A NOTE ON GALOIS REPRESENTATIONS VALUED IN REDUCTIVE GROUPS WITH OPEN IMAGE

SHIANG TANG

Abstract. Let $G$ be a split reductive group with $\dim Z(G) \leq 1$. We show that for any prime $p$ that is large enough relative to $G$, there is a finitely ramified Galois representation $\rho: \Gamma_Q \to G(\mathbb{Z}_p)$ with open image. We also show that for any given integer $e$, if the index of irregularity of $p$ is at most $e$ and if $p$ is large enough relative to $G$ and $e$, then there is a Galois representation $\rho: \Gamma_Q \to G(\mathbb{Z}_p)$ ramified only at $p$ with open image, generalizing a theorem of Ray [7]. The first type of Galois representation is constructed by lifting a suitable Galois representation into $G(\overline{\mathbb{F}}_p)$ using a lifting theorem of Fakhruddin–Khare–Patrikis [4], and the second type of Galois representation is constructed using a variant of the argument in Ray’s work [7].

1. Introduction

Galois representations arise naturally in algebraic number theory, for example, the $p$-adic Tate module of a rational elliptic curve $E$ gives rise to a continuous representation $\rho: \Gamma_Q \to \text{GL}_2(\mathbb{Q}_p)$, where $\Gamma_Q := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Moreover, by a result of Serre, $\rho$ has open-image when $E$ is non-CM. Such a Galois representation is part of the rich theory of geometric Galois representations (in the sense of Fontaine–Mazur). On the other hand, one does not expect Galois representations $\rho: \Gamma_Q \to \text{SL}_2(\mathbb{Q}_p)$ with open image that comes from the cohomology of algebraic varieties or automorphic forms (see, for example [10, Example 1.4]). Thus, for a given reductive algebraic group $G$, it is natural to ask if there is a continuous geometric Galois representation $\rho: \Gamma_Q \to G(\mathbb{Q}_p)$ with open image. Several people have constructed examples of this kind (notably for exceptional algebraic groups), for example, [14] and [15]. On the other hand, for groups like $\text{SL}_2$, it appears to be extremely difficult to disprove the existence of geometric Galois representations with open image. However, if one allows non-geometric Galois representations, a uniform answer can be obtained:

Theorem 1.1 (Theorem 2.7). Let $G$ be a split reductive group with $\dim Z(G) \leq 1$. Assume that $p$ is large enough relative to $G$. Then there is a finitely ramified continuous representation $\rho: \Gamma_Q \to G(\mathbb{Z}_p)$ with open image.

A similar but weaker result has been obtained in [10], where the author proves the existence of Galois representations $\rho: \Gamma_Q \to G(\overline{\mathbb{Q}}_p)$ with Zariski-dense image. Note that for a $p$-adic field $E$, a compact, Zariski-dense subgroup of $G(E)$ needs not to be open, unless $G$ is semisimple and $E = \mathbb{Q}_p$. On the other hand, working with $\mathbb{Q}_p$ (instead of its algebraic closure) imposes a condition on the center of $G$ coming from the structure of $\Gamma_Q$, see Proposition 2.9. We prove

\footnote{E-mail address: shiangtang1989@gmail.com.}

\footnote{This constant can be made effective, see Remark 2.8.}

the above theorem by lifting a suitable mod $p$ Galois representation $\overline{\rho}: \Gamma \to G(\mathbb{F}_p)$ that has no local obstructions using a lifting theorem of Fakhruddin–Khare–Patrikis [4, Theorem 6.21] (and the lifts produced by loc. cit. automatically have open image). Note that we have no control over the ramification loci of the lift $\rho: \Gamma \to G(\mathbb{Z}_p)$ due to the nature of the Ramakrishna style lifting argument in loc. cit. In contrast, the next theorem produces open-image Galois representations that ramify only at $p$, assuming a more restrictive condition on $p$. Let $\Gamma_{Q,p}$ be the Galois group of the maximal extension of $Q$ that is unramified away from $p$.

**Theorem 1.2** (Theorem 3.13). Let $G$ be a split reductive group with $\dim Z(G) \leq 1$. Let $e \geq 0$ and let $p$ be a prime number that is large enough relative to $G$ and $e$ whose index of irregularity is at most $e$. Then there is a continuous representation $\rho: \Gamma_{Q,p} \to G(\mathbb{Z}_p)$ with open image.

This generalizes a theorem of Ray [7], which studies the $GL_n$ case. Following the argument in loc. cit., we lift a mod $p$ Galois representation valued in a maximal torus of $G$ constructed from the mod $p$ cyclotomic character with no global obstructions, which demands certain conditions on the $p$-part of the class group of $Q(\mu_p)$. On the other hand, to ensure that the image of the lift is open, one modifies any $Z/p^2$-lift $\rho_2: \Gamma \to G(\mathbb{Z}/p^2)$ by an appropriate cocycle so that its image satisfies a group-theoretic condition expressed in terms of the Lie algebra $g$ (Lemma 3.8), which guarantees that any $\mathbb{Z}_p$-lift of $\rho_2$ has open image.

A similar result of Cornut and Ray [3] constructs continuous representations $\rho: \Gamma_{Q,p} \to G(\mathbb{Z}_p)$ with open image for simple adjoint groups $G$ and regular primes $p$ using a completely different method, generalizing work of Greenberg [6]. On the other hand, Maire [5] constructs continuous representations $\rho: \Gamma_{Q,\{2,p\}} \to GL_n(\mathbb{Z}_p)$ with open image for every prime $p \geq 3$ (with no regularity condition imposed).

**Remark 1.3.** If the numerators of the Bernoulli numbers are uniformly random modulo odd primes, then the natural density of primes with index of irregularity $r$ should be $e^{-1/2} \frac{1}{2^r}$. In particular, the density of primes with index of irregularity at most $r$ should be at least $1 - e^{-1/2} \frac{1}{2^r}$, which approaches 1 rapidly as $r$ increases.

**Remark 1.4.** Observe that the above theorems imply the existence of open image Galois representations of $\Gamma_F$ for any number field $F$. In fact, if $\rho: \Gamma \to G(\mathbb{Z}_p)$ has open image, then $\rho(\Gamma_F)$, being a closed subgroup of finite index, is open.

**Acknowledgements.** We would like to thank Yves Cornulier, Sean Cotner, and Christian Maire for helpful conversations and comments, and thank the anonymous referee for a careful reading and many comments that have helped us clarify the exposition.

### 1.1. Notation.

Let $G$ be a split connected reductive group with derived subgroup $G^{der}$. Let $g$ (resp. $g^{der}$) be a Lie algebra of $G$ (resp. $G^{der}$). When there is no chance of confusion, we will abuse notation and write $g$ (resp. $g^{der}$) for $g \otimes \mathbb{Z} F_p$ (resp. $g^{der} \otimes \mathbb{Z} F_p$).

Let $F$ be a number field. We write $\chi$ for the $p$-adic cyclotomic character and $\overline{\chi}$ for its mod $p$ reduction. Let $\Gamma_F := \text{Gal}(\overline{F}/F)$ denote the absolute Galois group of $F$. For any finite set
of primes $S$ of $F$, let $\Gamma_{F,S}$ denote $\text{Gal}(F(S)/F)$, where $F(S)$ is the maximal extension of $F$ inside $\overline{F}$ that is unramified outside the primes in $S$.

Given a homomorphism $\rho: \Gamma \to H$ some groups $\Gamma$ and $H$, and an $H$-module $V$, we will write $\rho(V)$ for the associated $\Gamma$-module (we will apply this with $V$ the adjoint representation of an algebraic group).

2. Finitely ramified Galois representations with open image

2.1. Coxeter elements. In this section, we review the notion of Coxeter elements, for more details, see [2, §10.1]. Let $G$ be a split simple, simply-connected group with root system $\Phi = \Phi(G,T)$. Let $\Delta = \{\alpha_1, \ldots, \alpha_r\} \subset \Phi$ be a set of simple roots. We write $W = W(G,T) = N_G(T)/T$ for the Weyl group of $G$. We call an element $w \in W$ a Coxeter element if it is conjugate in $W$ to an element of the form $w_{\alpha_1} \cdots w_{\alpha_r}$, where $w_{\alpha_i}$ is the simple reflection corresponding to $\alpha_i$. There is a unique conjugacy class of Coxeter elements in $W$. Their common order $h$ is called the Coxeter number of $G$.

**Lemma 2.1.** Let $w$ be a Coxeter element. Then there is an element $\tilde{w} \in N_G(T)(\mathbb{Z})$ lifting $w$. Its order $\tilde{h}$ depends only on $G$.

**Proof.** By [12], there is a finite subgroup $T \subset N_G(T)(\mathbb{Z})$ which is isomorphic to the extension of $W(G,T)$ by a subgroup of $T(\mathbb{Z})$. In particular, any element in $W$ lifts to a finite order element in $N_G(T)(\mathbb{Z})$. That the order of $\tilde{w}$ depends only on $G$ follows from [2, Proposition 10.2, (iii)].

**Proposition 2.2.** Let $k$ be a field of characteristic $p$. Assume that $p > 2h - 2$. Let $\Gamma \subset G(k)$ be a subgroup. Assume that

1. $\Gamma \subset N_G(T)(k)$.
2. The image of $\Gamma$ in $W(G,T)$ is the cyclic group generated by a Coxeter element.

Then $\Gamma$ is $G$-irreducible, i.e. $\Gamma$ is not contained in any proper parabolic subgroup of $G(\bar{k})$.

**Proof.** This follows from the proof of [2, Proposition 10.7, (i)].

2.2. Lifting Galois representations. In this section, we assume that $G = G_1 \times \cdots \times G_n$ is a direct product of simple, simply connected groups. For $1 \leq i \leq n$, let $T_i$ be a maximal torus of $G_i$ and let $T = T_1 \times \cdots \times T_n$. For each $i$, let $\tilde{w}_i \in N_{G_i}(T_i)(\mathbb{Z})$ be as in Lemma 2.1. Write $\tilde{h}_i$ for its order.

**Proposition 2.3.** Let $\mathfrak{G} \subset N_G(T)(\mathbb{F}_p)$ be the group generated by $T(\mathbb{F}_p)$ and the elements $\tilde{w}_i$ for $1 \leq i \leq n$. Assume that $p > c(\tilde{h}_1, \ldots, \tilde{h}_n)$ (a constant depending only on $\tilde{h}_i$ for $1 \leq i \leq n$). Then there is a finite Galois extension $M/\mathbb{Q}$ whose Galois group is isomorphic to $\mathfrak{G}$ in which $p$ is unramified.

**Proof.** This is an easy consequence of [10, Theorem 2.5]. Let $\mathfrak{H}$ be the group generated by $\tilde{w}_i$ for $1 \leq i \leq n$, then $\mathfrak{G}$ is a quotient of the semidirect product of $\mathfrak{H}$ and $T(\mathbb{F}_p)$. For each $i$, let $p_i$ be an odd prime for which $p_i \equiv 1 \pmod{\tilde{h}_i}$, and let $K_i$ be the fixed field of the
unique subgroup of $\text{Gal}(\mathbb{Q}(\mu_{p_i})/\mathbb{Q})$ of index $\tilde{h}_i$, and let $K = K_1 \cdots K_n$. Then $\text{Gal}(K/\mathbb{Q}) \cong \prod_i \mathbb{Z}/\tilde{h}_i \cong \mathfrak{g}$ as long as the primes $p_i$ are chosen to be distinct. Let $c(\tilde{h}_1, \cdots, \tilde{h}_n)$ be the smallest possible value of $\max\{p_1, \cdots, p_n\}$. Then loc. cit. implies that if $p$ is unramified in $K$ (in particular, if $p > c(\tilde{h}_1, \cdots, \tilde{h}_n)$), then there is a number field $M$ with claimed properties.

\begin{proof}
First note that the field $\tilde{F}$ in the statement of loc. cit. equals $\mathbb{Q}$ (since $G$ is connected) and $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p - 1$. The first item of loc. cit. holds since the projection of $\mathfrak{g}$ to $G_i(\overline{\mathbb{F}})$ is $G_i$-irreducible by Proposition 2.2. We claim that for all finite primes $v$, there exists a formally smooth deformation condition for $\overline{\rho}|_{\Gamma_v}$. In fact, for $v = p$, $H^2(\Gamma_{\mathbb{Q}_p}, \overline{\rho}(g)) = H^0(\Gamma_{\mathbb{Q}_p}, \overline{\rho}(g)(1)) \subset H^0(\mathcal{I}_{\mathbb{Q}_p}, \overline{\rho}(g)(1)) = 0$, where the first equality follows from local duality, and the last equality follows from the fact that $\overline{\rho}(\mathcal{I}_{\mathbb{Q}_p}) = 1$ (which holds since $p$ is unramified in the fixed field of $\overline{\rho}$). For $v \neq p$, since $\overline{\rho}(\mathcal{I}_{\mathbb{Q}_p}) \subset \mathfrak{g}$ is prime to $p$ (by the construction of $\mathfrak{g}$), we can take the (formally smooth) minimal prime to $p$ deformation condition for $\overline{\rho}|_{\Gamma_v}$ (see [14, §4.4]). Thus, the second item of [4, Theorem 6.21] holds. By loc. cit., $\overline{\rho}$ lifts to a finitely ramified representation $\rho: \Gamma_{\mathbb{Q}} \to \tilde{G}(\mathcal{O})$ whose image contains $\tilde{G}(\mathcal{O})$ for a finite extension $\mathcal{O}$ of $\mathbb{Z}_p$. Lastly, note that we may take $\mathcal{O} = \mathbb{Z}_p$ in our case since a formally smooth deformation condition exists at every finite place, see the third item of [4, Remark 1.3].

\end{proof}

2.3. The general case.

\begin{lemma}
Let $\tilde{G}$ and $G$ be algebraic groups defined over $\mathbb{Q}_p$ and let $\tilde{G} \to G$ be an isogeny. Then the induced map $\tilde{G}(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is open.

\begin{proof}
First note that if $f: X \to Y$ is a submersion of (real or $p$-adic) manifolds, then $f$ is open by the local structure theorem for submersions (see for example, [8, Part II, Ch. III, Section 10]). Moreover, the algebraic and analytic differentials are compatible, so if $X, Y$ are varieties over $\mathbb{Q}_p$ with $\dim X \geq \dim Y$ and if $f: X \to Y$ is a smooth morphism, then the induced map $X(\mathbb{Q}_p) \to Y(\mathbb{Q}_p)$ is a submersion, and hence open. Now if $\tilde{G} \to G$ is an isogeny of algebraic groups defined over $\mathbb{Q}_p$, then it is smooth, so $\tilde{G}(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is open by the above.

\end{proof}

\begin{remark}
It is possible to work out an explicit bound for $p$ in Proposition 2.3. In fact, [13] shows that the least prime congruent to 1 modulo $n$ is at most $2^{\phi(n)+1} - 1$.

Let $\overline{\rho}: \Gamma_{\mathbb{Q}} \to G(\mathbb{F}_p)$ be the mod $p$ Galois representation associated to the extension $M/\mathbb{Q}$ constructed above.

\begin{proposition}
Assume that $p$ is greater than $\max\{2h_i-2|1 \leq i \leq n\}, \max\{\tilde{h}_i|1 \leq i \leq n\}, c(\tilde{h}_1, \cdots, \tilde{h}_n)$, and $c_G$, where $c_G$ is a constant depending only on $G$ in [4, Theorem 6.11]. Then $\overline{\rho}$ lifts to a finitely ramified continuous representation $\rho: \Gamma_{\mathbb{Q}} \to G(\mathbb{Z}_p)$ whose image contains $\tilde{G}(\mathbb{Z}_p)$.

\begin{proof}
We apply [4, Theorem 6.21]. We will check its assumptions and explain why the lift can be chosen to have $\mathbb{Z}_p$-coefficients. First note that the field $\tilde{F}$ in the statement of loc. cit. equals $\mathbb{Q}$ (since $G$ is connected) and $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p - 1$. The first item of loc. cit. holds since the projection of $\mathfrak{g}$ to $G_i(\overline{\mathbb{F}})$ is $G_i$-irreducible by Proposition 2.2. We claim that for all finite primes $v$, there exists a formally smooth deformation condition for $\overline{\rho}|_{\Gamma_v}$. In fact, for $v = p$, $H^2(\Gamma_{\mathbb{Q}_p}, \overline{\rho}(g)) = H^0(\Gamma_{\mathbb{Q}_p}, \overline{\rho}(g)(1)) \subset H^0(\mathcal{I}_{\mathbb{Q}_p}, \overline{\rho}(g)(1)) = 0$, where the first equality follows from local duality, and the last equality follows from the fact that $\overline{\rho}(\mathcal{I}_{\mathbb{Q}_p}) = 1$ (which holds since $p$ is unramified in the fixed field of $\overline{\rho}$). For $v \neq p$, since $\overline{\rho}(\mathcal{I}_{\mathbb{Q}_p}) \subset \mathfrak{g}$ is prime to $p$ (by the construction of $\mathfrak{g}$), we can take the (formally smooth) minimal prime to $p$ deformation condition for $\overline{\rho}|_{\Gamma_v}$ (see [14, §4.4]). Thus, the second item of [4, Theorem 6.21] holds. By loc. cit., $\overline{\rho}$ lifts to a finitely ramified representation $\rho: \Gamma_{\mathbb{Q}} \to \tilde{G}(\mathcal{O})$ whose image contains $\tilde{G}(\mathcal{O})$ for a finite extension $\mathcal{O}$ of $\mathbb{Z}_p$. Lastly, note that we may take $\mathcal{O} = \mathbb{Z}_p$ in our case since a formally smooth deformation condition exists at every finite place, see the third item of [4, Remark 1.3].

\end{proof}

\end{remark}
We thank Sean Cotner for pointing out the above lemma.

**Theorem 2.7.** Let $G$ be a split reductive group with $\dim Z(G) \leq 1$. Assume that $p$ is large enough relative to $G$. Then there is a finitely ramified continuous representation $\rho : \Gamma_Q \to G(Z_p)$ with open image.

**Proof.** First assume that $G$ is semisimple, so there are simple, simply-connected groups $G_1, \ldots, G_n$, equipped with an isogeny $\tilde{G} = G_1 \times \cdots \times G_n \to G$. Construct $\phi : \Gamma_Q \to \tilde{G}(F_p)$ as in the previous section and apply Proposition 2.5, we obtain a finitely ramified representation $\rho : \Gamma_Q \to \tilde{G}(Z_p)$ with open image. Projecting down to $G$, we obtain a Galois representation with open image by Lemma 2.6. If $G$ is reductive with $\dim Z(G) = 1$, there is a canonical isogeny $G^{\text{der}} \times Z(G)^0 \to G$. The above gives an open image Galois representation into $G^{\text{der}}(Z_p)$. On the other hand, the cyclotomic character $\chi : \Gamma_{Q,p} \to G_m(Z_p) = Z(G)^0(Z_p)$ has open image. Thus by Lemma 2.6, their product gives a Galois representation into $G(Z_p)$ with open image.

**Remark 2.8.** The lower bound for $p$ in Theorem 2.7 can be made effective: by its proof, this bound is the maximum of the four constants in Proposition 2.5 associated to the simply-connected cover of $G$. By Remark 2.4, the constant $c(h_1, \ldots, h_n)$ can be bounded by an explicit formula, and by [4, Remark 6.17], the constant $c_G$ can be made effective as well.

**Proposition 2.9.** Let $G$ be a split reductive group. Suppose that there exists a continuous representation $\rho : \Gamma_Q \to G(Z_p)$ with open image. Then $\dim Z(G) \leq 1$.

**Proof.** Let $S(G) = G/G^{\text{der}}$. It is a split torus with $\dim Z(G) = \dim S(G) =: r$. Since $\rho$ has open image, so does $\rho \pmod{G^{\text{der}}} : \Gamma_Q \to S(G)(Z_p) = G_m(Z_p)^r$. In fact, $\text{Im} \rho \cap Z(G)^0(Q_p)$ is an open subgroup of $Z(G)^0(Q_p)$, which maps to an open subgroup of $S(G)^0(Q_p)$ under the canonical isogeny of tori $Z(G)^0 \to S(G)^0$ by Lemma 2.6. Since $Q$ has a unique $Z_p$-extension, this forces $r$ to be at most 1. □

3. Galois representations ramified at one prime with open image

Suppose that $G$ is a split reductive group. Given a continuous representation $\phi : \Gamma_{Q,(p)} \to G(F_p)$. Suppose that $\rho : \Gamma_{Q,(p)} \to G(Z_p)$ is a continuous lift of $\phi$. For $m \geq 1$, set $\rho_m$ to be the mod-$p^m$ reduction of $\rho \pmod{p^m}$.

The following fact is standard, see [11, §3.5]:

**Lemma 3.1.** There is a natural group isomorphism

$$\exp : g \otimes_{F_p} p^m Z/p^{m+1}Z \cong \ker(G(Z/p^{m+1}) \to G(Z/p^m))$$

**Definition 3.2.** For $m \geq 1$, set $\Phi_m(\rho) := \rho_{m+1}(\ker \rho_m) \subset G(Z/p^{m+1})$.

The following lemma follows immediately from the above, we omit the proof.

**Lemma 3.3.** $\Phi_m(\rho)$ may be identified as a submodule of $\phi(g)$: for $g \in \ker \rho_m$, $\rho_{m+1}(g) = \exp(p^m v)$ for a unique $v \in \phi(g)$, and we identify $\rho_{m+1}(g)$ with this $v$. 
Lemma 3.4. With the identification in Lemma 3.3, for \( l, m \geq 1 \), \([\Phi_l(\rho), \Phi_m(\rho)] \subset \Phi_{l+m}(\rho)\), where \([,]\) is the Lie bracket of \( g \).

Proof. Fix a faithful representation \( i: G \hookrightarrow \text{GL}_n\) defined over \( \mathbb{Z} \) for some integer \( n \), which induces a map on the Lie algebras as well. Note that \( i\Phi_m(\rho) = \Phi_m(i\rho) \). It follows that \( i[\Phi_l(\rho), \Phi_m(\rho)] = [i\Phi_l(\rho), i\Phi_m(\rho)] = [\Phi_l(i\rho), \Phi_m(i\rho)] \subset \Phi_{l+m}(i\rho) = i\Phi_{l+m}(\rho) \) where the \( \subset \) in the middle follows from [7, Lemma 2.8]. So \([\Phi_l(\rho), \Phi_m(\rho)] \subset \Phi_{l+m}(\rho)\).

Lemma 3.5. Let \( \rho: \Gamma_{\mathbb{Q},(p)} \to G(\mathbb{Z}_p) \) be a continuous representation lifting \( \overline{\rho} \). Let \( m \geq 1 \) be such that \( \Phi_m(\rho) \) contains \( \overline{\rho}(g^{\text{der}}) \). Then we have

\begin{enumerate}
\item \( \Phi_k(\rho) \) contains \( \overline{\rho}(g^{\text{der}}) \) for \( k \) divisible by \( m \).
\item The image of \( \rho \) contains \( U_m := \ker G^{\text{der}}(\mathbb{Z}_p) \to G^{\text{der}}(\mathbb{Z}_p/p^m) \).
\end{enumerate}

Proof. (1) follows from the identity \([\overline{\rho}(g^{\text{der}}), \overline{\rho}(g^{\text{der}})] = \overline{\rho}(g^{\text{der}})\) and Lemma 3.4. Let \( H \) be the image of \( \rho \). (1) implies that for infinitely many \( k \), \( H \pmod{p^k} \) contains \( U_m \pmod{p^k} \). If moreover, \( k \geq N_1 \), then we can apply the lemma below (with \( P = H \cap U_m \)) to conclude that that \( H \) contains \( U_m \).

Lemma 3.6. Let \( m \) be a positive integer. There is an integer \( N_1 \geq m \) depending only on \( m \) and \( G^{\text{der}} \) such that if \( k \geq N_1 \), any closed subgroup \( P \) of \( U_m \) whose reduction modulo \( p^k \) equals \( \ker G^{\text{der}}(\mathbb{Z}_p/p^k) \to G^{\text{der}}(\mathbb{Z}_p/p^m) \) must in fact equal \( U_m \).

Proof. This is essentially [4, Lemma 6.15], which proves the case when \( m = 1 \). The argument trivially generalizes to arbitrary \( m \).

For the rest of this section, we fix a maximal split torus \( T \) of \( G \). Let \( \Phi = \Phi(G, T) \) be the associated root system. Fix a set of simple roots \( \Delta \subset \Phi \). Let \( \Phi^+ \) denote the corresponding set of positive roots. For any \( \alpha \in \Phi \), write \( \alpha = \sum_{\beta \in \Delta} n_\beta \beta \) and define the height function

\[ \text{ht}(\alpha) := \sum_{\beta \in \Delta} n_\beta. \]

The following proposition is well-known, see [9, Chapter 1].

Proposition 3.7. There exist elements \( H_\alpha \in t = \text{Lie}T \) and \( X_\alpha \in g^{\text{der}} = \text{Lie}G^{\text{der}} \) for \( \alpha \in \Phi \), such that the elements \( H_\alpha \) for \( \alpha \in \Delta \) and \( X_\alpha \) for \( \alpha \in \Phi \) form an integral basis for \( g \) satisfying the relations below:

\begin{itemize}
\item \( [H_\alpha, H_\beta] = 0 \).
\item \( [H_\beta, X_\alpha] = \alpha(H_\beta)X_\alpha \) with \( \alpha(H_\beta) \in \mathbb{Z} \).
\item \( [X_\alpha, X_{-\alpha}] = H_\alpha \), and \( H_\alpha \) is an integral combination of the \( H_\beta \) with \( \beta \in \Delta \).
\item \( [X_\alpha, X_\beta] = N_{\alpha,\beta}X_{\alpha+\beta} \) with \( N_{\alpha,\beta} \in \mathbb{Z} - \{0\} \) if \( \alpha + \beta \in \Phi \).
\item \( [X_\alpha, X_\beta] = 0 \) if \( \alpha + \beta \neq 0 \) and \( \alpha + \beta \notin \Phi \).
\end{itemize}
Such a basis is called a **Chevalley basis**. It is unique up to sign changes and automorphisms. Moreover, the constant $n_{\alpha, \beta} := |N_{\alpha, \beta}|$ can be described purely in terms of the root system $\Phi$.

**Lemma 3.8.** Let $\rho: \Gamma_{\mathbb{Q}(p)} \to G(\mathbb{Z}_p)$ be a continuous representation lifting $\overline{\rho}$. Assume that $p$ is larger than $n_{\alpha, \beta}$ for all $\alpha, \beta \in \Phi$. Assume that $\Phi_4(\rho)$ contains an element $H \in \mathfrak{t} \subset \mathfrak{g}(\mathfrak{g})$ such that $\alpha(H)$ is a nonzero element in $\mathbb{F}_p$ for all $\alpha \in \Phi$. Furthermore, assume that it contains $X_\alpha$ for all $\alpha \in \Phi$ with $\text{ht}(\alpha)$ odd. Then we have

1. $\Phi_4(\rho)$ contains $\overline{\rho}(\mathfrak{g}^{\text{der}})$.
2. The image of $\rho$ in $\mathfrak{u}_4$.

**Proof.** In the course of the proof, we will use Lemma 3.4 several times without reference. Let $\alpha \in \Phi^+$ be a root with $\text{ht}(\alpha) = n$ even. Write $\alpha = \beta + \gamma$ for some $\beta \in \Delta$ and $\gamma \in \Phi^+$. Then $\text{ht}(\beta) = 1$ and $\text{ht}(\gamma) = n - 1$, both are odd. The relation $N_{\beta, \gamma}X_{\beta + \gamma} = [X_\beta, X_\gamma]$ and the assumption on $p$ imply that $X_\alpha = X_{\beta + \gamma} \in \Phi_2(\rho)$. A similar argument gives that $X_\alpha \in \Phi_2(\rho)$ for $\alpha \in \Phi^-$ with even height. Now let $\alpha \in \Phi$ be a root with $\text{ht}(\alpha)$ odd. The relation $[H, X_\alpha] = \alpha(H)X_\alpha$ and the assumption on $H$ imply that $X_\alpha \in \Phi_2(\rho)$.

Since $[\Phi_1(\rho), \Phi_2(\rho)] \subset \Phi_3(\rho)$, the relation $[H, X_\alpha] = \alpha(H)X_\alpha$ implies that $X_\alpha \in \Phi_3(\rho)$ for all $\alpha \in \Phi$. One more iteration of the same kind implies that $X_\alpha \in \Phi_4(\rho)$ for all $\alpha \in \Phi$. That $[\Phi_2(\rho), \Phi_2(\rho)] \subset \Phi_4(\rho)$ and the relation $[X_\alpha, X_{-\alpha}] = H_\alpha$ imply that $H_\alpha \in \Phi_4(\rho)$ for all $\alpha \in \Phi$. Thus, $\Phi_4(\rho)$ contains $\overline{\rho}(\mathfrak{g}^{\text{der}})$. The previous lemma now implies our claims. \qed

Let $\lambda \in X_\ast(T)$ be a cocharacter. We will impose conditions on $\lambda$ later. Let

$$\langle \cdot, \cdot \rangle: X^\ast(T) \times X_\ast(T) \to \text{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$$

denote the canonical pairing. Let $\overline{\rho}: \Gamma_{\mathbb{Q}(p)} \to T(\mathbb{F}_p)$ be $\lambda \circ \overline{\chi}$ (recall that $\overline{\chi}$ is the mod $p$ cyclotomic character).

Let $\mathcal{C}$ denote the mod $p$ class group of $\mathbb{Q}(\mu_p)$, i.e. $\mathcal{C} = \text{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$. It has a natural action of $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and $\mathcal{C}$ decomposes into eigenspaces

$$\mathcal{C} = \bigoplus_{0 \leq i \leq p-2} \mathcal{C}(\overline{\chi}^i)$$

where $\mathcal{C}(\overline{\chi}^i) = \{x \in \mathcal{C} | g \cdot x = \overline{\chi}^i(g)x\}$.

**Definition 3.9.** The index of irregularity $e_p$ of a prime $p$ is the number of eigenspaces $\mathcal{C}(\overline{\chi}^i)$ which are nonzero. If $e_p = 0$, we say $p$ is regular.

**Theorem 3.10.** Let $\lambda$ and $\overline{\rho}$ be as above. Assume that

1. $p$ is larger than $n_{\alpha, \beta}$ for all $\alpha, \beta \in \Phi$.
2. $0 < |\langle \alpha, \lambda \rangle| < p - 1$ for all $\alpha \in \Phi$.
3. $\langle \alpha, \lambda \rangle$ is odd for all $\alpha \in \Delta$.
4. The characters $\overline{\chi}^{\langle \alpha, \lambda \rangle}$ for all $\alpha \in \Phi$ are all distinct and are not equal to $\overline{\chi}$.
5. $\mathcal{C}(\overline{\chi}^{-(\alpha, \lambda)}) = 0$ for all $\alpha \in \Phi$. 


Hence, there exists a sequence that for any root \( \alpha \) with odd height, \( \mathcal{C}(\chi^{(\alpha, \lambda)}) \neq \varnothing \), and the local and global duality theorems. We refer the reader to the first part of the proof of Theorem 3.3 for details (the argument in loc. cit. is for \( \text{GL}_n \) but it trivially generalizes to \( G \)).

Let \( \chi_2 \) be \( \chi \mod p^2 \) and let \( \rho_2 := \lambda \circ \chi_2 \). Let \( \alpha \in \Phi \) be a root with odd height. Then by assumption, \( \langle \alpha, \lambda \rangle \) is odd, and hence \( H^0(\Gamma_{\mathbb{Q}_\infty}, F_p(\chi^{(\alpha, \lambda)})) = 0 \) and \( H^0(\Gamma_{\mathbb{Q}_{(p)}}, F_p(\chi^{(\alpha, \lambda)})) = 0 \). By the previous paragraph, \( H^2(\Gamma_{\mathbb{Q}_{(p)}}, F_p(\chi^{(\alpha, \lambda)})) = 0 \). It follows from the global Euler characteristic formula that \( H^1(\Gamma_{\mathbb{Q}_{(p)}}, F_p(\chi^{(\alpha, \lambda)})) \) is 1-dimensional. Let \( f_\alpha \) be a generator of \( H^1(\Gamma_{\mathbb{Q}_{(p)}}, F_p(\chi^{(\alpha, \lambda)})) \) and let \( F \in H^1(\Gamma_{\mathbb{Q}_{(p)}}, \mathcal{P}(g)) \) be the sum of all \( f_\alpha \) with \( \alpha \) ranging over roots in \( \Phi \) with odd height. Let \( \rho_2 := \exp(pF) \cdot \rho_2 = \exp(pF) \cdot (\lambda \circ \chi_2) \).

As \( H^2(\Gamma_{\mathbb{Q}_{(p)}}, \mathcal{P}(g)) = 0 \), \( \rho_2 \) lifts to a characteristic zero representation \( \rho : \Gamma_{\mathbb{Q}_{(p)}} \to G(\mathbb{Z}_p) \).

We want to show that the image of \( \rho \) contains \( U_4 \). By Lemma 3.8, it suffices to show that \( \Phi_1(\rho) \) contains

- \( X_\alpha \) for all \( \alpha \in \Phi \) with \( \text{ht}(\alpha) \) odd,
- an element \( H \in t \) such that \( \alpha(H) \) is a nonzero element in \( F_p \) for all \( \alpha \in \Phi \).

Since the image of \( \mathcal{P} \) is prime to \( p \), any Galois submodule \( M \) of \( \mathcal{P}(g) \) decomposes into

\[
M = M_1 \oplus \left( \bigoplus_{\alpha \in \Phi} M_{\chi^{(\alpha, \lambda)}} \right)
\]

where \( M_1 \) is the \( \Gamma_{\mathbb{Q}} \)-invariant submodule and \( M_{\chi^{(\alpha, \lambda)}} \) is the \( \chi^{(\alpha, \lambda)} \)-eigenspace. Since the characters \( \chi^{(\alpha, \lambda)} \) for all \( \alpha \in \Phi \) are all distinct and are nontrivial (by assumption), the above decomposition makes sense and \( M_{\chi^{(\alpha, \lambda)}} \) if nonzero, is the 1-dimensional space generated by \( X_\alpha \). Note that as \( H^1(\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}), F_p(\chi^{(\alpha, \lambda)})) = 0 \), it follows from the inflation-restriction sequence that for any root \( \alpha \) with odd height, the restriction of \( f_\alpha \) to \( \Gamma_{\mathbb{Q}(\mu_p)} \) is nonzero. Hence, there exists \( g \in \ker \mathcal{P} \) such that \( f_\alpha(g) \neq 0 \), and so the element \( \rho_2(g) \in \Phi_1(\rho) \) has nonzero \( X_\alpha \)-component. It follows from the above decomposition with \( M = \Phi_1(\rho) \) that \( X_\alpha \in \Phi_1(\rho) \) for all \( \alpha \in \Phi \) with odd height.

Finally, note that the cyclotomic character \( \chi \) induces an isomorphism \( \chi: \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong 1 + p\mathbb{Z}_p \). Let \( \gamma \in \Gamma_{\mathbb{Q}(\mu_p)} \) be chosen such that \( \chi(\gamma) = 1 + p \). Then \( \rho_2(\gamma) = \exp(pF(\gamma)) \cdot \lambda(\chi_2(\gamma)) = \exp(pF(\gamma)) \cdot \lambda(1 + p) \in \Phi_1(\rho) \). Let \( H \in t \subset \mathcal{P}(g) \) be the element such that \( \exp(pH) = \lambda(1 + p) \). Then \( H \in \Phi_1(\rho) \) and for any root \( \alpha, \alpha(H) = \langle \alpha, \lambda \rangle \) is nonzero mod \( p \) by Assumption (2).

Let \( r \) be the rank of \( \Phi \) and let \( \Delta = \{\alpha_1, \ldots, \alpha_r\} \). Let \( c_1, \ldots, c_r \) be positive integers such that \( \tilde{\alpha} = \sum c_i \alpha_i \) is the highest root. Let \( \lambda_1, \ldots, \lambda_r \) be cocharacters such that \( \langle \alpha_i, \lambda_j \rangle = \delta_{ij} \).

**Definition 3.11.** Define an strictly increasing sequence of integers \( N_0, N_1, N_2, N_3, \ldots \) as follows: \( N_0 = 1 \),

\[
N_{k+1} = c_1(N_k^* + 2) + c_2(N_k^* + 4) + \cdots + c_r(N_k^* + 2r)
\]
where \( N^*_k = N_k \) if \( N_k \) is odd, and \( N^*_k = N_k + 1 \) if \( N_k \) is even.

**Corollary 3.12.** Let \( e \geq 0 \) and let \( p \) be a prime number such that

1. \( p \) is larger than \( n_{\alpha, \beta} \) for all \( \alpha, \beta \in \Phi \).
2. \( p > 1 + 2N_{e+1} \).
3. The index of irregularity \( e_p \) is at most \( e \).

Then there is a continuous representation \( \rho : \Gamma_{\mathbb{Q}(p)} \to G(\mathbb{Z}_p) \) whose image contains \( U_4 \).

**Proof.** We only need to show that for any prime \( p \) satisfying the above conditions, there is a cocharacter \( \lambda \) satisfying the assumptions in Theorem 3.10. Let \( A \subset \mathbb{Z}/(p-1) \) be defined by \( n \in A \) if and only if at least one of \( \mathcal{C}(\overline{x}^{p+n}) \) or \( \mathcal{C}(\overline{x}^{p-n}) \) is nonzero. Then since \( e_p \leq e \), we have \( |A| \leq 2e \). It suffices to show that there is a cocharacter \( \lambda \) such that \( \lambda \) satisfies Theorem 3.10, (2)-(4) and \( (\alpha, \lambda) \notin A \) for all \( \alpha \in \Phi^+ \). We may assume that \( e_p = e \geq 1 \) and write the least positive representatives of the elements in \( A \) in ascending order

\[
0 \leq a_1 < \cdots < a_e \leq p - 1 - a_e < \cdots < p - 1 - a_1 \leq p - 1.
\]

We prove by induction that if \( p > 1 + 2N_{e+1} \), then there exists a cocharacter \( \lambda \) such that

- For \( 1 \leq j \leq r \), let \( x_j := \langle \alpha_j, \lambda \rangle \). Then \( x_j > 1 \) is odd and \( x_1, \ldots, x_r \) is an arithmetic progression with a common difference of 2.
- \( S := \{ \langle \alpha, \lambda \rangle | \alpha \in \Phi^+ \} \) falls in between \( a_i \) and \( a_{i+1} \) for some \( 0 \leq i \leq e - 1 \) (set \( a_0 = 0 \)) or in between \( a_e \) and \( p - 1 - a_e \).
- Moreover, \( S \) can be made so that \( \max S < a_e \) unless \( a_i \leq N_i \) for all \( i \) with \( 1 \leq i \leq e \).

Granted this, it clearly implies Theorem 3.10, (2)-(5), and so if we further require \( p \) to be larger than \( n_{\alpha, \beta} \) for all \( \alpha, \beta \in \Phi \), then we obtain a desired lift.

It remains to prove the claim. First suppose that \( e = 1 \) and \( p > 1 + 2N_2 \). If \( a_1 > N_1 = 3c_1 + 5c_2 + \cdots + (2r + 1)c_r \), we take \( \lambda = 3\alpha_1 + 5\alpha_2 + \cdots + (2r + 1)\alpha_r \), then since \( \tilde{\alpha} = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r \) is the highest root, for any \( \alpha \in \Phi^+ \), \( 0 < \langle \alpha, \lambda \rangle \leq \langle \tilde{\alpha}, \lambda \rangle = N_1 < a_1 \).

If \( a_1 \leq N_1 \), we take \( \lambda = (N_1^* + 2)\alpha_1 + \cdots + (N_r^* + 2r)\alpha_r \), then for any \( \alpha \in \Phi^+ \), \( a_1 \leq N_1 < \langle \alpha, \lambda \rangle \leq \langle \tilde{\alpha}, \lambda \rangle = N_2 < p - 1 - N_1 \leq p - 1 - a_1 \), where the second last inequality holds since \( p > 1 + 2N_2 > 1 + N_1 + N_2 \). Thus the claim holds for \( e = 1 \). Assume the claim holds for \( e \), and consider a sequence

\[
(0 \leq a_1 < \cdots < a_e < a_{e+1} \leq p - 1 - a_{e+1} < \cdots < p - 1 - a_{e+1} < p - 1).
\]

Let \( p \) be a prime with \( p > 1 + 2N_{e+2} \). If at least one of the \( a_i \) with \( 1 \leq i \leq e \) is greater than \( N_i \), the induction hypothesis (applied to the sequence with the \( a_{e+1} \) terms removed) implies that there is a cocharacter \( \lambda \) satisfying the properties in the claim with \( \max S < a_e \) and we are done. (Note that without the condition that \( \max S < a_e \), the \( S \) provided by induction could intersect with \( \{ a_{e+1} - p - 1 - a_{e+1} \} \).) If \( a_i \leq N_i \) for all \( 1 \leq i \leq e \) but \( a_{e+1} > N_{e+1} \), we take \( \lambda = (N_{e+1}^* + 2)\lambda_1 + \cdots + (N_r^* + 2r)\lambda_r \), then for any \( \alpha \in \Phi^+ \), \( a_e \leq N_e < \langle \alpha, \lambda \rangle \leq \langle \tilde{\alpha}, \lambda \rangle = N_{e+1} < a_{e+1} \) and we are done. If \( a_i \leq N_i \) for all \( 1 \leq i \leq e+1 \), we take \( \lambda = (N_{e+1}^* + 2)\lambda_1 + \cdots + (N_r^* + 2r)\lambda_r \), then for any \( \alpha \in \Phi^+ \), \( a_{e+1} \leq N_{e+1} < \langle \alpha, \lambda \rangle \leq \langle \tilde{\alpha}, \lambda \rangle = N_{e+2} < p - 1 - N_{e+1} \leq p - 1 - a_{e+1} \).
where the second last inequality holds since $p > 1 + 2N_{e+2} > 1 + N_{e+1} + N_{e+2}$. Thus the claim holds for $e + 1$ in all cases.

Finally, we obtain the following theorem:

**Theorem 3.13.** Let $G$ be a split reductive group with $\dim Z(G) \leq 1$. Let $e \geq 0$ and let $p$ be a prime number such that

1. $p$ is larger than $n_{\alpha,\beta}$ for all $\alpha, \beta \in \Phi$, where $n_{\alpha,\beta}$ is defined in Proposition 3.7.
2. $p > 1 + 2N_{e+1}$, where $N_\bullet$ is defined in Definition 3.11.
3. The index of irregularity $e_p$ is at most $e$, where $e_p$ is defined in Definition 3.9.

Then there is a continuous representation $\rho: \Gamma_{\mathbb{Q},\{p\}} \to G(Z_p)$ with open image.

**Proof.** If $G$ is semisimple, this follows immediately from Corollary 3.12. If $G$ is reductive with $\dim Z(G) = 1$, the same argument as in the proof of Theorem 2.7 gives us the desired representation. \qed

**References**

[1] Buhler, J. P., R. E. Crandall, and R. W. Sompolski. *Irregular primes to one million.* mathematics of computation 59.200 (1992): 717-722.

[2] Boeckle, Gebhard, Michael Harris, Chandrashekhar Khare, and Jack A. Thorne. *G*-local systems on smooth projective curves are potentially automorphic. Acta Mathematica 223, no. 1 (2019): 1-111.

[3] Cornut, Christophe, and Jishnu Ray. *Generators of the pro-$p$ Iwahori and Galois representations.* International Journal of Number Theory 14.01 (2018): 37-53.

[4] Fakhruddin, Najmuddin, Chandrashekhar Khare, and Stefan Patrikis. *Relative deformation theory, relative Selmer groups, and lifting irreducible Galois representations.* Duke Math. J. 170(16): 3505-3599 (1 November 2021).

[5] Maire, Christian. *On Galois representations with large image.* arXiv preprint arXiv:2104.02505 (2021).

[6] Greenberg, Ralph. *Galois representations with open image.* Annales mathématiques du Québec 40.1 (2016): 83-119.

[7] Ray, Anwesh. *Constructing Galois representations ramified at one prime.* Journal of Number Theory 222, 168-180.

[8] Serre, Jean–Pierre. *Lie algebras and Lie groups: 1964 lectures given at Harvard University.* Springer, 2009.

[9] Steinberg, Robert. *Lectures on Chevalley groups.* Notes prepared by John Faulkner and Robert Wilson. ULECT 66, AMS 2016.

[10] Tang, Shiang. *Algebraic monodromy groups of $l$-adic representations of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$.* Algebra Number Theory 13 (2019): 1353-1394.
[11] Tilouine, Jacques. *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. MR 1643682 (99i:11038)

[12] Tits, Jacques. *Normalisateurs de tores I. Groupes de Coxeter étendus*. Journal of algebra 4.1 (1966): 96-116.

[13] Thangadurai, Ravindranathan, and Akshaa Vatwani. *The least prime congruent to one modulo n*. The American Mathematical Monthly 118, no. 8 (2011): 737-742.

[14] Patrikis, Stefan. *Deformations of Galois representations and exceptional monodromy*. Inventiones mathematicae 205.2 (2016): 269-336.

[15] Yun, Zhiwei. *Motives with exceptional Galois groups and the inverse Galois problem*. Inventiones mathematicae 196.2 (2014): 267-337.