Journal of Number Theory 222 (2021) 168–180

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Constructing Galois representations ramified at one prime

Anwesh Ray

Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada

ARTICLE INFO

Article history:
Received 7 October 2020
Received in revised form 14 December 2020
Accepted 16 December 2020
Available online 13 January 2021
Communicated by F. Pellarin

Keywords:
Deformations of Galois representations

ABSTRACT

Let $n > 1$, $e \geq 0$ and a prime number $p \geq 2^{n+2+2e} + 3$, such that the index of regularity of p is $\leq e$. We show that there are infinitely many irreducible Galois representations $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Q}_p)$ unramified at all primes $l \neq p$. Furthermore, these representations are shown to have image containing a fixed finite index subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$. Such representations are constructed by lifting suitable residual representations $\bar{\rho}$ with image in the diagonal torus in $\mathrm{GL}_n(\mathbb{F}_p)$, for which the global deformation problem is unobstructed.

1. Introduction

Let p be an odd prime and n an integer. There is much interest in the study of continuous Galois representations

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$$

which are *geometric*, in the sense of Fontaine-Mazur (cf. [3]). Prototypical examples include Galois representations associated to abelian varieties over $\mathbb{Q}$ and Siegel modular

E-mail address: anweshray@math.ubc.ca.

https://doi.org/10.1016/j.jnt.2020.12.005
0022-314X/

forms. The Galois representations associated to abelian varieties have p-adic monodromy $\mathrm{GSp}_{2g}(\mathbb{Q}_p)$. On the other hand, Galois representations with big image in $\mathrm{GL}_n(\mathbb{Z}_p)$ for $n > 2$ are not expected to arise from automorphic forms.

In this article we study the following question:

Question 1.1. *Let p be a prime and $n > 1$. Does there exist a continuous Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ with suitably large image? If so, can one control the set of primes at which it may ramify?*

A parallel may be seen in the study of geometric Galois representations, where in the GL_2 case, the ramification may be controlled via Ribet's level lowering argument. For certain (p, n), Greenberg systematically constructed Galois representations $\mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ with image containing a finite index subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$. Let M be the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ which is unramified outside p. A theorem of Shafarevich shows that is p is a regular prime, then $\mathrm{Gal}(M/\mathbb{Q})$ is a free pro-p group with $\frac{p+1}{2}$ generators. Greenberg makes use of this to construct such Galois representations $\mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ when p is a regular prime greater than or equal to $4\lfloor n/2 \rfloor + 1$ (see [4, Proposition 1.1]). Cornut-Ray [2] further generalized Greenberg's results to more general algebraic groups, without relaxing the regularity assumption on p. In [10], Tang relaxed the regularity assumption of Greenberg, by constructing certain mod-p representations which lift to characteristic zero when they are allowed to ramify at an auxiliary set of primes. This relies on deformation techniques pioneered by Ramakrishna [8,9]. Thus, Tang provides an affirmative answer to the first part of Question 1.1. Our goal in this article is to control ramification. The residual representation is chosen to be unramified away from p so that the associated global deformation problem is *unobstructed*. This allows us to produce characteristic zero lifts without adding further ramification away from p. The construction in this paper is brief and self contained, relying only on well-known results in Galois cohomology. Let e_p denote the index of regularity, see Definition 3.1.

Theorem 1.2. *Let $n > 1$, $e \geq 0$ and p be a prime number such that*

(1) $p \geq 2^{n+2+2e} + 3$,
(2) the index of regularity $e_p \leq e$.

There are infinitely many continuous representations $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ such that the image of ρ contains $\ker\left(\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^4)\right)$.

It is noted, for instance in [1], that if the numerators of Bernoulli numbers are uniformly random modulo odd primes, then the density of irregular primes with index of irregularity equal to r should equal $e^{-1/2}/(2^r r!)$. This heuristic is supported by evidence, indeed, it is shown in [1] that among the first million primes, the highest index of irregularity observed is 6, and the only prime less than a million with index of irregularity

equal to 6 is 527377. The density $e^{-1/2}/(2^r r!)$ drops rather fast. The density of regular primes is expected to be $e^{-1/2} = 0.60653065...$, whilst the density of irregular primes with index of regularity 6 is expected to be 0.00001316.... In [5], it is shown that the maximum irregularity index for primes $p < 2^{31}$ is 9. Also note that it is known that Vandiver's conjecture is satisfied for all primes less than 2^{19}. Specializing the above to primes less than 2^{31}, we have the following:

Theorem 1.3. *Let n be such that $2 \leq n \leq 10$ and p a prime such that $2^{n+20} < p < 2^{31}$. There are infinitely many continuous representations $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ such that the image of ρ contains* $\ker\left(\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^4)\right)$.

When n and p are specified, it is indeed possible to check if the method in this article can be used to construct a Galois representation. One may try and construct the sequence $k_1, \ldots, k_n$ satisfying the properties of Theorem 3.3. However, the author was not able to realize a more refined statement which applies in suitable generality, than Theorem 1.2. It is natural to ask if the results in this manuscript can be generalized to split reductive algebraic groups over $\mathbb{Z}_p$, as is done in [2,10]. The author intentionally chooses a less general framework in which the inherent simplicity of the underlying ideas comes across easily.

Acknowledgments

The author would like to thank Ravi Ramakrishna for helpful conversations. The author is very grateful to the anonymous referee for her/his attentive and timely reading of the original submission.

2. The global deformation problem

In this section, we introduce some preliminary notions. Fix an odd prime p and a number $n > 1$. For each prime number l, denote by $\mathrm{G}_{\mathbb{Q}_l}$ the absolute Galois group of $\mathbb{Q}_l$. Choosing an embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_l$, we have an inclusion $\mathrm{G}_{\mathbb{Q}_l} \hookrightarrow \mathrm{G}_{\mathbb{Q}}$ of Galois groups. Denote by χ the p-adic cyclotomic character and $\bar{\chi}$ its mod-p reduction. For $m \geq 1$, denote by $\mathcal{U}_m \subseteq \mathrm{SL}_n(\mathbb{Z}_p)$ the kernel of the mod-p^m reduction map.

Fix a sequence of integers $k_1, k_2, \ldots, k_n$ and set $\bar{\rho}$ to denote the mod-p Galois representation which is a direct sum of characters $\bar{\chi}^{k_1} \oplus \cdots \oplus \bar{\chi}^{k_n}$. In other words, we have the residual representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^{k_1} & & & \\ & \bar{\chi}^{k_2} & & \\ & & \ddots & \\ & & & \bar{\chi}^{k_n} \end{pmatrix} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{F}_p).$$

In order to produce characteristic zero lifts of $\bar{\rho}$ with big image, we study the deformations of $\bar{\rho}$. For an introduction to the deformation theory of Galois representations, the reader may consult [6].

For a local ring R with maximal ideal $\mathfrak{m}_R$, let $\widehat{\mathrm{GL}_n}(R)$ be the group

$$\widehat{\mathrm{GL}_n}(R) := \ker\left\{\mathrm{GL}_n(R) \xrightarrow{\mathrm{mod}\,\mathfrak{m}_R} \mathrm{GL}_n(R/\mathfrak{m}_R)\right\}.$$

Definition 2.1. Let m be an integer such that $m \geq 1$. A mod-p^m lift of $\bar{\rho}$ is a continuous homomorphism $\rho_m : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$ such that $\bar{\rho} = \rho_m \bmod p$. Two lifts $\rho_m, \rho'_m : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$ of $\bar{\rho}$ are *strictly equivalent* if $\rho'_m = A\rho_m A^{-1}$ for some matrix $A \in \widehat{\mathrm{GL}_n}(\mathbb{Z}/p^m)$. A *deformation* is a strict equivalence class of lifts.

It was shown by Mazur that the global deformation functors associated to absolutely irreducible mod-p Galois representations are indeed representable by *universal deformations*. In this article, $\bar{\rho}$ is far from irreducible. We adopt a step by step lifting approach which does not rely on the existence of a universal deformation.

Let τ denote the determinant of $\bar{\rho}$ and $\tilde{\tau} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_1(\mathbb{Z}_p)$ denote the Teichmüller lift of τ. For any character $\phi : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{Z}_p)$, let ϕ_m denote the mod-p^m reduction of ϕ. When there is no cause for confusion, we shall simply use ϕ in place of ϕ_m. Fix a character ψ which is unramified outside $\{p\}$ such that $\psi_2 = (\tilde{\tau})_2$. For instance, ψ can be taken to be $\tilde{\tau}\chi^{p^2-p}$.

Convention 2.2. Let us note once and for all that all deformations of $\bar{\rho}$ are stipulated to have determinant equal to ψ.

In order to prove Theorem 1.2, it is shown that for a suitable choice of $k_1, \ldots, k_n$ it is shown that $\bar{\rho}$ lifts to a characteristic zero irreducible representation which is unramified at all primes $l \neq p$.

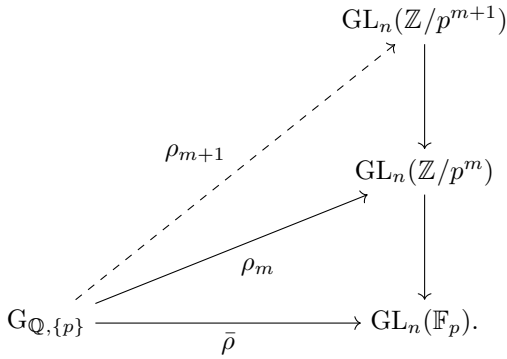
(1) First, it is shown that there is a mod-p^5 lift $\rho_5 : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^5)$ such that the image of ρ_5 contains

$$\ker\left\{\mathrm{SL}_n(\mathbb{Z}/p^5) \to \mathrm{SL}_n(\mathbb{Z}/p^4)\right\}.$$

(2) Next, it is shown that the (unramified outside $\{p\}$) infinitesimal lifting problem is unobstructed. This implies that any mod-p^m deformation

$$\rho_m : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$$

of $\bar{\rho}$ lifts one more step as depicted:



It follows that ρ_5 lifts to a characteristic zero continuous representation $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$.

(3) It is shown that the image of ρ contains $\mathcal{U}_4$.

Let us describe the infinitesimal deformation problem.

Definition 2.3. Set $\mathrm{Ad}\,\bar{\rho}$ to denote the Galois module whose underlying vector space consists of $n \times n$ matrices with entries in $\mathbb{F}_p$. Let $\mathrm{Ad}^0\,\bar{\rho}$ be the Galois stable submodule of trace zero matrices. The Galois action is as follows: for $g \in \mathrm{G}_{\mathbb{Q},\{p\}}$ and $v \in \mathrm{Ad}\,\bar{\rho}$, set $g \cdot v := \bar{\rho}(g) v \bar{\rho}(g)^{-1}$.

The module $\mathrm{Ad}\,\bar{\rho}$ is equipped with a Lie bracket $[X, Y] := XY - YX$. The underlying vector space of $\mathrm{Ad}\,\bar{\rho}$ (resp. $\mathrm{Ad}^0\,\bar{\rho}$) is the Lie algebra of $\mathrm{GL}_{n/\mathbb{F}_p}$ (resp. $\mathrm{SL}_{n/\mathbb{F}_p}$). Let $e_{i,j} \in \mathrm{Ad}^0\,\bar{\rho}$ denote the matrix with 1 at the (i,j) entry and 0 at all other entries. The adjoint Galois-module $\mathrm{Ad}^0\,\bar{\rho}$ is a direct sum

$$\mathrm{Ad}^0\,\bar{\rho} = \mathfrak{t} \oplus \left(\bigoplus_{(i,j), i \neq j} \mathbb{F}_p(\bar{\chi}^{k_i - k_j}) \right),$$

where $\mathfrak{t}$ is the submodule of diagonal matrices and the sum runs over (i,j) with $i \neq j$. The Galois action on $\mathfrak{t}$ is trivial.

Suppose that $m \geq 1$ and $\rho_m : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$ is a deformation of $\bar{\rho}$. A continuous lift (not necessarily a homomorphism) $\varrho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^{m+1})$ of ρ_m with determinant ψ_{m+1} does always exist. Identify $\mathrm{Ad}^0\,\bar{\rho}$ with the kernel of the mod-p^m map $\mathrm{SL}_n(\mathbb{Z}/p^{m+1}) \to \mathrm{SL}(\mathbb{Z}/p^m)$ by associating a vector $X \in \mathrm{Ad}^0\,\bar{\rho}$ with $\mathrm{Id} + p^m X$. Let $\mathcal{O}(\rho_m)$ be the cohomology class in $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho})$ defined by the 2-cocycle

$$(g, h) \mapsto \varrho(gh)\varrho(h)^{-1}\varrho(g)^{-1}.$$

The associated cohomology class $\mathcal{O}(\rho_m)$ so defined is independent of the lift ϱ. The following is easy to check.

Fact 2.4. A mod-p^m deformation ρ_m does lift one more step to a Galois representation which is unramified outside $\{p\}$

$$\rho_{m+1} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^{m+1})$$

if and only if $\mathcal{O}(\rho_m) = 0$.

The next fact states that the set of deformations ρ_{m+1} of ρ_m have the structure of an $H^1(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho})$-pseudotorsor.

Fact 2.5. Suppose that there exist deformations $\rho_{m+1}, \rho'_{m+1} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^{m+1})$ of ρ_m. Then there is a unique class $h \in H^1(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho})$ such that

$$\rho'_{m+1} = (\mathrm{Id} + p^m h)\rho_{m+1}.$$

We say that the "unramified outside $\{p\}$" deformation problem for $\bar{\rho}$ is *unobstructed* if $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho})$ is equal to zero. For future reference, we take note of the following, which follows from the previous discussion.

Lemma 2.6. *Suppose that $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$ and suppose that we are given a deformation $\rho_m : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$ of $\bar{\rho}$. There exists a deformation*

$$\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$$

such that $\rho_m = \rho \bmod p^m$.

In the next section, appropriate choices of $\bar{\rho}$ are shown to be unobstructed outside $\{p\}$ in the sense described. The results proven in the remainder of this section are used in showing that the characteristic zero lifts thus constructed do indeed have big image in $\mathrm{SL}_n(\mathbb{Z}_p)$. Suppose that $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ is a lift of $\bar{\rho}$. For $m \geq 1$, set ρ_m to be the mod-p^m reduction $\rho \bmod p^m$.

Definition 2.7. For $m \geq 1$, set $\Phi_m(\rho) := \rho_{m+1}(\ker \rho_m)$. Note that $\Phi_m(\rho)$ is isomorphic to $\ker \rho_m / \ker \rho_{m+1}$ and shall be viewed as a submodule of $\mathrm{Ad}\,\bar{\rho}$. Here, $\mathrm{Id} + p^m v = \rho_{m+1}(g)$ for $g \in \ker \rho_m$, is identified with $v \in \mathrm{Ad}\,\bar{\rho}$.

Recall from Definition 2.3 that the Galois action on $\mathrm{Ad}\,\bar{\rho}$ is from composing $\bar{\rho}$ with the adjoint action. Note that if $\sigma \in \mathrm{G}_{\mathbb{Q},\{p\}}$ and $v \in \mathrm{Ad}\,\bar{\rho}$, then

$$\rho_{m+1}(\sigma)(\mathrm{Id} + p^m v)\rho_{m+1}(\sigma)^{-1} = (\mathrm{Id} + p^m \bar{\rho}(\sigma) v \bar{\rho}(\sigma)^{-1}) = (\mathrm{Id} + p^m(\sigma \cdot v)).$$

It is easy to check that since $\ker \rho_m$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$, it follows that $\Phi_m(\rho) \subseteq \mathrm{Ad}\,\bar{\rho}$ is a Galois-stable submodule. Recall that the determinant of ρ is stipulated

to be equal to the character ψ, which is chosen to be congruent to $\tilde{\tau}$ modulo-p^2. As a result, for $g \in \ker \bar{\rho}$, it follows that $\det \rho_2(g) = 1$. Writing $\rho_2(g) = \mathrm{Id} + pX$, we have that

$$\det \rho_2(g) = 1 + p \operatorname{tr} X,$$

and hence $\operatorname{tr} X = 0$ in $\mathbb{Z}/p\mathbb{Z}$. It thus follows that $\Phi_1(\rho) \subseteq \mathrm{Ad}^0\, \bar{\rho}$.

Lemma 2.8. *Let ρ be as above. For $l, m \geq 1$, we have that $[\Phi_l(\rho), \Phi_m(\rho)] \subseteq \Phi_{l+m}(\rho)$.*

Proof. Set $\mathcal{G}_k$ denote the kernel of the mod-p^k map

$$\mathcal{G}_k := \ker \left\{ \mathrm{GL}_n(\mathbb{Z}/p^{k+1})) \to \mathrm{GL}_n(\mathbb{Z}/p^k) \right\}.$$

Let $c \in \Phi_l(\rho)$ and $d \in \Phi_m(\rho)$, consider the elements $\mathrm{Id} + p^l c \in \mathcal{G}_l$ and $\mathrm{Id} + p^m d \in \mathcal{G}_m$. Let $\tilde{c}, \tilde{d}$ be such that $A = \mathrm{Id} + p^l \tilde{c} \in \mathrm{GL}_n(\mathbb{Z}/p^{l+m+1})$ and $B = \mathrm{Id} + p^m \tilde{d} \in \mathrm{GL}_n(\mathbb{Z}/p^{l+m+1})$ lift $\mathrm{Id} + p^l c$ and $\mathrm{Id} + p^m d$ respectively. Assume without loss of generality that $l \leq m$. Since we are working mod-p^{l+m+1}, it follows that $(p^l \tilde{c})^{m+2} = 0$ and $(p^m \tilde{d})^3 = 0$. We have that

$$\begin{aligned}
ABA^{-1}B^{-1} =& (\mathrm{Id} + p^l \tilde{c})(\mathrm{Id} + p^m \tilde{d})(\mathrm{Id} + p^l \tilde{c})^{-1}(\mathrm{Id} + p^m \tilde{d})^{-1} \\
=& (\mathrm{Id} + p^m \tilde{d})^{-1} + (\mathrm{Id} + p^l \tilde{c}) p^m \tilde{d} (\mathrm{Id} + p^l \tilde{c})^{-1}(1 + p^m \tilde{d})^{-1} \\
=& (\mathrm{Id} - p^m \tilde{d} + (p^m \tilde{d})^2) \\
& + (\mathrm{Id} + p^l \tilde{c}) p^m \tilde{d} (\mathrm{Id} - p^l \tilde{c} + \cdots + (-1)^{m+1} (p^l \tilde{c})^{m+1})(\mathrm{Id} - p^m \tilde{d} + (p^m \tilde{d})^2) \\
=& (\mathrm{Id} - p^m \tilde{d} + (p^m \tilde{d})^2) + (\mathrm{Id} + p^l \tilde{c}) p^m \tilde{d} (\mathrm{Id} - p^l \tilde{c})(\mathrm{Id} - p^m \tilde{d}) \\
=& (\mathrm{Id} - p^m \tilde{d} + (p^m \tilde{d})^2) + (\mathrm{Id} + p^l \tilde{c}) p^m \tilde{d} (\mathrm{Id} - p^l \tilde{c}) - (p^m \tilde{d})^2 \\
=& (\mathrm{Id} - p^m \tilde{d} + (p^m \tilde{d})^2) + p^m \tilde{d} + p^{m+l}[c, d] - (p^m \tilde{d})^2 \\
=& \mathrm{Id} + p^{m+l}[c, d]. \quad \square
\end{aligned}$$

The following Lemma will be applied to show that the representations we construct contain a finite index subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$.

Lemma 2.9. *Let $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ be a continuous Galois representation lifting $\bar{\rho}$. Let $m \geq 1$ be such that $\Phi_m(\rho)$ contains $\mathrm{Ad}^0\, \bar{\rho}$. Then we have the following:*

(1) $\Phi_k(\rho)$ contains $\mathrm{Ad}^0\, \bar{\rho}$ for $k \geq m$,
(2) the image of ρ contains $\mathcal{U}_m$.

Proof. It is easy to check that $[\mathrm{Ad}^0\, \bar{\rho}, \mathrm{Ad}^0\, \bar{\rho}] = \mathrm{Ad}^0\, \bar{\rho}$. Part (1) follows from Lemma 2.8. Let H be the image of ρ. Since ρ is continuous and $\mathrm{G}_{\mathbb{Q},\{p\}}$ is compact, it follows that H is closed. For $l \geq 1$, let H_l be the projection of H to $\mathrm{GL}_n(\mathbb{Z}/p^l)$. Since H is closed, we

may identify it with the inverse limit $\varprojlim_l H_l$. Thus for part (2), we only need to check that H_k contains $\mathrm{Ad}^0\,\bar{\rho}$ for $k \geq m$. This follows from part (1). □

Lemma 2.10. *Let $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ be a continuous Galois representation lifting $\bar{\rho}$. Assume that $\Phi_1(\rho)$ contains an element $w := \sum_i a_i e_{i,i}$ such that $a_1, \ldots, a_n$ are all distinct. Furthermore, assume that it contains $e_{i,j}$ for all tuples (i,j) such that $(i+j)$ is odd. Then we have the following:*

(1) $\Phi_4(\rho)$ contains $\mathrm{Ad}^0\,\bar{\rho}$,
(2) the image of ρ contains $\mathcal{U}_4$.

Proof. First consider the case $n = 2$. Lemma 2.8 asserts that $[\Phi_1(\rho), \Phi_1(\rho)]$ is contained in $\Phi_2(\rho)$. The relations $[w, e_{1,2}] = (a_1 - a_2)e_{1,2}$ and $[w, e_{2,1}] = (a_2 - a_1)e_{2,1}$ imply that $e_{1,2}$ and $e_{2,1}$ are contained in $\Phi_2(\rho)$. The relation $[e_{1,2}, e_{2,1}] = 2(e_{1,1} - e_{2,2})$ implies that $e_{1,1} - e_{2,2}$ is also contained in $\Phi_2(\rho)$. Thus $\Phi_2(\rho)$ contains $\mathrm{Ad}^0\,\bar{\rho}$ and the conclusion follows from Lemma 2.9.

Consider the case $n > 2$. Let (i,j) be a tuple with $i \neq j$ and $i+j$ even. Since $n \geq 3$, we can pick l such that $l+i$ and $l+j$ are both odd. The relation $e_{i,j} = [e_{i,l}, e_{l,j}]$ implies that $\Phi_2(\rho)$ contains $e_{i,j}$. Let (i,j) be a pair with $i \neq j$ and $i+j$ is odd. The relation $[e_{i,j}, w] = (a_j - a_i)e_{i,j}$ implies that $e_{i,j}$ is contained in $\Phi_2(\rho)$.

Since $[\Phi_1(\rho), \Phi_2(\rho)]$ is contained in $\Phi_3(\rho)$, the relation $[w, e_{i,j}] = (a_i - a_j)e_{i,j}$ implies that $\Phi_3(\rho)$ contains all $e_{i,j}$, where (i,j) runs through pairs such that $i \neq j$. One more iteration of the same tells us that $\Phi_4(\rho)$ contains all $e_{i,j}$ where (i,j) runs through pairs such that $i \neq j$. Next, we note that $[\Phi_2(\rho), \Phi_2(\rho)]$ is contained in $\Phi_4(\rho)$. The relation $[e_{i,j}, e_{j,i}] = e_{i,i} - e_{j,j}$ implies that all elements $e_{i,j} - e_{j,j} \in \mathfrak{t}$ are contained in $\Phi_4(\rho)$. We have thus shown that $\Phi_4(\rho)$ contains $\mathrm{Ad}^0\,\bar{\rho}$. The conclusion follows from Lemma 2.9. □

3. Proof of main results

Recall that $\bar{\rho}$ is the representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^{k_1} & & & \\ & \ddots & & \\ & & \bar{\chi}^{k_{n-1}} & \\ & & & \bar{\chi}^{k_n} \end{pmatrix} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{F}_p).$$

Let A be the Class group of $\mathbb{Q}(\mu_p)$ and let $\mathcal{C}$ denote the mod-p class group $\mathcal{C} := A \otimes \mathbb{F}_p$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on $\mathcal{C}$ via the natural action. Since the order of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is prime to p, it follows that $\mathcal{C}$ decomposes into eigenspaces

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

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

Definition 3.1. The *index of regularity* e_p is the number of eigenspaces $\mathcal{C}(\bar{\chi}^i)$ which are non-zero.

Note that Vandiver's conjecture predicts that $\mathcal{C}(\bar{\chi}^i) = 0$ for i even (cf. [11, Chapter 8]). For a $\mathrm{G}_{\mathbb{Q},\{S\}}$-module M, which is a finite dimensional $\mathbb{F}_p$-vector space, we denote by $Ш^i_{\{p\}}(M)$, the kernel of the restriction map

$$Ш^i_{\{p\}}(M) := \ker\left(H^i(\mathrm{G}_{\mathbb{Q},\{p\}}, M) \to H^i(\mathrm{G}_{\mathbb{Q}_p}, M)\right).$$

Let $M^* := \mathrm{Hom}(M, \mu_p)$, where μ_p is the Galois module of p-th roots of unity. Note that $\mu_p \simeq \mathbb{F}_p(\bar{\chi})$. Global duality for Ш-groups states that there is a natural isomorphism $Ш^2_{\{p\}}(M) \simeq Ш^1_{\{p\}}(M^*)^\vee$.

Lemma 3.2. *For $0 \leq i \leq p-2$,*

(1) the group $Ш^1_{\{p\}}(\mathbb{F}_p(\bar{\chi}^i))$ is zero if $\mathcal{C}(\bar{\chi}^i)$ is zero,
(2) the group $Ш^2_{\{p\}}(\mathbb{F}_p(\bar{\chi}^i))$ is zero if $\mathcal{C}(\bar{\chi}^{p-i})$ is zero.

Proof. Let L be the subfield of the Hilbert Class field of $\mathbb{Q}(\mu_p)$ such that $\mathrm{Gal}(L/\mathbb{Q}(\mu_p))$ is isomorphic to $\mathcal{C}$. Since the order of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is prime to p, it follows that $H^j(\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}), \mathbb{F}_p(\bar{\chi}^i)) = 0$ for $j = 1, 2$. It follows that the restriction map $H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{F}_p(\bar{\chi}^i)) \to \mathrm{Hom}(\mathrm{G}_{\mathbb{Q}(\mu_p)}, \mathbb{F}_p(\bar{\chi}^i))^{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})}$ is an isomorphism. Via this isomorphism $Ш^1_{\{p\}}(\mathbb{F}_p(\bar{\chi}^i))$ consists homomorphisms $\mathrm{Hom}(\mathrm{Gal}(L/\mathbb{Q}(\mu_p)), \mathbb{F}_p(\bar{\chi}^i))$ that are unramified outside $\{p\}$ and trivial when restricted to the prime of $\mathbb{Q}(\mu_p)$ above p. The conclusion of the first part follows. The second part follows from the first part and global duality. □

Theorem 3.3. *Let $k_1, \ldots, k_n$ and $\bar{\rho}$ be as above. Assume that the following are satisfied:*

(1) $0 < k_i < \frac{p-1}{2}$,
(2) k_i is odd for i even and even for i odd,
(3) $\bar{\chi}^{k_i - k_j}$ is not equal to $\bar{\chi}$.
(4) The characters $\bar{\chi}^{k_i - k_j}$ for $i \neq j$ are all distinct.
(5) For (i, j) such that $i \neq j$, we have that $\mathcal{C}(\bar{\chi}^{p-(k_i - k_j)}) = 0$.

Then there exists a continuous lift $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ of $\bar{\rho}$ such that the image of ρ contains $\mathcal{U}_4$.

Proof. First, we exhibit a characteristic zero lift of $\bar{\rho}$ which is unramified outside $\{p\}$. We show that the unramified outside $\{p\}$ deformation problem is unobstructed, i.e., $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$. Note that $H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathrm{Ad}^0\,\bar{\rho})$ decomposes into

$$H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathrm{Ad}^0\,\bar{\rho}) = H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathfrak{t}) \oplus \left(\bigoplus_{(i,j)} H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathbb{F}_q(\bar{\chi}^{k_i-k_j})) \right),$$

where (i,j) runs through pairs for which $i \neq j$. By local duality, we have that

$$H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathfrak{t}) \simeq H^0(\mathrm{G}_{\mathbb{Q}_p}, \mathfrak{t}^*)^\vee, \text{ and } H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathbb{F}_q(\bar{\chi}^{k_i-k_j})) \simeq H^0(\mathrm{G}_{\mathbb{Q}_p}, \mathbb{F}_q(\bar{\chi}^{p-(k_i-k_j)}))^\vee.$$

By assumption, $\bar{\chi}^{k_i-k_j} \neq \bar{\chi}$. As a result, we have that $H^0(\mathrm{G}_{\mathbb{Q}_p}, \mathbb{F}_q(\bar{\chi}^{p-(k_i-k_j)})) = 0$. On the other hand, the Galois action on $\mathfrak{t}$ is trivial and the dual acquires a twist by $\bar{\chi}$, hence, $H^0(\mathrm{G}_{\mathbb{Q}_p}, \mathfrak{t}^*) = 0$. Thus, the local cohomology group $H^2(\mathrm{G}_{\mathbb{Q}_p}, \mathrm{Ad}^0\,\bar{\rho})$ is zero and hence,

$$H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = Ш^2_{\{p\}}(\mathrm{Ad}^0\,\bar{\rho}).$$

By global duality, we have that

$$Ш^2_{\{p\}}(\mathfrak{t}) \simeq Ш^1_{\{p\}}(\mathfrak{t}^*)^\vee.$$

It is a well known fact that $\mathcal{C}(\bar{\chi})$ is zero (cf. Proposition 6.16 of [11]). It follows (from Lemma 3.2) that $Ш^1_{\{p\}}(\mathbb{F}_p(\bar{\chi}))$ is zero, and thus, $Ш^1_{\{p\}}(\mathfrak{t}^*)$ is zero. By assumption, $\mathcal{C}(\bar{\chi}^{p-(k_i-k_j)})$ is zero, and hence, by Lemma 3.2,

$$Ш^2_{\{p\}}(\mathbb{F}_q(\bar{\chi}^{k_i-k_j})) = 0.$$

It has thus been shown that $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$.

Recall that χ_2 is $\chi \bmod p^2$, let ρ_2' be the lift

$$\rho_2' = \begin{pmatrix} \chi_2^{k_1} & & & \\ & \ddots & & \\ & & \chi_2^{k_{n-1}} & \\ & & & \chi_2^{k_n} \end{pmatrix} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^2).$$

Let (i,j) be a pair such that $i+j$ is odd. Since $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j})) = 0$ and $H^0(\mathrm{G}_{\mathbb{Q}_\infty}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j})) = 0$, it follows from the Global Euler characteristic formula (see [7, Theorem 8.7.4]) that $H^1(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j}))$ is one-dimensional. Let $f_{i,j}$ be a generator of $H^1(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j}))$. Let $F \in H^1((\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho})$ be the sum of all $f_{i,j}$ where (i,j) ranges over all $i \neq j$ such that $i+j$ is odd. Let ρ_2 be the twist $(\mathrm{Id} + pF)\rho_2' : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^2)$. Since $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$, it follows from Lemma 2.6 that ρ_2 lifts to a characteristic zero Galois representation $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$.

In order to show that the image of ρ contains $\mathcal{U}_4$, it suffices (by Lemma 2.10) to show that $\Phi_1(\rho)$ contains:

- $e_{i,j}$ for all tuples (i,j) such that $i+j$ is odd,
- an element $w = \sum a_i e_{i,i}$ in $\mathfrak{t}$ such that the a_i are distinct.

The image of $\bar{\rho}$ is prime to p and as a result, any Galois-submodule M of $\mathrm{Ad}^0\,\bar{\rho}$ decomposes into

$$M = M_1 \oplus \left(\bigoplus_{(i,j)} M_{\bar{\chi}^{k_i - k_j}} \right)$$

where $M_{\bar{\chi}^{k_i-k_j}}$ is the submodule

$$M_{\bar{\chi}^{k_i-k_j}} := \{x \in M \mid g \cdot x = \bar{\chi}^{k_i-k_j}(g)x\}$$

and M_1 the $\mathrm{G}_{\mathbb{Q}}$-invariant submodule. Note that it is assumed that all characters $\bar{\chi}^{k_i-k_j}$ are distinct for $i < j$. It follows from the bounds on k_i that all characters $\bar{\chi}^{k_i-k_j}$ are distinct for all tuples (i,j) with $i \neq j$. It is also clear that none of these is the trivial character. As a result, the above decomposition makes sense and $M_{\bar{\chi}^{k_i-k_j}}$, if non-zero, is the one-dimensional space generated by $e_{i,j}$. Since the order of $\mathbb{Q}(\mu_p)$ over $\mathbb{Q}$ is prime to p, it follows that

$$H^1(\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}), \mathbb{F}_p(\bar{\chi}^{k_i-k_j})) = 0.$$

It follows from the inflation restriction sequence that the restriction of $f_{i,j}$ to $\mathrm{G}_{\mathbb{Q}(\mu_p)}$ is non-zero. Hence, there exists $g \in \ker \bar{\rho}$ such that $f_{i,j}(g) \neq 0$. The element $\rho_2(g) \in \Phi_1(\rho)$ has non-zero $e_{i,j}$-component. It follows from the decomposition

$$\Phi_1(\rho) = \Phi_1(\rho)^{\mathrm{G}_{\mathbb{Q}}} \oplus \left(\bigoplus_{(i,j)} \Phi_1(\rho)_{\bar{\chi}^{k_i-k_j}} \right)$$

that $e_{i,j} \in \Phi_1(\rho)$ for all tuples (i,j) for which $i+j$ is odd. Note that the cyclotomic character χ induces an isomorphism

$$\chi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \xrightarrow{\sim} 1 + p\mathbb{Z}_p.$$

Let $\gamma \in \mathrm{G}_{\mathbb{Q}(\mu_p)}$ be chosen such that $\chi(\gamma) = 1+p$. With respect to the identification of $1 + pX \in \Phi_1(\rho)$ with $X \in \mathrm{Ad}^0\,\bar{\rho}$, the element $\rho_2(\gamma)$ coincides with $w := \sum k_i e_{i,i}$. We have thus shown that $\Phi_1(\rho)$ satisfies the required conditions, and this completes the proof. □

Proof of Theorem 1.2. Consider the $t := n+2e$ numbers $m_1, \ldots, m_t$, where $m_j = 2^{j+1} + \epsilon_j$ and

$$\epsilon_j := \begin{cases} 0 \text{ if } j \text{ is odd,} \\ 1 \text{ if } j \text{ is even.} \end{cases}$$

Note that $4 = m_1 < m_2 < \cdots < m_t < \frac{p-1}{2}$. Suppose that (i,j) and (k,l) are such that $i \neq j$, $k \neq l$ and

$$m_i - m_j \equiv m_k - m_l \mod p-1.$$

Then we show that $i = k$ and $j = l$. Since $|m_i - m_j|$ and $|m_k - m_l|$ are less than $\frac{p-1}{2}$, we have that $m_i - m_j = m_k - m_l$. Assume without loss of generality that $i > j$, and thus $m_i - m_j > 0$. This implies that $m_k > m_l$ and thus $k > l$. We have that

$$2^{i+1} - 2^{j+1} = 2^{k+1} - 2^{l+1} + \alpha,$$

where $-2 \leq \alpha \leq 2$. Since $i, j, k, l \geq 1$, we deduce that 4 divides α, and thus $\alpha = 0$. It thus suffices to show that $i = k$. Suppose not, assume without loss of generality that $i > k$. Then we have

$$2^{i+1} = 2^{j+1} + 2^{k+1} - 2^{l+1} \leq 2^i + 2^i - 2^{l+1} < 2^{i+1}.$$

Thus, it follows that $(i,j) = (k,l)$. It follows that the characters $\bar{\chi}^{p-(m_i-m_j)}$ are all distinct as (i,j) ranges over all tuples such that $i \neq j$. Let $\mathcal{S}_i$ be the set of characters $\bar{\chi}^{p-(m_i-m_j)}$ as j ranges from 1 to t such that $j \neq i$. Since the index of regularity e_p is less than or equal to e, it follows that there is a subset $\{i_1, \ldots, i_{n+e}\}$ of $\{1, \ldots, t\}$ such that for each character $\beta \in \bigcup \mathcal{S}_{i_j}$, the eigenspace $\mathcal{C}(\beta) = 0$. There is a subset of n numbers $\{k_1, \ldots, k_n\}$ of $\{i_1, \ldots, i_{n+e}\}$ such that k_i is odd if i is odd and even if i is even. Set a_i to be equal to m_{k_i}. Note that a_i is even for i odd and odd for i even. Moreover, the characters $\bar{\chi}^{p-(a_i-a_j)}$ are all distinct and $\mathcal{C}(\bar{\chi}^{p-(a_i-a_j)}) = 0$. It is clear from the definition of the original sequence $\{m_i\}$ that $a_i - a_j$ is not equal to 1. The result follows from Theorem 3.3. In fact, there are infinitely many Galois representations since there are infinitely many choices of

$$\psi : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_1(\mathbb{Z}_p)$$

such that $\psi_2 = (\tilde{\tau})_2$. □

References

[1] J.P. Buhler, R.E. Crandall, R.W. Sompolski, Irregular primes to one million, Math. Comput. 59 (200) (1992) 717–722.

[2] Christophe Cornut, Jishnu Ray, Generators of the pro-p Iwahori and Galois representations, Int. J. Number Theory 14 (01) (2018) 37–53.

[3] Jean-Marc Fontaine, Barry Mazur, Geometric Galois representations, in: Elliptic Curves, Modular Forms, and Fermat's Last Theorem, Hong Kong, 1993, in: Ser. Number Theory, vol. I, 1995, pp. 41–78.

[4] Ralph Greenberg, Galois representations with open image, Ann. Math. Québec 40 (1) (2016) 83–119.

[5] William Hart, David Harvey, Wilson Ong, Irregular primes to two billion, Math. Comput. 86 (308) (2017) 3031–3049.

[6] Barry Mazur, An introduction to the deformation theory of Galois representations, in: Modular Forms and Fermat's Last Theorem, Springer, New York, NY, 1997, pp. 243–311.

[7] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg, Cohomology of Number Fields, vol. 323, Springer Science and Business Media, 2013.
[8] Ravi Ramakrishna, Lifting Galois representations, Invent. Math. 138 (3) (1999) 537–562.
[9] Ravi Ramakrishna, Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur, Ann. Math. 156 (1) (2002) 115–154.
[10] Shiang Tang, Algebraic monodromy groups of G-valued l-adic Galois representations, Algebra Number Theory.
[11] Lawrence Washington, Introduction to Cyclotomic Fields, 2nd edition, Grad. Texts in Math., vol. 83, Springer-Verlag, Berlin, 1997.