Invent. math. 138, 537–562 (1999)
Digital Object Identifier (DOI) 10.1007/s002229900016

Inventiones mathematicae

Lifting Galois representations

Ravi Ramakrishna

Department of Mathematics, Cornell University, White Hall, Ithaca, NY 14853, USA

Oblatum 16-XI-1998 & 3-V-1999 / Published online: 20 August 1999

1. Introduction

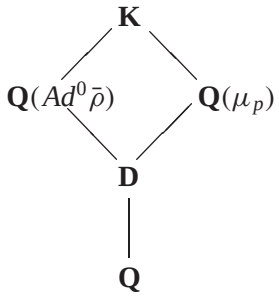
Let $p \geq 5$ be a prime and $\mathbf{k}$ be a finite extension of $\mathbf{F_p}$ the field of p elements. Let $\bar{\rho} : G_{\mathbf{Q}} = Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{k})$ be a continuous Galois representation. If $\bar{\rho}$ is odd (i.e. $\det\bar{\rho}(c) = -1$ where c is complex conjugation) and absolutely irreducible then Serre has conjectured in [Se1] that $\bar{\rho}$ "comes from" a modular newform f of prescribed weight $k(\bar{\rho})$, level $N(\bar{\rho})$ and character $\omega(\bar{\rho})$. Following work of Eichler-Shimura, Deligne and Deligne-Serre there would then exist a representation $\rho_f : G_{\mathbf{Q}} \to GL_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of some finite extension of $W(\mathbf{k})$, the ring of Witt vectors of $\mathbf{k}$, with the following properties:

- ρ_f is unramified at primes q not dividing $N(\bar{\rho})p$.
- For such q let $Frob_q$ denote the conjugacy class of Frobenius at q. Then $\mathrm{Trace}(\rho_f(Frob_q)) = a_q$, an algebraic integer which is the eigenvalue of the Hecke operator T_q acting on the newform f with coefficients in $\mathcal{O}$.
- If π is a uniformizer of $\mathcal{O}$ then $\rho_f \bmod \pi$ is equivalent to $\bar{\rho}$.

Serre's Conjecture thus trivially implies, in Mazur's language, that there is a characteristic zero deformation of $\bar{\rho}$. Conversely, the existence of such a deformation might be regarded as evidence for Serre's Conjecture. In [Kh] Khare has shown that if one is willing to allow additional ramification at a finite set of primes not dividing $N(\bar{\rho})p$ then there is a deformation to mod p^2, i.e. a representation $\rho_2 : G_{\mathbf{Q}} \to GL_2(W(\mathbf{k})/p^2)$. His method works for $\bar{\rho}$ even as well. If $\bar{\rho}$ is reducible Khare has shown that $\bar{\rho}$ can be deformed to $W(\mathbf{k})$ if additional ramification is allowed.

The main result of this paper is that with several technical hypotheses on an *absolutely irreducible* $\bar{\rho}$ one can deform $\bar{\rho}$ to $W(\mathbf{k})$. As in Khare's work more ramification must be allowed and the methods are independent of the parity of $\bar{\rho}$. We do not know if these deformations are potentially semistable at p in the sense of Fontaine. We also do not know whether, for unramified primes, the trace of Frobenii are algebraic.

After twisting $\bar{\rho}$ by a character we may (and do) assume the fields fixed by the kernel of $\bar{\rho}$ and the kernel of its associated projective representation are ramified at the same set of primes. We denote these fields $\mathbf{Q}(\bar{\rho})$ and $\mathbf{Q}(Ad^0\bar{\rho})$ throughout this paper. Note that any of twist $\bar{\rho}$ by a continuous $\mathbf{k}^*$-valued character can only increase the set of ramified primes of $\bar{\rho}$. Let S denote the union of this common set of primes, $\{p\}$, and the infinite prime. Let $G_S = Gal(\mathbf{Q_S}/\mathbf{Q})$ where $\mathbf{Q_S}$ is the maximal extension of $\mathbf{Q}$ ramified only at primes in S. Note $\bar{\rho}$ factors through G_S and that with the possible exception of the prime p and the infinite prime all twists of $\bar{\rho}$ are ramified at all primes of S. For a place v let $G_v = Gal(\bar{\mathbf{Q}}_\mathbf{v}/\mathbf{Q_v})$. Let $Ad^0\bar{\rho}$ denote the set of 2×2 trace zero matrices with entries in $\mathbf{k}$ and G_S action through $\bar{\rho}$ and by conjugation. Let $(Ad^0\bar{\rho})^*$ be its Cartier dual and N and N^d be the maximal subgroups of G_S that act trivially on $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ respectively. Note $\mathbf{Q}(Ad^0\bar{\rho})$ is the fixed field of N. Let $\mathbf{D} = \mathbf{Q}(Ad^0\bar{\rho}) \cap \mathbf{Q}(\mu_p)$ and $\mathbf{K}$ be the composite $\mathbf{Q}(Ad^0\bar{\rho})\mathbf{Q}(\mu_p)$. Observe $Gal(\mathbf{K}/\mathbf{D}) \simeq Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D})$. Finally note that for $Ad^0\bar{\rho}$ absolutely irreducible, the minimal field of definition of the representation of G_S on the three dimensional $\mathbf{k}$ space $Ad^0\bar{\rho}$ may in fact be a proper subfield of $\mathbf{k}$. We call this minimal field $\tilde{\mathbf{k}}$. This is discussed in Section 6. Note $\mathbf{k} \neq \tilde{\mathbf{k}}$ in the odd example of Section 8.



Theorem 1 *Let $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ be an absolutely irreducible Galois representation where the characteristic p of $\mathbf{k}$ is greater than or equal to 5. Assume $Ad^0\bar{\rho}$ is an absolutely irreducible $\mathbf{k}[G_S]$ module, that $H^1(G_S/N, Ad^0\bar{\rho})$ and $H^1(G_S/N^d, (Ad^0\bar{\rho})^*)$ are trivial, and that $H^2(G_v, Ad^0\bar{\rho}) = 0$ for all $v \in S$. Finally suppose there is an element*

$$a \times b \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D}) \simeq Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{K}/\mathbf{Q})$$

such that a corresponds to an element in the (projective) image of $\bar{\rho}$ whose eigenvalues have ratio $t \in \mathbf{F_p^*}$, where $t \neq \pm 1$, and $b \in Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \to (\mathbf{Z}/p)^*$ maps to the element t. Let $r = dim_\mathbf{k} H^2(G_S, Ad^0\bar{\rho})$. Then there is a set of primes $Q = \{q_1, q_2, .., q_r\}$ disjoint from S and a representation $\rho : G_{S\cup Q} \to GL_2(W(\mathbf{k}))$ such that $\rho \equiv \bar{\rho}$ mod p.

While the above theorem is stated quite generally it is not immediately clear whether the hypotheses can actually be satisfied in a case of interest! The following theorem is a corollary of Theorem 1. Recall that Serre's weight, $k(\bar{\rho})$, is an invariant of $\bar{\rho}\mid_{G_p=Gal(\bar{\mathbf{Q}}_\mathbf{p}/\mathbf{Q_p})}$, and therefore makes sense for $\bar{\rho}$ even as well as odd.

Theorem 2 *Let $p \geq 7$. Assume the image of $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ contains $SL_2(\mathbf{k})$. Also assume if $l \in S$ and $l \neq p$ that $l \not\equiv \pm 1$ mod p, that $k(\bar{\rho}) \neq p-1$ or $2p$, and that $k(\bar{\rho}) \not\equiv 2$ mod $p+1$. Let $r = dim_\mathbf{k} H^2(G_S, Ad^0\bar{\rho})$. Then there is a set of primes $Q = \{q_1, q_2, .., q_r\}$ disjoint from S and a representation $\rho : G_{S\cup Q} \to GL_2(W(\mathbf{k}))$ such that $\rho \equiv \bar{\rho}$ mod p.*

The method is to deform $\bar{\rho}$ one step at a time from mod p^n to mod p^{n+1} as in [R1-3]. Such deformation questions have been considered in [Ma1], [BM], [B1-3], [Bö], and [Kh]. As obstructions to deformation problems lie in $H^2(G_S, Ad^0\bar{\rho})$ the exact sequence

$$0 \to Ш^2_S(Ad^0\bar{\rho}) \to H^2(G_S, Ad^0\bar{\rho}) \to \oplus_{v\in S} H^2(G_v, Ad^0\bar{\rho})$$

is extremely important. A typical approach for lifting to characteristic zero (for $\bar{\rho}$ not known to be modular) has been to work with explicit examples where $H^2(G_S, Ad^0\bar{\rho})$ or at least $Ш^2_S(Ad^0\bar{\rho})$ can be shown to be trivial. Here we assume the right hand term in the exact sequence is trivial. Thus $Ш^2_S(Ad^0\bar{\rho}) = H^2(G_S, Ad^0\bar{\rho})$ or more loosely 'all obstructions to deformation questions arise from class group problems'.

By the work of Poitou-Tate the kernel of $H^1(G_S, (Ad^0\bar{\rho})^*) \to \oplus_{v\in S} H^1(G_v, (Ad^0\bar{\rho})^*)$, which is denoted $Ш^1_S((Ad^0\bar{\rho})^*)$, and $Ш^2_S(Ad^0\bar{\rho})$ are dual. (The duality uses the fact that S contains the infinite place.) For us $Ш^1_S((Ad^0\bar{\rho})^*)$ will play the role of the dual Selmer group in [Wi] and [TW]. Following those papers, we carefully choose a set Q of auxiliary primes that annihilates $Ш^1_{S\cup Q}((Ad^0\bar{\rho})^*)$. It will then turn out that global obstructions to deformation problems, allowing ramification in $S\cup Q$, need only be studied locally at primes in Q. The method of [R1-3] can then be used to remove these local obstructions. We cannot guarantee that ρ in the theorems will be ramified at the primes in Q. We only know ρ exists and is unramified outside $S\cup Q$.

In this paper we study the cohomology of $Ad^0\bar{\rho}$ as opposed to that of $Ad\bar{\rho}$, the set of *all* 2×2 matrices over $\mathbf{k}$. For our purposes this means we are fixing the determinant of all deformations of $\bar{\rho}$ that we consider once and for all. Let χ denote the cyclotomic character, both mod p and in characteristic zero. We then have $det\bar{\rho} = \omega(\bar{\rho})\chi^{k(\bar{\rho})-1}$. Let $\tilde{\omega}$ be the Teichmüller lift of ω. For definiteness we may assume the fixed determinant of all our deformations is $\tilde{\omega}\chi^{k(\bar{\rho})-1}$.

The author would like to thank the referee for numerous helpful suggestions. In particular, the referee suggested the formulation and proof of Lemma 7 which leads to the corrected proof we give for Lemma 8.

Notations

p: A prime ≥ 5.
$\mathbf{k}$: A finite field of characteristic $p \geq 5$.
$\tilde{\mathbf{k}}$: A subfield of $\mathbf{k}$ which is the minimal field of definition of $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$.
$\bar{\mathbf{k}}$: A separable closure of $\mathbf{k}$.
$\hat{\mathbf{k}}$: A finite extension of $\mathbf{k}$.
$\mathbf{k}(\phi)$: The one dimensional space $\mathbf{k}$ with Galois action by the character ϕ.
$W(\mathbf{k})$: The ring of Witt vectors of $\mathbf{k}$.
S: A finite set of places (including p and ∞).
Q: A finite set of primes disjoint from S.
$\mathbf{Q_v}$: The completion of $\mathbf{Q}$ at the place v.
$\mathbf{Q_S}$: The maximal separable extension of $\mathbf{Q}$ unramified outside the places of S.
$G_{\mathbf{Q}}$: $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$.
G_S: $Gal(\mathbf{Q_S}/\mathbf{Q})$.
G_v: $Gal(\bar{\mathbf{Q}}_\mathbf{v}/\mathbf{Q_v})$.
I_v: The inertia subgroup of G_v.
$\mathbf{1}$: The two by two identity matrix over $W(\mathbf{k})$ or $W(\mathbf{k})/p^m$ for suitable m.
χ: The cyclotomic character.
$\bar{\rho}$: A continuous representation from G_S to $GL_2(\mathbf{k})$.
$k(\bar{\rho})$: Serre's weight for $\bar{\rho}$.
$Ad^0\bar{\rho}$: The trace zero two by two matrices over $\mathbf{k}$ with G_S action through $\bar{\rho}$ and by conjugation.
$(Ad^0\bar{\rho})^*$: The Cartier dual of $Ad^0\bar{\rho}$.
$\widetilde{Ad}^0\bar{\rho}$: A descent of $Ad^0\bar{\rho}$ to its minimal field of definition $\tilde{\mathbf{k}}$.
$(\widetilde{Ad}^0\bar{\rho})^*$: A descent of $(\widetilde{Ad}^0\bar{\rho})^*$ to its minimal field of definition $\tilde{\mathbf{k}}$.

2. Deformation theory

We give a short introduction to deformation theory. See [Ma1], [BM], [Bo1] and [Bo2] for details and more results.

Let $\bar{\pi} : H \to GL_d(\mathbf{k})$ be an absolutely irreducible continuous representation of a profinite group H. Suppose $H^1(H, Ad^0\bar{\pi})$ is finite dimensional. Let $\mathcal{C}$ be the category of Artinian local rings with residue field $\mathbf{k}$ where the morphisms are homomorphisms that induce the identity map on $\mathbf{k}$. Let R be in $\mathcal{C}$. We call two lifts γ_1 and γ_2 of $\bar{\pi}$ to $GL_n(R)$ strictly equivalent if $\gamma_1 = A\gamma_2 A^{-1}$ for some A congruent to the identity matrix modulo the maximal ideal m_R of R. We call a strict equivalence class of lifts of $\bar{\pi}$ to R a deformation of $\bar{\pi}$ to R.

Mazur studied the deformations of $\bar{\pi}$ and proved the following fundamental theorem in [Ma1].

Theorem A There is a complete local Noetherian ring R^{un} with residue field $\mathbf{k}$ and a continuous homomorphism $\tilde{\pi} : H \to GL_d(R^{un})$ such that

1) Reduction of $\tilde{\pi}$ modulo the maximal ideal of R^{un} gives $\bar{\pi}$.

2) For any ring R in $\mathcal{C}$ and any deformation γ of $\bar{\pi}$ to $GL_d(R)$ there is a unique homorphism $\phi : R^{un} \to R$ in $\mathcal{C}$ such that $\phi \circ \tilde{\pi} = \gamma$ as deformations.

Moreover, if $\bar{\pi}$ is not absolutely irreducible the statements hold except the ϕ in part 2 may not be unique. We call R^{un} the universal deformation ring associated to H and $\bar{\pi}$ in the absolutely irreducible case. We call R^{un} the versal ring associated to H and $\bar{\pi}$ otherwise. In either case we have the following fact.

Fact R^{un} is a quotient of $W(\mathbf{k})[[T_1, T_2, ...T_m]]$ where $m = dim_{\mathbf{k}} H^1(H, Ad^0\bar{\pi})$.

The elements of $H^1(H, Ad^0\bar{\pi})$ correspond to the deformations of $\bar{\pi}$ to $\mathbf{k}[\epsilon] = \mathbf{k}[X]/(X^2)$, the dual numbers of $\mathbf{k}$. Given $f \in H^1(H, Ad^0\bar{\pi})$ the corresponding deformations of $\bar{\pi}$ to the dual numbers is given by $\pi_f(\sigma) = (I + \epsilon f(\sigma))\bar{\pi}(\sigma)$.

Let π_n be a deformation of $\bar{\pi}$ to $GL_d(W(\mathbf{k})/p^n)$. We ask if π_n deforms to $GL_d(W(\mathbf{k})/p^{n+1})$. The obstruction to deforming π_n to $GL_d(W(\mathbf{k})/p^{n+1})$ lies in $H^2(H, Ad^0\bar{\pi})$. If this obstruction is trivial π_n deforms to some π_{n+1} and $pr \circ \pi_{n+1} = \pi_n$ where $pr : W(\mathbf{k})/p^{n+1} \to W(\mathbf{k})/p^n$ is the canonical projection. When such a lift exists one sees that $H^1(H, Ad^0\bar{\pi})$ acts on the set of deformations of π_n to $GL_d(W(\mathbf{k})/p^{n+1})$. For $f \in H^1(H, Ad^0\bar{\pi})$ the action is given by $(f.\pi_{n+1})(\sigma) = (I + p^n f(\sigma))(\pi_{n+1}(\sigma))$. If $\bar{\pi}$ is absolutely irreducible $H^1(H, Ad^0\bar{\pi})$ acts on the deformations of π_n to $GL_d(W(\mathbf{k})/p^{n+1})$ as a principal homogeneous space.

Mazur has also shown that modifications could be made so related functors with the *ordinary* restriction are also representable. Here H is a Galois group and we insist that when restricted to a suitable inertia group I_p that we only consider lifts π of $\bar{\pi}$ whose restriction to I is of the form $\begin{pmatrix} \psi & * \\ 0 & 1 \end{pmatrix}$. See [Ma1] and [Ma2] for details.

3. Local at q_i deformation theory

Let $q_i \not\equiv \pm 1 \bmod p$ (and $q_i \neq p$) be a prime (at which we eventually wish to allow ramification) and let $G_{q_i} = Gal(\bar{\mathbf{Q}}_{\mathbf{q_i}}/\mathbf{Q}_{\mathbf{q_i}})$. Suppose $\bar{\rho} : G_{q_i} \to GL_2(\mathbf{k})$ is unramified at q_i and $\bar{\rho}(Frob_{q_i})$ has (necessarily distinct) eigenvalues $q_i x_i$ and x_i. We need to study the deformation theory of this local

at q_i representation to understand the role the q_i play in Theorems 1 and 2. The characteristic polynomial $p(z)$ of $\bar{\rho}(Frob_{q_i})$ is $z^2 - x_i(q_i+1)z + q_i x_i^2$ has coefficients in $\mathbf{k}$. But q_i is a rational integer so its reduction mod p lies in $\mathbf{F_p}$ and is therefore in $\mathbf{k}$. Since $x_i(q_i+1) \in \mathbf{k}$ we see $x_i \in \mathbf{k}$ so $p(z)$ has distinct roots in $\mathbf{k}$. Thus we may assume $\bar{\rho}(Frob_{q_i}) = \begin{pmatrix} q_i x_i & 0 \\ 0 & x_i \end{pmatrix}$ for a suitable choice of basis of the two dimensional $\mathbf{k}$ vector space on which G_{q_i} acts.

Recall we denote the cyclotomic character by χ. By $\mathbf{k}(\phi)$ we mean the one dimensional $\mathbf{k}$ vector space with Galois action by the character ϕ and by $\mathbf{k}$ we denote the one dimensional $\mathbf{k}$ vector space with trivial Galois action.

Lemma 1 *Let q_i be as above. Then $H^2(G_{q_i}, Ad^0\bar{\rho})$ is one dimensional and $H^1(G_{q_i}, Ad^0\bar{\rho})$ is two dimensional.*

Proof: Note that with G_{q_i} action, $Ad^0\bar{\rho} \simeq \mathbf{k} \oplus \mathbf{k}(\chi) \oplus \mathbf{k}(\chi^{-1})$. Since we are assuming $q_i \not\equiv 1 \bmod p$ we see $H^0(G_{q_i}, Ad^0\bar{\rho})$ is one dimensional. Observe $(Ad^0\bar{\rho})^* \simeq \mathbf{k}(\chi) \oplus \mathbf{k} \oplus \mathbf{k}(\chi^2)$. Thus for $q_i \not\equiv \pm 1 \bmod p$ we see $H^0(G_{q_i}, (Ad^0\bar{\rho})^*)$ is one dimensional. By local duality $H^0(G_{q_i}, (Ad^0\bar{\rho})^*)$ is dual to $H^2(G_{q_i}, Ad^0\bar{\rho})$ which is thus one dimensional. The local Euler-Poincare characteristic gives the result for $H^1(G_{q_i}, Ad^0\bar{\rho})$.

We want to consider deformations of $\bar{\rho}$ to $W(\mathbf{k})/p^n$. As $q_i \neq p$, such deformations factor through the Galois group of the maximal tamely ramified extension $\mathbf{Q}^{\mathbf{t}}_{\mathbf{q_i}}$ over $\mathbf{Q}_{\mathbf{q_i}}$. This group is well understood. See Chaiptre II, §5.6 of [Se2]. Thus we may choose topological generators of the tame quotient of G_{q_i}, σ_{q_i} and τ_{q_i} subject to the relation $\sigma_{q_i}\tau_{q_i}\sigma_{q_i}^{-1} = \tau_{q_i}^{q_i}$. Recall τ_{q_i} topologically generates inertia and σ_{q_i} maps to Frobenius under the surjection $Gal(\mathbf{Q}^{\mathbf{t}}_{\mathbf{q_i}}/\mathbf{Q}_{\mathbf{q_i}}) \to Gal(\bar{\mathbf{F}}_{\mathbf{q_i}}/\mathbf{F}_{\mathbf{q_i}})$. Let $\tilde{x}_i \in W(\mathbf{k})$ be the Teichmüller lift of x_i.

We call a deformation (or a representation in this equivalence class) of $\bar{\rho}$ to $W(\mathbf{k})/p^n$ (allowing $n = \infty$ in the case of a deformation to $W(\mathbf{k})$) of our "desired form" if it is given by $\sigma_{q_i} \mapsto \begin{pmatrix} q_i\tilde{x}_i & 0 \\ 0 & \tilde{x}_i \end{pmatrix}$ and $\tau_{q_i} \mapsto \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. The images of σ_{q_i} and τ_{q_i} satisfy the relation $\sigma_{q_i}\tau_{q_i}\sigma_{q_i}^{-1} = \tau_{q_i}^{q_i}$. We want to deform this to $W(\mathbf{k})/p^{n+1}$.

Lemma 2 *A deformation of our "desired form" to $W(\mathbf{k})/p^n$ deforms to $W(\mathbf{k})/p^{n+1}$.*

Proof: One need only lift $*$ from mod p^n to mod p^{n+1} to get a deformation to mod p^{n+1} of the "desired form".

We give a basis for $H^1(G_{q_i}, Ad^0\bar{\rho})$. Recall that $\bar{\rho}(\sigma_{q_i}) = \begin{pmatrix} q_i x_i & 0 \\ 0 & x_i \end{pmatrix}$ and $\bar{\rho}(\tau_{q_i}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. A nontrivial unramified deformation to $\mathbf{k}[\epsilon]$ is given by

$\rho(\sigma_{q_i}) = \begin{pmatrix} q_i x_i & 0 \\ 0 & x_i \end{pmatrix} + \epsilon \begin{pmatrix} q_i x_i & 0 \\ 0 & -x_i \end{pmatrix}$ and $\rho(\tau_{q_i}) = \mathbf{1} + \epsilon \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Let $g \in G_{q_i}$ and let n_g be the image of g under the composite map $G_{q_i} \to \hat{\mathbf{Z}} \to \mathbf{Z}/p$. Then $r_{q_i}(g) = \begin{pmatrix} n_g & 0 \\ 0 & -n_g \end{pmatrix}$.

A nontrivial *ramified* deformation to the dual numbers is given by $\rho(\sigma_{q_i}) = \begin{pmatrix} q_i x_i & 0 \\ 0 & x_i \end{pmatrix} + \epsilon \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\rho(\tau_{q_i}) = \mathbf{1} + \epsilon \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. We see $\sigma_{q_i} \tau_{q_i} \sigma_{q_i}^{-1} = \tau_{q_i}^{q_i}$ holds. The corresponding cohomology class is given by $s_{q_i}(\sigma_{q_i}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $s_{q_i}(\tau_{q_i}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Clearly the images of r_{q_i} and s_{q_i} in $H^1(G_{q_i}, Ad^0\bar{\rho})$ are linearly independent and therefore they span the two dimensional space $H^1(G_{q_i}, Ad^0\bar{\rho})$. Note that both r_{q_i} and s_{q_i}, or more precisely their corresponding deformations to $\mathbf{k}[\epsilon]$, cut out $\mathbf{Z}/p$ extensions of $\mathbf{Q}_{\mathbf{q_i}}(\bar{\rho})$, the extension of $\mathbf{Q}_{\mathbf{q_i}}$ fixed by the kernel of $\bar{\rho}$. Any linear combination $ur_{q_i} + vs_{q_i}$ with $u, v \neq 0$ in $\mathbf{k}$ cuts out the unique $\mathbf{Z}/p \times \mathbf{Z}/p$ extension of $\mathbf{Q}_{q_i}(\bar{\rho})$.

Also note that for any deformation to mod $W(\mathbf{k})/p^n$, $n \geq 2$, of our "desired form", *acting on it by the cohomology class s_{q_i} leaves it in the "desired form"*. One sees this by noting

$$(\mathbf{1} + p^{n-1} s_{q_i}(\sigma_{q_i})) \begin{pmatrix} q_i \tilde{x}_i & 0 \\ 0 & \tilde{x}_i \end{pmatrix} = \begin{pmatrix} q_i \tilde{x}_i & 0 \\ 0 & \tilde{x}_i \end{pmatrix}$$

and

$$(\mathbf{1} + p^{n-1} s_{q_i}(\tau_{q_i})) \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * + p^{n-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \tilde{*} \\ 0 & 1 \end{pmatrix}.$$

We call a cohomology class that preserves the "desired form" *null*. If a cohomology class does not preserve the desired form we call it *nonnull*. Observe r_{q_i} is nonnull.

Proposition 1 *Let $\bar{\rho} : G_{q_i} \to GL_2(\mathbf{k})$ be unramified and given by $\bar{\rho}(\sigma_{q_i}) = \begin{pmatrix} q_i x_i & 0 \\ 0 & x_i \end{pmatrix}$ with $q_i \not\equiv \pm 1$ mod p. Fix $f \in H^1(G_{q_i}, Ad^0\bar{\rho})$ such that f and s_{q_i} are linearly independent. Let ρ_n be a deformation of $\bar{\rho}$ to mod p^n of the "desired form" and ρ_{n+1} be any deformation of ρ_n to mod p^{n+1}. Then there is an $\nu_{n+1} \in \mathbf{k}$ such that $(\nu_{n+1} f).\rho_{n+1}$ is of our "desired form." Thus $\bar{\rho}$ can be lifted to $W(\mathbf{k})$ one step at a time with adjustments made at each step only by a multiple of f. In particular, we may take for f any nonzero multiple of the unramified cohomology class r_{q_i}.*

Proof: Note that from the discussion in Section 2 we see ρ_{n+1} differs from the "desired form" by the action of *some* element $\nu_{n+1} f + \mu_{n+1} s_{q_i}$ of the two dimensional space $H^1(G_{q_i}, Ad^0\bar{\rho})$. That is, $(\nu_{n+1} f + \mu_{n+1} s_{q_i}).\rho_{n+1}$ is of the

"desired form". Since the one dimensional subspace of null cohomology classes preserves this form we see $(\nu_{n+1} f).\rho_{n+1}$ is of the "desired form".

Remark: One possibility is that our characteristic zero representation may have $\tau_{q_i} \mapsto \mathbf{1}$, that is it might be unramified.

4. Local at $l \neq p$ obstructions

Lemma 3 *$H^2(G_v, Ad^0\bar{\rho}) \neq 0$ if and only if $Ad^0\bar{\rho}$ has a one dimensional quotient on which G_v acts by the cyclotomic character χ.*

Proof: In this lemma v is any finite prime, including p. By local duality we see $H^2(G_v, Ad^0\bar{\rho}) \neq 0$ if and only if $H^0(G_v, (Ad^0\bar{\rho})^*) \neq 0$. This happens exactly when $(Ad^0\bar{\rho})^*$ has a G_v stable one dimensional subspace, that is when $Ad^0\bar{\rho}$ has a one dimensional quotient (by a G_v stable two dimensional subspace) on which G_v acts by χ.

The aim of this section is to prove the proposition below.

Proposition 2 *Let $p \geq 5$ and l be a prime such that $l \neq p$, $l \not\equiv \pm 1$ mod p. Suppose $\bar{\rho} : G_l \to GL_2(\mathbf{k})$ and the action of G_l on $Ad^0\bar{\rho}$ is ramified. Then $H^2(G_l, Ad^0\bar{\rho}) = 0$.*

Remark: We choose $p \geq 5$ as *all* primes (other than 3 itself) are congruent to ± 1 mod 3. While the conditions of Proposition 2 are sufficient they are not necessary for the conclusions. We have chosen these strong hypotheses because they are easy to state and verify.

Proof: We know $H^2(G_l, Ad^0\bar{\rho}) = 0$ if and only if $Ad^0\bar{\rho}$ does not have a one dimensional quotient (by a two dimensional G_l stable subspace) on which G_l acts by χ. As $l \neq p$ this action is unramified and as $l \not\equiv \pm 1$ mod p we see χ has order at least 3. Let $\tilde{G}$ and $\tilde{I}$ be the images of G_l and its inertia subgroup I_l under the composite map $G_l \to GL_2(\mathbf{k}) \to PGL_2(\mathbf{k})$.

We need the following lemma to prove the proposition.

Lemma 4 *If $[\tilde{G} : \tilde{I}] \leq 2$ then $Ad^0\bar{\rho}$ has no one dimensional quotient on which G_l acts by χ. Thus $H^2(G_l, Ad^0\bar{\rho}) = 0$ in such cases.*

Proof: The order of χ would have to be 1 or 2, i.e. $l \equiv \pm 1$ mod p. We are excluding these cases.

We recall the classification in [Di1] of two dimensional local mod p Galois representations. Note that we are reversing the roles of l and p in [Di1] and the classification is often only given up to a twist. Since $Ad^0\bar{\rho}$ as a $\mathbf{k}[G_l]$ module is insensitive to twists by $\mathbf{k}^*$-valued characters this does not affect our computations. We do not need to worry about possible difficulties

arising from scalar extensions associated to these twists or about the minimal field of definition of $Ad^0\bar{\rho}$ as $H^2(G_l, Ad^0\bar{\rho}) \otimes_{\mathbf{k}} \overline{\mathbf{k}} \simeq H^2(G_l, Ad^0\bar{\rho} \otimes_{\mathbf{k}} \overline{\mathbf{k}})$ where $\overline{\mathbf{k}}$ is a separable closure of $\mathbf{k}$. Thus we extend scalars and consider $Ad^0\bar{\rho}$ and (the representation space of) $\bar{\rho}$ as $\overline{\mathbf{k}}[G_l]$ module.

In his classification Diamond has four cases that he calls P, S, V and H. We recall these below under the hypotheses that $l \not\equiv \pm 1 \bmod p$ and $\bar{\rho}$ is ramified. We do not give all of Diamond's equivalent formulations of each case.

- P : $\bar{\rho}$ is twist equivalent to a representation of the form $\begin{pmatrix} \psi & 0 \\ 0 & 1 \end{pmatrix}$ for some ramified character ψ.
- S : $\bar{\rho}$ is twist equivalent to $\begin{pmatrix} \chi & u \\ 0 & 1 \end{pmatrix}$ where χ is the cyclotomic character and u is a not coboundary.
- V : $\tilde{I}$ is cyclic of order not divisible by p and $\tilde{G}$ is dihedral of twice that order.
- H : a) $\tilde{I}$ is dihedral of order $2l^r$ for some $r \geq 1$ and $\tilde{G}$ is dihedral of order dividing $4l^r$, or
  b) $l = 2$, $\tilde{I}$ (respectively $\tilde{G}$) is isomorphic to D_4 (respectively A_4), A_4 (respectively A_4), or A_4 (respectively S_4).

Proof of Proposition 2: In case V the hypotheses of Lemma 4 are satisfied so Proposition 2 holds in this case.

In case P we see $\bar{\rho}$ is a direct sum of the trivial character and a ramified character. One easily sees that as a $\overline{\mathbf{k}}[G_l]$ module $Ad^0\bar{\rho}$ becomes a direct sum of three one dimensional $\overline{\mathbf{k}}[G_l]$ modules. One of these is trivial and the other two have ramified G_l action. Thus $H^2(G_l, Ad^0\bar{\rho})$ is nontrivial only if χ is the trivial character, that is $l \equiv 1 \bmod p$. We are excluding this case.

In case S we have $\bar{\rho} = \begin{pmatrix} \chi & u \\ 0 & 1 \end{pmatrix}$. Then $Ad^0\bar{\rho}$ has a unique one dimensional quotient and G_l acts on this quotient by χ^{-1}. Since $l \not\equiv -1 \bmod p$ we know $\chi^{-1} \neq \chi$. Thus $H^2(G_l, Ad^0\bar{\rho}) = 0$ in this case.

It remains to consider case H. Here the hypotheses of Lemma 2 are satisfied except when $l = 2$, $\tilde{I} \simeq D_4$ and $\tilde{G} \simeq A_4$. By Lemma 3 we know that for $H^2(G_l, Ad^0\bar{\rho})$ *not* to be trivial there must be a one dimensional quotient of $Ad^0\bar{\rho}$ on which G_l acts via χ. This quotient must be by a two dimensional G_l stable subspace. Since $\#\tilde{G} = 12$ and $p \geq 5$ we see that G_l acts on $Ad^0\bar{\rho}$ via a quotient of order prime to p. By the theory of representations of finite groups of order prime to the characteristic we see $Ad^0\bar{\rho}$ is a semisimple representation of A_4. Since A_4 acts faithfully on $Ad^0\bar{\rho}$ we easily see $Ad^0\bar{\rho}$ is an irreducible three dimensional representation

of A_4. Thus there are no two dimensional invariant subspaces so we must have $H^2(G_l, Ad^0\bar{\rho}) = 0$ in this last case.

Proposition 2 is now proved.

5. Local at p obstructions

Recall that Serre attaches in [Se1] a weight $k(\bar{\rho})$ to a mod p Galois representation that depends only on its restriction to I, the inertia subgroup of G_p. (We use I for inertia in this section to be consistent with [Se1]). This definition therefore applies to $\bar{\rho}$ even as well as odd.

Proposition 3 *Let $p \geq 5$ and $\bar{\rho} : G_p \to GL_2(\mathbf{k})$ be given. If $k(\bar{\rho}) \neq p-1$ or $2p$ and $k(\bar{\rho}) \not\equiv 2$ mod $(p+1)$ then $H^2(G_p, Ad^0\bar{\rho}) = 0$.*

Remark: As before the hypotheses are sufficient for the conclusion but not necessary. See for example Section 11 of [Ma3]. As in Section 4 (of this paper) we need not worry about possible scalar extensions since such extensions do not change the *dimension* of the cohomology groups. Thus we consider $Ad^0\bar{\rho}$ as a $\bar{\mathbf{k}}[G_p]$ module.

Proof: Following Section 2 of [Se1] we will separate the cases when inertia acts (through $\bar{\rho}$) via characters of level two and characters of level one. By Lemma 3, to show $H^2(G_p, Ad^0\bar{\rho}) = 0$, it suffices to show that $Ad^0\bar{\rho}$ has no one dimensional quotient on which G_p acts via χ. Here χ is ramified. We will study the $\bar{\mathbf{k}}[I]$ module $Ad^0\bar{\rho}$ and show that if the conditions of Proposition 3 are satisfied then $Ad^0\bar{\rho}$ has no one dimensional quotient on which I acts via χ.

If inertia acts through $\bar{\rho}$ via characters of level two, then by Section 2.2 of [Se1] we see $\bar{\rho}\mid_{G_p}$ is irreducible and $\bar{\rho}\mid_I = \begin{pmatrix} \phi & 0 \\ 0 & \phi^p \end{pmatrix}$ where ϕ is a character of level two. Thus as a $\bar{\mathbf{k}}[I]$ module $Ad^0\bar{\rho}$ decomposes as a direct sum of 3 one dimensional spaces, one with trivial I action, one with I action via ϕ^{p-1} and one with I action via ϕ^{1-p}. To show $H^2(G_p, Ad^0\bar{\rho}) = 0$ it suffices to show neither ϕ^{p-1} nor ϕ^{1-p} equal χ.

From [Se1] we see that we can write $\phi = \psi^{a+pb}$ where ψ is a fundamental character of level two and $0 \leq a, b \leq p-1$. Thus $\phi^{p-1} = \psi^{a(p-1)+b(p^2-p)}$. Recall $\chi = \psi^{p+1}$ and that ψ has order p^2-1.

Lemma 5 *With ϕ as above, neither ϕ^{p-1} nor ϕ^{1-p} equal χ. Therefore if I acts (through $\bar{\rho}^{ss}$) via characters of level two then $H^2(G_p, Ad^0\bar{\rho}) = 0$.*

Proof: Setting $\phi^{p-1} = \chi$ we see $\psi^{a(p-1)+b(p^2-p)} = \psi^{p+1}$ or equivalently $a(p-1)+b(p^2-p) \equiv p+1 \bmod (p^2-1)$. This becomes $(a-b)(p-1) \equiv p+1 \bmod (p^2-1)$. Since $p-1$ divides p^2-1 this last equation holds mod $(p-1)$ and becomes $0 \equiv 2 \bmod (p-1)$ so $p = 3$. We are excluding this case. The computation for ϕ^{1-p} is similar.

We now turn to the case where inertia acts through $\bar{\rho}$ via characters of level one.

If wild inertia acts trivially, $\bar{\rho}\mid_I = \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$ where $0 \le a \le b \le p-2$. Keeping in mind $p \ge 5$ we see $Ad^0\bar{\rho}$ has a one dimensional quotient on which I acts by χ only if $b-a=1$. In that case, by Section 2.3.2 of [Se1] we have $k(\bar{\rho}) = 1+pa+b = 2+a(p+1)$. We are excluding such weights from our consideration. Note if $\bar{\rho}$ is unramified at p then $a=b=0$ and Serre *defines* $k(\bar{\rho})$ to be p.

If wild inertia acts nontrivially, $\bar{\rho}\mid_I = \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$ where $0 \le \alpha \le p-2$ and $1 \le \beta \le p-1$ and $\bar{\rho}\mid_I$ is a nontrivial extension class. One easily sees that $Ad^0\bar{\rho}$ has a one dimensional quotient on which I acts by χ if and only if $\chi^{\alpha-\beta} = \chi$, that is if and only if $\alpha - \beta \equiv 1 \bmod (p-1)$. (Recall χ has order $p-1$). From the bounds on α and β we see $-(p-1) \le \alpha-\beta \le p-3$ so $\alpha-\beta = 1$ or $-(p-2)$. In the first case $\alpha = \beta+1$ so following [Se1] $k(\bar{\rho}) = 1+p\beta+\beta+1 = 2+\beta(p+1)$. In the second case $\beta = p-2$ or $p-1$ so $\alpha = 0$ or 1 respectively and $k(\bar{\rho}) = p-1$ or $2p$ respectively. (Recall $p \ne 3$.) As we have excluded these cases Proposition 3 is now proved.

For the lemma below we treat $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ as $\mathbf{k}[G_p]$ and $\mathbf{k}[I]$ modules. We also will extend scalars to the quadratic extension $\hat{\mathbf{k}}$ of $\mathbf{k}$ to diagonalize $\bar{\rho}\mid_I$ as necessary.

Lemma 6 *$Ad^0\bar{\rho} \not\simeq (Ad^0\bar{\rho})^*$ as $\mathbf{F_p}[G_p]$ modules.*

Proof: Recall we are assuming $p \ge 5$. In particular we know $p \ne 2$. It suffices to show $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are not isomorphic as $\mathbf{F_p}[I]$ modules.

Consider first the case where $\bar{\rho}$ acts through I via fundamental characters of level one. We study $Ad^0\bar{\rho}^{ss}$, the semisimplification of $Ad^0\bar{\rho}$ as a $\mathbf{F_p}[I]$ module. One easily sees $(Ad^0\bar{\rho})^{ss} \simeq \mathbf{k} \oplus \mathbf{k}(\chi^m) \oplus \mathbf{k}(\chi^{-m})$ as $\mathbf{k}[I]$ modules for some integer m. Thus $((Ad^0\bar{\rho})^*)^{ss} \simeq \mathbf{k}(\chi) \oplus \mathbf{k}(\chi^{1-m}) \oplus \mathbf{k}(\chi^{1+m})$. As $p \ne 2$ it is easy to see these semisimplifications are not isomorphic as $\mathbf{k}[I]$ modules. Since $\mathbf{k}$ is finite over $\mathbf{F_p}$, counting $\mathbf{F_p}$ eigenspaces shows $(Ad^0\bar{\rho})^{ss}$ and $((Ad^0\bar{\rho})^*)^{ss}$ are not isomorphic as $\mathbf{F_p}[I]$ modules. Thus $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are not isomorphic as $\mathbf{F_p}[G_p]$ modules.

Suppose now I acts via character of level two. We know that (after a possible quadratic extension of scalars to a field $\hat{\mathbf{k}}$) that $\bar{\rho}\mid_I = \begin{pmatrix} \psi^{a+pb} & 0 \\ 0 & \psi^{b+pa} \end{pmatrix}$ so

$$Ad^0\bar{\rho} \simeq \hat{\mathbf{k}} \oplus \hat{\mathbf{k}}(\psi^{(p-1)(b-a)}) \oplus \hat{\mathbf{k}}(\psi^{(p-1)(a-b)})$$

as $\hat{\mathbf{k}}[I]$ modules. We see

$$(Ad^0\bar{\rho})^* \simeq \hat{\mathbf{k}}(\chi) \oplus \hat{\mathbf{k}}(\chi\psi^{(p-1)(a-b)}) \oplus \hat{\mathbf{k}}(\chi\psi^{(p-1)(b-a)})$$

as $\hat{\mathbf{k}}[I]$ modules. If the $\mathbf{k}[G_p]$ modules $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are isomorphic as $\mathbf{F_p}[G_p]$ modules we would necessarily have that the $\hat{\mathbf{k}}[G_p]$ modules $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are isomorphic as $\mathbf{F_p}[G_p]$ modules and thus as $\mathbf{F_p}[\mathbf{I}]$ modules. Without loss of generality we would then have $\chi = \psi^{(p-1)(a-b)}$. Thus $Ad^0\bar{\rho} \simeq \hat{\mathbf{k}} \oplus \hat{\mathbf{k}}(\chi) \oplus \hat{\mathbf{k}}(\chi^{-1})$ as $\hat{\mathbf{k}}[I]$ modules. Since $p \neq 2$ this is not self-dual as a $\hat{\mathbf{k}}[I]$ module. Counting $\mathbf{F_p}$ eigenspaces we see the $\hat{\mathbf{k}}$ modules $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are not isomorphic as $\mathbf{F_p}[I]$ modules. Thus $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ are not isomorphic as $\mathbf{F_p}[G_p]$ modules. The lemma is now proved.

6. Descents

In the introduction we alluded to the fact that the minimal field of definition of the three dimensional representation of G_S on $Ad^0\bar{\rho}$ could conceivably be smaller than $\mathbf{k}$. We have the following fact which is Lemma 6.13 of [DS].

Fact Let $\tau : G \to GL_n(\mathbf{k})$ be a semisimple representation. Let $\tilde{\mathbf{k}}$ be the subfield of $\mathbf{k}$ generated be the coefficients of the characteristic polynomials of elements of G. Then τ is realizable over $\tilde{\mathbf{k}}$, i.e. it is isomorphic to a semisimple representation $\phi : G \to GL_n(\tilde{\mathbf{k}})$ and $\phi \otimes_{\tilde{\mathbf{k}}} \mathbf{k} \simeq \tau$. The descent to $\tilde{\mathbf{k}}$ is semisimple and unique up to non-canonical isomorphism.

I am grateful to the referee for pointing out the following lemma and its proof.

Lemma 7 *Let $\tau : G \to GL_n(\tilde{\mathbf{k}})$ be absolutely irreducible with minimal field of definition $\tilde{\mathbf{k}}$. Let $V = \tilde{\mathbf{k}}^n$ be the representation space. Suppose W is a nonzero $\mathbf{F_p}$ subspace of V stable under the action of G. Then $W = V$.*

Proof: First we show V is a semisimple $\mathbf{F_p}[G]$ module. Let V_0 be a nonzero irreducible G stable $\mathbf{F_p}$ subspace of V. If $V_0 = V$ then V is a simple $\mathbf{F_p}[G]$ module. Assume $V_0 \neq V$. Since V_0 is G stable so is its $\tilde{\mathbf{k}}$ span. Since τ is irreducible we see the $\tilde{\mathbf{k}}$ span of V_0 is all of V. For $\alpha \in \tilde{\mathbf{k}}$, $\alpha \neq 0$, consider αV_0, the $\mathbf{F_p}$ subspace of V consisting of all multiples of elements of V_0 by α. Clearly αV_0 is G stable and an irreducible $\mathbf{F_p}[G]$ module. Note also that for $\alpha, \beta \in \tilde{\mathbf{k}}$, $\alpha, \beta \neq 0$, we have αV_0 and βV_0 intersect trivially or they are equal. Since the $\tilde{\mathbf{k}}$ span of V_0 is all of V we see V is contained in the span of simple $\mathbf{F_p}[G]$ modules and therefore V itself is a semisimple $\mathbf{F_p}[G]$ module.

To prove the lemma it suffices to show V is irreducible as an $\mathbf{F_p}[G]$ module. To show this it is enough to show the injection $\tilde{\mathbf{k}} \to End_{\mathbf{F_p}[G]}(V)$ is an isomorphism. For if V were a direct sum of more than one irreducible constituent $End_{\mathbf{F_p}[G]}(V)$ would contain noninvertible elements.

We will show that $[\tilde{\mathbf{k}}:\mathbf{F_p}] = dim_{\mathbf{F_p}}(End_{\mathbf{F_p}[G]}(V))$ by extending scalars and checking the equivalent statement $[\tilde{\mathbf{k}} : \mathbf{F_p}] = dim_{\tilde{\mathbf{k}}}\left(End_{\tilde{\mathbf{k}}[G]}(\tilde{\mathbf{k}} \otimes_{\mathbf{F_p}} V)\right) = dim_{\tilde{\mathbf{k}}}\left(End_{\tilde{\mathbf{k}}[G]}((\tilde{\mathbf{k}} \otimes_{\mathbf{F_p}} \tilde{\mathbf{k}}) \otimes_{\tilde{\mathbf{k}}} V)\right)$.

Note that $\tilde{\mathbf{k}} \otimes_{\mathbf{F_p}} \tilde{\mathbf{k}} \simeq \prod_s \tilde{\mathbf{k}}$ where the isomorphism is as left $\tilde{\mathbf{k}}$ algebras and the product is indexed by the elements $s \in Gal(\tilde{\mathbf{k}}/\mathbf{F_p})$ and the sth factor has right $\tilde{\mathbf{k}}$ algebra structure via the automorphism s of $\tilde{\mathbf{k}}$. Thus $End_{\tilde{\mathbf{k}}[G]}(\tilde{\mathbf{k}} \otimes_{\mathbf{F_p}} V) = End_{\tilde{\mathbf{k}}[G]}(\prod_s V_s)$ where V_s is the absolutely irreducible $\tilde{\mathbf{k}}[G]$ module obtained from V by base change by s. Note $End_{\tilde{\mathbf{k}}[G]} V_s = \tilde{\mathbf{k}}$.

We claim that for s, t distinct in $Gal(\tilde{\mathbf{k}}/\mathbf{F_p})$ that V_s and V_t are *not* isomorphic as $\tilde{\mathbf{k}}[G]$ modules so $Hom_{\tilde{\mathbf{k}}[G]}(V_s, V_t) = 0$. Since $\tilde{\mathbf{k}}$ is the minimal field of definition of τ and st^{-1} is not trivial in $Gal(\tilde{\mathbf{k}}/\mathbf{F_p})$ there must be some $g \in G$ so that the characteristic polynomials over $\tilde{\mathbf{k}}$ of the action of g on V_s and V_t are distinct. The irreducible $\tilde{\mathbf{k}}[G]$ modules V_s and V_t are thus not isomorphic so $End_{\tilde{\mathbf{k}}[G]}(\tilde{\mathbf{k}} \otimes_{\mathbf{F_p}} V) = \prod_s End_{\tilde{\mathbf{k}}[G]}(V_s) = \prod_s \tilde{\mathbf{k}}$ which has dimension $\#Gal(\tilde{\mathbf{k}}/\mathbf{F_p}) = [\tilde{\mathbf{k}} : \mathbf{F_p}]$ over $\tilde{\mathbf{k}}$ as desired.

Denote by $\widetilde{Ad}^0\bar{\rho}$ and $(\widetilde{Ad}^0\bar{\rho})^*$ descents of $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ to $\tilde{\mathbf{k}}$.

Lemma 8 *Suppose $\bar{\rho}: H \to GL_2(\mathbf{k})$ is absolutely irreducible and that $\widetilde{Ad}^0\bar{\rho}$ is absolutely irreducible as a representation of H. Let $f \in H^1(H, \widetilde{Ad}^0\bar{\rho})$ be non-zero. Let $\rho : H \to GL_2(\mathbf{k}[\epsilon])$ be the deformation to the dual numbers corresponding to f. Let A and B be the kernels of $\bar{\rho}$ and ρ respectively. Suppose also that $H^1(H/A, \widetilde{Ad}^0\bar{\rho})$ is trivial. In terms of the choice of f, the $\mathbf{F_p}[H]$ module A/B can be naturally endowed with a structure of a $\tilde{\mathbf{k}}$ vector space so that $\widetilde{Ad}^0\bar{\rho} = (A/B) \otimes_{\tilde{\mathbf{k}}} \mathbf{k}$ as $\mathbf{k}[H]$ modules. In particular A/B is a simple $\mathbf{F_p}[H]$ module and has cardinality $(\#\tilde{\mathbf{k}})^3$.*

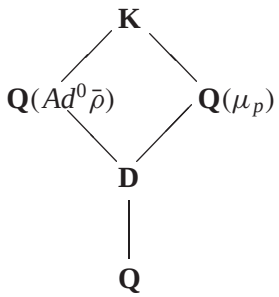
Proof: Consider the inflation-restriction sequence

$$0 \to H^1(H/A, \widetilde{Ad}^0\bar{\rho}) \to H^1(H, \widetilde{Ad}^0\bar{\rho}) \to H^1(A, \widetilde{Ad}^0\bar{\rho})^{H/A}.$$

Since $f \neq 0$ and $H^1(H/A, \widetilde{Ad}^0\bar{\rho}) = 0$ we see see that $f \in H^1(H, \widetilde{Ad}^0\bar{\rho})$ maps to a nonzero element $\tilde{f}$ of $H^1(A, \widetilde{Ad}^0\bar{\rho})^{H/A} = Hom_H(A, \widetilde{Ad}^0\bar{\rho})$. The last equality follows because A acts trivially on $\widetilde{Ad}^0\bar{\rho}$. So f gives rise to a nonzero H equivariant map $\tilde{f} : A \to \widetilde{Ad}^0\bar{\rho}$. That the kernel of $\tilde{f}$ is B follows from the explicit description of the correspondance between elements of $H^1(H, \widetilde{Ad}^0\bar{\rho})$ and deformations of $\bar{\rho}$ to the dual numbers described in Section 2. Let $\tilde{\mathbf{k}}$ be the minimal field of definition of the representation of H on $\widetilde{Ad}^0\bar{\rho}$. We know the image of A/B under $\tilde{f}$ is a nonzero $\mathbf{F_p}[H]$ submodule of $\widetilde{Ad}^0\bar{\rho}$. By Lemma 7 the image equals $\widetilde{Ad}^0\bar{\rho}$ and we are done.

7. Global methods

We recall our set-up for Theorem 1 in preparation for its proof. We have $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ a continuous absolutely irreducible Galois representation where $\mathbf{k}$ is a finite field of characteristic ≥ 5. We assume $Ad^0\bar{\rho}$ is absolutely irreducible. This necessarily implies that $(Ad^0\bar{\rho})^*$ is an absolutely irreducible $\mathbf{k}[G_S]$ module as well. We assume $H^1(G_S/N, Ad^0\bar{\rho})$ and $H^1(G_S/N^d, (Ad^0\bar{\rho})^*)$ are trivial where N and N^d are the maximal subgroups of G_S that act trivially on $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ respectively. Let $\mathbf{Q}(Ad^0\bar{\rho})$ and $\mathbf{Q}(Ad^0\bar{\rho}^*)$ be the fixed fields of N and N^d. Put $\mathbf{D} = \mathbf{Q}(Ad^0\bar{\rho}) \cap \mathbf{Q}(\mu_p)$ and $\mathbf{K} = \mathbf{Q}(Ad^0\bar{\rho})\mathbf{Q}(\mu_p)$. We assume that $H^2(G_v, Ad^0\bar{\rho}) = 0$ for all $v \in S$. Also recall there exists an element $a \times b \in Gal(\mathbf{K}/\mathbf{Q})$ as described in Theorem 1.



We refer the reader to [Ha] and [Mi] for the main theorems of global Galois cohomology. Recall $\widetilde{Ad}^0\bar{\rho}$ and $(\widetilde{Ad}^0\bar{\rho})^*$ are decents of $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ to $\tilde{\mathbf{k}}$. Henceforth we study these objects. The truth of our cohomological assumptions for $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ implies the truth of the corresponding statements for $\widetilde{Ad}^0\bar{\rho}$ and $(\widetilde{Ad}^0\bar{\rho})^*$.

Studying the exact sequence

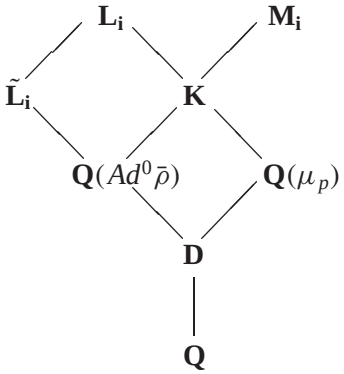
$$0 \to Ш^2_S(\widetilde{Ad}^0\bar{\rho}) \to H^2(G_S, \widetilde{Ad}^0\bar{\rho}) \to \oplus_{v\in S} H^2(G_v, \widetilde{Ad}^0\bar{\rho})$$

we see we have an isomorphism $Ш^2_S(\widetilde{Ad}^0\bar{\rho}) \to H^2(G_S, \widetilde{Ad}^0\bar{\rho})$. Let r be the common $\tilde{\mathbf{k}}$ dimension of these cohomology groups. Recall that by global Poitou-Tate duality $Ш^2_S(\widetilde{Ad}^0\bar{\rho})$ is dual to $Ш^1_S((\widetilde{Ad}^0\bar{\rho})^*)$, the kernel of the map $H^1(G_S, (\widetilde{Ad}^0\bar{\rho})^*) \to \oplus_{v\in S} H^1(G_v, (\widetilde{Ad}^0\bar{\rho})^*)$. Also using global duality and the global Euler characteristic we find $H^1(G_S, \widetilde{Ad}^0\bar{\rho})$ is r or $r+2$ dimensional as $\bar{\rho}$ is even or odd. Let $\{g_1, g_2, .., g_r\}$ be a basis of $Ш^1_S((\widetilde{Ad}^0\bar{\rho})^*)$ and $\{f_1, f_2, ..., f_r\}$ be linearly independent in $H^1(G_S, \widetilde{Ad}^0\bar{\rho})$. Our plan, is for each i, $1 \leq i \leq r$, to find a prime $q_i \notin S$ such that

- $q_i \not\equiv \pm 1 \bmod p$ and $\bar{\rho}(Frob_{q_i})$ has eigenvalues with ratio q_i. By the remarks at the beginning of Section 3 the distinct eigenvalues of $\bar{\rho}(Frob_{q_i})$ will lie in $\mathbf{k}$.
- $g_i\,|_{G_{q_i}} \neq 0$.
- $f_i\,|_{G_{q_i}} \neq 0$ is unramified and therefore nonnull at q_i by the results of Section 3.
- For $i \neq j$ we have $f_i\,|_{G_{q_j}} = 0$ and $g_i\,|_{G_{q_j}} = 0$.

Letting $Q = \{q_1, q_2, .., q_r\}$ we will then have $Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*)$ is trivial and by global duality that $Ш^2_{S\cup Q}(\widetilde{Ad}^0\bar{\rho}) = 0$. The map $H^2(G_{S\cup Q}, \widetilde{Ad}^0\bar{\rho}) \to \oplus_{v\in S\cup Q} H^2(G_v, \widetilde{Ad}^0\bar{\rho})$ is therefore injective. Since $(\widetilde{Ad}^0\bar{\rho})^*$ is assumed absolutely irreducible we have $H^0(G_S, (\widetilde{Ad}^0\bar{\rho})^*) = 0$ and the H^2 restriction map above is surjective by Chapter I, Theorem 4.10 of [Mi]. Since $H^2(G_v, \widetilde{Ad}^0\bar{\rho})$ is assumed trivial for $v \in S$ the map $H^2(G_{S\cup Q}, \widetilde{Ad}^0\bar{\rho}) \to \oplus_{v\in Q} H^2(G_v, \widetilde{Ad}^0\bar{\rho})$ is an isomorphism. *Thus obstructions to deformation problems for $\bar{\rho}$ with ramification in $S \cup Q$ need only be analyzed at exactly the primes in Q*. But for each q_i we have, by our choice of the q_i, a nonnull cohomology class in $H^1(G_S, \widetilde{Ad}^0\bar{\rho})$ available, namely f_i. We use these as in Proposition 1 to at each stage put the deformation in our "desired form" at q_i. Since $f_i\,|_{G_{q_j}} = 0$ for $i \neq j$ adjusting by f_i will not change the deformation at q_j.

The idea of seeking the set Q to annihilate $Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*)$ comes from the work of [Wi] and [TW]. However, unlike the situation in [Wi] and [TW] our auxiliary primes cannot be congruent to 1 mod p. Had we chosen them so the f_i would have been *null* for q_i. Thus f_i could not be used to bring the local deformation problem at q_i to an unobstructed form. (The 'shape' of the local at q_i deformation theory for $q_i \equiv 1 \bmod p$ is different than that given in Section 3. See the lemma in the appendix of [TW].) Chebotarev's theorem will provide us with the q_i.



Recall N and N^d are normal subgroups of G_S that fix $\mathbf{Q}(Ad^0\bar{\rho})$ and $\mathbf{Q}((Ad^0\bar{\rho})^*)$ respectively.

Lemma 9
1) Let $\tilde{f}_i$ be the image of f_i in $H^1(N, \widetilde{Ad}^0\bar{\rho})^{G_S/N} = Hom_{G_S}(N, \widetilde{Ad}^0\bar{\rho})$. The kernel of $\tilde{f}_i$ fixes a field $\tilde{\mathbf{L}}_\mathbf{i} \subseteq \mathbf{Q_S}$ Galois over $\mathbf{Q}$ with $Gal(\tilde{\mathbf{L}}_\mathbf{i}/\mathbf{Q}(Ad^0\bar{\rho}))$ isomorphic to the $\tilde{\mathbf{k}}[G_S]$ module $\widetilde{Ad}^0\bar{\rho}$. The exact sequence

$$1 \to Gal(\tilde{\mathbf{L}}_\mathbf{i}/\mathbf{Q}(Ad^0\bar{\rho})) \to Gal(\tilde{\mathbf{L}}_\mathbf{i}/\mathbf{Q}) \to Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{Q}) \to 1$$

splits.

2) Let $\tilde{g}_i$ be the image of g_i in $H^1(N^d, (\widetilde{Ad}^0\bar{\rho})^*)^{G_S/N^d} = Hom_{G_S}(N^d, (\widetilde{Ad}^0\bar{\rho})^*)$. The composite of the field fixed by the kernel of $\tilde{g}_i$ and $\mathbf{K}$ is a field $\mathbf{M_i} \subseteq \mathbf{Q_S}$ Galois over $\mathbf{Q}$ with $Gal(\mathbf{M_i}/\mathbf{K})$ isomorphic to the $\tilde{\mathbf{k}}[G_S]$ module $(\widetilde{Ad}^0\bar{\rho})^*$. The sequence

$$1 \to Gal(\mathbf{M_i}/\mathbf{K}) \to Gal(\mathbf{M_i}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

splits.

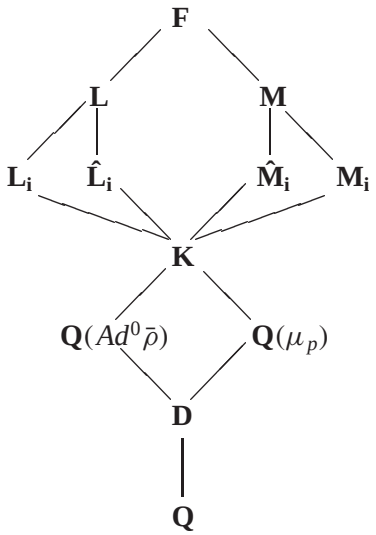
Proof: Recall $H^1(G_S/N, \widetilde{Ad}^0\bar{\rho})$ is assumed trivial, N acts trivially on $\widetilde{Ad}^0\bar{\rho}$, and $\widetilde{Ad}^0\bar{\rho}$ is an absolutely irreducible $\mathbf{k}[G_S]$ module. Consider the inflation-restriction sequence

$$0 \to H^1(G_S/N, (\widetilde{Ad}^0\bar{\rho})^N) \to H^1(G_S, \widetilde{Ad}^0\bar{\rho}) \to H^1(N, \widetilde{Ad}^0\bar{\rho})^{G_S/N} \to H^2(G_S/N, (\widetilde{Ad}^0\bar{\rho})^N).$$

Then $f_i \in H^1(G_S, \widetilde{Ad}^0\bar{\rho})$ maps to non-zero element $\tilde{f}_i$ of $H^1(N, \widetilde{Ad}^0\bar{\rho})^{G_S/N} = Hom_{G_S}(N, \widetilde{Ad}^0\bar{\rho})$ as desired. The image of $\tilde{f}_i$ is a nonzero $\mathbf{F_p}[G_S]$ submodule of $\widetilde{Ad}^0\bar{\rho}$. The map $\tilde{f}_i : N \to \widetilde{Ad}^0\bar{\rho}$ is surjective by Lemma 8. Let $\tilde{\mathbf{L}}_\mathbf{i}$ be the fixed field of the kernel of $\tilde{f}_i$. Observe $Gal(\tilde{\mathbf{L}}_\mathbf{i}/\mathbf{Q}(Ad^0\bar{\rho}))$ inherits a $\tilde{\mathbf{k}}$ structure from $\widetilde{Ad}^0\bar{\rho}$. The sequence splits because $\tilde{f}_i$ maps to zero in $H^2(G_S/N, \widetilde{Ad}^0\bar{\rho})$ by exactness.

For the second part we note $N^d \supseteq Gal(\mathbf{Q_S}/\mathbf{K})$ and $H^1(G_S/N^d, (\widetilde{Ad}^0\bar{\rho})^*)$ is assumed trivial. Replace $Ad^0\bar{\rho}$ and N by $(Ad^0\bar{\rho})^*$ and N^d in the exact sequence above. If the fixed field of N^d is not $\mathbf{K}$ let $\mathbf{M_i}$ be the composite of $\mathbf{K}$ and the field fixed by the kernel of $\tilde{g}_i$.

Let $\mathbf{L_i}$ be the composite $\tilde{\mathbf{L}}_\mathbf{i}\mathbf{K}$. Note $[\mathbf{L_i} : \mathbf{K}] = [\tilde{\mathbf{L}}_\mathbf{i} : \mathbf{Q}(Ad^0\bar{\rho})] = (\#\tilde{\mathbf{k}})^3$ as $[\mathbf{K} : \mathbf{Q}(Ad^0\bar{\rho})] = [\mathbf{Q}(\mu_p) : \mathbf{D}]$ is prime to p. Let $\hat{\mathbf{L}}_\mathbf{j}$ be the composite of all the $\mathbf{L_i}$ except $\mathbf{L_j}$. Define $\hat{\mathbf{M}}_\mathbf{j}$ similarly. Let $\mathbf{L}$ be the composite of all the $\mathbf{L_i}$ and $\mathbf{M}$ the composite of all the $\mathbf{M_i}$. Let $\mathbf{F} = \mathbf{LM}$.



Lemma 10 *1)* $\mathbf{L_i} \cap \hat{\mathbf{L}}_\mathbf{i} = \mathbf{K}$.
2) $\mathbf{M_i} \cap \hat{\mathbf{M}}_\mathbf{i} = \mathbf{K}$
3) $\mathbf{L} \cap \mathbf{M} = \mathbf{K}$.

Proof: Recall $Gal(\tilde{\mathbf{L}}_\mathbf{i}/\mathbf{Q}(Ad^0\bar{\rho})) \simeq Gal(\mathbf{L_i}/\mathbf{K}) \simeq \widetilde{Ad}^0\bar{\rho}$ as $\tilde{\mathbf{k}}[G_S]$ modules by Lemma 9. Since $\widetilde{Ad}^0\bar{\rho}$ is a simple $\mathbf{F_p}[G_S]$ module and the $\mathbf{L_i}$ and $\hat{\mathbf{L}}_\mathbf{i}$ are Galois over $\mathbf{Q}$ we see $\mathbf{L_i} \cap \hat{\mathbf{L}}_\mathbf{i} = \mathbf{L_i}$ or $\mathbf{K}$. If the intersection is $\mathbf{L_i}$ we would have $\mathbf{L_i} \subseteq \hat{\mathbf{L}}_\mathbf{i}$. Suppose this happens. Then, as a $\tilde{\mathbf{k}}[G_S]$ module, $Gal(\mathbf{L}/\mathbf{K})$ has at most $r-1$ copies of $\widetilde{Ad}^0\bar{\rho}$ in its Jordan-Hölder sequence. Consider the inflation-restriction sequence

$$0 \to H^1(Gal(\mathbf{K}/\mathbf{Q}), (\widetilde{Ad}^0\bar{\rho})^{Gal(\mathbf{L}/\mathbf{K})}) \to H^1(Gal(\mathbf{L}/\mathbf{Q}), \widetilde{Ad}^0\bar{\rho}) \to H^1(Gal(\mathbf{L}/\mathbf{K}), \widetilde{Ad}^0\bar{\rho})^{Gal(\mathbf{K}/\mathbf{Q})}.$$

The first term is $H^1(G_S/N, (\widetilde{Ad}^0\bar{\rho})^N)$ which is assumed trivial. As $Gal(\mathbf{L}/\mathbf{K})$ acts trvially on $\widetilde{Ad}^0\bar{\rho}$ the last term becomes $Hom_{G_S}(Gal(\mathbf{L}/\mathbf{K}), \widetilde{Ad}^0\bar{\rho})$ and is at most $r-1$ dimensional. Thus $H^1(Gal(\mathbf{L}/\mathbf{Q}), \widetilde{Ad}^0\bar{\rho})$ is at most $r-1$ dimensional. This contradicts the independence of $\{f_1, f_2, .., f_r\}$, so the $\mathbf{L_i} \cap \hat{\mathbf{L}}_\mathbf{i} = \mathbf{K}$. The second part is handled similarly.

For the third part, observe the simple terms in the composition series for the $\tilde{\mathbf{k}}[G_s]$ module $Gal(\mathbf{L}/\mathbf{K})$ are all $\widetilde{Ad}^0\bar{\rho}$. Those of $Gal(\mathbf{M}/\mathbf{K})$ are all $(\widetilde{Ad}^0\bar{\rho})^*$. By Lemma 6 these are, after scalar extension to $\mathbf{k}$, nonisomorphic $\mathbf{F_p}[G_p]$ modules so they are nonisomorphic $\tilde{\mathbf{k}}[G_S]$ modules. Thus $\mathbf{L} \cap \mathbf{M} = \mathbf{K}$.

Remark: $Gal(\mathbf{L}/\mathbf{K})$ and $Gal(\mathbf{M}/\mathbf{K})$ inherit $\tilde{\mathbf{k}}$ structures from the $\tilde{\mathbf{k}}$ modules $Gal(\mathbf{L_i}/\mathbf{K})$ and $Gal(\mathbf{M_i}/\mathbf{K})$.

Lemma 11 *1)* $Gal(\mathbf{L}/\mathbf{K}) \simeq (\widetilde{Ad}^0\bar{\rho})^r$ *as* $\tilde{\mathbf{k}}[G_S]$ *modules and the exact sequence*

$$1 \to Gal(\mathbf{L}/\mathbf{K}) \to Gal(\mathbf{L}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

splits.
2) $Gal(\mathbf{M}/\mathbf{K}) \simeq ((\widetilde{Ad}^0\bar{\rho})^*)^r$ *as* $\tilde{\mathbf{k}}[G_S]$ *modules and the exact sequence*

$$1 \to Gal(\mathbf{M}/\mathbf{K}) \to Gal(\mathbf{M}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

splits.

Proof: The $\mathbf{L_i}$ are linearly disjoint over $\mathbf{K}$ by Lemma 10. Since each $Gal(\mathbf{L_i}/\mathbf{K})$ is isomorphic to the $\tilde{\mathbf{k}}[G_S]$ module $\widetilde{Ad}^0\bar{\rho}$ we see $Gal(\mathbf{L}/\mathbf{K}) \simeq (\widetilde{Ad}^0\bar{\rho})^r$. The splitting follows from Lemma 9. This proves part 1. The proof of part 2 is similar.

Lemma 12 $Gal(\mathbf{F}/\mathbf{K}) \simeq Gal(\mathbf{L}/\mathbf{K}) \times Gal(\mathbf{M}/\mathbf{K})$.

Proof: Immediate from part 3 of Lemma 10.

Lemma 13 $Gal(\mathbf{F}/\mathbf{Q}) \simeq Gal(\mathbf{F}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{Q})$.

Proof: We have that the exact sequences

$$1 \to Gal(\mathbf{L}/\mathbf{K}) \to Gal(\mathbf{L}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

and

$$1 \to Gal(\mathbf{M}/\mathbf{K}) \to Gal(\mathbf{M}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

both split by Lemma 11. Since $Gal(\mathbf{F}/\mathbf{K}) \simeq Gal(\mathbf{L}/\mathbf{K}) \times Gal(\mathbf{M}/\mathbf{K})$ we see (using part 3 of Lemma 10) that the exact sequence

$$1 \to Gal(\mathbf{F}/\mathbf{K}) \to Gal(\mathbf{F}/\mathbf{Q}) \to Gal(\mathbf{K}/\mathbf{Q}) \to 1$$

splits.

In Theorem 1 we assume an element $a \times b \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D}) \simeq Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{K}/\mathbf{Q})$ exists where a is in the *projective* image of $\bar{\rho}$, the eigenvalues of a have ratio t and b corresponds to the class of $t \in (\mathbf{Z}/p)^*$ where $t \not\equiv \pm 1 \bmod p$. Note that we insist that t lie in the multiplicative group of the *prime* field $\mathbf{F_p}$. Let $c = a \times b$. Let d be the (multiplicative) order of $t \bmod p$. Note d is prime to p and c has order d in $Gal(\mathbf{K}/\mathbf{Q})$.

Lemma 14 *1) Consider the action of c on* $Gal(\mathbf{L_i}/\mathbf{K}) \simeq \widetilde{Ad}^0\bar{\rho}$. *There are nontrivial elements of* $Gal(\mathbf{L_i}/\mathbf{K})$ *on which c acts trivially.*
2) There are nontrivial elements of $Gal(\mathbf{M_i}/\mathbf{K})$ *on which c acts trivially.*

Proof: 1) One easily sees that b acts trivially on $Ad^0\bar{\rho}$. (Not $\widetilde{Ad}^0\bar{\rho}$!). Using that the projective element a has distinct eigenvalues with ratio t, we see that $Ad^0\bar{\rho}$ decomposes under the action of c into one dimensional $\mathbf{k}$ vector spaces. Thus the action of c is via multiplication by t, 1 and $1/t$ respectively. As $t \in \mathbf{F_p}$ we see $Ad^0\bar{\rho}$ decomposes as an $\mathbf{F_p}$ vector space into c eigenspaces with c acting by t, 1 and $1/t$.

Recall we have an injection $\widetilde{Ad}^0\bar{\rho} \to Ad^0\bar{\rho}$ by extending scalars and this injection is G_S equivariant. Thus the $\mathbf{F_p}$ vector space $\widetilde{Ad}^0\bar{\rho}$ decomposes into eigenspaces with eigenvalues t, 1, and $1/t$ under the action of c. Suppose there are no eigenspaces with eigenvalue 1. Then under the scalar extension map $\widetilde{Ad}^0\bar{\rho} \to Ad^0\bar{\rho}$ the image of $\widetilde{Ad}^0\bar{\rho}$ lies in the two dimensional $\mathbf{k}$ vector space spanned by the one dimensional $\mathbf{k}$ eigenspaces on which c acts by t and $1/t$. Since the image of $\widetilde{Ad}^0\bar{\rho}$ in $Ad^0\bar{\rho}$ is G_S stable its $\mathbf{k}$ span is also G_S stable. But the $\mathbf{k}$ span is a two dimensional $\mathbf{k}$ subspace of $Ad^0\bar{\rho}$. This contradicts the absolute irreducibility of $Ad^0\bar{\rho}$.
2) The proof is identical, except the action of c on $(Ad^0\bar{\rho})^*$ decomposes $(Ad^0\bar{\rho})^*$ into one dimensional $\mathbf{k}$ vector spaces with eigenvalues 1, t and t^2.

Lemma 15 *Let $\alpha_i \in Gal(\mathbf{L}/\mathbf{K}) \simeq (\widetilde{Ad}^0\bar{\rho})^r$ be the element all of whose entries are* 0 *except the the ith entry which is a nonzero element on which c acts trivially. Put*

$$\beta_i = \alpha_i \rtimes c \in Gal(\mathbf{L}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{L}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{Q}) \simeq Gal(\mathbf{L}/\mathbf{Q}).$$

Then β_i has order pd in $Gal(\mathbf{L}/\mathbf{Q})$. Let u_i be a prime of $\mathbf{Q}$ unramified in $\mathbf{L}$ with Frobenius in the conjugacy class of β_i in $Gal(\mathbf{L}/\mathbf{Q})$. Then for $j \neq i$ the primes above u_i in $\mathbf{K}$ split completely from $\mathbf{K}$ to $\mathbf{L_j}$ but these primes do NOT *split completely from $\mathbf{K}$ to $\mathbf{L_i}$.*

Proof: The order of β_i in $Gal(\mathbf{L}/\mathbf{Q})$ is the least common multiple of the orders of α_i and c, namely pd. The remaining statements follow from projecting $\beta_i \in Gal(\mathbf{L}/\mathbf{Q})$ to $Gal(\mathbf{L_j}/\mathbf{Q})$ and $Gal(\mathbf{L_i}/\mathbf{Q})$ and observing the order of the projections are d and pd respectively.

Corollary 1 *$f_i \mid_{G_{u_i}} \neq 0$ and is unramified. Therefore by the results of Section 3 it is nonnull at u_i. For $j \neq i$ we have $f_j \mid_{G_{u_i}} = 0$.*

Proof: By the choice of c prior to Lemma 14 we see u_i is a prime as in Section 3 and all the results there apply. By the choice of u_i we see G_{u_i} acts on $Ad^0\bar{\rho}$ through a quotient of order d. If we complete the extension $\mathbf{L_i}/\mathbf{Q}$ at a prime above u_i the degree of the local extension is pd. This follows from Lemma 15 and the fact that $\widetilde{Ad}^0\bar{\rho}$ is a p-group. Observe $(\mathbf{1}+\epsilon f_i)\bar{\rho} \mid_{G_{u_i}}$ is the restriction to G_{u_i} of the deformation to the dual numbers $\mathbf{k}[\epsilon]$ corresponding to $f_i \in H^1(G_S, Ad^0\bar{\rho})$. The projective representation associated to this representation has image of order pd. Since the order of the image of the

projective representation associated to $\bar{\rho}\mid_{G_{u_i}}$ is d we see $f_i\mid_{G_{u_i}} \neq 0$ and it is clearly unramified at u_i. That $f_i\mid_{G_{u_j}} = 0$ follows from the fact that the local degree at u_i of $\mathbf{L_j}/\mathbf{Q}$ is d.

Lemma 16 *Let* $\gamma_i \in Gal(\mathbf{M}/\mathbf{K}) \simeq ((\widetilde{Ad}^0\bar{\rho})^*)^r$ *be the element with all entries* 0 *except the* i*th which is a nonzero element on which* c *acts trivially. Put*

$$\delta_i = \gamma_i \rtimes c \in Gal(\mathbf{M}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{M}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{Q}) \simeq Gal(\mathbf{M}/\mathbf{Q}).$$

Then δ_i *has order* pd *in* $Gal(\mathbf{M}/\mathbf{Q})$. *Let* v_i *be a prime with Frobenius in the conjugacy class of* δ_i *in* $Gal(\mathbf{M}/\mathbf{Q})$. *Then for* $j \neq i$ *the primes above* v_i *in* $\mathbf{K}$ *split completely from* $\mathbf{K}$ *to* $\mathbf{M_j}$, *but they do* NOT *split completely from* $\mathbf{K}$ *to* $\mathbf{M_i}$.

Proof: The proof is the same as Lemma 15.

Corollary 2 $g_i\mid_{G_{v_i}} \neq 0$ *and for* $j \neq i$ *we have* $g_j\mid_{G_{v_i}} = 0$.

Proof: The proof is as in Corollary 1.

Proposition 4 *Let*

$$\eta_i \in Gal(\mathbf{F}/\mathbf{Q}) \simeq Gal(\mathbf{F}/\mathbf{K}) \rtimes Gal(\mathbf{K}/\mathbf{Q}) \simeq \Big(Gal(\mathbf{L}/\mathbf{K}) \times Gal(\mathbf{M}/\mathbf{K})\Big) \rtimes Gal(\mathbf{K}/\mathbf{Q})$$

be the element $(\alpha_i \times \gamma_i) \rtimes c$. *Let* q_i *be a prime of* $\mathbf{Q}$ *unramified in* $\mathbf{F}$ *with Frobenius in the conjugacy class of* η_i *in* $Gal(\mathbf{F}/\mathbf{Q})$. *Let* $Q = \{q_1, q_2, .., q_r\}$. *Then* $Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*) = 0$.

Proof: Note that $(\alpha_i \times \gamma_i) \rtimes c \in Gal(\mathbf{F}/\mathbf{Q})$ projects to β_i, δ_i, and c in $Gal(\mathbf{L}/\mathbf{Q})$, $Gal(\mathbf{M}/\mathbf{Q})$ and $Gal(\mathbf{K}/\mathbf{Q})$ respectively. Thus if q_i is a prime with Frobenius in the conjugacy class of $(\alpha_i \times \gamma_i) \rtimes c \in Gal(\mathbf{F}/\mathbf{Q})$ we see q_i is a prime as in Section 3 by Corollary 1. By Corollaries 1 and 2 we see that $f_i\mid_{G_{q_i}} \neq 0$, $g_i\mid_{G_{q_i}} \neq 0$ and for $i \neq j$ that $f_i\mid_{G_{q_j}} = 0$ and $g_i\mid_{G_{q_j}} = 0$.

Consider the natural injection $Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*) \to Ш^1_S((\widetilde{Ad}^0\bar{\rho})^*)$. Let $h \in Ш^1_S((\widetilde{Ad}^0\bar{\rho})^*)$. Then $h = \sum_{i=1}^r \nu_i g_i$ where $\nu_i \in \tilde{\mathbf{k}}$ and we see $h\mid_{G_{q_i}} = \nu_i g_i$. If $h \in Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*)$ then $h\mid_{G_{q_i}}$ is trivial so we must have $\nu_i = 0$ for all $1 \leq i \leq r$, that is $h = 0$.

Proposition 5 *The map* $H^2(G_{S\cup Q}, \widetilde{Ad}^0\bar{\rho}) \to \oplus_{v\in Q} H^2(G_v, \widetilde{Ad}^0\bar{\rho})$ *is an isomorphism.*

Proof: For all $v \in S$ we assume $H^2(G_v, \widetilde{Ad}^0\bar{\rho}) = 0$. Thus the right side of the above map is actually $\oplus_{v\in S\cup Q} H^2(G_v, \widetilde{Ad}^0\bar{\rho})$. Injectivity follows from the fact that $Ш^2_{S\cup Q}(\widetilde{Ad}^0\bar{\rho})$ is dual to $Ш^1_{S\cup Q}((\widetilde{Ad}^0\bar{\rho})^*)$ which is trivial. Surjectivity follows from Chapter I, Theorem 4.10 of [Mi].

Theorem 1 *Let $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ be an absolutely irreducible Galois representation where the characteristic p of $\mathbf{k}$ is greater than or equal to 5. Assume $Ad^0\bar{\rho}$ is an absolutely irreducible $\mathbf{k}[G_S]$ module, that $H^1(G_S/N, Ad^0\bar{\rho})$ and $H^1(G_S/N^d, (Ad^0\bar{\rho})^*)$ are trivial, and that $H^2(G_v, Ad^0\bar{\rho}) = 0$ for all $v \in S$. Finally suppose there is an element*

$$a \times b \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D}) \simeq Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{K}/\mathbf{Q})$$

such that a corresponds to an element in the (projective) image of $\bar{\rho}$ whose eigenvalues have ratio $t \in \mathbf{F}_\mathbf{p}^*$, where $t \neq \pm 1$, and $b \in Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \to (\mathbf{Z}/p)^*$ maps to the element t. Let $r = dim_\mathbf{k} H^2(G_S, Ad^0\bar{\rho})$ Then there is a set of primes $Q = \{q_1, q_2, .., q_r\}$ disjoint from S and a representation $\rho : G_{S\cup Q} \to GL_2(W(\mathbf{k}))$ such that $\rho \equiv \bar{\rho}$ mod p.

Proof: Let Q be as in Proposition 4. We apply induction to deform from $W(\mathbf{k})/p^n$ to $W(\mathbf{k})/p^{n+1}$ one step at a time. We note that for all the q_i, $\bar{\rho}\mid_{G_{q_i}}$ is of the "desired form" of Section 3. This is the base case in our induction. Suppose we have a deformation $\rho_n : G_{S\cup Q} \to GL_2(W(\mathbf{k})/p^n)$ with $\rho_n \mid_{G_{q_i}}$ of the desired form for $1 \leq i \leq r$. Since the local at q_i deformation problems (to mod p^{n+1}) are then unobstructed we can by Proposition 5 deform ρ_n to mod p^{n+1}, that is there is a $\tilde{\rho} : G_{S\cup Q} \to GL_2(W(\mathbf{k})/p^{n+1})$ with $\tilde{\rho} \equiv \rho_n \bmod p^n$. The local at q_i representations $\tilde{\rho}\mid_{G_{q_i}}$ may not be of the "desired form". However we know f_i is nonnull at q_i by Corollary 1. Using Proposition 1, we can alter $\tilde{\rho}$ by an appropriate multiple $\nu_i \in \mathbf{k}$ of f_i so that $(\nu_i f_i).\tilde{\rho}\mid_{G_{q_i}}$ is of the "desired form" at q_i. Let $\rho_{n+1} = (\sum \nu_i f_i).\tilde{\rho}$. As $f_j \mid_{G_{q_i}}$ is trivial for $j \neq i$ we have by Corollary 1 that $\rho_{n+1}\mid_{G_{q_i}} = (\nu_i f_i).\tilde{\rho}\mid_{G_{q_i}}$ and the deformation problem is unobstructed at q_i. Then $\rho_{n+1} = \left(\sum \nu_i f_i\right).\tilde{\rho}$ is of the "desired form" at G_{q_i} for $1 \leq i \leq r$. The induction is now complete and the theorem follows.

We now prove Theorem 2. Recall $\mathbf{Q}(\bar{\rho})$ is the field fixed by the kernel of $\bar{\rho}$ and that we assume the image of $\bar{\rho}$, denoted $Im\bar{\rho}$, contains $SL_2(\mathbf{k})$.

Lemma 17 *Let $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ be such that $Im\bar{\rho} \supseteq SL_2(\mathbf{k})$ where the characteristic p of $\mathbf{k}$ is greater than or equal to 5. Then $\bar{\rho}$ and $Ad^0\bar{\rho}$ are absolutely irreducible and the minimal field of definition of $Ad^0\bar{\rho}$ is $\mathbf{k}$.*

Proof: If $\bar{\rho}$ is not absolutely irreducible then it is conjugate (over $\bar{\mathbf{k}}$) to a representation over $\bar{\mathbf{k}}$ that is upper triangular. This implies $Im\bar{\rho}$ is solvable. As we assume $p \geq 5$ we know $Im\bar{\rho}$ is not solvable.

To show absolute irreducibility of $Ad^0\bar{\rho}$ it suffices to show the action of $SL_2(\mathbf{k})$ on the two by two matrices with trace 0 over $\mathbf{k}$ is absolutely irreducible. It suffices to prove the special case that the action of $SL_2(\mathbf{F_p})$ on the two by two matrices with trace 0 over $\mathbf{F_p}$ is absolutely irreducible.

Since p is odd we may cite [CR], example 17.17. The absolutely irreducible representations of $SL_2(\mathbf{F_p})$ are given by actions of $SL_2(\mathbf{F_p})$ on the $d+1$ dimensional space M_d of homogeneous polynomials in two variables (say X and Y) of degree d over $\bar{\mathbf{F}}_\mathbf{p}$. Let $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbf{F_p})$. Then g acts on M_d by $g.X = rX + sY$ and $g.Y = tX + uY$. When d is odd note that $-\mathbf{1} \in SL_2(\mathbf{F_p})$ acts nontrivially on M_d. Since $-\mathbf{1}$ acts trivially on $Ad^0\bar{\rho}$ we see the Jordan-Hölder sequence for $Ad^0\bar{\rho}$ can contain only M_d with d even. The only possibilities are the one dimensionsal space M_0 and the three dimensional space M_2. If M_0 occurs in the Jordan-Hölder sequence it occurs with multiplicity three and as in the first paragraph of this proof one sees $PSL_2(\mathbf{F_p})$ is solvable for $p \geq 5$, a contradiction. The absolutely irreducible representation M_2 is $Ad^0\bar{\rho}$ and we are done.

Let $q = \#\mathbf{k}$. As for the minimal field of definition of $Ad^0\bar{\rho}$, consider the the elements of $\widetilde{Ad}^0\bar{\rho}$ stabilized by the group of matrices U of order q of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbf{k})$. Since we have a p group acting on a p group there are nonzero elements of $\widetilde{Ad}^0\bar{\rho}$ fixed by the action of U. Clearly the $\tilde{\mathbf{k}}$ span of these elements in $\widetilde{Ad}^0\bar{\rho}$ is pointwise fixed under the action of U. If this $\tilde{\mathbf{k}}$ span were greater than one dimensional then on extending scalars to $\mathbf{k}$ we see U would pointwise fix a two (or greater) dimensional $\mathbf{k}$ subspace of $Ad^0\bar{\rho}$. It is easy to see this is not the case. Let l_1 be the one dimensional $\tilde{\mathbf{k}}$ subspace of $\widetilde{Ad}^0\bar{\rho}$ pointwise fixed by U. We ask what other elements of $SL_2(\mathbf{k})$ pointwise fix l_1. These elements of $SL_2(\mathbf{k})$ pointwise fix the $\mathbf{k}$ span of l_1 in $Ad^0\bar{\rho}$ and we easily see that $\pm U$ is the stabilizer of l_1. Let $x_0 \in l_1$ be nonzero. The orbit of x_0 under the action of $SL_2(\mathbf{k})$ has cardinality $\#SL_2(\mathbf{k})/(2\#U) = (q^2-1)/2$. So $\widetilde{Ad}^0\bar{\rho}$ contains at least distinct $(q^2-1)/2$ elements. If the minimal field of definition $\tilde{\mathbf{k}}$ is strictly smaller than $\mathbf{k}$ then $\#\tilde{\mathbf{k}} \leq q^{1/2}$. Thus $\widetilde{Ad}^0\bar{\rho}$ contains at most $q^{3/2}$ distinct elements. Since $q \geq 5$ we see $q^{3/2} < (q^2-1)/2$, a contradiction. The minimal field of definition of $Ad^0\bar{\rho}$ is $\mathbf{k}$.

Remark: Since, with the hypotheses of Theorem 2, we have $\tilde{\mathbf{k}} = \mathbf{k}$ we will use $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ for the rest of this section.

Lemma 18 *Let $p \geq 5$ and suppose the image of $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ contains $SL_2(\mathbf{k})$. Recall $\mathbf{D} = \mathbf{Q}(Ad^0\bar{\rho}) \cap \mathbf{Q}(\mu_p)$. Then $[\mathbf{D} : \mathbf{Q}] = 1$ or 2. As $[\mathbf{Q}(\mu_p) : \mathbf{Q}] = p-1$ we have that $Gal(\mathbf{Q}(\mu_p)/\mathbf{D})$ is not the trivial group.*

Proof: As $\mathbf{D} \subseteq \mathbf{Q}(\mu_p)$, we see $\mathbf{D}/\mathbf{Q}$ is abelian so $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{D})$ contains the commutator subgroup of $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{Q}) = Im\bar{\rho}$. As $Im\bar{\rho} \supseteq SL_2(\mathbf{k})$ and

$\#\mathbf{k} \geq 4$ we see this commutator subgroup is just $SL_2(\mathbf{k})$. As $\mathbf{D} \subseteq \mathbf{Q}(Ad^0\bar{\rho})$, the fixed field of the projective representation associated to $\bar{\rho}$, we have that $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{D})$ contains the scalar matrices in $Im\bar{\rho}$ which we denote Z. Thus $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{D})$ contains $Z \cdot SL_2(\mathbf{k})$ as a normal subgroup.

Let A be in $Im\bar{\rho}$ with determinant $a \in \mathbf{k}$. Then $A^2 \in Im\bar{\rho}$ has determinant a^2 so $A^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot X$ where $X \in SL_2(\mathbf{k})$, that is $A^2 \in Z \cdot SL_2(\mathbf{k})$. Since $Im\bar{\rho}/SL_2(\mathbf{k}) \subseteq \mathbf{k}^*$ is cyclic we have $[Im\bar{\rho} : Z \cdot SL_2(\mathbf{k})] = 1$ or 2. We conclude $[\mathbf{D} : \mathbf{Q}] = 1$ or 2.

Lemma 19 *If $\#\mathbf{k} \geq 7$ and $Im\bar{\rho} \supseteq SL_2(\mathbf{k})$ then $H^1(G_S/N, Ad^0\bar{\rho})$ is trivial.*

Proof: Let B' be the Borel subgroup of upper triangular matrices in $Im\bar{\rho}$. Since $[Im\bar{\rho} : B']$ is easily seen to be prime to p it suffices to show $H^1(B', M^0) = 0$ where M^0 is the set of two by two trace zero matrices over $\mathbf{k}$. But as a B' module M^0 has a 3 step filtration. By computing the cohomology of the various one dimensional subquotients the result follows. See Lemma 1.2 of [Fl]. Note that during this argument the fact that B' contains diagonal elements the ratio of whose eigenvalues is not ± 1 is used. This is why we require $\#\mathbf{k} \geq 7$. Alternatively, if $\mathbf{k} = \mathbf{F_5}$ and $Im\bar{\rho} = GL_2(\mathbf{F_5})$ the same methods can be used to show $H^1(GL_2(\mathbf{F_5}), Ad^0\bar{\rho}) = 0$.

Lemma 20 *$[NN^d : N]$ is prime to p.*

Proof: Note that $NN^d/N^d \simeq N/(N \cap N^d)$. Recall that $N = Gal(\mathbf{Q_S}/\mathbf{Q}(Ad^0\bar{\rho}))$ and that $N^d \supseteq Gal(\mathbf{Q_S}/\mathbf{K})$. So $N \cap N^d \supseteq Gal(\mathbf{Q_S}/\mathbf{K})$. Thus $N/(N \cap N^d)$ is isomorphic to a subquotient of $Gal(\mathbf{K}/\mathbf{Q}(Ad^0\bar{\rho}))$ which is in turn isomorphic to $Gal(\mathbf{Q}(\mu_p)/\mathbf{D})$ which has order prime to p.

Lemma 21 *If $p \geq 5$ and $Im\bar{\rho} \supseteq SL_2(\mathbf{k})$ then $H^1(G_S/N^d, (Ad^0\bar{\rho})^*) = 0$.*

Proof: We apply the inflation-restriction sequence to G_S/N^d and its normal subgroup NN^d/N^d. The quotient is G_S/NN^d and since N^d fixes $(Ad^0\bar{\rho})^*$ we see $(Ad^0\bar{\rho})^{*^{NN^d/N^d}} = (Ad^0\bar{\rho})^{*^N}$. We get the exact sequence

$$0 \to H^1(G_S/NN^d, (Ad^0\bar{\rho})^{*^N}) \to H^1(G_S/N^d, (Ad^0\bar{\rho})^*) \to H^1(NN^d/N, Ad^0\bar{\rho})^{G_s/NN^d}$$

where the last term is trivial as NN^d/N has order prime to p by Lemma 20. As N acts trivially on $Ad^0\bar{\rho}$ we see the action of N on $(Ad^0\bar{\rho})^*$ is $\chi\ |_N$, which is nontrivial by Lemma 18. so $((Ad^0\bar{\rho})^*)^N = 0$. Thus the left term in the sequence is trivial so $H^1(G_S/N^d, (Ad^0\bar{\rho})^*) = 0$.

Theorem 2 *Let $p \geq 7$. Assume the image of $\bar{\rho} : G_S \to GL_2(\mathbf{k})$ contains $SL_2(\mathbf{k})$. Also assume if $l \in S$ and $l \neq p$ that $l \not\equiv \pm 1$ mod p, that $k(\bar{\rho}) \neq p-1$ or $2p$, and that $k(\bar{\rho}) \not\equiv 2$ mod $p+1$. Let $r = dim_{\mathbf{k}} H^2(G_S, Ad^0\bar{\rho})$.*

Then there is a set of primes $Q = \{q_1, q_2, .., q_r\}$ *disjoint from S and a representation* $\rho : G_{S\cup Q} \to GL_2(W(\mathbf{k}))$ *such that* $\rho \equiv \bar{\rho}$ *mod p.*

Proof: Recall N and N^d are the kernels of the actions of G_S on $Ad^0\bar{\rho}$ and $(Ad^0\bar{\rho})^*$ respectively. By Lemmas 19 and 21 we have $H^1(G_S/N, Ad^0\bar{\rho})$ and $H^1(G_S/N^d, (Ad^0\bar{\rho})^*)$ are trivial. The hypotheses on the ramified primes and the weight $k(\bar{\rho})$ imply, by the results of Sections 4 and 5, that $H^2(G_v, Ad^0\bar{\rho}) = 0$ for all $v \in S$. Since p is odd we easily see $H^2(G_\infty, Ad^0\bar{\rho}) = 0$. By Lemma 17 we see $\bar{\rho}$ is absolutely irreducible and $Ad^0\bar{\rho}$ is an absolutely irreducible $\mathbf{k}[G_S]$ module.

By Theorem 1 it remains to find $a \times b \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D}) \simeq Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{K}/\mathbf{Q})$ such that a corresponds to an element in the (projective) image of $\bar{\rho}$ whose eigenvalues have ratio $t \in \mathbf{F_p^*}$, $t \neq \pm 1$, and $b \in Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \to (\mathbf{Z}/p)^*$ maps to the element t. as in Theorem 1.

Since $p \geq 7$ there is an $x \in \mathbf{F_p^*}$ such that $x^2 \neq \pm 1$ in $\mathbf{F_p^*}$. As $Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \simeq \mathbf{F_p^*}$ we consider the element x^2 in $Gal(\mathbf{Q}(\mu_p)/\mathbf{Q})$. Since x^2 is a 2nd power and $[\mathbf{D} : \mathbf{Q}] = 1$ or 2 by Lemma 18 we see $x^2 \in Gal(\mathbf{Q}(\mu_p)/\mathbf{D})$.

Recall that by the proof of Lemma 18 that $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{D}) \supseteq SL_2(\mathbf{k})$. We have that $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in Gal(\mathbf{Q}(\bar{\rho})/\mathbf{D})$. We consider the projection of this element, $\tilde{x}$, in $Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D})$, i.e. its image in the projective representation associated to $\bar{\rho}$. Finally, we take $a \times b$ to be $\tilde{x} \times x^2 \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{D}) \times Gal(\mathbf{Q}(\mu_p)/\mathbf{D}) \simeq Gal(\mathbf{K}/\mathbf{D}) \subseteq Gal(\mathbf{K}/\mathbf{Q})$. Theorem 1 now applies.

8. Examples

We give an even and odd example that illustrate the theorems.

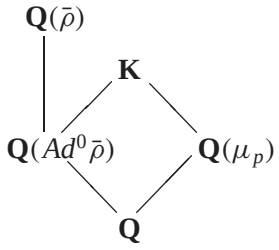
Consider the polynomial $j(x) = x^7 - 22x^6 + 141x^5 - 204x^4 - 428x^3 + 768x^2 + 320x - 512$ of [ZM]. The splitting field of $j(x)$ is a totally real field with Galois group over $\mathbf{Q}$ isomorphic to $PSL_2(\mathbf{F_7})$. We abuse notation for a moment and call this splitting field $\mathbf{Q}(Ad^0\bar{\rho})$. Zeh-Marschke has shown that there is a quadratic extension (which we call $\mathbf{Q}(\bar{\rho})$) of $\mathbf{Q}(Ad^0\bar{\rho})$ Galois over $\mathbf{Q}$ with $Gal(\mathbf{Q}(\bar{\rho})/\mathbf{Q}) \simeq SL_2(\mathbf{F_7})$. This extension gives our even $\bar{\rho}$. The discriminant of $j(x)$ is $2^{50}19^4367^2$. As mentioned in the introduction prior to the statement of Theorem 1, we may assume these are the only ramified primes in $\mathbf{Q}(\bar{\rho})/\mathbf{Q}$. These primes are not congruent to ± 1 mod 7 and $\bar{\rho}$ is unramified at $p = 7$ so by Serre's definition of weight we see $k(\bar{\rho}) = p = 7$. The hypotheses of Theorem 2 are satisfied. Thus there is a finite set of primes Q and a deformation ρ of $\bar{\rho}$ with $\rho : G_{S\cup Q} \to SL_2(\mathbf{Z_7})$. That this representation is surjective follows from [Se3], Chapter IV, Lemma 3.

In Section 5 of [Se1] Serre has given an absolutely irreducible odd representation $\bar{\rho} : G_{\mathbf{Q}} \to GL_2(\mathbf{F_{49}})$. The image of Galois in $PGL_2(\mathbf{F_{49}})$ is

$PSL_2(\mathbf{F_7})$ and is the splitting field of the polynomial $h(x) = x^7 - 7x + 3$. (The polynomial is due to Trinks). Note $\mathbf{k} = \mathbf{F_{49}}$ and $\tilde{\mathbf{k}} = \mathbf{F_7}$. The splitting field of $h(x)$ is complex and is our $\mathbf{Q}(Ad^0\bar{\rho})$. As $h(x)$ has discriminant $3^8 7^8$ we see $\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{Q}$ is ramified only at 3,7 and ∞, and we may assume $\mathbf{Q}(\bar{\rho})/\mathbf{Q}$ is ramified only at 3,7 and ∞. Since 3 is not congruent to ± 1 mod 7 we have $H^2(G_3, Ad^0\bar{\rho}) = 0$. Serre has shown that a twist of $\bar{\rho}$ is weight 3 so by Proposition 3 we have $H^2(G_7, Ad^0\bar{\rho}) = 0$.

We see that $H^1(G_S/N, \widetilde{Ad}^0\bar{\rho}) = H^1(PSL_2(\mathbf{F_7}), \widetilde{Ad}^0\bar{\rho})$. This last cohomology group is trivial (essentially) by Lemma 19 so $H^1(G_S/N, \widetilde{Ad}^0\bar{\rho}) = 0$. Similarly, $H^1(G_S/N^d, (\widetilde{Ad}^0\bar{\rho})^*) = 0$ essentially by Lemma 21.

As $\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{Q}$ is an extension with Galois group the simple group $PSL_2(\mathbf{F_7})$ we see $\mathbf{Q}(Ad^0\bar{\rho}) \cap \mathbf{Q}(\mu_p) = \mathbf{Q}$ so in this example $\mathbf{D} = \mathbf{Q}$.



Serre has shown $Im\bar{\rho} \supset SL_2(\mathbf{F_7})$ so $\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \in Im\bar{\rho}$. Let a be the projection of this element in $Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{Q})$. Consider $a \times b = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \times 4 \in Gal(\mathbf{Q}(Ad^0\bar{\rho})/\mathbf{Q}) \times Gal(\mathbf{Q}(\mu_7)/\mathbf{Q}) \simeq Gal(\mathbf{K}/\mathbf{Q})$. This element satisfies the last hypothesis of Theorem 1 and we see $\bar{\rho}$ deforms to $W(\mathbf{F_{49}})$ after allowing ramification at an additional finite set of primes.

References

[Bö] Böckle, G., A local-to-global principle for deformations of Galois Representations, J. Reine Angew. Math. **509** (1999) 199-236

[Bo1] Boston, N., Deformation Theory of Galois Representations, Harvard Ph.D Thesis, 1987

[Bo2] Boston, N., Explicit deformation of Galois Representations, Invent. math. **103** (1991) 181-196

[Bo3] Boston, N., Families of Galois Representation- Increasing the Ramification, Duke Math. J. **103** (1990) 357-367

[BM] Boston, N., Mazur, B., Explicit Universal Deformations of Galois Representations, Advanced Studies in Pure Mathematics 1989

[CR] Curtis, C., Reiner, I., Methods of representation theory, vol I, John Wiley and sons, 1981

[Da] Darmon, H., The Shimura-Taniyama Conjecture d'apres Wiles, Monographes CICMA Lecture Notes, 1994-02

[DDT] Darmon, H., Diamond, F., Taylor, R., Fermat's Last Theorem, in Current Developments in Mathematics, 1995, Bott, R. et al., eds.
[DS] Deligne, P., Serre, J.-P., Formes Modulaires de Poids 1, Ann. Scient. Éc. Norm. Sup. 4^e série, t. 7 (1974) 507-530
[deS] de Shalit, E., Hecke Rings and Universal Deformation Rings, in Modular Forms and Fermat's Last Theorem. Cornell, G., Silverman, J., Stevens, G., eds.
[Di1] Diamond, F., An Extension of Wiles' Results, in Modular Forms and Fermat's Last Theorem, Cornell, G., Silverman, J., Stevens, G., eds.
[Di2] Diamond, F., The refined conjecture of Serre, in Elliptic Curves, Modular Forms, and Fermat's Last Theorem, Coates, J., Yau, S.T., eds.
[Fl] Flach, M., A finiteness theorem for the symmetric square of an elliptic curve, Invent. math. **109** (1992) 307-327
[FM] Fontaine, J-M., Mazur, B., Geometric Galois Representations, in Elliptic Curves, Modular Forms, and Fermat's Last Theorem, Coates, J., Yau, S.T., eds.
[Ha] Haberland, K., Galois Cohomology of Algebraic Number Fields, VEB Deutscher Verlag der Wissenschaften 1978
[Kh] Khare, C., Base Change, Lifting and Serre's Conjecture, J. Number Theory **63** (1997) 387-395
[Ma1] Mazur, B., Deforming Galois Representations, in Proceedings of the March 1987 Workshop on "Galois Groups over Q" held at MSRI, Berkeley, California, Ihara, Y., Ribet, K., Serre, J.-P., eds.
[Ma2] Mazur, B., An Introduction to the Deformation Theory of Galois Representations, in Modular Forms and Fermat's Last Theorem, Cornell, G., Silverman, J., Stevens, G., eds.
[Ma3] Mazur, B., An "infinite fern" in the universal deformation space of Galois representations, Collect. Math. **48** (1997) 155-93
[Mi] Milne, J., Arithmetic Duality Theorems, Academic Press, Inc. 1986
[Ra1] Ramakrishna, R., Deforming an even representation, Invent. math. **132** (1998) 563-580
[Ra2] Ramakrishna, R., Deforming an even representation II, raising the level, J. Number Theory **72** (1998) 92-109
[Ra3] Ramakrishna, R., Infinitely ramified Galois Representations, preprint
[Se1] Serre, J.-P., Sur les Représentations Modulaires de Degré 2 de $Gal(\bar{Q}/Q)$, Duke Math. J. **54** (1987) 179-230
[Se2] Serre, J.-P., Cohomologie Galoisienne, Lect. Notes Math. **5**, Cinquième édition, révisée et complétée, Springer-Verlag, 1994
[Se3] Serre, J.-P., Abelian l-adic representations and elliptic curves, Benjamin, 1968
[TW] Taylor, R., Wiles, A., Ring-theoretic properties of certain Hecke algebras, Ann. Math. (2) **141**(3) (1995) 553-572
[Wi] Wiles, A., Modular Elliptic Curves and Fermat's Last Theorem, Ann. Math. (2) **141**(3) (1995) 443-551
[ZM] Zeh-Marschke, A., $SL_2(\mathbf{Z}/7)$ als Galoisgruppe über $\mathbf{Q}$, unpublished note