Canad. J. Math. Vol. **60** (1), 2008 pp. 208–221

Constructing Galois Representations with Very Large Image

Ravi Ramakrishna

Abstract. Starting with a 2-dimensional mod p Galois representation, we construct a deformation to a power series ring in infinitely many variables over the p-adics. The image of this representation is full in the sense that it contains SL_2 of this power series ring. Furthermore, all $\mathbb{Z}_p$ specializations of this deformation are potentially semistable at p.

1 Introduction

The main theorem of this paper is the following.

Theorem 1.1 *Let $p \geq 7$ be a prime and $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$ be a continuous representation whose image contains $SL_2(\mathbb{Z}/p\mathbb{Z})$. There exists a deformation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p[\![T_1, \dots, T_d, \dots]\!])$ of $\bar{\rho}$ with $\mathbb{Z}_p^*$-valued determinant all of whose $\mathbb{Z}_p$ specialisations are potentially semistable at p and whose image is full, that is, the image contains $SL_2(\mathbb{Z}_p[\![T_1, \dots, T_d, \dots]\!])$.*

This result is independent of the parity of $\bar{\rho}$. We remark that if $p \geq 7$ and

$$\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective, then after a suitable twist one gets from the proof a surjective

$$\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to SL_2(\mathbb{Z}_p[\![T_1, \dots, T_d, \dots]\!]).$$

The representations of the theorem are ramified at infinitely many places. One expects this condition is necessary. Indeed, for $\bar{\rho}$ odd the work of Wiles and others suggests that such deformation rings which include the conditions of finite ramification, fixed determinant and potential semistability are always finite and flat over $\mathbb{Z}_p$. Since the representations constructed here are mainly of interest as curiosities, we have not sought maximal generality. We expect, with some added technical work, that similar results could be obtained for *any* residual representations of the absolute Galois group of an arbitrary number field.

We sketch the proof. We fix determinants of all deformations considered in this paper to be $\phi\chi^r$ where ϕ is a finite order $\mathbb{Z}_p^*$-valued character, χ is the cyclotomic

Received by the editors April 11, 2005.
The author was partially supported by NSF Grant DMS-0400232
AMS subject classification: 11F80.
Keywords: Galois representation, deformation.

character, and r is a suitable nonnegative integer. Let S be the union of $\{p\}$ and the set of places at which $\bar{\rho}$ is ramified. For a place v let G_v be a decomposition group in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ at v. In [R2, T] a class $\mathcal{C}_v$ of deformations of $\bar{\rho}|_{G_v}$ to Artinian rings was chosen. A subspace $\mathcal{N}_v \subset H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$ was chosen that preserved the class via the action of $H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$ on deformations. In this paper we choose for each $v \in S$ any single deformation of $\bar{\rho}|_{G_v}$ to $\mathbb{Z}_p$ that has determinant $\phi\chi^r|_{G_v}$ and is potentially semistable. This forces $\mathcal{N}_v = 0$. We use the ideas of [R2, T] to add new primes at which we will allow ramification to achieve a trivial tangent space to the global deformation problem. Starting from this point, we successively construct a sequence of deformation problems ramified at more and more (but only finitely many) primes. We impose nontrivial deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ at these ramified primes. The corresponding deformation rings will be $R_n = \mathbb{Z}_p[\![T_1, \dots, T_n]\!]/J_n$ where $J_n \subseteq (p, T_1, \dots, T_n)^n$. Let m_{R_n} be the maximal ideal of R_n. The deformation $\rho_n\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(R_n/\mathrm{m}_{R_n}^n)$ will satisfy all the deformation conditions of the $(n+1)$st deformation ring. Thus we will have surjections $R_{n+1}/\mathrm{m}_{R_{n+1}}^{n+1} \twoheadrightarrow R_n/\mathrm{m}_{R_n}^n$. Taking the inverse limit will give us our ρ. Fullness (that the image contains SL_2) at each stage will follow from a criterion of Boston. Fullness in the limit follows from fullness at each stage.

This work was in part motivated by Rohrlich's study of Galois representations with big image [Ro1, Ro2].

Many of the technical ingredients of this paper involve computation of local deformation rings. The local results we need are in [B, R1, R2, T]. For the most part they are suppressed here, being apparent only in the choices of various subspaces $\mathcal{N}_v$ of the local Galois cohomology groups $H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$.

2 Recollections

We briefly recall Mazur's deformation theory in the general setting. Let $\mathbb{F}$ be a finite field, $W(\mathbb{F})$ its ring of Witt vectors and H a profinite group. Let $\bar{\gamma}\colon H \to GL_n(\mathbb{F})$ be a continuous representation. Let $\mathrm{Ad}\,\bar{\gamma}$ denote the set of $n \times n$ matrices over $\mathbb{F}$ with H action via $\bar{\gamma}$ and conjugation. We suppose that $m = \dim H^1(H, \mathrm{Ad}\,\bar{\gamma})$ is finite. Mazur has shown [M1] (see also [M2]) that there exists a ring $R^{\mathrm{ver}} = W(\mathbb{F})[\![T_1, \dots, T_m]\!]/I$ and a continuous homomorphism $\gamma^{\mathrm{ver}}\colon H \to GL_n(R^{\mathrm{ver}})$ whose reduction mod the maximal ideal $\mathrm{m}_{R^{\mathrm{ver}}}$ of R^{ver} is $\bar{\gamma}$. Furthermore any continuous lifting of $\bar{\gamma}$ to $GL_n(R)$ where R is a complete local Noetherian ring with residue field $\mathbb{F}$ factors through γ^{ver}. (To be precise, we should consider strict equivalence classes of continuous liftings called deformations). If the centraliser of the image of $\bar{\gamma}$ is exactly the scalar matrices, then the pair $(\gamma^{\mathrm{ver}}, R^{\mathrm{ver}})$ is *universal* and any such lifting factors through γ^{ver} in a unique way.

Let R be a complete local Noetherian ring with residue field $\mathbb{F}$ and maximal ideal m_R. Suppose we are given a continuous homomorphism $\gamma_t\colon H \to GL_n(R/\mathrm{m}_R^t)$ with reduction $\bar{\gamma}$. The obstruction to deforming γ_t to a continuous homomorphism $\gamma_{t+1}\colon H \to GL_n(R/\mathrm{m}_R^{t+1})$ lies in $H^2(H, \mathrm{Ad}\,\bar{\gamma} \otimes \mathrm{m}_R^t/\mathrm{m}_R^{t+1})$. If two such deformations exist, say $\gamma_{t+1,1}$ and $\gamma_{t+1,2}$, then there is an element $\alpha \in H^1(H, \mathrm{Ad}\,\bar{\gamma} \otimes \mathrm{m}_R^t/\mathrm{m}_R^{t+1})$ such that $\gamma_{t+1,1} = (I + \alpha)\gamma_{t+1,2}$.

We return to the setting of Theorem 1.1. Since we will always be fixing the determinants of our deformations, we work with the cohomology of $\mathrm{Ad}^0\bar{\rho}$, the set of trace zero matrices. For $v \in S$, the (possibly versal) deformation rings R^v of $\bar{\rho}|_{G_v}$ were worked out in [B, R2]. In most cases a "large enough" smooth quotient $R^{v,sm}$ of the deformation ring R^v was found in [R2]. The quotient map $R^v \to R^{v,sm}$ induced a subspace $\mathcal{N}_v$ of $H^1(G_v, \mathrm{Ad}^0\bar{\rho})$, the mod p dual tangent space of R^v. Here we need not concern ourselves with these smooth quotients. We will simply choose for all $v \in S$ any potentially semistable deformation of $\bar{\rho}|_{G_v}$ to $\mathbb{Z}_p$ that we like with our chosen determinant. Potential semistability is automatic for $v \neq p$. For $v = p$ we can always choose a potentially semistable lift. See [R2]. The maps $R^v \to \mathbb{Z}_p$ induce the trivial subspace of $H^1(G_v, \mathrm{Ad}^0\bar{\rho})$. For $v \in S$ we define $\mathcal{N}_v \subset H^1(G_v, \mathrm{Ad}^0\bar{\rho})$ to be trivial.

Definition 2.1 Suppose $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$ is given as in Theorem 1.1. We say a prime q is *nice* (for $\bar{\rho}$) if

- q is not ± 1 mod p;
- $\bar{\rho}$ is unramified at q;
- the eigenvalues of $\bar{\rho}(\sigma_q)$ (where σ_q is Frobenius at q) have ratio q.

Let R be a complete Noetherian local ring with residue field $\mathbb{Z}/p\mathbb{Z}$ and let J be an ideal of finite index in R. Let $\rho_{R/J}$ be a deformation of $\bar{\rho}$ to $GL_2(R/J)$. We say a prime q is $\rho_{R/J}$-*nice* if

- q is nice for $\bar{\rho}$;
- $\rho_{R/J}$ is unramified at q, and the eigenvalues of $\rho_{R/J}(\sigma_q)$ have ratio q;
- $\rho_{R/J}(\sigma_q)$ has the same (prime to p) order as $\bar{\rho}_{R/J}(\sigma_q)$.

Note that since q is nice, the characteristic polynomial of $\rho_{R/J}(\sigma_q)$ has distinct roots that are units, so the eigenvalues of $\rho_{R/J}(\sigma_q)$ are well defined in R/J.

Proposition 2.2 *For a given $\rho_{R/J}$ deforming $\bar{\rho}$ there is a conjugacy class C in the image of $\rho_{R/J}$ such that the primes with Frobenius in C are $\rho_{R/J}$-nice.*

Proof For a representation ρ, let $P\rho$ denote the corresponding projective representation. We know nice primes exist, the key point being [R1, Lemma 18]. Their existence comes from the fact that $\mathbb{Q}(P\bar{\rho}) \cap \mathbb{Q}(\mu_p)$ is at most a degree 2 extension of $\mathbb{Q}$. Consider $\mathrm{Kernel}(P\bar{\rho})/\mathrm{Kernel}(P\rho_{R/J})$. The fact that the image of $\bar{\rho}$ contains $SL_2(\mathbb{Z}/p\mathbb{Z})$ implies that, when considered as $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q})$-modules, the Jordan–Hölder constituents of this quotient are all copies of the irreducible module $\mathrm{Ad}^0\bar{\rho}$. Thus $\mathbb{Q}(P\rho_{R/J}) \cap \mathbb{Q}(\mu_{p^\infty})$ is at most degree 2 over $\mathbb{Q}$. We can lift the image under $\bar{\rho}$ of Frobenius of a nice prime q to an element of the image of $\rho_{R/J}$. Raising it to a large enough power of p gives an element whose order is that of $\bar{\rho}(\sigma_q)$ and therefore prime to p. Then we use the above field disjointness properties to get a class of $\rho_{R/J}$-nice primes with Frobenius in the conjugacy class of this element. ■

Ramification at a nice q in any deformation of $\bar{\rho}|_{G_q}$ will be pro-p and thus tame. Since the Galois group over $\mathbb{Q}_q$ of the maximal tamely ramified extension is generated by Frobenius σ_q and a generator of tame inertia τ_q subject to the relation

$\sigma_q \tau_q \sigma_q^{-1} = \tau_q^q$, a versal deformation is specified by the images of σ_q and τ_q. See [R1, §3] for the local deformation theory of nice primes.

Let $(\mathrm{Ad}^0 \bar{\rho})^* := \mathrm{Hom}(\mathrm{Ad}^0 \bar{\rho}, \mu_p)$ be the $\mathbb{G}_m$-dual of $\mathrm{Ad}^0 \bar{\rho}$. Since the eigenvalues of $\bar{\rho}(\sigma_q)$ have ratio q, the eigenvalues of σ_q acting on $\mathrm{Ad}^0 \bar{\rho}$ are q, 1 and q^{-1} so

$$\mathrm{Ad}^0 \bar{\rho} \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}(1) \oplus \mathbb{Z}/p\mathbb{Z}(-1),$$

$$(\mathrm{Ad}^0 \bar{\rho})^* \simeq \mathbb{Z}/p\mathbb{Z}(1) \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}(2).$$

As $q \not\equiv \pm 1 \bmod p$ we have that q, 1 and q^{-1} are distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Thus in each of the above decompositions the three terms are distinct. The proof of Fact 2.3 below can be found in [R1, §3]. See also [KLR1, §2].

Fact 2.3 *Let q be a nice prime for $\bar{\rho}$. Then $H^1(G_q, \mathbb{Z}/p\mathbb{Z}(r)) = 0$ for $r \neq 0, 1$. Furthermore $H^i(G_q, \mathrm{Ad}^0 \bar{\rho})$ and $H^i(G_q, (\mathrm{Ad}^0 \bar{\rho})^*)$ are both isomorphic to $H^i(G_q, \mathbb{Z}/p\mathbb{Z}) \oplus H^i(G_q, \mathbb{Z}/p\mathbb{Z}(1))$ for $i = 0, 1, 2$ and have dimensions 1, 2 and 1, respectively. Let τ_q be a generator of tame inertia. The local deformation ring R^q has a smooth one dimensional quotient $\mathbb{Z}_p[[T]]$ the deformation to which, up to twist, is given by*

$$\sigma_q \mapsto \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}, \quad \tau_q \mapsto \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}.$$

This quotient induces a one dimensional subspace

$$\mathcal{N}_q = H^1(G_q, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_q, \mathrm{Ad}^0 \bar{\rho})$$

and by local duality its annihilator is the one dimensional subspace

$$\mathcal{N}_q^{\perp} = H^1(G_q, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_q, (\mathrm{Ad}^0 \bar{\rho})^*).$$

We recall a proposition of Wiles [W, Proposition 1.6]. See also [NSW, Theorem 8.6.20].

Fact 2.4 *Let $T \supset S$ be a finite set of places. For $v \in T$ let $\mathcal{L}_v \subset H^1(G_v, \mathrm{Ad}^0 \bar{\rho})$ be a subspace with annihilator $\mathcal{L}_v^{\perp} \subset H^1(G_v, (\mathrm{Ad}^0 \bar{\rho})^*)$. Define $H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0 \bar{\rho})$ and $H^1_{\mathcal{L}^{\perp}}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$ to be, respectively, the kernels of the restriction maps*

$$H^1(G_T, \mathrm{Ad}^0 \bar{\rho}) \to \bigoplus_{v \in T} \frac{H^1(G_v, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{L}_v},$$

$$H^1(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) \to \bigoplus_{v \in T} \frac{H^1(G_v, (\mathrm{Ad}^0 \bar{\rho})^*)}{\mathcal{L}_v^{\perp}}.$$

Then

$$\begin{aligned} \dim H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0 \bar{\rho}) &- \dim H^1_{\mathcal{L}^{\perp}}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) \\ &= \dim H^0(G_T, \mathrm{Ad}^0 \bar{\rho}) - \dim H^0(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) \\ &\qquad + \sum_{v \in T} \big(\dim(\mathcal{L}_v) - \dim H^0(G_v, \mathrm{Ad}^0 \bar{\rho}) \big). \end{aligned}$$

The above groups are called the Selmer and dual Selmer groups for the set T and deformation conditions $\mathcal{L}_v$ and $\mathcal{L}_v^{\perp}$, respectively. The formula shows the difference in dimension between the Selmer and dual Selmer groups for a set of places T and deformation conditions $\mathcal{L}_v$ and $\mathcal{L}_v^{\perp}$ can be readily computed.

3 The Setup

Fact 3.1 below follows from [KLR1, Lemmas 7 and 8].

Fact 3.1 *We may enlarge S (to a set we also denote by S) by adding nice primes to it so that for any set $T \supseteq S$ both $\text{Ш}^2_T(\operatorname{Ad}^0 \bar{\rho})$ and its dual $\text{Ш}^1_T((\operatorname{Ad}^0 \bar{\rho})^*)$ are trivial. For any nice prime $q \notin T$ the inflation map $H^1(G_T, \operatorname{Ad}^0 \bar{\rho}) \to H^1(G_{T\cup\{q\}}, \operatorname{Ad}^0 \bar{\rho})$ has one-dimensional cokernel.*

Henceforth we will assume that S is as in Fact 3.1, $T \supseteq S$ and $T\backslash S$ consists of nice primes.

Recall by global duality [NSW, 8.6.13] that the images of the restriction maps

$$\Psi_T\colon H^1(G_T, \operatorname{Ad}^0 \bar{\rho}) \to \bigoplus_{v\in T} H^1(G_v, \operatorname{Ad}^0 \bar{\rho}),$$
$$\Psi_T^*\colon H^1(G_T, (\operatorname{Ad}^0 \bar{\rho})^*) \to \bigoplus_{v\in T} H^1(G_v, (\operatorname{Ad}^0 \bar{\rho})^*)$$

are exact annihilators of one another under the pairing of summing the invariants of local cup products.

Proposition 3.2 *Let $(z_v)_{v\in T} \in \bigoplus_{v\in T} H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$ be given such that*

$$(z_v)_{v\in T} \notin \Psi_T(H^1(G_T, \operatorname{Ad}^0 \bar{\rho})).$$

Then there exists a $\zeta \in H^1(G_T, (\operatorname{Ad}^0 \bar{\rho})^*)$ such that $\Psi_T^*(\zeta)$ does not annihilate $(z_v)_{v\in T}$.

Proof Since $(z_v)_{v\in T} \notin \Psi_T(H^1(G_T, \operatorname{Ad}^0 \bar{\rho}))$ we see the annihilator of $(z_v)_{v\in T}$ does not contain $\Psi_T^*(H^1(G_T, (\operatorname{Ad}^0 \bar{\rho})^*))$. So there exists a nonzero $\zeta \in H^1(G_T, (\operatorname{Ad}^0 \bar{\rho})^*)$ such that $\Psi_T^*(\zeta)$ does not annihilate $(z_v)_{v\in T}$. ∎

Definition 3.3 Let $(z_v)_{v\in T}$ as in Proposition 3.2. For q nice we call

$$h^{(q)} \in H^1(G_{T\cup\{q\}}, \operatorname{Ad}^0 \bar{\rho})$$

a solution to the local condition problem $(z_v)_{v\in T}$ if $h^{(q)}|_{G_v} = z_v$ for all $v \in T$.

For $\zeta \in H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), (\operatorname{Ad}^0 \bar{\rho})^*)$ and $z_v \in H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$ we will write $\zeta \cup z_v$ for $\zeta|_{G_v} \cup z_v$.

Proposition 3.4 *Assume some $\rho_{R/J}$ is given as in Definition 2.1. Let $(z_v)_{v\in T}$ and ζ be as in Proposition 3.2. Let $\{\zeta_1, \dots, \zeta_s\}$ be a basis of ${\Psi_T^*}^{-1}(\operatorname{Ann}((z_v)_{v\in T}))$. Let Q be the Chebotarev set of $\rho_{R/J}$-nice primes q such that*

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

(i) $\zeta_i|_{G_q} = 0$ *for* $i = 1, \dots, s$,
(ii) $\zeta|_{G_q} \neq 0$,
(iii) *for all* $f \in H^1(G_T, \mathrm{Ad}^0 \bar{\rho})$ *we have* $f|_{G_q} = 0$.

Then for any $q \in Q$ *there is an* $h^{(q)} \in H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0 \bar{\rho})$ *that is a solution to the local condition problem* $(z_v)_{v\in T}$.

Proof That Q comes from a Chebotarev condition follows from [R1, Lemma 10] which gives that the splitting conditions of Proposition 2.2 are independent of those imposed by ζ and the ζ_i. See also [KLR1, Lemma 6].

As $(z_v)_{v\in T}$ spans a line, its annihilator in $\bigoplus_{v\in T} H^1(G_v, (\mathrm{Ad}^0 \bar{\rho})^*)$ is codimension one. Proposition 3.2 implies $\Psi_T^{*\,-1}(\mathrm{Ann}((z_v)_{v\in T})) \neq H^1(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$, so $\Psi_T^{*\,-1}(\mathrm{Ann}((z_v)_{v\in T}))$ is codimension one in $H^1(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$. Clearly $\{\zeta_1, \dots, \zeta_s, \zeta\}$ is a basis of $H^1(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$.

For $v \in T$ put $\mathcal{L}_v = 0$ and $\mathcal{L}_q = H^1(G_q, \mathrm{Ad}^0 \bar{\rho})$. We have the Selmer group map

$$H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0 \bar{\rho}) \to \bigoplus_{v\in T} \Big(\frac{H^1(G_v, \mathrm{Ad}^0 \bar{\rho})}{0}\Big) \oplus \Big(\frac{H^1(G_q, \mathrm{Ad}^0 \bar{\rho})}{H^1(G_q, \mathrm{Ad}^0 \bar{\rho})}\Big) \tag{3.1}$$

and the dual Selmer group map

$$H^1(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*) \to \Big(\bigoplus_{v\in T} \frac{H^1(G_v, (\mathrm{Ad}^0 \bar{\rho})^*)}{H^1(G_v, (\mathrm{Ad}^0 \bar{\rho})^*)}\Big) \oplus \Big(\frac{H^1(G_q, (\mathrm{Ad}^0 \bar{\rho})^*)}{0}\Big)$$

for the set $T \cup \{q\}$. There are similar maps for T.

By Fact 2.3, $\dim H^0(G_q, \mathrm{Ad}^0 \bar{\rho}) = 1$ and $\dim(H^1(G_q, \mathrm{Ad}^0 \bar{\rho})) = 2$. Fact 2.4 implies

$$\begin{aligned}\dim(H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0 \bar{\rho})) - \dim H^1_{\mathcal{L}}(G_{T\cup\{q\}}, \mathrm{Ad}^0 \bar{\rho}) \\ = \dim H^1_{\mathcal{L}^\perp}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) - \dim H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*) - 1.\end{aligned} \tag{3.2}$$

We show $H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*)$ is spanned by (the inflations of) $\{\zeta_1, \dots, \zeta_s\}$. Observe that $H^1(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) = H^1_{\mathcal{L}^\perp}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$ has basis $\{\zeta_1 \dots, \zeta_s, \zeta\}$. As $\zeta_i|_{G_q} = 0$, (the inflations of) these elements are in $H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*)$. Any element of $H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*)$ is trivial at q and thus unramified at q and therefore inflates from $H^1_{\mathcal{L}^\perp}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*)$. It remains to consider ζ. Since $\zeta|_{G_q} \neq 0$ and $\mathcal{L}_q^\perp = 0$, we see (the inflation of) ζ is not in $H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*)$. Thus

$$\dim H^1_{\mathcal{L}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0 \bar{\rho})^*) = \dim H^1_{\mathcal{L}^\perp}(G_T, (\mathrm{Ad}^0 \bar{\rho})^*) - 1,$$

so both sides of equation (3.2) are 0. The choice of $\mathcal{L}_q = H^1(G_q, \mathrm{Ad}^0 \bar{\rho})$ implies that $H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0 \bar{\rho}) \subseteq H^1_{\mathcal{L}}(G_{T\cup\{q\}}, \mathrm{Ad}^0 \bar{\rho})$, so we have

$$H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0 \bar{\rho}) = H^1_{\mathcal{L}}(G_{T\cup\{q\}}, \mathrm{Ad}^0 \bar{\rho}).$$

We have shown that the map of equation (3.1) and

$$H^1(G_T, \mathrm{Ad}^0\,\bar\rho) \to \bigoplus_{v\in T}\Big(\frac{H^1(G_v, \mathrm{Ad}^0\,\bar\rho)}{0}\Big) \tag{3.3}$$

have identical kernels. By Fact 3.1 we see that the image of the map of equation (3.1) is one dimension bigger than image of the map in equation (3.3). Thus there is a $g \in H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$ such that $(g|_{G_v})_{v\in T} \notin \mathrm{Image}(\Psi_T)$. Recall $\{\zeta_1,\dots,\zeta_s\}$ is a basis of $\Psi_T^{*\,-1}(\mathrm{Ann}((z_v)_{v\in T}))$ and $\zeta_i|_{G_q} = 0$ by the choice of q. Then for $i = 1,\dots,s$ we see that for any c

$$0 = \sum_{v\in T\cup\{q\}} \mathrm{inv}_v(\zeta_i \cup g) = \sum_{v\in T} \mathrm{inv}_v(\zeta_i \cup g) = \sum_{v\in T} \mathrm{inv}_v\big(\zeta_i \cup (g - cz_v)\big)\,, \tag{3.4}$$

where the first equality is the global reciprocity law. Consider $\sum_{v\in T} \mathrm{inv}_v(\zeta \cup g)$. If this sum were zero, we would have that all the ζ_i and ζ annihilate g. As the annihilator of $\Psi_T^*(H^1(G_T, (\mathrm{Ad}^0\,\bar\rho)^*)$ is exactly $\Psi_T(H^1(G_T, \mathrm{Ad}^0\,\bar\rho))$, we would have that $(g|_{G_v})_{v\in T}$ is in the image of Ψ_T, a contradiction. Thus $\sum_{v\in T} \mathrm{inv}_v(\zeta \cup g) = a \neq 0$. Proposition 3.2 implies $\sum_{v\in T} \mathrm{inv}_v(\zeta \cup z_v) = b \neq 0$ for some b, so $\sum_{v\in T} \mathrm{inv}_v(\zeta \cup (g - \frac{a}{b}z_v)) = 0$. Setting $c = a/b$ in equation (3.4)), every element of the basis $\{\zeta_1,\dots,\zeta_s,\zeta\}$ of $H^1(G_T, (\mathrm{Ad}^0\,\bar\rho)^*)$ annihilates $(g - \frac{a}{b}z_v)_{v\in T}$. Thus there is a $k \in H^1(G_T, \mathrm{Ad}^0\,\bar\rho)$ such that $\Psi_T(k) = (g - \frac{a}{b}z_v)_{v\in T}$. Then, bearing in mind $a \neq 0$, we set $h^{(q)} = \frac{b}{a}(g - k) \in H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$ and have $h^{(q)}|_{G_v} = z_v$ for $v \in T$. ■

Proposition 3.5 *We retain the notations of Proposition 3.4. Let $\mathcal{P}_v = 0$ for all $v \in T$ (so $\mathcal{P}_v^\perp = H^1(G_v, (\mathrm{Ad}^0\,\bar\rho)^*)$ for $v \in T$) and let $\mathcal{P}_q = \mathcal{N}_q$ as in Fact 2.3. Then*

$$\dim H^1_{\mathcal{P}^\perp}(G_T, (\mathrm{Ad}^0\,\bar\rho)^*) = \dim H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*)$$

and the intersection $H^1_{\mathcal{P}^\perp}(G_T, (\mathrm{Ad}^0\,\bar\rho)^*) \cap H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*)$ is codimension one in each of the spaces. There is an element $\psi^{(q)} \in H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*)$ such that $\psi^{(q)} \notin H^1_{\mathcal{P}^\perp}(G_T, (\mathrm{Ad}^0\,\bar\rho)^*)$. The sum $\sum_{v\in T} \mathrm{inv}_v(\psi^{(q)} \cup h^{(q)})$ is well defined in the sense that it only depends on the image of $\psi^{(q)}$ in the one dimensional space

$$\frac{H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*)}{H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*) \cap H^1_{\mathcal{P}^\perp}(G_T, (\mathrm{Ad}^0\,\bar\rho)^*)}. \tag{3.5}$$

If $h^{(q)}|_{G_q} \notin \mathcal{P}_q$, we can scale $\psi^{(q)}$ such that

$$\mathrm{inv}_q(\psi^{(q)} \cup h^{(q)}) = -\sum_{v\in T} \mathrm{inv}_v(\psi^{(q)} \cup h^{(q)}) = 1/p.$$

Proof Since q was chosen as in Proposition 3.4, we have $f|_{G_q} = 0$ for all $f \in H^1(G_T, \mathrm{Ad}^0\,\bar\rho)$. (The inflation of) $H^1_{\mathcal{P}}(G_T, \mathrm{Ad}^0\,\bar\rho)$ is contained in $H^1_{\mathcal{P}}(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$.

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

We establish equality. A typical element of $H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$ is of the form $j+\alpha h^{(q)}$ with $j \in H^1(G_T, \mathrm{Ad}^0\,\bar\rho)$. Suppose $j+\alpha h^{(q)} \in H^1_{\mathcal{P}}(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$. As $h^{(q)}$ solves a local condition problem at T which is not solvable by elements of $H^1(G_T, \mathrm{Ad}^0\,\bar\rho)$, we immediately see $\alpha = 0$ and $j \in H^1_{\mathcal{P}}(G_T, \mathrm{Ad}^0\,\bar\rho)$. Thus

$$H^1_{\mathcal{P}}(G_T, \mathrm{Ad}^0\,\bar\rho) = H^1_{\mathcal{P}}(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho).$$

The equality of dimensions of dual Selmer groups follows from that of the Selmer groups, that q is nice and Facts 2.3 and 2.4.

Since ζ is unramified at q and $\zeta|_{G_q} \neq 0$, we see $\zeta \notin \mathcal{N}_q = \mathcal{P}_q$, so

$$\zeta \notin H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*).$$

The equality of dimensions of the dual Selmer groups for T and $T\cup\{q\}$ implies some $\psi^{(q)}$ must exist. A basis for the denominator of (3.5) is given by $\{\zeta_1,\dots,\zeta_s\}$. This establishes the codimension one statement. Proposition 3.4 and its proof imply that $\sum_{v\in T}\mathrm{inv}_v(\zeta_i\cup g) = 0$ for $i = 1,\dots,s$. As $\zeta \in H^1(G_T, (\mathrm{Ad}^0\,\bar\rho)^*)$ and the k of Proposition 3.4 is in $H^1(G_T, \mathrm{Ad}^0\,\bar\rho)$, the global reciprocity law implies $\sum_{v\in T}\mathrm{inv}_v\,(\zeta\cup k) = 0$. As $h^{(q)} = \frac{b}{a}(g-k)$, we see $\sum_{v\in T}\mathrm{inv}_v(\zeta_i\cup h^{(q)}) = 0$. The well-definedness of $\sum_{v\in T} inv_v(\psi^{(q)}\cup h^{(q)})$ is established.

The global reciprocity law implies $\sum_{v\in T}\mathrm{inv}_v(\psi^{(q)}\cup h^{(q)}) = -\,\mathrm{inv}_q(\psi^{(q)}\cup h^{(q)})$. Suppose $h^{(q)}|_{G_q} \notin \mathcal{P}_q$. By the definition of $H^1_{\mathcal{P}^\perp}(G_{T\cup\{q\}}, (\mathrm{Ad}^0\,\bar\rho)^*)$ we have $\psi^{(q)}|_{G_q} \in \mathcal{P}_q^\perp$ and is ramified at q. By Fact 2.3 we know $\mathcal{P}_q$ and $\mathcal{P}_q^\perp$ are one-dimensional in underlying two-dimensional spaces so $\mathrm{inv}_q(h^{(q)}\cup\psi^{(q)}) \neq 0$. Note $h^{(q)}$ is uniquely determined but $\psi^{(q)}$ is only determined up to scalar multiple. Now scale $\psi^{(q)}$ so that $\mathrm{inv}_q(\psi^{(q)}\cup h^{(q)}) = 1/p$. ■

Let R be given with ideals $\tilde J \supset J$ satisfying $[\tilde J : J] = p$. Let $\rho_{R/\tilde J}\colon G_T \to GL_2(R/\tilde J)$ be given and let $\rho_{R/J}$ be a deformation of $\rho_{R/\tilde J}$. For $v \in T$ we choose local deformations δ_v of $\bar\rho|_{G_v}$ to R/J such that $\delta_v \equiv \rho_{R/J} \bmod \tilde J$. Then for every $v \in T$ there will be a cohomology class $z_v \in H^1(G_v, \mathrm{Ad}^0\,\bar\rho\otimes \tilde J/J)$ such that $(I+z_v)\rho_{R/J}|_{G_v} = \delta_v$. We will find a $\rho_{R/J}$-nice prime q such that

$$h^{(q)}|_{G_q} \in H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho\otimes\tilde J/J) \simeq H^1(G_{T\cup\{q\}}, \mathrm{Ad}^0\,\bar\rho)$$

solves the local condition problem $(z_v)_{v\in T}$. If $h^{(q)}|_{G_q} \in \mathcal{N}_q$, then $(I+h^{(q)})\rho_{R/J}|_{G_q} \in \mathcal{C}_q$. Of course, $h^{(q)}|_{G_q}$ may not be in $\mathcal{N}_q$. (Deciding this seems to be a very hard problem). If $h^{(q)}|_{G_q} \notin \mathcal{N}_q$, then by allowing ramification at two $\rho_{R/J}$-nice primes q_1, q_2 we can find a linear combination $h = \alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)}$ such that $h|_{G_v} = z_v$ for $v \in T$, $h|_{G_{q_i}} \in \mathcal{N}_{q_i}$ and $(I+h)\rho_{R/J}|_{G_{q_i}} \in \mathcal{C}_q$ for $i = 1, 2$. Proposition 3.6 below and its proof are minor variations of [KLR1, Proposition 10] and its proof there.

Proposition 3.6 *Let $\rho_{R/J}$ and a local condition problem $(z_v)_{v\in T}$ be given. Let Q be a Chebotarev collection of $\rho_{R/J}$-nice primes for T as in Proposition* 3.4. *For each $q \in Q$*

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

let $h^{(q)}$ be the cohomology class of Proposition 3.4 *that solves the local condition problem $(z_v)_{v\in T}$. Then either there exists a q such that $h^{(q)}|_{G_q} \in \mathcal{N}_q$ or there are two primes $q_1, q_2 \in Q$ and a linear combination $h = \alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)}$ such that h solves the local condition problem $(z_v)_{v\in T}$ and $h|_{G_{q_i}} \in \mathcal{N}_{q_i}$ for $i = 1, 2$.*

Proof Recall from Fact 2.3 that

$$H^1(G_q, \mathrm{Ad}^0\,\bar\rho) \simeq H^1(G_q, \mathbb{Z}/p\mathbb{Z}) \oplus H^1(G_q, \mathbb{Z}/p\mathbb{Z}(1)).$$

We will write $h^{(q)}(\sigma_q)$ for the evaluation of the projection of $h^{(q)}$ to $H^1(G_q, \mathbb{Z}/p\mathbb{Z})$ at σ_q. Note $h^{(q)}|_{G_q} \in \mathcal{N}_q$ exactly when $h^{(q)}(\sigma_q) = 0$. If there is a $q \in Q$ with $h^{(q)}(\sigma_q) = 0$, then we are done.

Now assume for all primes $q \in Q$ as in Proposition 3.4 that $h^{(q)}(\sigma_q) \neq 0$. We will now find two primes $q_1, q_2 \in Q$ such that a linear combination of $h^{(q_1)}$ and $h^{(q_2)}$ will suffice to remove all local obstructions at places of v and ensure that there are no obstructions at q_1 and q_2.

Consider the 2×2 matrix $(h^{(q_i)}(\sigma_{q_j}))_{1\le i,j\le 2}$. By assumption it has nonzero diagonal entries.

	σ_{q_1}	σ_{q_2}
$h^{(q_1)}$	a	b
$h^{(q_2)}$	c	d

We want a linear combination $h := \alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)}$ for $\alpha_i \in \mathbb{Z}/p\mathbb{Z}$ such that $h(\sigma_{q_i}) = 0$ for $i = 1, 2$ and $\alpha_1 + \alpha_2 = 1$. The sum being 1 implies that h solves the local condition problem $(z_v)_{v\in T}$ as $h^{(q_1)}$ and $h^{(q_2)}$ solve it. Showing that α_1 and α_2 exist as required is equivalent to guaranteeing the matrix above has unequal rows and zero determinant.

Let y be the (necessarily nonzero) value of $h^{(q)}(\sigma_q)$ that occurs most often, that is, with maximal upper density. Let $Y = \{q \in Q \mid h^{(q)}(\sigma_q) = y\}$. Then Y may not have a density, but it has a positive upper density.

For any nice prime q define $\eta_q \in H^1(G_q, \mathbb{Z}/p\mathbb{Z}) \subset H^1(G_q, (\mathrm{Ad}^0\,\bar\rho)^*)$ by $\eta_q(\sigma_q)= 1$. As $h^{(q)}$ is ramified at q, we have for all $q \in Y$ that $\mathrm{inv}_q(\eta_q \cup h^{(q)})$ is nonzero. Let z be the value that occurs most often. Put $Z = \{q \in Y \mid \mathrm{inv}_q(\eta_q \cup h^{(q)}) = z\}$. Then Z has positive upper density.

Choose any $q_1 \in Z$. We will try to choose $q_2 \in Z$ so the 2×2 matrix

$$(h^{(q_i)}(\sigma_{q_j}))_{1\le i,j\le 2}$$

has unequal rows and determinant zero. As $q_1, q_2 \in Z \subseteq Y$, both diagonal entries will be y. Choosing $h^{(q_1)}(\sigma_{q_2})$ to be what we want (say $x \neq 0, y$) is simply a Chebotarev condition on q_2 in the field extension of $\mathbb{Q}(\mathrm{Ad}^0\,\bar\rho)$ corresponding to $h^{(q_1)}$. This condition is independent of those determining the set Q. Choosing $h^{(q_2)}(\sigma_{q_1})$ as we want (the nonzero value y^2/x in this case) involves invoking the global reciprocity law to make the choice a Chebotarev condition.

Proposition 3.5 implies $\psi^{(q_1)}|_{G_{q_1}} \in \mathcal{N}_{q_1}^{\perp} = H^1(G_{q_1}, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_{q_1}, (\mathrm{Ad}^0\,\bar{\rho})^*)$. Thus for $k \in H^1(G_{T\cup\{q_1,q_2\}}, \mathrm{Ad}^0\,\bar{\rho})$ we see $\mathrm{inv}_{q_1}(\psi^{(q_1)} \cup k)$ does not depend on the component of $k|_{G_{q_1}}$ that lies in $\mathcal{N}_{q_1} = H^1(G_{q_1}, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_{q_1}, \mathrm{Ad}^0\,\bar{\rho})$. Thus for q_1 fixed $\mathrm{inv}_{q_1}(\psi^{(q_1)} \cup k)$ depends only on $k(\sigma_{q_1})$. We have the equation in $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$:

$$\begin{aligned}
\frac{h^{(q_2)}(\sigma_{q_1})}{h^{(q_1)}(\sigma_{q_1})}\cdot 1/p &= \frac{h^{(q_2)}(\sigma_{q_1})}{h^{(q_1)}(\sigma_{q_1})}\cdot \mathrm{inv}_{q_1}(\psi^{(q_1)} \cup h^{(q_1)})\\
&= \mathrm{inv}_{q_1}(\psi^{(q_1)} \cup h^{(q_2)})\\
&= -\Big(\sum_{v\in T}\mathrm{inv}_v(\psi^{(q_1)} \cup h^{(q_2)})\Big) - \mathrm{inv}_{q_2}(\psi^{(q_1)} \cup h^{(q_2)})\\
&= -\Big(\sum_{v\in T}\mathrm{inv}_v(\psi^{(q_1)} \cup h^{(q_1)})\Big) - \mathrm{inv}_{q_2}(\psi^{(q_1)} \cup h^{(q_1)})\\
&= 1/p - \mathrm{inv}_{q_2}(\psi^{(q_1)} \cup h^{(q_2)})\\
&= 1/p - \psi^{(q_1)}(\sigma_{q_2})\,\mathrm{inv}_{q_2}(\eta_{q_2} \cup h^{(q_2)}) = 1/p - \psi^{(q_1)}(\sigma_{q_2})z.
\end{aligned}$$

The first equality uses Proposition 3.5 and the second the fact that $\mathrm{inv}_{q_1}(\psi^{(q_1)} \cup k)$ depends only on $k(\sigma_{q_1})$. The third equality is the global reciprocity law and the fourth uses the fact that $h^{(q_2)}|_{G_v} = h^{(q_1)}|_{G_v}$ for $v \in T$. The fifth equality follows from Proposition 3.5, the sixth from the definition of η_q and the seventh from the definition of the set Z. Finally

$$\frac{h^{(q_2)}(\sigma_{q_1})}{y}\cdot 1/p = 1/p - \psi^{(q_1)}(\sigma_{q_2})z.$$

So choosing $h^{(q_2)}(\sigma_{q_1})$ to be whatever value we like is equivalent to choosing $\psi^{(q_1)}(\sigma_{q_2})$ to be whatever value we like.

Having chosen $q_1 \in Z$, we need to choose $q_2 \in Z$ such that $h^{(q_1)}(\sigma_{q_2})$ and $\psi^{(q_1)}(\sigma_{q_2})$ are whatever we wish. Then we will be able to choose $h^{(q_1)}(\sigma_{q_2})$ and $h^{(q_2)}(\sigma_{q_1})$ to be a nonzero $x \neq y$ and y^2/x, respectively and we will be done. (By [R1, Lemma 10], $h^{(q_1)}$ and $\psi^{(q_1)}$ give independent Chebotarev conditions). Suppose for a given q_1 there is no $q_2 \in Z$ with the above properties. Then the set $Z\backslash\{q_1\}$ lies in Chebotarev classes that are complementary to the Chebotarev conditions on σ_{q_2} imposed by choosing $h^{(q_1)}(\sigma_{q_2}) = x$ where $x \neq 0, y$ and choosing $\zeta_{q_1}(\sigma_{q_2})$ to be whatever we like forces $h^{(q_2)}(\sigma_{q_1}) = y^2/x$. Let $D > 0$ be the density of set Q. Then these complementary Chebotarev classes form a set of density $D(1 - (p-2)/p^2)$.

Now replace q_1 by a sequence of different primes $l_i \in Z$, and assume they also allow no valid choice for the second prime. Then we see that $Z\backslash\{l_i\}$ also lies in the complimentary Chebotarev classes associated to $h^{(l_i)}$ and $\psi^{(l_i)}$. But these classes, for varying l_i, are all independent of one another ($\psi^{(l_i)}$ and $h^{(l_i)}$ being ramified at l_i), so upon imposing n such conditions, the density of the complementary classes is $D(1-(p-2)/p^2)^n$. Thus we have that $Z\backslash\{l_1,\dots,l_n\}$ is contained in a set of density $D(1-(p-2)/p^2)^n$. Letting n get arbitrarily large we get that Z is contained in a set of arbitrarily small density, so Z has upper density 0, a contradiction.

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

We can choose $\rho_{R/J}$-nice primes $\{q_1, q_2\}$ so that our matrix has the desired properties. Thus there is an $h := \alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)}$ that solves the local condition problem $(z_v)_{v\in T}$ and satisfies $h|_{G_{q_i}} \in \mathcal{N}_{q_i}$ for $i = 1, 2$. ∎

4 The Main Results

In this section for any prime v at which we will allow ramification, we will choose deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ where $\mathcal{C}_v$ is a class of deformations of $\bar{\rho}|_{G_v}$ and $\mathcal{N}_v \subset H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$ preserves $\mathcal{C}_v$. See [R2, T]. Assume

- there is a $\bar{\rho}\colon G_S \to GL_2(\mathbb{Z}/p\mathbb{Z})$ with $p \geq 5$ such that the image of $\bar{\rho}$ contains $SL_2(\mathbb{Z}/p\mathbb{Z})$ (contains $GL_2(\mathbb{Z}/p\mathbb{Z})$ if $p = 5$);
- $Ш^1_S((\mathrm{Ad}^0\,\bar{\rho})^*) = 0$ (see Fact 3.1);
- for each $v \in S$ a potentially semistable deformation to $\mathbb{Z}_p$ of $\bar{\rho}|_{G_v}$ that induces the trivial subspace $0 = \mathcal{N}_v \subset H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$.

All primes q to be added to our ramification set will be nice and the deformation conditions $(\mathcal{N}_q, \mathcal{C}_q)$ will be as in [R2]. See also Fact 2.3.

For the $\mathcal{N}_v$ chosen in [T] one had $\dim H^1_{\mathcal{N}}(G_T, \mathrm{Ad}^0\,\bar{\rho}) = \dim H^1_{\mathcal{N}^\perp}(G_T, (\mathrm{Ad}^0\,\bar{\rho})^*)$ for any $T \supseteq S$ for which $T\backslash S$ consisted only of nice primes. Our choice of $\mathcal{N}_v = 0$ for $v \in S$ forces $\mathcal{N}_v^\perp = H^1(G_v, (\mathrm{Ad}^0\,\bar{\rho})^*)$ for $v \in S$. Thus, in our setting

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

Using the results of [T], one can introduce nice primes q to the set S such that the Selmer group for this larger set of ramification is trivial. We now use [KLR1, Corollary 14] to find a set B of one or two nice primes such that the map $H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0\,\bar{\rho}) \hookrightarrow H^1_{\mathcal{N}}(G_{S\cup B}, \mathrm{Ad}^0\,\bar{\rho})$ has cokernel of dimension one. (We remark that [KLR1, Corollary 14] follows immediately from [KLR1, Proposition 10] of which Proposition 3.6 here is a variant suited for our purposes). Let $S_1 = S \cup B$.

We consider a sequence of deformation problems ramified at an increasing set of places S_n with specified deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ and deformation rings $R_n = \mathbb{Z}_p[\![T_1, \dots, T_n]\!]/J_n$ such that $J_n \subseteq (p, T_1, \dots, T_n)^n$. Note that $R_n/\,\mathrm{m}^n_{R_n} = \mathbb{Z}_p[\![T_1, \dots, T_n]\!]/(p, T_1, \dots, T_n)^n$. Furthermore, the deformation to $R_{n+1}/\,\mathrm{m}^{n+1}_{R_{n+1}}$ will satisfy all the deformation conditions of places in S_n. Thus we will have maps

$$R_{n+1} = \mathbb{Z}_p[\![T_1, \dots, T_{n+1}]\!]/J_{n+1} \twoheadrightarrow R_{n+1}/\,\mathrm{m}^{n+1}_{R_{n+1}} \twoheadrightarrow R_n/\,\mathrm{m}^n_{R_n} \twoheadleftarrow R_n.$$

Taking the inverse limit of the deformations to $GL_2(R_n/\,\mathrm{m}^n_{R_n})$ gives a deformation to $GL_2(\mathbb{Z}_p[\![T_1, \dots, T_d, \dots]\!])$.

We construct the sequence inductively, the base case of $n = 1$ being done. We may suppose we have a map $\rho_n\colon G_{S_n} \to GL_2(R_n/\,\mathrm{m}^n_{R_n})$ and $\dim H^1_{\mathcal{N}}(G_{S_n}, \mathrm{Ad}^0\,\bar{\rho}) = n$.

Corollary 14 of [KLR1] provides a set B of one or two $(\rho_n)_{R_n/\,\mathrm{m}^n_{R_n}}$-nice primes such that the map $H^1_{\mathcal{N}}(G_{S_n}, \mathrm{Ad}^0\,\bar{\rho}) \hookrightarrow H^1_{\mathcal{N}}(G_{S_n\cup B}, \mathrm{Ad}^0\,\bar{\rho})$ has cokernel of dimension one. Let U be the deformation ring and ρ_U the deformation for the augmented problem with deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ at $v \in S_n \cup B$. Since the prime(s) of B are

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

$(\rho_n)_{R_n/\mathfrak{m}_{R_n}^n}$-nice, we see $(\rho_n)_{R_n/\mathfrak{m}_{R_n}^n}|_{G_q} \in \mathcal{C}_q$ for $q \in B$ so U surjects onto $R_n/\mathfrak{m}_{R_n}^n$. Thus U has

$$\mathbb{Z}/p\mathbb{Z}[\![T_1,\ldots,T_{n+1}]\!]/(T_1,\ldots,T_{n+1})^2 \quad \text{and} \quad \mathbb{Z}_p[\![T_1,\ldots,T_n]\!]/(p,T_1,\ldots,T_n)^n$$

as quotients. Let $\tilde{J}$ be the intersection of the kernels of these quotient maps. Put $U_0 = U/\tilde{J}$. If U_0 has $\mathbb{Z}_p[\![T_1,\ldots,T_{n+1}]\!]/(p,T_1,\ldots,T_{n+1})^{n+1}$ as a quotient, the induction is complete.

If not, there is an inverse sequence of rings

$$U_0 \twoheadleftarrow U_1 \twoheadleftarrow \cdots \twoheadleftarrow \mathbb{Z}_p[\![T_1,\ldots,T_{n+1}]\!]/(p,T_1,\ldots,T_{n+1})^{n+1}$$

such that at each stage the kernel has order p. We will add more primes of ramification to realise each of these intermediate rings as a suitable deformation ring. At each stage the augmented local deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ will be satisfied by the previous ring.

The deformation ρ_{U_0} to U_0 induced by ρ_U satisfies $\rho_{U_0}|_{G_v} \in \mathcal{C}_v$ for $v \in S_n \cup B$. Thus there are no local obstructions to deforming ρ_{U_0} to U_1. By Fact 3.1, there is no global obstruction to deforming ρ_{U_0} to U_1. Let $\tilde{\rho}_{U_1}$ be such a deformation. If $\tilde{\rho}_{U_1}|_{G_v} \in \mathcal{C}_v$ for $v \in S_n \cup B$, we can deform $\tilde{\rho}_{U_1}$ to U_2. Henceforth we suppose that for any deformation $\tilde{\rho}_{U_1}$ of ρ_{U_0} that $\tilde{\rho}_{U_1}|_{G_v} \notin \mathcal{C}_v$ for some $v \in S_n \cup B$.

Let J be the (order p) kernel of the map $U_0 \leftarrow U_1$. Then there are cohomology classes $(z_v)_{v \in S_n \cup B}$ with $z_v \in H^1(G_v, \mathrm{Ad}^0\,\bar{\rho} \otimes J)$ such that $(I + z_v)\tilde{\rho}_{U_1}|_{G_v} \in \mathcal{C}_v$ for $v \in S_n \cup B$. Recall that $\Psi_{S_n \cup B}$ is the restriction map at all places of $S_n \cup B$. We are assuming that

$$(z_v)_{v \in S_n \cup B} \notin \Big(\bigoplus_{v \in S_N \cup B} \mathcal{N}_v\Big) \oplus \Psi_{S_n \cup B}(H^1(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho})).$$

Otherwise there is an $h \in H^1(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho} \otimes J)$ such that $(I + h)\tilde{\rho}_{U_1}|_{G_v} \in \mathcal{C}_v$ for all $v \in S_n \cup B$.

We now apply Proposition 3.6 to get a set A of one or two primes and a cohomology class $h \in H^1(G_{S_n \cup B \cup A}, \mathrm{Ad}^0\,\bar{\rho})$ such that

- any $q \in A$ is $\tilde{\rho}_{U_1}$-nice,
- $h|_{G_q} \in \mathcal{N}_q$ for $q \in A$,
- $h|_{G_v} = (z_v)$ for $v \in S_n \cup B$.

Proposition 4.1 *For A as above and*

$$(z_v)_{v \in S_n \cup B} \notin \Big(\bigoplus_{v \in S_N \cup B} \mathcal{N}_v\Big) \oplus \Psi_{S_n \cup B}(H^1(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho}))$$

we have $H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0\,\bar{\rho}) = H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho})$.

Proof By the third condition of Proposition 3.4 , elements of $H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho})$ are trivial at the places of B so $H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho}) \subseteq H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0\,\bar{\rho})$. It remains to check equality. If A contains one prime, then any element of

$$H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0\,\bar{\rho}) \backslash H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0\,\bar{\rho})$$

https://doi.org/10.4153/CJM-2008-009-7 Published online by Cambridge University Press

is necessarily of the form $f + \alpha h^{(q)}$ with $f \in H^1(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$ and $\alpha \neq 0$. Thus $\alpha h^{(q)}|_{G_v} = \alpha z_v \in -f + \mathcal{N}_v$ for all $v \in S_n \cup B \cup A$. Our hypothesis on $(z_v)_{v \in S_n \cup B}$ implies $\alpha = 0$, which is a contradiction.

Suppose A contains two primes. An element of

$$H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0 \bar{\rho}) \backslash H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$$

is necessarily of the form $f + \alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)}$ with $f \in H^1(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$. Thus $(\alpha_1 h^{(q_1)} + \alpha_2 h^{(q_2)})|_{G_v} = (\alpha_1 + \alpha_2) z_v \in -f + \mathcal{N}_v$ for all $v \in S_n \cup B \cup A$. Our hypotheses imply $\alpha_2 = -\alpha_1$. Thus we must check whether $f + \alpha_1(h^{(q_1)} - h^{(q_2)}) \in H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0 \bar{\rho})$. But $\alpha_1(h^{(q_1)} - h^{(q_2)})|_{G_v} = 0$ for all $v \in S_n \cup B$ which implies $f|_{G_v} \in \mathcal{N}_v$ for all $v \in S_n \cup B$ so $f \in H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$. By the third condition of Proposition 3.4 we see $f|_{G_{q_i}} = 0$ for $i = 1, 2$ so $f \in H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0 \bar{\rho})$. Thus $\alpha_1(h^{(q_1)} - h^{(q_2)}) \in H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0 \bar{\rho})$ so $\alpha_1(h^{(q_1)} - h^{(q_2)})|_{G_{q_i}} \in \mathcal{N}_{q_i}$ for $i = 1, 2$. This corresponds to the matrix in the proof of Proposition 3.6 having equal rows. The matrix was constructed to have unequal rows, so $\alpha_1 = 0$ and $f \in H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$, which is a contradiction.

Thus $H^1_{\mathcal{N}}(G_{S_n \cup B \cup A}, \mathrm{Ad}^0 \bar{\rho}) = H^1_{\mathcal{N}}(G_{S_n \cup B}, \mathrm{Ad}^0 \bar{\rho})$. ■

Put $\rho_{U_1} = (I + h)\tilde{\rho}_{U_1}|_{G_v}$. Then $\rho_{U_1}|_{G_v} \in \mathcal{C}_v$ for $v \in S_n \cup B \cup A$. We see that the deformation ring with deformation conditions $(\mathcal{N}_v, \mathcal{C}_v)$ at $v \in S_n \cup B \cup A$ has U_1 as a quotient. By Proposition 4.1 this ring has the same dual tangent space as U_0. Iterating this argument, we get, after allowing ramification at more primes, a deformation ring that has $\mathbb{Z}_p[[T_1, \dots, T_{n+1}]]/(p, T_1, \dots, T_{n+1})^{n+1}$ as quotient. Let S_{n+1} be the set of ramified places of this deformation. We have completed the induction described at the beginning of this section.

Taking the inverse limit of the representations $\rho_n \colon G_{S_n} \to GL_2(R_n/\,\mathrm{m}_R^n)$, we obtain a deformation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p[[T_1, \dots, T_d, \dots]])$. All that remains is to prove fullness of image.

Proposition 4.2 *For $n \geq 2$ we have that ρ_n is full.*

Proof By [Bo, Proposition 2], we need to show that the mod $(p, T_1, \dots, T_n)^2$ reduction of ρ_n is full. Observe that the kernel of the map $SL_2(R_n/\,\mathrm{m}^2_{R_n}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$, when viewed as a $\mathbb{Z}/p\mathbb{Z}[\mathrm{Image}(\bar{\rho})]$-module, consists of $n + 1$ copies of the adjoint. Since ρ_n is the solution of a deformation problem, there are n copies of $\mathrm{Ad}^0 \bar{\rho}$ corresponding to basis elements of the dual tangent space of our deformation problem. These give rise to split extensions. Since $n \geq 2$, there is also a deformation to $GL_2(\mathbb{Z}/p^2\mathbb{Z})$. For $p \geq 5$, a routine computation shows that an element of order p in $SL_2(\mathbb{Z}/p\mathbb{Z})$ deforms to an element of order p^2 in $SL_2(\mathbb{Z}/p^2\mathbb{Z})$. Thus the deformation to $\mathbb{Z}/p^2\mathbb{Z}$ provides a nonsplit extension which gives the last copy we need of $\mathrm{Ad}^0 \bar{\rho}$. ■

We now complete the proof of the Theorem 1.1. Let

$$R = \varprojlim_n R_n/\,\mathrm{m}^n_{R_n} \simeq \mathbb{Z}_p[[T_1, \dots, T_d, \dots]].$$

Clearly $R \twoheadrightarrow R_n/\mathfrak{m}_{R_n}^n$. Let $A \in SL_2(R)$ have determinant 1 with image $A_n \in SL_2(R_n/\mathfrak{m}_{R_n}^n)$. Then $A = \varprojlim_n A_n$. By Proposition 4.2 there is a $g_n \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\rho_n(g_n) = A_n$.

Since $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is compact and Hausdorff, we see there is a subsequence $\{g_{n_m}\}$ of $\{g_n\}$ that has a limit point $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We have

$$\rho(g) = \varprojlim_n \rho_n(g) = \varprojlim_n \rho_n(\varinjlim_m g_{n_m}) = \varprojlim_n \varinjlim_m \rho_n(g_{n_m})$$

where the last equality is by continuity of ρ_n. For $n_m > n$ we know ρ_{n_m} is a deformation of ρ_n so $n_m > n$ implies the image of $A_{n_m} = \rho_{n_m}(g_{n_m})$ in $SL_2(R_n/\mathfrak{m}_{R_n}^n)$ is A_n so $\rho_n(g_{n_m}) = A_n$. Thus

$$\rho_n(g) = \varinjlim_m \rho_n(g_{n_m}) = \varinjlim_m A_n = A_n$$

$$\rho(g) = \varprojlim_n \rho_n(g) = \varprojlim_n A_n = A.$$

Acknowledgements I thank the anonymous referee for several helpful comments. It is a pleasure to thank C. Khare and M. Larsen. My numerous conversations with them have proved invaluable. In particular I thank them for the invitation to collaborate in the project that resulted in [KLR1, KLR2]. The ideas of those papers were crucial in this one.

References

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

[Bo] N. Boston, Appendix to *On p-adic families of Galois representations*, by A. Wiles and B. Mazur. Compositio Math. **59**(1986), no. 2, 261–264.

[KLR1] C. Khare, M. Larsen, and R. Ramakrishna, *Constructing semisimple p-adic Galois representations with prescribed properties.* Amer. J. Math. **127**(2005), no. 4, 709–734.

[KLR2] ———, *Transcendental ℓ-adic Galois representations.* Math Res. Let. **12**(2005), no. 5-6, 685–699.

[M1] B. Mazur, *Deforming Galois representations.* In: Galois Groups over $\mathbb{Q}$. Math. Sci. Res. Inst. Publ. 16, Springer-Verlag, Berlin, 1989.

[M2] ———, *An introduction to the deformation theory of Galois representations.* In: Modular Forms and Fermat's Last Theorem. Springer, New York, 1997, pp. 243–311.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

[R1] R. Ramakrishna, *Lifting Galois representations.* Invent. Math. **138**(1999), no. 3, 537–562.

[R2] ———, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur.* Ann. of Math. **156**(2002), no. 1, 115–154.

[Ro1] D. Rohrlich, *False division towers of elliptic curves.* J. Algebra **229**(2000), no. 1, 249–279.

[Ro2] ———, *Modular units and the surjectivity of a Galois representation.* J. Number Theory **107**(2004), no. 1, 8–24.

[T] R. Taylor, *On icosahedral Artin representations. II.* Amer. J. Math. **125**(2003), no. 3, 549–566.

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

Department of Mathematics
Cornell University
Ithaca, NY 14853
U.S.A.
e-mail: ravi@math.cornell.edu