Canad. J. Math. Vol. **60** (5), 2008 pp. 1028–1049

Lifting n-Dimensional Galois Representations

Spencer Hamblen

Abstract. We investigate the problem of deforming n-dimensional mod p Galois representations to characteristic zero. The existence of 2-dimensional deformations has been proven under certain conditions by allowing ramification at additional primes in order to annihilate a dual Selmer group. We use the same general methods to prove the existence of n-dimensional deformations.

We then examine under which conditions we may place restrictions on the shape of our deformations at p, with the goal of showing that under the correct conditions, the deformations may have locally geometric shape. We also use the existence of these deformations to prove the existence as Galois groups over $\mathbb{Q}$ of certain infinite subgroups of p-adic general linear groups.

1 Introduction

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let k be a finite field of characteristic p; we then start with an n-dimensional mod p representation $\bar{\rho}\colon G_{\mathbb{Q}} \to GL_n(k)$, and make no assumptions on the origin of $\bar{\rho}$. We address two questions.

Question 1 Since elliptic curves and modular forms give rise to p-adic representations (which then project to mod p representations), under what conditions can we lift $\bar{\rho}$ to characteristic zero? That is, when does there exist a finite extension $\mathcal{O}$ of $\mathbb{Z}_p$ and a continuous representation $\rho\colon G_{\mathbb{Q}} \to GL_n(\mathcal{O})$ such that $\rho \equiv \bar{\rho} \mod p$?

Question 2 If we can lift $\bar{\rho}$ to ρ as in Question 1, is ρ potentially semistable? That is, does it look like representations arising from algebraic varieties or modular forms?

For $n = 2$ and $p \geq 3$, Ramakrishna [12, 13] and Taylor [19] have been able to prove the existence of lifts as in Question 1, and if $\bar{\rho}$ is odd (the determinant of the image of complex conjugation is -1), have proved the existence of geometric lifts as in Question 2 in all but a few explicit cases. Böckle and Khare [2] have used similar methods to Ramakrishna and Taylor to examine the general n-dimensional case for function fields.

Questions 1 and 2 relate to a conjecture of Serre that all 2-dimensional odd absolutely irreducible mod p Galois representations arise from modular forms with prescribed weight, level, and character. Ash and Sinnott [1] have developed a 3-dimensional analogue of Serre's conjecture; however, they relate mod p representations to the mod p cohomology of Hecke eigenclasses, and hence do not attempt to lift their representation to characteristic zero. There also is a conjecture of Fontaine and

Received by the editors October 4, 2005; revised May 19, 2006.
AMS subject classification: 11F80.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Mazur [6] that finitely ramified potentially semistable p-adic representations arise from the étale cohomology of an algebraic variety.

We say $\bar\rho$ *ramifies* at a rational prime v if v ramifies in the fixed field of $\ker\bar\rho$; let S be a finite set of primes including p, the prime at infinity, and all primes at which $\bar\rho$ ramifies. We then let $\mathbb{Q}_S$ be the maximal extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ unramified outside of S, and let $G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. Finally, for a prime v, let $G_v = \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$.

We look for deformations of $\bar\rho$ to $W(k)$, the ring of Witt vectors of k. We will be using the relation between deformations and group cohomology extensively; to that end, let $\mathrm{Ad}\,\bar\rho$ be the Galois module $M_n(k)$ with action via conjugation by $\bar\rho$. Let $\mathrm{Ad}^0\,\bar\rho$ be the trace zero submodule of $\mathrm{Ad}\,\bar\rho$, and let $(\mathrm{Ad}^0\,\bar\rho)^*$ be the $\mathbb{G}_m$ dual of $\mathrm{Ad}^0\,\bar\rho$. Note that $(\mathrm{Ad}^0\,\bar\rho)^*$ is irreducible if and only if $\mathrm{Ad}^0\,\bar\rho$ is irreducible. Finally, for a Galois module A, let $\ker(A)$ be the maximal Galois subgroup acting trivially on A.

Theorem 1.1 *Given a continuous representation $\bar\rho\colon G_{\mathbb{Q}} \to GL_n(k)$, let S be a finite set of primes of $\mathbb{Q}$ containing p and the ramified primes of $\bar\rho$. Assume:*

(i) $p \geq 2n+1$.

(ii) $\mathrm{im}(\bar\rho)$ *is sufficiently large that:*

  (a) $\mathrm{Ad}^0\,\bar\rho$ *is an absolutely irreducible G_S-module,*

  (b) $H^1(G_S/\ker(\mathrm{Ad}^0\,\bar\rho), \mathrm{Ad}^0\,\bar\rho)$ *and* $H^1(G_S/\ker((\mathrm{Ad}^0\,\bar\rho)^*), (\mathrm{Ad}^0\,\bar\rho)^*)$ *are trivial,*

  (c) *there exists $x \in \mathrm{im}\,\bar\rho$ with distinct eigenvalues and a ratio of eigenvalues in $\mathbb{F}_p$ of multiplicity 1 corresponding to a 1-dimensional eigenspace of Ad^0x.*

(iii) *For each $v \neq p \in S$, there exists a smooth quotient of the versal deformation ring of $\bar\rho|_{G_v}$ in $\dim_k H^0(G_p, \mathrm{Ad}^0\,\bar\rho)$ variables.*

(iv) *There exists a smooth quotient of the versal deformation ring of $\bar\rho|_{G_p}$ in*

$$\dim_k H^0(G_p, \mathrm{Ad}^0\,\bar\rho) + \dim_k H^0(G_\infty, \mathrm{Ad}^0\,\bar\rho)$$

variables.

Then there exists a finite set of primes $T \supseteq S$ and a continuous representation $\rho\colon G_T \to GL_n(W(k))$ such that $\rho \equiv \bar\rho \mod p$.

Depending on the image under $\bar\rho$ of complex conjugation, we can place restrictions on the images of these deformations at p. This gives us a first step toward determining under which conditions these deformations can be taken to be geometric. Let U_0 be the upper triangular subgroup of $\mathrm{Ad}^0\,\bar\rho$. Additionally, we say a representation is *upper triangular* if its image is conjugate to a subgroup of upper triangular matrices.

Theorem 1.2 *Suppose $\bar\rho$ meets the first three conditions of Theorem* 1.1. *Suppose*

(i) *the image of complex conjugation under $\bar\rho$ is conjugate to a diagonal matrix with alternating 1s and -1s on the diagonal;*

(ii) *$\bar\rho|_{G_p}$ is upper triangular;*

(iii) *$\bar\rho|_{G_p}$ is sufficiently non-unipotent (see Proposition* 4.2 *and Theorem* 5.2*);*

(iv) $H^2(G_p, U_0) = 0$.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Then there exists a finite set of primes $T \supseteq S$ and a continuous representation $\rho\colon G_T \to GL_n(W(k))$ such that $\rho \equiv \bar{\rho} \mod p$ and $\rho|_{G_p}$ is upper triangular.

We provide some 3-dimensional examples of representations meeting the conditions of our theorem, thus giving rise to lifts to characteristic zero. Some of these examples give lifts with large image in $GL_3(\mathbb{Z}_p)$.

Theorem 1.3 *Let $p \equiv 8 \text{ mod } 21$. Then there exist subgroups of $GL_3(\mathbb{Z}_p)$ containing the principal congruence subgroup of $SL_3(\mathbb{Z}_p)$ that arise as Galois groups over $\mathbb{Q}$.*

1.1 Basic Facts

We present some basic facts we will frequently use; for proofs and more discussion, see [8, 9, 13, 18].

Fact 1.4 **(Local Duality/Cup Product Pairing)** *Given a prime v and a finite G_v-module A, there exists a perfect pairing*

$$H^i(G_v, A) \times H^{2-i}(G_v, A^*) \xrightarrow{\cup} H^2(G_v, A \otimes A^*) \to H^2(G_v, \mu_\infty) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Fact 1.5 **(Local Euler–Poincaré Characteristic)** *For a finite G_v-module A, we have*

$$\#H^0(G_v, A) \cdot \#H^2(G_v, A) = \#H^1(G_v, A) \cdot (\mathbb{Z}_v : \#A \cdot \mathbb{Z}_v)^{-1}.$$

Fact 1.6 *Let A be a finite G_v-module, and let $I_v \subseteq G_v$ be inertia at v. Then*

$$\#H^1(G_v/I_v, A^{I_v}) = \#H^0(G_v/I_v, A^{I_v}) = \#H^0(G_v, A).$$

Fact 1.7 **(Global Euler–Poincaré Characteristic)** *For a number field K, a finite G_K-module A, and a finite set of primes S containing the primes dividing $|A|$ and the infinite primes,*

$$\frac{\#H^0(G_S, A) \cdot \#H^2(G_S, A)}{\#H^1(G_S, A)} = \prod_{v|\infty} \frac{\#H^0(G_v, A)}{|\#A|_v},$$

where $|a|_v = |a|$ if $K_v = \mathbb{R}$ and $|a|^2$ if $K_v = \mathbb{C}$.

Since we will often be looking at the k-dimension of our cohomology groups, for the rest of this work we let $h^i_\star = \dim_k H^i(G_\star, \operatorname{Ad}^0 \bar{\rho})$, if $\star$ is a prime v or a finite set of primes $T \supseteq S$. Additionally, let $hd^i_\star = \dim_k H^i(G_\star, (\operatorname{Ad}^0 \bar{\rho})^*)$ for similar $\star$.

Fact 1.8 **(Chebotarev's Theorem)** *Let L/K be a Galois extension of number fields. For $\sigma \in \operatorname{Gal}(L/K) = G$, let $P_{L/K}(\sigma)$ be the set of prime ideals $\mathfrak{p}$ of K unramified in L such that there exists a prime ideal $\mathfrak{P}$ of L with $\operatorname{Frob}_{\mathfrak{P}} = \sigma$. Let $\langle\sigma\rangle$ be the conjugacy class of σ in G. Then the density of $P_{L/K}(\sigma)$ in the set of all prime ideals is $\frac{\#\langle\sigma\rangle}{\#G}$.*

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

2 Existence Theorem

The smooth quotients in the third and fourth conditions of Theorem 1.1 will induce, for each $v \in S$, subgroups $\mathcal{N}_v$ of $H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$ which are our local deformation conditions. For each $v \in S$, we also define a class $\mathcal{C}_v$ of deformations of $\bar{\rho}|_{G_v}$ to $W(k)$; we choose the pair $(\mathcal{N}_v, \mathcal{C}_v)$ such that the class of mod p^n reductions from $\mathcal{C}_v$ is stable under the action of $\mathcal{N}_v$. Note that the $\mathcal{N}_v$ will be k-subspaces of $H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$; let $n_v = \dim_k \mathcal{N}_v$.

2.1 Taylor's Conditions

Definition 2.1 ([19, p. 3]) Let ρ_m be a deformation of $\bar{\rho}|_{G_v}$ to $W(k)/p^m$. We say that $\mathcal{N}_v$ and $\mathcal{C}_v$ satisfy *Taylor's conditions* if they satisfy all of the following:

(i) $\bar{\rho}|_{G_v} \in \mathcal{C}_v$.
(ii) If $\rho_m \in \mathcal{C}_v$, then the residue of ρ_m in $W(k)/p^r$ is in $\mathcal{C}_v$ for all $1 \le r \le m-1$.
(iii) $\mathcal{C}_v$ is closed under inverse limits.
(iv) For all m, there exists $\rho_m \in \mathcal{C}_v$ such that $\bar{\rho}|_{G_v} \equiv \rho_m \mod p$.
(v) $\mathcal{C}_v$ is closed under the action of $\mathcal{N}_v$; that is, given a deformation $\rho_m \in \mathcal{C}_v$, and $h \in \mathcal{N}_v$, we have $(I + p^{m-1}h).\rho_m \in \mathcal{C}_v$.

We note that the existence of such a $\mathcal{C}_v$ is assured if there exists a smooth quotient of the versal deformation ring at v in n_v variables.

We will need to work with the global pre-images of our local deformation conditions; accordingly, let $\operatorname{Res}\colon H^1(G_S, \operatorname{Ad}^0 \bar{\rho}) \to \bigoplus_{v\in S} H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$ be the restriction map, let $\mathcal{N}_S = \bigoplus_{v\in S} \mathcal{N}_v$, and let

$$H^1_{\mathcal{N}_S}(G_S, \operatorname{Ad}^0 \bar{\rho}) = \operatorname{Res}^{-1}(\mathcal{N}_S) \subseteq H^1(G_S, \operatorname{Ad}^0 \bar{\rho}).$$

For each $\mathcal{N}_v$, let $\mathcal{N}_v^\perp$ be the annihilator of $\mathcal{N}_v$ under the cup product pairing. Then let $\mathcal{N}_S^\perp$ and

$$H^1_{\mathcal{N}_S^\perp}(G_S, (\operatorname{Ad}^0 \bar{\rho})^*) = \operatorname{Res}_\perp^{-1}(\mathcal{N}_S^\perp) \subseteq H^1(G_S, (\operatorname{Ad}^0 \bar{\rho})^*)$$

be defined similarly. These are our Selmer and dual Selmer groups, and we let $h^1_{\mathcal{N}_S}$ and $hd^1_{\mathcal{N}_S^\perp}$, respectively, be their dimension over k. We cannot calculate

$$H^1_{\mathcal{N}_S}(G_S, \operatorname{Ad}^0 \bar{\rho}) \quad \text{and} \quad H^1_{\mathcal{N}_S^\perp}(G_S, (\operatorname{Ad}^0 \bar{\rho})^*)$$

directly, but fortunately we have a formula relating their respective dimensions.

Fact 2.2 ([22, Proposition 1.6]; see also [3]) *For a finite set of primes $T \supseteq S$,*

$$h^1_{\mathcal{N}_T} - hd^1_{\mathcal{N}_T^\perp} = h^0_{\mathbb{Q}} - hd^0_{\mathbb{Q}} + \sum_{v\in T} n_v - \sum_{v\in T} h^0_v.$$

Proposition 2.3 *Assume that for each $v \in S$, we have $\mathcal{N}_v$ and $\mathcal{C}_v$ satisfying Taylor's conditions. If $H^1_{\mathcal{N}_S^\perp}(G_S, (\operatorname{Ad}^0 \bar{\rho})^*)$ is trivial, then there exists $\rho\colon G_S \to GL_n(W(k))$ such that for every $v \in S$, $\rho|_{G_v} \in \mathcal{C}_v$.*

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Proof The Poitou–Tate exact sequence [9, p. 427]) gives us an exact sequence:

$$\begin{array}{ccc} H^1(G_S, \mathrm{Ad}^0 \bar\rho) & \xrightarrow{\mathrm{Res}} & \bigoplus_{v\in S} H^1(G_v, \mathrm{Ad}^0 \bar\rho)/\mathcal{N}_v \\ & & \downarrow \\ & & H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0 \bar\rho)^*)^* \\ & & \downarrow \\ \bigoplus_{v\in S} H^2(G_v, \mathrm{Ad}^0 \bar\rho) & \longleftarrow & H^2(G_S, \mathrm{Ad}^0 \bar\rho) \end{array}$$

Since $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0 \bar\rho)^*)$ is trivial, $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0 \bar\rho)^*)^\vee$ is also trivial, so the first map is a surjection and the last is an injection. Taylor [19, Lemma 1.1] shows that this suffices for $n = 2$, and the proof does not depend on the dimension of the representation. ■

2.2 Additional Ramification

The following proposition was proved by Taylor [19, Lemma 1.2] for the 2-dimensional case as a refinement of the results of [13]; here we extend the proof to the n-dimensional case. We want to find some $T \supseteq S$ such that $H^1_{\mathcal{N}_T^\perp}(G_T, (\mathrm{Ad}^0 \bar\rho)^*)$ is trivial; we can then apply Proposition 2.3.

Proposition 2.4 *Assume the hypotheses of Theorem* 1.1. *Then if for all $v \in S$ we have $\mathcal{N}_v$ and $\mathcal{C}_v$ satisfying Taylor's conditions, and $\sum_{v\in S} n_v \geq \sum_{v\in S} h^0_v$, then there exists a finite set of primes $T \supseteq S$ such that $H^1_{\mathcal{N}_T^\perp}(G_T, (\mathrm{Ad}^0 \bar\rho)^*) = 0$.*

Proof We are assuming that $\mathrm{Ad}^0 \bar\rho$ and $(\mathrm{Ad}^0 \bar\rho)^*$ are both irreducible as G_S modules; hence $H^0(G_{\mathbb{Q}}, \mathrm{Ad}^0 \bar\rho)$ and $H^0(G_{\mathbb{Q}}, (\mathrm{Ad}^0 \bar\rho)^*)$ are trivial. By Fact 2.2, if $\sum_{v\in T} n_v \geq \sum_{v\in T} h^0_v$, then we have

$$\dim_k H^1_{\mathcal{N}_T}(G_T, \mathrm{Ad}^0 \bar\rho) \geq \dim_k H^1_{\mathcal{N}_T^\perp}(G_T, (\mathrm{Ad}^0 \bar\rho)^*).$$

It suffices then to show that $H^1_{\mathcal{N}_T}(G_T, \mathrm{Ad}^0 \bar\rho)$ is trivial for some finite set T containing S satisfying $\sum_{v\in T} n_v \geq \sum_{v\in T} h^0_v$. Next assume that we can choose a $w \notin S$ such that

- $h^0_w = n - 1$ and $h^2_w = 1$ (hence $h^1_w = n$ by Fact 1.5),
- there exists a $\psi \in H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0 \bar\rho)^*)$ which maps to a non-zero element of $H^1(G_w/I_w, (\mathrm{Ad}^0 \bar\rho)^*)$.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Then using that $H^1(G_w, \mathrm{Ad}^0\,\bar\rho)^\perp$ is trivial and Fact 2.2, we have:

$$\begin{aligned} h^1_{\mathcal{N}_S \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)} - hd^1_{\mathcal{N}_S^\perp \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)^\perp} &= \Big(\sum_{v\in S} n_v\Big) + h^1_w - \Big(\sum_{v\in S} h^0_v\Big) - h^0_w \\ &= \Big(\sum_{v\in S} n_v\Big) + n - \Big(\sum_{v\in S} h^0_v\Big) - (n-1) \\ &= h^1_{\mathcal{N}_S} - hd^1_{\mathcal{N}_S^\perp} + 1. \end{aligned}$$

We rewrite this equation:

$$h^1_{\mathcal{N}_S \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)} - h^1_{\mathcal{N}_S} = 1 + hd^1_{\mathcal{N}_S^\perp \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)^\perp} - hd^1_{\mathcal{N}_S^\perp}. \tag{2.1}$$

Then since $H^1(G_w, \mathrm{Ad}^0\,\bar\rho)^\perp$ is trivial, we have

$$H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0\,\bar\rho)^*) \supseteq H^1_{\mathcal{N}_S^\perp \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)^\perp}(G_{S\cup\{w\}}, (\mathrm{Ad}^0\,\bar\rho)^*).$$

The existence of ψ above tells us that the containment is strict. We then get

$$hd^1_{\mathcal{N}_S^\perp} \geq 1 + hd^1_{\mathcal{N}_S^\perp \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)^\perp}.$$

From the left side of (2.1), we then have $h^1_{\mathcal{N}_S} \geq h^1_{\mathcal{N}_S \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)}$. But

$$H^1_{\mathcal{N}_S \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)}(G_{S\cup\{w\}}, \mathrm{Ad}^0\,\bar\rho)$$

injects into $H^1_{\mathcal{N}_S}(G_S, \mathrm{Ad}^0\,\bar\rho)$; therefore the groups must be equal. If we append a prime w to S and choose a local condition $\mathcal{N}_w$, we then have the exact sequence

$$\begin{array}{c} 0 \to H^1_{\mathcal{N}_{S\cup\{w\}}}(G_{S\cup\{w\}}, \mathrm{Ad}^0\,\bar\rho) \to H^1_{\mathcal{N}_S}(G_S, \mathrm{Ad}^0\,\bar\rho) \to H^1(G_w, \mathrm{Ad}^0\,\bar\rho)/\mathcal{N}_w \\ \| \\ H^1_{\mathcal{N}_S \cup H^1(G_w,\mathrm{Ad}^0\,\bar\rho)}(G_{S\cup\{w\}}, \mathrm{Ad}^0\,\bar\rho). \end{array}$$

Hence, we also wish to choose w to have a smooth quotient of its versal deformation ring of dimension $n-1$, inducing our local condition $\mathcal{N}_w$, such that there exists a $\phi \in H^1_{\mathcal{N}_S}(G_S, \mathrm{Ad}^0\,\bar\rho)$ which under the restriction map to $H^1(G_w, \mathrm{Ad}^0\,\bar\rho)$ lands *outside* $\mathcal{N}_w$. By Lemmas 2.5 and 2.7 below, such a prime will always exist if $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0\,\bar\rho)^*)$ is non-trivial. Then, since $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0\,\bar\rho)^*)$ is finite (by Hermite–Minkowski), by induction we have the proposition. ∎

We then prove the existence of the necessary additional primes. We call a local deformation ring R *ramified* if there exist deformations to R which add ramification to that of $\bar\rho$; equivalently, the corresponding subgroup of $H^1(G_v, \mathrm{Ad}^0\,\bar\rho)$ is not contained in the kernel of the restriction map to $H^1(I_v, \mathrm{Ad}^0\,\bar\rho)^{G_v/I_v}$.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

2.3 The Local Deformation Ring at w

Let $R_{\bar\rho}$ be the universal deformation ring of $\bar\rho$, and for a prime w, let $R^w_{\bar\rho}$ be the local versal deformation ring of $\bar\rho|_{G_w}$.

Lemma 2.5 *Assume the hypotheses of Theorem* 1.1. *Then there exist infinitely many primes $w \notin S$ such that*

(i) $h^2_w = 1$,
(ii) *the local versal deformation ring $R^{\bar\rho}_w$ of $\bar\rho|_{G_w}$ has a ramified smooth quotient in h^0_w dimensions.*

Remark. We only treat the case where the x in condition (iii) of Theorem 1.1 has eigenvalues all in k. This assumption allows us to explicitly calculate the versal deformation ring.

Proof If the x in condition (iii) of Theorem 1.1 has eigenvalues all in k, then there exists $\widetilde{w} \in k$ and a rational prime w such that $w \equiv \widetilde{w} \bmod p$, and $\bar\rho(\mathrm{Frob}_w) = x$ has eigenvalues in k of ratio $[a_{n-2} : a_{n-3} : \cdots : a_1 : \widetilde{w} : 1]$, with $a_i \in k^*$. Note that by the definition of x, we have $a_i \neq a_j$ and $a_i a_j^{-1} \neq \widetilde{w}$ for all i and j. By a change of basis we can write $\bar\rho(\mathrm{Frob}_w)$, up to scalar multiplication, as

$$\begin{pmatrix} a_{n-2} & & & 0 \\ & \ddots & & \\ & & \widetilde{w} & \\ 0 & & & 1 \end{pmatrix}.$$

Let A be an element of $\mathrm{Ad}^0\,\bar\rho$, and let $(A)_{(i,j)}$ be the (i,j)-th entry of A. Then the action of G_w on $\mathrm{Ad}^0\,\bar\rho$ is generated by the action of Frob_w, and by inspection, we have that $H^0(G_w, \mathrm{Ad}^0\,\bar\rho) = (\mathrm{Ad}^0\,\bar\rho)^{G_w}$ is therefore equal to the diagonal matrices of $\mathrm{Ad}^0\,\bar\rho$; this is an $n-1$ dimensional space. Let $k(a)$ be the Galois module k with Galois action via multiplication by a. By the conditions on w above, $\mathrm{Ad}^0\,\bar\rho$ decomposes under the action of G_w as

$$\mathrm{Ad}^0\,\bar\rho \cong \Big(\bigoplus_{\substack{a\in k \\ a\neq 1,\widetilde{w}}} k(a)^{b_a}\Big) \oplus k^{n-1} \oplus k(\widetilde{w}). \tag{2.2}$$

We then wish to show $H^2(G_w, \mathrm{Ad}^0\,\bar\rho)$ is 1-dimensional. We use local duality, and note that $(\mathrm{Ad}^0\,\bar\rho)^*$ decomposes as a G_w-module as

$$(\mathrm{Ad}^0\,\bar\rho)^* \cong \Big(\bigoplus_{\substack{a\in k \\ a\neq 1,\widetilde{w}}} k(\widetilde{w}a^{-1})^{b_a}\Big) \oplus k(\widetilde{w})^{n-1} \oplus k. \tag{2.3}$$

So $hd^0_w = h^2_w = 1$, and we note that the elements of $H^0(G_w, (\mathrm{Ad}^0\,\bar\rho)^*)$ are those sending $(A)_{(i,j)}$ to 0 for $(i,j) \neq (n-1,n)$ (see Lemma 2.7).

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Calculating the versal deformation ring explicitly becomes tricky in higher dimensions, but we can take advantage of the simplicity of $\bar{\rho}|_{G_w}$ to gather the information we need.

First note that if we have a deformation of $\bar{\rho}$ to a complete local Noetherian ring R, then $\ker(GL_n(R) \to GL_n(k))$ is a pro-p group. Therefore, since $w \neq p$ and $\bar{\rho}|_{G_w}$ is unramified (since $w \notin S$), deformations of $\bar{\rho}$ factor through the Galois group of the maximal tamely ramified extension of $\mathbb{Q}_w$ over $\mathbb{Q}_w$. This group has two generators, σ_w and τ_w (representing Frobenius and generating inertia, respectively), subject to the relation $\sigma_w \tau_w \sigma_w^{-1} = \tau_w^w$. Thus, let

$$R_w = W(k)[[T_1, \dots, T_n]]/(T_n(T_1 - T_2)),$$

let a_i be liftings of a_i to $W(k)$, and let a general deformation $\boldsymbol{\rho}\colon G_w \to GL_n(R_w)$ be given by

$$\sigma_w \mapsto x = \begin{pmatrix} \mathrm{a}_{n-2}\prod_{i=1}^{n-1}(1+T_i)^{-1} & & & & 0 \\ & \mathrm{a}_{n-3}(1+T_{n-1}) & & & \\ & & \ddots & & \\ & & & w(1+T_2) & \\ 0 & & & & 1+T_1 \end{pmatrix}$$

$$\tau_w \mapsto y = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & T_n \\ 0 & & & 1 \end{pmatrix}.$$

Then $xyx^{-1} = y^w$, $\det x = \det \bar{\rho}(\sigma_w)$, and $\det y = \det \bar{\rho}(\tau_w)$, and there exists an isomorphism of tangent spaces between $R_w^{\bar{\rho}}$ and R_w. Therefore there exists a surjective map from the versal deformation ring $R_w^{\bar{\rho}}$ to R_w, so if R_w has the desired smooth quotient, so will $R_w^{\bar{\rho}}$. We can also use all of the cohomological information about the versal deformation ring for R_w.

There are two distinct $(n-1)$-dimensional smooth quotients of R_w; the first is achieved by sending T_n to 0, but the resulting deformations are unramified. We instead take as our smooth quotient the ring X obtained by sending T_1 to S_1 and T_i to S_{i-1} for $i \geq 2$; note that $X \cong W(k)[[S_1, \dots, S_{n-1}]]$. ■

Remark. Note that we can get deformations of $\bar{\rho}|_{G_w}$ that are *not* the Teichmüller lift. If T_1 is not necessarily zero, the ratio of eigenvalues of our deformation will be different from that of $\bar{\rho}|_{G_w}$, even at the mod p^2 level.

Let t_X^* be the corresponding quotient of $t_{R_w}^*$, the cotangent space of R_w, and let π^* be the quotient map from $t_{R_w}^*$ to t_X^*. Let $t_X = \mathrm{Hom}_k(t_X^*, k)$, and π be the natural injection from t_X to the tangent space t_{R_w}. Let $\{r_1, \dots, r_n\}$ be the set of homomorphisms from $t_{R_w}^*$ to k defined by $r_i(T_j) = \delta_{ij}$, where $\delta_{ij} = 1$ if $i = j$, and is 0 otherwise. Let $\{x_1, \dots, x_{n-1}\}$ be the set of homomorphisms similarly defined on t_X^*; note that $\{r_i\}$ and $\{x_i\}$ are bases of t_{R_w} and t_X, respectively. Finally, let θ be the isomorphism from t_{R_w} to $H^1(G_w, \mathrm{Ad}^0 \bar{\rho})$; we then let $\mathcal{N}_w = \theta(\pi(t_X))$.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Lemma 2.6 *For all $\phi \in \mathcal{N}_w$ and $\sigma \in G_w$, $(\phi(\sigma))_{(n-1,n-1)} = (\phi(\sigma))_{(n,n)}$.*

Proof The map $\pi^*: t^*_{R_w} \to t^*_X$ is induced by sending $\pi^*(T_1) = S_1$ and $\pi^*(T_i) = S_{i-1}$ for $i \geq 2$; we therefore have $\pi(x_1)(T_j) = (r_1 + r_2)(T_j)$, and for $i \geq 2$, $\pi(x_i)(T_j) = r_{i+1}(T_j)$. So $\{r_1 + r_2, r_3, \dots, r_n\}$ is a basis for $\pi(t_X) \subseteq t_{R_w}$.

By Fact 1.5, we have

$$h^1_w(k(a)) = \begin{cases} 1 & \text{if } a = 0 \quad (\text{since } H^0(G_w, k) = k\ ), \\ 1 & \text{if } a = \widetilde{w} \quad (\text{since } \#H^2(G_w, k(\widetilde{w})) = \#H^0(G_w, k)), \\ 0 & \text{otherwise.} \end{cases}$$

By (2.2) and the fact that group cohomology respects direct sums, we can then decompose $H^1(G_w, \operatorname{Ad}^0 \bar{\rho})$ as $[H^1(G_w, k)]^{n-1} \oplus H^1(G_w, k(\widetilde{w}))$.

The first part of the direct sum (which arises from $H^1(G_w/I_w, \operatorname{Ad}^0 \bar{\rho}^{I_w})$, and is hence unramified; see Lemma 1.6) comes from the diagonal entries of $\operatorname{Ad}^0 \bar{\rho}$; the second (which is ramified, coming from the H^2) comes from the $(n, n-1)$-th entry of $\operatorname{Ad}^0 \bar{\rho}$. Let $e_{(i,j)} \in M_n(k)$ have a 1 in the (i, j)-th entry, and 0 elsewhere; a basis for $H^1(G_w, \operatorname{Ad}^0 \bar{\rho})$ is then $\{v_1, \dots, v_n\}$, where the v_i's are 1-cocycles such that

$$\begin{aligned} &v_i(\sigma_w) = e_{(n+1-i,n+1-i)} - e_{(1,1)} && v_i(\tau_w) = 0 \qquad \text{for } 1 \leq i \leq n-1, \\ &v_n(\sigma_w) = 0 && v_n(\tau_w) = e_{(n-1,n)}. \end{aligned}$$

Note that the v_i for $1 \leq i \leq n-1$ are independent since their images lie in distinct G_w-submodules of $\operatorname{Ad}^0 \bar{\rho}$.

We then have $\theta : t_{R_w} \xrightarrow{\sim} H^1(G_w, \operatorname{Ad}^0 \bar{\rho})$ sending r_i to v_i; so $\{v_1 + v_2, v_3, \dots, v_n\}$ is a basis for $\mathcal{N}_w$. ■

2.4 Shrinking the Dual Selmer Group

Lemma 2.7 *Assume the hypotheses of Theorem* 1.1. *Let $T \supseteq S$ be a finite set of primes such that $H^1_{\mathcal{N}_T^\perp}(G_T, (\operatorname{Ad}^0 \bar{\rho})^*)$ is non-trivial, and suppose*

$$\sum_{v \in T} n_v \geq \sum_{v \in T} h^0_v.$$

Then there exists a non-zero $\phi \in H^1_{\mathcal{N}_T}(G_T, \operatorname{Ad}^0 \bar{\rho})$ and $\psi \in H^1_{\mathcal{N}_T^\perp}(G_T, (\operatorname{Ad}^0 \bar{\rho})^*)$, and a prime $w \notin T$ (dependent on ϕ and ψ) satisfying the conditions of Lemma 2.5 *such that:*

- *ϕ maps to a non-trivial element of $H^1(G_w, \operatorname{Ad}^0 \bar{\rho})/\mathcal{N}_w$;*
- *ψ maps to a non-trivial element of $H^1(G_w/I_w, (\operatorname{Ad}^0 \bar{\rho})^*)$.*

Proof Since we are assuming that $H^1_{\mathcal{N}_T^\perp}(G_T, (\operatorname{Ad}^0 \bar{\rho})^*) \neq 0$, by Fact 2.2 there exist non-zero elements $\phi \in H^1_{\mathcal{N}_T}(G_T, \operatorname{Ad}^0 \bar{\rho})$ and $\psi \in H^1_{\mathcal{N}_T^\perp}(G_T, (\operatorname{Ad}^0 \bar{\rho})^*)$. Let $L = \mathbb{Q}(\mu_p)\mathbb{Q}(\operatorname{Ad}^0 \bar{\rho})$, the compositum of the fixed fields of the kernel of the action of $G_\mathbb{Q}$ on μ_p and $\operatorname{Ad}^0 \bar{\rho}$, and let $G_L \cong \operatorname{Gal}(\overline{\mathbb{Q}}/L)$. As G_L acts on $\operatorname{Ad}^0 \bar{\rho}$ and $(\operatorname{Ad}^0 \bar{\rho})^*$ trivially,

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

the restrictions of ϕ and ψ to G_L are just homomorphisms to $\mathrm{Ad}^0\,\bar{\rho}$ and $(\mathrm{Ad}^0\,\bar{\rho})^*$, respectively. We therefore let L_ϕ and L_ψ be the fixed fields of the kernel of the actions of ϕ and ψ, respectively, and let $M = L_\phi L_\psi$.

Note that $H^1(G_S/G_L, \mathrm{Ad}^0\,\bar{\rho})$ is trivial (from the second condition of Theorem 1.1); therefore, by the inflation-restriction sequence, ϕ has non-trivial image in

$$H^1(G_L, \mathrm{Ad}^0\,\bar{\rho})^{\mathrm{Gal}(L/\mathbb{Q})} = \mathrm{Hom}_{G_S}(G_L, \mathrm{Ad}^0\,\bar{\rho}).$$

We can therefore talk about the image of $\mathrm{Gal}(L_\phi/L)$ under ϕ, which must be a non-zero k-subspace of $\mathrm{Ad}^0\,\bar{\rho}$. But by the second condition of Theorem 1.1, $\mathrm{Ad}^0\,\bar{\rho}$ is an irreducible G_S-module, so $\phi(\mathrm{Gal}(L_\phi/L))$ must be all of $\mathrm{Ad}^0\,\bar{\rho}$. Therefore there exists $\sigma \in \mathrm{Gal}(L_\phi/L)$ such that $(\phi(\sigma))_{(n-1,n-1)} \neq (\phi(\sigma))_{(n,n)}$; we fix this σ and note that by Lemma 2.6, ϕ does not map to an element of $\mathcal{N}_w$.

For ψ, first note that $\#H^1(G_w/I_w, (\mathrm{Ad}^0\,\bar{\rho})^*) = \#H^0(G_w, (\mathrm{Ad}^0\,\bar{\rho})^*)$ by Fact 1.6; by (2.3), we have that $H^0(G_w, (\mathrm{Ad}^0\,\bar{\rho})^*)$ is one dimensional and generated by $f_{(n-1,n)} \in \mathrm{Hom}(\mathrm{Ad}^0\,\bar{\rho}, \mu_p)$, where for $A \in \mathrm{Ad}^0\,\bar{\rho}$, we have $f_{(n-1,n)}(A) = (A)_{(n-1,n)}$. So, to satisfy the second condition of the lemma, we need to find a $\tau \in \mathrm{Gal}(L_\psi/L)$ such that $\psi(\tau)(e_{(n-1,n)}) \neq 0$. As above, since $(\mathrm{Ad}^0\,\bar{\rho})^*$ is an irreducible G_S-module and ψ is non-zero (by the triviality of $H^1(G_S/G_L, (\mathrm{Ad}^0\,\bar{\rho})^*)$ and the inflation-restriction sequence), the image of ψ cannot be contained in any proper k-subspace of $(\mathrm{Ad}^0\,\bar{\rho})^*$. But the elements of $\mathrm{Hom}(\mathrm{Ad}^0\,\bar{\rho}, \mu_p)$ which do not depend on the $(n-1,n)$-th entry form a k-subspace of $(\mathrm{Ad}^0\,\bar{\rho})^*$, so there must exist $\tau \in (\mathrm{Ad}^0\,\bar{\rho})^*$ with the desired property; we then fix this τ.

Now $M/\mathbb{Q}$ is a finite extension, so suppose there exists an element $\xi \in \mathrm{Gal}(M/\mathbb{Q})$ such that $\phi(\xi) = \phi(\sigma)$, $\psi(\xi) = \psi(\sigma)$, and there exists $\widetilde{w} \in k^*$ such that $\bar{\rho}(\xi)$ has eigenvalues in k of ratio $[\widetilde{w}^{a_n} : \widetilde{w}^{a_{n-1}} : \cdots : \widetilde{w}^{a_3} : \widetilde{w}^{a_2=1} : \widetilde{w}^{a_1=0}]$ (see the proof of Lemma 2.5). Then by Chebotarev's theorem, there exists a rational prime $w \notin T$ such that $\mathrm{Frob}_w = \xi$, and all of the conditions of the lemma would be met. Given the structure of M, it suffices to show that $L_\phi \cap L_\psi = L$. But $\mathrm{Gal}(L_\phi/L)$ injects into $\mathrm{Ad}^0\,\bar{\rho}$, and $\mathrm{Gal}(L_\psi/L)$ injects into $(\mathrm{Ad}^0\,\bar{\rho})^*$ [12, Lemma 9]. Since by (2.2) and (2.3) the actions of G_w on $\mathrm{Ad}^0\,\bar{\rho}$ and $(\mathrm{Ad}^0\,\bar{\rho})^*$ are different, then $\mathrm{Ad}^0\,\bar{\rho}$ and $(\mathrm{Ad}^0\,\bar{\rho})^*$ cannot possibly be isomorphic as G_S-modules.

We then consider the k-span of the images of $\mathrm{Gal}(L_\phi/L)$ and $\mathrm{Gal}(L_\psi/L)$ in $\mathrm{Ad}^0\,\bar{\rho}$ and $(\mathrm{Ad}^0\,\bar{\rho})^*$, respectively. They are clearly Galois stable, and their intersection

$$\mathrm{Gal}(L_\phi \cap L_\psi/L)$$

must be contained in the intersection of the irreducible G_S-modules $\mathrm{Ad}^0\,\bar{\rho}$, $(\mathrm{Ad}^0\,\bar{\rho})^*$; it must therefore be trivial. ■

Propositions 2.3 and 2.4 together give us Theorem 1.1. We now investigate which representations will meet the third and fourth conditions of Theorem 1.1.

3 Local Obstructions

Mazur [7] showed that $\dim_k(R_v/\mathfrak{m}R_v) \geq h^1_v - h^2_v$, where $\mathfrak{m}$ is the maximal ideal of R_v. Therefore, if we have that for all $v \in S$ that $H^2(G_v, \mathrm{Ad}^0\,\bar{\rho}) = 0$, then the

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

third and fourth conditions of Theorem 1.1 are automatically satisfied, as the versal deformation rings will be smooth in the correct number of variables by Fact 1.5. We therefore determine $H^2(G_v, \mathrm{Ad}^0\,\bar{\rho})$ for all possible $\bar{\rho}|_{G_v}$, or at least as many as we can. Note that if $\bar{\rho}|_{G_p}$ is unramified, the fourth condition of Theorem 1.1 is automatically satisifed (as then $h_p^2 = 0$). Additionally, in some cases when $H^2(G_v, \mathrm{Ad}^0\,\bar{\rho}) \neq 0$, we can exhibit the necessary $\mathcal{N}_v$.

These situations increase in complexity quickly as n increases; while almost every possible image of $\bar{\rho}|_{G_v}$ can be admitted if $n = 2$ [13], we must place more restrictions on the admissible images of $\bar{\rho}|_{G_v}$ if we raise the dimension.

3.1 Local Obstructions for $v = p$

The action of I_p, the inertial subgroup at p, is easier to write explicitly than the action of G_p. Recall that I_p acts via fundamental characters; for a full discussion, see [15,16].

Definition 3.1 A character is of *level* r if it is a product of fundamental characters of level r, but not a product of fundamental characters of level s for all $s < r$.

We will need the following lemma to calculate $H^0(I_p, (\mathrm{Ad}^0\,\bar{\rho})^*)$; recall that χ is the cyclotomic character.

Lemma 3.2 *If there exist characters ϕ_i and ϕ_j of levels i and j, respectively, such that $\phi_i\phi_j^{-1} = \chi^a$ for some a, then $i = j$.*

Proof Without loss of generality, assume $j \geq i$. Then $\phi_j\chi^a = \phi_i$, and as we can write the left-hand side as a product of powers of the fundamental characters of level j. It is easy to see that a character of level m can only be written as a product of fundamental characters of a lesser level m' if the powers of the characters repeat with period m' dividing the original level. As this is not true of ϕ_i (since ϕ_j is a character of level j), we must have $i \geq j$. ■

We then restrict our inspection of the action of I_p further by looking at the semi-simplification of $\bar{\rho}|_{G_p}$, which we denote $\bar{\rho}|_{G_p}^{\mathrm{ss}}$. We denote the restriction of this representation to inertia as $\bar{\rho}^{\mathrm{ss}}|_{I_p}$. From [16], we have that $\bar{\rho}^{\mathrm{ss}}|_{I_p}$ acts through characters $\{\phi_i\}$, the set of which is fixed by the p-th power map. We can then group the characters by their orbits under the p-th power map; let m be the number of orbits. Reindexing the characters (and possibly extending scalars to $\mathbb{F}_{p^{\max\{a_i\}}}$), we have

$$\bar{\rho}^{\mathrm{ss}}|_{I_p} = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}, \text{ where } A_i = \begin{pmatrix} \phi_{i,1} & & 0 \\ & \ddots & \\ 0 & & \phi_{i,a_i} \end{pmatrix},$$

where for each i we have ordered the $\phi_{i,j}$ so that $\phi_{i,j} = \phi_{i,j+1}^p$. These are characters of level a_i, and since the set $\{\phi_{i,j}\}$ is fixed by the p-th power map, we have $\prod_{j=1}^{a_i} \phi_{i,j} = \chi^{b_i}$ for some $b_i \in \mathbb{F}_p^*$.

Lemma 3.3 *Let $\bar\rho^{ss}|_{I_p}$ be as above, and assume $p \geq n+2$. Then $\phi_{r,s}\phi_{r,t}^{-1} \neq \chi$ for all r, s, and t.*

Proof Assume $\phi_{r,s}\phi_{r,t}^{-1} = \chi$ for some r, s, and t. Then, since the set $\{\phi_{r,i}\}$ is fixed by the p-th power map, we have (taking indices mod a_r) $\phi_{r,s-i}\phi_{r,t-i}^{-1} = \chi$ for all $1 \leq i \leq a_r$. Then, multiplying all of these equations together, we get

$$\prod_{i=0}^{a_r-1} \chi = \frac{\prod_{i=0}^{a_r-1} \phi_{r,s-i}}{\prod_{i=0}^{a_r-1} \phi_{r,t-i}}$$

$$\chi^{a_r} = \frac{\prod_{i=0}^{a_r-1} \phi_{r,i}}{\prod_{i=0}^{a_r-1} \phi_{r,i}} = 1.$$

This implies that $(p-1)|a_r$. But $a_r \leq n < p-1$ by hypothesis; therefore no two characters in the same block A_r of $\bar\rho^{ss}|_{I_p}$ can have ratio χ. ■

We then write $\mathrm{Ad}^0(\bar\rho|_{G_v}^{ss})$ for the set of trace zero matrices with action via $\bar\rho|_{G_v}^{ss}$ for all v. Note that the action of G_v on $\mathrm{Ad}^0(\bar\rho|_{G_v}^{ss})$ is *not* semisimple if $\bar\rho|_{G_v}$ is not diagonal. We therefore need the following lemma to be able to use the semisimplification of $\bar\rho|_{G_p}$ and to simplify our calculations; we will also use this lemma in the $v \neq p$ case.

Lemma 3.4 *If $H^2(G_v, \mathrm{Ad}^0\bar\rho) \neq 0$, then $H^2(G_v, \mathrm{Ad}^0(\bar\rho|_{G_v}^{ss})) \neq 0$.*

Proof First note that if $\bar\rho|_{G_v}$ is irreducible, then $\bar\rho^{ss}v = \bar\rho|_{G_v}$, and we trivially have $H^2(G_v, \mathrm{Ad}^0\bar\rho) = H^2(G_v, \mathrm{Ad}^0(\bar\rho|_{G_v}^{ss}))$. Next, assume $\bar\rho|_{G_v} = \left(\begin{smallmatrix} A & C \\ 0 & B \end{smallmatrix}\right)$ where A is an $a \times a$ block and B is an $(n-a) \times (n-a)$ block. Accordingly, we can break $\mathrm{Ad}^0\bar\rho$ into the direct sum of four subgroups $\{L_i\}$ (not submodules) aligned with the four corners of $\bar\rho$: $\mathrm{Ad}^0\bar\rho = \left(\begin{smallmatrix} L_1 & L_2 \\ L_3 & L_4 \end{smallmatrix}\right)$. Finally, we break $(\mathrm{Ad}^0\bar\rho)^*$ into four similar subgroups $\{F_i\}$ such that $F_i(L_j) = 0$ if $i \neq j$. To deal with the trace zero restriction, we omit the (n,n)-th entry in L_4; similarly we omit the (n,n)-th entry in F_4. Choose a basis $\{\phi_{i,j}\}$ for each F_i.

We then have a filtration of $(\mathrm{Ad}^0\bar\rho)^*$ as G_v-modules, which we label $\{M_i\}$:

$$M_0 = \{0\} \subset \langle F_3 \rangle \subset \langle F_3, F_1, F_4 \rangle \subset (\mathrm{Ad}^0\bar\rho)^* = M_3.$$

Assume $\phi \in (\mathrm{Ad}^0\bar\rho)^*$ is non-trivial and is fixed by the action of G_v via $\bar\rho$; then $\phi = \sum_{\phi_{i,j} \in M_3} \alpha_{i,j}\phi_{i,j}$ for some $\alpha_{i,j} \in k$.

Let $s \in \{0,1,2\}$ be the greatest number such that the image of ϕ in M_3/M_s is non-trivial; let $\overline{\phi^s}$ be this image. Then $\overline{\phi^s}$ is fixed by the action of G_v on M_3/M_s via $\bar\rho$ (since $\phi \in [(\mathrm{Ad}^0\bar\rho)^*]^{G_v}$), and this action on $\overline{\phi^s}$ is exactly the same as the action of G_v via $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ on $\phi' = \sum_{\phi_{i,j} \notin M_s} \alpha_{i,j}\phi_{i,j}$. By definition, ϕ' is non-trivial, and we therefore have a non-zero element of $H^0(G_v, (\mathrm{Ad}^0\bar\rho)^*)$. Note that A and B need not be irreducible; we can therefore remove blocks above the diagonal for the purpose of determining when our H^2 is trivial. ■

Lemmas 3.2 and 3.3 imply that for two characters on the diagonal of $\bar\rho^{ss}|_{I_p}$ to have the ratio χ, they must be of the same level and of different blocks of $\bar\rho^{ss}|_{I_p}$. As we will show below, we can construct a basis for $H^0(I_p, (\mathrm{Ad}^0(\bar\rho^{\mathrm{ss}}|_{I_p}))^*)$ such that each element corresponds to such a pair of characters.

Let $f_{ij} \in (\mathrm{Ad}^0\,\bar\rho)^*$ be defined by $f_{ij}(e_{(r,s)}) = \delta_{ir}\delta_{js}$ if $r \neq s$ and $f_{ij}(e_{(r,r)} - e_{(n,n)}) = \delta_{ir}\delta_{jr}$. Then $\{f_{ij}\} = \{f_{ij}\}^{1\le i,j\le n}_{(i,j)\neq(n,n)}$ constitutes a basis of $(\mathrm{Ad}^0\,\bar\rho)^*$ and $(\mathrm{Ad}^0(\bar\rho|^{\mathrm{ss}}_{G_p}))^*$; by a computation similar to (2.3), a subset of the $\{f_{ij}\}$ can be used as a basis for $H^0(I_p, (\mathrm{Ad}^0(\bar\rho^{\mathrm{ss}}|_{I_p}))^*)$.

Lemma 3.5 *There exists $\mathfrak{F} \subseteq \{f_{ij}\}$ such that $H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*) = \bigoplus_{f_{ij}\in\mathfrak{F}}\langle f_{ij}\rangle$.*

Proof Assume there exists a non-zero $f \in H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$; since $f \in (\mathrm{Ad}^0\,\bar\rho)^*$, we can write $f = \sum a_{ij} f_{ij}$ for some $a_{ij} \in k$. Choose (r,s) on the upper-right-most non-zero diagonal of the matrix (a_{ij}) such that $a_{rs} \neq 0$ (and note that (r,s) need not be unique). Then since $\bar\rho|_{I_p}$ is upper triangular (extending scalars if necessary), if (i,j) is on a lower diagonal than (r,s) (*i.e.*, $j-i > r-s$), then $\big(\bar\rho(g)^{-1}e_{(r,s)}\bar\rho(g)\big)_{(i,j)} = 0$. We then have, for all $g \in I_p$,

$$\begin{aligned}
f_{rs}(e_{(r,s)}) &= f(e_{(r,s)}) && \text{(by definition of } f_{ij})\\
&= g.f(e_{(r,s)}) && (\text{since } f \in H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*))\\
&= \chi(g) f(\bar\rho(g)^{-1}e_{(r,s)}\bar\rho(g))\\
&= \chi(g) f(\alpha_{rs}e_{(r,s)} + \sum_{j-i>r-s}\alpha_{ij}e_{(i,j)}) && (\text{for some } \alpha_{ij}\in k)\\
&= \chi(g) f_{rs}(\alpha_{rs}e_{(r,s)}) && (f(e_{(i,j)}) = 0 \text{ for } j-i>r-s)\\
&= g.f_{rs}(e_{(r,s)}).
\end{aligned}$$

So $f_{rs} \in H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$, and similarly for all nonzero a_{ij} in $f = \sum a_{ij} f_{ij}$, we have $f_{ij} \in H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$. ■

We therefore consider the (i,j)-th contribution to $H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$; if these are all zero, then $H^2(G_p, \mathrm{Ad}^0\,\bar\rho) = 0$. Even if we do have a pair of characters whose ratio is χ, we can still prove that the (i,j)-th contribution to $H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$ is zero if the image of $\bar\rho|_{G_p}$ is sufficiently large. To work with individual entries in the image of $\bar\rho|_{G_p}$, we say that $(\bar\rho|_{G_p})_{ij}$ is *trivial* if for all $g \in G_p$, $\big(\bar\rho|_{G_p}(g)\big)_{(i,j)} = 0$. Otherwise we say $(\bar\rho|_{G_p})_{ij}$ is *nontrivial*.

Lemma 3.6 *Assume $\phi_{r,s}$ and $\phi_{t,u}$ are characters along the diagonal of $\bar\rho|_{I_p}$ such that $r > t$ and $\phi_{r,s}\phi_{t,u}^{-1} = \chi$. Let i and j be the rows in which $\phi_{r,s}$ and $\phi_{t,u}$ occur, respectively. Then if there exists x with $i < x < j$ and either $(\bar\rho|_{G_p})_{ix}$ or $(\bar\rho|_{G_p})_{xj}$ is nontrivial, or if $(\bar\rho|_{G_p})_{ij}$ is nontrivial, then the (i,j)-th contribution to $H^0(G_p, (\mathrm{Ad}^0\,\bar\rho)^*)$ is zero.*

Proof If $(\bar\rho|_{G_p})_{ix}$ is nontrivial, then there exists $g \in G_p$ such that

$$\big([\bar\rho|_{G_p}(g)]^{-1}[e_{(x,j)}][\bar\rho|_{G_p}(g)]\big)_{(i,j)} \neq 0.$$

Therefore $f_{ij}(e_{(x,j)}) \neq g.f_{ij}(e_{(x,j)})$, so $f_{ij} \notin H^0(I_p, (\mathrm{Ad}^0\,\bar\rho)^*)$. If $(\bar\rho|_{G_p})_{xj}$ or $(\bar\rho|_{G_p})_{ij}$ is nontrivial, we have the same result. ■

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Combining Lemmas 3.2, 3.3, and 3.6, we have reached the limit of cases where we can determine that $H^2(G_p, \mathrm{Ad}^0\,\bar{\rho}) = 0$. This condition is not strictly necessary, but if $h_p^2 = 0$, we know a smooth quotient of the versal deformation ring exists. Thus if a representation $\bar{\rho}$ avoids the criteria of the proposition below, we know that the fourth condition of Theorem 1.1 can be satisfied.

Proposition 3.7 *Let*

$$\bar{\rho}^{\mathrm{ss}}|_{I_p} = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}$$

(after possibly extending scalars), where

$$A_i = \begin{pmatrix} \phi_{i,1} & & 0 \\ & \ddots & \\ 0 & & \phi_{i,a_i} \end{pmatrix}$$

and each $\phi_{i,j}$ is a character of level a_i. Then $H^2(G_p, \mathrm{Ad}^0\,\bar{\rho})$ is trivial, unless

- *$a_r = a_t$ for some $1 \leq r, t \leq m$ with $r \neq t$,*
- *there exist s and u such that $\phi_{r,s}\phi_{t,u}^{-1} = \chi^{\pm 1}$,*
- *if $\phi_{r,s}\phi_{t,u}^{-1} = \chi$, and i and j are the rows in which $\phi_{r,s}$ and $\phi_{t,u}$ occur, respectively, then $(\bar{\rho})_{ik}$ and $(\bar{\rho})_{kj}$, for $i < k < j$ (if $i \leq j$), and $(\bar{\rho})_{ij}$ are all trivial.*

Note that if $n = 3$, Proposition 3.7 implies that $h_p^2 = 0$ if $\bar{\rho}|_{G_p}$ is unramified or $\bar{\rho}^{\mathrm{ss}}|_{I_p}$ acts via characters of level 2 or 3.

3.2 Local Obstructions for $v \neq p$

In the case where $v \neq p$, we need a smooth quotient of the versal deformation ring in $h_v^1 - h_v^2$ variables. We can always find this if $n = 2$ [13], as we have a nice classification of possible images of $\bar{\rho}|_{G_v}$ [4].

The higher dimensional case has been treated in some detail in the function field case by Böckle and Khare [2]. We state the two relevant propositions here, noting that the proofs are identical in our case. Let $H^1_{\mathrm{unr}}(G_v, \mathrm{Ad}^0\,\bar{\rho}) = H^1(G_v/I_v, (\mathrm{Ad}^0\,\bar{\rho})^{I_v})$ be the *unramified* 1-cohomology, and recall that $\#H^1(G_v/I_v, (\mathrm{Ad}^0\,\bar{\rho})^{I_v}) = \#H^0(G_v, \mathrm{Ad}^0\,\bar{\rho})$ by Lemma 1.6.

Proposition 3.8 ([2, Proposition 2.16]; due to [19, Case E1]) *Suppose $\#\bar{\rho}(I_v)$ is prime to p. Then there exists a smooth quotient of the versal deformation ring in $h^1 - h^2 = h^0$ variables, corresponding to $H^1_{\mathrm{unr}}(G_v, \mathrm{Ad}^0\,\bar{\rho})$.*

Proposition 3.9 ([2, Proposition 2.17]) *Suppose $\bar{\rho}|_{G_v}$ is at most tamely ramified. Then there exists a smooth quotient of the versal deformation ring in $h^1 - h^2 = h^0$ variables, corresponding to $H^1_{\mathrm{unr}}(G_v, \mathrm{Ad}^0\,\bar{\rho})$.*

By using Lemma 3.4, [4], and the methods of [13], we can prove the existence of a smooth quotient of dimension $h_v^1 - h_v^2$ in some other cases.

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

Proposition 3.10 *Suppose $n = 3$. Then if $v \in S$, $v \not\equiv \pm 1 \mod p$, and $\bar{\rho}|_{G_v}\colon G_v \to GL_3(k)$ is reducible, then there exists a smooth quotient of the versal deformation ring at v in $h^1 - h^2 = h^0$ variables.*

Proof There are two cases to consider: where $\bar{\rho}|_{G_v}$ has a 2-dimensional irreducible quotient or sub-representation, and where $\bar{\rho}|_{G_v}$ is upper triangular. We first deal with the latter case.

If $\bar{\rho}|_{G_v}$ is upper triangular, note that it has a 2-dimensional reducible subrepresentation and a 2-dimensional reducible quotient representation. By [4], they must be twist equivalent to one of:

P1 $\left(\begin{smallmatrix}\psi & 0\\ 0 & 1\end{smallmatrix}\right)$, for some character ψ;
P2 $\left(\begin{smallmatrix}1 & \alpha\\ 0 & 1\end{smallmatrix}\right)$, for an additive unramified character α; or
S $\left(\begin{smallmatrix}\chi & u\\ 0 & 1\end{smallmatrix}\right)$, where χ is the mod p cyclotomic character and $u \in H^1(G_v, k(1))$.

We then examine all combinations of these, noting that if either is of type **P1**, then there exists another quotient or subrepresentation which again must fall into one of the three types above. Additionally, we note that since $v \in S$, the image of $\bar{\rho}|_{G_v}$ must be ramified.

There are then 17 distinct possibilities for $\bar{\rho}|_{G_v}$, if we distinguish between representations with different ratios of eigenvalues (most importantly, whether the cyclotomic character appears as a ratio of eigenvalues) and the possible size of $H^2(G_v, \operatorname{Ad}^0 \bar{\rho})$. In 14 of the cases, if $v \not\equiv \pm 1 \mod p$, we have $H^2(G_v, \operatorname{Ad}^0 \bar{\rho}) = 0$. We do not reproduce these here, but note that even if $v \equiv \pm 1 \mod p$, the necessary smooth quotient often exists by Propositions 3.8 or 3.9, or the methods outlined in [13]. This leaves three cases, which we treat below. Note here that $u, u' \in H^1(G_v, k(1))$ are ramified.

Case 1.
$$\begin{pmatrix}\phi & 0 & 0\\ 0 & \chi^{\pm 1} & 0\\ 0 & 0 & 1\end{pmatrix} \quad \text{for a ramified character } \phi$$

Case 2.
$$\begin{pmatrix}\chi^2 & 0 & 0\\ 0 & \chi & u\\ 0 & 0 & 1\end{pmatrix}$$

Case 3.
$$\begin{pmatrix}\chi^2 & u & *\\ 0 & \chi & u'\\ 0 & 0 & 1\end{pmatrix}$$

The necessary smooth quotient exists for Case 1 by the work in Section 2.3. In Case 2, and if $v \equiv 1 \mod p$ (excluded by our hypotheses) or $v^3 \equiv 1 \mod p$ in Case 3, we have $h_v^2 \neq 0$. In both cases, however, $\bar{\rho}|_{G_v}$ is at most tamely ramified, so the smooth quotient exists by Proposition 3.9.

We now turn to the case where $\bar{\rho}|_{G_v}$ is not upper triangular; that is, $\bar{\rho}|_{G_v}$ has a 2-dimensional irreducible quotient or sub-representation. We claim that

$$H^2(G_v, \operatorname{Ad}^0 \bar{\rho}) = 0.$$

By Lemma 3.4, we can assume that $\bar{\rho}|_{G_v}$ is semisimple; we therefore can assume $\bar{\rho}|_{G_v} = \left(\begin{smallmatrix} A & 0 \\ 0 & \phi \end{smallmatrix}\right)$, where A is an irreducible 2-dimensional representation and ϕ is a mod p character. Then $\mathrm{Ad}^0 \bar{\rho}$ decomposes as a G_v-module into $\bigoplus_{i=1}^4 L_i$ (see the proof of Lemma 3.4). We can assume that L_4 is trivial, since we are looking at trace zero matrices; since $v \not\equiv 1 \bmod p$, this does not affect our H^2 calculation. Also, note that $H^2(G_v, L_i) \neq 0$ only if L_i has a 1-dimensional quotient on which G_v acts via χ [12, Lemma 3]).

G_v acts on L_2 and L_3 via multiplication by $\phi^{-1}A$ on the left and $A^{-1}\phi$ on the right, respectively. The existence of a 1-dimensional quotient of either action would imply the existence of a 1-dimensional subrepresentation of A, which was assumed irreducible. Finally, G_v acts on L_1 via conjugation by A; L_1 is therefore the full 2-dimensional adjoint representation. By [13, Lemma 4], $H^2(G_v, L_2) = 0$ if $v \not\equiv -1 \mod p$, so $H^2(G_v, \mathrm{Ad}^0 \bar{\rho}) = 0$. ■

Remark. If $v \equiv -1 \mod p$, $H^2(G_v, \mathrm{Ad}^0 \bar{\rho})$ is not necessarily trivial in the last case above, but by extending the work in [13], we can still get the necessary smooth quotient in this case.

4 Deformation Conditions

Recall that we are assuming $p \geq 2n + 1$, so $p \neq 2$; we then classify the possible parities of $\bar{\rho}$, equivalently via the image of complex conjugation and the size of $H^0(G_\infty, \mathrm{Ad}^0 \bar{\rho})$.

Definition 4.1 Let $c \in G_\infty$ be complex conjugation. Then we say:

- $\bar{\rho}$ is *even* if $\bar{\rho}(c)$ is a scalar matrix (equivalently, $H^0(G_\infty, \mathrm{Ad}^0 \bar{\rho}) = \mathrm{Ad}^0 \bar{\rho}$);
- $\bar{\rho}$ is *odd* if $\bar{\rho}(c)$ is not a scalar matrix (equivalently, $H^0(G_\infty, \mathrm{Ad}^0 \bar{\rho}) \subsetneq \mathrm{Ad}^0 \bar{\rho}$);
- $\bar{\rho}$ is *completely odd* if $\bar{\rho}(c)$ is conjugate to a diagonal matrix with alternating ± 1s on the diagonal (equivalently, h^0_∞ is minimized).

Note that the parity condition in Ash and Sinnott's analogue of Serre's conjecture [1] is that $\bar{\rho}$ must be completely odd.

If $\bar{\rho}$ is odd, we get room to place restrictions on our deformations; we would like to get global deformations which are potentially semistable (ordinary, crystalline, flat). (See [5] for the full definitions and motivations of these conditions.) The existence of such deformations would give evidence for a higher dimensional analogue of Serre's conjecture (though not of the same sort as Ash and Sinnott's).

Flat Deformations

We start by looking for *flat* representations, *i.e.,* representations arising from the generic fibre of a finite flat group scheme over $\mathbb{Z}_p$, as in [11] (see also [14]); these are analogous to representations on p^n-torsion of the Tate module at places of good reduction on abelian varieties. We therefore seek a smooth quotient of the versal deformation ring corresponding to flat deformations of $\bar{\rho}$ in enough variables to satisfy the fourth condition of Theorem 1.1. Unfortunately, by following the calculations of [11] for higher dimensional representations, we find that such smooth quotients only exist if $n \leq 2$.

4.1 Reducible Deformations

We now assume that $\bar{\rho}|_{G_p}$ is upper triangular, and look at *reducible* deformations, that is, deformations of $\bar{\rho}$ such that the local deformation of $\bar{\rho}|_{G_p}$ is also upper triangular. Perrin–Riou [10] has proved that reducible deformations with descending powers of the cyclotomic character along the diagonal (up to unramified characters) are crystalline, and therefore geometric. After finding these reducible lifts, we can try to place restrictions on the characters on the diagonal of our deformation.

Let U_0 be the subgroup of $\mathrm{Ad}^0\,\bar{\rho}$ consisting of upper triangular matrices; we have $\dim_k U_0 = [n(n+1)/2] - 1 = (n^2+n-2)/2$. Let $H^1_{\mathrm{red}}(G_p, \mathrm{Ad}^0\,\bar{\rho})$ be the image of $H^1(G_p, U_0)$ in $H^1(G_p, \mathrm{Ad}^0\,\bar{\rho})$ induced by the injection $U_0 \to \mathrm{Ad}^0\,\bar{\rho}$, and let

$$h^1_{\mathrm{red}} = \dim_k H^1_{\mathrm{red}}(G_p, \mathrm{Ad}^0\,\bar{\rho}).$$

This subgroup induces the *reducible deformation ring*, a quotient of the versal deformation ring of $\bar{\rho}|_{G_v}$.

We must also deal with the obstruction to reducible at p deformations; let

$$H^2_{\mathrm{red}}(G_p, \mathrm{Ad}^0\,\bar{\rho}) = H^2(G_p, U_0),$$

and let $h^2_{\mathrm{red}} = \dim_k H^2_{\mathrm{red}}(G_p, \mathrm{Ad}^0\,\bar{\rho})$. Then let $\mathcal{N}_p$ be the subspace of $H^1_{\mathrm{red}}(G_p, \mathrm{Ad}^0\,\bar{\rho})$ of codimension h^2_{red} induced by a smooth quotient of the reducible deformation ring (we assume such a quotient exists where necessary).

In order for this $\mathcal{N}_p$ to satisfy the fourth condition of Theorem 1.1, we need

$$n_p = h^1_{\mathrm{red}} - h^2_{\mathrm{red}} \geq h^0_p + h^0_\infty. \tag{4.1}$$

We first determine a formula for h^0_∞. We assume that the image of complex conjugation (after conjugation) is diagonal with eigenvalues only ± 1. Let z be the number of -1s on the diagonal; then $h^0_\infty = z^2 + (n-z)^2 - 1 = 2z^2 - 2nz + n^2 - 1$.

We then look at the long exact sequence associated with the short exact equence $0 \to U_0 \to \mathrm{Ad}^0\,\bar{\rho} \to \mathrm{Ad}^0\,\bar{\rho}/U_0 \to 0$ to calculate h^1_{red}:

$$0 \to U_0^{G_p} \to (\mathrm{Ad}^0\,\bar{\rho})^{G_p} \to (\mathrm{Ad}^0\,\bar{\rho}/U_0)^{G_p} \to \\ H^1(G_p, U_0) \xrightarrow{i_1} H^1(G_p, \mathrm{Ad}^0\,\bar{\rho}) \to H^1(G_p, \mathrm{Ad}^0\,\bar{\rho}/U_0) \to \cdots.$$

We want to understand the image of i_1 above. For a finite Galois module A, let $h^i_v(A) = \dim_k H^i(G_v, A)$; then by counting dimensions we have

$$\begin{aligned} h^1_{\mathrm{red}} = \dim_k(\mathrm{im}\, i_1) &= h^1_p(U_0) - h^0_p(\mathrm{Ad}^0\,\bar{\rho}/U_0) + h^0_p - h^0_p(U_0) \\ &\overset{\text{Fact 1.5}}{=} h^2_p(U_0) + \tfrac{1}{2}(n^2+n-2) - h^0_p(\mathrm{Ad}^0\,\bar{\rho}/U_0) + h^0_p. \end{aligned}$$

Remember also that $h^2_{\text{red}} = h^2_p(U_0)$. Putting these into (4.1), we have

$$
\begin{aligned}
h^2_p(U_0) + \tfrac{1}{2}(n^2+n-2) - h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) + h^0_p - h^2_p(U_0) &\geq h^0_p + h^0_\infty,\\
\tfrac{1}{2}(n^2+n-2) - h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) &\geq 2z^2 - 2nz + n^2 - 1,\\
n - 2h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) &\geq 4z^2 - 4nz + n^2,\\
n - 2h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) &\geq (2z-n)^2.
\end{aligned}
\tag{4.2}
$$

When $n = 2$, we have $1 - h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) \geq 2(z-1)^2$. If $z = 0$ or 2 ($\bar\rho$ is even), this clearly cannot be satisfied. But if $z = 1$ ($\bar\rho$ is odd), the equation is satisfied as long as $h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) \neq 2$, which is equivalent to saying that $\bar\rho|_{G_p}$ is not twist equivalent to a unipotent representation; we therefore recover a consequence of part (b) of [13, Theorem 1].

We can give some intuitive guidelines for when $\bar\rho|_{G_p}$ will satisfy (4.2). If $(2z-n)^2$ is sufficiently small, (for example, if $\bar\rho$ meets the parity condition of [1]), we need $h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0)$ to be sufficiently small. The inequality is frequently satisfied if $\bar\rho|_{G_p}$ has no large unipotent quotient or subrepresentations; we have the following results for $n = 3, 4$.

Proposition 4.2 *Suppose $\bar\rho\colon G_{\mathbb{Q}} \to GL_n(k)$ meets the hypotheses of Theorem* 1.1, *except possibly at p. Suppose further that $\bar\rho$ is completely odd, and $\bar\rho|_{G_p}$ is upper triangular. If either*

- *$n = 3$ and the image of $\bar\rho|_{G_p}$ is not twist equivalent to a subgroup of the unipotent matrices, or*
- *$n = 4$ and the image of $\bar\rho|_{G_p}$ does not contain a 3-dimensional subrepresentation or quotient representation twist equivalent to a subgroup of the unipotent matrices,*

then there exists a deformation ρ of $\bar\rho$ to $W(k)$ that is upper triangular at p and ramified at only finitely many primes.

Proof For $n = 3$, the hypotheses imply that there exist two distinct characters on the diagonal, and so $h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) \leq 1$, and so the inequality in (4.1) is satisfied. For $n = 4$, the hypotheses imply $h^0_p(\mathrm{Ad}^0\,\bar\rho/U_0) \leq 2$, and again the inequality in (4.1) is satisfied. We then have the existence of ρ by Theorem 1.1. ■

Ordinary Deformations

We continue to assume that $\bar\rho|_{G_p}$ is upper triangular. We now seek reducible deformations having descending powers of the cyclotomic character on the diagonal; they are therefore crystalline by [10]. We call these deformations *ordinary*, following the definitions of [13,22]. To calculate the size of the ordinary subspace of $H^1(G_p, \mathrm{Ad}^0\,\bar\rho)$ we follow calculations similar to those of [13].

Much like the case of flat deformations, however, if $n > 2$, we cannot find a smooth quotient of the versal deformation ring corresponding to ordinary deformations in enough variables to satisfy the fourth condition of Theorem 1.1. It is possible that for $n > 2$ an intermediate condition exists that is strong enough to guarantee that our deformations are potentially semistable, but we do not currently know of such a condition.

5 Examples

Irreducible representations to $GL_n(k)$, with $n \geq 3$ and char $k = p \geq 7$ are difficult to come by. It is known that there exist extensions of $\mathbb{Q}$ with Galois group $GL_n(\mathbb{F}_p)$ or $SL_n(\mathbb{F}_p)$ (for example, see [20, 21]) for certain classes of n and p. But the known examples often require n to be large with respect to p (thus violating $p \geq 2n+1$), and do not often yield explicit examples.

5.1 Examples from $PSL_2(\mathbb{F}_7)$

We can, however, use lower dimensional examples to build examples. Many Galois representations onto $PSL_2(\mathbb{F}_7)$ are known, and $PSL_2(\mathbb{F}_7)$ has two mutually dual irreducible representations to $PGL_3(\mathbb{Z}[\sqrt{-7}])$. Then given a prime p such that $p \equiv 0$, 1, 2, 4 mod 7 and $p \equiv 2$ mod 3, these representations reduce mod p to irreducible representations to $GL_3(\mathbb{F}_p)$. Given such a p and a representation $\bar{\rho}_0$ onto $PSL_2(\mathbb{F}_7)$, let $\bar{\rho}$ be the corresponding representation from $G_{\mathbb{Q}}$ to $GL_3(\mathbb{F}_p)$ (factoring through $PSL_2(\mathbb{F}_7)$).

We check that such a $\bar{\rho}$ would meet our various criteria. First, note that

$$\# PSL_2(\mathbb{F}_7) = 168 = 2^3 \cdot 3 \cdot 7,$$

so if $p > 7$ the order of the image of $\bar{\rho}$ will be prime to p, and

$$H^1(G_S/\ker(\mathrm{Ad}^0 \bar{\rho}), \mathrm{Ad}^0 \bar{\rho}) \quad \text{and} \quad H^1(G_S/\ker((\mathrm{Ad}^0 \bar{\rho})^*), (\mathrm{Ad}^0 \bar{\rho})^*)$$

are trivial. We must show that im $\bar{\rho}$ contains matrices that correspond to the primes of additional ramification from Lemma 2.7. But to do this, we must examine the specific image of $PSL_2(\mathbb{F}_7)$ in $GL_3(\mathbb{F}_p)$. We then narrow our search to primes $p \equiv 8$ mod 21; this ensures that there exist elements of order 7 in $\mathbb{F}_p^*$. The representations here are taken from the Atlas of Finite Group Representations [23].

Let a and b generate $PSL_2(\mathbb{F}_7)$, with $a^2 = b^3 = (ab)^7 = [a,b]^4 = 1$, and let $\alpha = \frac{-1+\sqrt{-7}}{2} \in \mathbb{F}_p$. Let $i\colon PSL_2(\mathbb{F}_7) \to GL_3(\mathbb{F}_p)$ be defined by

$$i(a) = x = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -1-\alpha & \alpha & 1 \end{pmatrix}, \quad i(b) = y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then the eigenvalues of

$$i(ab) = xy = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & -1-\alpha & \alpha \end{pmatrix}$$

must all be in $\mathbb{F}_p$; moreover, their product must be 1. The characteristic polynomial of xy is $\mathrm{char}(xy) = X^3 - \alpha X^2 - (1+\alpha)X - 1$, and the discriminant of $\mathrm{char}(xy)$ is 7;

https://doi.org/10.4153/CJM-2008-046-4 Published online by Cambridge University Press

therefore, since $p \equiv 8 \mod 21$, xy has no repeated eigenvalues. Finally, 1 is never a root of $\mathrm{char}(xy)$, giving us that for a suitable seventh root of unity ζ_7, the eigenvalues of xy must be $\{\zeta_7^4, \zeta_7^2, \zeta_7\}$ or $\{\zeta_7^5, \zeta_7^6, \zeta_7^3\}$. The ratio of the eigenvalues of $\bar{\rho}$ is thus, for some seventh root of unity ζ_7', $[\zeta_7'^3 : \zeta_7' : 1]$. We fix the element xy in the image of $\bar{\rho}$, and choose primes $w \notin S$ for Lemma 2.7 with Frobenius in its conjugacy class.

5.1.1 Even Examples

We examine an even example from Zeh-Marschke:[1] let $f(x) = x^7 - 22x^6 + 141x^5 - 204x^4 - 428x^3 + 768x^2 + 320x - 512$, and let K be the splitting field of $f(x)$. Then K is totally real, with Galois group over $\mathbb{Q}$ isomorphic to $PSL_2(\mathbb{F}_7)$. Fix $p \equiv 8 \bmod 21$, and let $\bar{\rho}\colon G_{\mathbb{Q}} \to GL_3(F_p)$ be the composition

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to PSL_2(\mathbb{F}_7) \overset{i_p}{\hookrightarrow} GL_3(F_p).$$

Since K is totally real, complex conjugation is in the kernel of $\bar{\rho}$, so $\bar{\rho}$ is even. The discriminant of $f(x) = 2^{50}19^4367^2$, so we let

$$S = \{p, \infty\} \cup \{v \mid v \text{ divides the discriminant of } f(x)\} = \{p, 2, 19, 367, \infty\}.$$

For 2, 19 and 367, note that since the order of the image is prime to p, Proposition 3.8 proves the existence of the smooth quotient necessary for the third condition of Theorem 1.1. Then, note that p does not divide the discriminant of $f(x)$ (since $367 \not\equiv 8 \mod 21$), so $\bar{\rho}$ is unramified at p. Therefore $\bar{\rho}$ meets the conditions of Proposition 3.7 (specifically, the note after the proposition), so $H^2(G_p, \mathrm{Ad}^0\,\bar{\rho}) = 0$. So by Theorem 1.1, there exists a characteristic zero lift ρ of $\bar{\rho}$.

In general, if the image of $\bar{\rho}$ is prime to p (as in this example), we need to ensure that ρ is not the Teichmüller lift of $\bar{\rho}$. If our dual Selmer group $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0\,\bar{\rho})^*)$ is non-trivial, then the image of ρ at the primes added to S as in Lemma 2.7 is not the same as the image of the Teichmüller lift, since we have chosen our local deformations to have different ratios of eigenvalues at the mod p^2 level (see Lemma 2.5). If $H^1_{\mathcal{N}_S^\perp}(G_S, (\mathrm{Ad}^0\,\bar{\rho})^*)$ is trivial, then we can still allow ρ to be ramified at an extra prime $w \notin S$ as in Lemma 2.7. This guarantees that ρ is not the Teichmüller lift, and if adding w to S causes the dual Selmer group to become non-trivial, then we can allow ramification at other primes w_i to create a set $T \supseteq S$ such that $H^1_{\mathcal{N}_T^\perp}(G_T, (\mathrm{Ad}^0\,\bar{\rho})^*) = 0$.

Proposition 5.1 *Suppose $\bar{\rho}$ is even and satisfies the conditions of Theorem* 1.1. *Then there exists a deformation ρ of $\bar{\rho}$ to $W(k)$ such that the image of ρ contains the principal congruence subgroup of $SL_n(W(k))$.*

Proof In the even case we have no restrictions on our deformations, so the image of a deformation of $\bar{\rho}$ to mod p^m contains all matrices of the form $I_n + p^{m'}M$, for all $M \in M_n^0(k)$ and all $m' < m$. The proof then follows from the n-dimensional analogue of [17, Ch. IV, Lemma 3] (the proof is identical to the 2-dimensional version). ■

[1] A. Zeh-Marschke, $SL_2(\mathbb{Z}/7)$ als Galoisgruppe über $\mathbb{Q}$. Unpublished note

We then have a way of constructing Galois groups over $\mathbb{Q}$ isomorphic to p-adic linear groups, giving us Theorem 1.3. We summarize our results from Propositions 4.2 and 5.1 and Section 3, giving a refinement of Theorem 1.1.

Theorem 5.2 *Given $\bar{\rho}\colon G_{\mathbb{Q}} \to GL_n(k)$ and a set of primes S containing p, ∞, and all the primes where $\bar{\rho}$ ramifies, suppose $\bar{\rho}$ meets the first two conditions of Theorem* 1.1 *and that for each $v \neq p$ in S, $\bar{\rho}|_{G_v}$ meets the hypotheses of one of Propositions* 3.8, 3.9, *or* 3.10, *or $H^2(G_v, \mathrm{Ad}^0\,\bar{\rho}) = 0$.*

(i) *If $\bar{\rho}$ is even and $H^2(G_p, \mathrm{Ad}^0\,\bar{\rho}) = 0$, then there exists a finite set of primes $T \supseteq S$ and a continuous representation $\rho\colon G_T \to GL_n(W(k))$ such that $\rho \equiv \bar{\rho} \bmod p$, and $\rho(G_T)$ contains the principal congruence subgroup of $SL_n(W(k))$.*

(ii) *If $\bar{\rho}$ is completely odd, $\bar{\rho}|_{G_p}$ is upper triangular, and $n/2 \geq h^0(\mathrm{Ad}^0\,\bar{\rho}/U_0)$ (assuming the existence of the necessary smooth quotient if $H^2(G_p, U_0) \neq 0$), then there exists a finite set of primes $T \supseteq S$ and a continuous representation $\rho\colon G_T \to GL_n(W(k))$ such that $\rho \equiv \bar{\rho} \bmod p$ and $\rho|_{G_p}$ is upper triangular.*

5.1.2 Odd Examples

We can also use the methods above to get an odd 3-dimensional representation, using Trinks' $PSL_2(\mathbb{F}_7)$ example.[2] Let $f(x) = x^7 - 7x + 3$, and let K be the splitting field of $f(x)$. Then, as above, $\mathrm{Gal}(K/\mathbb{Q}) \cong PSL_2(\mathbb{F}_7)$, and so, as above, this induces $\bar{\rho}\colon G_{\mathbb{Q}} \to GL_3(\mathbb{F}_p)$ for $p \equiv 8 \mod 21$.

This f has complex roots, and complex conjugation in $\mathrm{Gal}(K/\mathbb{Q})$ has non-scalar image in $GL_2(\mathbb{F}_7)$; this implies that $\bar{\rho}$ is odd. The discriminant of $f(x)$ is $3^8 7^8$, so here $S = \{3, 7, p, \infty\}$. As in the previous example, $\bar{\rho}|_{G_3}$ and $\bar{\rho}|_{G_7}$ have image prime to p, so again by Proposition 3.8 the necessary smooth quotient exists.

We need to ensure that $\bar{\rho}|_{G_p}$ is upper triangular, not unipotent, and that the reducible deformation ring contains the necessary smooth quotient. Since p does not divide the discriminant of $f(x)$ (since $p \geq 29$), we have that $\bar{\rho}|_{G_p}$ is unramified. Therefore no 1-dimensional quotient of $\mathrm{Ad}^0\,\bar{\rho}$ exists on which $\bar{\rho}$ acts via χ (since χ is ramified); hence $H^2(G_p, \mathrm{Ad}^0\,\bar{\rho}) = 0$.

Finally, when the splitting field of $f(x)$ over $\mathbb{Q}_p$ is degree 7 cyclic extension, (as is the case when $p = 29$ or 701), $\bar{\rho}|_{G_p}$ is upper triangular and not unipotent since all subgroups of order 7 in the image of $PSL_2(\mathbb{F}_7)$ in $GL_3(\mathbb{F}_p)$ have eigenvalues with ratio $[\zeta_7^3 : \zeta_7 : 1]$ and are split. So by Proposition 4.2, we can get a deformation of $\bar{\rho}$ to characteristic zero which is upper triangular at p.

References

[1] A. Ash and W. Sinnott, *An analogue of Serre's Conjecture for Galois Representations and Hecke Eigenclasses in the mod p cohomology of $GL(n,\mathbb{Z})$.* Duke Math. J. **105**(2000), no. 1, 1–24, 2000.

[2] G. Böckle and C. Khare, *Mod l representations of arithmetic fundamental groups. I.* Duke Math. J. **129**(2005), no. 2, 339–369.

[3] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem.* In: Current Developments in Mathematics. International Press, Cambridge, MA, 1995, pp. 1–154.

[2] W. Trinks, *Ein Beispiel eines Zahlkörpers mit der Galoisgruppe $PSL(3,2)$ uber* $\mathbb{Q}$. Manuscript, Universität Karlsruhe, 1968.

[4] F. Diamond, *An extension of Wiles' results.* In: Modular Forms and Fermat's Last Theorem. Springer-Verlag, New York, 1997.

[5] J.-M. Fontaine, *Représentations p-adiques semi-stables.* Astérique No. 223, 1994, pp. 113–184.

[6] J.-M. Fontaine and B. Mazur, *Geometric Galois representations.* In: Elliptic Curves, Modular Forms, and Fermat's Last Theorem. International Press, Cambridge, MA, 1995, pp. 47–71.

[7] B. Mazur, *Deforming Galois representations.* In: Galois Groups over $\mathbb{Q}$. Math. Sci. Res. Inst. Publ. 16. Springer, New York, 1989, pp. 385–437.

[8] J. Neukirch, *Algebraic Number Theory.* Grundlehren der Mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999.

[9] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields.* Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

[10] B. Perrin-Riou, *Théorie d'Iwasawa des représenttions p-adiques sur un corps local.* Invent. Math. **115**(1994), no. 1, 81–149.

[11] R. Ramakrishna, *On a Variation of Mazur's Deformation Functor.* Compos. Math. **87**(1993), no. 3, 269–286.

[12] ———, *Lifting Galois representations.* Invent. Math. **138**(1999), no. 3, 537–562.

[13] ———, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur.* Ann. of Math. **156**(2002), no. 1, 115–154.

[14] M. Raynaud, *Schémas en groupes de type* $(p, p, \dots, p)$. Bull. Soc. Math. France **102**(1974), 241–280.

[15] K. Ribet and W. Stein, *Lectures on Serre's conjecture.* In: Arithmetic Algebraic Geometry, IAS/Park City Mathematics Series. American Mathematical Society, Providence, RI, 1999.

[16] J.-P. Serre, Sur les représentations modulaires de degré 2 de Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54**(1987), no. 1, 179–230.

[17] ———, *Abelian l-adic representations and elliptic curves.* Research Notes in Mathematics 7. A K Peters, Wellesley, MA, 1998.

[18] ———, *Galois Cohomology*. Springer-Verlag, Berlin, 2002.

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

[20] J. G. Thompson, PSL_3 *and Galois groups over Q.* In: Proceedings of the Rutgers Group Theory Year, 1983–1984, Cambridge University Press, 1985, pp. 309–319.

[21] H. Völklein, $GL_n(q)$ *as Galois group over the rationals.* Math. Ann. **293**(1992), no. 1, 163–176.

[22] A. Wiles, *Modulare elliptic curves and Fermat's last theorem.* Ann. of Math. **141**(1995), no. 3, 443–551.

[23] R. Wilson et al. *ATLAS of Finite Group Representations, Version 1.* http://web.mat.bham.ac.uk/atlas/v1.html.

Department of Mathematics and Computer Science, McDaniel College, Westminster, MD, 21157-4390
e-mail: shamblen@mcdaniel.edu