Galois Representations Ramified at One Prime and With Suitably Large Image

Anwesh Ray

Abstract. Let \( p \geq 7 \) be a prime and \( n > 1 \) be a natural number. We show that there exist infinitely many Galois representations \( \rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\mathbb{Z}_p) \) which are unramified outside \( \{p, \infty\} \) with large image. More precisely, the Galois representations constructed have image containing the kernel of the mod-\( p^t \) reduction map \( \text{SL}_n(\mathbb{Z}_p) \to \text{SL}_n(\mathbb{Z}/p^t\mathbb{Z}) \), where \( t := 8(n^2 - n)\left(3 + \lceil \log_p(2^n + 1) \rceil \right) + 8 \). The results are proven via a purely Galois theoretic lifting construction. When \( p \equiv 1 \mod 4 \), our results are conditional since in this case, we assume a very weak version of Vandiver’s conjecture.

1. Introduction

Let \( p \) be an odd prime number and \( n > 1 \) be an integer. The inverse Galois problem posits that Galois extensions of \( \mathbb{Q} \) (and other fields of interest) may be constructed so as to realize any finite group. Similarly, it is of natural interest for one to ponder over the existence of Galois representations with large image in a group of the form \( \mathcal{G}(\mathbb{Z}_p) \), where \( \mathcal{G} \) is a smooth reductive group-scheme over \( \mathbb{Z}_p \). We consider the simplest case of natural interest, i.e., that of \( \text{GL}_n \). The study of Galois representations is of central importance in number theory. The case when \( n = 2 \) is special, since in this case, such representations abundantly arise from elliptic curves and modular forms. However, for larger values of \( n \), it is natural to consider higher dimensional motives. For \( n > 2 \), it proves difficult to construct geometric Galois representations whose image contains an open subgroup of \( \text{SL}_n(\mathbb{Z}_p) \). For instance, a Galois representation that arises from the \( p \)-primary torsion in an abelian variety defined over \( \mathbb{Q} \), must respect the Weil pairing, and this restricts the image.

Instead of relying on the study of motives and their associated Galois representations, we resort to purely Galois theoretic methods, and our constructions are based in Galois deformation theory. One hopes to construct large Galois representations with special ramification properties that do not necessarily arise from automorphic forms or motives in algebraic geometry. Let \( E := \mathbb{Q}(\mu_p) \) be the cyclotomic field extension of \( \mathbb{Q} \) generated by the \( p \)-th roots of unity and \( \tilde{E} \) the maximal pro-\( p \) extension of \( E \) which is unramified at all finite primes \( v \) of \( E \) such that \( v \nmid p \). A result of Shafarevich shows that when \( p \) is a regular prime (i.e., \( p \) does not divide the class number of \( E \)), the Galois group \( \text{Gal}(\tilde{E}/E) \) is a free pro-\( p \) group with \( \left(\frac{p + 1}{2}\right) \)-generators. R. Greenberg uses this result to construct Galois representations \( \rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\mathbb{Z}_p) \) that are unramified at all finite primes outside \( \{p\} \), whenever \( p \geq 4\left\lceil \frac{n}{2} \right\rceil + 1 \) is a regular prime (cf. [Gre16, Proposition 1.1]). N. Katz [Kat20] adopts a different approach, and constructs finitely ramified Galois representations with large image in \( \text{GL}_n(\mathbb{Z}_p) \) for \( p \equiv 1 \mod 3 \) and \( p \equiv 1 \mod 4 \).
mod 4 and all \( n \geq 6 \). Such Galois representations are defined over certain cyclotomic fields \( \mathbb{Q}(\mu_N) \) and are constructed via geometric techniques and a beautiful application of the Hilbert irreducibility theorem. Galois representations that are finitely ramified and with big image in more general reductive groups are constructed by S. Tang (cf. [Tan]).

The above mentioned Galois representations are typically ramified at a large number of primes, especially when the dimension of the group \( \mathcal{G} \) is large. Returning to the original result of Greenberg, consider the following refined question [Ray21, Question 1.1].

**Question 1.1.** Let \( p \) be any prime number and \( n > 1 \) be an integer. Does there exist a continuous Galois representation \( \rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{Z}_p) \) with suitably large image? If so, can one control the set of primes at which it may ramify? In particular, can such Galois representations be constructed so as to be unramified at all primes \( \ell \not\in \{p, \infty\} \)?

By having suitably large image, we mean that the image contains an open subgroup of \( \operatorname{SL}_n(\mathbb{Z}_p) \). There are parallels between the above question certain refinements of the inverse Galois problem. For instance, Abhyankar’s conjecture posits the existence of finite Galois extensions of function fields in positive characteristic, with prescribed Galois group and a predetermined set of ramification subject to certain constraints. Such Galois extensions were constructed via the patching method by D. Harbater (cf. [Har94]). We also refer to [HOPS18] and references therein for further details. It does lead us to wonder if there are indeed constraints on the number of primes that may ramify in Galois representations to \( \operatorname{GL}_n(\mathbb{Z}_p) \) with suitably large image.

There has been some recent interest Question 1.1. Let \( \mathbb{Q}_p \) be the maximal algebraic extension of \( \mathbb{Q} \) which is unramified outside \( \{p, \infty\} \), and set \( G_{(p)} := \operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}) \). Let \( \tilde{\chi} \) denote the mod-\( p \) cyclotomic character. We shall let \( \mathcal{C} \) denote the mod-\( p \) class group of the cyclotomic field \( \mathbb{Q}(\mu_p) \). Recall that \( p \) is regular if \( \mathcal{C} = 0 \) and irregular otherwise. Note that \( \mathcal{C} \) is a module over \( \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \), and therefore over \( G_{(p)} \). As a Galois module, \( \mathcal{C} \) decomposes into eigenspaces \( \mathcal{C} = \bigoplus_{i=0}^{p-2} \mathcal{C}(\tilde{\chi}^i) \), where \( \mathcal{C}(\tilde{\chi}^i) := \{ \mathcal{I} \in \mathcal{C} \mid g : \mathcal{I} = \tilde{\chi}^i(g)\mathcal{I} \} \). Note that when \( i \) is even, \( \mathcal{C}(\tilde{\chi}^i) \) arises from the mod-\( p \) class group of \( \mathbb{Q}(\mu_p)^\oplus \), the totally real subfield of \( \mathbb{Q}(\mu_p) \). Vandiver’s conjecture predicts that the mod-\( p \) class group of \( \mathbb{Q}(\mu_p)^\oplus \) is equal to 0, and thus, each even eigenspace of \( \mathcal{C} \) is 0. The index of irregularity \( e(p) \) is the number of integers \( i \) that are in the range \( 0 \leq i \leq p - 2 \) such that \( \mathcal{C}(\tilde{\chi}^i) \neq 0 \). Given \( k > 0 \), let \( \mathcal{U}_k \) denote the kernel of the mod-\( p^k \) reduction map

\[
\operatorname{SL}_n(\mathbb{Z}_p) \to \operatorname{SL}_n(\mathbb{Z}/p^k\mathbb{Z}).
\]

In [Ray21], the author shows that for \( n > 1, p \geq 2^{n+2+2e(p)} \), there are infinitely many Galois representations \( \rho : G_{(p)} \to \operatorname{GL}_n(\mathbb{Z}_p) \) whose image contains \( \mathcal{U}_k \). This shows that Greenberg’s result can be extended to irregular primes as well, provided the prime \( p \) is suitably large. This result has been extended to more general groups by S. Maletto [Mal22] and S. Tang [Tan22]. Subsequently, C. Maire [Mai21] shows that for all odd primes \( p \), there is a Galois representation \( \rho : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{Z}_p) \) with big image, which is unramified outside \( \{2, p, \infty\} \).

### 1.1. Statement of the main result

We now state the main result, which entirely resolves Question 1.1 for all \( n > 1 \) and all primes \( p \geq 7 \). The case \( n = 1 \) is an easy exercise. When \( p \equiv 1 \mod 4 \), we need to assume a weak form of Vandiver’s conjecture, which we briefly explain.
Assumption (Assumption 2.2). There is an odd positive integer \( k \) that lies in the range
\[ 3 \leq k \leq \left( \frac{p-1}{2} \right) \]
such that \( C(\bar{\chi}^{1+k}) = C(\bar{\chi}^{p-k}) = 0. \)

The above assumption is clearly a consequence of Vandiver’s conjecture, which predicts that all even eigenspaces of \( C \) must vanish. In fact, it is easy to see that if the number of non-zero even eigenspaces of \( C \) is strictly less than \( \left[ \frac{p-2}{4} \right] \), then the above assumption is automatically satisfied (cf. Proposition 2.1). Also, for primes \( p \equiv 3 \mod 4 \) such that \( p \geq 7 \), the above assumption is automatically satisfied (cf. Remark 2.3).

Theorem (Theorem 5.5). Let \( p \geq 7 \) be a prime and \( n > 1 \) be a natural number. Suppose that the above assumption holds. Then, there exist infinitely many Galois representations \( \bar{\rho} : \text{Gal}(\bar{Q}/Q) \to \text{GL}_n(Z_p) \) which are unramified outside \( \{ p, \infty \} \) whose image contains \( \beta_t \), where \( t := 8(n^2 - n) \left( 3 + \left\lfloor \log_p(2^n + 1) \right\rfloor \right) + 8. \)

1.2. Method of proof. Let us briefly summarize the construction. We begin with a suitable choice of a residual representation
\[ \bar{\rho} : G_{\{p\}} \to \text{GL}_n(Z/pZ) \]
which is carefully lifted to a characteristic zero representation via a step by step process. This residual representation is a diagonal representation, i.e., a direct sum of 1-dimensional characters, defined in section 2.1. Set \( M := (n^2 - n) \left( 3 + \left\lfloor \log_p(2^n + 1) \right\rfloor \right) + 1 \) and \( N := 2M. \) A diagonal representation
\[ \rho_\beta = \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_{n-1} & \beta_n \\ \end{pmatrix} : G_{\{p\}} \to \text{GL}_n(Z/p^N Z), \]
that lifts \( \bar{\rho} \) is carefully chosen. We set \( \rho_N := \rho_\beta \) and set \( \rho_M \) to denote the mod-\( p^M \) reduction of \( \rho_\beta \). Any other lift \( \rho_\beta' : G_{\{p\}} \to \text{GL}_n(Z/p^M Z) \) of \( \rho_\beta \) may be constructed by twisting \( \rho_N \) by a suitable cohomology class taking values in the adjoint representation \( \text{Ad} \rho_M \) (cf. the discussion following Definition 3.2). We carefully construct a suitable cohomology class \( f \in H^1(G_{\{p\}}, \text{Ad} \rho_M) \) and then set \( \rho_\beta' \) to denote the twist of \( \rho_N \) by \( f \) (cf. (5.4)). This twist has many advantageous properties. Let \( L := \mathbb{Q}(\rho_M) \) be the finite Galois extension of \( \mathbb{Q} \) which is fixed by the kernel of \( \rho_M \). One of the key properties exhibited by \( \rho_\beta' \) is that \( \rho_\beta'(\text{Gal}(\mathbb{Q}_{\{p\}}/L)) \) has suitably large image in
\[ \mathcal{A} := \ker \left( \text{GL}_n(Z/p^M Z) \to \text{GL}_n(Z/p^n Z) \right). \]
It is easy to see that \( \mathcal{A} \) is an abelian group and can be identified with \( n \times n \)-matrices with coefficients in \( Z/p^M Z \). By virtue of being an abelian group, \( \mathcal{A} \) acquires a natural Galois action and is isomorphic to the adjoint representation \( \text{Ad} \rho_M \). Of crucial importance is that this adjoint representation decomposes into a direct sum of a trivial module arising from the diagonal torus, and a direct sum of distinct cyclic Galois-modules. It should be noted that the residual adjoint representation \( \text{Ad} \bar{\rho} \) does not necessarily have this favorable property. The infinitesimal deformation problem associated to \( \bar{\rho} \) is unobstructed,
implies that the lifts of $\rho_N$ exhibits infinitely many lifts to characteristic zero. The twist $\rho'_N$ satisfies a number of key properties, and Proposition 4.5 implies that the lifts of $\rho'_N$ all have image containing a large open subgroup of $\text{SL}_n(\mathbb{Z}_p)$.

1.3. Organization. Including the introduction, the manuscript consists of five sections. In section 2, we introduce notation and prove a number of preliminary results. In this section, we recall the main assumption when $p \equiv 1 \mod 4$ (i.e., Assumption 2.2) and explain why it is significantly weaker than Vandiver’s conjecture. We then introduce the choice of residual representation $\bar{\rho}$, and show that it is unobstructed (cf. Proposition 2.6). Also in this section, we discuss properties of diagonal representations and introduce the notion of admissibility. In section 3, we systematically introduce the deformation theory of Galois representations, and discuss how deformations of a given Galois representation may be twisted by cohomology classes valued in the adjoint module. In section 4, we prove results that allow us to state conditions for the image of a Galois representation to be suitably large in $\text{GL}_n(\mathbb{Z}_p)$. The main criterion proven in this section is Proposition 4.5, which is crucially used in the proof of the main theorem. Finally, in section 5, we give a proof of the main result of the manuscript.

1.4. Acknowledgment. The author is supported by the CRM-Simons postdoctoral fellowship. He thanks the anonymous referee for the helpful report.

2. Preliminaries

This section is preliminary in nature. We introduce some key notation that will aid our constructions in later sections, and prove a few basic yet crucial results. Throughout $p$ will be a fixed prime number and $n > 1$ an integer. We assume throughout that $p \geq 7$. Set $\mathbb{Q}_p$ to denote the field of $p$-adic numbers and $\mathbb{Z}_p := \lim_{\leftarrow m} \mathbb{Z}/p^m\mathbb{Z}$ the ring of $p$-adic integers. Let $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}}_p$) denote the algebraic closure of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$). We let $\mathbb{F}_p$ denote the field with $p$ elements, i.e., $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. At each prime $\ell$, let $\iota_\ell : \mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}_\ell$ be a chosen embedding, and set $G_\ell$ to denote the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q})$. The choice of $\iota_\ell$ corresponds to a choice of a prime that lies above $\ell$, and an inclusion of $G_\ell$ into the absolute Galois group $G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $I_\ell$ be the inertia subgroup of $G_\ell$. Given a unital commutative ring $R$, let $M_n(R)$ consist of all $n \times n$ matrices with entries in $R$. Let $e_{i,j}(R)$ denote the matrix in $M_n(R)$ with 0s in all positions except at $(i, j)$, where the entry is equal to 1. When there is no cause for confusion, we simply write $e_{i,j}$ in place of $e_{i,j}(R)$.

It benefits us to consider quotients of the absolute Galois group $G_\mathbb{Q}$ in which all primes outside a prescribed finite set are unramified. Given a finite set of prime numbers $S$, denote by $\mathbb{Q}_S$ the maximal extension of $\mathbb{Q}$ which is contained in $\overline{\mathbb{Q}}$ in which all primes $\ell \notin S \cup \{\infty\}$ are unramified. Note that the extension $\mathbb{Q}_S$ is necessarily Galois over $\mathbb{Q}$. Set $G_S$ to denote the Galois group $\text{Gal}(\mathbb{Q}_S/\mathbb{Q})$. Given a Galois representation $\rho : G_S \to \text{GL}_n(\cdot)$, let $\rho|_\ell$ denote the restriction of $\rho$ to $G_\ell$. We say that $\rho$ is unramified at $\ell$ if $\rho|_\ell$ is trivial when restricted to $I_\ell$. For each integer $m \geq 1$ let $\mu_{p^m}$ denote the $p^m$-th roots of unity. Let $\chi : G_{\{p\}} \to \mathbb{Z}_p^\times$ be the $p$-adic cyclotomic character and denote by $\bar{\chi}$ (resp. $\chi_m$) the mod-$p$ (resp. mod-$p^m$) reduction of $\chi$. By abuse of notation, when it is clear from the context, we shall simply write $\bar{\chi}$ instead of $\chi_m$. 

i.e., $H^2(G_{\{p\}}, \text{Ad}\bar{\rho}) = 0$ (cf. Proposition 2.6). As a result, it follows (cf. Proposition 4.1) that $\rho_N$ exhibits infinitely many lifts to characteristic zero. The twist $\rho'_N$ satisfies a number of key properties, and Proposition 4.5 implies that the lifts of $\rho'_N$ all have image containing a large open subgroup of $\text{SL}_n(\mathbb{Z}_p)$. 

1.3. Organization. Including the introduction, the manuscript consists of five sections. In section 2, we introduce notation and prove a number of preliminary results. In this section, we recall the main assumption when $p \equiv 1 \mod 4$ (i.e., Assumption 2.2) and explain why it is significantly weaker than Vandiver’s conjecture. We then introduce the choice of residual representation $\bar{\rho}$, and show that it is unobstructed (cf. Proposition 2.6). Also in this section, we discuss properties of diagonal representations and introduce the notion of admissibility. In section 3, we systematically introduce the deformation theory of Galois representations, and discuss how deformations of a given Galois representation may be twisted by cohomology classes valued in the adjoint module. In section 4, we prove results that allow us to state conditions for the image of a Galois representation to be suitably large in $\text{GL}_n(\mathbb{Z}_p)$. The main criterion proven in this section is Proposition 4.5, which is crucially used in the proof of the main theorem. Finally, in section 5, we give a proof of the main result of the manuscript.

1.4. Acknowledgment. The author is supported by the CRM-Simons postdoctoral fellowship. He thanks the anonymous referee for the helpful report.

2. Preliminaries
Proposition 2.1. Suppose that the number of non-zero even eigenspaces of $C$ is strictly less than $\lfloor \frac{p-2}{4} \rfloor$. Then, there is an odd positive integer $k$ that lies in the range $3 \leq k \leq \left( \frac{p-1}{2} \right)$ such that $C(\bar{\chi}^{1+k}) = C(\bar{\chi}^{p-k}) = 0$.

Proof. Suppose that by way of contradiction that for each odd $k$ in the range $3 \leq k \leq \left( \frac{p-1}{2} \right)$, either $C(\bar{\chi}^{1+k})$ or $C(\bar{\chi}^{p-k})$ is non-zero. First, suppose that $p \equiv 1 \mod 4$, i.e., $p = 4s + 1$. Then, the number of odd values of $k$ in the range $3 \leq k \leq \left( \frac{p-1}{2} \right) = 2s$ is $(s-1) = \left[ \frac{p-2}{4} \right]$. On the other hand, suppose that $p \equiv 3 \mod 4$, i.e., $p = 4s + 3$. Then, the number of odd values of $k$ is $s = \left[ \frac{p-2}{4} \right]$. In both cases, the number of even eigenspaces must be $\geq \left[ \frac{p-2}{4} \right]$, a contradiction. Therefore, there must exist $k$ as above such that $C(\bar{\chi}^{1+k}) = C(\bar{\chi}^{p-k}) = 0$. \hfill $\square$

We make the above into an assumption, which is clearly significantly weaker than Vandiver’s conjecture.

Assumption 2.2. There is an odd positive integer $k$ that lies in the range $3 \leq k \leq \left( \frac{p-1}{2} \right)$ such that $C(\bar{\chi}^{1+k}) = C(\bar{\chi}^{p-k}) = 0$.

Remark 2.3. When $p \equiv 3 \mod 4$ and $k = \left( \frac{p-1}{2} \right)$, then, the above assumption stipulates that $C(\bar{\chi}^{\frac{p+1}{2}}) = 0$. This result is proven by Osburn (see [Osb05]). Therefore, the above is an assumption only for $p \equiv 1 \mod 4$.

We fix an integer $k$ in the range $3 \leq k \leq \left( \frac{p-1}{2} \right)$ such that the above assumption holds and let $\nu$ denote the character $\bar{\chi}^k$.

2.1. Diagonal Galois representations. Our construction is based on the study of suitable lifts of diagonal Galois representations, i.e., Galois representations that are expressed as a direct sum of 1-dimensional characters. Throughout, we shall fix a suitable residual representation. Let $\bar{\rho} : G_{\{p\}} \to \text{GL}_n(\mathbb{F}_p)$ be the diagonal Galois representation given by

$$\bar{\rho} = \bar{\rho}^{(n)} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix},$$

where

$$\alpha_i = \begin{cases} 1 \text{ if } i \text{ is odd,} \\ \nu \text{ if } i \text{ is even.} \end{cases} \quad (2.1)$$

Thus the representations we consider for $n = 2, 3, 4, \ldots$ are as follows

$$\bar{\rho}^{(2)} = \begin{pmatrix} 1 \\ \nu \end{pmatrix}, \bar{\rho}^{(3)} = \begin{pmatrix} 1 \\ \nu \\ 1 \end{pmatrix} \quad \text{and} \quad \bar{\rho}^{(4)} = \begin{pmatrix} 1 \\ \nu \\ 1 \\ \nu \end{pmatrix}, \ldots, \text{etc.}$$
Henceforth, we suppress the dependence of $n$ in our notation, and simply denote the residual representation by $\bar{\rho}$. We set $\alpha$ to denote the tuple $(\alpha_1, \ldots, \alpha_n)$, and given an integer $N > 0$, let $\beta = (\beta_1, \ldots, \beta_n)$ be a tuple of characters $\beta_i : G_{(p)} \to \left(\mathbb{Z}/p^N\mathbb{Z}\right)^\times$. We say that $\beta_i$ lifts $\alpha_i$ if $\alpha_i = \beta_i \mod p$, and that $\beta$ lifts $\alpha$ if $\beta_i$ lifts $\alpha_i$ for all $i = 1, \ldots, n$. In order to emphasize the dependence on $N$, we say that that $\beta$ is an $N$-lift of $\alpha$.

**Definition 2.1.** Let $m$ and $N$ be positive integers such that $m \leq N$. Let $\beta = (\beta_1, \ldots, \beta_n)$ be an $N$-lift of $\alpha$. We say that the tuple $\beta$ is $m$-admissible if the following conditions are satisfied.

1. For $i = 1, \ldots, n$, the character $\beta_i$ is of the form $\chi^{k_i}$ for some integer $k_i \geq 1$.
2. The characters $\beta_i$ are all distinct modulo $p^m$.
3. As $(i, j)$ ranges over all pairs such that $i \neq j$, the characters $\beta_{i,j} := \beta_i\beta_j^{-1}$ are all distinct modulo $p^m$.

Thus condition (2) implies that $\beta_{i,j} \neq 1$ modulo $p^m$ whenever $i \neq j$.

**Remark 2.4.** We observe the following.

1. Since $\beta$ lifts $\alpha$, we find that $k_i \equiv \left(\frac{1 + (-1)^i}{2}\right) k \mod (p - 1)$ for all $i$.
2. Note that (2) is equivalent to the condition that $k_i \neq k_j \mod p^{m-1}(p - 1)$ for $i \neq j$. By the above remark, this condition is automatically satisfied if $i \neq j$ mod $2$.
3. The condition (3) is equivalent to the condition that $k_i - k_j \neq k_s - k_t \mod p^{m-1}(p - 1)$ for all distinct pairs $(i, j)$ and $(s, t)$ such that $i \neq j$ and $s \neq t$.

Given an $N$-lift $\beta$ of $\alpha$, we consider the associated Galois representation

$$
\rho_\beta = \begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_{n-1} \\
\beta_n
\end{pmatrix} : G_{(p)} \to \text{GL}_n(\mathbb{Z}/p^N\mathbb{Z}).
$$

Note that since $\beta$ is a lift of $\alpha$, it follows that $\rho_\beta$ is a lift of $\bar{\rho}$. We say that $\rho_\beta$ is $m$-admissible if $\beta$ is $m$-admissible.

The following result shows that for any integer $n > 1$, an $m$-admissible lift of $\alpha$ does exist for an explicit choice of $m$.

**Lemma 2.5.** Let $m$ be an integer such that $m > 2 + \log_2(p^{2^n} + 1)$, and let $N \geq m$. For an integer $i$ in the range $1 \leq i \leq n$, let $\epsilon_i := \frac{1 + (-1)^i}{2} k$, $k_i := 2^i p + \epsilon_i$, and set $\beta_i := \chi^{k_i} \mod p^N$. Then, $\beta = (\beta_1, \ldots, \beta_n)$ is an $m$-admissible $N$-lift of $\alpha$.

**Proof.** Note that since $p^{m-1} > p^{2^n} + 1$, it follows that $\frac{1}{2} p^{m-1}(p - 1) > k_n = p^{2^n} + \epsilon_n$. Since $k_i \neq k_j$, it follows that $k_i \neq k_j \mod p^{m-1}(p - 1)$. On the other hand, suppose there are two distinct pairs $(i, j)$ and $(s, t)$ such that $i \neq j$, $s \neq t$, and

$$
\quad k_i - k_j \equiv k_s - k_t \mod p^{m-1}(p - 1).
$$

Then, since

$$
\max\{|k_i - k_j|,|k_s - k_t|\} \leq \frac{1}{2} p^{m-1}(p - 1),
$$

we have

$$
\quad \rho_\beta(i) = \rho_\beta(j) = \rho_\beta(s) = \rho_\beta(t),
$$

where $\rho_\beta(i), \rho_\beta(j), \rho_\beta(s), \rho_\beta(t)$ are the representations corresponding to the characters $\beta_i, \beta_j, \beta_s, \beta_t$. Therefore, $\beta$ is a lift of $\alpha$. 


we deduce that \(k_i - k_j = k_s - k_t\). Without loss of generality, assume that \(i > j, s, t\). Then, we find that \(p(2^i - 2^j) = p(2^s - 2^t) + b\), where \(|b| < p\). Then, we find that \(2^i - 2^j = 2^s - 2^t\) and \(b = 0\). But then, \(2^i = 2^j + 2^s - 2^t < 2 \cdot 2^{i-1} = 2^i\), a contradiction. Hence, we have proven that \(\beta\) is \(m\)-admissible.

\[\square\]

2.2. The adjoint representation. Let \(\mathfrak{g} = M_n(F_p)\) denote the Lie algebra of \(GL_n(F_p)\), consisting of \(n \times n\) matrices with entries in \(F_p = \mathbb{Z}/p\mathbb{Z}\). Denote by \(\mathfrak{g}_0\) the subspace of \(\mathfrak{g}\) consisting of matrices with trace equal to 0. We give \(\mathfrak{g}\) the structure of a Galois module as follows. Let \(v \in \mathfrak{g}\) and \(g \in G\). Then, \(g \cdot v\) is defined to be \(\tilde{\rho}(g)v\tilde{\rho}(g)^{-1}\). The action is referred to as the adjoint action. When referring to the Galois module, we simply use \(\text{Ad} \tilde{\rho}\), and when referring to the underlying space, we use \(\mathfrak{g}\). Note that \(\mathfrak{g}_0\) which consists of trace zero matrices is a submodule, which we also denote by \(\text{Ad}^0 \tilde{\rho}\). Set \(\alpha_{i,j}\) to denote \(\alpha_i \alpha_j^{-1}\). Recall that \(\alpha_i = \tilde{\chi} \left( \frac{1 + (-1)^i}{2} \right)^k\), and therefore, we find that

\[
\alpha_{i,j} = \begin{cases} 
1 & \text{if } i \equiv j \mod 2, \\
\nu = \tilde{\chi}^k & \text{if } i \text{ is even and } j \text{ is odd,} \\
\nu^{-1} = \tilde{\chi}^{-k} & \text{if } i \text{ is odd and } j \text{ is even.}
\end{cases}
\]

Let \(t\) (resp. \(t_0\)) denote the submodule of \(\text{Ad} \tilde{\rho}\) (resp. \(\text{Ad}^0 \tilde{\rho}\)) consisting of diagonal matrices. Note that the Galois action on \(t\) is trivial and we have the following decompositions

\[
\text{Ad} \tilde{\rho} = t \oplus \left( \bigoplus_{i \neq j} F_p(\alpha_{i,j}) \right),
\]

\[
\text{Ad}^0 \tilde{\rho} = t_0 \oplus \left( \bigoplus_{i \neq j} F_p(\alpha_{i,j}) \right).
\]

Given a module \(M\) over \(G_S\) and an integer \(i \geq 0\), we denote by \(H^i(G_S, M)\) the \(i\)-th cohomology group. Denote by \(\Pi^i_S(M)\) the kernel of the restriction maps

\[
\Pi^i_S(M) := \ker \left\{ H^i(G_S, M) \to \bigoplus_{\ell \in S} H^i(G_\ell, M) \right\}.
\]

Given a representation \(\tilde{\rho} : G_S \to GL_n(F_p)\), we say that \(\tilde{\rho}\) is \(S\)-unobstructed if the cohomology group \(H^2(G_S, \text{Ad} \tilde{\rho})\) vanishes. When \(\tilde{\rho}\) is unramified at all primes \(\ell \neq p\), we shall say that \(\tilde{\rho}\) is unobstructed to mean that it is \(\{p\}\)-unobstructed. When \(\tilde{\rho}\) is the residual representation \(\text{diag}(\alpha_1, \ldots, \alpha_n)\), the representation \(\tilde{\rho}\) is always unobstructed, as the following result shows.

**Proposition 2.6.** Let \(n > 1\) be an integer, and let \(\tilde{\rho}\) be the Galois representation \(\text{diag}(\alpha_1, \ldots, \alpha_n)\), where \(\alpha_i\) is given by (2.1). Then, we find that \(H^2(G_{\{p\}}, \text{Ad} \tilde{\rho}) = 0\).

**Proof.** Consider the exact sequence

\[
0 \to \Pi^2_{\{p\}}(\text{Ad} \tilde{\rho}) \to H^2(G_{\{p\}}, \text{Ad} \tilde{\rho}) \to H^2(G_p, \text{Ad} \tilde{\rho}).
\]
It suffices to show that \( \text{III}^2_{\{p\}}(\text{Ad} \, \bar{\rho}) = 0 \) and that \( H^2(G_p, \text{Ad} \, \bar{\rho}) = 0 \). Note that the Galois module \( \text{Ad} \, \bar{\rho} \) decomposes as follows

\[
\text{Ad} \, \bar{\rho} = \mathfrak{t} \oplus \left( \bigoplus_{i \neq j} \mathbb{F}_p(\alpha_{i,j}) \right).
\]

Note that the Galois action on \( \mathfrak{t} \) is the trivial one. Since the characters in the above decomposition all belong to \( \{1, \nu, \nu^{-1}\} \), we are to show that \( \text{III}^2_{\{p\}}(\mathbb{F}_p(\psi)) = 0 \) and that \( H^2(G_p, \mathbb{F}_p(\psi)) = 0 \) for all characters \( \psi \in \{1, \nu, \nu^{-1}\} \).

First let us show that \( \text{III}^1_{\{p\}}(\mathbb{F}_p(\psi)) = 0 \) for the above mentioned characters. Note that by global duality of III-groups \([\text{NSW13}]\), we have that \( \text{III}^2_{\{p\}}(\mathbb{F}_p(\psi)) \) are \( \text{III}^1_{\{p\}}(\mathbb{F}_p(\bar{\psi}^{-1})) \) are naturally dual to one another. Therefore, we are to check to that

\[
\text{III}^1_{\{p\}}(\mathbb{F}_p(\bar{\psi}^{-1})) = 0
\]

for the characters \( \psi \in \{1, \nu, \nu^{-1}\} \). A straightforward application of inflation-restriction shows that \( \text{III}^1_{\{p\}}(\mathbb{F}_p(\bar{\psi}^{-1})) = 0 \) if \( \mathcal{C}(\bar{\chi}) = 0 \) (cf. [Ray21, Lemma 3.2]). It is a well known fact that the first eigenspace \( \mathcal{C}(\bar{\chi}) = 0 \), cf. [Was97, Proposition 6.16]. On the other hand, the vanishing of \( \mathcal{C}(\bar{\chi}^{\nu \pm 1}) \) follows from Assumption 2.2. Therefore, we deduce that \( \text{III}^2_{\{p\}}(\text{Ad} \, \bar{\rho}) = 0 \).

Next, we show that \( H^2(G_p, \text{Ad} \, \bar{\rho}) = 0 \). It suffices to show that \( H^2(G_p, \mathbb{F}_p(\psi)) = 0 \) for each character \( \psi \in \{1, \nu, \nu^{-1}\} \). By local duality, we have that \( H^2(G_p, \mathbb{F}_p(\psi)) \) is dual to \( H^0(G_p, \mathbb{F}_p(\bar{\psi}^{-1})) \). Since \( \psi|_{G_p} \) is not equal to \( \bar{\chi} \), it follows that \( H^0(G_p, \mathbb{F}_p(\bar{\psi}^{-1})) = 0 \), and thus, \( H^2(G_p, \mathbb{F}_p(\psi)) = 0 \) for \( \psi \) as above. It follows that \( H^2(G_p, \text{Ad} \, \bar{\rho}) = 0 \) and it follows that \( H^2(G_p, \text{Ad} \, \bar{\rho}) = 0 \).

3. Deformation theory

In this section, we study the deformation theory of diagonal representations. The results in this section shall further aid our lifting construction. For a comprehensive treatment of the subject, the reader may refer to [Maz97].

Let \( G \) be a group, \( R \) be a commutative unital local ring, with maximal ideal \( \mathfrak{m}_R \). Recall that \( M_n(R) \) is the ring of \( n \times n \)-matrices with entries in \( R \). Given a representation \( \rho : G \to \text{GL}_n(R) \), the associated adjoint module denoted \( \text{Ad} \, \rho \), is the module \( M_n(R) \) on which \( g \in G \) acts via \( g \cdot v := \rho(g)v\rho(g)^{-1} \). There is a direct sum decomposition

\[
\text{Ad} \, \rho = \text{Ad}^0 \, \rho \oplus R \cdot I_n,
\]

where \( \text{Ad}^0(R) \) consists of matrices with trace equal to 0 and \( I_n \) is the identity in \( M_n(R) \).

We note that the Galois action on the second factor in the above decomposition is trivial.

**Definition 3.1.** Let \( \pi : S \to R \) be a homomorphism of commutative unital local rings and let I denote the kernel of \( \pi \). In this manuscript, we shall say that \( \pi \) is a small-extension if the following conditions hold

1. \( \pi \) is surjective,
2. \( I^2 = 0 \),
3. \( I \) is principal.
Given a small extension $\pi$, let $\pi^* : \text{GL}_n(S) \to \text{GL}_n(R)$ be the homomorphism obtained by applying $\pi^*$ to each entry.

The following example illustrates the above definition. Note that if $M$ and $N$ are integers such that $M < N$, then, the quotient map

$$\pi_{M,N} : \mathbb{Z}/p^NZ \to \mathbb{Z}/p^MZ$$

is a small extension provided $N \leq 2M$ and that the kernel of $\pi_{M,N}$ is generated by $p^M$.

Let us now introduce some further notation. The ideal $I$ is generated by the element $t$. Consider the map $R \to I$ sending $r$ to $tr$. Let $J$ denote the kernel of this map and set $R'$ to denote the quotient $R/J$. Thus the map sending $r$ to $tr$ induces an isomorphism of $R$-modules $R' \xrightarrow{\sim} I$. Let us introduce a little bit of notation which will be used throughout the manuscript. Given a matrix $A \in M_n(R')$ let $\tilde{A}$ be a lift of $A$ to $M_n(S)$. Let

$$t\tilde{A} \in \ker \{ M_n(S) \to M_n(R) \}$$

be the matrix obtained by multiplying all entries of $\tilde{A}$ by $t$. Clearly, the matrix $t\tilde{A}$ is independent of the choice of lift $A$, and we denote this product by $tA$.

**Proposition 3.1.** Let $\pi$ be a small extension. Then, the kernel of $\pi^* : \text{GL}_n(S) \to \text{GL}_n(R)$ defined above is abelian and can be identified with $M_n(R')$. The association takes a matrix $A \in M_n(R')$ to $I_n+tA$ in $\ker (\text{GL}_n(S) \to \text{GL}_n(R))$.

**Proof.** Since $t^2 = 0$, it follows that $I_n+tA$ is an invertible matrix with inverse $I_n-tA$. Moreover, the map sending $A \mapsto I_n+tA$ is seen to be a homomorphism, due to the relation

$$(I_n+tA)(I_n+tB) = (I_n+t\tilde{A})(I_n+t\tilde{B}) = I_n+t(\tilde{A} + \tilde{B}) = I_n+t(A + B).$$

It is also clear that any element in the kernel of $\pi^*$ is of the form $I_n+tA$, where $A \in M_n(R')$. \qed

Our discussion returns to the map $\pi_{M,N}$ (subject to the condition that $N \leq 2M$). We set $k := N - M$ and we find that $R' = \mathbb{Z}/p^k\mathbb{Z}$. The Proposition 3.1 asserts that the kernel of the reduction map $\text{GL}_n(\mathbb{Z}/p^NZ) \to \text{GL}_n(\mathbb{Z}/p^M\mathbb{Z})$ is identified with $M_n(\mathbb{Z}/p^k\mathbb{Z})$, upon associating a matrix $A \in M_n(\mathbb{Z}/p^k\mathbb{Z})$ with $I_n+p^MA$. For instance, say $n = 2$, $M = 2$, $N = 4$ and $k = 2$. Consider the matrix $A = \begin{pmatrix} 0 & 1 + p \\ -1 & 0 \end{pmatrix}$ and let $t = p^2$. Then, the product $p^2A$ is given by $\begin{pmatrix} 0 & p^2 + p^3 \\ -p^2 & 0 \end{pmatrix}$, and $I_2 + p^2 \begin{pmatrix} 0 & 1 + p \\ -1 & 0 \end{pmatrix}$ is given by $\begin{pmatrix} 1 & p^2 + p^3 \\ -p^2 & 1 \end{pmatrix} \in M_2(\mathbb{Z}/p^4\mathbb{Z})$.

Let us now discuss the notion of a deformation. Let $\pi : S \to R$ be any surjective map of commutative rings and $G$ be a group. Let $\rho : G \to \text{GL}_n(R)$ be a representation of $G$ on a free $R$-module of rank $n$. 


**Definition 3.2.** A lift of \( \rho \) is a representation \( \tilde{\rho} : G \to \text{GL}_n(S) \), which fits into a commutative triangle

\[
\begin{array}{ccc}
G & \xrightarrow{\rho} & \text{GL}_n(R) \\
\downarrow \tilde{\rho} & & \downarrow \\
\text{GL}_n(S) & \xrightarrow{\pi^*} & \text{GL}_n(R).
\end{array}
\]

where the vertical map is \( \pi^* \). Two lifts \( \tilde{\rho} \) and \( \tilde{\rho}' \) are said to be strictly equivalent if \( \tilde{\rho}' = B\tilde{\rho}B^{-1} \) for some matrix \( B \in \text{ker}(\text{GL}_n(S) \xrightarrow{\pi^*} \text{GL}_n(R)) \). A deformation of \( \rho \) is a strict equivalence class of lifts.

For the rest of this discussion, let us assume that \( \pi : S \to R \) is a small extension, and that \( I \simeq R' \simeq R/J \) as an \( R \)-module. Given \( \rho : G \to \text{GL}_n(R) \), let us assume that there exists a deformation \( \tilde{\rho} : G \to \text{GL}_n(S) \). Then, any other deformation is given by \( r = (I_n + tf)\tilde{\rho} \) for a uniquely determined cohomology class \( f \in H^1(G, \text{Ad} \rho_0) \), where \( \rho_0 \) is the reduction of \( \rho \) modulo \( J \). In greater detail, let \( F \) be a cocycle representing \( f \), consider the representation given by the formula \( (I_n + tf)\tilde{\rho} : G \to \text{GL}_n(S) \). This prescribes a well-defined lift of \( \rho \). The cocycle relation for \( F \) implies that the following relation holds for all \( h_1, h_2 \in G \),

\[
(I_n + tf(h_1)) \tilde{\rho}(h_1) (I_n + tf(h_2)) \tilde{\rho}(h_2) = (I_n + tf(h_1 h_2)) \tilde{\rho}(h_1 h_2).
\]

Thus, \((I_n + tf)\tilde{\rho}\) defines a well defined homomorphism, and \((I_n + tf)\tilde{\rho}\) defines a well defined deformation of \( \rho \). Indeed, if \( F_1 \) and \( F_2 \) are two cocycles that differ by a coboundary \( z = F_2 - F_1 \), we have that

\[
(I_n + tfz)\tilde{\rho} = (I_n + tf_1)(I_n + tz)\tilde{\rho}.
\]

By virtue of being a coboundary,

\[
z(h) = x - hx = x - \rho_0(h)x\rho_0(h)^{-1}.
\]

Therefore, we find that

\[
(I_n + tz(h)) = (I_n + tx) \left( I_n + t\rho_0(h)x\rho_0(h)^{-1} \right)^{-1}
\]

\[
(I_n + tx) \tilde{\rho}(h) \left( I_n + tx \right)^{-1} \tilde{\rho}(h)^{-1}.
\]

Therefore, combining (3.1) and (3.2), we find that

\[
(I_n + tf_2)\tilde{\rho} = (I_n + tx)(I_n + tf_1)\tilde{\rho}(I_n + tx)^{-1},
\]

i.e., the lifts \((I_n + tf_1)\tilde{\rho}\) and \((I_n + tf_2)\tilde{\rho}\) are strictly equivalent. One thus checks that \((I_n + tf)\tilde{\rho}\) is a well defined deformation of \( \rho \).

Recall that Lemma 2.5 guarantees the existence of an \( m \)-admissible lift of \( \alpha \), for \( m := m(p,n) = 3 + \lfloor \log_p(2^n + 1) \rfloor \). It is perhaps of interest to note that \( m \) decreases when \( p \) gets larger, and hence for large enough values of \( p \) and fixed \( n \) the value of \( m \) is 3. We shall of course fix a value of both \( n \) and \( p \) in our discussion throughout the paper. Set \( M \)
Lemma 3.3. With respect to notation above, let

\[ A := \ker \left( \text{GL}_n(\mathbb{Z}/p^{2M}) \to \text{GL}_n(\mathbb{Z}/p^M) \right) . \]

We set \( N := 2M \) and set \( \rho_N \) to denote the Galois representation \( \rho_\beta \) where \( \beta \) is an \( m \)-admissible \( N \)-lift of \( \alpha \). Let \( i \) be an integer which lies in the range \( 1 \leq i \leq N \) and \( \rho_i \) be the reduction of \( \rho_N \) modulo \( p^i \). Let \( \gamma = (\gamma_1, \ldots, \gamma_n) \) be the reduction of \( \beta \) modulo \( p^M \). Thus \( \rho_M \) is the diagonal representation \( \rho_\gamma \).

Given a Galois representation \( \varrho : G_\mathbb{Q} \to \text{GL}_n(R) \), the field \( Q(\varrho) := \mathbb{Q}^{\ker \varrho} \) is the field fixed by the kernel of \( \varrho \). We shall refer to \( Q(\varrho) \) as the field cut out by \( \varrho \) and we note that \( \varrho \) induces an injection from \( \text{Gal}(Q(\varrho)/\mathbb{Q}) \to \text{GL}_n(R) \). If the ring \( R \) is finite, then, \( Q(\varrho) \) is a finite Galois extension of \( \mathbb{Q} \). From here on in, set \( L := Q(\rho_M) \) to be the extension which is cut out by \( \rho_M \). Let \( M \) be the submodule of \( A \) which is the image of \( \rho_{N|G_L} : G_L \to A \). Note that by Proposition 3.1, \( A \) is identified with \( \text{Ad} \rho_M \) upon identifying \( I_n + p^M A \) with \( A \in \text{Ad} \rho_M \). Thus \( M \) is viewed as a \( \mathbb{Z}/p^M \mathbb{Z} \)-submodule of \( \text{Ad} \rho_M \), where

\[ \text{Ad} \rho_M = t_M \oplus \left( \bigoplus_{i \neq j} \mathbb{Z}/p^M \mathbb{Z}(\gamma_{i,j}) \right) , \]

where \( \gamma_{i,j} := \gamma_i \gamma_j^{-1} \). Here, \( t_M \) is the diagonal torus, with trivial action.

**Proposition 3.2.** With respect to notation above, \( M \) is a \( G_{(p)} \)-stable submodule of \( \text{Ad} \rho_M \).

**Proof.** Let \( x \in \rho_N(G_L) \), and let \( A \in \text{Ad} \rho_M \) be such that \( x = I_n + p^M A \). Thus, in particular, \( A \) is contained in \( M \), in accordance with the identification of \( A \) with \( \text{Ad} \rho_M \), as is explained above. Let \( h \in G_L \) be such that \( x = \rho_N(h) \). For \( g \in G_{(p)} \), note that \( ghg^{-1} \) is in \( G_L \). We find that

\[ \rho_N(ghg^{-1}) = \rho_N(g)x\rho_N(g)^{-1} = \rho_N(g)\left(I_n + p^M A\right)\rho_N(g)^{-1} = \left(I_n + p^M \rho_M(g)A\rho_M(g)^{-1}\right) = \left(I_n + p^M g \cdot A \right) . \]

Therefore, \( g \cdot A \) is contained in \( M \). \( \square \)

Recall that \( e_{i,j} \) be the matrix with all entries \( (s,t) \neq (i,j) \) equal to 0 and \((i,j)\)-th entry equal to 1. For \( i \neq j \), \( e_{i,j} \) a generator of the submodule of \( \text{Ad} \rho_M \) isomorphic to \( \mathbb{Z}/p^M \mathbb{Z}(\gamma_{i,j}) \). Given \( x \in A \), let \( x_0 \) be the projection of \( x \) to \( t_M \), and let \( x_{i,j} \) be the projection to the \( \gamma_{i,j} \)-component. We find that \( x_{i,j} = y_{i,j} e_{i,j} \), where \( y_{i,j} \in \mathbb{Z}/p^M \mathbb{Z} \). Thus, we find that \( x = x_0 + \sum_{i,j} y_{i,j} e_{i,j} \), where the sum ranges over all pairs \((i,j)\) such that \( i \neq j \). We remind the reader that \( M := m(n^2 - n) + 1 \), \( N := 2M \), and \( \rho_N = \rho_\beta \), where \( \beta \) is an \( m \)-admissible \( N \)-lift of \( \alpha \).

**Lemma 3.3.** With respect to notation above, let \((i,j)\) be a pair such that \( 1 \leq i,j \leq n \) and \( i \neq j \). Let \( x \in M \) and write \( x_{i,j} = y_{i,j} e_{i,j} \), where \( y_{i,j} \in \mathbb{Z}/p^M \mathbb{Z} \).

1. Suppose that \( y_{i,j} \) is not divisible by \( p \), then, \( M \) contains \( p^m(n^2-n)e_{i,j} \).
(2) Furthermore, $\mathcal{M}$ contains $p^{m(n^2-n)}x_0$.

Proof. Let $(i, j)$ be a pair such that $i \neq j$ and assume that the $y_{i,j}$ is not divisible by $p$. Since $\gamma$ is $m$-admissible, $\gamma_{(s,t)} \neq \gamma_{(i,j)} \mod p^m$ for all pairs $(s,t) \neq (i,j)$. Let $\mathfrak{R} := \mathbb{Z}/p^M\mathbb{Z}[G_{(p)}]$ denote the group ring with coefficients in $\mathbb{Z}/p^M\mathbb{Z}$. For each pair $(s,t) \neq (i,j)$ and $s \neq t$, may choose $g_{s,t} \in G_{(p)}$ such that $p^m$ does not divide $(\gamma_{s,t}(g_{s,t}) - \gamma_{i,j}(g_{s,t}))$. For each pair $(s,t) \neq (i,j)$ and $s \neq t$, let $h_{s,t} \in \mathfrak{R}$ denote the element $\gamma_{s,t}(g_{s,t}) - g_{s,t}$. Let $g_0 \in G_{(p)}$ be such that $p^m$ does not divide $1 - \gamma_{i,j}(g_0)$, and set $h_0 := 1 - g_0$.

Let $z \in \mathcal{A}$, we write $z$ as a linear combination $z = \sum_{k,l} a_{k,l}e_{k,l}$, where $a_{k,l}$ is the coefficient of $e_{k,l}$. The diagonal component of $z$ is $z_0 = \sum_k a_{k,k}e_{k,k}$. We find that

$$h_{s,t}z = \sum_{k,l} a_{k,l} (\gamma_{s,t}(g_{s,t}) - \gamma_{k,l}(g_{s,t})) e_{k,l},$$

$$h_0z = \sum_{k,l} a_{k,l} (1 - \gamma_{k,l}(g_0)) e_{k,l}.$$

Thus, applying $h_{s,t}$ to $z$ has an effect of killing the $e_{s,t}$-component and applying $h_0$ has the effect of killing the diagonal component $z_0$.

Set $H_{i,j}$ to denote the product $h_0 \prod_{(s,t)} h_{s,t}$, where $(s,t)$ ranges over all pairs such that $(s,t) \neq (i,j)$ and $s \neq t$. Then, we set $x' := H_{i,j}x$. Clearly, $x'$ belongs to $\mathcal{M}$. From the discussion in the previous paragraph, we find that the $(s,t)$ component of $h_{s,t}x$ is $0$ for all pairs $(s,t) \neq (i,j)$, such that $s \neq t$, and the diagonal component of $h_0 x$ is $0$. Therefore, $x'$ is a constant multiple of $e_{i,j}$. In fact, we find that

$$x' = u \left(1 - \gamma_{i,j}(g_0)\right) \prod_{(s,t)} (\gamma_{s,t}(g_{s,t}) - \gamma_{i,j}(g_{s,t})) e_{i,j},$$

where the above product runs through all pairs $(s,t) \neq (i,j)$ such that $s \neq t$, and $u$ is a unit in $\mathbb{Z}/p^k\mathbb{Z}$. In fact $u$ is the $e_{i,j}$-coefficient of $x$, which is assumed to not be divisible by $p$. Since $(\gamma_{s,t}(g_{s,t}) - \gamma_{i,j}(g_{s,t}))$ is not divisible by $p^m$ and there are $n^2 - n - 1$ pairs $(s,t) \neq (i,j)$ such that $s \neq t$, we find that the order of $p$ dividing $\prod_{(s,t)} (\gamma_{s,t}(g_{s,t}) - \gamma_{i,j}(g_{s,t}))$ in the above product is at most $m(n^2 - n - 1)$. Therefore, the power of $p$ dividing

$$(1 - \gamma_{i,j}(g_0)) \prod_{(s,t)} (\gamma_{s,t}(g_{s,t}) - \gamma_{i,j}(g_{s,t}))$$

is at most $m(n^2 - n)$. We therefore have shown that $p^{m(n^2-n)}e_{i,j}$ is also contained in $\mathcal{M}$, thus proving part (1). The proof of part (2) is identical to that of (1), hence, we omit it. \hfill \Box

4. Controlling the Image of Galois representations

Let $\rho : G_{(p)} \rightarrow \text{GL}_n(\mathbb{Z}_p)$ be a Galois representation. In this section, we illustrate conditions for the image of $\rho$ to contain $U_k$ for some large value of $k$. Throughout, $\tilde{\rho}$ is the residual representation of $\rho$, as defined in section 2.1. Recall that $\tilde{\rho}$ is said to be $\{p\}$-unobstructed if $H^2(G_{(p)}, \text{Ad} \tilde{\rho}) = 0$. Note that by Proposition 2.6, $\tilde{\rho}$ is $\{p\}$-unobstructed.
Proposition 4.1. With respect to notation above, let
\[ \rho_N : G_{\{p\}} \to \text{GL}_n(\mathbb{Z}/p^N\mathbb{Z}) \]
be any lift of \( \bar{\rho} \). Let \( \tau : G_{\{p\}} \to \text{GL}_1(\mathbb{Z}_p) \) be any character lifting \( \det \rho_N \). Then, there exists a lift \( \rho : G_{\{p\}} \to \text{GL}_n(\mathbb{Z}_p) \) of \( \bar{\rho} \) such that
\[ \rho_N = \rho \mod p^N \text{ and } \det \rho = \tau. \]

Proof. The above result follows from a well known argument, for further details, we refer to [Ray21, Fact 2.4 and Lemma 2.6]. \( \square \)

Since there are infinitely many choices of \( \tau \) that lift \( \det \rho_N \), it follows that there are infinitely many lifts \( \rho \) of \( \rho_N \).

For \( m \geq 1 \), set \( C_{n,m} := \ker \{ \text{GL}_n(\mathbb{Z}/p^{m+1}) \to \text{GL}_n(\mathbb{Z}/p^m) \} \) let
\[ \exp_m : M_n(\mathbb{F}_p) \to C_{n,m} \]
be the map taking \( A \in M_n(\mathbb{F}_p) \) to \( I_n + p^mA \). Here, we define \( p^mA \) by choosing a suitable lift of \( A \) and then noting that the product \( p^mA \) is independent of the choice of lift. It is easy to see that \( (4.1) \) is an isomorphism of abelian groups. We let \( \log_m : C_{n,m} \to M_n(\mathbb{F}_p) \) be the inverse of \( \exp_m \). Given a Galois representation \( \rho : G_{\{p\}} \to \text{GL}_n(\mathbb{Z}/p^N\mathbb{Z}) \), and \( i \leq N \) define a subspace \( \Phi_i(\rho) \) of \( M_n(\mathbb{F}_p) \) as follows. Set \( g_i \) to denote the mod-\( p^i \) reduction of \( g \), and set \( L_i \) be the field \( \mathbb{Q}(g_i) \). Consider the representation
\[ g'_i := g_i|_{L_i} : \text{Gal} \left( \mathbb{Q}_{\{p\}}/L_i \right) \to \text{GL}_n(\mathbb{Z}/p^{i+1}\mathbb{Z}). \]

Note that the image of the above homomorphism is by design contained in \( C_{n,i} \).

Definition 4.1. With respect to notation above, let \( \Phi_i(\rho) \) be the image of the composite
\[ \log_m \circ g'_i : G_{\{p\}} \to M_n(\mathbb{F}_p). \]

Lemma 4.2. Identify \( M_n(\mathbb{F}_p) \) with \( \text{Ad} \bar{\rho} \). With respect to notation above, then \( \Phi_i(\rho) \) is a \( G_{\{p\}} \)-submodule of \( \text{Ad} \bar{\rho} \).

Proof. Let \( A \) be in \( \Phi_i(\rho) \), then, there exists \( g' \in \text{Gal} \left( \mathbb{Q}_{\{p\}}/L_i \right) \) such that \( g'_i(g') = I_n + p^{i-1}A \). Let \( g \in G_{\{p\}} \), then, \( gg'g^{-1} \in \text{Gal} \left( \mathbb{Q}_{\{p\}}/L_i \right) \). We find that
\[ g'_i(gg'g^{-1}) = I_n + p^{i-1}(g \cdot A). \]

Hence, \( g \cdot A \) is also contained in \( \Phi_i(\rho) \). \( \square \)

Proposition 4.3. With respect to notation above, such that \( i + j \leq N \), then we find that
\[ [\Phi_i(\rho), \Phi_j(\rho)] \subseteq \Phi_{i+j}(\rho). \]

Proof. See the proof of [Ray21, Lemma 2.8]. \( \square \)

The module \( \text{Ad} \bar{\rho} \) is equipped with a Lie bracket \( [X, Y] := XY - YX \). Note that
\[ \text{Ad}^0 \bar{\rho} = [\text{Ad}^0 \bar{\rho}, \text{Ad}^0 \bar{\rho}]. \]

Lemma 4.4. Suppose that \( \rho : G_{\{p\}} \to \text{GL}_n(\mathbb{Z}_p) \) is a Galois representation such that for some \( i \geq 1 \), \( \Phi_i(\rho) \) contains \( \text{Ad}^0 \bar{\rho} \). Then,
\begin{enumerate}
  \item for all \( j \geq i \), \( \Phi_j(\rho) \) contains \( \text{Ad}^0 \bar{\rho} \),
  \item the image of \( \rho \) contains \( U_i \).
\end{enumerate}
Proof. The above result is [Ray21, Lemma 2.9]. □

Let $\mu$ be the element $\mu = \sum_{i=1}^{n} a_i e_{i,i} \in \text{Ad} \bar{\rho}$, where $a_i = \frac{1+(-1)^i}{2}$ in $t$.

**Proposition 4.5.** Suppose that $\rho : G_{\{p\}} \to \text{GL}_m(\mathbb{Z}_p)$ is a Galois representation such that for some $m \geq 1$, $\Phi_m(\rho)$ contains the following elements

1. the element $\mu$ as defined above,
2. $e_{i,j}$ for all pairs $(i,j)$ such that $i + j$ is odd.

Then, the following assertions hold

1. $\Phi_{m}(\rho)$ contains $\text{Ad}^0 \bar{\rho}$,
2. the image of $\rho$ contains $U_{4m}$.

**Proof.** First, we assume that $n > 2$. Let us show that $\Phi_{2m}(\rho)$ contains all $e_{i,j}$ for which $(i,j)$ is a pair such that $i \neq j$. Note that by Proposition 4.3, we have that $[\Phi_m(\rho), \Phi_m(\rho)] \subseteq \Phi_{2m}(\rho)$. Let $(i,j)$ be a pair such that $i + j$ is odd. Since $\mu$ and $e_{i,j}$ are both contained in $\Phi_m(\rho)$, it follows that $[\mu, e_{i,j}] \in \Phi_{2m}(\rho)$. Note that $[\mu, e_{i,j}] = (a_i - a_j)e_{i,j}$. Since $i \neq j \mod 2$, either $i$ is odd and $j$ is even, or, $i$ is even and $j$ is odd. We find that

$$[\mu, e_{i,j}] = \begin{cases} e_{i,j} \text{ if } i \text{ is even and } j \text{ is odd}, \\ -e_{i,j} \text{ if } j \text{ is even and } i \text{ is odd.} \end{cases}$$

Therefore, we find that $e_{i,j}$ is contained in $\Phi_{2m}(\rho)$ for all pairs $(i,j)$ such that $i + j$ is odd. Now, let $(i,j)$ be a pair such that $i \neq j$ and $i + j$ is even, i.e., $i \equiv j \mod 2$. Since $n \geq 3$, there exists $l$ such that $i + l$ and $j + l$ are both odd. Then, by assumption $e_{i,l}$ and $e_{i,j}$ are both contained in $\Phi_m(\rho)$. The relation $e_{i,j} = [e_{i,l}, e_{i,j}]$ implies that $e_{i,j}$ is contained in $\Phi_{2m}(\rho)$. Therefore, we have shown that $e_{i,j}$ is contained in $\Phi_{2m}(\rho)$ for all pairs $(i,j)$ such that $i \neq j$.

Note that $[\Phi_m(\rho), \Phi_{(r-1)m}(\rho)]$ is contained in $\Phi_{rm}(\rho)$ for $r \in \mathbb{Z}_{\geq 2}$. By induction on $r$, the same argument as above shows that for all $r \in \mathbb{Z}_{\geq 2}$, $\Phi_{rm}(\rho)$ contains $e_{i,j}$ for all pairs such that $i \neq j$. Since $[\Phi_{2m}(\rho), \Phi_{2m}(\rho)]$ is contained in $\Phi_{4m}(\rho)$, we find that $e_{i,i} - e_{j,j} = [e_{i,j}, e_{j,j}]$ is contained in $\Phi_{4m}(\rho)$ for all pairs $(i,j)$. Hence, we have shown that $\Phi_{4m}(\rho)$ contains $\text{Ad}^0 \bar{\rho}$, the subspace of $\text{Ad} \bar{\rho}$ consisting of trace 0 matrices. It follows from Lemma 4.4 then the image of $\rho$ contains $U_{4m}$. Therefore, we have proved the result for the case when $n > 2$.

Next, we assume that $n = 2$. In this case, a slightly different argument is required. Since $[\text{Ad}^0 \bar{\rho}, \text{Ad}^0 \bar{\rho}] = \text{Ad}^0 \bar{\rho}$, it suffices to show that $\Phi_{2m}(\rho)$ contains $\text{Ad}^0 \bar{\rho}$. Note that by assumption, $\Phi_m(\rho)$ contains $\mu = e_{1,1}$, $e_{1,2}$ and $e_{2,1}$. Therefore, $\Phi_{2m}(\rho)$ contains

$$e_{1,2} = [e_{1,1}, e_{1,2}],$$

$$e_{2,1} = [e_{2,1}, e_{1,1}],$$

$$e_{1,1} - e_{2,2} = [e_{1,2}, e_{2,1}],$$

and therefore, contains $\text{Ad}^0 \bar{\rho}$. Thus, the result follows from Lemma 4.4. □

5. **Proof of the main result**

In this section, we shall prove the main result. We begin with a few preliminary Lemmas.
Lemma 5.1. Suppose that $\psi : G_{\{p\}} \to \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ is a character with mod $p$ reduction $\bar{\psi}$. Assume that all of the following conditions are satisfied

1. $\bar{\psi}$ is odd, i.e., $\bar{\psi}(c) = -1$, where $c$ denotes complex conjugation,
2. $H^0\left(G_{\{p\}}, F_p(\bar{\psi})\right) = 0$,
3. $H^2\left(G_{\{p\}}, F_p(\bar{\psi})\right) = 0$.

Then, there is an isomorphism $H^1\left(G_{\{p\}}, \mathbb{Z}/p^k\mathbb{Z}(\psi)\right) \simeq \mathbb{Z}/p^k\mathbb{Z}$.

Proof. First, we prove the result when $k = 1$, in which case, $\psi$ is identified with its reduction $\bar{\psi}$. Since $\bar{\psi}$ is odd and $H^i\left(G_{\{p\}}, F_p(\bar{\psi})\right) = 0$ for $i = 0, 2$, it follows from the global Euler characteristic formula (cf. [NSW13, Theorem 8.7.4]) that $H^1\left(G_{\{p\}}, F_p(\bar{\psi})\right) \simeq \mathbb{Z}/p\mathbb{Z}$.

For $i \leq k$, let $\psi_i$ be the mod-$p^i$ reduction of $\psi$. Since $H^0(G_{\{p\}}, F_p(\bar{\psi})) = 0$, it follows that $H^0\left(G_{\{p\}}, \mathbb{Z}/p^{k-1}\mathbb{Z}(\psi_{k-1})\right) = 0$. Consider the long exact sequence in cohomology associated with the following short exact sequence of Galois modules

$$0 \to F_p(\bar{\psi}) \to \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^{k-1}\mathbb{Z}(\psi_{k-1}) \to 0.$$ 

Thus, we have the short exact sequence of cohomology groups

$$0 \to H^1\left(G_{\{p\}}, F_p(\bar{\psi})\right) \to H^1\left(G_{\{p\}}, \mathbb{Z}/p^k\mathbb{Z}(\psi)\right) \to H^1\left(G_{\{p\}}, \mathbb{Z}/p^{k-1}\mathbb{Z}(\psi_{k-1})\right) \to 0.$$ 

By induction, assume that the group $H^1\left(G_{\{p\}}, \mathbb{Z}/p^{k-1}\mathbb{Z}(\psi_{k-1})\right)$ is isomorphic to $\mathbb{Z}/p^{k-1}\mathbb{Z}$.

This shows that $H^1\left(G_{\{p\}}, \mathbb{Z}/p^k\mathbb{Z}(\psi)\right)$ is either isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^{k-1}\mathbb{Z}$ or to $\mathbb{Z}/p^k\mathbb{Z}$. Since the last map is the mod-$p^{k-1}$ reduction map, it follows that $H^1\left(G_{\{p\}}, \mathbb{Z}/p^k(\psi)\right)$ must be isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. This completes the proof. \(\square\)

Recall that $\rho_M$ is the diagonal Galois representation $\rho_\gamma$ associated with an $m$-admissible $M$-lift $\gamma = (\gamma_1, \ldots, \gamma_m)$ of $\alpha$. Let $L$ (resp. $L_0$) be the field extension $\mathbb{Q}(\rho_M)$ (resp. $\mathbb{Q}(\bar{\rho})$). Note that since $\rho_M$ is a diagonal representation, $L/\mathbb{Q}$ is an abelian extension. Set $\Delta := \text{Gal}(L/\mathbb{Q})$ (resp. $\Delta_0 := \text{Gal}(L_0/\mathbb{Q})$). Let $\bar{\psi}$ denote the character $\gamma_{i,j} := \gamma_{i,j}^{-1}$ for a pair $(i, j)$ such that $i + j$ is odd. In this case, we note that $\bar{\psi} = \bar{\gamma}_{i,j} = \alpha_{i,j}$ and hence is odd.

It follows from the argument in the proof of Proposition 2.6 that $H^1\left(G_{\{p\}}, F_p(\bar{\psi})\right) = 0$ for $i = 0, 2$. Recall from Lemma 5.1 that $H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\psi))$ is isomorphic to $\mathbb{Z}/p^M\mathbb{Z}$ and let $f_{i,j}$ be a generator. The Galois action of $\text{Gal}(\mathbb{Q}_{\{p\}}/L)$ on $\mathbb{Z}/p^M\mathbb{Z}(\psi)$ is trivial. Therefore, $H^1\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)$ consists of homomorphisms. There is a natural action of $\Delta$ on $\text{Hom}\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)$, which is described as follows. The restriction to $\text{Gal}(\mathbb{Q}_{\{p\}}/L)$ gives a homomorphism

$$\text{res} : H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\psi)) \to \text{Hom}\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)^\Delta.$$
Given $\sigma \in \Delta$, choose a lift $\tilde{\sigma}$ to $G_{\{p\}}$. For $g \in \text{Gal}(\mathbb{Q}_{\{p\}}/L)$, observe that $\tilde{\sigma}g\tilde{\sigma}^{-1}$ is contained in $\text{Gal}(\mathbb{Q}_{\{p\}}/L)$, since $L/\mathbb{Q}$ is a Galois extension. Let $h$ be a homomorphism in $\text{Hom}\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)$. Note that the value $h(\tilde{\sigma}g\tilde{\sigma}^{-1})$ is independent of the choice of lift $\tilde{\sigma}$ of $\sigma$, since $h$ must factor through an abelian quotient of $\text{Gal}(\mathbb{Q}_{\{p\}}/L)$. The action of $\Delta$ is given by setting $(\sigma \cdot h)(g) := \psi(\sigma)^{-1}h(\tilde{\sigma}g\tilde{\sigma}^{-1})$. Therefore, the subgroup $\text{Hom}\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)^\Delta$ consists of those homomorphisms which satisfy the condition

$$h(\tilde{\sigma}g\tilde{\sigma}^{-1}) = \psi(\sigma)h(g).$$

**Lemma 5.2.** With respect to notation above, the restriction map

$$\text{res} : H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\psi)) \to \text{Hom}\left(\text{Gal}(\mathbb{Q}_{\{p\}}/L), \mathbb{Z}/p^M\mathbb{Z}(\psi)\right)^\Delta$$

is injective. In other words, the homomorphism $\text{res}(f_{i,j})$ surjects onto $\mathbb{Z}/p^M\mathbb{Z}$.

**Proof.** Recall that $\psi = \gamma_{i,j}$ is a character modulo-$p^M$ such that $i + j$ is stipulated to be odd. Since $f_{i,j}$ is chosen to be a generator of $H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\psi))$, it is clear that the injectivity of (5.3) is equivalent to the condition that $p^k\text{res}(f_{i,j}) \neq 0$ for all $k < M$. This in turn is equivalent to the condition that the homomorphism $\text{res}(f_{i,j})$ is surjective.

From the inflation-restriction sequence (cf. [NSW13]), it suffices to show that

$$H^1\left(\Delta, \mathbb{Z}/p^M\mathbb{Z}(\psi)\right) = 0.$$

We point out here that

$$\left(\mathbb{Z}/p^M\mathbb{Z}(\psi)\right)^{\text{Gal}(\mathbb{Q}_{\{p\}}/L)} = \left(\mathbb{Z}/p^M\mathbb{Z}(\psi)\right)$$

since $\psi$, when restricted to $\text{Gal}(\mathbb{Q}_{\{p\}}/L)$ is trivial. First, we show that $H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) = 0$. Let $\mathcal{N}$ denote the Galois group $\text{Gal}(L/L_0)$. Note that $\mathcal{N}$ is an abelian group since $\Delta := \text{Gal}(L/\mathbb{Q})$ is abelian. Furthermore, $\mathcal{N}$ is a $p$-group. Consider the inflation-restriction sequence

$$0 \to H^1(\Delta_0, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) \to H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) \to H^1(\mathcal{N}, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi}))^{\Delta_0}.$$

Since $\Delta_0$ is isomorphic to the image of the diagonal representation $\tilde{\rho}$, it is easy to see that $p \nmid \#\Delta_0$. Therefore, it follows (from a standard application of restriction-corestriction) that $H^1(\Delta_0, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) = 0$. We show that $\text{Hom}\left(\mathcal{N}, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})\right)^{\Delta_0} = 0$, and thus deduce that $H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) = 0$. The action of $\Delta_0$ on $\mathcal{N}$ is induced via conjugation. In greater detail, given $\sigma \in \mathcal{N}$ and $x \in \mathcal{N}$, we choose a lift $\tilde{\sigma} \in \Delta$ of $\sigma$, and set $\sigma \cdot x := \tilde{\sigma}x\tilde{\sigma}^{-1}$. Since $\mathcal{N}$ is abelian, the action is well defined and $\tilde{\sigma}x\tilde{\sigma}^{-1}$ is independent of the choice of lift $\tilde{\sigma}$. Since $\Delta$ is abelian, this action is trivial, i.e., $\sigma \cdot x = x$. Note that $\tilde{\psi} \neq 1$, and therefore, it follows that $\text{Hom}\left(\mathcal{N}, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})\right)^{\Delta_0} = 0$. We have thus shown that $H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\tilde{\psi})) = 0$.

To conclude the proof, we show that for all $k \leq M$, $H^1(\Delta, \mathbb{Z}/p^k\mathbb{Z}(\psi_k)) = 0$. Here, $\psi_k$ is the mod-$p^k$ reduction of $\psi$. The result is proven by induction on $k$. The case when $k = 1$ has been proven. Consider the short exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z}(\tilde{\psi}) \to \mathbb{Z}/p\mathbb{Z}(\psi_k) \to \mathbb{Z}/p^{k-1}\mathbb{Z}(\psi_{k-1}) \to 0,$$
and the associated exact sequence
\[ H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\bar{\psi})) \to H^1(\Delta, \mathbb{Z}/p^k(\psi_k)) \to H^1(\Delta, \mathbb{Z}/p^{k-1}(\psi_{k-1})) \].

If we assume that
\[ H^1(\Delta, \mathbb{Z}/p\mathbb{Z}(\bar{\psi})) = 0 \] and \[ H^1(\Delta, \mathbb{Z}/p^{k-1}(\psi_{k-1})) = 0 \],
then, it follows that \( H^1(\Delta, \mathbb{Z}/p^k(\psi_k)) = 0 \). Therefore, by induction, it follows that
\[ H^1(\Delta, \mathbb{Z}/p^M(\psi)) = 0. \]

We make final preparations for the proof of the main theorem. First, we recall some context. Note that \( p \geq 7 \) is a prime number such that the Assumption 2.2 holds. Let \( \bar{\rho} \) be the representation \( \text{diag}(\alpha_1, \ldots, \alpha_n) \) as defined in section 2.1. Recall that Proposition 2.6 asserts that \( \bar{\rho} \) is \( \{p\}\)-unobstructed, i.e., \( H^2(G_{\{p\}}, \text{Ad} \bar{\rho}) = 0 \). Recall that the numbers \( m, M, N \) are defined as follows
\[ m := 3 + \lfloor \log_p(2^n + 1) \rfloor, \quad M := m(n^2 - n) + 1 \] and \( N := 2M \).

Recall that \( \beta \) be an \( m\)-admissible \( N\)-lift of \( \alpha \) and \( \gamma \) is the mod-\( p^M \) reduction of \( \beta \). In particular, \( \gamma \) is also \( m\)-admissible. Let \( \rho_N := \rho_{\beta} \) (resp. \( \rho_M := \rho_{\gamma} \)). As explained previously, it follows from Lemma 5.1 that for each pair \((i, j)\) such that \( 1 \leq i, j \leq n \) and \( i + j \) is odd,
\[ H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\gamma_{i,j})) \simeq \mathbb{Z}/p^M\mathbb{Z}. \] Let \( f_{i,j} \) be a generator of \( H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\gamma_{i,j})) \) for such a pair \((i, j)\). Let \( \mathfrak{B} \) be the set of all pairs \((i, j)\) such that \( 1 \leq i, j \leq n \) and \( i + j \) is odd. Set \( f = \sum_{(i,j)\in \mathfrak{B}} f_{i,j} \), the sum is taken over the generators \( f_{i,j} \). This is viewed as an element in
\[ H^1(G_{\{p\}}, \text{Ad} \rho_M) = \bigoplus_{(i,j)} H^1(G_{\{p\}}, \mathbb{Z}/p^M\mathbb{Z}(\gamma_{i,j})). \]

Let \( \rho'_N \) be the twist
\[ (I_n + p^Mf)\rho_N, \tag{5.4} \]
as defined in section 3. The representation \( \rho'_N \) is a deformation of \( \rho_M \).

By Proposition 2.6, \( \bar{\rho} \) is \( \{p\}\)-unobstructed. Therefore, it follows from Proposition 4.1, \( \rho'_N \) lifts to a characteristic zero lift \( \varrho : G_{\{p\}} \to \text{GL}_n(\mathbb{Z}_p) \). We recall that from the line prior to the statement of Proposition 4.3 that \( \mu = \sum_{i=1}^n a_i e_{i,j} \), where \( a_i := \frac{1+(-1)^i}{2} \). The field \( L \) is the field \( \mathbb{Q}(\rho_M) \) cut out by \( \rho_M \).

The Galois stable submodule \( \mathcal{M} \) of \( \text{Ad} \rho_M \) is defined in the paragraph above Proposition 3.2. The definition of \( \Phi_N(\varrho) \) is given in Definition 4.1.

**Proposition 5.3.** There is a natural Galois equivariant isomorphism of
\[ \Phi_N(\varrho) \simeq p^{M-1}\mathcal{M}. \]

**Proof.** Consider the map
\[ \iota : \text{Ad} \bar{\rho} \to \text{Ad} \rho_M, \]
which takes a matrix \( A \) to \( \iota(A) := p^{M-1} \tilde{A} \), where \( \tilde{A} \) is any choice of lift of \( A \) to \( \text{Ad} \rho_M \). Clearly, \( p^{M-1} \tilde{A} \) is independent of the choice of lift \( \tilde{A} \), and we simply denote this product
by $p^{M-1}A$. We show that $\mathfrak{t}$ induces the isomorphism $\Phi_N(\rho) \xrightarrow{\sim} \rho^M\mathcal{M}$. Let $A$ be a matrix in $\text{Ad} \rho_M$ and suppose that $A$ is contained in $\mathcal{M}$. This means that $I_n + p^MA$ is contained in the image of $\rho_N$. Now suppose that $A = p^{M-1}B$ for some matrix $B \in \text{Ad} \bar{\rho}$. Then, $I_n + p^{2M-1}B = I_n + p^{N-1}B$ is contained in the image of $\rho_N$. It thus follows that $B \in \Phi_N(\rho)$. Conversely, for $B \in \Phi_N(\rho)$, it is clear that $p^{M-1}B$ is in $\mathcal{M}$, by the same reasoning. The map $\mathfrak{t}$ is clearly Galois equivariant, and thus, induces the isomorphism $\Phi_N(\rho) \xrightarrow{\sim} \rho^M\mathcal{M}$.

\noindent \textbf{Lemma 5.4.} With respect to notation above, $\Phi_N(\rho)$ contains $\mu$ and all matrices $e_{i,j}$ such that $i + j$ is odd.

\textit{Proof.} Recall that for each pair $(i,j) \in \mathcal{B}$, Lemma 5.2 shows that the restricted homomorphism $f_{i,j} : \text{Gal}(\mathbb{Q}(p)/L) \to \mathbb{Z}/p^M\mathbb{Z}$ is surjective. Therefore, for $(i,j) \in \mathcal{B}$, there exists $g_{i,j} \in \text{Gal}(\mathbb{Q}(p)/L)$ such that $f_{i,j}(g_{i,j}) = 1$. We write $\rho_N^*(g_{i,j}) = I_n + p^Mx_i$. Then by construction the $e_{i,j}$-component of $x$ is 1, and hence, by Lemma 5.3, $\mathcal{M}$ contains $p^{n(n^2-n)}e_{i,j} = p^{M-1}e_{i,j}$ for each pair $(i,j) \in \mathcal{B}$. By Proposition 5.3, $\rho^M\mathcal{M} = p^{n(n^2-n)}\mathcal{M}$ can be identified with $\Phi_N(\rho)$. We make this identification. It follows that for each pair $(i,j) \in \mathcal{B}$, $\Phi_N(\rho)$ contains $e_{i,j}$.

Let $g$ in $\text{Gal}(\mathbb{Q}(p)/L)$ be an element such that $\chi(g) = 1 + p^M$. Then, we find that $\rho_N^*(g) = I_n + p^M\mu$. Let $x$ be the element such that $\rho_N^*(g) = I_n + p^Mx$. Since $f(g)$ consists of 0s along the diagonal, it follows that the diagonal projection $x_0 = \mu$. Lemma 5.3 then implies that $\mathcal{M}$ contains $p^{n(n^2-n)}\mu$. Hence, By Proposition 5.3 implies that $\Phi_N(\rho)$ contains $\mu$.

\noindent \textbf{Theorem 5.5.} Let $p \geq 7$ be a prime and $M := (n^2-n)\left(3 + \lceil \log_p(2^n+1) \rceil \right) + 1$. Suppose that Assumption 2.2 holds. Then, there are infinitely many Galois representations $\rho : G_{\mathbb{F}_p} \to \text{GL}_n(\mathbb{Z}_p)$ whose image contains $\mathcal{U}_{8M}$.

\textit{Proof.} Recall the $N$ is set to be $2M$ and let $\rho$ be as in the discussion above. According to the Lemma 5.4, $\Phi_N(\rho)$ contains $\mu$ and $e_{i,j}$ for all $(i,j)$ such that $i + j$ is odd. It follows from Proposition 4.5 that the image of $\rho$ contains $\mathcal{U}_{4N} = \mathcal{U}_{8M}$. It follows from Proposition 4.1, that there are infinitely many Galois representations $\rho$ that lift $\rho_N$, and hence, infinitely many Galois representations unramified outside $\{p, \infty\}$ and with image containing $\mathcal{U}_{8M}$.

\noindent \textbf{References}

[Gre16] Ralph Greenberg. Galois representations with open image. \textit{Annales mathématiques du Québec}, 40(1):83–119, 2016.

[Har94] David Harbater. Abhyankar’s conjecture on galois groups over curves. \textit{Inventiones mathematicae}, 117(1):1–26, 1994.

[HOPS18] David Harbater, Andrew Obus, Rachel Pries, and Katherine Stevenson. Abhyankar’s conjectures in galois theory: current status and future directions. \textit{Bulletin of the American Mathematical Society}, 55(2):239–287, 2018.

[Kat20] Nicholas M Katz. A note on galois representations with big image. \textit{L’Enseignement Mathématique}, 65(3):271–301, 2020.

[Mai21] Christian Maire. On galois representations with large image. \textit{arXiv preprint arXiv:2104.02505}, 2021.

[Mal22] Simone Maletto. Galois representations with big image in the general symplectic group $GSp_4(\mathbb{Z}_p)$. \textit{arXiv preprint arXiv:2208.11049}, 2022.
GALOIS REPRESENTATIONS RAMIFIED AT ONE PRIME

[Maz97] Barry Mazur. An introduction to the deformation theory of galois representations. In Modular forms and Fermat's last theorem, pages 243–311. Springer, 1997.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. Cohomology of number fields, volume 323. Springer Science & Business Media, 2013.

[Osb05] Robert Osburn. Vanishing of eigenspaces and cyclotomic fields. Int. Math. Res. Not., (20):1195–1202, 2005.

[Ray21] Anwesh Ray. Constructing galois representations ramified at one prime. Journal of Number Theory, 222:168–180, 2021.

[Tan] Shiang Tang. Algebraic monodromy groups of g-valued l-adic galois representations. Algebra & Number Theory, available as.

[Tan22] Shiang Tang. A note on galois representations valued in reductive groups with open image. arXiv preprint arXiv:2205.00502, 2022.

[Was97] Lawrence C Washington. Introduction to cyclotomic fields, volume 83. Springer Science & Business Media, 1997.