ON GALOIS REPRESENTATIONS WITH LARGE IMAGE

by

Christian Maire

Abstract. — For every prime number $p \geqslant 3$ and every integer $m \geqslant 1$, we prove the existence of a continuous Galois representation $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ which has open image and is unramified outside $\{p, \infty\}$ (resp. outside $\{2, p, \infty\}$) when $p \equiv 3 \bmod 4$ (resp. $p \equiv 1 \bmod 4$).

Let K be a number field having r_2 non-real embeddings, let p be a prime number and let G be a finitely generated pro-p group of p-rank at most $r_2 + 1$. When the field K is p-rational (see §1.2 for the full definition and background), the Galois group of the maximal p-extension of K unramified outside p is a free pro-p group of rank $r_2 + 1$. Hence the group G can be realized as the Galois group of an extension over K unramified outside p, thanks to the universal property of free groups. In the context of Galois representations, Greenberg in [**11**] developed this approach to realize continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ of the absolute Galois $G_{\mathbb{Q}}$ of $\mathbb{Q}$, with open image and such that ρ is unramified outside $\{p, \infty\}$, under the hypotheses that p is a regular prime and m satisfies $1 + 4[m/2] \leqslant p$. The regularity of p is important because for the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, it is equivalent to the p-rationality of K.

A few years later this method was extended by Cornut and J. Ray [**4**] for more general linear groups, but always under the assumption that p is regular and that all large m are excluded when p is fixed.

In fact, it is possible to relax the condition on p-rationality to realize Galois representations with big image: this has been recently done by A. Ray in [**21**]. For example, when $p \geqslant 2^{m+2+2e_p}$, where e_p is the index of irregularity of p, A. Ray shows the existence of continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$ with open image. But as in [**11**] and [**4**], the dimension of the representations is bounded for fixed p.

2000 ***Mathematics Subject Classification.*** — 11F80, 11R37, 11R32.

Key words and phrases. — Galois representations, uniform groups, pro-p extensions unramified outside p.

The author thanks Ralph Greenberg for his feedback, Ravi Ramakrishna for interesting exchanges and for the careful reading of the paper, Farshid Hajir for his strong encouragement and comments, Anwesh Ray for many useful and inspiring discussions, Cécile Armana for useful remarks, Jean-Marc Couveignes, Georges Gras and Jan Mináč for discussions and encouragement. This work was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002).

By a different approach, Katz in [**13**] constructs geometric Galois representations over cyclotomic extensions, and by descent he gets finitely ramified continuous Galois representations of $G_{\mathbb{Q}}$ with open image in $Gl_m(\mathbb{Z}_p)$, for $p \equiv 1 \bmod 3$ or $p \equiv 1 \bmod 4$ for every even $m \geqslant 6$. In particular, for such primes p, the result of Katz shows the existence of Galois representations with open image for large m. We note that the representations constructed by Katz are motivic but are ramified at sets consisting of primes of potentially many different residue characteristics, whereas the earlier approach yields representations unramified outside $\{p, \infty\}$ which are, by contrast, what Katz calls "non-motivic".

In this work, by extending the arithmetical approaches of [**11**], [**4**] and [**21**], we are able to prove (Corollary 4.4):

Theorem A. — *Given a prime number $p \geqslant 3$, and an integer $m \geqslant 1$, there exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ with open image satisfying:*

(*i*) *ρ is unramified ouside $\{p, \infty\}$ if $p \equiv -1 \bmod 4$,*

(*ii*) *ρ is unramified ouside $\{2, p, \infty\}$ if $p \equiv 1 \bmod 4$, and has potentially good reduction at* 2.

Remark. — *The representations we construct have the property that "half" of the eigenvalues of complex conjugation are $+1$, the others being -1.*

Remark. — *For $m = 1$ take the $\mathbb{Z}_p$-extension of $\mathbb{Q}$.*

Our criteria coincide with those of Greenberg when the number field K fixed by the residual representation is p-rational. However our approach also works in greater generality. In particular by passing through the number field $K = \mathbb{Q}(\zeta_p)$, the criteria we give are specially adapted to produce, for many primes $p \equiv 1 \bmod 4$ and large m, continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ ramified only at $\{p, \infty\}$ with open image. In fact, this is the case for all but six primes $p \equiv 1 \bmod 4$ less than $4 \cdot 10^5$. The main technical result we obtain can be viewed as a refinement of Theorem A, (*ii*). To explain it, let v_2 be the 2-adic valuation, and let ω be the mod p reduction of the cyclotomic character. We prove (Theorem 4.6):

Theorem B. — *Let $p \equiv 1 \bmod 4$ be a prime number, and let $m \geqslant 3$. Write $p - 1 = 2^\lambda a$ where $2 \nmid a$, so $\lambda = v_2(p-1)$. Let $\{\omega^{k_1}, \cdots, \omega^{k_e}\}$ be the characters corresponding to the nontrivial components of the p-Sylow of the class group of $\mathbb{Q}(\zeta_p)$. Suppose that:*

(*i*) *$v_2(m-1) \geqslant \lambda$ if m is odd and $v_2(m-2) \geqslant \lambda$ if m is even;*

(*ii*) *$a \nmid (k_i - 1)$ for $i = 1, \cdots, e$.*

Then there exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$, and with open image.

Example. — *For $p \leqslant 4 \cdot 10^5$, there are only six cases for which* (*ii*) *fails, and the index of irregularity e is 1 for all of them:*

p	257	3329	11777	114689	163841	184577
k_1	93	1951	8879	34343	140801	49029

.

Here is a sketch of our approach. We first revisit the question of the lifting of residual Galois representations (of order coprime to p) in terms of embedding problems, by using the criteria of Hoechsmann (see for example [**19**, Chapter III, §5]). The result we obtain involves the adjoint representation of a uniform group G (Theorem 3.3). We then exploit a result of Kuranishi [**14**] that shows that a semisimple Lie algebra can be generated by 2 elements; in particular we use the explicit form for $\mathfrak{sl}_m$ recently given by Detinko-De Graaf [**5**], and Chistopolskaya [**3**]. Thus we apply our embedding criteria to some special subgroup H of $Sl_m(\mathbb{Z}_p)$ generated by two elements. Instead of considering number fields of large degree, namely $\mathbb{Q}(\zeta_p)$, we reduce the study of the existence of Galois representations with open image, to properties of certain imaginary quadratic extensions.

In this work we restrict our attention to the problem introduced by Greenberg [**11**] for the group $Sl_m(\mathbb{Z}_p)$. But it seems likely the methods we introduce will apply more generally for realizing other groups as well.

The paper contains 4 sections. In Section 2 and in Section 3, we recall facts about the maximal pro-p-extension of a number field unramified outside p, and generalities regarding uniform groups and $\mathbb{Z}_p$-Lie algebras. In Section 4, we develop the approach of lifting mod p^k representations via the embedding problem; in particular we give criteria for lifting in some given uniform group (Theorem 3.3). The last section is devoted to applications; in particular we prove the results presented in the Introduction.

Notations. Throughout this article p is a prime number.
• If M is a finitely generated $\mathbb{Z}_p$-module, set $d_pM := dim_{\mathbb{F}_p}M/M^p$, $M[p] := \{m \in M, pm = 0\}$, and $Tor(M) = \{m \in M, \exists k, p^km = 0\}$.
• If G is a pro-p group, set $G^{ab} := G/[G,G]$, $G^{p,el} := G^{ab}/(G^{ab})^p$, and $d_pG := d_pG^{ab}$.
• If A is a Hausdorff, abelian and locally compact topological group, set $A^\wedge$ to be Pontryagin dual of A.

For the computations we have used the program PARI/GP [**20**].

1. On the maximal pro-p extension unramified outside p: the results we need

1.1. On pro-p groups. — For classical properties on cohomology and homology of pro-p groups, see for example [**19**, Chapters I and II].
Let $1 \longrightarrow G \longrightarrow \Gamma \longrightarrow \Delta \longrightarrow 1$ be an exact sequence of profinite groups where G is a finitely presented pro-p group, and Δ is a finite group of order coprime to p. Recall that by the Schur-Zassenhaus Theorem one has $\Gamma \simeq G \ltimes \Delta$.

Proposition 1.1. — *Let M be a finite Γ-module of exponent p on which G acts trivially. Then for $i \geqslant 1$, we have the isomorphism: $H^i(\Gamma, M) \simeq (H^i(G,\mathbb{Z}/p) \otimes M)^\Delta$.*

Proof. — First, by the algebraic universal coefficients Theorem for G-homology over $\mathbb{F}_p$, one has the isomorphism

$$F : H_i(G,\mathbb{Z}/p) \otimes M^\wedge \xrightarrow{\sim} H_i(G, M^\wedge), \qquad (1)$$

where the tensor product is taken over $\mathbb{F}_p$, and where F is defined by

$$F([f] \otimes m) = [f \otimes m],$$

showing that (1) is also an isomorphism of Δ-modules. See for example [**12**, Chapter VI, §15, Theorem 15.1]. By Pontryagin duality, we obtain $H^i(G,M) \simeq H^i(G,\mathbb{Z}/p) \otimes M$, as Δ-modules. Since $|\Delta|$ is coprime to p, by the Hochschild-Serre spectral sequence one also has $H^i(\Gamma, M) \simeq H^i(G,M)^\Delta$ (see for example [**19**, Chapter II, §1, Lemma 2.1.2]). By combining these two observations we finally obtain the claimed isomorphism. □

Let us write $G^{ab} \simeq \mathbb{Z}_p^t \oplus \mathscr{T}$, where $\mathscr{T}$ is the torsion subgroup of G^{ab}.

Proposition 1.2. — *Let M be a finite Γ-module of exponent p on which G acts trivially. If $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p) = 0$ then $H^2(G,M) \simeq \big(\mathscr{T}[p]^\wedge \otimes M\big)^\Delta$.*

Proof. — By taking the G-homology of the exact sequence $0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$, we get the exact sequence of $\mathbb{F}_p[\Delta]$-modules

$$H_2(G,\mathbb{Z}_p)/p \longrightarrow H_2(G,\mathbb{Z}/p) \twoheadrightarrow H_1(G,\mathbb{Z}_p)[p].$$

After observing that $H_2(G,\mathbb{Z}_p)^\wedge \simeq H^2(G,\mathbb{Q}_p/\mathbb{Z}_p) = 0$, then $H^2(G,\mathbb{Z}/p)$ is isomorphic to $\big(H_1(G,\mathbb{Z}_p)[p]\big)^\wedge \simeq \mathscr{T}[p]^\wedge$, and we conclude by Proposition 1.1. □

By the way, the proof of Proposition 1.2 allows us to obtain:

Proposition 1.3. — *One has*

$$d_pH^1(G,\mathbb{Z}/p) - d_pH^2(G,\mathbb{Z}/p) = t - d_pH_2(G,\mathbb{Z}_p).$$

1.2. Restricted ramification. — Let K be a number field. To simplify when $p = 2$ we assume K totally imaginary. Set

- $E_K := \mathbb{Z}_p \otimes \mathscr{O}_K^\times$ the pro-p completion of the group of units of the ring of integers $\mathscr{O}_K$ of K,
- Cl_K the p-Sylow subgroup of the class group of K,
- $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}|p$, $U_\mathfrak{p}$ the local units of $K_\mathfrak{p}$,
- $\mathscr{U}_\mathfrak{p} := \varprojlim_n U_\mathfrak{p}/U_\mathfrak{p}^{p^n}$ the pro-p completion of $U_\mathfrak{p}$, and $\mathscr{U}_p := \prod_{\mathfrak{p}|p} \mathscr{U}_\mathfrak{p}$,
- $\iota_{K,p} : E_K \to \mathscr{U}_p$ the diagonal embedding of E_K into p-adic units.

1.2.1. The pro-p group $G_{K,p}$. — Let K_p/K be the maximal pro-p extension of K unramified outside p; set $G_{K,p} = Gal(K_p/K)$. The pro-p group $G_{K,p}$ is finitely presented. More precisely, one has (see [**19**, Chapter VIII, Proposition 8.3.18; Chapter X, Corollary 10.4.9, Theorem 10.7.13]):

Theorem 1.4. — *The pro-p group $G_{K,p}$ is of cohomological dimension 1 or 2, and $d_pH^1(G_{K,p},\mathbb{Z}/p) - d_pH^2(G_{K,p},\mathbb{Z}/p) = r_2 + 1$.*

Here as usual (r_1, r_2) is the signature of K.
Let us write $G_{K,p}^{ab} \simeq \mathscr{F}_{K,p} \oplus \mathscr{T}_{K,p}$, where $\mathscr{T}_{K,p} := Tor(G_{K,p}^{ab})$ is the torsion of $G_{K,p}^{ab}$, and where $\mathscr{F}_{K,p} := G_{K,p}^{ab}/\mathscr{T}_{K,p} \simeq \mathbb{Z}_p^{t_p}$ is the free part; the quantity t_p is the $\mathbb{Z}_p$-rank of $G_{K,p}^{ab}$. By class field theory one has:

$$t_p = dim_{\mathbb{Q}_p} coker(\iota_{K,p}) = r_2 + 1 + dim_{\mathbb{Q}_p} ker(\iota_{K,p}). \tag{2}$$

(See for example [**8**, Chapter III, §1, Corollary 1.6.3].)
Recall also that Leopoldt's conjecture asserts that $ker(\iota_{K,p}) = 1$, and thanks to Baker and Brumer [**2**] one knows that Leopoldt's conjecture is true for abelian extensions $K/\mathbb{Q}$. One also has the following well-known result (see for example [**19**, Chapter X, Corollary 10.3.7]):

Proposition 1.5. — *One has $ker(\iota_{K,p}) = 1 \iff H_2(G_{K,p},\mathbb{Z}_p) = 1$.*

Proof. — By Proposition 1.3 and Theorem 1.4 one has:

$$t_p - d_pH_2(G_{K,p},\mathbb{Z}_p) = r_2 + 1;$$

thus by combining with (2), we get: $dim_{\mathbb{Q}_p}ker(\iota_{K,p}) = d_pH_2(G_{K,p},\mathbb{Z}_p)$. Observe now that $H_2(G_{K,p},\mathbb{Z}_p)$ is an abelian pro-p group, so $H_2(G_{K,p},\mathbb{Z}_p)$ is trivial if and only if $d_pH_2(G_{K,p},\mathbb{Z}_p) = 0$. □

Regarding $\mathscr{T}_{K,p}$, we have the following:

Proposition 1.6. — *Suppose $Cl_K = 1$. Then $\mathscr{T}_{K,p} \simeq Tor\Big(\mathscr{U}_p/\iota_{K,p}(E_K)\Big)$.*

Proof. — By class field theory one has $\mathscr{U}_p/\iota_{K,p}(E_K) \simeq G^{ab}_{K,p}$ when $Cl_K = 1$. □

Hence, given a number field K, up to a finite set of primes (those that divide $|Cl_K|$) the computation of $\mathscr{T}_{K,p}$ is reduced to the computation of the torsion of $\mathscr{U}_p/\iota_{K,p}(E_K)$. And having some nontrivial element in $Tor\big(\mathscr{U}_p/\iota_{K,p}(E_K)\big)$ is something that is rare; one has the following conjecture ([**7**, Conjecture 8.11]).

Conjecture 1.7 **(Gras)**. — *Given a number field K, then $\mathscr{T}_{K,p} = 1$ for $p \gg 0$.*

Regarding this conjecture many computations provide some evidence, but very little is known in general. See [**8**, Chapter IV, §3 and §4] and [**9**] for a good exposition. Nevertheless, the p-group $\mathscr{T}_{K,p}$ is a deep arithmetical object associated to K, as we can see from the following result, for example.

Proposition 1.8. — *The pro-p group $G_{K,p}$ is free pro-p (on $r_2 + 1$ generators) if and only if $ker(\iota_{K,p}) = 1$ and $\mathscr{T}_{K,p} = 1$.*

Proof. — If $G_{K,p}$ is free pro-p then $G^{ab}_{K,p} \simeq \mathbb{Z}_p^{t_p}$, $\mathscr{T}_{K,p} = 1$, $H^2(G_{K,p},\mathbb{Q}_p/\mathbb{Z}_p) = 0$, and by Proposition 1.5 one gets $ker(\iota_{K,p}) = 1$.
For the reverse, suppose that $ker(\iota_{K,p}) = 1$ and $G_{K,p} \simeq \mathbb{Z}_p^{t_p}$. By Proposition 1.5, $H_2(G_{K,p},\mathbb{Z}_p) = 0$; by Proposition 1.2, one gets $H^2(G_{K,p},\mathbb{Z}/p) = 0$ (take Δ trivial and $M = \mathbb{Z}/p$), and then $G_{K,p}$ is pro-p free.
Regarding the p-rank of $G_{K,p}$, see Theorem 1.4. □

Example 1.9. — Take $p > 3$, and let $K/\mathbb{Q}$ be an imaginary quadratic field. Observe that $E_K = 1$ and that $\mathscr{U}_p$ is torsion free. Hence when $Cl_K = 1$, the pro-p group $G_{K,p}$ is free pro-p on 2 generators.

Finally, let us recall that when $G_{K,p}$ is free pro-p then K is said to be *p-rational* ([**18**]).

1.2.2. With semisimple action. — Let Δ be a finite group of order coprime to p. Let Ψ_p be the set of irreducible $\mathbb{F}_p$-characters of Δ. Let M be a finite $\mathbb{F}_p[\Delta]$-module. For $\varphi \in \Psi_p$, set $r_\varphi M$ to be the φ-rank of M: that is the number of times that φ appears in the decomposition of M as $\mathbb{F}_p[\Delta]$-module. In particular if $\chi(M)$ denotes the character of M, then $\chi(M) = \sum_{\varphi\in\Psi_p} r_\varphi\varphi$. Put $\chi(M)^{-1} := \sum_{\varphi\in\Psi_p} r_\varphi\varphi^{-1}$, where $\varphi^{-1}(g) := \varphi(g^{-1})$. Recall that for a finite $\mathbb{Z}_p[\Delta]$-module M, one has $\chi(M/M^p) = \chi(M[p])$.

Definition 1.10. — Two finite $\mathbb{F}_p[\Delta]$-modules M and N are said to be *orthogonal*, and write $M \perp N$, if for every $\varphi \in \Psi_p$ one has $r_\varphi M \cdot r_\varphi N = 0$.

We denote by Reg the character of the regular representation, by $\mathbf{1}$ the trivial character, and for a subgroup D of Δ, by $\mathrm{Ind}_D^\Delta \mathbf{1}_D$ the induced character from D to Δ of the trivial character $\mathbf{1}_D$ of D.
Since $\chi(M \otimes N) = \chi(M)\chi(N)$ and $\chi(M^\wedge) = \chi^{-1}(M)$, one has:

Lemma 1.11. — *Let M and N be two finite $\mathbb{F}_p[\Delta]$-modules.*
Then $\Big(M^\wedge \otimes N\Big)^\Delta = 0$ if and only if $M \perp N$.

Proof. — Indeed, $\chi\Big(M^\wedge \otimes N\Big)^\Delta = \langle \chi(M^\wedge)\chi(N), \mathbf{1}\rangle = \langle \chi(N), \chi(M)\rangle = \sum_\varphi (r_\varphi M \cdot r_\varphi N)$. □

For the end of this section, let us consider the following frame.
Let K/k be a finite Galois extension of degree coprime to p; put $\Delta = Gal(K/k)$. Observe that K_p/k is Galois and that Δ acts on $G_{K,p}$, $\mathscr{T}_{K,p}$, $\mathscr{F}_{K,p}$, etc. Put $\Gamma = Gal(K_p/k) \simeq G_{K,p} \ltimes \Delta$.
As we will see, we need that the two pieces $\mathscr{F}_{K,p}$ and $\mathscr{T}_{K,p}$ of $G_{K,p}^{ab}$ must be orthogonal to each other (as Δ-modules). First, the next Theorem will be essential to lift residual representation.

Theorem 1.12. — *Let M be a finite Γ-module of exponent p on which $G_{K,p}$ acts trivially. Assuming Leopoldt's conjecture for K at p, then $H^2(\Gamma, M) \simeq \big(\mathscr{T}_{K,p}[p]^\wedge \otimes M\big)^\Delta$. In particular $H^2(\Gamma, M) = 0$ if and only if $\mathscr{T}_{K,p}[p] \perp M$.*

Proof. — This is a consequence of Proposition 1.2, Proposition 1.5 and Lemma 1.11. □

Remark 1.13. — When K contains ζ_p, the character of $\mathscr{T}_{K,p}[p]$ is related to the mirror character of Cl'_K, where Cl'_K is the p-Sylow of the p-class group of K. Typically when $K = \mathbb{Q}(\zeta_p)$, $r_\varphi \mathscr{T}_{K,p}[p] = r_{\varphi^*} Cl_K$, where $\varphi^* := \omega\varphi^{-1}$. In this case, $\mathbb{Q}(\zeta_p)$ is p-rational if and only if p is regular. For more general results see [**10**].

To finish, the following proposition will be the starting point for realizing residual representations as Galois extensions of number fields.

Proposition 1.14. — *Assuming the Leopoldt conjecture for K at p, one has*

$$\chi(\mathscr{F}_{K,p}/p) = \mathbf{1} + n\mathrm{Reg} - \sum_{v|\infty} \mathrm{Ind}_{D_v}^G \mathbf{1}_{D_v},$$

where $n = [k : \mathbb{Q}]$. In particular if K/k is a CM-field one has $\chi(\mathscr{F}_{K,p}/p) = \mathbf{1} + n\varphi$, where φ is the nontrivial character of $Gal(K/k)$.

Proof. — One has $\mathbb{Q}_p \otimes \mathscr{F}_{K,p} = \mathbb{Q}_p \otimes \mathscr{U}_p \Big/ \mathbb{Q}_p \otimes \iota_{K,p}(E_K)$. Then use for example [**10**, §5 Theorem 5.12, and §6]. □

2. Uniform groups and Lie algebras

2.1. Generalities. — For this section we refer to [**6**, Chapters 4, 7 and 9].

Let G be a finitely generated pro-p group. Set $G_1 = G$, and for $n \geqslant 1$, $G_{n+1} = G_n^p[G, G_n]$. The (G_n) is the p-descending central series of G. For $n \geqslant 1$, consider the morphism:

$$\begin{array}{rcl} \alpha_n : G_n/G_{n+1} & \to & G_{n+1}/G_{n+2} \\ x & \mapsto & x^p. \end{array}$$

Definition 2.1. — The pro-p group G is said to be *uniform* if for every n, the map α_n is an isomorphism.

Hence when G is uniform, there exists some d such that $G_n/G_{n+1} \simeq (\mathbb{Z}/p)^d$; the integer d is called the dimension of G.

Theorem 2.2. — *Let G be a uniform pro-p group. Then for all $n \geqslant 1$, G_{n+1} is uniform and also equal to:*
(i) $G_n^p[G_n, G_n]$,
(ii) $G^{p^n} = \langle g^{p^n}, g \in G\rangle$,
(iii) $(G_n)^p = \langle g_n^p, g_n \in G_n\rangle$.

Proof. — See [**6**, Chapter 3, Theorem 3.6]. □

Recall that a *p-adic analytic group* is a topological group G having a structure of p-adic analytic manifold for which the sum and the inverse are analytic. Since Lazard [**15**] one knows that uniform pro-p groups are the socle of p-adic analytic groups. Indeed:

Theorem 2.3. — (i) *A uniform group G of dimension d is a p-adic analytic group of dimension d (as analytic manifold).*
(ii) *Every p-adic analytic group of (analytic) dimension d contains an open subgroup which is uniform of dimension d.*
(iii) *Let G be a pro-p group which is a p-adic analytic group, then $G \hookrightarrow Gl_m(\mathbb{Z}_p)$ for some m.*

Proof. — See [**6**, Interlude A]. □

In what follows, we will consider uniform groups G as subgroups of $Gl_m(\mathbb{Z}_p)$.

2.2. Exponential and logarithm. —

2.2.1. The Lie algebras $\mathfrak{gl}_m$ and $\mathfrak{sl}_m$. — Set $\varepsilon = 0$ if $p > 2$, and $\varepsilon = 1$ if $p = 2$.

Take $m \geqslant 2$. Let $\mathfrak{gl}_m$ be the $\mathbb{Z}_p$-free module of dimension m^2 generated by the matrices $E_{i,j}(p) := p^{1+\varepsilon}E_{i,j}$, where $E_{i,j}$ are the elementary matrices. Then $\mathfrak{gl}_m$ is a $\mathbb{Z}_p$-Lie algebra, subalgebra of the algebra $\mathfrak{gl}_m(\mathbb{Q}_p)$ of the matrices of size $m \times m$ with coefficients in $\mathbb{Q}_p$, equipped with the Lie bracket $(A, B) = AB - BA$.
It is not difficult to see that $(\mathfrak{gl}_m, \mathfrak{gl}_m) \subset p^{1+\varepsilon}\ \mathfrak{gl}_m$: the algebra $\mathfrak{gl}_m$ is said to be *powerful* (see [**6**, Chapter 9, §9.4]).
Thanks to [**15**, Chapter IV, Theorem 1.3.5.1], one knows that the exponential map $exp : x \mapsto \sum_{n \geqslant 0}(n!)^{-1}x$ and the logarithm map $log(z) := \sum_{n \geqslant 1}(-1)^{n+1}n^{-1}(z-1)^n$ converge for $x \in \mathfrak{gl}_m$ and $z \in Gl_m^1$, where $Gl_m^1 = \{A \in Gl_m(\mathbb{Z}_p), A \equiv 1 \bmod p^{1+\varepsilon}\}$. Moreover exp and log are reciprocal on these two spaces. Hence $exp(\mathfrak{gl}_m) = Gl_m^1$ and since $\mathfrak{gl}_m$ is powerful, Gl_m^1 is uniform ([**6**, Chapter 5, Theorem 5.2]).
Let $\mathfrak{sl}_m$ be the $\mathbb{Z}_p$-Lie subalgebra of $\mathfrak{gl}_m$ consisting of matrices with zero trace. The algebra $\mathfrak{sl}_m$ is also powerful, and then $Sl_m^1 := exp(\mathfrak{sl}_m)$ is uniform. More, since $\mathfrak{sl}_m(\mathbb{Q}_p) := \mathbb{Q}_p \otimes \mathfrak{sl}_m$ is simple, one has $\mathfrak{sl}_m(\mathbb{Q}_p) = (\mathfrak{sl}_m(\mathbb{Q}_p, \mathfrak{sl}_m(\mathbb{Q}_p))$ which implies that the abelianization of

$Sl_m(\mathbb{Z}_p)$ is finite. Observe that $exp \circ Trace = det \circ exp$, confirming that $Sl_m^1 = exp(\mathfrak{sl}_m)$ is also the subgroup of Gl_m^1 of matrices of determinant 1.

2.2.2. Uniform groups and $\mathbb{Z}_p$-Lie algebras. — For $k \geqslant 1$, let φ_k be the reduction map:

$$\varphi_k : Gl_m(\mathbb{Z}_p) \to Gl_m(\mathbb{Z}/p^k\mathbb{Z}).$$

Set $Gl_m^{(k)} = ker(\varphi_{k+\varepsilon})$ and $Sl_m^{(k)} = ker(\varphi_{k+\varepsilon}) \cap Sl_m(\mathbb{Z}_p)$

Proposition 2.4. — *(i) One has $Gl_m^1 = Gl_m^{(1)}$ and $Sl_m^1 = Sl_m^{(1)}$.*
(ii) The subgroups $Gl_m^{(k)}$ (resp. $Sl_m^{(k)}$) correspond to the p-descending central series of Gl_m^1 (resp. Sl_m^1). In other words, $Gl_m^{(k)} = (Gl_m)_k$ and $Sl_m^{(k)} = (Sl_m)_k$.
(iii) For $k \geqslant 1$ one has $Gl_m^{(k)} = exp(p^{k-1}\mathfrak{gl}_m)$, and $Sl_m^{(k)} = exp(p^{k-1}\mathfrak{sl}_m)$.

Proof. — For (i) and (ii) see [**6**, Chapter 5, Theorem 5.2]; for (iii) see [**6**, Chapter 4, Lemma 4.14]. □

Proposition 2.4 is a special case of the following result:

Theorem 2.5. — *There is an isomorphism between the category of uniform pro-p groups G and the category of powerful $\mathbb{Z}_p$-Lie algebras $\mathfrak{L}$. When $G \subset Gl_m^1$ this correspondence is given by the exponential and the logarithm; in particular $\mathfrak{L} = log(G) \in \mathfrak{gl}_m$.*

Proof. — See [**6**, Chapter 9, Theorem 9.10]. □

Definition 2.6. — Let $G \subset Gl_m^1$ be a uniform pro-p group of dimension d. Set $\mathfrak{g} := log(G) \subset \mathfrak{gl}_m$, and $\mathfrak{g}_p := \mathfrak{g}/p\mathfrak{g}$. Observe that $\mathfrak{g}_p$ is a $\mathbb{F}_p$-vector space of dimension d.

As for Gl_m^1 in Proposition 2.4, the p-descending central series (G_n) of a uniform group $G \subset Gl_m(\mathbb{Z}_p)$ is easy to describe. Indeed:

Proposition 2.7. — *One has $G_n = exp(p^{n-1}\mathfrak{g})$.*
In particular, $G_n/G_{n+1} \simeq p^{n-1}\mathfrak{g}/p^n\mathfrak{g} \simeq \mathfrak{g}_p$.

Proof. — See [**6**, Chapter 4, Lemma 4.14]. □

2.2.3. The Lie algebra $\mathfrak{g}$ as a sub-module of $\mathfrak{gl}_m$. — Let $G \subset Gl_m^1$ be uniform; set $\mathfrak{g} = log(G)$. Recall that $\mathfrak{g}$ is the powerful sub-Lie $\mathbb{Z}_p$-algebra of $\mathfrak{gl}_m$ such that $exp(\mathfrak{g}) = G$. Let Δ' be a finite subgroup of $Gl_m(\mathbb{Z}_p)$ of order coprime to p, acting by conjugation on G; observe that Δ' also acts on Gl_m, on $\mathfrak{gl}_{m,p} := \mathfrak{gl}_m/p\mathfrak{gl}_m$, and on $\mathfrak{g}_p$. Since $p \nmid |\Delta'|$, the $\mathbb{Z}_p[\Delta']$-module $\mathfrak{gl}_m$ is projective (see [**22**, Chapter 14, §14.4]) and then, $\mathfrak{gl}_{m,p}$ and $\mathfrak{gl}_m(\mathbb{Q}_p) := \mathbb{Q}_p \otimes \mathfrak{gl}_m$ have the 'same' character (as Δ'-modules). Of course, for the same reason, $\mathfrak{g}_p$ and $\mathfrak{g}(\mathbb{Q}_p)$ have the same character. Since $\mathfrak{g}(\mathbb{Q}_p) \subset \mathfrak{gl}_m(\mathbb{Q}_p)$ we obtain:

Proposition 2.8. — *Let $\Delta' \subset Gl_m(\mathbb{Z}_p)$ be a subgroup of order coprime to p acting on $\mathfrak{g}$ by conjugation. Then $\mathfrak{g}_p$ is isomorphic to a sub-Δ'-module of $\mathfrak{gl}_{m,p}$.*

Definition 2.9. — When the action is given via a Galois representation $\rho_0 : \Delta \to Gl_m(\mathbb{Z}_p)$ (here $\Delta' = \rho_0(\Delta)$), the Δ-module $\mathfrak{g}_p$ is called *the adjoint of G following ρ_0*.

2.3. Semisimple algebras. — The next Theorem, due to Kuranishi ([**14**]), is essential for our strategy. See also [**1**].

Theorem 2.10 **([14])**. — *Let $\mathscr{L}$ be a semisimple $\mathbb{Q}_p$-Lie algebra. Then $\mathscr{L}$ can be generated by 2 elements.*

Let $\mathfrak{L} \subset \mathfrak{gl}_m$ be a powerful $\mathbb{Z}_p$-Lie algebra. For $x \in \mathfrak{L}$, put $w_{\mathfrak{L}}(x) := max\{k, x \in p^k\mathfrak{L}\}$, $w_{\mathfrak{L}}(0) = \infty$; it is a valuation on $\mathfrak{L}$ (following Lazard's terminology, see [**15**, Chapter I, §2.2]). When starting with a uniform group G, for $g \in G$ define $w_G(g) := w_{\mathfrak{g}}(log(g))$, where $\mathfrak{g} = log(G)$: this is a filtration on G (see [**15**, Chapter II, §1]).

Definition 2.11. — Two topological groups G and H are said to be *locally the same* if they have a common open subgroup.

As corollary of Theorem 2.10 we get

Corollary 2.12. — *Let $G \subset Gl_m^1$ be a uniform group such that $\mathfrak{g}(\mathbb{Q}_p)$ is semisimple. Then there exist two elements g and g' in G such that*

(*i*) $w_G(g) = w_G(g')$,

(*ii*) $g \notin \langle g' \rangle G_{k+1}$,

(*iii*) *the group G and the (closed) subgroup H generated by g and g', are locally the same.*

Proof. — Let $\mathfrak{g} := log(G)$ be the powerful $\mathbb{Z}_p$-Lie algebra associated to G, and equipped with the valuation $\omega_{\mathfrak{g}}$. Set $\mathscr{L} := \mathbb{Q}_p \otimes \mathfrak{g}$. By Theorem 2.10 there exist $x, y \in \mathscr{L}$ such that $\mathscr{L} = \langle x, y \rangle$. By multiplying x and y by some powers of p, we can assume that x and y have the same valuation k (and are also in $\mathfrak{g}$). Suppose now that $x \equiv a_0 y \mod p^{k+1}\mathfrak{g}$ for some $a_0 \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$; then $x - a_0 y$ and $p^{k_1}y$ are of the same valuation $k_1 + k$ for some $k_1 \geqslant 1$. Suppose moreover that $x - a_0 y \equiv a_1 p^{k_1} y \mod p^{k+k_1+1}\mathfrak{g}$ for some $a_1 \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$; then for some k_2, the elements $x - a_0 y - a_1 p^{k_1} y$ and $p^{k_2} y$ are of the same valuation $k_2 + k \geqslant k_1 + k + 1$. If this process does not stop, we can construct a sequence of integers (k_n), $k_{n+1} > k_n$, and a sequence of p-adic integers (a_n) such that $x - a_0 y - a_1 p^{k_1} y - \cdots - a_n p^{k_n} y$ is of valuation $k_{n+1} + k$, showing that $x \in \langle y \rangle$, which is impossible since $\mathscr{L}$ is not abelian. In conclusion, there exists $a_0, \cdots, a_{k_i} \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$, and integers $k_1, \cdots, k_i$ such that $x' := x - a_0 y - \cdots a_{k_i} p^{k_i} y$ is of valuation $k + k_{i+1}$, but such that $x' \notin \langle p^{k_{i+1}} y \rangle + p^{k+k_{i+1}+1}\mathfrak{g}$.
By abuse we note x by x', $p^{k_{i+1}}y$ by y, and $k + k_i$ by k. Thus, we may assume that x and y are in $\mathfrak{g}$ with the same valuation k, that they generate $\mathscr{L}$, and that $\{x, y\}$ is free in $p^k\mathfrak{g}/p^{k+1}\mathfrak{g} \simeq \mathfrak{g}_p \simeq (\mathbb{F}_p)^d$, where d is the dimension of G.
Set $g = exp(x)$ and $g' = exp(y)$. Then by the previous observations one has: $g \notin \langle g' \rangle G_{k+1}$. Let $H = \langle g, g' \rangle$ be the closed subgroup of G generated by g and g'. The pro-p group H is p-adic analytic as closed subgroup of a p-adic analytic group; let U be an open uniform subgroup of H. Then for $r \gg 0$, g^{p^r} and $(g')^{p^r}$ are in U. Hence the $\mathbb{Z}_p$-Lie algebra $\mathscr{L}_U = log(U)$ of U contains $p^r x$ and $p^r y$, and then $\mathbb{Q}_p \otimes \mathscr{L}_U = \mathscr{L}$. Thus, U and G are locally isomorphic and even locally the same (due to the fact that $U \subset G$), see for example [**23**, Part II, Chapter V, §2, Corollary 2], or [**6**, Chapter 9, §9.5, Theorem 9.11]. In other words, G and H are locally the same. □

The two next examples make explicit Theorem 2.10.

Example 2.13. — Take $m = 2$. Set $x = E_{1,2}(p) + E_{2,1}(p)$, and $y = E_{1,1}(p) - E_{2,2}(p)$. Observe that $(x, y) = 2p\big(E_{2,1}(p) - E_{1,2}(p)\big)$, hence x and y generate the Lie algebra

$\mathfrak{sl}_2(\mathbb{Q}_p)$. Set $g = exp(x)$ and $g' = exp(y)$, and $H = \langle g, g' \rangle$. Then H has $Sl_2^{(2)}$ as open subgroup.

Example 2.14 **([5] or [3]).** — Take $m \geqslant 3$. The Lie algebra $\mathfrak{sl}_m$ is simple. Set $x = \sum_{i=1}^{m-1} E_{i,i+1}(p)$, and

$$y = \begin{cases} E_{m,1}(p) & m \text{ odd,} \\ E_{m-1,1}(p) + E_{m,2}(p) & m \text{ even.} \end{cases}$$

Observe that $\langle x, y \rangle_{\mathbb{Z}_p} \subset \mathfrak{sl}_m$. Thanks to [**5**, Proposition 2.5 and Proposition 2.6] and [**3**, Example 2] one has $\langle x, y \rangle = \mathfrak{sl}_m(\mathbb{Q}_p)$. Put $g = exp(x)$, $g' = exp(y)$ and $H = \langle g, g' \rangle \subset Gl_m^1$. Observe that $w_G(g) = w_G(g') = 1$. Then H has $Sl_m^{(k)}$ as an open subgroup for some $k \gg 0$.

3. Lifting in uniform pro-p groups

To simplify we take $p > 2$. The goal of this section is to give lifting criteria for uniform groups including the well-known conditions when $G = Sl_m^1$ of Gl_m^1 (see [**17**, §1.6]).

3.1. Compatible actions. — Let $\mathscr{G}$ be a pro-p group of p-rank $\geqslant d$, and let $\Delta \subset Aut(\mathscr{G})$ be finite of order coprime to p. Set $\Gamma = \mathscr{G} \ltimes \Delta$.

Let $\mathscr{G}^{p,el} := \mathscr{G}/\mathscr{G}^p[\mathscr{G}, \mathscr{G}]$ be the maximal abelian p-elementary quotient of $\mathscr{G}$; observe that $\mathscr{G}^{p,el}$ is a $\mathbb{F}_p[\Delta]$-module.
Let M be a sub-$\mathbb{F}_p[\Delta]$-module of $\mathscr{G}^{p,el}$, and let $\rho_0 : \Delta \to Gl_m(\mathbb{Z}_p)$ be a representation of Δ such that $ker(\rho_0)$ acts trivially on M. Put $\Delta' = \rho_0(\Delta)$. Hence M is also a Δ'-module by $\rho_0(s) \cdot m := s \cdot m$.

Let $Pr_M : \mathscr{G} \to \mathscr{G}^{p,el} \to M$ be the projection of $\mathscr{G}$ on M.

Let $H \subset Gl_m(\mathbb{Z}_p)$ be a pro-p group such that $d_pH = d_pM$. Suppose that $\rho_0(\Delta)$ acts on H by conjugation. Hence $H^{p,el}$ becomes a Δ-module via ρ_0, by $s \cdot g' := \rho_0(s) \cdot g'$. We suppose now that the action of Δ on M is compatible with that of Δ on $H^{p,el}$: in other words, $\chi(H^{p,el}) = \chi(M)$, as Δ-modules. Hence there exists a Δ-isomorphism $\beta : H^{p,el} \xrightarrow{\sim} M$ (which is equivalent to be an isomorphism of Δ'-modules).

3.2. Embedding problem. — Let $G \subset Gl_m^1$ be a uniform pro-p group of dimension d. Set $\mathfrak{g} := log(G) \subset \mathfrak{gl}_m$. Given $1 \leqslant s \leqslant d$ and $k \geqslant 0$, let $z_1, \cdots, z_s \in p^k\mathfrak{g}$ be some independent elements in $p^k\mathfrak{g}/p^{k+1}\mathfrak{g} \simeq (\mathbb{Z}/p)^d$. Set $g_i = exp(z_i)$. Then for $i = 1, \cdots, k$, one has $w_G(g_i) = k$.

Let us consider the closed subgroup H of G generated by the g_i's. The group H is p-adic analytic. Observe that $H \subset G_k \subset Gl_m^{(k)} = ker(Gl_m(\mathbb{Z}_p) \to Gl_m(\mathbb{Z}/p^k))$. Recall that (G_n) is the p-central descending series of G.

For $n \geqslant 1$, put $H_{[n]} := H \cap G_{n+k-1}$. Hence $H_{[1]} = H$.

Lemma 3.1. — *(i) The pro-p group H is of p-rank s, and $H^{p,el} \simeq H/H_{[2]}$.*
(ii) For each $n \geqslant 1$, $H_{[n]} \lhd H$, the quotient $H_{[n]}/H_{[n+1]}$ is p-elementary abelian, and H acts trivially (by conjugation) on $H_{[n]}/H_{[n+1]}$.
(iii) The $H_{[n]}$ are open in H, and $\bigcap_n H_{[n]} = \{1\}$.

Proof. — (i) One has the commutative diagram:

$$\begin{tikzcd}
H/H_{[2]} \arrow[r, hook] & G_k/G_{k+1} \arrow[r, "\simeq", "log"'] & p^k\mathfrak{g}/p^{k+1}\mathfrak{g} \\
& H/H^p[H,H] \arrow[ul, two heads, "P"] \arrow[ur, "log"'] &
\end{tikzcd}$$

Hence the family $\{g_1H_{[2]},\cdots,g_sH_{[2]}\}$ is free in $H/H_{[2]}$, showing that $d_pH \geqslant d_pH/H_{[2]} \geqslant s$. But H is generated by the g_i's. Thus $d_pH = s$, and P is an isomorphism.
(ii) Clearly $H_{[n]} \lhd H$. Since $G_{n+1} = G_n^p[G,G_n]$ one has:

$$\begin{aligned}
H_{[n]}/H_{[n+1]} &= H \cap G_n/H \cap G_{n+1} \\
&= \big(H \cap G_n\big)G_n^p[G,G_n]/G_n^p[G,G_n].
\end{aligned}$$

Hence $H_{[n]}/H_{[n+1]}$ is p-elementary abelian, and G and then H acts trivially on $H_{[n]}/H_{[n+1]}$.
(iii) Point (ii) shows that the $G_{[n]}$ are of finite index in H, and then open since H is pro-p finitely generated. Regarding the intersection, that is obvious since $\bigcap_n G_n = \{1\}$. □

We now summarize conditions of Section 3.1.
Via β and ρ_0, suppose that $H^{p,el}$ can be seen as a sub-Δ-module of $\mathscr{G}^{p,el}$; or equivalently, $H^{p,el}$ is Δ'-isomorphic to a subspace M of $\mathscr{G}^{p,el}$.
Hence there exists a surjective morphism $f_2 : \Gamma \to H/H_{[2]} \ltimes \Delta'$, such that

(i) $(f_2)_{|\mathscr{G}} = \beta^{-1} \circ Pr_M$,
(ii) $(f_2)_{|\Delta} = \rho_0$.

Recall that $H/H_{[2]} = H^{p,el}$.

More generally, suppose that for some $n \geqslant 2$, there exists a surjective morphism $f_n : \Gamma \to H/H_{[n]} \ltimes \Delta'$, where $(f_n)_{|\Delta} = \rho_0$. Then let us consider the embedding problem $(\mathscr{E}_n)$:

$$\begin{tikzcd}
& & & \Gamma = \mathscr{G} \ltimes \Delta \arrow[dl, dotted, "\psi_n"'] \arrow[d, two heads, "f_n"] \\
1 \arrow[r] & H_{[n]}/H_{[n+1]} \arrow[r] & H/H_{[n+1]} \ltimes \Delta' \arrow[r, two heads, "g_n"'] & H/H_{[n]} \ltimes \Delta'
\end{tikzcd}$$

where g_n is the natural map (in particular $g_{n|\Delta'}$ is the identity).
Thanks to the criteria of Hoechsmann (see for example [**19**, Chapter III, §5]), $(\mathscr{E}_n)$ has some solution when $H^2(\Gamma, H_{[n]}/H_{[n+1]}) = 0$, where the action of Γ on $H_{[n]}/H_{[n+1]}$ is induced by conjugation via f_n. See for example [**19**, Chapter III, §5, Proposition 3.5.9]. In fact we need more:

Proposition 3.2. — *If $(\mathscr{E}_n)$ has a solution ψ_n, then ψ_n is an epimorphism (the solution is called proper).*

Proof. — The question is to see if the map ψ_n is surjective. Since $H/H_{[n+1]}$ and $H/H_{[n]}$ are p-groups, it is equivalent to see if these two groups have the same minimal number of generators: that is Lemma 3.1, (i). □

3.3. Main Theorem. — We can now state the key theoretical result of our paper. Let us write $\mathscr{G}^{ab} \simeq \mathscr{T} \oplus \mathbb{Z}_p^t$, where $\mathscr{T}$ is the torsion part of $\mathscr{G}^{ab}$. Let us keep the notations of the previous sections. In particular G is a uniform group of dimension d, H is a closed subgroup of G, β is a Δ-isomorphism from $H^{p,el}$ to a sub-Δ-module of $\mathscr{G}^{p,el}$, $\rho_0 : \Delta \to Gl_m(\mathbb{Z}_p)$ is a representation of Δ, and $\Delta' = \rho_0(\Delta)$. We suppose moreover that Δ' acts by conjugation on G. Hence, via ρ_0, the group Δ acts also on $\mathfrak{g} := log(G) \subset \mathfrak{gl}_n$, and on $\mathfrak{g}_p := \mathfrak{g}/p\mathfrak{g}$ (see §2.2.3).

Theorem 3.3. — *With the above notations, suppose given $f : \Gamma = \mathscr{G} \ltimes \Delta \twoheadrightarrow H/H^p[H,H] \ltimes \Delta'$ where $f_{|\Delta} = \rho_0$, such that: (i) $H^2(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$; and (ii) $\mathscr{T}[p] \perp \mathfrak{g}_p$. Then the embedding problem*

$$\begin{tikzcd}
& \Gamma = \mathscr{G} \ltimes \Delta \arrow[ld, dotted, two heads, "\psi"'] \arrow[d, two heads, "f"] \\
H \ltimes \Delta' \arrow[r, two heads, "g"'] & H/H_{[2]} \ltimes \Delta'
\end{tikzcd}$$

has a (proper) continuous solution ψ.

Proof. — We proceed step by step.

- First, for $n \geqslant 2$ suppose we are given a surjective morphism $f_n : \Gamma \to H/H_{[n]} \ltimes \Delta'$, where $(f_n)_{|\Delta} = \rho_0$. And consider the embedding problem $(\mathscr{E}_n)$.
- Observe now that

$$\begin{tikzcd}
H_{[n]}/H_{[n+1]} \arrow[r, equal] & G \cap G_n/H \cap G_{n+1} \arrow[r, "\sim"] & (H \cap G_n)G_{n+1}/G_{n+1} \arrow[d, hook] \\
& G_n/G_{n+1} & G_nG_{n+1}/G_{n+1} \arrow[l, "\sim"']
\end{tikzcd}$$

Since G is uniform, $G_n/G_{n+1} \simeq \mathfrak{g}_p$, and this isomorphism is also compatible with the action of Δ. In particular, $H_{[n]}/H_{[n+1]}$ is a sub-Δ-module of $\mathfrak{g}_p$.

- Since $f_n(\mathscr{G}) \subset H/H_{[n]}$, by Lemma 3.1 the group $\mathscr{G}$ acts trivially (via f_n) on $H_{[n]}/H_{[n+1]}$. By Theorem 1.12 we get

$$H^2(\Gamma, H_{[n]}/H_{[n+1]}) \simeq \left(\mathscr{T}[p]^\wedge \otimes H_{[n]}/H_{[n+1]}\right)^\Delta .$$

- But by hypothesis $\mathscr{T}[p] \perp \mathfrak{g}_p$. Then as $H_{[n]}/H_{[n+1]} \hookrightarrow \mathfrak{g}_p$, one has $\mathscr{T}[p] \perp H_{[n]}/H_{[n+1]}$. By Lemma 1.11 we finally get $H^2(\Gamma, H_{[n]}/H_{[n+1]}) = 0$: the embedding problem $(\mathscr{E}_n)$ has some proper solution ψ_n thanks to Proposition 3.2.

Put $f_{n+1} := \psi_n$.

- By hypothesis f_2 is given. Hence by the previous computation one deduces that $(\mathscr{E}_2)$ has a proper solution, which gives the existence of one f_3. Then $(\mathscr{E}_3)$ has a proper solution, etc. To conclude, it suffices to take the projective limit of a system of compatible solutions ψ_n, and to remember that $\bigcap\limits_n H_{[n]} = \{1\}$. □

Remark 3.4. — Observe that $H \ltimes \Delta' \hookrightarrow Gl_m(\mathbb{Z}_p)$. Hence the continuous map ψ induces a continuous Galois representation $\rho : \Gamma \to Gl_m(\mathbb{Z}_p)$ with image containing H as open subgroup. Moreover for $\delta \in \Delta$, one has $\psi(\delta) = \rho_0(\delta)$; thus $\rho_{|\Delta} \simeq \rho_0$. In other words, ρ is a lift of ρ_0. Finally observe that changing the map β (which is possible since $p > 2$), changes the representation ρ.

4. Applications

Before developing the arithmetical context, let us make a quick observation.

Proposition 4.1. — *Let k be a number field such that $r_2 > 0$. Suppose the Leopoldt and Gras conjectures for k at p. Take $p \gg 0$. Then for every p-analytic group G for which the Lie algebra is semisimple, there exist continuous Galois representations $\rho : Gal(\overline{k}/k) \to Gl_m(\mathbb{Z}_p)$ with image locally the same as G.*

Proof. — Here we assume that the pro-p group $G_{k,p}$ is free of p-rank r_2+1. Let $U \subset G$ be a uniform subgroup of G. The group U is pro-p. We can assume that $U \subset Gl_m^1$, and we conclude with Corollary 2.12 (as consequence of Theorem 2.10). □

When k is totally real, one strategy is to start with a residual Galois representation of $Gal(\overline{k}/k)$ of order coprime to p (typically of order 2) in which at least one real place is ramified.

4.1. The principle.

— We apply Section 2.2.3 in our arithmetical context as developed by Greenberg [**11**], Ray [**21**], etc.

• Let us start with a Galois extension K/k with Galois group Δ of order coprime to p. Recall that Δ acts on $G_{K,p}$, etc. Set $\Gamma = Gal(K_p/K) \simeq G_{K,p} \ltimes \Delta$.
Suppose $ker(\iota_{K,p})$ trivial (equivalently, assume Leopoldt's conjecture for K at p). Then $H^2(G_{K,p}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ by Proposition 1.5.

• Let $\rho_0 : \Delta \to Gl_m(\mathbb{Z}_p)$ be a Galois representation of $Gal(K/k)$.
For $i = 1, \cdots, s$, let L_i/K be cyclic degree p extensions in K_p/K. Let L be the compositum of the L_i's and set $M = Gal(L/K)$. We suppose that Δ acts on M but also that $ker(\rho_0)$ acts trivially on M as in Section 3.1. Hence $\Delta' := \rho_0(\Delta)$ acts on M by $\rho_0(s) \cdot m := s \cdot m$.

• Let $G \subset Gl_m^1$ be a uniform group, and let H be an open subgroup of G as in Section 3.2. Recall that $H = \langle g_1, \cdots, g_s \rangle$ where the g_i's are in $G_k \backslash G_{k+1}$. In particular $H \subset G_k$. Observe that $G_{k+1} = G^{p^{k+1}}$ by Theorem 2.3. Write $G/p^{k+1} := (G \bmod G^{p^{k+1}})$.
We suppose now that $\rho_0(\Delta)$ acts by conjugation on H, such that there exists a Δ-isomorphism $\beta : H^{p,el} \to M$ (which is equivalent to say that is a Δ'-isomorphism). Hence, we also get $Gal(L/K) \ltimes \rho_0(\Delta) \simeq H^{p,el} \ltimes \Delta'$. By Lemma 3.1 recall that

$$H^{p,el} \simeq H/H^p[H,H] \simeq H/H_{[2]} \simeq HG_{k+1}/G_{k+1}.$$

We then have a continuous Galois representation

$$\rho_1 : Gal(K_p/k) \to G/p^{k+1} \ltimes \Delta'$$

such that:

(i) $(\rho_1)_{|Gal(K_p/K)} = \beta^{-1} \circ Pr_M$,
(ii) $\rho_1{}_{|_{Gal(K/k)}} = \rho_0$,
(iii) $\rho_1 \bmod G^{p^k} \simeq \rho_0$.

The Galois representation ρ_1 plays the role of the function f of Theorem 3.3.

• As Δ' (or Δ) acts by conjugation on H, we assume moreover that it also acts on G. Set $\mathfrak{g} := log(G) \subset \mathfrak{gl}_n$. Hence $\mathfrak{g}_p$ becomes a Δ-module (via ρ_0).

As consequence of Theorem 3.3 and Remark 3.4, we get:

Corollary 4.2. — *If* $\ker(\iota_{K,p}) = 1$ *and* $\mathscr{T}_{K,p}[p] \perp \mathfrak{g}_p$*, then the representation* ρ_0 *lifts to a Galois representation* $\rho : Gal(K_p/k) \to Gl_m(\mathbb{Z}_p)$ *with image containing* H *as an open subgroup.*

4.2. Galois representations via imaginary quadratic fields. — We start with an imaginary quadratic extension $K/\mathbb{Q}$. Let $p > 2$ be a prime number. Put $\Delta = Gal(K/\mathbb{Q}) = \langle s \rangle$, and let φ be the nontrivial character of Δ.

• Suppose that $p \nmid |Cl_K|$. For $p = 3$, we assume moreover that $\mathscr{U}_p/\iota_{K,p}(E_K)$ is torsion free; typically $K = \mathbb{Q}(\sqrt{-3})$. The pro-$p$ group $G_{K,p}$ is free (see Example 1.9), and $\chi(G_{K,p}^{ab}/p) = \mathbf{1} + \varphi$ by Proposition 1.14. Take $M = G_{K,p}^{p,el} = \langle h_1, h_2 \rangle \simeq (\mathbb{Z}/p)^2$, such that $s \cdot h_1 = h_1$ and $s \cdot h_2 = h_2^{-1}$.

• We recall observation of Example 2.14 from [**3**] and [**5**].

Take $m \geqslant 3$, and consider $z_1 = E_{1,2}(p) + E_{2,3}(p) + \cdots + E_{m-1,m}(p) \in \mathfrak{gl}_m$, and

$$z_2 = \begin{cases} E_{m,1}(p) & m \text{ odd} \\ E_{m-1,1}(p) + E_{m,2}(p) & m \text{ even.} \end{cases}$$

Set $g_1 = exp(z_1) \in Gl_m^1$ and $g_2 = exp(z_2) \in Gl_m^1$, and $H = \langle g_1, g_2 \rangle$. Take the uniform group $G := Sl_m^1$. Of course $H \subset G$. As seen in 2.14 (thanks to Corollary 2.12), the analytic groups H and $Sl_m(\mathbb{Z}_p)$ are locally the same.

Set $A = \sum_i (-1)^{i+1} E_{i,i}$. By conjugation, $A \cdot z_1 = -z_1$ and $A \cdot z_2 = z_2$, and then A acts by -1 on g_1 and by $+1$ on g_2. Of course A acts also on $Sl_m(\mathbb{Z}_p)$.

Let $\rho_0 : Gal(K/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ be the Galois representation defined by $\rho_0(s) = A$. Here $ker(\rho_0) = 1$, and the map $\beta : M \to H^{p,el}$ defined by $\beta(h_1) = g_1 H^p[H,H]$ and $\beta(h_2) = g_2 H^p[H,H]$ is an isomorphism of Δ-modules.

For $m = 2$, consider Example 2.13 and take $z_1 = E_{1,1}(p) - E_{2,2}(p)$, $z_2 = E_{1,2}(p) + E_{2,1}(p)$, $g_1 = exp(x_1)$, $g_2 = exp(x_2)$, and $A = E_{1,1} - E_{2,2}$.

In conclusion, the principle of Section 4.1 allows us to lift ρ_0 to a Galois representation of $Gal(K_p/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$.

Theorem 4.3. — *Given* $p > 3$*, and* $m \geqslant 1$*. Let* $K/\mathbb{Q}$ *be an imaginary quadratic extension such that* $p \nmid |Cl_K|$*. Then there exist continuous Galois representations* $\rho : Gal(K_p/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ *with open image.*

Proof. — Here the field K is p-rational and $E_K = 1$; then apply Corollary 4.2. Hence there exists a continuous Galois representation $\rho' : Gal(K_p/\mathbb{Q}) \to Sl_m^1 \ltimes \rho_0(\Delta) \hookrightarrow Gl_m(\mathbb{Z}_p)$ with image containing Sl_m^k for some $k \gg 0$, as open subgroup.

Let $\omega' : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the cyclotomic character. Now, recall that since $Sl_m(\mathbb{Q}_p)$ is semisimple, every open subgroup of Sl_m^1 has finite abelianization. Hence the image of the Galois representation $\rho := \rho' \otimes \omega' : Gal(K_p/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ has p-adic dimension m^2; in conclusion the image of ρ is open in $Gl_m(\mathbb{Z}_p)$. □

As a corollary, we obtain:

Corollary 4.4. — *There exist continuous Galois representations* $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ *with open image satisfying:*

(*i*) ρ *is unramified ouside* $\{p, \infty\}$ *if* $p \equiv -1 \bmod 4$,

(*ii*) ρ *is unramified ouside* $\{2, p, \infty\}$ *if* $p \equiv 1 \bmod 4$.

Proof. — Take $K = \mathbb{Q}(\sqrt{-p})$. Thanks to an explicit version of Brauer-Siegel (see for example [**16**]), $p \nmid |Cl_K|$. (For $p = 3$, the number field $\mathbb{Q}(\sqrt{-3})$ is 3-rational). Apply Theorem 4.3. □

Remark 4.5. — Observe that ramification at 2 only occurs in $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$.

4.3. Galois representations via $K = \mathbb{Q}(\zeta_p)$. — The study of Galois representations through $\mathbb{Q}(\zeta_p)$ allows us to realize, for many primes $p \equiv 1 \bmod 4$ and large m, Galois representations $\rho : G_\mathbb{Q} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$, and with open image.

Take $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_p)$. Let s be a generator of $\Delta = Gal(K/\mathbb{Q})$. Recall that $\iota_{K,p}$ is injective, and by Proposition 1.14, $\chi(\mathscr{F}_{K,p}/p) = \mathbf{1} + \omega + \omega^3 + \cdots + \omega^{p-2}$, where $\omega : G_\mathbb{Q} \to \mathbb{F}_p^\times \subset \mathbb{Z}_p^\times$ is the mod p reduction of the cyclotomic character.

Take $m \geqslant 3$. Let g_1 and g_2 be the elements of Sl_m^1 as in the previous section. Set $H = \langle g_1, g_2 \rangle \subset Sl_m^1$.

Given an odd integer a, set $A_a(s) = \sum_{i=1}^{m} \omega^{ia}(s) E_{i,i}$. Consider the Galois representation $\rho_0 : Gal(K/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ defined by $\rho_0(s) = A_a(s)$.

Then $A_a(s) \cdot z_1 = \omega^{-a}(s)\ z_1$ and

$$A_a(s) \cdot z_2 = \begin{cases} \omega^{a(m-1)}(s)\ z_2 & m \text{ odd} \\ \omega^{a(m-2)}(s)\ z_2 & m \text{ even.} \end{cases}$$

Put $g_1 = exp(z_1)$ and $g_2 = exp(z_2)$. The action of $A_a(s)$ is odd on g_1, and even on g_2. Of course $A_a(s)$ acts also on Sl_m^1.

Thanks to the decomposition of $\chi(\mathscr{F}_{K,p}/p)$, we can find h_1 and h_2 in $\mathscr{F}_{K,p}$ such that $s \cdot h_1 = h_1^{\omega^a(s)}$, and $s \cdot h_2 = h_2^{\omega^{a(m-1)}(s)}$ if $a(m-1) = 0 \bmod p-1$ for m odd, and $s \cdot h_2 = h_2^{\omega^{a(m-2)}}$ if $a(m-2) = 0 \bmod p-1$ for m even; there is no condition for the odd character, but the even character must be trivial.

Put $M = \mathbb{F}_p h_1 + \mathbb{F}_p h_2 \subset G_{K,p}^{p,el}$. Then Δ acts on M, $ker(\rho_0) = ker(\omega^a)$ acts trivially on M, and the two Δ-modules M and $H^{p,el}$ are isomorphic.

Here, it is not difficult to see that the character $\chi(\mathfrak{gl}_{m,p})$ of $\mathfrak{gl}_{m,p}$ (via ρ_0) contains only characters of the form $\omega^{(i-j)a}$ with $i, j \in \{1, \cdots, m\}$.

We can apply the previous techniques. As before, the representation ρ_0 lifts when $\omega^{aa'}$ does not appear in $\chi(\mathscr{T}_{K,p}[p]) = \chi^*(Cl_K[p])$, for every $a' \in \{\pm 1, \pm 2, \cdots, \pm m\}$ (in fact class modulo $p-1$ of).

Let a be the odd part of $p-1$; in other words, $p - 1 = a2^\lambda$ with $2 \nmid a$; so $\lambda = v_2(p-1)$. We obtain the first condition (regarding the existence of h_1 and h_2): for m odd we must have $v_2(m-1) \geqslant v_2(p-1)$; for m even we must have $v_2(m-2) \geqslant v_2(p-1)$. For a regular prime p, that is the only condition.

Regarding the condition so that $\mathscr{T}_{K,p} \perp \mathfrak{gl}_{m,p}$: Let us start with a character ω^{k_i} that appears in $\chi(Cl_K[p])$, that is equivalent to say that ω^{1-k_i} appears in $\chi(\mathscr{T}_{K,p}[p])$; if ω^{1-k_i} appears in $\chi(\mathfrak{gl}_{m,p})$ then a divides $k_i - 1$.

Let us look at the $p \equiv 3 \bmod 4$ case; here $a = (p-1)/2$.

There is no condition on m, and the condition regarding $\mathscr{T}_{K,p}$ becomes $r_{\omega^{(p-1)/2}}(\mathscr{T}_{K,p}) = 0$. Observe that $r_{\omega^{(p-1)/2}}(\mathscr{T}_{K,p}) = r_\varphi(\mathscr{T}_{K_0,p})$, where $K_0 = \mathbb{Q}(\sqrt{-p})$ and where φ is the nontrivial character of $Gal(K_0/\mathbb{Q})$. Hence since $r_\varphi \mathscr{T}_{K_0,p} = 0$ (see the proof of Corollary 4.4), we get that there is no obstruction for the embedding problem. In fact, observe that in this case the representation we obtain through $\mathbb{Q}(\zeta_p)$ can be deduced by the one of Corollary 4.4.

We have proved:

Theorem 4.6. — *Let* $p \equiv 1 \bmod 4$ *be a prime number, and let* $m \geqslant 3$. *Write* $p-1 = 2^\lambda a$ *where* $2 \nmid a$. *Let* $\{\omega^{k_1}, \cdots, \omega^{k_e}\}$ *be the characters corresponding to the nontrivial components of the p-Sylow of the class group of* $\mathbb{Q}(\zeta_p)$. *Suppose that:*

(i) $v_2(m-1) \geqslant v_2(p-1)$ *if m is odd, and* $v_2(m-2) \geqslant v_2(p-1)$ *if m is even;*

(ii) $a \nmid (k_i - 1)$ *for* $i = 1, \cdots, e$.

Then there exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ *unramified outside* $\{p, \infty\}$*, and with open image.*

Corollary 4.7. — *Let* $p \equiv 1 \bmod 4$ *be a regular prime. Then there exist continuous Galois representations* $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ *unramified outside* $\{p, \infty\}$ *and with open image, for every odd m such that* $v_2(m-1) \geqslant v_2(p-1)$*, and for every even m such that* $v_2(m-2) \geqslant v_2(p-1)$.

References

[1] J.-M. Bois, *Generators of simple Lie algebras in arbitrary characteristics.*, Math. Z. **262** (2009), no. 4, 715-741.

[2] A. Brumer, *On the units of algebraic number fields*, Mathematika bf 14 (1967), 121-124.

[3] A. Chistopolskaya, *On nilpotent generators of the special linear Lie algebra*, Linear Algebra and its Applications **559** (2018), 73-79.

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

[5] A. S. Detinko, W. A. De Graaf, 2*-generation of simple Lie algebras and free dense subgroups of algebraic groups*, Journal of Algebra **545** (2020), 159-173.

[6] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups*, Cambridge studies in advances mathematics 61, Cambridge University Press, 1999.

[7] G. Gras, *Les* Θ*-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canadian Journal of Math. **68** (2016), 571-624.

[8] G. Gras, Class Field Theory, From Theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[9] G. Gras, *Practice of the Incomplete p-Ramification over a Number Field – History of Abelian p-Ramification*, Comm. in Adv. Math. Sciences **II** no. 4 (2019), 251-280.

[10] G. Gras, *Théorèmes de réflexion*, J. Théor. Nombres Bordeaux **10** (1998), no. 2, 399–499.

[11] R. Greenberg, *Galois representations with open image*, Annales Math. Québec **40** (2016), issue 1, 83-119.

[12] P.J. Hilton, U. Stammbach, A course in Homological Algebra, Graduate Texts in Math. 4, 2nde edition, Springer-Verlag New-York, Inc, 1997.

[13] N. Katz, *A note on Galois representations with big image*, Enseign. Math. **65** (2019), no. 3-4, 271-301.

[14] M. Kuranishi, *Two elements generations on semi-simple Lie groups*, Kodai Math. Sem. Rep., no. 5-6, dec. 1949.

[15] M. Lazard, *Groupes analytiques p-adiques*, IHES, Publ. Math. **26** (1965), 389-603.

[16] S. Louboutin, *The Brauer-Siegel Theorem*, J. London Math. Soc. (2) **72** (2005), 40-52.

[17] B. Mazur, Deforming Galois representations In : Galois groups over $\mathbb{Q}$, Y. Ihara, K. Ribet, J.-P. Serre eds., MSRI Publ.16, Springer-Verlag, 1987, 385-437.

[18] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, PhD Université Paris VII, 1988.

[19] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, GMW 323, Second Edition, Corrected 2nd printing, Springer-Verlag Berlin Heidelberg, 2013.

[20] The PARI Group, PARI/GP version2.9.4, Univ. Bordeaux, 2018, http ://pari.math.u-bordeaux.fr/.

[21] A. Ray, *Constructing Galois representations ramified at one prime*, Journal of Number Theory **222** (2021), 168-180.

[22] J.-P. Serre, Linear representations of finite groups, GTM 42, Springer-Verlag, New-York Heidelberg Berlin, 1977.

[23] J.-P. Serre, Lie Algebras and Lie groups, Lecture Notes in Math. 1500, Springer-Verlag Berlin Heidelberg, 1992.

April 18, 2021

CHRISTIAN MAIRE, FEMTO-ST Institute, Université Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, FRANCE • *E-mail :* christian.maire@univ-fcomte.fr