QUANTITATIVE LEVEL LOWERING FOR GALOIS REPRESENTATIONS

NAJMUDDIN FAKHRUDDIN, CHANDRASHEKHAR KHARE, AND RAVI RAMAKRISHNA

ABSTRACT. We use Galois cohomology methods to produce optimal mod $p^d$ level lowering congruences to a $p$-adic Galois representation that we construct as a well chosen lift of a given residual mod $p$ representation. Using our explicit Galois cohomology methods, we construct for a reductive group $G$ and a given residual representation $\bar{\rho} : \Gamma \to G(k)$, ramified at a finite set of primes $S_i$, in favorable conditions that we identify, a finite set of lifts $\rho \in \{\rho^i\}$ of $\bar{\rho}$ to $G(W(k))$ with the following properties: $\rho : \Gamma \to G(W(k))$ is ramified precisely at $S \cup Q$, with $Q$ a finite set of primes disjoint from $S$. For $q \in Q$, $\rho_q : G \to G(W(k))$ is unramified outside $S \cup Q \setminus \{q\}$ and $\rho$ and $\rho^q$ are congruent mod $p^d$ if $\rho$ mod $p^d$ is unramified at $q$. Furthermore, the Galois representations $\{\rho^i\}$ are "independent".

1. INTRODUCTION

The study of congruences between modular forms is an important ingredient in studying the relationship between deformation rings of Galois representations and Hecke algebras. The work of Ribet on level raising and level lowering congruences between modular forms, cf. [Rib84], [Rib90], used cohomological and arithmetic-geometric properties of Jacobians of modular curves. More recently the lifting method of [KW09], and its generalizations in [BLGGT14], produces level raising and lowering congruences between Galois representations (and a fortiori automorphic forms) using automorphy lifting methods which have their origin in [Wil95].

1.1. Our results. In this paper we use Galois cohomology to produce congruences between Galois representations which do not seem accessible by the usual methods. For instance, in the classical case of reducible odd representations $\bar{\rho} : \Gamma \to GL_2(k)$ with $k$ a finite field of characteristic $p > 3$, we prove the following theorem which does not seem amenable to geometric [Rib84] or automorphy lifting [KW09] methods.

**Theorem 1.1.** Let $\bar{\rho} : \Gamma \to GL_2(\mathbb{F}_p)$ be an odd, irreducible modular mod $p > 3$ surjective representation of square-free conductor $N(\bar{\rho}) = N$ and finite flat at $p$ with determinant the mod $p$ cyclotomic character. Assume that the minimal Selmer group is non-zero. Then there are newforms $f \in S_2(\Gamma_0(N\Pi_{q\in Q}q))$, with $Q = \{q_1, \cdots, q_r\}$ a finite set of primes that are coprime to $Np$, such that the corresponding Galois representation associated to an embedding $\iota : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $\rho_{f,\iota} : \Gamma \to GL_2(\mathbb{Z}_p)$ lifts $\bar{\rho}$ and has the following properties:

- $\rho_{f,\iota}(\tau_q)$, for $\tau_q$ a generator of the $\mathbb{Z}_p$-quotient of the inertia group $I_q$ at $q$, is of the form
  \[
  \begin{pmatrix}
  1 & p^d \\
  0 & 1
  \end{pmatrix},
  \]
  for all $q \in Q$ and for some integer $d \geq 2$.

- For each $1 \leq i \leq r$, there is a subset $Q_i$ of $Q$ that omits $q_i$ and contains $\{q_1, \cdots, q_{i-1}\}$, and there is a newform $f_i$ in $S_2(\Gamma_0(N\Pi_{q\in Q_i}q))$, new at $Q_i$, with $f_i$ congruent to $f$ modulo $p^d$.

We in fact prove such a result for Galois representations without assuming $\bar{\rho}$ is modular, and deduce the statement for newforms in the case when $\bar{\rho}$ is modular using level raising results for modular forms. We regard our result as a quantitative level lowering result for the $p$-adic Galois
representation \( \rho_{f,v} \). As we show in \( \text{[4]} \), the “independent” level-lowering congruences we produce in such a result can be used in proving automorphy lifting results. Note that the terminology of quantitative level-lowering has been used earlier in \( \text{[PW11]} \). (The technical condition of the initial dual Selmer being non-trivial for our applications is not too burdensome, otherwise the minimal deformation ring is smooth and hence proven to be isomorphic to the corresponding Hecke algebra by the results of \( \text{[DT91]} \).)

Theorem \( \text{[1.3]} \) is a particular case of the main result of this paper, Theorem \( \text{[2.16]} \) which we now state. We refer to \( \text{[1.2]} \) for the basic notation used in the theorem, and the main body of the paper for the precise assumptions.

**Theorem 1.2.** Let \( F \) be any number field, \( S \) a finite set of finite primes of \( F \) and \( \bar{\rho} : \Gamma_S \to G(k) \) a continuous representation. We assume \( \bar{\rho} \) has “large image” (i.e., satisfies Assumption \( \text{[2.1]} \) and \( p = \text{char}(k) \) is sufficiently large (i.e., the hypotheses of Proposition \( \text{[2.4]} \) hold). We assume further that we are given smooth local conditions \( N = \{N_v\}_{v \in S} \) for \( \bar{\rho} \) which are “balanced”, i.e., the dimensions of the corresponding Selmer and dual Selmer groups are equal (see Assumption \( \text{[2.14]} \) to an integer \( n \) which we assume is nonzero. Then there exists a set \( Q = \{q_1, q_2, \ldots, q_m\} \) of nice primes of \( F \) (see Definition \( \text{[2.1]} \)), \( m \in \{n + 1, n + 3\} \), and an integer \( d \geq 2 \) such that

- \( Q \) is auxiliary (see Definition \( \text{[2.1]} \)) and the versal deformation \( \rho_{S \cup Q}^{Q-\text{new}} : \Gamma_{S \cup Q} \to G(R_{S \cup Q}^{Q-\text{new}}) = G(W(k)) \) is ramified mod \( p^d \) at all \( q \in Q \).
- for each \( 1 \leq i \leq m \) there is an auxiliary set \( Q_i \subset Q \) satisfying
  - \( \{1, 2, \ldots, q_{i-1}\} \subset Q_i \),
  - \( q_i \notin Q_i \),
  - \( \rho_{S \cup Q_i}^{Q-\text{new}} \equiv \rho_{S \cup Q}^{Q-\text{new}} \mod p^{d-1} \), \( \rho_{S \cup Q_i}^{Q-\text{new}} \mod p^{d-1} \) is special (see Definition \( \text{[2.1]} \)) at \( q_i \),
  - but \( \rho_{S \cup Q_i}^{Q-\text{new}} \mod p^d \) is not special at \( q_i \).

Our Galois cohomological method to produce congruences has its origin in the method of lifting mod \( p \) Galois representations to characteristic 0 introduced in \( \text{[Ram02]} \). The last author showed in loc. cit. that given an odd irreducible representation \( \bar{\rho} : \Gamma_Q \to GL_2(k) \) satisfying mild technical conditions, with \( k \) a finite field of characteristic \( p \), there is a geometric lift that is uniquely determined by suitably chosen ramification conditions (e.g., the condition of being Steinberg at the finite set \( Q \) of auxiliary primes). This method has been generalized by Patrikis in \( \text{[Pat16]} \) to the setting of representations \( \bar{\rho} : \Gamma_F \to G(k) \), with \( G \) a reductive algebraic group over \( W(k) \) and \( F \) a CM field, considering deformations that are balanced. (The results in loc. cit. are proved under several technical hypotheses which we will need to assume in our work as well, see Theorem \( \text{[2.16]} \) below: for example, the image of \( \bar{\rho} \) is assumed to be large in a suitable sense. We note that the recent paper \( \text{[FKP19]} \) addresses lifting residual representations without assuming they have large image.)

The lifting method of \( \text{[Ram02]} \) in the classical case (and its generalization in \( \text{[Pat16]} \)) considers deformations of \( \bar{\rho} \) that are unramified outside \( S \cup Q \) with \( Q \) a suitable auxiliary finite set of places. Here \( S \) consists of places at which \( \bar{\rho} \) is ramified and the places above \( p \), \( \infty \) with balanced, smooth, minimal deformation conditions at these places. The set \( Q \) consists of residually Steinberg places \( v \), i.e., \( v \) such that (in the 2-dimensional case) \( \bar{\rho}(\text{Frob}_v) \) has eigenvalues \( \alpha_v, \beta_v \) with ratio \( \alpha_v/\beta_v = q_v \neq \pm 1 \mod p \). The deformation condition for \( v \in Q \) is of being Steinberg at \( v \), i.e., deformations such that the image of (a lift of) \( \text{Frob}_v \) has eigenvalues \( \tilde{\alpha}_v, \tilde{\beta}_v \), which lift \( \alpha_v, \beta_v \) and their ratio \( \tilde{\alpha}_v/\tilde{\beta}_v = q_v \). This condition is smooth, is non-minimal, and cuts out a subspace of the local cohomology that intersects the unramified cohomology in a codimension one subspace, and the tangent space has dimension \( h^0(\Gamma_v, \text{Ad}^0\bar{\rho}) \). The corresponding deformation problem is balanced and the resulting
deformation ring $R_{1Q}^{Q-new}$ has a presentation of the form $W(k)[[X_1, \cdots, X_r]]/(f_1, \cdots, f_s)$ with $r = s = h^1_{L} = h^1_{L\perp}$. The main innovation of [Ram02], as formulated in [Tay03], is a method of killing the dual Selmer group for a residual representation $\bar{\rho}$ when deformation conditions considered at auxiliary places are smooth. (Killing dual Selmer for $\bar{\rho}$ with smooth conditions is essential to lift $\bar{\rho}$ to characteristic 0. The method of Wiles which allows one to kill dual Selmer with unrestricted, and hence non-smooth, conditions at auxiliary primes does not imply the existence of liftings of $\bar{\rho}$.) It produces a set $Q$ consisting of finitely many residually Steinberg places for $\bar{\rho}$ as above with the Steinberg deformation condition at these places, such that the global deformation problem is smooth. The corresponding balanced smooth deformation ring $R_{S\cup Q}^{Q-new}$ is $W(k)$.

The work of [KR03] in the classical case, and its generalization in [MMS17] to the context of $G$-valued representations considered in [Pat16], shows that we can choose $Q$ with the further property that the universal representation $\rho^{Q-new}$ is ramified at primes in $Q$. This gives that the augmentation $\pi: R_{S\cup Q} \to R_{S\cup Q}^{Q-new}$, where $R_{S\cup Q}$ parametrizes deformations with “rank one” ramification allowed at $Q$, has finite cotangent space, and thus the $Q$-new quotient is an irreducible component of $R_{S\cup Q}$. The main work in this paper is to construct such $Q$ with the additional property that there are congruences of $\pi$ to other augmentations which can be thought of as level lowering congruences.

Building on [Ram02] and its generalization in [Pat16] to $G$-valued representations, and improving upon the “doubling method” of [KLR05], we prove Theorem 2.10 below in [2]. The second author had conceived of a result like Theorem 1.1 at the time of writing [Kha03], but was unable to prove it at the time. Our proof draws upon developments of the method of the third author [Ram02] since that time (cf. [KLR05]).

1.2. Motivation. One of the motivations of our work is an attempt to find a technique to prove that certain deformation rings are of the expected dimension. Let $\bar{\rho}: \Gamma_F \to G(k)$ be a continuous, irreducible representation with $G$ a reductive algebraic group over $W(k)$. Let $S$ be a finite set of places $\mathcal{P}$ of $F$, where $S$ includes the places of $F$ above $p$ and places at which $\bar{\rho}$ is ramified. We consider deformations $\rho: \Gamma_F \to G(R)$ of $\bar{\rho}$ to complete noetherian local $W(k)$-algebras $R$ with residue field $k$. At places outside $S$ the deformation condition is that of being unramified, and at places in $S$ the deformations $\mathcal{D}_v$ satisfy an infinitesimal lifting property (i.e., smoothness), and the corresponding tangent spaces $\mathcal{L}_v$ satisfy one of the following:

- favorable condition $\sum_{v \in S} \dim_k \mathcal{L}_v \geq \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$, or the more restrictive,
- balanced condition $\sum_{v \in S} \dim_k \mathcal{L}_v = \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$.

Here $\bar{\rho}(\mathfrak{g}^{\text{der}})$ denotes the Lie algebra of the derived group of $G$ with the action of $\Gamma_F$ induced by composing $\bar{\rho}$ with the adjoint representation of $G$. Typically this is achieved by imposing deformation conditions at places of $\mathcal{P}$ not above $p$ (and $\infty$) such that $\dim_k \mathcal{L}_v = h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$, and at places above $p$ that $\sum_{v \in S_p} \dim_k \mathcal{L}_v \geq \sum_{v \in S_p} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})) + \sum_{v \in S_{\infty}} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$. (The spaces $\mathcal{L}_v$ are trivial for $v$ the infinite places of $F$ (for $p > 2$).) We have the corresponding Selmer and dual Selmer groups $H^1_{\mathcal{L}}(\Gamma_F, \bar{\rho}(\mathfrak{g}^{\text{der}}))$ and $H^1_{\mathcal{L}\perp}(\Gamma_F, \bar{\rho}(\mathfrak{g}^{\text{der}}))$ whose dimension over $k$ is denoted by $h^1_{\mathcal{L}}$ and $h^1_{\mathcal{L}\perp}$. When deformation conditions are favorable we have the inequality $h^1_{\mathcal{L}} \geq h^1_{\mathcal{L}\perp}$, and in the balanced case the equality $h^1_{\mathcal{L}} = h^1_{\mathcal{L}\perp}$. We remark that known methods to produce finitely ramified liftings succeed only when these dimensions satisfy the favorable inequality $h^1_{\mathcal{L}} \geq h^1_{\mathcal{L}\perp}$.

As we are assuming the deformation conditions are smooth at places in $S$ (e.g., minimal deformation conditions), the corresponding deformation ring $R_S$ has a presentation as a quotient $W(k)[[X_1, \cdots, X_r]]/(f_1, \cdots, f_s)$, with $r = h^1_{\mathcal{L}}, s = h^1_{\mathcal{L}\perp}$. In favorable situations one expects that
if in addition the local conditions are natural (unrestricted, ordinary, ...) then the corresponding deformation ring is a finite flat complete intersection of relative dimension $h_{\ell}^1 - h_{\ell}^1$ over $W(k)$. Thus, in balanced situations one might expect that in many cases the ring $R_S$ is a finite $W(k)$-module. (This may not always be the case as was pointed out to us by G. Boxer and F. Calegari.)

Using Theorem 2.16 we get an auxiliary set $S$ such that a related ring $R_{S\cup Q}^{Q-new} = W(k)$, and thus an augmentation $\pi : R_{S\cup Q}^{Q-new} \rightarrow W(k)$ which gives rise to the Galois representation $\rho_{S\cup Q}^{Q-new} : \Gamma_{S\cup Q} \rightarrow G(R_{S\cup Q}^{Q-new}) = G(W(k))$ such that that $\rho_{S\cup Q}^{Q-new}$ is ramified at all the primes in $Q$. Furthermore there is an integer $d$ such that $\rho_{S\cup Q}^{Q-new} \bmod p^d$ is unramified at all the primes in $Q$, and $\rho_{S\cup Q}^{Q-new} \bmod p^{d+1}$ is ramified at all the primes in $Q$. This allows one to prove that the cotangent space at $\pi$ is finite, and in fact we can compute it to be exactly $\oplus_q W(k)/p^d$ (Theorem 3.1). Wiles's numerical criterion, which we attempt to enhance in §5 (Proposition 5.1), suggests that if we can verify his numerical coincidence $\#\Phi_{\pi} = \#W(k)/\eta_{\pi}$, with $\Phi_{\pi}$ the cotangent space of $\pi$ and $\eta_{\pi} = \pi(Ann_{R_{S\cup Q}}(Ker \pi))$, in this situation we could get a grip on $R_{S\cup Q}$ (and hence $R_S$). The depth of $\pi(Ann_{R_{S\cup Q}}(Ker \pi))$ is related to congruences between $\pi$ and other augmentations, and we produce in a sense optimal level lowering congruences to $\rho_{S\cup Q}^{Q-new}$. This still falls short of getting the Wiles numerical coincidence, but is suggestive of it.

Here is a description of the contents of the paper. In the key §2 we prove our main theorem Theorem 2.16. In §3 we give an exact computation of Selmer groups associated to the Galois representation we construct and prove that it is a smooth point of the relevant deformation ring. In §4 we illustrate the use of our main theorem, in conjunction with Wiles's numerical isomorphism criterion, to prove automorphy lifting in the classical case. In §5 we refine Wiles's numerical isomorphism criterion, which was prompted by the motivation we mention above.

1.3. Notation. For a field $K$, $\Gamma_K$ will denote the absolute Galois group of $K$. If $F$ is a number field and $q$ is a prime of $\mathcal{O}_F$, the ring of integers of $F$, then the absolute Galois group of the completion of $F$ at $q$ will be denoted by $\Gamma_q$ with $I_q \subset \Gamma_q$ denoting the inertia subgroup; we will implicitly identify, by making a choice, $\Gamma_q$ with a decomposition subgroup of $\Gamma_F$. For $X$ a finite set of (finite) primes of $\mathcal{O}_F$, $\Gamma_X$ denotes the group $Gal(F_X/F)$, where $F_X$ is the maximal extension of $F$ (in a fixed algebraic closure) unramified outside primes in $X$ (and the infinite primes). Throughout this paper we fix a rational prime $p$ and denote let $\kappa : \Gamma_F \rightarrow \mathbb{Z}_p^\times$ be the $p$-adic cyclotomic character; we also use $\kappa$ to denote the characters arising from $\kappa$ by restriction to subgroups of $\Gamma_F$, on quotients of $\Gamma_F$ by subgroups containing $Ker(\kappa)$, or by extension of scalars to any $\mathbb{Z}_p$-algebra $R$. We let $k$ be a finite field of characteristic $p$ and $W(k)$ the ring of Witt vectors of $k$.

For $M$ a finitely generated free module over a $\mathbb{Z}_p$-algebra $R$ we let $M^\vee$ denote the module $\text{Hom}_R(M,R)$. If $M$ also has a Galois action we denote by $M^*$ the Galois module $\text{Hom}(M,R(\kappa))$. For $M$ a finite $W(k)$-module, $\ell(M)$ denotes the length of $M$.

Let $G$ be a split (connected) reductive group scheme over $W(k)$ and let $G^{sc}$ be the simply connected cover of the derived group scheme $G^{der} = [G,G]$; we assume that $G^{der}$ is almost simple.

---

1Here is an example suggested by Boxer and Calegari which illustrates that favorable deformation conditions may not always imply that the generic fiber of the corresponding deformation ring has the expected relative dimension $h_{\ell}^1 - h_{\ell}^1$. Consider 2-dimensional ordinary representations for a CM field $K$ with totally real subfield $F$, $\tilde{\rho} : \Gamma_K \rightarrow GL_2(k)$, and impose the favorable deformation condition that the weights are equal at complex conjugate places of $K$ above $p$. Then the dimension of the ordinary deformation ring of $\tilde{\rho}$ will be bigger than the expected dimension ($= 0$) if $\tilde{\rho}$ is restricted from the totally real subfield. The locus of lifts which come by restriction from $F$ gives a component of dimension $[F : \mathbb{Q}]$. The “discrepancy” of the actual dimension from the expected one is explained by functoriality.
Let \( \mu : G \to C \) be the maximal torus quotient of \( G \). Let \( \mathfrak{g} \) be the Lie algebra of \( G \) and \( \mathfrak{g}^\text{der} \) the Lie algebra of \( G^\text{der} \); it is also the kernel of the map on Lie algebras induced by \( \mu \). We assume that \( p \) is sufficiently large so that the Killing form induces a \( G \)-equivariant isomorphism of \( \mathfrak{g}^\text{der} \) and its linear dual (see, e.g. \[Sel57\], for explicit bounds on \( p \)).

1.4. **Acknowledgements.** C.K. was partially supported by NSF grant DMS-1601692 and a Humboldt Research Award, and thanks TIFR for its hospitality in periods during which the work was carried out. R.R. was partially supported by Simons Collaboration grant #524863. We thank Mohammed Zuhair for helpful conversations.

2. Quantitative level lowering for Galois representations

The main result of this section is Theorem 2.16. We begin by introducing nice primes and prove several local results related to them. After this, the main theorem is stated precisely in 2.4. We then prove some global lemmas and the main steps of the proof are given in 2.7, 2.8 and 2.9.

Let \( F \) be a number field and and \( \overline{\rho} : \Gamma_F \to G(k) \) a continuous homomorphism. Let \( S \) be a finite set of primes of \( \mathcal{O}_F \) including all primes ramified in \( \overline{\rho} \) and all primes lying over \( p \); henceforth view \( \overline{\rho} \) as a map \( \Gamma_S \to G(k) \). Fix \( \nu : \Gamma_S \to \mathcal{C}(W(k)) \) a continuous lift of the map \( \mu \circ \overline{\rho} : \Gamma_S \to \mathcal{C}(k) \) and use the same notation for all maps induced by \( \nu \) (in the same way as for \( \kappa \)). All (local and global) deformations that we consider will have “fixed determinant”, i.e., give \( \nu \) after composing with \( \mu \).

Denote by \( \overline{\rho}(\mathfrak{g}^\text{der}) \) the composition of \( \overline{\rho} \) with the adjoint representation of \( G(k) \) on \( \mathfrak{g}_k^\text{der} \). The tangent space of the fixed determinant deformation functor corresponding to \( \overline{\rho} \) is given by \( H^1(\Gamma_S, \overline{\rho}(\mathfrak{g}^\text{der})) \), where \( \Gamma \) is a local or global Galois group.

From now on, unless explicitly stated otherwise, we make the following assumption on \( \overline{\rho} \):

**Assumption 2.1.** \( \overline{\rho}(\Gamma_S) \) contains the image of \( G^\text{sc}(k) \) in \( G(k) \).

**Remark 2.2.** If \( p \) is a “very good” prime for \( G \), it follows from \[Ste16\] Theorem 43 that \( \mathfrak{g}_k^\text{der} \) is an absolutely irreducible representation of \( G^\text{sc}(k) \); moreover, the only \( \mathbb{F}_p[G^\text{sc}(k)] \)-submodules of \( \mathfrak{g}_k^\text{der} \) are 0 and \( \mathfrak{g}_k^\text{der} \). To see the “moreover”, we observe that by Steinberg’s theorem the \( \mathbb{F}_p[G^\text{sc}(\mathbb{F}_p)] \)-submodules of \( \mathfrak{g}_p^\text{der} \) are 0 and \( \mathfrak{g}_p^\text{der} \), and \( \mathfrak{g}_p^\text{der} \) generates \( \mathfrak{g}_p^\text{der} \) as an \( \mathbb{F}_p[G^\text{sc}(k)] \)-module.

It then follows from the first condition that \( h^0(\Gamma_S, \overline{\rho}(\mathfrak{g}^\text{der})) = h^0(\Gamma_S, \overline{\rho}(\mathfrak{g}^\text{der})) = 0 \), so the global deformation functor is representable.

2.1. **Nice primes.** Under our assumptions on \( \overline{\rho} \) we prove the existence of (a Chebotarev set of) primes \( q \) that will make up the auxiliary set \( Q \) of Theorem 2.16.

**Definition 2.3.** A prime \( q \) of \( \mathcal{O}_F \) is called a **nice** prime for \( \overline{\rho} \) if:

1. Norm(\( q \)) is not congruent to \( \pm 1 \) mod \( p \);
2. \( \overline{\rho}(I_q) = \{1\} \) and \( \overline{\rho}(\text{Frob}_q) \) is a regular semisimple element of \( G(k) \);
3. there is a unique root \( \alpha \) of \( \Phi(G,T) \), with \( T \) the identity component of the centralizer of \( \overline{\rho}(\text{Frob}_q) \) in \( G \) (assumed to be a maximal split torus of \( G \)), such that \( \Gamma_q \) acts on \( \mathfrak{g}_\alpha \) (the corresponding root space) by \( \kappa \).

The uniqueness of the root \( \alpha \), which is not needed simply to kill dual Selmer, plays an essential role in our proofs.

**Proposition 2.4.** Let \( \overline{\rho} \) be as above and assume in addition that:

- \( \left[ F(\mu_p) : F \right] = p - 1 \);
There is a regular semisimple element \((1)\) and \((3)\) in the definition of nice primes, so we explain the necessary modifications.

Proof. We follow the proof of [Pat16, Theorem 6.4].

Let \(L = F(\mu_p) \cap F(\overline{\rho(g^{\text{der}})})\). It is shown after the proof of [Pat16, Lemma 6.6] that \([L : F] \mid \#Z_{G^{sc}}\), so the two assumptions together imply that \(F(\mu_p) \subseteq F(\overline{\rho(g^{\text{der}})})\). Then (1) follows from [Pat16, Lemma 6.6].

The differences in our setup as compared to that of [Pat16, Theorem 6.4] are the extra conditions \((1)\) and \((3)\) in the definition of nice primes, so we explain the necessary modifications.

Claim 2.5. There is a regular semisimple element \(x \in \overline{\rho(\Gamma_L)} \cap G^{\text{der}}(k)\) contained in a split maximal torus \(T\) of \(G\) and a root \(\alpha \in \Phi(G,T)\), such that

- \(\beta(x) \neq \alpha(x)\) for any root \(\beta \neq \alpha\),
- \(\alpha(x)\) lies in \(\text{Gal}(F(\mu_p)/L)\), where we use the canonical identification \(\text{Gal}(F(\mu_p)/F) \cong \mathbb{F}_p^\times\),
- \(\alpha(x) \neq \pm 1\).

Assuming the claim, choose \(\tau \in \Gamma_L\) so that \(\overline{\rho}(\tau) = x\). Then there exists \(\sigma \in \text{Gal}(K/L)\) such that

- \(\sigma \mapsto \tau\big|_{F(\overline{\rho(g^{\text{der}})})} \in \text{Gal}(F(\overline{\rho(g^{\text{der}})})/L)\),
- \(\sigma \mapsto \alpha(x) \in \text{Gal}(F(\mu_p)/F)\).

The desired Chebotarev set of nice primes is the set of primes \(q\) of \(\mathcal{O}_F\) whose Frobenius element in \(\text{Gal}(K/F)\) is (conjugate to) \(\sigma\). The image of \(\sigma\) in \(G^{\text{ad}}(k)\) is equal to the image of \(x\), so the image of \(\sigma\) in \(G(k)\) lies in \(T(k)\) and is regular semisimple.

We now prove the claim:

For any generator \(g \in k^\times\), we let \(t = q^{\#Z_{G^{sc}}} \div 2\) or \(t = q^{\#Z_{G^{sc}}}\) depending on whether \(\#Z_{G^{sc}}\) is even or odd. The element \(2\rho^\vee(g)\) (where \(2\rho^\vee\) is the sum of the positive coroots) is in the image of \(G^{\text{sc}}(k)\), hence in \(\overline{\rho}^\vee(\Gamma_F)\), so by the discussion at the beginning of the proof \(2\rho^\vee(t) \in \overline{\rho}(\Gamma_L)\). It is regular, since for all positive roots \(\beta\), \(\beta(x) = t^{2h_1\beta}\), the maximum height of a root is \(h - 1\), and none of \(t^2, t^4, \ldots, t^{2h-2}\) equals 1 (or even \(-1\)) by our assumption on \(p\). Also, for any positive root \(\beta, \beta(x) \in \text{Gal}(F(\mu_p)/L)\).

We then take \(\alpha\) to be the highest root (usually denoted by \(\delta\), i.e., the unique positive root of height \(h - 1\)). All the elements \(t^2, t^4, \ldots, t^{2h-2}, t^{-2}, t^{-4}, \ldots, t^{-(2h-2)}\) of \(k^\times\) are distinct (and not equal to \(\pm 1\)) by our assumptions on \(p\), so \(\alpha(x) \neq \beta(x)\) for any root \(\beta \neq \alpha\), proving the claim.

Remark 2.6. The bounds for \(p\) in Proposition 2.4 are not the best possible and can be improved for particular choices of \(G\). If \(G = GL_2\) and \(p \geq 5\) then \([L : F] \leq 2\), so the condition \(F(\mu_p) \subseteq F(\overline{\rho(g^{\text{der}})})\) (used in the proof) is satisfied whenever \([F(\mu_p) : F] > 2\). Also, from [DDT97, Lemma 2.48] one sees that the vanishing in (1) holds whenever \([k] > 5\) or \(k = \mathbb{F}_5\) and \(\overline{\rho}(\Gamma_F) = GL_2(\mathbb{F}_5)\).

Let \(\alpha\) be the standard positive root and set \(d := [F(\mu_p) : L]\). Since \(\overline{\rho}(\Gamma_L) \supset SL_2(k)\), if \([L : F] = 2\) we may take \(x\) to be \([b \ 0 \ \ 0 \ b^{-1}]\), with \(b = a^{(p-1)/2d}\) for any generator of \(\mathbb{F}_p^\times\). Then \(\alpha(x) = a^{(p-1)/d} \neq \pm 1\) if \(d > 2\). If \(F = L\) we may take \(x\) to be \([b \ 0 \ 0 \ b^{-1}]\), with \(b = a^{(p-1)/d}\) for any
generator of $\mathbb{F}_p^\times$. Then $\alpha(x) = a^{2(p-1)/d} \neq \pm 1$ if $d > 4$. In either case, we see that the bulleted conditions in Claim 2.5 are satisfied if $[F(\mu_p) : F] > 4$ and so (2) also holds in this case.

Now suppose $[F(\mu_p) : F] = 4$ and $\bar{\rho}(\Gamma_F) \supset \text{GL}_2(\mathbb{F}_p)$. If $F = L$ we may take $x$ to be $\begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}$, with $b = a^{(p-1)/4}$ and $a$ any generator of $\mathbb{F}_p^\times$. Then $\alpha(x) = b \neq \pm 1$ so again (2) holds. If $F \neq L$, suppose that $\text{det}(\bar{\rho})$ is $\kappa$ (resp. $\kappa^{-1}$), so $p = 5$ (since $\bar{\rho}(\Gamma_F) \supset \text{GL}_2(\mathbb{F}_p)$). Without appealing to (the proof of) Proposition 2.3, one sees in this case that we may take any prime whose Frobenius in $\text{Gal}(F(\bar{\rho})/F)$ is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (resp. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$).

**Lemma 2.7.** Let $p \geq 5$ be a very good prime for $G$ and let $H$ be a subgroup of $G^{ad}(W(k)/p^nW(k))$ whose image in $G^{ad}(k)$ contains the image of $G^{sc}(k)$. Then

1. $H$ contains the kernel of the reduction map $G^{ad}(W(k)/p^nW(k)) \to G(k)$.
2. For $t \leq n$, let $H_t$ be the image of $H$ in $G^{ad}(W(k)/p^tW(k))$. The sequence

$$0 \to K_t \to H_t \to H_{t-1} \to 1$$

is nonsplit for all $t \geq 2$. Here $K_t$ is the kernel of the reduction map $H_t \to H_{t-1}$ which, using (1), can be seen to be isomorphic to $\mathfrak{g}_k^{\text{der}}$.

**Proof.** This is a simple consequence of results from [Vas03]. To prove (1), let $H'$ be the inverse image of $H$ in $G^{sc}(W(k))$. Since $H$ contains the image of $G^{sc}(k)$, it follows that $H'$ surjects onto $G^{sc}(k)$ so by [Vas03] Theorem 1.3 $H' = G^{sc}(W(k))$. Since $p$ is very good, the map on Lie algebras induced by the homomorphism $G^{sc} \to G^{ad}$ is an isomorphism, so $\text{Ker}(G^{sc}(W(k)) \to G^{sc}(k))$ maps onto $\text{Ker}(G^{ad}(W(k)) \to G^{ad}(k))$, giving (1).

The statement in (2) for $t = 2$ is Proposition 4.4.1 of [Vas03], where it is the main ingredient in the proof of the main theorem. In fact, in our setting of a split group with $p \geq 5$ a very good prime, (2) can be reduced to the case of $SL_2$ (see the first paragraph of loc. cit.). In this case it follows from the fact that the matrix $A = \begin{bmatrix} 1 & p^{t-1} \\ 0 & 1 \end{bmatrix}$, viewed as an element of $SL_2(W(k)/p^tW(k))$, is of order $p$ but there is no matrix of order $p$ in $SL_2(W(k)/p^tW(k))$ reducing to $A$. \hfill $\square$

The following analogue of Fact 5 from [KLR05] plays a crucial role in allowing us to find nice primes with various desired properties.

**Lemma 2.8.** Let $\rho_n$ be a deformation of $\bar{\rho}$ to $W(k)/p^nW(k)$. Let $\{f_1, f_2, \ldots, f_r\}$ be linearly independent in $H^1(\Gamma_F, \bar{\rho}(\mathfrak{g}_k^{\text{der}}))$ and $\{\phi_1, \phi_2, \ldots, \phi_s\}$ be linearly independent in $H^1(\Gamma_F, \bar{\rho}(\mathfrak{g}_k^{\text{der}}))$. Let $K = F(\bar{\rho}(\mathfrak{g}_k^{\text{der}}), \mu_p)$ as before, and let $K_{f_i}$ (resp. $K_{\phi_j}$) be the fixed field of the kernel of the restriction of $f_i$ (resp. $\phi_j$) to $\Gamma_K$. Then as a $k[\text{Gal}(K/F)]$–module $\text{Gal}(K_{f_i}/K)$ (resp. $\text{Gal}(K_{\phi_j}/K)$) is isomorphic to $\bar{\rho}(\mathfrak{g}_k^{\text{der}})$ (resp. $\bar{\rho}(\mathfrak{g}_k^{\text{der}})$). Let $K_{P_{f_i}}$ be the fixed field of the kernel of the composite of $\rho_n$ with the adjoint representation $G(W(k)/p^tW(k)) \to GL(\mathfrak{g}_k^{\text{der}}W(k)/p^tW(k))$. Then each of the fields $K_{f_i}$, $i = 1, \ldots, r$, $K_{\phi_j}$, $j = 1, \ldots, s$, $K_{P_{f_i}}$, $K(\mu_{p^\infty})$ is linearly disjoint over $K$ with the compositum of the others.

Let $L = F(\mu_p) \cap F(\bar{\rho}(\mathfrak{g}_k^{\text{der}}))$, and let $x \in \bar{\rho}(\Gamma_L) \cap G^{\text{der}}(k)$, $T$ and $\alpha$ be as in Claim 2.5. For $i = 1, 2, \ldots, r$, let $a_i \in \mathfrak{g}_k^{\text{der}}$ be any element fixed by $x$ and for $j = 1, 2, \ldots, s$, let $b_j \in (\mathfrak{g}_k^{\text{der}})^x$ be any element on which $x$ acts by $\alpha^{-1}(x)$. Furthermore, let $y$ be any element of the image of $\rho_n$ reducing to $x$. There exists a Chebotarev set of nice primes $q$ such that

1. $\bar{\rho}(\text{Frob}_q) = x$,
2. for $i = 1, 2, \ldots, r$, $f_i|_{\Gamma_q}$ (which is an element of $H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_k^{\text{der}}))$ so can be viewed as a homomorphism $\Gamma_q/I_q \to (\mathfrak{g}_k^{\text{der}})_{\text{Frob}_q}$) is given by $\text{Frob}_q \to a_i$, 


(3) for \( j = 1, 2, \ldots, s \), \( \phi_j|_{\Gamma_q} \) (which is an element of \( H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\mathrm{der}})^*) \)) so can be viewed as a homomorphism \( \Gamma_q/I_q \to ((\mathfrak{g}_{k}^{\mathrm{der}})^*)^{\text{Frob}_q} \) is given by \( \text{Frob}_q \to b_j \),

(4) \( p_m(\text{Frob}_q) = y \).

Proof. Our assumptions on \( \bar{\rho} \) and \( p \) and Remark \( 2.2 \) imply that \( \bar{\rho}(\mathfrak{g}_{\mathrm{der}}) \) and \( \bar{\rho}(\mathfrak{g}_{\mathrm{der}})^* \) are non-isomorphic absolutely irreducible representations of \( \Gamma_F \), so the statements about the images of the cocycles and linear disjointness of \( K_{f_i} \) and \( K_{\phi_j} \) are immediate consequences of Proposition \( 2.1 \) (1).

We have to do a little more work in order to include \( K_{P_n} \). For this we consider the exact sequences

\[
1 \to \text{Gal}(K_{f_i}/K) \to \text{Gal}(K_{f_i}/F) \to \text{Gal}(K/F) \to 1
\]

and

\[
1 \to \text{Gal}(K_{\phi_j}/K) \to \text{Gal}(K_{\phi_j}/F) \to \text{Gal}(K/F) \to 1.
\]

The first short exact sequence, viewed as an element of \( H^2(\text{Gal}(K/F), \bar{\rho}(\mathfrak{g}_{\mathrm{der}})) \), is obtained by first restricting \( f_i \) to \( \Gamma_K \) and then applying the map \( H^1(\Gamma_K, \bar{\rho}(\mathfrak{g}_{\mathrm{der}}))^{\text{Gal}(K/F)} \to H^2(\text{Gal}(K/F), \bar{\rho}(\mathfrak{g}_{\mathrm{der}})) \) from the inflation-restriction sequence, the exactness of which then implying that this element is zero. Thus, the sequence splits and the same argument implies that the second sequence also splits.

For any \( t \leq n \), let \( \rho_t \) be the reduction of \( \rho_n \) modulo \( p^t \). By Lemma \( 2.7 \) (1) the image of \( \bar{\rho}_t \), the composite of \( \rho_t \) with the adjoint representation as above, contains the image of \( G^{\mathrm{sc}}(W(k)/p^nW(k)) \).

Furthermore, it follows from Lemma \( 2.7 \) (2) that the induced extensions

\[
1 \to \mathfrak{g}_{k}^{\mathrm{der}} \to \text{Im}(\bar{\rho}_t) \to \text{Im}(\bar{\rho}_{t-1}) \to 1
\]

are non-split for \( t \geq 2 \).

Given the above, we get (strong) linear disjointness of all the \( K_{f_i} \), \( K_{\phi_j} \) and \( K_{P_n} \). The fact that \( K(K/F) \) is linearly disjoint from the compositum of all these fields follows from the fact that \( \text{Gal}(K/F) \) acts trivially on \( \text{Gal}(K(\mu_{p^n})/K) \) while the Galois groups of the other extensions have no such non-trivial quotient.

To construct the desired Chebotarev set of nice primes we proceed as follows:

We apply (the proof) of Proposition \( 2.1 \) to get a Chebotarev set of nice primes \( q \) for \( \bar{\rho}(\mathfrak{g}_{\mathrm{der}}) \) in \( \mathcal{O}_F \) determined by the choice of a suitable Frobenius element \( \sigma \in \text{Gal}(K/F) \) (with \( K = F(\bar{\rho}(\mathfrak{g}_{\mathrm{der}}), \mu_p) \)).

The conditions in (2), (3) and (4) are all Chebotarev conditions on the field extensions \( K_{f_i}/K \), \( K_{\phi_j}/K \) and \( K_{P_n}/K \) and then the linear disjointness proved above implies that all these conditions can be realised simultaneously by choosing a suitable element of \( \text{Gal}(\bar{K}/F) \), with \( \bar{K} \) the compositum of all the \( K_{f_i} \), \( K_{\phi_j} \) and \( K_{P_n} \).

\[ \square \]

2.2. Local computations I.

2.2.1. Let \( \Gamma \) be the absolute Galois group of any local field with residue characteristic prime to \( p \). We recall that for any \( W(k)[\Gamma] \)-module \( M \) which is finite as a \( W(k) \)-module Tate’s Euler characteristic formula states (Mil06 Theorem 2.8) :

\[
(2.1) \quad \ell(H^0(\Gamma, M)) - \ell(H^1(\Gamma, M)) + \ell(H^2(\Gamma, M)) = 0.
\]

Furthermore, if \( M \) is a free \( W(k)/p^n \)-module for some \( n \), then local Tate duality gives a perfect pairing (Mil06 Corollary 2.3):

\[
(2.2) \quad H^1(\Gamma, M) \times H^{2-i}(\Gamma, M^*) \xrightarrow{\text{inv}} H^2(\Gamma, (W(k)/p^n)(\kappa)) \cong W(k)/p^n.
\]
2.2.2. From now on we will assume that all nice primes \( q \) we consider correspond to some fixed element of \( \bar{\rho}(\Gamma_S) \cap T(k) \) (for a fixed split maximal torus \( T \)) and a fixed root \( \alpha \in \Phi(G, T) \). That such primes suffice for our needs is due to Remark 2.2. To simplify notation in what follows, we fix isomorphisms of \( \mathfrak{l}_\alpha \) and \( \mathfrak{g}_\alpha^* \) with \( k; \) for \( \mathfrak{l}_\alpha \) we use the natural one corresponding to the map on Lie algebras induced by \( \alpha^* \) but for \( \mathfrak{g}_\alpha^* \) there is no canonical choice. The spaces are unique, the choice is for the isomorphism. For nice primes \( q \) as above these isomorphisms are also isomorphisms as \( \Gamma_q \)-modules. Using these identifications, for \( f \in H^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) \) we will denote by \( f(\text{Frob}_q) \) the element of \( k \) obtained by evaluating the \( \mathfrak{l}_\alpha \) component of \( f \) (which is a homomorphism \( \Gamma_q \to k \)) at \( \text{Frob}_q \). Similarly, for \( \phi \in H^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})^*) \) we will denote by \( \phi(\text{Frob}_q) \) the element of \( k \) corresponding to the \( \mathfrak{g}_\alpha^* \) component of \( \phi \). (These elements are well defined since \( \text{Norm}(q) \not\equiv 1 \) mod \( p \) implies that \( H^1(\Gamma_q, k) = H^1_{nr}(\Gamma_q, k) \).

The lemma below is the reason why we work with nice primes rather than the more general class of primes used in [Pat16, §4.2]: without the uniqueness of the root a none of the statements would be true and we would not have enough control to make our global arguments work.

**Lemma 2.9.** For \( q \) a nice prime for \( \bar{\rho} \) we have:

1. \( h^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) - h^0(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) = 1. \)
2. \( h^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) - \dim \mathcal{N}_q = 1. \)
3. Fix \( f \in H^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) \) ramified at \( q \). Then for all unramified \( \phi \in H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})^*), \)
   \[ \text{inv}_q(f \circ \phi) = \gamma_f \phi(\text{Frob}_q), \]
   where \( \gamma_f \) is a nonzero constant depending only on \( f \).
4. Fix \( \phi \in H^1(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})^*) \) ramified at \( q \). After appropriately scaling \( \phi \), for any \( f \in H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) \)
   we have \( \text{inv}_q(f \circ \phi) = f(\text{Frob}_q) \).

**Proof.** Let \( \chi : \Gamma_q \to k^\times \) be any character and denote the associated \( \Gamma_q \)-module by \( k(\chi) \). We then have that \( H^i(\Gamma_q, k(\chi)) = 0 \) for all \( i \) if \( \chi \) is not trivial or the cyclotomic character: this well-known fact follows from (2.2) and (2.1) since the computation of \( h^0 \) is trivial, \( h^2 \) is computed using duality, and then \( h^1 \) can be determined using the vanishing of the Euler characteristic. For the trivial character we have \( h^0(\Gamma_q, k) = h^1(\Gamma_q, k) = 1 \) and \( h^2(\Gamma_q, k) = 0 \) and for the cyclotomic character \( \kappa \) we have \( h^0(\Gamma_q, k(\kappa)) = 0 \) and \( h^1(\Gamma_q, k(\kappa)) = h^2(\Gamma_q, k(\kappa)) = 1. \)

From the definition of niceness, it follows that \( \bar{\rho}(\mathfrak{g}_{\text{der}})^* \) is a sum of characters of \( \Gamma_q \), precisely one of which is trivial, so \( h^0(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})^*) = h^2(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) = 1 \) which gives (1) using (2.1). The claim in (2) follows from (1) since \( \dim(\mathcal{N}_q) = h^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) = h^0(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) \).

To prove (3) and (4) we use the fact that \( H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})) \) pairs trivially with \( H^1_{nr}(\Gamma_q, \bar{\rho}(\mathfrak{g}_{\text{der}})^*) \). We also have \( H^1(\Gamma_q, t) = H^1_{nr}(\Gamma_q, t) \) since the action is trivial and \( H^1(\Gamma_q, \mathfrak{g}_\beta) = H^1_{nr}(\Gamma_q, \mathfrak{g}_\beta) \) for any root \( \beta \neq \alpha \) (and this is nonzero iff the action on \( \mathfrak{g}_\beta \) is trivial).

Thus, \( \text{inv}_q(f \circ \phi) \) in (3) is determined by the \( \mathfrak{g}_\alpha \) component of \( f \) and this pairs non-degenerately with the \( \mathfrak{g}_\alpha^* \) component of \( \phi \), so (3) follows. The proof of (4) is dual to this, so we skip the details.

**Remark 2.10.** While the proofs of parts (3) and (4) of Lemma 2.9 are dual to one another, we will apply them as asymmetrically stated, especially in Case 3) of the proof of Theorem 2.16.

2.3. The local condition at nice primes. For a root \( \alpha \in \Phi(G, T) \) we denote by \( H_\alpha \) the subgroup of \( G \) generated by \( T \) and \( U_\alpha \) (the corresponding root subgroup of \( G \)), so \( \alpha \) extends to a homomorphism \( H_\alpha \to \mathbb{G}_m \). We let \( T_\alpha \) be the identity component of \( \text{Ker}(\alpha) \), \( t_\alpha \) its Lie algebra and let \( \mathfrak{l}_\alpha \) be the Lie algebra of the image of the coroot associated to \( \alpha \), so \( t = t_\alpha \oplus \mathfrak{l}_\alpha \).
Associated to a nice prime $q$ there is a smooth deformation condition $\mathcal{D}_q$ introduced in [Pat16], generalizing the one introduced for $GL_2$ in [Ram02]. Lifts $\rho : \Gamma_q \to G(A)$ (of $\bar{\rho}|_{\Gamma_q} \to G(k)$) to Artin local $W(k)$-algebras $A$ with residue field $k$ are in $\mathcal{D}_q$ if they are $\widehat{G}(A)$ conjugate to lifts factoring through $H_\alpha(A)$ and such that $\alpha \circ \rho : \Gamma_q \to A^\times$ is $\kappa$; this condition forces $\rho(I_q)$ to be contained in $U_\alpha(A)$. Its tangent space is $\mathcal{N}_q = H^1(\Gamma_q, W) \subset H^1(\Gamma_q, \bar{\rho}(\mathfrak{g}^{\text{der}}))$, where $W = t_\alpha \oplus \mathfrak{g}_\alpha$. We refer to [Pat16] §4.2 for the proofs.

**Definition 2.11.** We will say that a lift of $\bar{\rho}$ to $G(W(k)/p^nW(k))$ is special at a nice prime $q$ if its restriction to $\Gamma_q$ lies in $\mathcal{D}_q$.

For $\alpha$ a root associated to a nice prime as constructed in Proposition 2.4 let $G_\alpha$ be the subgroup of $G$ generated by $U_\alpha$ and $U_{-\alpha}$ (which is isomorphic to $SL_2$ or $PGL_2$). Let $S_\alpha$ be the subgroup of $G$ generated by $G_\alpha$ and $T$; it is a (split) reductive group of semisimple rank one, so is isomorphic to $GL_2 \times T'$, $SL_2 \times T'$ or $PGL_2 \times T'$, for some split torus $T'$. Henceforth, we fix such a decomposition with the property that $\alpha$ corresponds to the standard positive root of $GL_2$, $SL_2$ or $PGL_2$ and $T = T'D$ with $D$ the (image of) the diagonal matrices in the first factor.

**Lemma 2.12.** Let $q$ be a nice prime for $\bar{\rho}$ and let $\rho_n : \Gamma_F \to G(W(k)/p^nW(k))$, $n \geq 2$, be a lift of $\bar{\rho}$.

1. There is a Chebotarev class of nice primes $q'$ such that $\bar{\rho}($Frob$_q) = \bar{\rho}($Frob$_{q'})$, $\rho_n($Frob$_{q'}) \in T(W(k)/p^nW(k))$ and $\rho_n$ is special at $q'$ (with respect to the root $\alpha$).

2. There is a Chebotarev class of nice primes $q''$ with $\text{Norm}(q'') \equiv \text{Norm}(q') \mod p^n$ and such that $\rho_n($Frob$_{q''}) \in T(W(k)/p^nW(k))$ is equal to $\rho_n($Frob$_{q'}) \cdot (A_n, \text{Id}_T)$, with $q''$ as above and $A_n$ the matrix $\begin{bmatrix} 1-p^{n-1} & 0 \\ 0 & 1+p^{n-1} \end{bmatrix}$. Here $A_n$ is viewed as an element of $SL_2$ or $GL_2$ and in the $PGL_2$ case we replace it by its image in $PGL_2$. Thus, $\rho_n$ is not special at $q''$ but $\rho_{n-1}$ is special at $q''$.

**Proof.** An element $g \in G(W(k)/p^nW(k))$ lies in $T(W(k)/p^nW(k))$ iff its image in $G_{\text{ad}}(W(k)/p^nW(k))$ lies in $T_{\text{ad}}(W(k)/p^nW(k))$, where $T_{\text{ad}}$ is the image of $T$ in $G_{\text{ad}}$. From this observation and Lemma 2.7 (1), (1) of this lemma follows by considering the extension $K_{P_n}K(p^n)/F$ and choosing an appropriate element in its Galois group. Item (2) follows in the same way once we note that the image of $SL_2(W(k)/p^nW(k))$ in $G(W(k)/p^nW(k))$ is contained in $\rho_n(\Gamma_F)$ by Lemma 2.7 (1). \qed

2.4. **Main theorem.** Let $X$ be a finite set of primes of $O_F$. Let $M$ be a finite $W(k)[\Gamma_X]$-module and for each $v \in X$ let $\mathcal{L}_v$ be a submodule of $H^1(\Gamma_v, M)$. We call $\mathcal{L} := \{\mathcal{L}_v\}_{v \in X}$ a Selmer condition.

**Definition 2.13.** Selmer group $H^1_{\mathcal{L}}(\Gamma_X, M)$ is defined to be the kernel of the (global to local) restriction map

$$H^1(\Gamma_X, M) \to \bigoplus_{v \in X} \frac{H^1(\Gamma_v, M)}{\mathcal{L}_v}.$$

If $M$ as above is a free $W(k)/p^n$-module, let $\mathcal{L}^\perp_v \subset H^1(\Gamma_v, M^*)$ be the annihilator of $\mathcal{L}_v$ with respect to the pairing 2.2 Then the dual Selmer group is defined to be $H^1_{\mathcal{L}^\perp}(\Gamma_X, M^*)$.

From now on we make the following additional assumption on $\bar{\rho}$.

**Assumption 2.14.** For each prime $v$ in $S$ we are given a smooth local deformation condition $\mathcal{D}_v$ for $\bar{\rho}|_{\Gamma_v}$ with tangent space $\mathcal{N}_v \subset H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$ such that the set of Selmer conditions $\mathcal{N}$ is balanced, i.e.,

$$\dim H^1_{\mathcal{N}}(\Gamma_S, \bar{\rho}(\mathfrak{g}^{\text{der}})) = \dim H^1_{\mathcal{N}^*}(\Gamma_S, \bar{\rho}(\mathfrak{g}^{\text{der}})^*)$$.
Definition 2.15. An auxiliary set for $\bar{\rho}$ is a finite set $Q$ of nice primes (with $Q \cap S = \emptyset$) such that the new-at-$Q$ Selmer group $H^1_X(\Gamma_{S\cup Q}, \bar{\rho}(g^{\text{der}})) = 0$.

Here $\mathcal{N}$ is defined using the given local conditions at primes in $S$ and the condition described above at primes $q$ in $Q$. In this situation the versal deformation ring $R^Q_{S\cup Q}$, defined using the given local deformation conditions at $v \in S$ and the above conditions at $q \in Q$, is isomorphic to $W(k)$.

Theorem 2.16. Let $\bar{\rho} : \Gamma_S \to G(k)$ satisfy Assumptions 2.1 and 2.14 let $p = \text{char}(k)$ be such that the hypotheses of Proposition 2.14 hold. Assume that the Selmer and dual Selmer groups of $\bar{\rho}$ with respect to the given local conditions at primes in $S$ are nontrivial of (the same) dimension $n$. Then there exists a set $Q = \{q_1, q_2, \ldots, q_m\}$ of nice primes, $m \in \{n + 1, n + 3\}$, and an integer $d \geq 2$ such that

- $Q$ is auxiliary and the versal deformation $\rho^Q_{S\cup Q} : \Gamma_{S\cup Q} \to G(R^Q_{S\cup Q}) = G(W(k))$ is ramified mod $p^d$ at all $q \in Q$.
- for each $1 \leq i \leq m$ there is an auxiliary set $Q_i \subset Q$ satisfying
  - $\{1, 2, \ldots, q_{i-1} \} \subset Q_i$,
  - $q_i \notin Q_i$,
  - $\rho^Q_{S\cup Q_i} \equiv \rho^Q_{S\cup Q} \pmod{p^{d-1}}$, $\rho^Q_{S\cup Q_i} \pmod{p^{d-1}}$ is special at $q_i$ but $\rho^Q_{S\cup Q_i} \pmod{p^d}$ is not special at $q_i$.

Remark 2.17. Implicit in the formulation of the theorem is that $\rho^Q_{S\cup Q} : \Gamma_{S\cup Q} \to G(R^Q_{S\cup Q}) = G(W(k))$ is ramified at all $q \in Q$ mod $p^d$ and is unramified at all $q \in Q$ mod $p^{d-1}$. The proof will show that we can in fact take $d = 2$.

Note that we are not claiming that $\rho^Q_{S\cup Q_i}$ is ramified at all $v \in S \cup Q_i$, although it would be nice to get this refinement of the theorem.

Example 2.18. Using Remark 2.14 one sees that if $G = GL_2$, sufficient conditions for the main theorem to hold are that $\bar{\rho}(\Gamma_F) \supset SL_2(k)$ and

- $[F(\mu_p) : F] > 4$ (so we must have $p > 5$), or
- $[F(\mu_p) : F] = 4$, $\bar{\rho}(\Gamma_F) \supset GL_2(\mathbb{F}_p)$, and
  - $F(\bar{\rho}(g^{\text{der}})) \cap F(\mu_p) = F$,
  - $\det(\bar{\rho})$ is a power of the cyclotomic character $\kappa$.

As mentioned in the introduction, the theorem will be proved below using only Galois cohomology (and Chebotarev’s theorem).

2.5. Global to local restriction maps.

2.5.1. Controlling the dimensions of Selmer and dual Selmer groups is fundamental to our arguments and the main tool for doing this is the Greenberg–Wiles formula ([DDT97, Theorem 2.19]):

\[
\ell(H^1_L(\Gamma_X, M)) - \ell(H^1_L(\Gamma_X, M^*)) = \ell(H^0(\Gamma_X, M)) - \ell(H^0(\Gamma, M^*)) + \sum_{v \in X(\infty)} (\ell(L_v) - \ell(H^0(\Gamma_v, M))),
\]

where $X(\infty)$ denotes the union of $X$ and the infinite primes of $F$ and $L_v$ for an infinite prime is taken to be $0$.

The following result from global duality theory, which also plays an important role in our proofs, is the “exactness in the middle” of the Poitou–Tate exact sequence ([Mil06, Theorem 4.10 (b)]).
Theorem 2.19. Let $X$ be a finite set of primes of $F$ containing all primes above $p$ and $\infty$, and let $M$ be a finitely generated and free $W(k)/p^n$-module with a $W(k)$-linear action of $\Gamma_X$. Consider the restriction maps
\[
\text{Res}_X : H^1(\Gamma_X, M) \to \bigoplus_{v \in X} H^1(\Gamma_v, M)
\]
and
\[
\text{Res}_X^* : H^1(\Gamma_X, M^*) \to \bigoplus_{v \in X} H^1(\Gamma_v, M^*).
\]
Then the sum of the local duality pairings of (2.2) induces a perfect pairing
\[
\text{Im}(\text{Res}_X) \times \text{Im}(\text{Res}_X^*) \xrightarrow{(\sum_{v \in X} \text{Im}(\text{Res}_v)) \circ \delta} W(k)/p^n.
\]

2.5.2. Let $X$ be a finite set of primes of $\mathcal{O}_F$ containing $S$, and let $(h_v)_{v \in X}$ be a collection of elements of $H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))$. We call $(h_v)_{v \in X}$ a local condition problem and we are interested in knowing whether there exists a global class $h \in H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}}))$ whose restriction at $v \in X$ is $h_v$.

In general, such a class need not exist so let us suppose that this is the case, i.e., $(h_v)_{v \in X}$ is not in the image of the restriction map
\[
\text{Res}_X : H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})).
\]

We will show that there exists a Chebotarev set $Q$ of nice primes $q$ such that $(h_v)_{v \in X}$ is in the image of the map
\[
\text{Res}_X^Q : H^1(\Gamma_X \cup \{q\}, \bar{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})).
\]

Lemma 2.20. Let $(h_v)_{v \in X}$ be a local condition problem such that the line $l$ spanned by $(h_v)_{v \in X}$ is not in the image of
\[
\text{Res}_X : H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}}))
\]
Then the annihilator of $l$ in $\bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})^*)$ does not contain the image of the map
\[
\text{Res}_X^* : H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}})^*) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})^*)
\]

Proof. By Theorem 2.19 the images of $\text{Res}_X$ and $\text{Res}_X^*$ are exact annihilators of one another, so
\[
\text{Ann}(l) \supset \text{Im}(\text{Res}_X^*) \iff l \subset \text{Im}(\text{Res}_X).
\]
The latter condition is false by hypothesis, so the former is false as well.

Proposition 2.21. Let $(h_v)_{v \in X}$ be a local condition problem such that the line $l$ spanned by it is not in the image of
\[
\text{Res}_X : H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})).
\]
Then there is a basis $\{\zeta_1, \ldots, \zeta_s, \zeta\}$ of $H^1(\Gamma_X, \bar{\rho}(\mathfrak{g}^{\text{der}})^*)$ such that $\{\zeta_1, \ldots, \zeta_s\}$ all annihilate $l$. Let $Q$ be the Chebotarev set of nice primes satisfying
\begin{itemize}
  \item $\zeta_i|_{\Gamma_q} = 0$ for $i = 1, 2, \ldots, s$ and
  \item the $\mathfrak{g}_\alpha^*$ component of $\zeta|_{\Gamma_q}$ is nonzero.
\end{itemize}
Then for any $q \in Q$, the image of
\[
\text{Res}_X^Q : H^1(\Gamma_X \cup \{q\}, \bar{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(\mathfrak{g}^{\text{der}})^*)
\]
contains $l$. 
Proof. By Lemma 2.20 we may choose a basis \( \{ \zeta_1, \ldots, \zeta_s, \zeta \} \) of \( H^1(\Gamma_X, \bar{\rho}(g_{\text{der}})^*) \) as required and we also have \( \text{Res}_X^X(\zeta) \notin \text{Ann}(l) \). We may also assume that the \( \zeta_i \) are ordered so that they first include a basis of \( \text{III}_X^X(\bar{\rho}(g_{\text{der}})^*) = \text{Ker}(\text{Res}_X^X) \). The assumptions on \( \bar{\rho} \) and the linear disjointness from Lemma 2.8 imply that \( Q \) as in the statement is a set of primes of positive density.

For \( v \in X \), let \( \mathcal{L}_v = H^1(\Gamma_v, \bar{\rho}(g_{\text{der}})) \) and also let \( \mathcal{L}_q = H^1(\Gamma_q, \bar{\rho}(g_{\text{der}})) \). Let \( \mathcal{L} = \{(\mathcal{L}_v)_{v \in X}\} \) and let \( \mathcal{L}' = \{(\mathcal{L}_v)_{v \in X \cup \{q\}}\} \). Comparing the Greenberg-Wiles formula (2.3) applied to \( \mathcal{L} \) and \( \mathcal{L}' \), we see that

\[
(2.4) \quad (h^1_\mathcal{L}(\Gamma_X, \bar{\rho}(g_{\text{der}})) - h^1_\mathcal{L}'(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}}))) - (h^1_\mathcal{L}(\Gamma_X, \bar{\rho}(g_{\text{der}})') - h^1_\mathcal{L}'(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})'))
= h^1_{nr}(\Gamma_q, \bar{\rho}(g_{\text{der}})) - h^1(\Gamma_q, \bar{\rho}(g_{\text{der}})).
\]

By definition, \( H^1_\mathcal{L}(\Gamma_X, \bar{\rho}(g_{\text{der}})) \) is the full \( H^1 \) and \( H^1_\mathcal{L}'(\Gamma_X, \bar{\rho}(g_{\text{der}})) \) is the \( \text{III}^1 \). By assumption, we have \( \zeta_i|_{\Gamma_q} = 0 \) for all \( i \), so \( H^1_\mathcal{L}(\Gamma_X, \bar{\rho}(g_{\text{der}})) = H^1_\mathcal{L}'(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})) \). Thus,

\[
(2.5) \quad h^1(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})) = h^1(\Gamma_X, \bar{\rho}(g_{\text{der}})) + h^1(\Gamma_q, \bar{\rho}(g_{\text{der}})) - h^1_{nr}(\Gamma_q, \bar{\rho}(g_{\text{der}})).
\]

We now compare the kernels of \( \text{Res}_X : H^1(\Gamma_X, \bar{\rho}(g_{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(g_{\text{der}})) \) and \( \text{Res}_X^X : H^1(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \bar{\rho}(g_{\text{der}})) \). For this we let \( \mathcal{L}_v = 0 \) for \( v \in X \), \( \mathcal{L}_q = H^1(\Gamma_q, \bar{\rho}(g_{\text{der}})) \) and \( \mathcal{L} = \{(\mathcal{L}_v)_{v \in X}\}, \mathcal{L}' = \{(\mathcal{L}_v)_{v \in X \cup \{q\}}\} \) and apply the Greenberg-Wiles formula as in (2.3).

Now \( H^1_\mathcal{L}(\Gamma_X, \bar{\rho}(g_{\text{der}})) = H^1(\Gamma_X, \bar{\rho}(g_{\text{der}})) \) which has basis \( \{\zeta_1, \ldots, \zeta_s, \zeta\} \). As \( \mathcal{L}_q = 0 \), \( \zeta_i|_{\Gamma_q} = 0 \) and \( \zeta|_{\Gamma_q} \neq 0 \), we have that \( H^1_\mathcal{L}(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})) \) is the span of \( \{\zeta_1, \ldots, \zeta_s\} \). Combining (2.4) and (2.5) we get

\[
(2.6) \quad (h^1(\Gamma_{X \cup \{q\}}, \bar{\rho}(g_{\text{der}})) - \dim \text{Ker}(\text{Res}_X^X(\zeta_{X \cup \{q\}}))) - ((h^1(\Gamma_X, \bar{\rho}(g_{\text{der}})) - \dim \text{Ker}(\text{Res}_X)) = 1
\]

Thus, the rank of \( \text{Res}_X^X(\zeta_{X \cup \{q\}}) \) is one greater than the rank of \( \text{Res}_X \).

If \( l \not\subseteq \text{Im}(\text{Res}_X^X(\zeta_{X \cup \{q\}})) \), then \( \text{Im}(\text{Res}_X) \) is of codimension at least two in \( l + \text{Im}(\text{Res}_X^X(\zeta_{X \cup \{q\}})) \), so \( \text{Ann}(l + \text{Im}(\text{Res}_X^X(\zeta_{X \cup \{q\}}))) \) is of codimension at least two in \( \text{Ann}(\text{Im}(\text{Res}_X)) \). However, by Theorem 2.19 the latter space is precisely the image of \( \text{Res}_X^X \), so spanned by the (images of) \( \zeta \) and \( \zeta \). By construction, all the \( \zeta_i \) annihilate \( l \) and since \( \zeta_i|_{\Gamma_q} = 0 \) for all \( i \), it follows by reciprocity that all the \( \zeta_i \) also annihilate \( \text{Im}(\text{Res}_X^X(\zeta_{X \cup \{q\}})) \). We conclude that \( l \subseteq \text{Im}(\text{Res}_X^X(\zeta_{X \cup \{q\}})) \).

2.6. Infinitesimal adjustment of lifts. The process of “adjusting” a representation \( \rho : \Gamma_F \to G(W(k)/p^mW(k)) \), \( m > 0 \), by a cocycle (representing) \( f \in H^1(\Gamma_F, \bar{\rho}(g_{\text{der}})) \) to get another representation \( \rho' : \Gamma_F \to G(W(k)/p^mW(k)) \) plays a key role in the sequel. We recall here what this means: the kernel of the reduction map \( G(W(k)/p^mW(k)) \to G(W(k)/p^{m-1}W(k)) \) is naturally identified [14, §3.5] with \( g_k \) using the first order exponential map and the generator \( p^{m-1} \) of the kernel of the reduction map \( W(k)/p^mW(k) \to W(k)/p^{m-1}W(k) \). We denote this identification by \( x \mapsto \exp(p^{m-1}x) \), \( x \in g_k \).

For \( \rho, f \) as above, the map \( \rho' : \Gamma_F \to G(W(k)/p^mW(k)) \) given by \( \gamma \mapsto \exp(p^{m-1}f(\gamma)) \cdot \rho(\gamma) \) is a continuous homomorphism, equivalent to \( \rho \mod p^{m-1} \). Moreover, since \( f \) takes values in \( g_{\text{der}}^k \subset g_k \) and \( g_{\text{der}}^k \) is the kernel of the map on Lie algebras induced by \( \mu : G \to C \), the maps \( \mu \circ \rho \) and \( \mu \circ \rho' \) from \( \Gamma_F \) to \( C(W(k)/p^mW(k)) \) are equal.
Definition 2.22. We call $\rho'$ the representation obtained from $\rho$ by adjusting it by $f$ and denote it by $\exp(p^{m-1}f)\rho$.

We use similar notation when $\Gamma_F$ is replaced by $\Gamma_v$, for $v$ a prime of $\mathcal{O}_F$.

2.7. A matricial condition for auxiliary sets. Recall that $\mathcal{N} = (\mathcal{N}_v)_{v \in \mathcal{S}}$ is the set of tangent spaces to the (balanced) smooth local deformation conditions $(\mathcal{D}_v)_{v \in \mathcal{S}}$ from Assumption 2.14.

Let $\{f_1, f_2, \ldots, f_n\}$ be a basis of $H^1(\mathcal{N}, \tilde{\rho}(\mathcal{g}^{\text{der}}))$ and $\{\phi_1, \phi_2, \ldots, \phi_n\}$ a basis of $H^1(\mathcal{N}, \rho(\mathcal{g}^{\text{der}})^*)$.

By Assumption 2.1 and Remark 2.2, it follows that $f_i|_{\Gamma_K : \Gamma_K \rightarrow \mathcal{g}^{\text{der}}, K = F(\tilde{\rho}(\mathcal{g}^{\text{der}}), \mu_\rho)}$, is a surjective homomorphism and similarly for $\phi_i|_{\Gamma_K}$. Therefore, using the Chebotarev density theorem and Lemma 2.23, we may pick a set $\tilde{Q} = \{q_1, q_2, \ldots, q_n\}$ of nice primes for $\rho$ such that

- the $t_\alpha \oplus (\oplus_\beta \mathcal{g}_\beta)$ component of $f_i$ restricted to $\Gamma_{q_j}$ is 0 for all $i, j$,
- the $t_\alpha$ component of $f_i$ restricted to $\Gamma_{q_j}$ is 0 for $i \neq j$,
- the $t_\alpha$ component of $f_i$ restricted to $\Gamma_{q_i}$ is 1 (using the identification fixed in (2.22) and

- the $t^* \oplus (\oplus_\beta \mathcal{g}_\beta^*)$ component of $\phi_i$ restricted to $\Gamma_{q_j}$ is 0 for all $i, j$,
- the $\mathcal{g}_\alpha^*$ component of $\phi_i$ restricted to $\Gamma_{q_j}$ is 0 for $i \neq j$,
- the $\mathcal{g}_\alpha^*$ component of $\phi_i$ restricted to $\Gamma_{q_i}$ is 1 (using the identification fixed in (2.22).

Lemma 2.23. If we augment $\mathcal{N}$ by using the condition of (2.3) at the primes in $\tilde{Q}$, then the Selmer groups $H^1(\mathcal{N}, \mathcal{g}^{\text{der}})$ and $H^1(\mathcal{N}, \rho(\mathcal{g}^{\text{der}})^*)$ are both trivial, so $\tilde{Q}$ is auxiliary.

Proof. The third condition on $f_i$ implies that $f_i|_{\Gamma_{q_i}} \notin \mathcal{N}_{q_i}$ and the third condition on $\phi_i$ implies that $\phi|_{\Gamma_{q_i}} \notin \mathcal{N}_{q_i}$. The rest of the argument consists in inductively applying the Greenberg–Wiles formula (2.3), see [Pat16] 5.11, especially the argument after the statement of Lemma 5.3. □

Note that not all the conditions imposed above are necessary for $\tilde{Q}$ to be auxiliary, but they will all be used later in the proof of Theorem 2.16.

Lemma 2.24. Let $X = S \cup \tilde{Q}$ with $\tilde{Q}$ auxiliary and let $\{q_{n+1}, q_{n+2}, \ldots, q_{n+s}\}$ be a set of nice primes for $\rho$ disjoint from $X$. The kernel of the restriction maps

$$\text{Res}^{n+i} : H^1(\Gamma_{X \cup \{q_{n+i}\}}, \rho(\mathcal{g}^{\text{der}})) \to \bigoplus_{v \in X} H^1(\Gamma_v, \rho(\mathcal{g}^{\text{der}}))$$

is one dimensional and we let $f_{n+i}$ be any nonzero element in it. Then $\tilde{Q} \cup \{q_{n+1}, q_{n+2}, \ldots, q_{n+s}\}$ is auxiliary iff the matrix $[f_{n+i}(\text{Prob}_{q_{n+j}})]_{1 \leq i, j \leq s}$ is invertible.

Proof. Let $\mathcal{L}_v = \mathcal{N}_v$ for $v \in X$, $\mathcal{L}_{q_{n+i}} = H^1(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}}))$ and $\mathcal{L}' = (\mathcal{L}_v)_{v \in X \cup \{q_{n+i}\}}$. Since $\tilde{Q}$ is auxiliary, both $H^1(\mathcal{L}, \rho(\mathcal{g}^{\text{der}}))$ and $H^1(\mathcal{L}', \rho(\mathcal{g}^{\text{der}})^*)$ vanish and so $H^1(\mathcal{L}', \rho(\mathcal{g}^{\text{der}})^*)$ also vanishes since it is contained in $H^1(\mathcal{L}', \rho(\mathcal{g}^{\text{der}})^*)$. Applying the Greenberg–Wiles formula (2.3), as in (2.4) we get

$$h_{\mathcal{L}}(\Gamma_{X \cup \{q_{n+i}\}}, \rho(\mathcal{g}^{\text{der}})) = h^1(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}})) - h_{nr}(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}})) \cdot h_{\mathcal{L}}(\Gamma_{X \cup \{q_{n+i}\}}, \rho(\mathcal{g}^{\text{der}})) \cdot$$

Since $h_{nr}(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}})) = h^0(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}}))$, it follows from (2.1) that the RHS of (2.7) equals $h^2(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}}))$. By (2.2), this is equal to $h^0(\Gamma_{q_{n+i}}, \rho(\mathcal{g}^{\text{der}})^*) = 1$ by the uniqueness of the root $\alpha$ in the definition of nice primes.
Let $K$ be the kernel of the restriction map
\[ H^1(\Gamma, \rho) \to \bigoplus_{v \in \mathcal{X}} H^1(\Gamma_v, \bar{\rho}(\text{der})) / \mathcal{N}_v. \]

The set \{\(f_{n+1}, f_{n+2}, \ldots, f_{n+s}\)\} spans an \(s\)-dimensional subspace of \(K\) since \(f_n\) is ramified at \(q_{n+i}\) but not at \(q_{n+j}\) for \(i \neq j\). Applying the Greenberg–Wiles formula \((2.8)\) one sees that \(\dim(K) = s\), so we have equality. Thus, the set is auxiliary iff the map
\[ \text{Span}\{f_{n+1}, f_{n+2}, \ldots, f_{n+s}\} \to \bigoplus_{j=1}^{s} H^1(\Gamma_{q_{n+j}}, \bar{\rho}(\text{der})) / \mathcal{N}_{q_{n+j}} \]
is an isomorphism. Each quotient on the RHS is one dimensional by (2) of Lemma \(2.9\) and the image is spanned by the row vectors \([f_{n+i}(\text{Frob}_{q_{n+j}})]_{1 \leq j \leq s}\), so the lemma follows. \(\square\)

2.8. Controlling the kernel of a restriction map. In \((2.7)\) we have chosen a set \(\tilde{Q}\) of nice primes for \(\bar{\rho}\) satisfying a list of conditions. By Lemma \(2.23\) \(\tilde{Q}\) is auxiliary, so the ring \(R_{\text{der}}(\tilde{Q})\) is \(W(k)\) and \(\rho_{\tilde{Q}}^{\text{der}} : \Gamma_{\tilde{Q}} \to G(W(k))\).

Let \(n_i\) be the minimum of the set of integers such that \(\rho_{\tilde{Q}}^{\text{der}}\) is ramified modulo \(p^{n_i}\) at \(q_i\). Set \(d\) to be the minimum of all the \(n_i\) if this is not \(\infty\), else set \(d = 2\). For each \(v \in \tilde{Q},\) choose \(g_v \in H^1(\Gamma_v, \rho(\text{der}))\) as follows:
- For \(v \in S\), let \(g_v = 0\)
- For \(q_i \in \tilde{Q}\) choose \(0 \neq g_{q_i} \in \mathcal{N}_{q_i}\) such that:
  - If \(\rho_{\tilde{Q}}^{\text{der}}\) is unramified modulo \(p^{d-1}\) at \(q_i\) but is ramified modulo \(p^d\) then choose \(0 \neq g_{q_i} \in \mathcal{N}_{q_i}\) such that \(\exp(p^{d-1}g_{q_i})(\rho_{\tilde{Q}}^{\text{der}}|_{\Gamma_{q_i}})\) modulo \(p^d\) is unramified at \(q_i\). This \(g_{q_i}\) is ramified at \(q_i\).
  - Otherwise choose \(g_{q_i}\) to be any ramified element of \(\mathcal{N}_{q_i}\).

The point of these choices is that for all \(a \in k\), \(\exp(p^{d-1}ag_v)(\rho_{\tilde{Q}}^{\text{der}}|_{\Gamma_v})\) is in the smooth local deformation condition \(\mathcal{D}_v\) for \(v \in \tilde{Q}\) and when \(a \neq 1\) it is ramified at \(v = q_i \in \tilde{Q}\). However, the triviality of the Selmer groups implies that the local deformation problem \((g_v)_{v \in \tilde{Q}}\) is not solvable.

By Proposition \(2.21\) there exists a Chebotarev set of nice primes \(Q_0\) such that for \(q \in Q_0\) there exists \(f(q) \in H^1(\Gamma_{Q_0 \cup \{q\}}, \rho(\text{der}))\) such that \(f(q)|_{\Gamma_v} = g_v\) for all \(v \in Q_0 \cup \tilde{Q}\). We would like to use \(q \in Q_0\) as \(n_{n+1}\), so want all the sets \(\tilde{Q} \cup \{q_{n+1}\} - \{q_i\}\) to be auxiliary.

In order for this to hold, we need that the \(n \times (n+1)\) matrices \([f_i(\text{Frob}_{q_i})]\) and \([\phi_i(\text{Frob}_{q_i})]\) are invertible after deleting any column. To ensure this, using Lemma \(2.3\) we impose the further condition that \(f_i(\text{Frob}_{q_{n+1}}) = 1\) for all \(i\). This is independent of the conditions in Proposition \(2.21\) since they involve cocycles for \(\rho^{\text{der}}\) as opposed to \(\bar{\rho}(\text{der})^*\). We also require that
\begin{equation}
(2.8) \quad \rho_{\tilde{Q}}^{\text{der}}(\text{Frob}_{q_{n+1}}) \in T(W(k)/p^dW(k)) \mod p^d
\end{equation}

(\(\rho_{\tilde{Q}}^{\text{der}}\) is not special at \(q_{n+1}\)). To see that this is achievable we use that our hypotheses on \(p\) and \(\bar{\rho}\) and Lemma \(2.7\) imply that the kernel of the reduction map \(G(W(k)/p^dW(k)) \to G(W(k)/pW(k))\) is contained in the image of \(\rho_{\tilde{Q}}^{\text{der}} \mod p^d\). This is also independent from the previously imposed conditions by Lemma \(2.8\).

Finally, we also require that \(\phi_i(\text{Frob}_{q_{n+1}}) \neq 0\) for all \(i\).
Lemma 2.25. These conditions do not conflict with the conditions imposed in Proposition 2.21.

This is not obvious since both sets of conditions involve cocycles with values in $\tilde{\rho}(g^{\text{der}})^*$. 

Proof. For $v \in S$ we have $g_v = 0$ and for $q_j \in \tilde{Q}\setminus\{q_i\}$, we have by assumption that $\phi_i|_{\Gamma_q} = 0$. Thus, $\text{inv}_v(g_v, \phi_i) = 0$ for $v \in S \cup \tilde{Q}\setminus\{q_i\}$. However, $\text{inv}_v(q_i, \phi_i) \neq 0$ by Lemma 2.9, so $\text{Res}_{S \cup \tilde{Q}}(\phi_i)$ is not in the annihilator of the line $l$ spanned by $(g_v)_{v \in S \cup \tilde{Q}}$. It follows that writing $\phi_i = d_i \zeta + \sum_j b_i \zeta_j$, where $\{\zeta_1, \ldots, \zeta_s, \zeta\}$ is the basis of $H^1(\Gamma_{S \cup \tilde{Q}}, \tilde{\rho}(g^{\text{der}})^*)$ as in Proposition 2.21, we have $a_i \neq 0$. By evaluating the RHS at $\text{Frob}_{q_{n+1}}$, bearing in mind the conditions of Proposition 2.21, we see that $\phi_i(\text{Frob}_{q_{n+1}}) \neq 0$.

Thus, the nonempty Chebotarev set of nice primes $q \in Q_0$ satisfying:

- $\zeta_i|_{\Gamma_q} = 0$ for $i = 1, 2, \ldots s$,
- the $g_i^*$ component of $\zeta|_{\Gamma_q}$ is nonzero,

\begin{equation}
\tag{2.9}
f_i(\text{Frob}_q) = 1 \text{ for all } i,
\end{equation}

\begin{equation}
\tilde{\rho}_{S \cup \tilde{Q}}^\text{new}(\text{Frob}_q) \in \Gamma(W(k)/p^dW(k)) \mod p^d \text{ is as in Lemma 2.12 (2),}
\end{equation}

also satisfies

\begin{equation}
\tag{2.10}
\exists f^{(q)} \in H^1(\Gamma_{S \cup \tilde{Q}\cup\{q\}}, \tilde{\rho}(g^{\text{der}})) \text{ such that } f^{(q)}|_{\Gamma_v} = g_v \text{ for all } v \in S \cup \tilde{Q},
\end{equation}

Lemma 2.26. For $\tilde{Q}$ as above and any $q \in Q_0$, $f^{(q)}$ spans the one dimensional kernel of the restriction map

\begin{equation}
\tag{2.11}
H^1(\Gamma_{S \cup \tilde{Q}\cup\{q\}}, \tilde{\rho}(g^{\text{der}})) \rightarrow \bigoplus_{v \in S \cup \tilde{Q}} H^1(\Gamma_{\{v\}}, \tilde{\rho}(g^{\text{der}})) \bigotimes_{\mathcal{N}_v}.
\end{equation}

Proof. The fact that the kernel is one dimensional follows from the same argument as in the first part of the proof of Lemma 2.24. Since $g_v \in \mathcal{N}_v$ for $v \in S \cup \tilde{Q}$, $f^{(q)}$ lies in the kernel and is nonzero, so it must span.

2.9. Proof of Theorem 2.16.

Proof of Theorem 2.16. Denote the density of the set of nice primes $Q_0$ constructed in 2.8 by $t_0$. At least one of the following must be true:

- $(1)$ $\exists q \in Q_0$ such that $f^{(q)}(\text{Frob}_q) \neq 0, 1$,
- $(2)$ $\exists Q_1 \subset Q_0$ having upper positive density such that $q \in Q_1 \Rightarrow f^{(q)}(\text{Frob}_q) = 1$,
- $(3)$ $\exists Q_1 \subset Q_0$ having positive upper density such that $q \in Q_1 \Rightarrow f^{(q)}(\text{Frob}_q) = 0$.

We expect that all three cases do actually occur, but this seems difficult to verify so we prove the theorem by considering all three cases separately.

For a prime $q_{n+1}$ we use the more compact notation $f_{n+1}$ instead of $f^{(q_{n+1})}$. At various points in the proof we will, for auxiliary sets $A$ and $B$, move from $\rho_{S \cup A}^{\text{new}} \mod p^d$ to $\rho_{S \cup B}^{\text{new}} \mod p^d$ by adjusting by one or two cohomology classes. While our choices may seem arbitrary, since $A$ and $B$ are auxiliary, there is exactly one class that works and after adjustment by this class the problem is uniquely liftable.
In each case we must determine the auxiliary sets \( Q \) and \( Q_i \) as in Theorem 2.16 show that \( \rho_{S\cup Q}^{Q_{\text{new}}} \) is ramified at all \( q \) \( \in \) \( Q \) and also that \( \rho_{S\cup Q_i}^{Q_{\text{new}}} \) is unramified and not special at \( q_i \). Note that \( \exp(p^{d-1}f_{n+1})\rho_{S\cup Q}^{Q_{\text{new}}} \) mod \( p^d \) is only special at \( q_{n+1} \) in Case 2).

**Proof of Case (1)** Choose any \( q_{n+1} \in Q_0 \) such that \( f^{(q_{n+1})}(\text{Frob}_{q_{n+1}}) = a \neq 0,1 \) and set
\[
Q = \tilde{Q} \cup \{q\}, \quad Q_i = Q \setminus \{q_i\}, \quad i = 1, 2, \ldots, n.
\]
We first show that \( Q \) and all \( Q_i \) are auxiliary. Recall that for \( v \in S \cup \tilde{Q}, \ f_{n+1}|_{\Gamma_v} \in \mathcal{N}_v \). The map
\[
H^1(\Gamma_{S \cup \tilde{Q}}, \tilde{\rho}(\tilde{g}^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q}} \frac{H^1(\Gamma_v, \tilde{\rho}(\tilde{g}^{\text{der}}))}{\mathcal{N}_v}
\]
is an isomorphism since \( \tilde{Q} \) is auxiliary and by Lemma 2.26 the kernel of the map
\[
H^1(\Gamma_{S \cup Q}, \tilde{\rho}(\tilde{g}^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q}} \frac{H^1(\Gamma_v, \tilde{\rho}(\tilde{g}^{\text{der}}))}{\mathcal{N}_v}
\]
is spanned by \( f_{n+1} \). As \( f_{n+1}(\text{Frob}_{q_{n+1}}) \neq 0 \), so \( f_{n+1}|_{\Gamma_{q_{n+1}}} \notin \mathcal{N}_{q_{n+1}} \), the restriction map
\[
H^1(\Gamma_{S \cup Q}, \tilde{\rho}(\tilde{g}^{\text{der}})) \to \bigoplus_{v \in S \cup Q} \frac{H^1(\Gamma_v, \tilde{\rho}(\tilde{g}^{\text{der}}))}{\mathcal{N}_v}
\]
is an injection, so \( Q \) is auxiliary.

Using the third part of (2.9) and the first part of (2.10) we see that the \( n \times (n + 1) \) matrix
\[
F = [ f_i(\text{Frob}_{q_j}) ] \quad (\text{resp. } \Phi = [ \tilde{\phi}_i(\text{Frob}_{q_j}) ])
\]
is the identity matrix with an extra column all of whose entries are 1 (resp. nonzero). Such matrices are invertible upon the deletion of any column so by Lemma 2.23 the sets \( Q_i \) are all auxiliary.

We now show that \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is ramified at all \( q_i \in Q \). Recall that for \( 1 \leq i \leq n \), \( f_i|_{\Gamma_{q_i}} \notin \mathcal{N}_{q_i} \) and for \( v \in S \cup \tilde{Q}, f_i|_{\Gamma_v} \in \mathcal{N}_v \). By (2.8) we know that \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) is not special at \( q_{n+1} \) but is special at all \( v \in S \cup \tilde{Q} \). We adjust \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) by \( \frac{1}{a}f_{n+1} \), i.e., we consider the representation
\[
\rho' = \exp(p^{d-1}f_{n+1})\rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \mod p^d.
\]
Then \( \rho' \) is special at \( q_{n+1} \) and is also ramified at \( q_{n+1} \) since \( f_{n+1} \) is. As \( f_{n+1}|_{\Gamma_v} \in \mathcal{N}_v \) for all \( v \in S \cup \tilde{Q} \), \( \rho' \) is liftable at all \( v \in S \cup \tilde{Q} \) so (by uniqueness) we have \( \rho' = \rho_{S \cup Q}^{Q_{\text{new}}} \mod p^d \). As \( a \neq 1 \), \( \frac{1}{a}f_{n+1}|_{\Gamma_{q_i}} = \frac{1}{a}g_{q_i} \neq g_{q_i} \), so this class introduces ramification at all \( q_i \) that were unramified and does not remove ramification at any \( q_i \). Thus \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is ramified at all primes of \( Q \) and this ramification occurs mod \( p^d \) for all these primes.

It remains to show that \( \rho_{S \cup Q_i}^{Q_{\text{new}}} \) mod \( p^d \) is not special at \( q_i \). As \( Q_{n+1} = \tilde{Q} \) and \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) is not special at \( q_{n+1} \) the \( i = n + 1 \) case is settled.

When \( 1 \leq i \leq n \), to get from \( \rho_{S \cup Q}^{Q_{\text{new}}} \) mod \( p^d \) to \( \rho_{S \cup Q_i}^{Q_{\text{new}}} \) mod \( p^d \) we need to remove ramification at \( q_i \) and make the representation nonspecial there while preserving liftability at all other primes. As \( f_{n+1}|_{\Gamma_v} = g_v \), adjusting by \( f_{n+1} \) removes the ramification at \( q_i \) (and perhaps some other \( q_j \)) while preserving specialness and liftability there. Our Case 1) assumption implies that this adjustment also keeps the representation nonspecial at \( q_{n+1} \). Recall \( f_i(\text{Frob}_{q_i}) = f_i(\text{Frob}_{q_{n+1}}) = 1 \). Adjusting further by a suitable nonzero multiple of \( f_i \) makes the representation special at \( q_{n+1} \) and nonspecial at \( q_i \) as desired. As \( f_i \) is in the Selmer group for \( S \) and trivial when restricted to \( \Gamma_{q_j} \) for \( j \leq n, j \neq i \), the representation remains liftable at all other primes.
Proof of Case (2) The sets \( Q \) and \( Q_i \) of Case (1) are auxiliary in this case as well, but we cannot use them as we cannot guarantee ramification of \( \rho_{S \cup Q}^{new} \) at all \( q_i \in Q \). The problem is that as \( f_{n+1}(\text{Frob}_{q_{n+1}}) = 1 \), adjusting by \( f_{n+1} \) makes the representation special at \( q_{n+1} \) and liftable at all other primes, but will remove ramification at all \( q_i \) at which \( \rho_{S \cup \tilde{Q}}^{new} \) mod \( p^d \) is ramified. We will need to add three primes to \( \tilde{Q} \) to form \( Q \) in this case.

Assume now that \( Q_1 = \{ q \in \mathcal{Q}_0 | f(q)(\text{Frob}_q) = 1 \} \) has positive upper density. Note that \( Q_1 \) is almost certainly not a Chebotarev set, though this seems difficult to settle one way or the other.

In this case \( Q = \tilde{Q} \cup \{ q_{n+1}, q_{n+2}, q_{n+3} \} \) where \( q_i \in Q_1 \) are carefully chosen; the \( Q_i \) will be described later. We will find three primes such that \( [f_{n+i}(\text{Frob}_{q_{n+i}})]_{i,j, k=1}^{3} = I_3 \). While we could make do with less, the argument is quite transparent with this choice of matrix. Also, our method shows that the techniques of \([KLR05]\) can be strengthened with more effort.

Choose \( q_{n+1} \in Q_1 \). The \( n \times (n+1) \) matrices \( F = [f_i(\text{Frob}_q)] \) and \( \Phi = [\phi_i(\text{Frob}_q)] \) are the \( n \times n \) identity matrix augmented by a column with no zero entries (by the third line of (2.9) and the first line of (2.10)). For \( q_{n+2} \in Q_1 \), the matrix \( [f_{n+i}(\text{Frob}_{q_{n+i}})]_{i,j, k=1}^{3} = [\frac{1}{2}, 0, 1] \). For our eventual \( 3 \times 3 \) matrix to be the identity we need \( x = z = 0 \).

We now choose an appropriate \( q_{n+2} \). We need \( f_{n+1}(\text{Frob}_{q_{n+2}}) = 0 \) and also \( f_{n+2}(\text{Frob}_{q_{n+1}}) = 0 \). The first of these is a Chebotarev condition disjoint from those determining \( \mathcal{Q}_0 \) and we will see that the second is as well! Dualizing the proof of Lemma 2.29 (taking \( \mathcal{L}_q = 0 \) instead of \( H^1(\Gamma, \bar{\rho}_h(g_{der})) \)) one sees that for \( e \in \{ n+1, n+2 \} \), the map

\[
H^1(\Gamma_{S \cup Q \cup \{ q_e \}}, \bar{\rho}(g_{der})^e) \to H^1(\Gamma_v, \bar{\rho}(g_{der})^e) / \mathcal{N}_v^e
\]

has one dimensional kernel. Choose \( \phi_e \) to span this kernel and scale it— that this is possible follows from Lemma 2.9—so that for any \( h \in H^1(\Gamma_{q_e}, \bar{\rho}(g_{der})) \), \( \text{inv}_{q_e}(h \cup \phi_e) = h(\text{Frob}_{q_e}) \).

The first equality below is the global reciprocity law. The second follows since for \( v \in S \cup \tilde{Q} \), \( f_{n+2}|_{\Gamma_v} \in \mathcal{N}_v \) and \( \phi_{n+1}|_{\Gamma_v} \in \mathcal{N}_v^e \) annihilate each other.

\[
0 = \sum_{v \in S \cup \{ q_1, q_2, ..., q_{n+2} \}} \text{inv}_v(f_{n+1} \cup \phi_{n+2}) = \text{inv}_{q_{n+1}}(f_{n+1} \cup \phi_{n+2}) + \text{inv}_{q_{n+2}}(f_{n+1} \cup \phi_{n+2}).
\]

(2.12)

We then have

\[
f_{n+1}(\text{Frob}_{q_{n+2}}) = 0 \iff \text{inv}_{q_{n+2}}(f_{n+1} \cup \phi_{n+2}) = 0
\]

\[
\iff \text{inv}_{q_{n+1}}(f_{n+1} \cup \phi_{n+2}) = 0 \iff \phi_{n+2}(\text{Frob}_{q_{n+1}}) = 0,
\]

where the middle “iff” follows from (2.12) and the outer ones follow from the choice of \( \phi_e \).

We will need the set of \( q_{n+2} \in Q_1 \) satisfying

\[
(f_{n+1}, \phi_{n+1})(\text{Frob}_{q_{n+2}}) = (0, 0)
\]

(2.13)

to have positive upper density. Note that the complement of these two Chebotarev conditions on \( f_{n+1} \) and \( \phi_{n+1} \) is a set of density \( t_0(1 - \frac{1}{|\mathcal{Q}_0|}) \) within \( \mathcal{Q}_0 \). Suppose that for our choice of prime \( q_{n+1} \) the set of desired second primes in \( Q_1 \) has density 0. Rename \( q_{n+1} \) to \( \ell_1 \) and let \( S_1 \subset Q_1 \) be the density 0 set of primes satisfying the above equation. Then \( Q_1 \setminus \{ \ell_1 \} \) lies in a subset of \( \mathcal{Q}_0 \) that is the complement of the conditions of (2.13) and which has density \( t_0(1 - \frac{1}{|\mathcal{Q}_0|}) \). Now choose \( \ell_2 \in Q_1 \setminus \{ \ell_1 \} \). If the set of second primes, \( S_2 \), that gives us the desired Frobenius matrix has density 0, then \( Q_1 \setminus \{ \ell_1, \ell_2 \} \) is contained in a subset of \( \mathcal{Q}_0 \) that is the complement of two sets
of independent conditions \([2.12]\). This set has density \(t_0(1 - \frac{1}{|\Gamma|^2})^2\). Continuing in this way, we get that \(q_1\) \((\ell_1, \ell_2, \ldots, \ell_r) \cup S_1 \cup S_2 \cup \cdots \cup S_r\) is contained in a set of density \(t_0(1 - \frac{1}{|\Gamma|^2})^r\). Since \(Q_1\) has positive upper density, if each \(S_i\) has density 0 then we get a contradiction for large \(r\). Thus there is a \(q_{n+1} \in Q_1\) such that for a set \(Q_2 \subset Q_1\) of positive density 
\[
(f_{n+1}, \phi_{n+1})(\text{Frob}_{q_{n+2}}) = (0, 0) \iff f_{n+1}(\text{Frob}_{q_{n+2}}) = 0, f_{n+2}(\text{Frob}_{q_{n+1}}) = 0 .
\]

Choose \(q_{n+2} \in Q_{n+2}\). For any \(q_{n+3} \in Q_2\) we then have \([f_{n+i}(\text{Frob}_{q_{n+j}})]_{1 \leq i,j \leq 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ 0 & b & 1 \end{bmatrix}\) and we need \(a = b = 0\). As before,
\[
f_{n+3}(\text{Frob}_{q_{n+2}}) = 0 \iff \phi_{n+2}(\text{Frob}_{q_{n+3}}) = 0
\]
so we need the independent Chebotarev conditions 
\[(f_{n+2}, \phi_{n+2})(\text{Frob}_{q_{n+3}}) = (0, 0)\]
to hold. Suppose for our choice of \(q_{n+2}\) there is no \(q_{n+3} \in Q_2\) satisfying (2.14). Repeating the same limiting argument as above, we see that we can find some other \(q_{n+2} \in Q_2\) so that there is a prime \(q_{n+3} \in Q_2\) satisfying (2.14).

We have thus found primes \(q_{n+1}, q_{n+2}, q_{n+3}\) so that \([f_{n+i}(\text{Frob}_{q_{n+j}})]_{1 \leq i,j \leq 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}\). Set 
\[Q = \hat{Q} \cup \{q_{n+1}, q_{n+2}, q_{n+3}\}\]
that \(Q\) is auxiliary then follows from Lemma \([2.23]\).

We now establish that \(\rho_{\hat{Q}}^{\text{new}}\) is ramified at all \(q \in Q\). To get from \(\rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\) mod \(p^d\) to \(\rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\) mod \(p^d\) requires making the representation special at \(q_{n+1}, q_{n+2}, q_{n+3}\), so we adjust by \(h = f_{n+1} + f_{n+2} + f_{n+3}\). Observe that \(h(\text{Frob}_{q_{n+i}}) = 1\) for \(i = 1, 2, 3\), and for \(v \in S \cup \tilde{Q}\), \(h|_{\Gamma_v} = 3g_v \in \mathcal{N}_v\) and \(h|_{\Gamma_v} \neq g_v\), so if \(\rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\) is unramified at \(v\) we are introducing ramification and if it is ramified at \(v\) we are not removing the ramification. Also, adjusting by \(h\) introduces ramification at each of \(q_{n+1}, q_{n+2}, q_{n+3}\) and makes the representation special at each of these primes so this adjusted representation must be equal to \(\rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\) mod \(p^d\) (which is then ramified at all \(q \in Q\)).

For \(i \leq n\) our choice of \(Q_i\) depends on whether or not \(\rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\) mod \(p^d\) is ramified at \(q_i\). We set
\[
Q_i = \begin{cases} 
Q \setminus \{q_i\} & i = n + 2, n + 3 \\
\{q_1, q_2, \ldots, q_n\} & i = n + 1 \\
\{q_1, q_2, \ldots, q_{n+1}\} \setminus \{q_i\} & i \leq n, \rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\text{ mod } p^d\text{ is unramified at } q_i \\
Q \setminus \{q_i, q_{n+1}\} & i \leq n, \rho_{\hat{Q} \cup \tilde{Q}}^{\text{new}}\text{ mod } p^d\text{ is ramified at } q_i .
\end{cases}
\]

When \(i = n + 2, n + 3\), that \(Q_i\) is auxiliary follows from Lemma \([2.24]\) since the relevant principal minors of \([f_{n+i}(\text{Frob}_{q_{n+j}})]_{1 \leq i,j \leq 3}\) are invertible. That \(Q_{n+1}\) is auxiliary is clear since \(Q_{n+1} = \hat{Q}\).

For \(1 \leq i \leq n\) we will show both choices of \(Q_i\) are auxiliary; we need both to guarantee nonspecialness at \(q_i\). That the first choice of \(Q_i\) is auxiliary was demonstrated in Case (1) when we saw that the \(n \times (n + 1)\) matrices \(F = [f_i(\text{Frob}_{q_j})]\) and \(\Phi = [\phi_i(\text{Frob}_{q_j})]\) are the \(n \times n\) identity matrix augmented by a column with no zero entries. We now show our second choice of \(Q_i\) is auxiliary. The set \(\{q_1, q_2, \ldots, q_n, q_{n+1}\} \setminus \{q_i\}\) is auxiliary and the map
\[
H^1(\Gamma_{\hat{Q} \cup \tilde{Q} \setminus \{q_i\}}, \tilde{\rho}(g^{\text{der}})) \to \bigoplus_{v \in \hat{Q} \cup \tilde{Q} \setminus \{q_i\}} H^1(\Gamma_v, \tilde{\rho}(g^{\text{der}})) \bigotimes \mathcal{N}_v
\]
has kernel spanned by \( f_i \). We claim that the map

\[
H^1(\Gamma_{S \cup \tilde{Q} \cup \{q_{n+1}\} \backslash \{q_i\}}, \bar{\rho}(g^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q} \cup \{q_{n+1}\} \backslash \{q_i\}} \frac{H^1(\Gamma_v, \bar{\rho}(g^{\text{der}}))}{N_v}
\]

also has kernel spanned by \( f_i \). Clearly \( f_i \) is in the kernel and the only other possibility is that the kernel is two dimensional. If it were, then changing the target direct sum as below

\[
H^1(\Gamma_{S \cup \tilde{Q} \cup \{q_{n+1}\} \backslash \{q_i\}}, \bar{\rho}(g^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q} \cup \{q_{n+1}\} \backslash \{q_i\}} \frac{H^1(\Gamma_v, \bar{\rho}(g^{\text{der}}))}{N_v}
\]

would yield at least a one dimensional kernel which contradicts that \( \tilde{Q} \cup \{q_{n+1}\} \backslash \{q_i\} \) is auxiliary. Thus the kernel of \((2.15)\) is spanned by \( \rho \) and so the kernel of

\[
H^1(\Gamma_{S \cup \tilde{Q} \cup \{q_{n+1}, q_{n+2}\} \backslash \{q_i\}}, \bar{\rho}(g^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q} \cup \{q_{n+1}, q_{n+2}\} \backslash \{q_i\}} \frac{H^1(\Gamma_v, \bar{\rho}(g^{\text{der}}))}{N_v}
\]

is two dimensional. Set \( g_{n+1} = f_i \) and \( g_{n+2} = f_{n+1} - f_{n+2} \). The \( 2 \times 2 \) matrix \([g_{n+i}(\text{Frob}_{q_{n+i}})] = [\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}]\) is invertible, so by (the proof of) Lemma \( 2.24 \)

\[
H^1(\Gamma_{S \cup \tilde{Q} \cup \{q_{n+1}, q_{n+2}\} \backslash \{q_i\}}, \bar{\rho}(g^{\text{der}})) \to \bigoplus_{v \in S \cup \tilde{Q} \cup \{q_{n+1}, q_{n+2}\} \backslash \{q_i\}} \frac{H^1(\Gamma_v, \bar{\rho}(g^{\text{der}}))}{N_v}
\]

is an isomorphism and \( Q_i \) is auxiliary.

Finally, we show that \( \rho_{\tilde{Q}_i} \mod p^d \) is not special at \( q_i \) in all cases:

- \( i = n + 2 \): to get from \( \rho_{\tilde{Q}_i} \mod p^d \) to \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) we adjust by \( h = f_{n+1} + f_{n+3} \) to make the representation special at \( q_{n+1} \) and \( q_{n+3} \). As \( h(\text{Frob}_{q_{n+2}}) = 0 \), the action of \( \text{Frob}_{q_{n+2}} \) on the \( g_a \) component of \( \exp(p^{d-1}h)\rho_{\tilde{Q}_{n+2}} \mod p^d \) is given by multiplication by \( \text{Norm}(q_{n+2}) - p^{d-1} \) so is not special. For \( v \in S \cup \tilde{Q} \), \( h|_{\Gamma_v} = 2g_v \in \mathcal{N}_v \), so adjusting by \( h \) keeps the representation liftable at \( v \) without removing ramification. We conclude as before by uniqueness.
- \( i = n + 3 \): set \( h = f_{n+1} + f_{n+2} \) and proceed as in the \( i = n + 2 \) case.
- \( i = n + 1 \): as \( Q_{n+1} = \tilde{Q} \) and \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) is not special at \( q_{n+1} \) by construction we are done.
- \( i \leq n \): we go from \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) to \( \rho_{\tilde{Q}_i} \mod p^d \). Our starting point is not special at \( q_i \).
  - If \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) is unramified at \( q_i \) then adjust by a (nonzero) multiple of \( f_i \) to make the representation special at \( q_{n+1} \). This makes the representation nonspecial at \( q_i \) as desired (but preserves unramifiedness) and preserves liftability at the other primes in \( S \cup \tilde{Q} \), so we are done. (If \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) were ramified at \( q_i \) and we used this \( Q_i \), we would need to adjust by \( f_{n+1} \) to remove ramification at \( q_i \). But then the representation would be special at both \( q_i \) and \( q_{n+1} \) and liftable elsewhere. We need nonspecialness at \( q_i \), which is why we need the \( Q_i \) below in the ramified case.)
  - If \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) is ramified at \( q_i \), then when going from \( \rho_{\tilde{Q}_{n+2}} \mod p^d \) to \( \rho_{\tilde{Q}_i} \mod p^d \) we need to make the representation special at \( q_{n+1} \) and \( q_{n+2} \) and unramified and nonspecial at \( q_i \). The cohomology class \( h \) that we use must satisfy:
* $h(\text{Frob}_{q_{n+1}}) = 1$ for $i = 1, 2$ (specialness at $q_{n+1}, q_{n+2}$),
* $h|_{\Gamma_{q_i}} = q_{q_i}$ a nonspecial unramified class (removes ramification at $q_i$ and makes it nonspecial),
* $h$ is unramified at $q_{n+3}$,
* $h|_{\Gamma_v} \in N_v$ for $v \in S \cup \hat{Q} \setminus \{ q_i \}$ (preserves liftability at these places).

The class $h = \prod (f_i + f_{n+1} + f_{n+2})$ satisfies all these conditions, so we are done by uniqueness. Note that in this case the representation may become unramified at some $v \in S \cup \hat{Q}$ (besides $q_i$).

**Proof of Case 3** This is the most delicate of the three cases and makes important use of parts 3) and 4) of Lemma 2.9.

Assume $Q_1 = \{q \in Q_0 | f_{n+1}(\text{Frob}_q) = 0 \}$ has positive upper density. Note that this is almost certainly not a Chebotarev set, but again this seems difficult to prove. Our set $Q$ will be $\hat{Q} \cup \{q_{n+1}, q_{n+2}, q_{n+3}\}$ for three carefully chosen primes in $Q_1$ such that the matrix

$$[f_{n+1}(\text{Frob}_{q_{n+j}})]_{1 \leq i,j \leq 3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$  

After constructing $Q$ we will describe the sets $Q_i$.

Choose $q_{n+1} \in Q_1$. Then the map

$$H^1(\Gamma_{S \cup \hat{Q} \cup \{q_{n+1}\}}, \overline{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in S \cup \hat{Q}} H^1(\Gamma_v, \overline{\rho}(\mathfrak{g}^{\text{der}})) / N_v$$

has kernel spanned by $f_{n+1}$ and since $q_{n+1} \in Q_1 \Rightarrow f_{n+1}|_{\Gamma_{q_{n+1}}} \in N_{q_{n+1}}$, we see that $f_{n+1}$ spans the kernel of

$$H^1(\Gamma_{S \cup \hat{Q} \cup \{q_{n+1}\}}, \overline{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in S \cup \hat{Q} \cup \{q_{n+1}\}} H^1(\Gamma_v, \overline{\rho}(\mathfrak{g}^{\text{der}})) / N_v$$

as well.

For $q_{n+1}$ fixed, consider another prime $q_{n+2} \in Q_1$. The matrix $[f_{n+1}(\text{Frob}_{q_{n+j}})]_{1 \leq i,j \leq 2} = \begin{bmatrix} 0 & x \\ z & 0 \end{bmatrix}$ and we want $x = z = 1$. As the kernel of

$$H^1(\Gamma_{S \cup \hat{Q} \cup \{q_{n+1}, q_{n+2}\}}, \overline{\rho}(\mathfrak{g}^{\text{der}})) \to \bigoplus_{v \in S \cup \hat{Q}} H^1(\Gamma_v, \overline{\rho}(\mathfrak{g}^{\text{der}})) / N_v$$

is spanned by $\{f_{n+1}, f_{n+2}\}$, Lemma 2.24 implies that $S \cup \hat{Q} \cup \{q_{n+1}, q_{n+2}\}$ is auxiliary if this holds.

For a potential second prime $q_{n+2} \in Q_1$, we need that $f_{n+1}(\text{Frob}_{q_{n+2}}) = 1$ and this is a Chebotarev condition disjoint from the one determining $Q_0$. We also need $f_{n+2}(\text{Frob}_{q_{n+1}}) = 1$. For $e \in \{n+1, n+2\}$, let $\phi_e$ as before span the kernel of

$$H^1(\Gamma_{S \cup \hat{Q} \cup \{q_e\}}, \overline{\rho}(\mathfrak{g}^{\text{der}})^*) \to \bigoplus_{v \in S \cup \hat{Q}} H^1(\Gamma_v, \overline{\rho}(\mathfrak{g}^{\text{der}})^*) / N_v$$

and scale it as in (4) of Lemma 2.9. The first equality below is the global reciprocity law and the second holds as, for $v \in S \cup \hat{Q}$, $f_{n+1}|_{\Gamma_v} \in N_v$ and $\phi_{n+1}|_{\Gamma_v} \in N_v^{\perp}$ annihilate each other. The third uses parts (3) and (4) of Lemma 2.9. We finally see the reason for the asymmetry in our statements for these parts since we have the freedom to scale $\phi_{n+1}$ but not $f_{n+2}$ as it comes from Proposition
Note that $\gamma_{q_{n+1}}$ only depends on $f_{n+2}$ and thus on $q_{n+2}$ but not $q_{n+1}$. Since $Q_1$ has positive upper density and $k^\times$ is finite, there is a $\gamma_0 \in k^\times$ and a subset $Q_2 \subset Q_1$ of positive upper density such that $q \in Q_2 \Rightarrow \gamma_q = \gamma_0$. So for $q_{n+1}, q_{n+2} \in Q_2$,

$$f_{n+2}(\text{Frob}_{q_{n+1}}) + \gamma_0 \phi_{n+1}(\text{Frob}_{q_{n+2}}) = 0,$$

or equivalently

$$f_{n+2}(\text{Frob}_{q_{n+1}}) = -\gamma_0\phi_{n+1}(\text{Frob}_{q_{n+2}}).$$

Henceforth, we will only choose primes from $Q_2$. Having chosen $q_{n+1} \in Q_2$, we want the set of $q_{n+2} \in Q_2$ satisfying

$$(f_{n+1}(\text{Frob}_{q_{n+2}}) = 1 \text{ and } f_{n+2}(\text{Frob}_{q_{n+1}}) = 1) \Leftrightarrow (f_{n+1}, \phi_{n+1})(\text{Frob}_{q_{n+2}}) = (1, -1/\gamma_0)$$

to have positive upper density. Note that the complement of these two Chebotarev conditions associated to $f_{n+1}$ and $\phi_{n+1}$ on primes of $Q_2$ forms a set of density $t_0(1 - 1/|k^\times|)$ within $Q_0$. Suppose that for our choice of $q_{n+1}$ the set of desired second primes $q_{n+2} \in Q_2$ has density 0. Using the limiting argument as before, we see that by changing $q_{n+1}$ there is a set $Q_3 \subset Q_2$ of positive upper density such that for $q_{n+2} \in Q_3$, $f_{n+1}(\text{Frob}_{q_{n+2}}) = 1 = f_{n+2}(\text{Frob}_{q_{n+1}})$.

Having chosen $q_{n+1}$, for $q_{n+2}, q_{n+3} \in Q_3$ we have $[f_{n+i}(\text{Frob}_{q_{n+i}})]_{1 \leq i, j \leq 3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. We want $a = b = 1$, so we fix $q_{n+2}$ and vary $q_{n+3}$. Choosing

$$(f_{n+2}, \phi_{n+2})(\text{Frob}_{q_{n+3}}) = (1, -1/\gamma_0)$$

is a pair of Chebotarev conditions independent of those determining $Q_0$. If a $q_{n+3}$ exists satisfying these conditions we are done. If not, using the same limiting argument as before we see that we can change $q_{n+2}$ so that a $q_{n+3}$ satisfying these conditions will indeed exist. Thus, we now have primes $q_{n+1}, q_{n+2}, q_{n+3}$ such that $[f_{n+i}(\text{Frob}_{q_{n+i}})]_{1 \leq i, j \leq 3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.

We are now ready to settle Case (3). Set

$$Q_i = \{q_1, q_2, \ldots, q_{n+1}, q_{n+2}, q_{n+3}\},$$

$$Q_i = \{q_1, q_2, \ldots, q_{n}, q_{n+1}\} \setminus \{q_i\} \quad i \leq n + 1$$

$$Q_i = \{q_1, q_2, \ldots, q_{n+1}, q_{n+2}, q_{n+3}\} \setminus \{q_i\} \quad i = n + 2, n + 3.$$

That $Q$ is auxiliary follows from Lemma 2.24. For $i \leq n + 1$, that $Q_i$ is auxiliary follows as before from the fact that the $n \times (n + 1)$ matrices $F = [f_i(\text{Frob}_{q_i})]$ and $\Phi = [\phi_i(\text{Frob}_{q_i})]$ are the $n \times n$ identity matrix augmented by a column with no zero entries. That $Q_i$ is auxiliary for $i = n + 2, n + 3$ follows from Lemma 2.24 since the relevant principal minors of the matrix $[f_{n+i}(\text{Frob}_{q_{n+i}})]_{1 \leq i, j \leq 3}$ are invertible.

We show that $\rho_{S \cup \hat{Q}}^{Q_{\text{new}}} \mod p^d$ is ramified at all primes in $Q$. To get from $\rho_{S \cup \hat{Q}}^{Q_{\text{new}}} \mod p^d$ to $\rho_{S \cup \hat{Q}}^{Q_{\text{new}}} \mod p^d$ requires making the representation special at $q_{n+1}, q_{n+2}, q_{n+3}$. The class $h = \frac{1}{2}(f_{n+1} + f_{n+2} + f_{n+3})$ satisfies $h(\text{Frob}_{q_{n+1}}) = 1$, so adjusting by this class yields specialness and ramification at $q_{n+1}, q_{n+2}, q_{n+3}$. Note that $h|_{\Gamma_v} = \frac{3}{2}g_v$ for $v \in S \cup \hat{Q}$, so if $\rho_{S \cup \hat{Q}}^{Q_{\text{new}}} \mod p^d$ is unramified at $v$ we are introducing ramification and if it is ramified at $v$ we are not removing
ramification. By uniqueness as before, the adjusted representation must be equal to \( \rho_{S \cup Q}^{Q_{\text{new}}} \) mod \( p^d \) which is therefore ramified at all primes \( q \in Q \).

It remains to show that \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is not special at \( q \). Recall that \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is unramified at \( q \) and if \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is ramified at \( q \), then the ramification first occurs mod \( p^d \).

- \( i = n + 2 \): to get from \( \rho_{S \cup Q}^{Q_{\text{new}}} \) mod \( p^d \) to \( \rho_{S \cup Q_{n+2}}^{Q_{\text{new}}} \) mod \( p^d \) we adjust by \( h = f_{n+1} + f_{n+3} \) to make the representation ramified and special at \( q_{n+1} \) and \( q_{n+3} \). As \( h(\text{Frob}_{q_{n+2}}) = 2 \), the adjusted representation is not special at \( q_{n+2} \). For \( v \in S \cup \tilde{Q} \), \( h|_{\Gamma_v} = 2g_v \) so the representation remains special (and ramified) for such a \( v \).
- \( i = n + 3 \): the same argument as above works with \( h = f_{n+1} + f_{n+2} \).
- \( i = n + 1 \): this follows since \( Q_{n+1} = \tilde{Q} \) and \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) is not special at \( q_{n+1} \) by construction.
- \( i \leq n \) we move from \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) to \( \rho_{S \cup Q_i}^{Q_{\text{new}}} \) mod \( p^d \). This breaks into two cases.
  - if \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) is unramified at \( q_i \) we use a nonzero multiple of \( f_i \) to make the representation special at \( q_{n+1} \). This keeps the representation unramified at \( q_i \) and also makes it nonspecial at \( q_i \).
  - if \( \rho_{S \cup \tilde{Q}}^{Q_{\text{new}}} \) mod \( p^d \) is ramified at \( q_i \), using that \( f_{n+1}|_{\Gamma_{q_i}} = g_{q_i} \) we adjust by \( f_{n+1} \) to remove ramification at \( q_i \). Then as \( f_{n+1}(\text{Frob}_{q_{n+1}}) = 0 \), the representation at \( q_{n+1} \) is nonspecial before and after adjustment. Now use a nonzero multiple of \( f_i \) to make the representation special at \( q_{n+1} \). This keeps the representation unramified at \( q_i \) and also makes the representation nonspecial at \( q_i \).

This completes the proof of Case (3) of Theorem 2.16 and hence also the proof of the theorem.

\[ \square \]

3. AN EXACT COMPUTATION OF SELMER GROUPS

A simple consequence of Theorem 2.16 is that given suitable \( \tilde{\rho} : \Gamma_S \to G(k) \) and a set \( S \) of primes of \( F \) (including all the ramified primes) together with balanced local conditions at these primes, there exists a finite set \( Q \) of nice primes such that \( R_{S \cup Q}^{Q_{\text{new}}} \cong W(k) \) and \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is ramified at all primes \( q \in Q \). This was first proved for \( G = GL_2 \) in [KRe33] and similar statements for \( GL_n \) appear in [MMS17, Theorem 1] and for general \( G \) in [Pat16, Theorem 3.16].

We let \( \rho_{S \cup Q} : \Gamma_{S \cup Q} \to G(R_{S \cup Q}) \) be the versal deformation representing the functor of deformations of \( \tilde{\rho} \), where we allow arbitrary lifts at primes in \( Q \) but still require the lifts to be in the given local conditions \( D_v \) at primes \( v \in S \). There is a natural surjection \( \pi : R_{S \cup Q} \to R_{S \cup Q}^{Q_{\text{new}}} \) and we let \( \eta = \text{Ker}(\pi) \).

**Theorem 3.1.** Let \( \tilde{\rho} : \Gamma_F \to G(k) \) satisfy the assumptions of Theorem 2.16 and let \( Q \) be as in the conclusion of the theorem. For each \( q \in Q \), let \( m_q \) be the smallest integer such that \( \rho_{S \cup Q}^{Q_{\text{new}}} \) is ramified at \( q \) modulo \( p^{m_q} \). Then

\[ \eta/\eta^2 \cong \bigoplus_{q \in Q} W(k)/p^{m_q} W(k) ; \]

in particular, \( \eta/\eta^2 \) is a finite \( W(k) \)-module and \( \text{Spec}(R_{S \cup Q}^{Q_{\text{new}}}) \) is an irreducible component of \( \text{Spec}(R_{S \cup Q}) \).
Finiteness of $\eta/\eta^2$, in fact that $\eta/\eta^2$ is isomorphic to a submodule of $\bigoplus_{v \in S} W(k)/p^nW(k)$, in the case $G = GL_2$ was first proved in [KR03] (where equality was conjectured), and a version of this statement for $G = GL_n$ was also proved in [MMS17] §4.

3.1. Selmer and dual Selmer groups modulo $p^n$. Let $K$ be the quotient field of $W(k)$. For any finitely generated free $W(k)$-module $M$ let $M_{\infty}$ denote $M \otimes_{W(k)} K/W(k)$ and for $n > 0$ let $M_n = M/p^nM$ denote the $p^n$-torsion in $M_{\infty}$. For each $v \in S \cup Q$ and $n > 0$, the choice of smooth local condition $D_v$ at each such prime, the given condition at primes in $S$ and the one defined in §2.3 at primes in $Q$, gives rise to a $W(k)$-submodule $N_{v,n} \subset H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_n)$; see, for example, [FKP19] §4. The module $N_{v,1}$ is the tangent space of the deformation condition, denoted $N_v$ in §2.4. We let $N_{v,n}^\perp \subset H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{n})$ denote the annihilator of $N_{v,n}$ with respect to the Tate duality pairing (generalising the one in §2.2). We let $N_{v,\infty} \subset H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{\infty})$ be the direct limit of all the $N_{v,n}$.

We let $N_{v,n}' = N_{v,n}$ for $v \in S$ and let $N_{v,n}' = H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{n})$ for $v \in Q$.

- For $\bullet$ being $n$ or $\infty$, we define the Selmer groups $H^1_{N_{\bullet}}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{\bullet})$ to be, as in Definition 2.13, the kernel of the map

$$H^1(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{\bullet}) \to \bigoplus_{v \in S\cup Q} H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{\bullet})$$

and define $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet})$ in the same way with $N_{v,n}$ replaced by $N_{v,n}'$.

- We also define dual Selmer groups $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet})$ to be the kernel of the map

$$H^1(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet}) \to \bigoplus_{v \in S\cup Q} H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet})$$

and define $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet})$ similarly.

- Tate duality gives a perfect pairing of $W(k)$-modules:

$$H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*) \times H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*) \to K/W(k)$$

and we let $N_{v,\infty}^\perp \subset H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*)$ be the annihilator of $N_{v,\infty} \subset H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{\infty})$.

We then define the integral dual Selmer group $H^1_{N_{v,\infty}^\perp}(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*)$ to be the kernel of the map

$$H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*) \to \bigoplus_{v \in S\cup Q} H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*)$$

Lemma 3.2.

1. $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet}) = 0$ and $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet}) = 0$ for all $\bullet$ ($= n$ or $\infty$);
2. $H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})^*_{\bullet}) = 0$ for all $n > 0$;
3. The map

$$H^1_{N_{\bullet}'}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{n}) \to \bigoplus_{v \in S\cup Q} H^1(\Gamma_v, \rho_{S\cup Q}^{Q-new}(g_{\text{der}})_{n})$$

is an injection for all $n$;
(4) \( H^1_{\mathcal{N}, \mathcal{L}}(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \) is annihilated by a power of \( p \).

Proof. Item (1) for \( \bullet = n \) follows from Lemma 6.1 of [FKP19] and the fact that since \( Q \) is auxiliary, the statement holds for \( n = 1 \), and for \( \bullet = \infty \) it follows by taking limits.

Item (2) follows from (1) since \( H^1_{\mathcal{N}, \mathcal{L}}(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \) is a submodule of \( H^1_{\mathcal{N}, \mathcal{L}}(\Gamma_{S/\mathcal{Q}}, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \) (which is immediate from the definitions).

Item (3) follows from the vanishing of \( H^1_{\mathcal{N}, \mathcal{L}}(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \) in (1) and the definition of the Selmer groups.

For \( v \in S \cup Q \), let \( \mathcal{N}_v^{\infty, \perp} \) be the image of \( \mathcal{N}_v^{\mathcal{L}} \) in \( H^1(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \); it is contained in \( \mathcal{N}_v^{\perp} \) by the definition of \( \mathcal{N}_v^{\infty, \perp} \). The finite generation of \( g^{\text{der}} \) as \( W(k) \)-module implies that kernel of the map
\[
H^1(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \to H^1(\Gamma_{S/\mathcal{Q}}, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*)
\]
is killed by a power \( p^a \) of \( p \) depending only on \( v \), so the same holds for \( \mathcal{N}_v^{\infty, \perp} / \mathcal{N}_v^{\infty, \perp} \). Then (1) implies that \( H^1_{\mathcal{N}, \mathcal{L}}(\Gamma_v, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) \) is killed by \( p^a \), where \( a = \max \{a_v\} \in S \cup Q \), so (4) follows. □

Lemma 3.3. There is a canonical isomorphism
\[
\text{Hom}_{W(k)}(\eta/\eta^2, K/W(k)) \cong H^1_{\mathcal{N}^\mathcal{L}}(\Gamma_{\mathcal{S}/\mathcal{Q}}, \rho^{Q-\text{new}}_{\mathcal{S}/\mathcal{Q}}(g^{\text{der}})^*) .
\]

Proof. See [DTT97] Lemma 2.40 for the proof in the case of \( GL_n \) (which works in general). □

3.2. Local computations II. Let \( q \) be a nice prime for \( \bar{\rho} \) and let \( \alpha \) be the root associated to \( q \). Then by definition of the local condition at \( q \) (2.3), any deformation of \( \bar{\rho}|_{\Gamma_q} \) to \( W(k) \) in \( D_q \) has a representative (up to \( \tilde{G}(W(k))-\text{conjugacy} \) \( \rho : \Gamma_q \to G(W(k)) \) factoring through \( H_\alpha(W(k)) \). We fix such a \( \rho \) and we assume that it is ramified; let \( m \geq 1 \) be the maximal integer such that \( \rho \) is unramified modulo \( p^m \).

For any root \( \beta \in \Phi(G, T) \) such that \( \beta \neq \pm \alpha \), we have that \( [g_\alpha, g_\beta] \subset g_{\alpha + \beta} \) if \( \alpha + \beta \) is a root and it is zero otherwise. It follows from this and the definition of \( H_\alpha \), that as an \( H_\alpha \)-module (via the adjoint action) there is a decomposition
\[
g^{\text{der}} = V_\alpha \oplus (t_\alpha \cap g^{\text{der}}) \oplus W_\alpha \text{ with } V_\alpha = g_\alpha \oplus \mathfrak{I}_\alpha \oplus g_{-\alpha} \text{ and } W_\alpha = \bigoplus_{\beta \neq \pm \alpha} g_\beta .
\]
Furthermore, \( W_\alpha \) has a finite filtration, with each term a sum of root spaces, such that \( U_\alpha \subset H_\alpha \) acts trivially on the associated graded and as a \( T \)-module the associated graded is simply \( \bigoplus_{\beta \neq \pm \alpha} g_\beta \) with its natural \( T \)-action. This decomposition and filtration clearly induce a decomposition and filtration of \( g^{\text{der}} \) as a \( \Gamma_q \)-module.

Lemma 3.4.

(1) \( H^1(\Gamma_q, (W_\alpha)_n) = 0 \) for all \( n > 0 \);
(2) \( H^i(\Gamma_q, W_\alpha \otimes_{W(k)} K) = 0 \) for \( i = 0, 1, 2 \);
(3) \( H^i(\Gamma_q, V_\alpha \otimes_{W(k)} K) = 0 \) for \( i = 0, 1, 2 \);
(4) For all \( n \geq m \),
\[
H^1(\Gamma_q, (V_\alpha)_n) \cong H^1(\Gamma_q, (V_\alpha)_n) \oplus \text{Im}(H^1(\Gamma_q, (g_\alpha)_n)) \to H^1(\Gamma_q, (V_\alpha)_n)
\]
\[
\cong W(k)/p^m \oplus W(k)/p^m ;
\]
(5) \( \text{Im}(H^1(\Gamma_q, (g_\alpha)_x)) \to H^1(\Gamma_q, (V_\alpha)_x) = 0 \);
(6) \( H^1(\Gamma_q, (V_\alpha)_x) \cong W(k)/p^m \).
Proof. Items (1) and (2) follow by induction using the filtration discussed above and the fact that the analogous vanishing holds for each \( g_\beta \), with \( \beta \neq \alpha \). This uses the assumption that \( q \) is a nice prime so the character giving the \( \Gamma_q \)-action on \( g_\beta \) is neither the trivial character nor the cyclotomic character \( \kappa \).

For (3) we note that \( V_\alpha \) also has a filtration as \( \Gamma_q \)-module

\[ 0 = V_0 \subset V_1 \subset V_2 \subset V_3 = V_\alpha \]

with \( V_1 = g_\alpha, V_2/V_1 = I_\alpha \) and \( V_3/V_2 = g_{-\alpha} \). By the niceness assumption we have vanishing of all cohomology for \( g_{-\alpha} \). We conclude by using the known cohomology of the trivial (for \( I_\alpha \)) and cyclotomic (for \( g_\alpha \)) characters and noting that the extension

\[ 0 \rightarrow g_\alpha \otimes_{W(k)} K \rightarrow V_2 \otimes_{W(k)} K \rightarrow I_\alpha \otimes_{W(k)} K \rightarrow 0 \]

is non-split since \( \rho \) is ramified.

For (4) we first use the vanishing of all cohomology of \( g_{-\alpha} \) as above to replace \( V_\alpha \) by \( V_2 \). We then use the exact sequences

\[ 0 \rightarrow (g_\alpha)_n \rightarrow (V_2)_n \rightarrow (I_\alpha)_n \rightarrow 0 , \]

the known cohomology of the first and third (nonzero) terms and the structure of the action of \( I_q \) (determined by the definition of \( D_q \)). This gives that \( (V_\alpha)_n^I = (g_\alpha)_n \oplus (I_\alpha)_m \) and \( H^1(\Gamma_q, (V_\alpha)_n) \cong W(k)/p^m \) (again using that \( q \) is a nice prime). The fact that \( \text{Im}(H^1(\Gamma_q, (g_\alpha)_n) \rightarrow H^1(\Gamma_q, (V_\alpha)_n) \cong W(k)/p^m \) follows by considering the long exact sequence of cohomology associated to the short exact sequence above: the structure of the action of inertia implies that the image of the boundary map \( H^0(\Gamma_q, (I_\alpha)_n) \rightarrow H^1(\Gamma_q, (g_\alpha)_n) \) has image isomorphic to \( W(k)/p^{m-n} \).

The two submodules \( H^1(\Gamma_q/I_q, (V_\alpha)_n^I) \) and \( \text{Im}(H^1(\Gamma_q, (g_\alpha)_n) \rightarrow H^1(\Gamma_q, (V_\alpha)_n) \) are seen to intersect trivially by using the map \( (V_2)_n \rightarrow (I_\alpha)_n \). We see that they generate all of \( H^1(\Gamma_q, (V_\alpha)_n) \) by computing \( h^2(\Gamma_q, (V_\alpha)_n) \) using (2.2) and then using (2.1) to compute \( h^1(\Gamma_q, (V_\alpha)_n) \).

Item (5) holds since a divisible \( W(k) \)-module which is killed by \( p^m \) must be zero.

Item (6) follows from (4) and (5) since the inclusions \( (I_\alpha)_n \rightarrow (I_\alpha)_\infty \) induce injections on (un-ramified) cohomology.

\[ \square \]

3.3. Proof of Theorem [3.1]

Proof of Theorem [3.1] We apply the computations of Lemma [3.4] with \( \rho = \rho_{S \cup Q}^{Q-\text{new}} \).

The module \( N_{\alpha,n} \subset H^1(\Gamma_q, \rho_{S \cup Q}^{Q-\text{new}}(g_{\text{der}})_n) \) for \( q \in Q \) corresponds to the summand

\[ \text{Im}(H^1(\Gamma_q, (g_\alpha)_n) \rightarrow H^1(\Gamma_q, (V_\alpha)_n)) \oplus H^1(\Gamma_q, (I_\alpha) \cap g_{\text{der}}) \]

so by (4) it follows that the quotient \( \frac{H^1(\Gamma_v, \rho_{S \cup Q}^{Q-\text{new}}(g_{\text{der}})_n)}{N_{v,n}} \) is isomorphic to \( W(k)/p^{m_q} \) for all \( q \in Q \). To prove the theorem it suffices, by Lemmas [3.2] and [3.3] to show that the length of \( H^1_{N_{\alpha,n}}(\Gamma_{S \cup Q}, \rho_{S \cup Q}^{Q-\text{new}}(g_{\text{der}})_n) \) as \( W(k) \)-module is \( \sum_{q \in Q} m_q \).

This follows by comparing the Greenberg–Wiles formula for the Selmer conditions given by \( N_{\alpha,n} \) and \( N_{\alpha,v} \). Since the dual Selmer group for \( N_{\alpha,n} \) vanishes by (2) of Lemma [3.2], it follows from (1) of that Lemma and the definitions of \( N_{\alpha,v} \) and \( N_{\alpha,v} \) for all \( v \in S \cup Q \), that the only contribution to the length of \( H^1_{N_{\alpha,n}}(\Gamma_{S \cup Q}, \rho_{S \cup Q}^{Q-\text{new}}(g_{\text{der}})_n) \) comes from the primes in \( Q \). This contribution is precisely

\[ \ell(H^1(\Gamma_v, \rho_{S \cup Q}^{Q-\text{new}}(g_{\text{der}})_n)) - \ell(N_{v,n}) = m_q. \]

\[ \square \]
3.4. Vanishing of $H^2$. Let $R$ be the versal ring representing all deformations of $\tilde{\rho} : \Gamma_{S\cup Q} \to G(k)$ (with fixed determinant). There is a natural surjection $\xi: R \to R^Q_{S\cup Q} \cong W(k)$.

**Theorem 3.5.**

1. $H^2(\Gamma_{S\cup Q}, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) \rightarrow \oplus_{v\in S\cup Q} H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k))$.
2. $H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ for all $v \in Q$.
3. Thus, if $H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ for all $v \in S$, then it follows that $H^2(\Gamma_{S\cup Q}, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$, and so $\xi$ gives rise to a formally smooth (closed) point of $\text{Spec}(R[1/p])$.

**Remark 3.6.**

- The condition of $H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ is also phrased as saying that $\rho_{Q\cup S}^{Q-new}(g^{\text{der}})$ is generic at $v$.
- Instead of the condition $H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ for all $v \in S$ we could assume the stronger condition that $H^2(\Gamma_v, \tilde{\rho}(g^{\text{der}})) = 0$ for all $v \in S$; this is perhaps more intrinsic since it does not depend on the set $Q$.

**Proof.** The first part follows from the fact that $H^1_{\text{N}^1}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ which follows from Lemma 3.2 (4).

As the Poitou–Tate exact sequence gives that the dual of $H^1_{\text{N}^1}(\Gamma_{S\cup Q}, \rho_{S\cup Q}^{Q-new}(g^{\text{der}}) \otimes W(k))$ surjects onto the kernel of $H^2(\Gamma_{S\cup Q}, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) \rightarrow \oplus_{v\in S\cup Q} H^2(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k))$, we are done with the first part.

For the second part, by Tate duality it suffices to show that $H^0(\Gamma_v, \rho_{Q\cup S}^{Q-new}(g^{\text{der}}) \otimes W(k)) = 0$ for all $v \in Q$. This follows from the fact that $\rho_{Q\cup S}^{Q-new}$ is ramified for all $v \in Q$, and by choice the primes in $Q$ are nice for $\tilde{\rho}$, so in particular:

- $\text{Norm}(q)$ is not $1$ mod $p$;
- there is a unique root $\alpha$ of $\Phi(G,T)$, with $T$ the identity component of the centralizer of $\tilde{\rho}(\text{Frob}_q)$ in $G$ (assumed to be a maximal split torus of $G$), such that $\Gamma_q$ acts on $g_{\alpha}$ (the corresponding root space) by $k^{-1}$.

The third part follows directly from the first two parts.

4. Level lowering mod $p^n$ (via Theorem 2.16) and modularity lifting

Using Theorem 2.16 applied to odd irreducible representations $\tilde{\rho} : \Gamma_{Q} \to GL_2(k)$ we sketch a different proof of modularity lifting along the lines of §4 of [Kha03].

We recall the situation of loc. cit and how when combined with the work in this paper one gets a different approach to automorphy lifting. We consider a semistable $\tilde{\rho} : G_Q \to GL_2(k)$ with a $k$ a finite field of characteristic $p > 3$, that arises from a newform $f \in S_2(\Gamma_0(N(\tilde{\rho}))$ with $\delta = 0,1$ according to whether $\rho$ is finite flat at $p$ or not. We assume that the minimal Selmer group for $\tilde{\rho}$ is non-zero (as otherwise we have an easy $R = \mathbb{T}$ theorem in the minimal case).

Consider a finite set of primes $Q = \{q_1, \ldots, q_k\}$ such that $q_i$ is not $\pm 1$ mod $p$ and prime to $N(\tilde{\rho})p$, that are special for $\tilde{\rho}$, i.e $\tilde{\rho}(\text{Frob}_{q_i})$ has eigenvalues with ratio $q_i$. As in [Kha03] we define rings $R_Q^{Q-new}$ that parametrize semistable deformations of $\tilde{\rho}$ that have (in particular) determinant the $p$-adic cyclotomic character, unramified outside the primes that divide $N(\tilde{\rho})p$ and primes in $Q$, finite flat at $p$ if $\tilde{\rho}$ is finite flat at $p$, and Steinberg at $Q$. 


Now we define the related Hecke rings like $\mathbb{T}_Q^{\alpha \cup \beta \text{-new}}$. For a subset $\alpha$ of $Q$ consider the module $H^1(X_0(N(\bar{\rho})^\delta Q), W(k))^{\alpha \text{-new}}$ which is defined as the maximal torsion-free quotient of the quotient of $H^1(X_0(N(\bar{\rho})^\delta Q), W(k))$ by the $W(k)$-submodule spanned by the images of $H^1(X_0(N(\bar{\rho})^\delta Q), W(k))^2$ in $H^1(X_0(N(\bar{\rho})^\delta Q), W(k))$, as $q$ runs through the primes of $\alpha$, under the standard degeneracy maps (here and below for a finite set of primes $Q$ we abusively denote by $Q$ again the product of the primes in it).

We consider the standard action of Hecke operators $T_r$ for all primes $T_r$ (note that we are using $T_r$ for operators that normally get called $U_r$). By [DT94] there is a maximal ideal $m$ of the $W(k)$-algebra generated by the action of these $T_r$'s such that $T_r - \alpha_r \in m$ for $\alpha_r$ a lift to $W(k)$ of the trace of $\bar{\rho}(\text{Frob}_r)$ and $(r, N(\bar{\rho})^\delta Q) = 1$, and $T_r - \bar{\alpha}_r \in m$ for $r | N(\bar{\rho})^\delta Q$, where $\alpha_r$ is the unique root of the characteristic polynomial of $\bar{\rho}(\text{Frob}_r)$ congruent to $\pm 1$ when $r | Q$, it is the scalar by which (the arithmetic Frobenius) Frobenius acts on the unramified quotient of $\bar{\rho}(\text{Frob}_r)$ when $r | N(\bar{\rho})^\delta Q$ and $p$ is ordinary for $\bar{\rho}$ if $r = p$ (if $r = p$ and $\bar{\rho}$ is not ordinary at $p$ we take $\alpha_r$ to be 0), and $\bar{\alpha}_r$ is any lift of $\alpha_r$ to $W(k)$. Then we define $\mathbb{T}_Q^{\alpha \text{-new}}$ to be the localisation at $m$ of the $W(k)$-algebra generated by the action of these Hecke operators on the finite flat $W(k)$-module $H^1(X_0(N(\bar{\rho})^\delta Q), W(k))^{\alpha \text{-new}}$. An analog of Lemma 1 gives that we have natural surjective maps $R_Q^{\alpha \text{-new}} \rightarrow \mathbb{T}_Q^{\alpha \text{-new}}$ (where we take care of the fact that all $T_r$'s are in the image, including $r | N(\bar{\rho})^\delta Q$, as in Section 2 of [W] relying on results of [Ca1]).

We need properties of $\mathbb{T}_Q^{\alpha \text{-new}}$ that are accessible (see [Hel07] and [DT94]) by exploiting another description of these algebras that we recall for orienting the reader (although we do not make explicit use of the alternative descriptions in this sketch). For this fix a subset $\beta$ of the prime divisors of $N(\bar{\rho})^\delta$. Denote by $B_{\alpha, \beta}$ the quaternion algebra over $Q$ ramified at the primes in $\alpha \cup \beta$ and further at $\infty$ if the cardinality $n' = |\alpha \cup \beta|$ is odd. Denote by $A$ the adeles over $Q$. For the standard open compact subgroup $U_{\alpha, \beta} := U_0(N(\bar{\rho})^\delta Q_{\alpha^{-1}})^{-1}$ of the $A$-valued points of the algebraic group $G_{\alpha, \beta}$ (over $Q$) corresponding to $B_{\alpha, \beta}$, $G_{\alpha, \beta}(A)$, we consider the coset space $X_{U_{\alpha, \beta}} = G_{\alpha, \beta}(Q) \backslash G_{\alpha, \beta}(A)/U_{\alpha, \beta}$. Depending on whether $n'$ is odd or even, this double coset space either is merely a finite set of points, or can be given the structure of a Riemann surface (that is compact if $n' \neq 0$ and can be compactified by adding finitely many points if $n' = 0$). If $n'$ is odd we consider the space of functions $S_{U_{\alpha, \beta}} := \{f : X_{U_{\alpha, \beta}} \rightarrow W(k)\}$ modulo the functions which factorise through the norm map, and in the case of $n'$ even we consider the first cohomology of the corresponding Riemann surface $X_{U_{\alpha, \beta}}$, i.e., $S_{U_{\alpha, \beta}} := H^1(X_{U_{\alpha, \beta}}, W(k))$. These $W(k)$-modules have the standard action of Hecke operators $T_r$ (see Sections 2 and 3 of [DT1]). By the results of [DT] and the Jacquet–Langlands correspondence there is a maximal ideal that we denote by $m$ again in the support of the $W(k)$-algebra generated by the action of the $T_r$'s on $S_{U_{\alpha, \beta}}$ characterised as before. We denote the localisation at $m$ of this Hecke algebra by $\mathbb{T}_Q^{\alpha \cup \beta \text{-new}}$. Then by the Jacquet–Langlands correspondence, which gives an isomorphism $\mathbb{T}_Q^{\alpha \cup \beta \text{-new}} \otimes Q_p \cong \mathbb{T}_Q^{\alpha \text{-new}} \otimes Q_p$ that takes $T_r$ to $T_r$, and the freeness of $\mathbb{T}_Q^{\alpha \cup \beta \text{-new}}$ and $\mathbb{T}_Q^{\alpha \text{-new}}$ as $W(k)$-modules (which for the former is a standard consequence of $m$ being non-Eisenstein), we have $\mathbb{T}_Q^{\alpha \cup \beta \text{-new}} \cong \mathbb{T}_Q^{\alpha \text{-new}}$, an isomorphism of local $W(k)$-algebras. We consider an auxiliary set $Q = \{q_1, \cdots, q_n\}$ as in Theorem 1.4 (see also Example 2.18) such that $R_Q^{\alpha \text{-new}} \cong \mathbb{T}_Q^{\alpha \text{-new}} \cong W(k)$.

**Theorem 4.1.** Let $\bar{\rho} : \Gamma_Q \rightarrow GL_2(\mathbb{F}_p)$ be an odd, semistable, irreducible modular mod $p > 3$ surjective representation that arises from $S_2(\Gamma_0(N(\bar{\rho})^\delta)).$ Assume that the minimal dual Selmer for $\bar{\rho}$ is not zero. Then there is a finite set of primes $Q = \{q_1, \cdots, q_r\}$ that are special for $\bar{\rho}$ such that:
• \( R_{Q_i}^{Q_i-\text{new}} = W(k) \) and \( R_{Q_i}^{Q_i-\text{new}} = T_{Q_i}^{Q_i-\text{new}} \), and the corresponding Galois representation \( \rho_{Q_i}^{Q_i-\text{new}} : \Gamma_Q \to GL_2(W(k)) \), has the following properties:
  • \( \rho_{Q_i}^{Q_i-\text{new}}(\tau_q) \), for \( \tau_q \) a generator of the \( \mathbb{Z}_p \)-quotient of the inertia group \( I_q \) at \( q \), is of the form \( \begin{pmatrix} 1 & p^n \\ 0 & 1 \end{pmatrix} \), for all \( q \in Q \) for an integer \( n \geq 2 \);
  • For each \( 1 \leq i \leq r \), there is a subset \( Q_i \) of \( Q \) that omits \( q_i \) and contains \( \{q_1, \ldots, q_{i-1}\} \), such that \( R_{Q_i}^{Q_i-\text{new}} = T_{Q_i}^{Q_i-\text{new}} = W(k) \) and \( \rho_{Q_i}^{Q_i-\text{new}} \) is congruent modulo \( p^n \) to \( \rho_{Q_i}^{Q_i-\text{new}} \).

If the minimal dual Selmer for \( \bar{\rho} \) is zero, then as there is a minimal modular lift of \( \bar{\rho} \), we have an automorphy lifting theorem in the minimal case. Thus the non-vanishing of the minimal dual Selmer is not too burdensome an assumption.

**Proof.** The assertions related to the set of primes \( Q \) and subsets \( Q_i \) with \( R_{Q_i}^{Q_i-\text{new}}, R_{Q_i}^{Q_i-\text{new}} = W(k) \) and the congruences between \( \rho_{Q_i}^{Q_i-\text{new}} \) and \( \rho_{Q_i}^{Q_i-\text{new}} \) follow from Theorem 2.16 and its specialisation Theorem 4.1. The assertions that \( R_{Q_i}^{Q_i-\text{new}} = T_{Q_i}^{Q_i-\text{new}} \) follow from this upon using the level raising results of [DT94].

We sketch the proof of the result below to go from restricted modularity lifting theorems to more general ones: we are reproving known results by a new method which exploits the independent level lowering congruences our work produces in Theorem 4.1.

**Corollary 4.2.** Keeping the notation above, we deduce an isomorphism \( R_Q = T_Q \).

**Proof.** The argument is very similar to loc. cit. and the main ingredients are:

– Wiles’s numerical isomorphism criterion
– Level raising results of Diamond and Taylor in [DT94]
– Quantitative level lowering as in Theorem 4.1
– Gorenstein properties of Hecke algebras arising from Shimura curves (results of [Hel07]; we may invoke these as for \( q \in Q \), \( q \) is not 1 mod \( p \)).

In loc. cit. we used an idea of level substitution mod \( p^n \) to deduce an \( R_Q = T_Q \) theorem from \( R_{Q_i}^{Q_i-\text{new}} = T_{Q_i}^{Q_i-\text{new}} \). Here we use use Theorem 4.1 instead of the the level substitution step in [Kha03].

Using Theorem 4.1, we have augmentations \( \pi : T_Q \to T_{Q}^{Q-\text{new}} = W(k) \), \( \pi' : T_Q \to T_{Q}^{Q-\text{new}} = W(k) \) such that \( \pi \) and \( \pi' \) are congruent mod \( p^n \) and \( \pi' \) does not factor through \( T_{Q}^{Q-\text{new}} \). Further it is known (see Section 8 of [Hel07] and note that we are assuming our primes \( q \) are not 1 mod \( p \)) the Hecke algebra \( T_{Q}^{Q-\text{new}} \) is Gorenstein.

We claim that the ideal \( (\pi(\text{Ann}_{T_{Q_i}^{Q_i-\text{new}}} (\ker(\pi)))) \) of \( W(k) \) is contained in \( p^n(\langle \pi(\text{Ann}_{T_{Q_i}^{Q_i-\text{new}}} (\ker(\pi)))) = (p^n) \).

To prove the claim the two ingredients are the morphism \( \pi' : T_{Q}^{Q-\text{new}} \to W(k) \) which does not factor through \( T_{Q}^{Q-\text{new}} \) by construction, and the fact that these Hecke algebras are Gorenstein. For ease of notation set \( \mathbf{T}' = T_{Q}^{Q-\text{new}} \) and \( \mathbf{T} = T_{Q}^{Q-\text{new}} \) and denote the natural map \( \mathbf{T}' \to \mathbf{T} \) by \( \beta \).

We justifying the claim using these 2 ingredients as in loc. cit. (see also Lemma 5.10), an argument that is due to the referee of [Kha03]. Because \( \mathbf{T} \) and \( \mathbf{T}' \) Gorenstein, we have that

\[
\pi' \beta(\text{Ann}_{\mathbf{T}'} (\ker(\pi' \beta))) = \pi' \beta(\text{Ann}_{\mathbf{T}'} (\ker(\beta))) \pi(\text{Ann}_{\mathbf{T}} (\ker(\pi)))
\]
as ideals of $W(k)$. Choose $a \in \ker(\beta)$ such that $\pi'(x) \neq 0$. Consider $y \in \Ann_R(\ker(\beta))$. Then as $xy = 0$ this implies $\pi'(xy) = 0$, which implies $\pi'(y) = 0$, which implies $\pi(\pi(y)) = \pi(0)$ as $\pi'$ and $\pi$ are congruent mod $p^n$ which proves the claim.

This combined with the injection of the cotangent space at (the pull-back) $\pi : R_{Q,new}^Q$ into $W(k)/p^nW(k)$ (see Lemma 3.3 or Proposition 2 of [Kha03]), and the Wiles numerical criterion gives an isomorphism $R_{Q,new}^Q = T_{Q,new}^Q$. Iterating the argument yields that $R_Q = T_Q$.

□

5. Appendix: Wiles numerical isomorphism criterion

Wiles in his work on the modularity of elliptic curves [Wil95] proved a numerical criterion for a complete Noetherian local $\mathcal{O}$-algebra $A$ which is:

- finite flat over $\mathcal{O}$,
- and with an augmentation $\pi_A : A \to \mathcal{O}$ with $\Phi_A := (\Ker(\pi_A))^{2}$ a finite abelian group

to be a complete intersection of dimension 1. Here $\mathcal{O}$ is a discrete valuation ring that is finite over $\mathbb{Z}_p$. He used this criterion to deduce that isomorphisms of deformation rings and Hecke algebras at minimal level also imply such isomorphisms at non-minimal levels.

We generalize in [5.1] the Wiles criterion, which was later refined by Lenstra [Len95], for rings $A$ that we do not assume are finite over $\mathcal{O}$, but assume have depth at least one (weaker than assuming $A$ is flat over $\mathcal{O}$). Our results, Propositions 5.1 and 5.6 are refinements of a theorem that is due to Wiles and Lenstra [DDT97 Theorem 5.27]. The proof of Proposition 5.1 is easily deduced from the work of Wiebe [Wie69] and that of Proposition 5.6 is a variant of arguments of Wiles and Lenstra.

Our motivation was to find a sufficient criterion given $(A, \pi_A)$ with $\Phi_A$ finite, for $A$ being of dimension one. Taking a cue from the Wiles–Lenstra criterion, we guessed this should be implied by the numerical equality $#\Phi_A = #\mathcal{O}/\eta_A$, with $\eta_A = \pi_A(\Ann(\Ker(\pi_A)))$. Proposition 5.1 verifies that the numerical equality implies $A$ is a complete intersection of dimension 1 if and only if $A$ is of depth one. We raise the question (without assuming that $A$ is of depth one) whether just the numerical equality implies that $A$ is of dimension 1.

5.1. A refinement of Wiles’s numerical isomorphism criterion. All rings will be commutative, Noetherian and also local and complete. Some of the statements make sense without the completeness condition but they can be immediately reduced to the complete case.

We try to follow as much as possible the notations of [DDT97]. So $\mathcal{O}$ will always be a discrete valuation ring but we do not usually assume that it is a finite extension of $\mathbb{Z}_p$ or that the rings being considered are $\mathcal{O}$-algebras.

For a complete local ring $(A, m_A)$ as above we consider a surjection $\pi_A : A \to \mathcal{O}$ such that $\Phi_A := \Ker(\pi_A)/\Ker(\pi_A)^2$ is of finite length. It follows, as in [DDT97 Section 5.2], that for $\eta_A := \pi_A(\Ann(\Ker(\pi_A)))$ we have that $\mathcal{O}/\eta_A$ is also of finite length and

\begin{equation}
\ell(\Phi_A) \geq \ell(\mathcal{O}/\eta_A).
\end{equation}

Hereafter, we will refer to the data $\pi_A : A \to \mathcal{O}$ as above simply as an augmented ring.

Our first goal is to prove the following generalisation of the Wiles–Lenstra criterion for complete intersections.

Proposition 5.1. Let $\pi_A : A \to \mathcal{O}$ be an augmented ring with $\text{depth}(A) \geq 1$. Then $A$ is a complete intersection ring iff $\ell(\Phi_A) = \ell(\mathcal{O}/\eta_A)$. 

The main improvement over the original result of Wiles, as extended by Lenstra, is that we have no other finiteness assumption on $A$. The condition on the depth is implied by the finite free condition in the setup of Wiles.

**Proof.** We first prove the forward direction:

For an ideal $I$ in a ring $R$, we denote by $\text{Fitt}(I)$ the zeroth Fitting ideal of $I$ and recall that $\text{Fitt}(I) \subseteq \text{Ann}(I)$. Therefore $\text{Fitt}(\text{Ker}(\pi_A)) \subseteq \text{Ann}(\text{Ker}(\pi_A))$. The equality $\ell(\Phi_A) = \ell(\mathcal{O}/\eta_A)$ implies that $\pi_A(\text{Fitt}(\text{Ker}(\pi_A))) = \pi_A(\text{Ann}(\text{Ker}(\pi_A)))$. Since the depth of $A$ is at least one, $\text{Ann}(\text{Ker}(\pi_A)) \cap \text{Ker}(\pi_A) = \{0\}$, so $\pi_A$ is injective when restricted to $\text{Ann}(\text{Ker}(\pi_A))$. It follows that $\text{Fitt}(\text{Ker}(\pi_A)) = \text{Ann}(\text{Ker}(\pi_A))$.

The set of zero-divisors in any ring is the union of the finite set of associated primes. Since the maximal ideal of $A$ is not an associated prime, it follows from the “prime avoidance lemma” ([BH93 Lemma 1.2.2]) that there exists a non-zero divisor $x \in A$ such that $\pi_A(x)$ is a uniformizer of $\mathcal{O}$; equivalently, $x$ and $\text{Ker}(\pi_A)$ generate $m_A$. Let $\overline{A} := A/(x)$ and let $p : A \to \overline{A}$ be the quotient map. By construction, we have that $p(\text{Ker}(\pi_A)) = m_{\overline{A}}$ and so $p(\text{Ann}(\text{Ker}(\pi_A))) \subseteq \text{Ann}(m_{\overline{A}})$.

Let $y$ be any element of $\text{Ann}(\text{Ker}(\pi_A))$ with $\pi_A(y)$ a generator of $\eta_A$. If $p(y) = 0$, then there exists $a \in A$ so that $y = ax$. For any $b \in \text{Ker}(\pi_A)$, we have $by = abx = 0$. Since $x$ is a non-zero divisor, we must have $ab = 0$ and so $a \in \text{Ann}(\text{Ker}(\pi_A))$. But since $y = ax$ and $\pi_A(x)$ is not a unit, this is a contradiction. Thus, $p(\text{Ann}(\text{Ker}(\pi_A))) \neq \{0\}$ and so $\text{Fitt}(m_{\overline{A}}) \neq 0$. It then follows from a theorem of Wiebe ([Wie69 Satz 3], [BH93 Theorem 2.3.16]) that $\overline{A}$ is a zero dimensional complete intersection ring and so, since $x$ is a non-zero divisor, that $A$ is also a complete intersection ring (of dimension one).

The converse direction is an easy consequence of a result of Tate as in [Wie69 Satz 2]: this shows that $\text{Fitt}(\text{Ker}(\pi_A)) = \text{Ann}(\text{Ker}(\pi_A))$ and so the desire equality follows by applying $\pi_A$. Moreover, since $A$ is a one dimensional complete intersection, its depth is equal to one.

We note that de Smit and Schoof [ders97] have also used Wiebe’s theorem to give a generalisation of the the Wiles–Lenstra criterion, but in a different direction.

The depth condition in Proposition 5.1 is essential: if $A$ is a complete intersection and $I \subseteq (\text{Ker}(\pi_A))^n$ is any ideal, then the equality of lengths continues to hold for $A/I$ (with its induced augmentation) if $n \gg 0$ (cf. [ddt97 Remark 5.2.5]). However, all examples that we know of are of dimension one. We are thus led to ask:

**Question 5.2.** Let $\pi_A : A \to \mathcal{O}$ be an augmented ring. If $\ell(\Phi_A)$ is finite and equal to $\ell(\mathcal{O}/\eta_A)$, then is $A$ one dimensional?

We say that an augmented ring $(A, \pi_A)$ is well presented if $A \simeq \mathcal{O}[[X_1, \cdots, X_r]]/(f_1, \cdots, f_r)$. An answer to the following related question would also be relevant in applications:

**Question 5.3.** Let $\pi_A : A \to \mathcal{O}$ be an augmented ring that is well-presented. If $\ell(\Phi_A)$ is finite and equal to $\ell(\mathcal{O}/\eta_A)$, then is $A$ a complete intersection of dimension one?

A stronger version of Question 5.2, suggested by some computer calculations, is

**Question 5.4.** Let $\pi_A : A \to \mathcal{O}$ be an augmented ring. Is it always true that $\ell(\Phi_A) \geq \ell(\mathcal{O}/\eta_A) + \dim(A) - 1$?

Here is a modest result in support of an affirmative answer to the question above.

**Lemma 5.5.** Let $\pi_A : A \to \mathcal{O}$ be an augmented ring of dimension $d$. If $A$ is a quotient of a regular local ring $R$ with $\dim(R) = d + 1$, then $\ell(\Phi_A) \geq \ell(\mathcal{O}/\eta_A) + d - 1$. 
Proof. We just sketch the proof since we do not use it later.

If \( \dim(A) = 1 \), there is nothing to prove so we may assume that \( \dim(A) > 1 \). Choose a surjection \( p : R \to A \) as in the statement of the lemma and let \( f_1, \ldots, f_r \) be generators of \( J = \ker(p) \). Let \( D \subset \text{Spec}(A) \) be an irreducible component with \( \dim(D) = \dim(A) \). Since \( R \) is a UFD, \( D \) is the zero set of an element irreducible element \( g \in m_R \) and we have for all \( i \), \( f_i = g f'_i \) for some \( f'_i \) in \( m_R \).

Let \( J' = (f'_1, \ldots, f'_r) \) and set \( A' = R/J' \). Since \( g \notin K := \ker(p) \circ p, f'_i \in K \) for all \( i \), so we have a factorisation of \( \pi_A \) through a map \( \pi_{A'} : A' \to O \).

By construction, we have \( J = gJ' \). This implies that \( (J : K) = (J' : K) \) and so

\[
\pi_A(\text{Ann}(\ker(\pi_A))) = \pi_A \circ p(g) \pi_{A'}(\text{Ann}(\ker(\pi_{A'})))
\]

On the other hand, we have

\[
\pi_A(\text{Fitt}(\ker(\pi_A))) = \pi_A \circ p(g^d) \pi_{A'}(\text{Fitt}(\ker(\pi_{A'})))
\]

since \( K \) is generated by a subset of a regular system of parameters of \( R \) of size \( d \). We conclude using the trivial inequality \( \ell(\Phi_A) \geq \ell(O/\eta_A) \) and the fact that \( \pi_A \circ p(g) \) is not a unit in \( O \). \( \square \)

5.2. The isomorphism criterion of Wiles–Lenstra [DDT97, Theorem 5.28] can also be extended to our setting.

**Proposition 5.6.** Let \( \phi : A \to B \) be a map of augmented rings with \( B \) of depth one. If \( \ell(\Phi_A) \leq \ell(O/\eta_B) < \infty \) then the map is an isomorphism and the rings are complete intersections.

**Proof.** The standard inequalities imply that

\[
\ell(\Phi_A) = \ell(\Phi_B) = \ell(O/\eta_B) = \ell(O/\eta_B)
\]

so it follows from Proposition 5.1 that \( B \) is a complete intersection. Let \( x \in B \) be a non-zero divisor mapping to a uniformizer of \( O \) and let \( x' \) be any element of \( A \) lifting \( x \). We conclude that \( A/x' \) is also a zero dimensional complete intersection, so \( A \) is one dimensional.

Now by applying Lemma 5.7 we choose a complete intersection augmented ring \( \tilde{A} \) with a surjective map to \( A \) inducing an isomorphism \( \Phi_A \to \Phi_A \). Since

\[
\ell(\Phi_A) = \ell(\Phi_{\tilde{A}}) \geq \ell(O/\eta_{\tilde{A}}) \geq \ell(O/\eta_B) = \ell(\Phi_B),
\]

we deduce that \( \ell(O/\eta_{\tilde{A}}) = \ell(O/\eta_B) \). Finally, by applying Lemma 5.8 we deduce that \( \phi \) is an isomorphism. \( \square \)

**Lemma 5.7.** Let \( A \) be a one dimensional augmented ring such that \( \Phi_A \) is of finite length. Then there is a map of augmented rings \( \tilde{A} \to A \) which induces an isomorphism \( \Phi_{\tilde{A}} \to \Phi_A \) and such that \( \tilde{A} \) is a complete intersection.

This is the version of [DDT97, Theorem 5.26] that we shall need.

**Proof.** Let \( R \) be a regular local ring of dimension \( d + 1 \) with a surjection \( \psi : R \to A \). We view \( R \) as an augmented ring via the map \( \pi_R := \pi_A \circ \psi \). Since \( O \) is a dvr, \( \ker(\pi_A) \) is generated by \( n \) elements, so \( \Phi_R \) is a free \( O \)-module of rank \( d \). Therefore, the kernel \( K \) of the map \( \Phi_R \to \Phi_A \) is also generated by \( n \) elements. We let \( f_1, \ldots, f_d \) be elements in \( I := \ker(\psi) \) whose images in \( \Phi_R \) generate \( K \); this is possible since \( \psi \) induces a surjection \( (\ker(\Phi_R))^2 \to (\ker(\Phi_A))^2 \).

Let \( f'_i = f_i \). Having chosen \( f'_1, \ldots, f'_d \) in \( I \) for some \( i, 1 \leq i < d \), so that the dimension of \( R_i = R/(f'_1, \ldots, f'_i) \) is \( d + 1 - i \) and such that \( f'_i \equiv f_i \mod(\ker(\pi_R))^2 \), we apply the prime avoidance lemma [BH93, Lemma 1.2.2] to the primes corresponding to the generic points of the
Lemma 5.8. Let \( \phi : A \to B \) be a surjective morphism of augmented rings. If \( A \) is a complete intersection, \( B \) has depth one, and \( \eta_A = \eta_B \neq (0) \), then \( \phi \) is an isomorphism.

This is essentially [DDT97, Theorem 5.24]; the depth condition replaces the flatness condition therein. Also, as in loc. cit. we only need that \( A \) be Gorenstein.

**Proof.** We follow the proof of [DDT97, Theorem 5.24] with appropriate modifications. We first note that since \( \eta_A \neq (0) \) and \( A \) is a complete intersection we have that \( A \) is one dimensional and then since \( B \) is a quotient of \( A \) and is augmented, it is also one dimensional.

As in loc. cit. we see that

\[
\text{Ker}(\pi_A) \cap \text{Ann}_A(\text{Ker}(\pi_A)) = (0)
\]

and similarly for \( B \). Any element in this ideal vanishes at any point of \( \text{Spec}(A) \) which is not the closed point so the depth condition implies that it must be 0.

Continuing as in loc. cit., we get an exact sequence

\[
0 \to \text{Ker}(\phi) \oplus \text{Ann}_A(\text{Ker}(\pi_A)) \to A \to B/(\text{Ann}_B(\text{Ker}(\pi_B))) \to 0
\]

of \( A \)-modules. Furthermore, we have a natural injection

\[
B/(\text{Ann}_B(\text{Ker}(\pi_B))) \to \text{End}_B(\text{Ker}(\pi_B)).
\]

Since \( B \) has depth one, \( \text{Ker}(\pi_B) \) also has depth one since an element of \( B \) which is a non-zero divisor for any \( B \)-module is trivially a non-zero divisor of any submodule. This implies that \( \text{End}_B(\text{Ker}(\pi_B)) \) and so also \( B/(\text{Ann}_B(\text{Ker}(\pi_B))) \) have depth one (use the same element!).

Now we use that \( A \) is Gorenstein, so by Lemma 5.9 we have \( \text{Ext}_A^1(B/(\text{Ann}_B(\text{Ker}(\pi_B))), A) = 0 \). Thus we get a surjection

\[
A \cong \text{Hom}_A(A, A) \to \text{Hom}_A(\text{Ker}(\phi), A) \oplus \text{Hom}_A(\text{Ann}_A(\text{Ker}(\pi_A)), A) \to 0.
\]

Both summands in (5.4) are non-zero—consider the tautological inclusions—if \( \text{Ker}(\phi) \) is non-zero. This leads to a contradiction by tensoring the sequence with \( A/m_A \) and using Nakayama’s lemma as in [DDT97].

\[\square\]

5.3. Annihilators and Gorenstein rings. The statement of Lemma 5.10 below is close to a statement on page 216 of [Kha03] which is due to the referee of that paper.

We first collect some well known facts about Gorenstein local rings.

**Lemma 5.9.** Let \( A \) be a Gorenstein local ring. Then

(1) For any finite \( A \)-module \( M \) with depth \( (M) = \dim(A) \), we have \( \text{Ext}_A^i(M, A) = 0 \) for \( i > 0 \). Consequently, the functor \( M \mapsto M^* := \text{Hom}_A(M, A) \) preserves exact sequences of such modules; moreover, \( (M^*)^* \) is canonically isomorphic to \( M \).

(2) Let \( B \) be a Cohen–Macaulay local ring of the same dimension as \( A \) and \( \phi : A \to B \) a homomorphism which makes \( B \) into a finite \( A \)-module. Then \( B^* \cong B \) as an \( A \)-module iff \( B \) is Gorenstein.

\[\text{In the notation of [BH93] we take } M = R, x_1 = f_{i+1} \text{ and } x_2, \ldots, x_n \text{ to be generators of } I \cap (\text{Ker}(\pi_R))^2.\]
Proof. The first part of (1) follows from [BH93, Corollary 3.5.11] since $A$, being Gorenstein, is a canonical module for itself. The preservation of exact sequences then follows from the vanishing of $\text{Ext}^1$. The isomorphism of $(M^*)^*$ is a consequence of the fact that $A$ (as a complex in degree 0) is a dualising complex for $A$ and then the vanishing of the $\text{Ext}^i$ for $i > 0$ implies that $\text{RHom}_A(M, A) = M^*$.

(2) follows from duality for the finite map $\phi : A$ is Gorenstein we have that $\text{RHom}_A(B, A)$, which is isomorphic to $B^*$ under the depth assumption, is a dualising complex for $B$, so it is isomorphic to $B$ iff $B$ is Gorenstein.

□

In the following lemma, $R$ denotes $\mathcal{O}$ or $\mathcal{O}/\varpi^n$, where $\varpi$ is a uniformizer of $\mathcal{O}$. Note that both these rings are Gorenstein.

Lemma 5.10. Let $A$ be a Gorenstein local ring with a surjection $\pi_A : A \to R$. We assume that $\dim(A) = \dim(R)$ and that $\text{Ann}_A(\text{Ker}(\pi_A))$ is of finite length as an $A$-module. Suppose that $\pi_A$ factors through a surjection $\phi : A \to B$ with $B$ Cohen–Macaulay. Then

$$\phi(\text{Ann}_A(\text{Ker}(\pi_A))) = \phi(\text{Ann}_A(\text{Ker}(\phi))) \text{Ann}_B(\text{Ker}(\pi_B))$$

where $\pi_B : B \to R$ is the induced surjection.

Proof. Since $A$ is a Gorenstein ring of dimension $\leq 1$, $\text{Ker}(\phi)$, being a submodule of $A$, has depth equal to $\text{depth}(A) = \dim(A)$. Thus, applying the functor $\text{Hom}_A(-, A)$ to the exact sequence of $A$-modules

$$0 \to \text{Ker}(\phi) \to A \to B \to 0 \quad (5.5)$$

and using Lemma 5.9 we get an exact sequence

$$0 \to B^* \xrightarrow{\phi^*} A \to K \to 0 \quad (6.6)$$

where $K := \text{Ker}(\phi)^*$. Applying the functor $\text{Hom}_A(R, -)$ to this exact sequence gives rise to an exact sequence

$$0 \to \text{Hom}_A(R, B^*) \to \text{Hom}_A(R, A) \to \text{Hom}_A(R, K) \to \text{Ext}^1_A(R, B^*) \to 0 \quad (5.7)$$

since $\text{Ext}^1_A(R, A) = 0$.

By Lemma 5.9 (1), since $B$ and $R$ both have depth equal to $\text{depth}(A)$, we have $\text{Ext}^1_A(R, B^*) \cong \text{Ext}^1_A(B, R)$. The long exact sequence of $\text{Ext}$ associated to $(5.5)$ gives an exact sequence

$$0 \to \text{Hom}_A(B, R) \to \text{Hom}_A(A, R) \to \text{Hom}_A(\text{Ker}(\phi), R) \xrightarrow{d} \text{Ext}^1(B, R) \to 0$$

since $\text{Ext}^1_A(A, R) = 0$. Since the surjection from $A$ to $R$ factors through $B$, the induced map from $\text{Hom}_A(B, R)$ to $\text{Hom}_A(A, R)$ is an isomorphism. It follows that the map $d$ is an isomorphism.

Now $\text{depth}(K) = \text{depth}(A)$, so duality also gives us an isomorphism $\text{Hom}_A(R, K) \cong \text{Hom}_A(\text{Ker}(\phi), R)$, hence $\text{Hom}_A(R, K) \cong \text{Ext}^1_A(R, B)$. These being finitely generated modules over a noetherian ring, the fourth map in $(5.7)$, being a surjection, must in fact be an isomorphism. It follows that the second map in $(5.7)$ is also an isomorphism.

Now $\text{Hom}_A(R, A) = \text{Ann}_A(\text{Ker}(\pi_A))$ and similarly for $B$. Since $\text{Hom}_A(B, A) = \text{Ann}_A(\text{Ker}(\phi))$ and $\phi^*$ corresponds to a generator of this ideal, we conclude that

$$\phi(\text{Ann}_A(\text{Ker}(\pi_A))) = \phi(\text{Ann}_A(\text{Ker}(\phi))) \text{Ann}_B(\text{Ker}(\pi_B))$$

□
Lemma 5.11. Let $A$ be a Gorenstein local ring with a surjection $\pi_A : A \rightarrow R$. We assume that $\dim(A) = \dim(R)$ and that $\text{Ann}_A(\ker(\pi_A))$ is of finite length as an $A$-module. Assume that $\pi_A$ factors through a surjection $\phi_B : A \rightarrow B$ and let $C$ be the largest quotient of $B$ which is Cohen–Macaulay, so there are surjections $\phi_C : A \rightarrow C$, $\pi_B : B \rightarrow R$ and $\pi_C : C \rightarrow R$. Then

$$\phi_C(\text{Ann}_A(\ker(\pi_A))) = \phi_C(\text{Ann}_A(\ker(\phi_B))) \text{Ann}_C(\ker(\pi_C)).$$

Proof. We may apply Lemma 5.10 to the map $\phi_C$, since $C$ is Cohen–Macaulay, to deduce that

$$\phi_C(\text{Ann}_A(\ker(\pi_A))) = \phi_C(\text{Ann}_A(\ker(\phi_B))) \text{Ann}_C(\ker(\pi_C)),$$

so we need to prove that $\phi_C(\text{Ann}_A(\ker(\phi_B))) = \phi_C(\text{Ann}_A(\ker(\phi_C)))$. If $\dim(R) = 0$ then $B = C$, so we may assume $\dim(R) = 1$. We have $\ker(\phi_B) \subset \ker(\phi_C)$ and the quotient is a finite length $A$-module. It follows that $\text{Ann}_A(\ker(\phi_B))$ is a finite length $A$-module. Since it is a submodule of $A$ and $A$ is Gorenstein with $\dim(A) = 1$, it follows that it is 0. Thus, $\text{Ann}_A(\ker(\phi_B)) = \text{Ann}_A(\ker(\phi_B))$ and so we are done. □

References

[BH93] Winfried Bruns and Jürgen Herzog. Cohen–Macaulay rings, volume 39 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1993.

[BLGGT14] Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor. Potential automorphy and lifting irreducible Galois representations. Duke Math. J., 74(2):253–269, 1994.

[FKP19] Najmuddin Fakhruddin, Chandrashekhar Khare, and Stefan Patrikis. Relative deformation theory and lifting irreducible Galois representations. Duke Math. J., 147(5):1353–1381, 2011.

[Kha03] Chandrashekhar Khare. On isomorphisms between deformation rings and Hecke rings.

[KR03] Chandrashekhar Khare and Ravi Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. Ann. of Math. (2), 154(1):199–222, 2003. With an appendix by Gebhard Böckle.

[Len95] H. W. Lenstra, Jr. Complete intersections and Gorenstein rings. In Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, pages 99–109. Int. Press, Cambridge, MA, 1995.

[Mil06] J. S. Milne. Arithmetic duality theorems. BookSurge, LLC, Charleston, SC, second edition, 2006.

[MMS17] Mohammedzuhair Mullath Mohammed Sheriff. Ramified Lifts of Galois Representations and Dimension of Ordinary Deformation Rings. ProQuest LLC, Ann Arbor, MI, 2017. Thesis (Ph.D.)–University of California, Los Angeles.

[Pat16] Stefan Patrikis. Deformations of Galois representations and exceptional monodromy. Invent. Math., 205(2):269–336, 2016.

[PW11] Robert Pollack and Tom Weston. On anticyclotomic $\mu$-invariants of modular forms. Compos. Math., 147(5):1353–1381, 2011.

[Ram02] Ravi Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. Ann. of Math. (2), 156(1):115–154, 2002.

[Rib84] Kenneth A. Ribet. Congruence relations between modular forms. In Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), pages 503–514. PWN, Warsaw, 1984.
[Rib90] K. A. Ribet. On modular representations of Gal(\overline{\mathbb{Q}}/\mathbb{Q}) arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Sel57] George B. Seligman. Some remarks on classical Lie algebras. *J. Math. Mech.*, 6:549–558, 1957.

[Ste16] Robert Steinberg. *Lectures on Chevalley groups*, volume 66 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2016. Notes prepared by John Faulkner and Robert Wilson, Revised and corrected edition of the 1968 original [MR0466335], With a foreword by Robert R. Snapp.

[Tay03] Richard Taylor. On icosahedral Artin representations. II. *Amer. J. Math.*, 125(3):549–566, 2003.

[Til96] Jacques Tilouine. *Deformations of Galois representations and Hecke algebras*. Published for The Mehta Research Institute of Mathematics and Mathematical Physics, Allahabad; by Narosa Publishing House, New Delhi, 1996.

[Vas03] Adrian Vasiu. Surjectivity criteria for $p$-adic representations. I. *Manuscripta Math.*, 112(3):325–355, 2003.

[Wie69] Hartmut Wiebe. Über homologische Invarianten lokaler Ringe. *Math. Ann.*, 179:257–274, 1969.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat’s last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, USA

Department of Mathematics, Cornell University, Ithaca, USA

*E-mail address*: naf@math.tifr.res.in, shekhar@math.ucla.edu, ravi@math.cornell.edu