (full) deformation problem for $\bar\rho$ is unobstructed, that is, $\mathrm{H}^2(G_S, W) = 0$ for all primes $p \geq k+1$, for the six cusp forms above (if $\bar\rho$ is absolutely irreducible). In particular the summand $\mathrm{H}^2(G_S, W_0)$ also vanishes for these primes. The global Euler characteristic formula then shows $\dim \mathrm{H}^1(G_S, W_0) = 2$. ∎

Let $d = \dim(\ker(t) \cap \ker(u))$. As mentioned above we may assume $d > 0$. It follows from the lemma that $d = 1$ or 2. Assuming (i) the image of s gives rise to a d-dimensional space of $\mathbb{Z}/p$-extensions of $K_{\mathfrak{q}}$, the completion of the inertia field K at $\mathfrak{q} = \mathfrak{q}_1$, the prime of K lying under $\mathfrak{P}_1$. Note that $K_{\mathfrak{q}}$ is the unique unramified extension of $\mathbb{Q}_p$ of degree $f(\mathfrak{q}/p)$. We hope that:

(ii) The cyclotomic $\mathbb{Z}/p$-extension of $K_{\mathfrak{q}}$ (coming from r) does not lie in the d-dimensional span of $\mathbb{Z}/p$-extensions of $K_{\mathfrak{q}}$ coming from s.

This seems out of reach, but here are some further comments.

Lemma 5.2 *$\mathrm{H}^1(\mathrm{GL}_2(\mathbb{F}_p), W_0) = 0$ if $p \geq 5$.*

Proof This is well known (see for instance [Fla92, Lemma 1.2] or [Böc99, Lemma 2.10]), but for completeness we sketch the proof here. Let B denote the upper triangular matrices, U the upper triangular unipotent matrices, and T the diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. We have

$$\mathrm{H}^i(\mathrm{GL}_2(\mathbb{F}_p), W_0) \hookrightarrow \mathrm{H}^i(B, W_0) \xrightarrow{\sim} \mathrm{H}^i(U, W_0)^T.$$

https://doi.org/10.4153/CJM-2010-084-3 Published online by Cambridge University Press

The injectivity of the first restriction map follows, since the index of B in $\mathrm{GL}_2(\mathbb{F}_p)$ is prime to p. The fact that the second restriction map is an isomorphism follows from the Hochschild–Serre spectral sequence, since the index of U in B is prime to p. One checks directly that if $i = 1$, the last group vanishes if $p \geq 5$. ■

By the lemma, the restriction map

$$\mathrm{H}^1(G_S, W_0) \hookrightarrow \mathrm{H}^1(G_{H,S}, W_0)^G = \mathrm{Hom}_G(G_{H,S}, W_0)$$

is injective if $p \geq 5$, at least if $G = \mathrm{Gal}(H/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_p)$. This was automatic in the tame dihedral case, but continues to hold in the present non-tame setting.

Assume now that $d = 2$ (the worst case scenario). Write M and N for the (p, p, p)-extensions of H cut out by a basis of $\mathrm{H}^1(G_S, W_0)$. Write M_1, M_2, and M_3 for the $\mathbb{Z}/p$-extensions of H in M on which $I(\mathfrak{P}_1/p)$ acts by ω^{k-1}, 1, and ω^{1-k} respectively. Define N_1, N_2, and N_3 similarly. Let L_2 and L_3 be the corresponding extensions of K obtained from M_2 and N_2 by descent. Write L_1 for the cyclotomic $\mathbb{Z}/p$-extension of K. Finally, let L be the compositum of L_1, L_2, and L_3. We need to show that after completion, the index $[L_{\mathfrak{P}} : K_{\mathfrak{q}}] = p^3$.

The proof of this seems out of reach presently. Even in the "smallest" case of $f = \Delta_{26}$ and $p = 107$, we would need to carry out a class field theoretic computation in the field K that has degree roughly 10^6 over $\mathbb{Q}$. Remarkably, there is room for the above index to be p^3, since in this case $K_{\mathfrak{q}} = \mathbb{Q}_{p^2}$ has exactly three independent $\mathbb{Z}/p$-extensions!

6 Reducible Case

We now turn to the case where the residual representation $\bar{\rho}$ is reducible. In this case it is possible to deduce that the characteristic zero local representation is indecomposable if a certain Bernoulli number is indivisble by p, using a result of Ribet. We thank F. Calegari for pointing this out to us; this direct argument allows us to avoid the tangent space computations that were contained in an earlier version of this paper. For a study of $R = \mathbb{T}$ theorems for reducible residual representations we refer the reader to [Cal06].

We first recall some well-known facts from the theory of cyclotomic fields (see [Was96]). Let p be an odd prime and let ζ_p be a primitive p-th root of 1. Let ω be the mod p cyclotomic character. Let A be the p-part of the class group of $\mathbb{Q}(\zeta_p)$. Let i be an integer with $0 \leq i \leq p-2$. Then

$$\dim\Big(\ker\big(\mathrm{H}^1(G_S, \mathbb{F}(\omega^i)) \to \mathrm{H}^1(I_p, \mathbb{F}(\omega^i))\big)\Big) = p\text{-rank of } A_i,$$

where A_i is the ω^i-th eigenspace of A under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and the p-rank of $A_i = \dim(A_i/A_i^p)$. It is known that $A_0 = A_1 = 0$. The Herbrand–Ribet theorem says that if i is odd and $3 \leq i \leq p-2$, then

$$A_i \neq 0 \iff p \mid B_{p-i},$$

where B_j is the j-th Bernoulli number. To get a better feel for the p-rank of A_i we recall a conjecture of Iwasawa that says that for an odd integer i with $3 \le i \le p-2$, A_i is isomorphic to the group $\mathbb{Z}_p/B_{1,\omega^{-i}}\mathbb{Z}_p$, where

$$B_{1,\omega^{-i}} = \frac{1}{p}\sum_{\alpha=1}^{p-2} a\,\omega^{-1}(a) \in \mathbb{Z}_p$$

is a twisted Bernoulli number. In particular for such i, the group A_i is conjecturally cyclic, so the p-rank of A_i is 0 or 1 depending on whether A_i is trivial or not. If p is an odd prime for which Vandiver's conjecture holds, *i.e.,* $A_i = 0$ for all even i, then Iwasawa's conjecture is known to hold. A weaker unconditional result due to Mazur and Wiles is that both A_i and $\mathbb{Z}_p/B_{1,\omega^{-i}}\mathbb{Z}_p$ have the same cardinality.

Let now f be a normalized cuspidal eigenform of level 1 and weight $k \ge 2$ (in this section we do not restrict to the six weights considered in the introduction). Let $\wp|p$ be a prime that is ordinary for f, and let $\rho_f\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\wp)$ be the Galois representation attached to f. Assume that the residual representations $\bar\rho\colon G_S \to \mathrm{GL}_2(\mathbb{F})$ attached to f are reducible. It is known that this happens exactly when $p|B_k$. We note that the reductions $\bar\rho$ depend on a choice of lattice (only their semi-simplifications are independent of the choice of lattice). We then have the following.

Theorem 6.1 *Say $p \ge k+3$ and $p|B_k$, so that the residual representations attached to f are reducible. If $p \nmid B_{p-k+1}$, then the local representation attached to ρ_f is indecomposable. More generally, every arithmetic member of the Hida family passing through f has a locally indecomposable Galois representation.*

Proof Choose a lattice and a representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ such that the reduction $\bar\rho$ has the following shape (cf. [Rib76, Theorem 1.3]):

$$\bar\rho = \begin{pmatrix} 1 & u \\ 0 & \omega^{k-1}\end{pmatrix} \tag{6.1}$$

where $u\colon G_S \to \mathbb{F}$ is a map satisfying the following property: if $[c_{\mathrm{unr}}]$ is the cohomology class in $\mathrm{H}^1(G_S, \mathbb{F}(\omega^{1-k}))$ defined by $c_{\mathrm{unr}} = \omega^{1-k}\cdot u$, then $[c_{\mathrm{unr}}]$ is a non-zero element in the kernel of the restriction map

$$\mathrm{H}^1(G_S, \mathbb{F}(\omega^{1-k})) \longrightarrow \mathrm{H}^1(G_p, \mathbb{F}(\omega^{1-k})).$$

That such a non-zero class exists is consistent with the aforementioned facts about cyclotomic fields. Indeed $\omega^{1-k} = \omega^{p-k}$, so letting $i = p-k$, we see that i is odd and $3 \le i \le p-2$, since $p \ge k+3$. Now $\ker\left(\mathrm{H}^1(G_S, \mathbb{F}(\omega^{p-k})) \to \mathrm{H}^1(I_p, \mathbb{F}(\omega^{p-k}))\right) \ne 0$ if and only if $A_{p-k} \ne 0$, which holds by the Herbrand–Ribet theorem, since $p|B_k$.

By an important but simple result of Ribet [Rib76, Proposition 2.1] we may also choose a lattice such that the reduction of ρ_f has the "opposite shape", *i.e.,* $\bar\rho$ looks like:

$$\bar\rho = \begin{pmatrix} \omega^{k-1} & u' \\ 0 & 1\end{pmatrix}$$

with $u' \neq 0$ (more precisely, $\bar{\rho}$ is not semi-simple). The map $\mathrm{H}^1(G_p, \mathcal{O}(\omega^{k-1})) \to \mathrm{H}^1(G_p, K_\wp(\omega^{k-1}))$ is injective, since its kernel is $\mathrm{H}^0(G_p, K_\wp/\mathcal{O}(\omega^{k-1})) = 0$, so ρ_f is locally split if and only if the $\mathcal{O}$-valued representation corresponding to this lattice is locally split. Hence, if ρ_f is locally split, then so is the above residual representation. Thus $\bar{\rho}$ cuts out an unramified ω^{k-1}-extension of $\mathbb{Q}(\zeta_p)$, so $A_{k-1} \neq 0$ and $p \mid B_{p-k+1}$, a contradiction.

A similar argument applies to any arithmetic member of the Hida family passing through f. ■

7 Explicit Examples

7.1 The Δ Function

We now apply the various results proved in this paper to the Ramanujan Delta function $f = \Delta$. We obtain the following.

Corollary 7.1 *The p-adic Galois representation ρ_Δ attached to Δ has locally non-split Galois representation for all ordinary primes $p < 10,000$.*

Proof The only interesting primes are $p = 23$ and $p = 691$, since for all other ordinary primes p less than $10,000$ one knows that the residual representation is absolutely irreducible, p-distinguished, and not locally split, so the characteristic zero representation cannot be locally split [Gha05, Proposition 6]. For $p = 23$, we have seen that the mod p representation is locally split (Δ is its own mod 23 companion form). However, by Theorem 4.4 the 23-adic representation attached to Δ is not locally split. For $p = 691$, we have $691 | B_{12}$ and the residual representations $\bar{\rho}$ are reducible. Since the conditions of Theorem 6.1 are well known to be satisfied, the 691-adic representation is also not locally split. ■

The same proof shows the stronger result.

Corollary 7.2 *No arithmetic member of the $\wp$-ordinary family passing through Δ has locally split Galois representation for all ordinary primes $p < 10,000$.*

7.2 The Next Few Cusp Forms

As for the other five cusp forms of level 1, we have the following result.

Corollary 7.3 *Let $f = \Delta_{16}$, Δ_{18}, Δ_{20}, Δ_{22}, or Δ_{26} and let $p < 10,000$ be an ordinary prime for f. Then every arithmetic member of the $\wp$-adic family passing through f has an indecomposable local Galois representation, except possibly for $p = 397$, 271, 139 or 379, $\cdot$, and 107, respectively.*

Proof For Δ_{16} the only interesting primes are the dihedral prime 31 for which we again conclude by Theorem 4.4 and the full prime 397 that we cannot yet treat. The reducible prime $p = 3617$ can also be treated by checking the conditions of Theorem 6.1. A similar analysis applies to the other four cusp forms (note that some of the reducible primes are larger than 10,000, but of course can still be treated by Theorem 6.1). ■

Acknowledgments We thank Rob de Jeu and Ravi Ramakrishna for useful conversations. We also thank Frank Calegari for providing us with the direct argument in the reducible case that avoids the tangent space computations contained in an earlier version of this paper.

References

[Böc99] G. Böckle, *Explicit universal deformations of even Galois representations.* Math. Nachr. **206**(1999), 85–110.

[BM89] N. Boston and B. Mazur, *Explicit universal deformations of Galois representations.* In: Algebraic number theory, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989, pp. 1–21.

[Cal06] F. Calegari, *Eisenstein deformation rings.* Compos. Math. **142**(2006), no. 1, pp. 63–83. doi:10.1112/S0010437X05001661

[Fla92] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve.* Invent Math. **109**(1992), no. 2, 307–327. doi:10.1007/BF01232029

[GV04] E. Ghate and V. Vatsal, *On the local behaviour of ordinary Λ-adic representations.* Ann. Inst. Fourier (Grenoble) **54**(2004), no. 7, 2143–2162.

[Gha05] E. Ghate, *Ordinary forms and their local Galois representations.* In: Algebra and number theory, Hindustan Book Agency, Delhi, 2005, pp. 226–242.

[Gou97] F. Gouvêa, *Non-ordinary primes: a story.* Experiment. Math. **6**(1997), no. 3, 195–205.

[Gre91] R. Greenberg, *Iwasawa theory for motives.* In: L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991, pp. 211–233.

[Gro90] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p).* Duke. Math. J. **61**(1990), no. 2, 445–517. doi:10.1215/S0012-7094-90-06119-8

[Hid86] H. Hida, *Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms.* Invent. Math. **85**(1986), no. 3, 545–613. doi:10.1007/BF01390329

[Maz89] B. Mazur, *Deforming Galois representations.* In: Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989, pp. 385–437.

[MW86] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations.* Compositio Math. **59**(1986), 231–264.

[Oht06] S. Ohtani, *Deformations of locally abelian Galois representations and unramified extensions.* J. Number Theory **120**(2006), no. 2, 272–286. doi:10.1016/j.jnt.2005.12.002

[Rib76] K. Ribet, *A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$.* Invent. Math. **34**(1976), no. 3, 151–162. doi:10.1007/BF01403065

[Ser73] J.-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer].* Séminaire Bourbaki (1971/1972), 416, Lecture Notes in Mathematics, 317, Springer, Berlin, 1973, pp. 319–338.

[Ser89] ———, *Abelian l-adic representations and elliptic curves.* Second ed., Advanced Book Classics, Addison-Wesley Publishing Company, Redwood City, CA, 1989.

[Was96] L. Washington, *Introduction to cyclotomic fields.* Second ed., Springer-Verlag, Berlin-New York, 1996.

[Wes04] T. Weston, *Unobstructed modular deformation problems.* Amer. J. Math. **126**(2004), no. 6, 1237–1252. doi:10.1353/ajm.2004.0052

[Wil88] A. Wiles, *On ordinary λ-adic representations associated to modular forms.* Invent. Math. **94**(1988), no. 3, 529–573. doi:10.1007/BF01394275

[Yam04] A. Yamagami, *On the unobstructedness of the deformation problems of residual modular representations.* Tokyo J. Math. **27**(2004), no. 2, 443–455. doi:10.3836/tjm/1244208400

School of Mathematics, Tata Institute of Fundamental Research, Mumbai 400005, India.
e-mail: eghate@math.tifr.res.in

Department of Mathematics, University of British Columbia, Vancouver, BC
e-mail: vatsal@math.ubc.ca