CONSTRUCTION OF NON-ODD GALOIS REPRESENTATIONS WITH LARGE IMAGE

by

Donghyeok Lim & Christian Maire

Abstract. — In this work, we construct Galois representations with large image that are not GL_r-odd (or, equivalently, not regular at infinity). More precisely, for every prime $p \geqslant 3$, every integer $r \geqslant 2$, and every integer $a \in [(1-(-1)^r)/2,\, r-2]$ satisfying $a \equiv r \pmod 2$, we construct a continuous Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Q}_p)$ whose image is commensurable with $\mathrm{GL}_r(\mathbb{Z}_p)$ and satisfies $|\mathrm{tr}(\rho(c))| = a$, where c denotes a complex conjugation. We also obtain analogous results for the orthogonal group $\mathrm{O}_r(\mathbb{Q}_p)$.

1. Introduction

Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$, and let p be a prime number. Since the second half of the twentieth century, (continuous) Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Q}_p)$ have played a central role in number theory, particularly when they arise from geometry. A key object is the image $\rho(c)$ of (a class of) complex conjugation c. For instance, if ρ_E arises from the action of $G_{\mathbb{Q}}$ on the Tate module $T_p(E)$ of an elliptic curve E, then ρ_E is *odd*, meaning that $\det(\rho(c)) = -1$.

Let K be a number field and let G_K denote its absolute Galois group. We introduce the following invariant associated with a Galois representation $\rho : G_K \to \mathrm{GL}_r(\mathbb{Q}_p)$:

$$i(\rho) = \max_{v \ real} |\mathrm{tr}(\rho(c_v))|,$$

where c_v denotes a complex conjugation at the real place v. Since the eigenvalues of $\rho(c_v)$ are ± 1, we have $i(\rho) \leqslant r$ and $i(\rho) \equiv r \pmod 2$.

For Galois representations of dimension $r > 2$, one is naturally led to consider generalizations of the notion of oddness. We refer the reader to Calegari's note **[2]**, based on

2000 ***Mathematics Subject Classification.*** — 11R37, 11R32.
Key words and phrases. — Galois representations, non-regular at infinity, open image, $\mathbb{Z}_p$-Lie algebras.

This work was carried out during visiting positions held by the second author at Korea National University of Education. These visits were partially funded by the French-Korean International Research Network in Mathematics (CNRS). The first author was supported by the National Research Foundation of Korea (NRF) grants No. RS-2024-00462910. The second author was also partially supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne-Franche-Comté Region.

lectures given at the Institut Henri Poincaré in 2010. See also Gross's unpublished note [**8**]. In the present work, we focus on the following notion.

Definition. — *A Galois representation $\rho : G_K \to \mathrm{GL}_r(\mathbb{Q}_p)$ is said to be regular at infinity (or GL_r-odd) if $i(\rho) \leqslant 1$.*

Bellaiche-Chenevier [**1**], Taylor [**19**], Calegari [**3**], Caraiani-Le Hung [**4**] studied the behavior of $i(\rho)$ when K is totally real and ρ arises from an automorphic form. In all these works, ρ is regular at infinity.
In this context, Khare–Larsen [**11**, Appendix A] investigated the relationship between regularity at infinity and geometric lifts of mod p Galois representations. In particular, they suggest that any geometric lifting of a mod p Galois representation that is regular at all places above p (i.e. distinct Hodge-Tate weights for all places above p) should also be regular at infinity.

On the other hand, one may ask how to construct Galois representations with open image. Greenberg [**7**] initiated a Galois-theoretic approach to this question for representations valued in $\mathrm{GL}_r(\mathbb{Z}_p)$ with $r \geqslant 3$, motivated in part by the difficulty of producing such representations by geometric means. This line of research was subsequently developed by Ray [**16**] [**17**], Cornut-Ray [**5**], Maire [**14**], Tang [**18**], etc. In particular, [**14**] proves that for every $p > 2$ and every $r \geqslant 1$, there exists a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Z}_p)$ with open image. These constructions rely on group-theoretic methods rather than automorphic ones, although it seems nontrivial to prove that the resulting representations are not geometric.
Meanwhile, Katz [**10**] gave an alternative construction of Galois representations with open image in $\mathrm{GL}_r(\mathbb{Z}_p)$, for $r \geqslant 6$ and $p \equiv 1 \pmod 3$ or $p \equiv 1 \pmod 4$, using the Jacobian varieties of some explicit curves. However, in all the cases mentioned above, the resulting Galois representations are regular at infinity.

In this work, we construct Galois representations with large image that are not regular at infinity.

Let $\omega : G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{Z}_p)$ be the cyclotomic character. For an integer r, set $\epsilon(r) = \frac{1-(-1)^r}{2}$.

Theorem 1. — *For every prime $p \geqslant 3$, every $r \geqslant 2$, and every integer a satisfying $\varepsilon(r) \leqslant a \leqslant r-2$ and $a \equiv r \pmod 2$, there exists a continuous Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$ if $p \equiv 3$ mod 4 (resp. outside $\{2, p, \infty\}$ if $p \equiv 1$ mod 4) such that:*

(1) *$i(\rho) = a$;*
(2) *The image of ρ and $\mathrm{SL}_r(\mathbb{Z}_p)$ are commensurable. More precisely, let $k, m, n \in \mathbb{N}$ with $m \geqslant n \geqslant 1$ be such that*

$$m + n = r, \quad m - n = a, \quad p^k > m(m+2)(m+3),$$

then $\rho(G_{\mathbb{Q}})$ contains the principal congruence subgroup $\mathrm{SL}_r^{4kmn-2k+2}(\mathbb{Z}_p)$ as an open subgroup;
(3) *The Galois representation $\rho \otimes \omega : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Z}_p)$ has open image with $i(\rho \otimes \omega) = a$.*

Recall that two topological groups G and H are said to be *commensurable* if they have a common open subgroup.

In the same spirit as Cornut-Ray [**5**], Tang [**18**], and Maletto [**15**], we obtain the following result by varying the target group.

Theorem 2. — *For every $p \geqslant 3$, for every $r \geqslant 2$, for every a with $\varepsilon(r) \leqslant a \leqslant r-2$ and $a \equiv r \pmod 2$, there exist a continuous Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{O}_r(\mathbb{Z}_p)$ in the orthogonal group $\mathrm{O}_r(\mathbb{Z}_p)$, unramified outside $\{p, \infty\}$ (resp. outside $\{2, p, \infty\}$) if $p \equiv 3 \bmod 4$ (resp. $p \equiv 1 \bmod 4$) and such that:*

(1) *$i(\rho) = a$;*

(2) *The image of ρ is open. More precisely, let $k, m, n \in \mathbb{N}$ with $m \geqslant n \geqslant 1$ be such that*

$$m + n = r, \quad m - n = a, \quad p^k > \frac{3n(m+2)}{2} + m,$$

then $\rho(G_{\mathbb{Q}})$ contains the principal congruent subgroup $\mathrm{SO}_r^{2kmn-2k+2}(\mathbb{Z}_p)$ of $\mathrm{SO}_r(\mathbb{Z}_p)$.

Remark. — *We prove a slightly more general result than those stated above. More precisely, let $p \geqslant 3$ and let K be an imaginary quadratic field such that $p \nmid h_K$, where h_K denotes the class number of K. Then there exists a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{Z}_p)$ satisfying conditions $(1) - (2)$ of Theorem 1 (resp. Theorem 2), and such that ρ factors through the maximal pro-p extension of K unramified outside p. In particular, the ramification set of ρ consists of p together with the primes ramified in $K/\mathbb{Q}$.*

This paper is divided into three sections. The next section is devoted to the strategy developed in **[14]**, together with some Lie algebra-theoretic background. Its main result is Theorem 2.7, which relies on Kuranishi's theorem stating that every semisimple Lie algebra over a field of characteristic 0, in particular over $\mathbb{Q}_p$, is generated by two elements x and y. To obtain our main results, however, we require a refinement of this theorem. More precisely, fix a partition $r = m + n$ with $m \geqslant n \geqslant 1$, and let A be the $r \times r$ diagonal matrix whose first m diagonal entries are 1 and whose last n diagonal entries are -1. In Section 3, we refine Kuranishi's theorem for the semisimple Lie algebras $\mathfrak{sl}_r(\mathbb{Q}_p)$ and $\mathfrak{so}_r(\mathbb{Q}_p)$ by taking into account the involutive automorphism induced by conjugation by A. The final section is devoted to the proofs of the two theorems stated in the introduction.

2. Group-theoretic tools for lifting Galois representations

For a finitely generated pro-p group N, denote by $N^{p,el} := N/N^p[N,N]$ its maximal p-elementary quotient. Let $\pi_N : N \to N^{p,el}$ be the natural projection.

The starting point of our strategy is the following lifting result.

Theorem 2.1. — *Let $\Gamma \rtimes \Delta$ be a profinite group, where Γ is a finitely generated free pro-p group and $\Delta \subset \mathrm{Aut}(\Gamma)$ is a finite group of order coprime to p. Let H be a pro-p group equipped with an action of a finite group Δ', where $\Delta' \cong \Delta$. Fix an isomorphism $\rho_0 : \Delta \xrightarrow{\cong} \Delta'$ and regard H as a Δ-group vis ρ_0. Suppose that the Δ-module $H^{p,el}$ is isomorphic to a sub-Δ-module of $\Gamma^{p,el}$. Let $\alpha : \Gamma \rtimes \Delta \twoheadrightarrow H^{p,el} \rtimes \Delta'$ be the homomorphism induced by a surjective Δ-homomorphism $\Gamma^{p,el} \twoheadrightarrow H^{p,el}$ and ρ_0. Let $\pi : H \rtimes \Delta' \twoheadrightarrow H^{p,el} \rtimes \Delta'$ be the homomorphism determined by $\pi|_H = \pi_H$ and $\pi|_{\Delta'} = \mathrm{id}_{\Delta'}$. Then the embedding problem*

$$\begin{array}{ccc} & & \Gamma \rtimes \Delta \\ & \overset{\psi}{\swarrow} & \downarrow \alpha \\ H \rtimes \Delta' & \xrightarrow[\pi]{} & H^{p,el} \rtimes \Delta' \end{array}$$

admits a proper continuous solution ψ.

Since we start with a free pro-p group Γ, the lifting problem is simpler than the one considered in [**14**]. In particular, this theorem is proved in Greenberg [**7**, Proposition 2.3.1]. It also appears in [**9**, Proposition 2.14], where it is deduced from the unpublished work of Wingberg [**20**]. Since this result is crucial for our purposes, we choose to give the main arguments of the proof, following [**9**] and [**20**].

Proof. — The result is immediate if $\Delta = 1$. For the general case, by assumption, there exists an $\mathbb{F}_p[\Delta]$-module isomorphism $H^{p,el} \oplus M \cong \Gamma^{p,el}$ for some M. Hence, replacing $H \rtimes \Delta'$ by $(H \times M) \rtimes \Delta'$ and modifying the chosen homomorphism α accordingly, if necessary, we may assume that Γ and H have the same generator rank. Let $\iota_1 : \Delta \to \mathrm{Aut}(\Gamma)$ denote the homomorphism corresponding to the original action of Δ on Γ, and henceforth write the semidirect product $\Gamma \rtimes \Delta$ appearing in the statement as $\Gamma \rtimes_{\iota_1} \Delta$.
Let $\alpha' : \Gamma \to H$ be a lift of the restriction $\alpha \mid_\Gamma$ of α to Γ. By [**20**] or [**9**, Lemma 2.15], Γ admits a Δ-action defined by a homomorphism $\iota_2 : \Delta \to \mathrm{Aut}(\Gamma)$ for which α' is Δ-equivariant. Let $\Gamma \rtimes_{\iota_2} \Delta$ be the semidirect product associated with ι_2, and let $\beta : \Gamma \rtimes_{\iota_2} \Delta \to H \rtimes \Delta'$ be the surjection induced by α' and ρ_0.
The actions defined by ι_1 and ι_2 induce the same action on $\Gamma^{p,el}$. Thus, by the Schur-Zassenhaus theorem, there exists $g \in \mathrm{Ker}(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma^{p,el}))$ such that $g \circ \iota_1(s) = \iota_2(s) \circ g$ for every $s \in \Delta$ (cf. [**9**, Proposition 2.13]). It is straightforward to check that the composite of β with the homomorphism

$$\Gamma \rtimes_{\iota_1} \Delta \to \Gamma \rtimes_{\iota_2} \Delta \qquad (\gamma, s) \to (g(\gamma), s)$$

is a solution to the embedding problem. □

We now apply the above lifting theorem in the setting of imaginary quadratic fields.

2.1. The lifting theorem and imaginary quadratic fields. — Take $p \geqslant 3$. We begin with an imaginary quadratic extension $K/\mathbb{Q}$. Put $\Delta = Gal(K/\mathbb{Q}) = \langle s \rangle$. Let $\mathbf{1}$ denote the trivial $\mathbb{F}_p$-character of Δ, and let φ be its nontrivial character. Let K_p be the maximal pro-p extension of K unramified outside p, and set $G_{K,p} = Gal(K_p/K)$. Observe that Δ acts on $G_{K,p}$ and hence on $G_{K,p}^{p,el}$. We denote by $\chi(G_{K,p}^{p,el})$ the character of the $\mathbb{F}[\Delta]$-module $G_{K,p}^{p,el}$.
The following result is very well-known (see for example [**14**, Example 1.10]; the case $p = 3$ is also obvious).

Proposition 2.2. — *Let K be an imaginary quadratic field such that $p \nmid h_K$. The group $G_{K,p}$ is free pro-p on two generators and $\chi(G_{K,p}^{p,el}) = \mathbf{1} + \varphi$.*

Example 2.3. — Set $K = \mathbb{Q}(\sqrt{-p})$. Thanks to an explicit version of Brauer-Siegel Theorem (see for example [**13**]), $p \nmid h_K$, and therefore $G_{K,p}$ satisfies Proposition 2.2.

For our purposes, let us work in the setting of Proposition 2.2. Let G be a pro-p group having an automorphism t of order 2. Set $\Delta' = \langle t \rangle$, and consider the isomorphism $\rho_0 : \Delta \xrightarrow{\sim} \Delta'$. Suppose that $g_1, g_2 \in G$ satisfy $t(g_1) = g_1$ and $t(g_2) = g_2^{-1}$. Let $H := \langle g_1, g_2 \rangle$ be the closed subgroup of G generated by g_1 and g_2. Then Δ' is a subgroup of $\mathrm{Aut}(H)$, and Δ acts on H via ρ_0. The character $\chi(H^{p,el})$ of the $\mathbb{F}_p[\Delta]$-module $H^{p,el}$ is given by $\chi(H^{p,el}) = \mathbf{1} + \varphi$. As consequence of Theorem 2.1 and Proposition 2.2 applied to $\Gamma = G_{K,p}$, we obtain the following surjective morphism

$$\psi : Gal(K_p/\mathbb{Q}) \simeq G_{K,p} \rtimes \Delta \twoheadrightarrow H \rtimes \Delta'.$$

Let F be the subfield of K_p fixed by the kernel of ψ. Then $F/\mathbb{Q}$ is a Galois extension such that $Gal(F/\mathbb{Q}) \simeq H \rtimes Gal(K/\mathbb{Q})$. Thus, we have proved the following.

Theorem 2.4. — *Let $p \geqslant 3$, and let $K/\mathbb{Q}$ be an imaginary quadratic extension with $p \nmid h_K$. Let G be a pro-p group equipped with an automorphism t of order 2. Assume that there exist $g_1, g_2 \in G$ such that $t(g_1) = g_1$ and $t(g_2) = g_2^{-1}$, and set $H = \langle g_1, g_2 \rangle$. Then there exist a tower of Galois extensions $K_p/F/K/\mathbb{Q}$ such that $Gal(F/\mathbb{Q}) \simeq H \rtimes Gal(K/\mathbb{Q})$.*

2.2. p-adic analytic pro-p group. — In this section, we revisit the key ingredients from [**14**] concerning p-adic analytic groups. We shall apply Theorem 2.1 with a p-adic analytic pro-p group H, exploiting the correspondence between $\mathbb{Z}_p$-Lie algebras and p-adic analytic groups. We refer the reader to [**6**] for further details.

Take $p \geqslant 3$ and $r \geqslant 2$. Denote by $\mathrm{GL}_r(\mathbb{Z}_p)$ the general linear group over $\mathbb{Z}_p$, by $\mathrm{SL}_r(\mathbb{Z}_p)$ its subgroup of matrices of determinant 1. Let $O_r(\mathbb{Z}_p)$ be the subgroup of $\mathrm{GL}_r(\mathbb{Z}_p)$ consisting of matrices M satisfying $M^t M = I$, and set $\mathrm{SO}_r(\mathbb{Z}_p) := O_r(\mathbb{Z}_p) \cap \mathrm{SL}_r(\mathbb{Z}_p)$.
For each integer $k \geqslant 1$, let $\varphi_k : \mathrm{GL}_r(\mathbb{Z}_p) \to \mathrm{GL}_r(\mathbb{Z}/p^k\mathbb{Z})$ denote the natural reduction map. We then define the principal congruence subgroups by

$$\mathrm{GL}_r^k(\mathbb{Z}_p) := \ker(\varphi_k), \quad \mathrm{SL}_r^k(\mathbb{Z}_p) := \ker(\varphi_k) \cap \mathrm{SL}_r(\mathbb{Z}_p), \quad \mathrm{SO}_r^k(\mathbb{Z}_p) := \ker(\varphi_k) \cap \mathrm{SO}_r(\mathbb{Z}_p).$$

2.2.1. The $\mathbb{Z}_p$-Lie algebra $\mathfrak{gl}_r$. — Let $\mathfrak{gl}_r(\mathbb{Z}_p)$ denote the free $\mathbb{Z}_p$-module of rank r^2 with basis $\{E_{i,j}\}_{1 \leqslant i,j \leqslant r}$, where $E_{i,j}$ is the (i,j)th elementary matrix. Then $\mathfrak{gl}_r$ becomes a $\mathbb{Z}_p$-Lie algebra with Lie bracket $[A\ B] = AB - BA$. Set $\mathfrak{gl}_r(\mathbb{Q}_p) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{gl}_r$, the $\mathbb{Q}_p$-Lie algebra of all $r \times r$ matrices over $\mathbb{Q}_p$ with the same Lie bracket. For $k \geqslant 1$, let $\mathfrak{gl}_r^k := p^k \mathfrak{gl}(\mathbb{Z}_p)$. Since $[\mathfrak{gl}_r^k\ \mathfrak{gl}_r^k] \subset p\mathfrak{gl}_r^k$, $\mathfrak{gl}_r^k$ is a *powerful* $\mathbb{Z}_p$-Lie algebra (see [**6**, Chapter 9, §9.4]).

The exponential and logarithmic maps $\exp : \mathfrak{gl}_r^1 \to \mathrm{GL}_r^1(\mathbb{Z}_p)$ and $\log : \mathrm{GL}_r^1(\mathbb{Z}_p) \to \mathfrak{gl}_r^1$ are given by $\exp(x) = \sum_{n \geqslant 0} \frac{x^n}{n!}$ and $\log(z) = \sum_{n \geqslant 1} \frac{(-1)^{n+1}}{n}(z-1)^n$. Recall that exp and log are mutually inverse and induce an order-preserving bijection

$$L \longmapsto \exp(L), \qquad G \longmapsto \log(G)$$

between powerful $\mathbb{Z}_p$-Lie subalgebras L of $\mathfrak{gl}_r^1$ and uniform subgroups G of $\mathrm{GL}_r^1(\mathbb{Z}_p)$ ([**6**, Theorem 9.10]). It is well-known that $\exp(\mathfrak{gl}_r^k) = \mathrm{GL}_r^k(\mathbb{Z}_p)$ and that $\mathrm{GL}_r^k(\mathbb{Z}_p)$ is *uniform* for each k (cf. [**6**, Theorem 5.2, §4.1]).

Let $G \subset \mathrm{GL}_r^1(\mathbb{Z}_p)$ be a p-adic analytic group. Then G contains an open uniform subgroup G_0. Let $\mathfrak{g}_0 := \log(G_0)$. Then $\mathfrak{g}_0$ is a powerful $\mathbb{Z}_p$-Lie subalgebra of $\mathfrak{gl}_r^1$. The $\mathbb{Q}_p$-Lie algebra associated with G is defined as $\mathfrak{g}_0(\mathbb{Q}_p) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{g}_0$. This $\mathbb{Q}_p$-Lie algebra is independent of the choice of G_0. Thus, we may unambiguously write $\mathfrak{g}(\mathbb{Q}_p) := \mathfrak{g}_0(\mathbb{Q}_p)$.

2.2.2. The $\mathbb{Z}_p$-Lie algebras $\mathfrak{sl}_r$ and $\mathfrak{so}_r$. — Let $\mathfrak{sl}_r(\mathbb{Z}_p)$ denote the $\mathbb{Z}_p$-Lie subalgebra of $\mathfrak{gl}_r(\mathbb{Z}_p)$ consisting of trace-zero matrices. For each integer $k \geqslant 1$, set $\mathfrak{sl}_r^k := p^k \mathfrak{sl}_r(\mathbb{Z}_p) = \mathfrak{gl}_r^k \cap \mathfrak{sl}_r(\mathbb{Z}_p)$. It follows from $\exp(\mathfrak{sl}_r^1(\mathbb{Z}_p)) = \mathrm{SL}_r(\mathbb{Z}_p)$ that $\exp(\mathfrak{sl}_r^k) = \mathrm{SL}_r^k(\mathbb{Z}_p)$. Since $\mathfrak{sl}_r^k$ is powerful, $\mathrm{SL}_r^k(\mathbb{Z}_p)$ is uniform pro-p of dimension $r^2 - 1$. This equals the $\mathbb{Q}_p$-dimension of the $\mathbb{Q}_p$-Lie algebra $\mathfrak{sl}_r(\mathbb{Q}_p) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{sl}_r(\mathbb{Z}_p)$.

Next, let $\mathfrak{so}_r(\mathbb{Z}_p)$ denote the $\mathbb{Z}_p$-Lie subalgebra of $\mathfrak{gl}_r(\mathbb{Z}_p)$ consisting of matrices M satisfying $M + M^t = 0$. For each integer $k \geqslant 1$, set $\mathfrak{so}_r^k := p^k \mathfrak{so}_r(\mathbb{Z}_p)$. The algebra $\mathfrak{so}_r^k$ is powerful and consequently its exponential $\mathrm{SO}_r^k(\mathbb{Z}_p)$ is a uniform pro-p group. Its dimension is $\frac{r(r-1)}{2}$, equal to the $\mathbb{Q}_p$-dimension of the $\mathbb{Q}_p$-Lie algebra $\mathfrak{so}_r(\mathbb{Q}_p) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{so}_r(\mathbb{Z}_p)$. We shall write $\mathfrak{sl}_r$ (resp. $\mathfrak{so}_r$) for $\mathfrak{sl}_r(\mathbb{Z}_p)$ (resp. $\mathfrak{so}_r(\mathbb{Z}_p)$) whenever no confusion can arise.

2.2.3. Kuranishi pair. — The $\mathbb{Q}_p$-Lie algebras $\mathfrak{sl}_r(\mathbb{Q}_p)$ and $\mathfrak{so}_r(\mathbb{Q}_p)$ are semisimple. The following result is essential to our strategy.

***Theorem 2.5* (Kuranishi [12])**. — *A semisimple $\mathbb{Q}_p$-Lie algebra $\mathscr{L}$ can be generated by 2 elements.*

As a corollary of Theorem 2.5 we get

Corollary 2.6. — *Let $G \subset \mathrm{GL}_r^1(\mathbb{Z}_p)$ be a p-adic analytic group such that $\mathfrak{g}(\mathbb{Q}_p)$ is semisimple. Then there exist two elements g_1 and g_2 in G such that G and the (closed) subgroup H generated by g_1 and g_2 are commensurable.*

The proof is straightforward, but since this observation is essential, we include it.

Proof. — Let G_0 be an open uniform subgroup of G. Let $\mathfrak{g}_0 := \log(G_0)$ be the powerful $\mathbb{Z}_p$-Lie subalgebra of $\mathfrak{gl}_r^1$ associated to G_0, and set $\mathscr{L} := \mathfrak{g}_0(\mathbb{Q}_p) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{g}_0$. By Theorem 2.5, there exist $z_1, z_2 \in \mathscr{L}$ such that $\mathscr{L} = \langle z_1, z_2 \rangle$. After multiplying z_1 and z_2 by some powers of p, we can assume that z_1 and z_2 also belong to $\mathfrak{g}_0$. Set $g_1 = \exp(z_1)$ and $g_2 = \exp(z_2)$, and let $H = \langle g_1, g_2 \rangle$ be the closed subgroup of G_0 generated by g_1 and g_2. Since H is a closed subgroup of a p-adic analytic group G_0, it is itself p-adic analytic. Let H_0 be an open uniform subgroup of H. Then for $n \gg 0$, $g_1^{p^n}$ and $g_2^{p^n}$ are in H_0. Hence the $\mathbb{Z}_p$-Lie algebra $\mathscr{L}_{H_0} := \log(H_0)$ contains both $p^n z_1$ and $p^n z_2$, and then $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathscr{L}_{H_0} = \mathscr{L}$. Thus, H and G are commensurable. □

For what follows, we use the following terminology. Let G (resp. $\mathfrak{g}$) be a p-adic analytic group (resp. a $\mathbb{Z}_p$-Lie algebra). A pair (g_1, g_2) of elements of G (resp. (z_1, z_2) of $\mathfrak{g}$) is called a *Kuranishi pair* of G (resp. of $\mathfrak{g}$) if the closed subgroup generated by g_1 and g_2 (resp. the $\mathbb{Z}_p$-Lie subalgebra generated by z_1 and z_2) is open in G (resp. of finite index in $\mathfrak{g}$).

2.3. A key principle. — Now we explain the principle underlying our approach. We continue to work in the setting of the previous subsection. For a more general treatment, we refer the reader to [**14**]. Let G be a p-adic analytic group whose associated $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}(\mathbb{Q}_p)$ is semisimple. Let G_0 be an open uniform subgroup of G, and let (z_1, z_2) be a Kuranishi pair of $\mathfrak{g}_0 = \log(G_0)$. Set $g_i = \exp(z_i)$ for $i = 1, 2$ and let $H = \langle g_1, g_2 \rangle$. Then H and G are commensurable.
Assume moreover that there exists an element $A \in \mathrm{GL}_r(\mathbb{Z}_p)$ of order 2 satisfying $Az_1A^{-1} = z_1$ and $Az_2A^{-1} = -z_2$. By the equivariance of the exponential map with respect to conjugation, it follows that $Ag_1A^{-1} = g_1$ and $Ag_2A^{-1} = g_2^{-1}$. Hence the conjugation map $t_A : g \mapsto AgA^{-1}$ defines an automorphism of H of order 2. Combining Theorem 2.4 with the above discussion of Kuranishi pairs, we obtain the following.

Theorem 2.7. — *Assume that $p \geqslant 3$ and $r \geqslant 2$. Let $K/\mathbb{Q}$ be an imaginary quadratic field extension such that $p \nmid h_K$. Let $G \subset \mathrm{GL}_r(\mathbb{Q}_p)$ be a p-adic analytic group. Suppose that there exists a Kuranishi pair (g_1, g_2) of G and a matrix $A \in \mathrm{GL}_r(\mathbb{Z}_p)$ of order 2 such that $Ag_1A^{-1} = g_1$ and $Ag_2A^{-1} = g_2^{-1}$. Then there exists a continuous Galois representation $\rho : Gal(K_p/\mathbb{Q}) \to \mathrm{GL}_r(\mathbb{Q}_p)$ such that $\mathrm{im}(\rho)$ and G are commensurable. Moreover, $i(\rho) = |\mathrm{tr}(A)|$.*

Proof. — Set $\Delta' := \langle A \rangle$ and $\Delta = Gal(K/\mathbb{Q}) = \langle s \rangle$. Let $\rho_0 : \Delta \xrightarrow{\simeq} \Delta'$. Now observe that Δ acts on $H = \langle g_1, g_2 \rangle$ and the character of the Δ-module $H^{p,el}$ is given by $\chi(H^{p,el}) =$

$\mathbf{1}+\varphi$. By Theorem 2.4, we get a surjective morphism $\rho : G_{K,p} \rtimes \Delta \twoheadrightarrow H \rtimes \Delta'$, such that $\rho(s) = A$. We conclude by noting that $H \rtimes \Delta' \hookrightarrow \mathrm{GL}_r(\mathbb{Q}_p)$.
Let c denote the (conjugacy class of) complex conjugation. By the Schur-Zassenhaus theorem, A and $\rho(c)$ belong to the same conjugacy class. Hence, we have $i(\rho) = |\mathrm{tr}(A)|$. □

Let G be a uniform subgroup of $\mathrm{GL}_r(\mathbb{Z}_p)$ whose associated $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}(\mathbb{Q}_p)$ is semisimple. To apply Theorem 2.7 with $i(\rho) = a$, we therefore need to find a Kuranishi pair (z_1, z_2) in the $\mathbb{Z}_p$-Lie algebra $\mathfrak{g} := \log(G)$ and a matrix $A \in \mathrm{GL}_r(\mathbb{Z}_p)$ of order 2 satisfying $|\mathrm{tr}(A)| = a$ such that conjugation by A acts as $+1$ on z_1 and as -1 on z_2. In the next section, we verify that these conditions are satisfied for the $\mathbb{Z}_p$-Lie algebras $\mathfrak{sl}_r$ and $\mathfrak{so}_r$.

3. Lie algebra generators compatible with the involution

Let $r \geqslant 2$ be an integer. We fix a partition $r = m + n$ with $m \geqslant n \geqslant 1$, and let $d := d_{m,n}$ denote the $r \times r$ diagonal matrix whose first m diagonal entries are 1 and whose last n diagonal entries are -1. In this section, we refine Theorem 2.5 in the cases of $\mathfrak{sl}_r(\mathbb{Q}_p)$ and $\mathfrak{so}_r(\mathbb{Q}_p)$ by taking into account the involutive automorphism given by conjugation by d. This leads to the following result. Throughout this section, $\mathfrak{sl}_r$ and $\mathfrak{so}_r$ denote $\mathfrak{sl}_r(\mathbb{Z}_p)$ and $\mathfrak{so}_r(\mathbb{Z}_p)$, respectively.

Proposition 3.1. — *Let $\mathfrak{g}$ be either $\mathfrak{sl}_r$ or $\mathfrak{so}_r$, and let $\mathfrak{g}^+$ and $\mathfrak{g}^-$ denote the subspaces of $\mathfrak{g}$ on which the involution $x \to dxd^{-1}$ acts as multiplication by 1 and -1, respectively.*

(1) *There exist $\alpha \in \mathfrak{g}^+$ and $\beta \in \mathfrak{g}^-$ such that the $\mathbb{Z}_p$-Lie subalgebra $\langle \alpha, \beta \rangle$ of $\mathfrak{g}$ has the same $\mathbb{Z}_p$-rank as $\mathfrak{g}$.*
(2) *Assume that $k \in \mathbb{N}$ satisfies $p^k > m(m+2)(m+3)$. Then the elements $\alpha \in \mathfrak{sl}_r^+$ and $\beta \in \mathfrak{sl}_r^-$ may moreover be chosen so that $\langle \alpha, \beta \rangle \supseteq \mathfrak{sl}_r^{2(k-1)(2mn-1)}$.*
(3) *Assume that $k \in \mathbb{N}$ satisfies $p^k > 6(\lfloor m/2 \rfloor + 1) \cdot \lfloor n/2 \rfloor + 2\lfloor m/2 \rfloor$. Then the elements $\alpha \in \mathfrak{so}_r^+$ and $\beta \in \mathfrak{so}_r^-$ may moreover be chosen so that $\langle \alpha, \beta \rangle \supseteq \mathfrak{so}_r^{2(k-1)(mn-1)}$.*

Proposition 3.1 implies that if p is sufficiently large relative to r, then each of $\mathfrak{so}_r$ and $\mathfrak{sl}_r$ admits two generators, one lying in the 1-eigenspace and the other in the -1-eigenspace. The following variant of Proposition 3.1 is obtained by slightly modifying its proof and will be used in the proofs of the main theorems presented in the next section.

Proposition 3.2. — (1) *Assume that $k \in \mathbb{N}$ satisfies $p^k > m(m+2)(m+3)$. Then there exist $\alpha \in p\mathfrak{sl}_r^+$ and $\beta \in p\mathfrak{sl}_r^-$ such that $\langle \alpha, \beta \rangle \supseteq \mathfrak{sl}_r^{4mnk-2k+2}$.*
(2) *Assume that $k \in \mathbb{N}$ satisfies $p^k > 6(\lfloor m/2 \rfloor + 1) \cdot \lfloor n/2 \rfloor + 2\lfloor m/2 \rfloor$. Then there exist $\alpha \in p\mathfrak{so}_r^+$ and $\beta \in p\mathfrak{so}_r^-$ such that $\langle \alpha, \beta \rangle \supseteq \mathfrak{so}_r^{2mnk-2k+2}$.*

We first introduce some notation. For $\mathfrak{g} = \mathfrak{sl}_r$ or $\mathfrak{so}_r$, every element $x \in \mathfrak{g}$ admits a block decomposition

$$x = \begin{pmatrix} A & B_1 \\ B_2 & C \end{pmatrix}, \quad A \in M_m(\mathbb{Z}_p), \quad B_1 \in M_{m,n}(\mathbb{Z}_p), \quad B_2 \in M_{n,m}(\mathbb{Z}_p), \quad C \in M_n(\mathbb{Z}_p).$$

A direct computation shows that $\mathfrak{g}^+$ consists precisely of those elements with $B_1 = 0$ and $B_2 = 0$, whereas $\mathfrak{g}^-$ consists precisely of those for which $A = 0$ and $C = 0$. Accordingly, we write elements of $\mathfrak{g}^+$ and $\mathfrak{g}^-$ as $(A, C)^+$ and $(B_1, B_2)^-$, respectively.

For $\mathfrak{g} = \mathfrak{so}_r$, we further have $B_1^t = -B_2$. Accordingly, for $B \in M_{m,n}(\mathbb{Z}_p)$, we write $(B)_{\mathfrak{so}}$ for the element $(B, -B^t)^- \in \mathfrak{g}^-$. Since conjugation by d is a Lie algebra automorphism of $\mathfrak{g}$, we have $[\mathfrak{g}^- \ \mathfrak{g}^-] \subset \mathfrak{g}^+$. Moreover, each $x \in \mathfrak{g}^+$ induces a $\mathbb{Z}_p$-linear endomorphism $\mathrm{ad}_x : \mathfrak{g}^- \to \mathfrak{g}^-$ of $\mathfrak{g}^-$ defined by $\mathrm{ad}_x(y) := [x\ y]$. We also note that $\mathrm{rk}_{\mathbb{Z}_p}$, which denotes the $\mathbb{Z}_p$-rank, satisfies $\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{sl}_r^- = 2mn$ and $\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{so}_r^- = mn$.

Lemma 3.3. — *For $\mathfrak{g} = \mathfrak{sl}_r$ or $\mathfrak{so}_r$, we have $\mathfrak{g}^+ = [\mathfrak{g}^- \ \mathfrak{g}^-]$.*

Proof. — It suffices to show that $[\mathfrak{g}^- \ \mathfrak{g}^-]$ contains a $\mathbb{Z}_p$-basis of $\mathfrak{g}^+$. For $\mathfrak{g} = \mathfrak{sl}_r$, this follows from the identities

$$(E_{i,j}, 0)^+ = [(E_{i,1}, 0)^- \ (0, E_{1,j})^-], \qquad (0, E_{i,j})^+ = [(0, E_{i,1})^- \ (E_{1,j}, 0)^-]$$

for $i \neq j$, together with the identities $(E_{i,i}, -E_{j,j})^+ = [(E_{i,j}, 0)^- \ (0, E_{j,i})^-]$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Similarly, the claim for $\mathfrak{so}_r$ follows from the identities

$$(E_{i,j} - E_{j,i}, 0)^+ = [(E_{i,1})_{\mathfrak{so}} \ (-E_{j,1})_{\mathfrak{so}}], \qquad (0, E_{i,j} - E_{j,i})^+ = [-(E_{1,i})_{\mathfrak{so}} \ (E_{1,j})_{\mathfrak{so}}],$$

for $i \neq j$. □

We isolate the following technical lemma.

Lemma 3.4. — (1) *If $p^k > m(m+2)(m+3)$, there exist elements $\{\lambda_i\}_{1\leqslant i\leqslant m}$ and $\{\mu_j\}_{1\leqslant j\leqslant n}$ in $\mathbb{Z}_p$ such that $\sum_{i=1}^m \lambda_i + \sum_{j=1}^n \mu_j = 0$ and the $2mn$ elements of $\pm(\lambda_i - \mu_j)$ are pairwise distinct modulo p^k.*

(2) *If $p^k > 6(\lfloor m/2 \rfloor + 1) \cdot \lfloor n/2 \rfloor + 2\lfloor m/2 \rfloor$, then there exist elements $\{\lambda_i\}_{1\leqslant i\leqslant \lfloor m/2 \rfloor}$ and $\{\mu_j\}_{1\leqslant j\leqslant \lfloor n/2 \rfloor}$ in $\mathbb{Z}_p$ such that the elements $\pm\lambda_i \pm \mu_j$, $\pm\mu_j$, $\pm\lambda_i$, 0 are all distinct modulo p^k.*

Proof. — Recall that $m \geqslant n$. To prove (1), set $\lambda_i = -(n+1)i - 1$ for $1 \leqslant i \leqslant m$, $\mu_j = j$ for $1 \leqslant j \leqslant n-1$, and

$$\mu_n = -\sum_{i=1}^{m} \lambda_i - \sum_{j=1}^{n-1} \mu_j = \frac{(n+1)m(m+1)}{2} + m - \frac{n(n-1)}{2}.$$

A direct computation shows that

$$\begin{aligned} |\lambda_i - \mu_j| \leqslant \mu_n - \lambda_m &\leqslant \frac{m(m+1)(n+1)}{2} + m + (n+1)m \\ &\leqslant \frac{m(m+2)(m+1)}{2} + m(m+2) < \frac{p^k}{2}, \end{aligned}$$

and hence $\epsilon(\lambda_i - \mu_j) \equiv \epsilon'(\lambda_{i'} - \mu_{j'}) \pmod{p^k}$, $\epsilon, \epsilon' \in \{\pm 1\}$, if and only if $\lambda_i - \mu_j = \lambda_{i'} - \mu_{j'}$. It therefore remains to show that $\lambda_i - \lambda_{i'} = \mu_j - \mu_{j'}$ implies $i = i'$ and $j = j'$. This is immediate, since $|\mu_j - \mu_{j'}|$ is either less than n or is at least

$$\begin{aligned} \mu_n - \mu_{n-1} &= \frac{(n+1)m(m+1) - n(n-1)}{2} + m - (n-1) \\ &> \frac{nm(m+1)}{2} > (n+1)(m-1) = |\lambda_m - \lambda_1| \geqslant |\lambda_i - \lambda_{i'}|. \end{aligned}$$

To prove (2), set $\mu_j = (\lfloor m/2 \rfloor + 1) \cdot j$ for $1 \leqslant j \leqslant \lfloor n/2 \rfloor$ and $\lambda_i = 2(\lfloor m/2 \rfloor + 1) \cdot \lfloor n/2 \rfloor + i$ for $1 \leqslant i \leqslant \lfloor m/2 \rfloor$. Since $|\lambda_i| + |\mu_j| < p^k/2$, two elements among $\pm\lambda_i \pm \mu_j$, $\pm\mu_j$, $\pm\lambda_i$, 0 can be congruent modulo p^k only if they are equal. Moreover, the inequality $|\lambda_i| > 2|\mu_j|$

implies that $\pm\lambda_i \pm \mu_j \neq \mu_{j'}$ and $\pm\lambda_i \neq \pm\mu_j$. Finally, since $|\lambda_i - \lambda_{i'}| < \lfloor m/2 \rfloor + 1$, we have $\pm\lambda_i \pm \mu_j \neq \pm\lambda_{i'}$ and the elements $\pm\lambda_i \pm \mu_j$ are pairwise distinct. □

Lemma 3.5. — *Let* $\mathrm{M} \in M_d(\mathbb{Z}_p)$ *be diagonalizable over a finite extension* $K/\mathbb{Q}_p$ *with pairwise distinct eigenvalues* $\omega_1, \dots, \omega_d$. *Suppose that there exists an eigenbasis* $\mathrm{x}_1, \dots, \mathrm{x}_d$ *with* $\mathrm{M}\mathrm{x}_i = \omega_i \mathrm{x}_i$ *for all* i *such that* $\mathrm{P} = [\mathrm{x}_1, \dots, \mathrm{x}_d] \in \mathrm{GL}_d(\mathscr{O}_K)$, *where* $\mathscr{O}_K$ *is the ring of integers of* K. *Then, for any* $\mathrm{v} = \sum_{i=1}^d \alpha_i \mathrm{x}_i \in \mathbb{Z}_p^d$ *with* $\alpha_i \in \mathscr{O}_K^\times$, *the* $\mathbb{Z}_p$*-submodule* $L = \sum_{j=0}^{d-1} \mathbb{Z}_p \mathrm{M}^j \mathrm{v}$ *of* $\mathbb{Z}_p^d$ *contains* $p^N \mathbb{Z}_p^d$, *where*

$$p^N = \max_{1 \leqslant i \leqslant d} \left\{ \prod_{j \neq i} |\omega_i - \omega_j|_p^{-1} \right\}.$$

Here, $|\cdot|_p$ *denotes the* p*-adic absolute valuation normalized by* $|p|_p = p^{-1}$.

Proof. — Since $\mathrm{M}^j\mathrm{v} = \sum_{i=1}^d \alpha_i \omega_i^j \mathrm{x}_i$, we obtain $\mathrm{A} := \left[\mathrm{v}, \mathrm{M}\mathrm{v}, \dots, \mathrm{M}^{d-1}\mathrm{v} \right] = \mathrm{PDV}$, where D denotes the diagonal matrix $\mathrm{diag}(\alpha_1, \dots, \alpha_d)$ and $\mathrm{V} = V(\omega_1, \dots, \omega_d)$ is the Vandermonde matrix. In particular, A is invertible and L has finite index in $\mathbb{Z}_p^d$. The inclusion $p^N \mathbb{Z}_p^d \subseteq L$ is equivalent to $p^N \mathrm{A}^{-1} \in M_d(\mathbb{Z}_p)$. If $d = 2$, then $p^N = |\det(V)|_p^{-1}$, so that $p^N V^{-1} \in \mathrm{GL}_2(\mathscr{O}_K)$. Hence, we have $p^N A^{-1} \in \mathrm{GL}_2(\mathscr{O}_K) \cap M_2(\mathbb{Z}_p) = \mathrm{GL}_2(\mathbb{Z}_p)$. Assume henceforth that $d \geqslant 3$. Since the (i,j)th minor of the generic Vandermonde matrix $V(y_1, \dots, y_d)$ vanishes after specializing to $y_a = y_b$ for any distinct $a, b \neq i$, each entry of V^{-1} has a denominator dividing $\prod_{j \neq i}(\omega_i - \omega_j)$ for some $1 \leqslant i \leqslant d$. Thus, we have $p^N \mathrm{V}^{-1} \in \mathrm{GL}_d(\mathscr{O}_K)$, and the proof is completed exactly as in the case $d = 2$. □

Proof of Proposition 3.1. — For the case $\mathfrak{g} = \mathfrak{sl}_r$, let $k \in \mathbb{N}$ satisfy $p^k > m(m+2)(m+3)$. Let A and C be the diagonal matrices with diagonal entries $\{\lambda_i\}_{1 \leqslant i \leqslant m}$ and $\{\mu_j\}_{1 \leqslant j \leqslant n}$, respectively, as in Lemma 3.4 (1). Set $\alpha = (A, C)^+ \in \mathfrak{sl}_r^+$. Then the set

$$\mathscr{B}_{\mathfrak{sl}} := \{(E_{i,j}, 0)^-, (0, E_{j,i})^- \mid 1 \leqslant i \leqslant m, \quad 1 \leqslant j \leqslant n\}$$

is an eigenbasis for ad_α whose eigenvalues are $\{\pm(\lambda_i - \mu_j)\}_{i,j}$. The eigenbasis $\mathscr{B}_{\mathfrak{sl}}$ also forms a natural $\mathbb{Z}_p$-basis of $\mathfrak{sl}_r^- \cong \mathbb{Z}_p^{2mn}$.
Now define $\beta = \sum_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n} \left((E_{i,j}, 0)^- + (0, E_{j,i})^- \right) \in \mathfrak{sl}_r^-$. Then β satisfies the hypothesis on v in Lemma 3.5 with respect to the eigenbasis $\mathscr{B}_{\mathfrak{sl}}$. Moreover, by Lemma 3.4 (1), no difference of two distinct eigenvalues is divisible by p^k. Hence Lemma 3.5 yields

$$(\star) \qquad L := \sum_{j=0}^{\mathrm{rk}_{\mathbb{Z}_p} \mathfrak{sl}_r - 1} \mathbb{Z}_p \mathrm{ad}_\alpha^j(\beta) \supseteq p^{(k-1)(\mathrm{rk}_{\mathbb{Z}_p} \mathfrak{sl}_r^- - 1)} \mathfrak{sl}_r^- = p^{(k-1)(2mn-1)} \mathfrak{sl}_r^-.$$

Furthermore, Lemma 3.3 yields $[L\ L] \supseteq p^{2(k-1)(2mn-1)} \mathfrak{sl}_r^+$. Therefore, we have

$$\langle \alpha, \beta \rangle \supseteq L + [L\ L] \supseteq p^{(k-1)(2mn-1)} \mathfrak{sl}_r^- + p^{2(k-1)(2mn-1)} \mathfrak{sl}_r^+ \supset p^{2(k-1)(2mn-1)} \mathfrak{sl}_r.$$

Let us now consider the case $\mathfrak{g} = \mathfrak{so}_r$. We first note that $\mathfrak{so}_r^+ = 0$ if and only if $m = n = 1$. In this case, we may take $\alpha = 0$ and let β be a $\mathbb{Z}_p$-generator of $\mathfrak{so}_2^- \cong \mathbb{Z}_p$. Hence, we may assume that $m \geqslant 2$.
Let $k \in \mathbb{N}$ satisfy $p^k > 6(\lfloor m/2 \rfloor + 1) \cdot \lfloor n/2 \rfloor + 2\lfloor m/2 \rfloor$, and let $\alpha = (A, C)^+ \in \mathfrak{so}_r^+$, where

$$A = \sum_{i=1}^{\lfloor m/2 \rfloor} \lambda_i (E_{2i,2i-1} - E_{2i-1,2i}) \in M_m(\mathbb{Z}_p), \quad C = \sum_{j=1}^{\lfloor n/2 \rfloor} \mu_j (E_{2j,2j-1} - E_{2j-1,2j}) \in M_n(\mathbb{Z}_p)$$

with λ_i and μ_j as in Lemma 3.4 (2). Fix a square root z of -1. Then, for each $1 \leqslant i \leqslant \lfloor m/2 \rfloor$, the vectors

$$\hat{v}_i := ze_{2i-1} + e_{2i} \in \mathbb{Q}_p(z)^m, \quad \tilde{v}_i := -ze_{2i-1} + e_{2i} \in \mathbb{Q}_p(z)^m$$

are eigenvectors of A with eigenvalues $\lambda_i z$ and $-\lambda_i z$, respectively. If m is odd, then the standard basis vector $e_m \in \mathbb{Q}_p^m$ is an eigenvector of A with eigenvalue 0. Similarly, for each $1 \leqslant j \leqslant \lfloor n/2 \rfloor$, let $\hat{w}_j$ and $\tilde{w}_j$ denote the eigenvectors of C with eigenvalues $\mu_j z$ and $-\mu_j z$, respectively. If n is odd, then $e_n \in \mathbb{Q}_p^n$ is also an eigenvector of C. Since the eigenvalues of A and C are simple, the above eigenvectors form eigenbases $\mathscr{B}_A$ and $\mathscr{B}_C$ of A and C, respectively.
By abuse of notation, we also write $(B)_{\mathfrak{so}}$ for the corresponding element of $\mathscr{O}_{\mathbb{Q}_p(z)} \otimes_{\mathbb{Z}_p} \mathfrak{so}_r^-$, whenever $B \in M_{m,n}(\mathscr{O}_{\mathbb{Q}_p(z)})$. Then $\mathscr{B}_{\mathfrak{so}} := \{(x \cdot y^t)_{\mathfrak{so}} \mid x \in \mathscr{B}_A, y \in \mathscr{B}_C\} \subset \mathbb{Q}_p(z) \otimes_{\mathbb{Z}_p} \mathfrak{so}_r^-$ forms an eigenbasis of ad_α. Indeed, we have

$$\mathrm{ad}_\alpha((x \cdot y^t)_{\mathfrak{so}}) = (Ax \cdot y^t)_{\mathfrak{so}} - (x \cdot y^t C)_{\mathfrak{so}} = (Ax \cdot y^t)_{\mathfrak{so}} + (x \cdot (Cy)^t)_{\mathfrak{so}}.$$

By Lemma 3.4 (2), the eigenvalues of ad_α are pairwise distinct modulo p^k.
To apply Lemma 3.5, we identify $\mathfrak{so}_r^-$ with $\mathbb{Z}_p^{mn}$ via the $\mathbb{Z}_p$-basis $\{(E_{ij})_{\mathfrak{so}}\}_{i,j}$. Under this identification, the eigenbasis $\mathscr{B}_{\mathfrak{so}}$ satisfies the hypothesis on P in Lemma 3.5, since the change-of-basis matrices from the standard bases of $\mathbb{Q}_p^m$ (resp. $\mathbb{Q}_p^n$) to the eigenbasis $\mathscr{B}_A$ (resp. $\mathscr{B}_C$) belongs to $\mathrm{GL}_m(\mathscr{O}_{\mathbb{Q}_p(z)})$ (resp. $\mathrm{GL}_n(\mathscr{O}_{\mathbb{Q}_p(z)})$). We next observe that $\hat{v}_i + \tilde{v}_i = 2e_{2i} \in \mathbb{Z}_p^m$ and $\hat{w}_j + \tilde{w}_j = 2e_{2j} \in \mathbb{Z}_p^n$. Hence, the element $\beta = (S)_{\mathfrak{so}} \in \mathfrak{so}_r^-$, where

$$S = \left(\sum_{i=1}^{\lfloor m/2 \rfloor} (\hat{v}_i + \tilde{v}_i) + (m - 2\lfloor m/2 \rfloor)e_m \right) \cdot \left(\sum_{j=1}^{\lfloor n/2 \rfloor} (\hat{w}_j + \tilde{w}_j) + (n - 2\lfloor n/2 \rfloor)e_n \right)^t \in M_{m,n}(\mathbb{Z}_p)$$

satisfies the hypothesis on v in Lemma 3.5. The proof now proceeds exactly as in the $\mathfrak{sl}_r$ case. □

Proof of Proposition 3.2. — Let $\mathfrak{g}$ be either $\mathfrak{sl}_r$ or $\mathfrak{so}_r$. Let α and β be as in the proof of Proposition 3.1 and set $\alpha' = p\alpha$ and $\beta' = p\beta$. Since $\mathrm{ad}_{\alpha'}^j(\beta') = p^{j+1}\mathrm{ad}_\alpha^j(\beta)$, by $(\star)$, we obtain

$$L' := \sum_{j=0}^{\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{g}^- - 1} \mathbb{Z}_p \mathrm{ad}_{\alpha'}^j(\beta') \supseteq p^{\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{g}^-} \cdot p^{(k-1)\cdot(\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{g}^- - 1)}\mathfrak{g}^- = p^{k\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{g}^- - k + 1}\mathfrak{g}^-.$$

The claim now follows from $\langle \alpha', \beta' \rangle \supset [L'\, L'] + L'$. □

4. Proof of the main theorems

With the Lie algebra generators established in the previous section, we are now ready to prove the main theorems.

Proof of Theorem 1. — Let $p \geqslant 3$ be a prime and $r \geqslant 2$ an integer. For $a \in \mathbb{Z}$ satisfying $\epsilon(r) \leqslant a \leqslant r-2$ and $a \equiv r \pmod 2$, there exists a partition $r = m+n$ such that $m-n = a$. Let k be an integer satisfying $p^k > m(m+2)(m+3)$ and set $\gamma = 4kmn - 2k + 2$.
Let $\mathfrak{sl}_r^\pm$ be the ± 1-eigenspaces of $\mathfrak{sl}_r$ with respect to the conjugation action by $d_{m,n}$. By Proposition 3.2 (1), there exist $\alpha \in p\mathfrak{sl}_r^+$ and $\beta \in p\mathfrak{sl}_r^-$ such that the $\mathbb{Z}_p$-Lie subalgebra $\langle \alpha, \beta \rangle$ of $\mathfrak{sl}_r^1$ contains $\mathfrak{sl}_r^\gamma$. Set $g_1 = \exp(\alpha), g_2 = \exp(\beta)$, and let H be the closed subgroup

of $\mathrm{SL}_r^1(\mathbb{Z}_p)$ generated by g_1 and g_2. Then (g_1, g_2) is a Kuranishi pair of $\mathrm{SL}_r(\mathbb{Z}_p)$. Moreover, we have

$$H \supseteq \exp(\mathfrak{sl}_r^\gamma) = \mathrm{SL}_r^\gamma(\mathbb{Z}_p).$$

Now take $K = \mathbb{Q}(\sqrt{-p})$. Since $p \nmid h_K$ by Example 2.3, and 2 is ramified in $K/\mathbb{Q}$ if and only if $p \equiv 3 \pmod 4$, Theorem 2.7 yields statements (1) and (2).
The first assertion of (3) follows from the fact that, for any complex conjugation $c \in G_\mathbb{Q}$, we have $\rho \otimes \omega(c) = -\rho(c)$, and hence

$$\mathrm{tr}(\rho \otimes \omega(c)) = -\mathrm{tr}(\rho(c)) = -\mathrm{tr}(A) = -a.$$

For the second assertion, note that every open subgroup of $\mathrm{SL}_r(\mathbb{Z}_p)$ has finite abelianization. Hence for some open subgroup U of $\mathrm{Gal}(K_p/\mathbb{Q})$, we have $(\rho \otimes \omega)(U) \cong \rho(U) \times \mathbb{Z}_p$. It follows that $\mathrm{im}(\rho \otimes \omega) \subset \mathrm{GL}_r(\mathbb{Z}_p)$ has dimension r^2 as a p-adic analytic group. Since this coincides with the dimension of $\mathrm{GL}_r(\mathbb{Z}_p)$, the image $\mathrm{im}(\rho \otimes \omega)$ is open in $\mathrm{GL}_r(\mathbb{Z}_p)$. □

Proof of Theorem 2. — The proof is obtained by adapting the argument of Theorem 1 to $\mathfrak{so}_r$. Let $m + n = r$ with $m - n = a$, and let $k \in \mathbb{N}$ satisfy

$$p^k > \frac{3n(m+2)}{2} + m.$$

Set $\gamma := 2kmn - 2k + 2$. By Proposition 3.2 (2) applied to $d_{m,n}$, there exist $\alpha \in p\mathfrak{so}_r^+$ and $\beta \in p\mathfrak{so}_r^-$ such that the $\mathbb{Z}_p$-Lie subalgebra $\langle \alpha, \beta \rangle$ contains $\mathfrak{so}_r^\gamma$. Passing to the exponential map, the closed subgroup of $\mathrm{SO}_r^1(\mathbb{Z}_p)$ generated by $\exp(\alpha)$ and $\exp(\beta)$ contains the open subgroup $\mathrm{SO}_r^\gamma(\mathbb{Z}_p)$ of $\mathrm{SO}_r(\mathbb{Z}_p)$. The remainder of the proof is identical to that of Theorem 1. Note that $A = d_{m,n}$ has order 2 whereas $\mathrm{SO}_r^1(\mathbb{Z}_p)$ is torsion-free, being uniform. Hence, $\mathrm{SO}_r^1(\mathbb{Z}_p) \rtimes A$ embeds naturally into $\mathrm{O}_r(\mathbb{Z}_p)$, and the image of Galois representation $\rho : G_\mathbb{Q} \to \mathrm{SO}_r^1(\mathbb{Z}_p) \rtimes \langle A \rangle$ constructed above is contained in $\mathrm{O}_r(\mathbb{Z}_p)$. □

Remark 4.1. — In all previous works on non-geometric Galois representations, the resulting Galois representations are regular at infinity. For the constructions in **[17, 15, 16, 18]**, this can be checked from the description of the residual mod p representation: see §2.1 of **[17]**, Theorem 4.3(1) of **[15]**, Theorem 3.3(2) of **[16]**, and Condition (3) of Theorem 3.10 in **[18]**. In **[7]**, the action of Δ' on H is given, in our notation, by conjugation by a diagonal matrix whose diagonal entries alternate in parity (cf. Proposition 6.1). A similar argument appears in §3.4 of **[5]**, while the corresponding argument in **[14]** can be found in §4.2.

References

[1] Joël Bellaïche and Gaëtan Chenevier, *The sign of Galois representations attached to automorphic forms for unitary groups*, Compos. Math. **147** (2011), no. 5, 1337–1352. MR 2834723

[2] Frank Calegari, *Even Galois representations*, notes available at author's web page.

[3] _____, *Even Galois representations and the Fontaine–Mazur conjecture. II*, J. Amer. Math. Soc. **25** (2012), no. 2, 533–554. MR 2869026

[4] Ana Caraiani and Bao V. Le Hung, *On the image of complex conjugation in certain Galois representations*, Compos. Math. **152** (2016), no. 7, 1476–1488. MR 3530448

[5] Christophe Cornut and Jishnu Ray, *Generators of the pro-p Iwahori and Galois representations*, Int. J. Number Theory **14** (2018), no. 1, 37–53. MR 3726241

[6] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, second ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999. MR 1720368

[7] Ralph Greenberg, *Galois representations with open image*, Ann. Math. Qué. **40** (2016), no. 1, 83–119. MR 3512524

[8] Benedict H. Gross, *Odd Galois representations*.

[9] Farshid Hajir and Christian Maire, *Prime decomposition and the Iwasawa MU-invariant*, Math. Proc. Cambridge Philos. Soc. **166** (2019), no. 3, 599–617. MR 3933912

[10] Nicholas M. Katz, *A note on Galois representations with big image*, Enseign. Math. **65** (2019), no. 3-4, 271–301. MR 4113044

[11] Chandrashekhar B. Khare and Michael Larsen, *Liftable groups, negligible cohomology and Heisenberg representations*, Arithmetic geometry, Tata Inst. Fundam. Res. Stud. Math., vol. 41, Tata Inst. Fund. Res., Mumbai, [2024] ©2024, pp. 315–344. MR 4812707

[12] Masatake Kuranishi, *Two elements generations on semi-simple Lie groups*, Kodai Math. Sem. Rep. **1** (1949), no. 5-6, 9–10. MR 34766

[13] Stéphane R. Louboutin, *The Brauer-Siegel theorem*, J. London Math. Soc. (2) **72** (2005), no. 1, 40–52. MR 2145727

[14] Christian Maire, *On Galois representations with large image*, Trans. Amer. Math. Soc. **376** (2023), no. 10, 7087–7106. MR 4636685

[15] Simone Maletto, *Galois representations with big image in the general symplectic group* $\mathrm{GSp}_4(\mathbb{Z}_p)$, J. Number Theory **244** (2023), 204–223. MR 4503067

[16] Anwesh Ray, *Constructing Galois representations ramified at one prime*, J. Number Theory **222** (2021), 168–180. MR 4215811

[17] ———, *Galois representations ramified at one prime and with suitably large image*, Trans. Amer. Math. Soc. **376** (2023), no. 10, 7287–7305. MR 4636690

[18] Shiang Tang, *A note on Galois representations valued in reductive groups with open image*, J. Number Theory **243** (2023), 1–12. MR 4492604

[19] Richard Taylor, *The image of complex conjugation in l-adic representations associated to automorphic forms*, Algebra Number Theory **6** (2012), no. 3, 405–435. MR 2966704

[20] Kay Wingberg, *Free quotients of Demuskin groups with operators*, (2004).

August 4, 2026

Donghyeok Lim, Department of Mathematics Education, Korea National University of Education, Cheongju 28173, South Korea • *E-mail :* donghyeokklim@gmail.com

Christian Maire, Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, F-25000 Besançon, France • *E-mail :* christian.maire@univ-fcomte.fr