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 $\{p, \infty\}$ if $p \equiv 3 \bmod 4$ and is unramified outside $\{2, p, \infty\}$ if $p \equiv 1 \bmod 4$. We also revisit the question of the lifting of residual Galois representations in terms of embedding problems; that allows us to produce Galois representations with open image in the group of upper triangular matrices with diagonal entries equal to 1, unramified outside $\{p, \infty\}$, for m "small" comparing to p.

Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$, and let p be a prime number.
The last decades have shown the importance in arithmetic geometry of continuous Galois representations

$$\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$$

deriving from geometric objects. Thanks to Serre in [**25**], one knows that the action of $G_{\mathbb{Q}}$ on torsion points of elliptic curves without complex multiplication produces 2-dimensional Galois representations with open image in $Gl_2(\mathbb{Z}_p)$. But as observed by Greenberg in [**11**], it seems more difficult to produce geometric Galois representations with open image in dimensions $m \geqslant 3$. In [**11**], Greenberg himself suggested a method from group theory for constructing higher-dimensional Galois representations with open image. Let us be a little more specific.

Let K be a number field having r_2 pairs of non-real embeddings, 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

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

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

A first version of this work has been posted on Arxiv, in April 2021: https://arxiv.org/abs/2104.02505. 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, and Shiang Tang for his interest for this paper. The author also wants to thank the anonymous referee for thoroughly reading the paper, making a number of helpful suggestions. This work was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002).

the universal property of free groups. This approach allowed Greenberg to realize Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ 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 done by A. Ray in [**24**]. 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.

By a different approach, Katz in [**15**] 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 $m \geqslant 6$. We note that the representations constructed by Katz are motivic but are ramified at sets consisting of primes of potentially many different residue characteristics.

More recently Tang [**29**][1] by using a lifting theorem of Fakruddhin-Khare-Patrikis, showed the existence of Galois representations with open image when $p \gg m$; in this case there is no control of the set of ramification of the Galois representations due to the nature of the Ramakrishna style lifting argument.

In this work, by extending the arithmetical approaches of [**11**], we are able to prove (Corollary 4.6):

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 ramification index 2 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 $\mathbb{Q}$.*

Here is the key idea of our approach. We exploit a result of Kuranishi [**16**] 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 the embedding criteria of Greenberg 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 certain imaginary quadratic extensions for which p does not divide its class number.

By passing through the maximal abelian 2-extension $K/\mathbb{Q}$ inside $\mathbb{Q}(\zeta_p)$, the same strategy allows us to produce, for many primes $p \equiv 1 \bmod 4$ and unbounded m, continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ ramified only at $\{p, \infty\}$ with open image. This is the

[1] Tang's paper https://arxiv.org/abs/2205.00502 is later than the first version of this work.

case for all but six primes $p \equiv 1 \bmod 4$ less than $4 \cdot 10^5$; for those situations the number fields K are p-rational. See Section 4.3.1 and Corollary 4.8.

The strategy of Greenberg applies when the number field K fixed by the kernel of the residual representation is p-rational. In this work we also extend this approach. To do this we 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.

For a finitely generated pro-p group G, let $G^{ab} := G/[G,G]$ be the abelianization and $G^{p,el} := G^{ab}/(G^{ab})^p$ the maximal p-elementary quotient.
Set $\varepsilon = 0$ if $p > 2$, and $\varepsilon = 1$ if $p = 2$, and consider the following congruence subgroup

$$Gl_m^1 = \{A \in Gl_m(\mathbb{Z}_p), A \equiv 1 \bmod p^{1+\varepsilon}\}.$$

We prove (Theorem 3.3):

Theorem B. — *Let $\Gamma = \mathscr{G} \rtimes \Delta$ be a profinite group where $\mathscr{G}$ is a finitely generated pro-p group and where Δ is a finite group of order coprime to p. Let H be a closed subgroup of a p-adic analytic uniform group $G \subset Gl_m^1$ generated by elements having the same valuation. Let*

$$\rho_0 : \Delta \hookrightarrow Gl_m(\mathbb{Z}_p)$$

be an injective representation of Δ. Suppose that Δ acts by conjugation (via ρ_0) on G and on H, such that the Δ-module $H^{p,el}$ is isomorphic to a sub-Δ-module of $\mathscr{G}^{p,el}$. Let

$$f : \Gamma = \mathscr{G} \rtimes \Delta \twoheadrightarrow H^{p,el} \rtimes \Delta'$$

be a surjective map induced by this isomorphism, where $f_{|\Delta} = \rho_0$ and $\Delta' = \rho_0(\Delta)$. Suppose moreover that:

(i) $H^2(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$; and
(ii) $\mathscr{G}^{ab}[p]$ and the tangent space $\mathfrak{g}$ of G are orthogonal to each other as Δ-modules.

Then the embedding problem

$$\begin{tikzcd}
& \Gamma = \mathscr{G} \rtimes \Delta \arrow[dl, dotted, two heads, "\psi"'] \arrow[d, two heads, "f"] \\
H \rtimes \Delta' \arrow[r, two heads, "g"'] & H^{p,el} \rtimes \Delta'
\end{tikzcd}$$

has a proper continuous solution ψ.

For the notion of valuation, see Section 2.2.2, and for the notion of being orthogonal, see Definition 1.11.
As example of application, we focus on $T_m \subset Sl_m(\mathbb{Z}_p)$, the group of upper triangular matrices with diagonal entries equal to 1.

Corollary C. — *Let $e \geqslant 0$, and let p be a prime number with index of irregularity $e_p \leqslant e$. There is a constant c_e depending on e such that for every*

$$m \leqslant c_e(p-1)^{1/(e+1)},$$

there exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$ and with open image in T_m. One can take $c_0 = 1/2$ and $c_1 = 1/4$.

The paper contains four sections. In Section 1 and in Section 2, we recall facts about pro-p groups, 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 3, we develop the approach of lifting residual representations via the embedding problem; in particular we prove Theorem B. The last section is devoted to applications with the proofs of Theorem A and Corollary C. It seems likely the methods we introduce can apply more generally for realizing other groups, and with partial ramification at p as well; we also discussed this at the end of the last section.

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 finitely generated 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 the Pontryagin dual of A.

For the computations we have used the program PARI/GP [**23**].

1. On pro-p groups and on pro-p extensions 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 [**22**, 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 $\Gamma \simeq G \rtimes \Delta$.

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

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

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 [**13**, 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 [**22**, 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 $H^2(G, M) \simeq \left(\mathscr{T}[p]^\wedge \otimes M\right)^\Delta$.*

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

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

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. □

The proof of Proposition 1.2 also allows us to obtain:

Proposition 1.3. — *One has*

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

Suppose now that G is a free pro-p group on d generators, and let H be a pro-p group of p-rank $d' \leqslant d$. Since G is projective, the pro-p group H can be seen as quotient of G. For our work we need a little bit more to take into account the action of Δ. The following proposition can be found in the paper of Greenberg [**11**, Proposition 2.3.1] and partially in an unpublished paper of Wingberg [**30**].

Proposition 1.4. — *Let $\Gamma = G \rtimes \Delta$ be a profinite group where G is free pro-p on d generators and where Δ is a finite group of order n coprime to p. Let H be a finitely generated pro-p group on d' generators, with $d \geqslant d'$. Suppose that there exists a homomorphism $\Delta \to Aut(H)$ such that the Δ-module $H^{p,el}$ is isomorphic to a sub-Δ-module of $G^{p,el}$. Then there exists a normal subgroup N of G, stable under Δ, such that G/N is Δ-isomorphic to H and so we have a surjection $\Gamma \twoheadrightarrow H \rtimes \Delta$.*

Here, $Aut(H)$ is the group of continuous automorphisms of H.
A proof is given in [**12**, Section 2.2] in the spirit of [**30**].

1.2. Restricted ramification.

— Let K be a number field. As usual (r_1, r_2) is the signature of K. 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 $G_{K,p}$. — This section contains only well known results, but is included for the sake of clarity.

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 [**22**, Chapter VIII, Proposition 8.3.18; Chapter X, Corollary 10.4.9, Theorem 10.7.13]):

Theorem 1.5. — *The pro-p group $G_{K,p}$ is of cohomological dimension $\leqslant 2$, and $d_pH^1(G_{K,p},\mathbb{Z}/p) - d_pH^2(G_{K,p},\mathbb{Z}/p) = r_2 + 1$.*

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 (see for example [**8**, Chapter III, §1, Corollary 1.6.3]):

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

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 [**22**, Chapter X, Corollary 10.3.7]):

Proposition 1.6. — *One has* $ker(\iota_{K,p}) = 1 \Longleftrightarrow H_2(G_{K,p}, \mathbb{Z}_p) = 0$.

Proof. — This is a consequence of Proposition 1.3 and Theorem 1.5. □

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

Proposition 1.7. — *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 $\mathscr{U}_p/\iota_{K,p}(E_K) \simeq G_{K,p}^{ab}$ when $Cl_K = 1$. □

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

Conjecture 1.8 **(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 next proposition, for example.
The fact that $G_{K,p}$ may be a noncommutative free pro-p group can be found, maybe for the first time, in a paper of Shafarevich [**28**, §4]. Let us recall that when $G_{K,p}$ is free pro-p then K is said to be *p-rational* ([**21**]).

Proposition 1.9. — *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 $G_{K,p}^{ab} \simeq \mathbb{Z}_p^{t_p}$, $\mathscr{T}_{K,p} = 1$, $H^2(G_{K,p}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, and by Proposition 1.6 one gets $ker(\iota_{K,p}) = 1$.
For the converse, suppose that $ker(\iota_{K,p}) = 1$ and $G_{K,p} \simeq \mathbb{Z}_p^{t_p}$. By Proposition 1.6, $H_2(G_{K,p}, \mathbb{Z}_p) = 0$; 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 free pro-p.
Regarding the p-rank of $G_{K,p}$, see Theorem 1.5. □

Example 1.10. — 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.

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. In particular if $\chi(M)$ denotes the character of M, then $\chi(M) = \sum_{\varphi\in\Psi_p} (r_\varphi M)\varphi$. Put $\chi^{-1}(M) := \sum_{\varphi\in\Psi_p} (r_\varphi M)\varphi^{-1}$, where $\varphi^{-1}(g) := \varphi(g^{-1})$.

Definition 1.11. — 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 1.12. — *Let M and N be two finite $\mathbb{F}_p[\Delta]$-modules.*
Then $\left(M^\wedge \otimes N\right)^\Delta = 0$ if and only if $M \perp N$.

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

For the end of this section, let us consider the following setting.
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 $\Gamma = Gal(K_p/k) \simeq G_{K,p} \rtimes \Delta$.
First, the next Theorem will be essential to lift residual representations.

Theorem 1.13. — *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 $H^2(\Gamma, M) \simeq \left(\mathscr{T}_{K,p}[p]^\wedge \otimes M\right)^\Delta$. 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 1.6 and Lemma 1.12. □

Remark 1.14. — 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 1.15. — *Assuming the Leopoldt conjecture for K at p, one has*

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

where $n = [k : \mathbb{Q}]$, and where Δ_v is the group of decomposition of v in K/k. 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].
Set $\varepsilon = 0$ if $p > 2$, and $\varepsilon = 1$ if $p = 2$.
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 map:

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

Definition 2.1. — The pro-p group G is said to be *uniform* if $G/G^{(1+\varepsilon)p}$ is abelian and if for every n, the map α_n induces 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 product and the inverse are analytic. Since Lazard [**17**] 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 $\mathfrak{sl}_m$. — 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 [**17**, Chapter IV, Theorem 1.3.5.1], one knows that the exponential series

$$exp(x) := \sum_{n \geqslant 0} \frac{1}{n!} x$$

and the logarithm series

$$log(z) := \sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n}(z-1)^n$$

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 inverse 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; one has $Sl_m^1 = Sl_m(\mathbb{Z}_p) \cap Gl_m^1$ (see for example [**6**, Chapter 9, Exercise 8]). 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^1 is finite.

2.2.2. Uniform groups and $\mathbb{Z}_p$*-Lie algebras.* — Let us start with a classical result showing the power of the exponential and the logarithm.
For $k \geqslant 1$, consider the congruence subgroups:

$$Gl_m^k = \{A \in Gl_m(\mathbb{Z}_p), A \equiv 1 \bmod p^{k+\varepsilon}\},\ Sl_m^k := Sl_m(\mathbb{Z}_p) \cap Gl_m^k.$$

Proposition 2.4. — *(i) One has* $Gl_m^k = exp(p^{k-1}\mathfrak{gl}_m)$*, and* $Sl_m^k = exp(p^{k-1}\mathfrak{sl}_m)$*.*
(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* $Sl_m^k = (Sl_m)_k$*.*

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

In fact, Gl_m^1 is a special case of the following result:

Theorem 2.5. — *There is an equivalence between the category of uniform pro-p groups G and the category of powerful* $\mathbb{Z}_p$*-Lie algebras* $\mathfrak{L}$ *(i.e. verifying* $\mathfrak{L} \simeq \mathbb{Z}_p^d$ *and* $(\mathfrak{L}, \mathfrak{L}) \subset p^{1+\varepsilon}\mathfrak{L}$*). 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]. □

Let $\mathfrak{L} \subset \mathfrak{gl}_m$ be a powerful $\mathbb{Z}_p$-Lie algebra. For $x \in \mathfrak{L}$, put $w_{\mathfrak{L}}(x) := max\{k, x \in p^{k-1}\mathfrak{L}\}$, $w_{\mathfrak{L}}(0) = \infty$; it is a valuation on $\mathfrak{L}$ (following Lazard's terminology, see [**17**, 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 [**17**, Chapter II, §1]).

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 [**26**, 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 ([**16**]), is essential for our strategy. See also [**1**].

Theorem 2.10 **([16])**. — *Let $\mathscr{L}$ be a semisimple $\mathbb{Q}_p$-Lie algebra. Then $\mathscr{L}$ can be generated by 2 elements.*

Definition 2.11. — Two topological groups G and H are said to be *commensurable* 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 the group G and the (closed) subgroup H generated by g and g', are commensurable.*

Proof. — Let $\mathfrak{g} := log(G)$ be the powerful $\mathbb{Z}_p$-Lie algebra associated to 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 are also in $\mathfrak{g}$.
Set $g = exp(x)$ and $g' = exp(y)$, and 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 a 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 commensurable (due to the fact that $U \subset G$), see for example [**27**, Part II, Chapter V, §2, Corollary 2], or [**6**, Chapter 9, §9.5, Theorem 9.11]. In other words, G and H are commensurable. □

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 $(x, y) = 2p^{1+\varepsilon}\big(E_{2,1}(p) - E_{1,2}(p)\big)$, 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 $Sl_2^{2+2\varepsilon}$ 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

The goal of this section is to give lifting criteria for uniform groups including the well-known conditions when $G = Sl_m^1$ (see [**20**, §1.6]).

3.1. Compatible actions. — Let $\mathscr{G}$ be a pro-p group of p-rank $\geqslant d$, and let be a homomorphism $\Delta \to Aut(\mathscr{G})$, where Δ is a finite group of order coprime to p.
Set $\Gamma = \mathscr{G} \rtimes \Delta$. 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 $\rho_0 : \Delta \hookrightarrow Gl_m(\mathbb{Z}_p)$ be an injective representation of Δ. 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 a 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 $\beta : H^{p,el} \xrightarrow{\sim} M$.

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 $k \geqslant 1$, let $z_1, \cdots, z_s \in p^{k-1}\mathfrak{g}$ be some independent elements in $p^{k-1}\mathfrak{g}/p^k\mathfrak{g} \simeq (\mathbb{Z}/p)^d$. 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 $H \subset G_k \subset Gl_m^k$.

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:

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

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 $G_{n+k} = G_{n+k-1}^p[G, G_{n+k-1}]$ one has:

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

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 $H_{[n]}$ 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 M of $\mathscr{G}^{p,el}$. Hence there exists a surjective morphism $f_2 : \Gamma \to H/H_{[2]} \rtimes \Delta'$, 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

$$f_n : \Gamma \to H/H_{[n]} \rtimes \Delta',$$

where $(f_n)_{|\Delta} = \rho_0$. Then let us consider the embedding problem $(\mathscr{E}_n)$:

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

where g_n is the natural map (in particular $g_{n|\Delta'}$ is the identity).
Thanks to the criteria of Hoechsmann, $(\mathscr{E}_n)$ has a 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 [**22**, 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: this is the case since $H/H_{[2]} = H^{p,el}$. □

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 $G \subset Gl_m^1$ 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 $\mathscr{G}^{p,el}$, $\rho_0 : \Delta \hookrightarrow Gl_m(\mathbb{Z}_p)$ 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* (Theorem B).** — *With the above notations, suppose given*

$$f : \Gamma = \mathscr{G} \rtimes \Delta \twoheadrightarrow H^{p,el} \rtimes \Delta',$$

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

$$\begin{tikzcd}
& \Gamma = \mathscr{G} \rtimes \Delta \arrow[dl, dotted, "\psi"'] \arrow[d, two heads, "f"] \\
H \rtimes \Delta' \arrow[r, two heads, "g"'] & H^{p,el} \rtimes \Delta'
\end{tikzcd}$$

has a proper continuous solution ψ.

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

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

Since G is uniform, $G_{n+k-1}/G_{n+k} \simeq \mathfrak{g}_p$, 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 Proposition 1.2 and (i) 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 1.12 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 $\bigcap_n H_{[n]} = \{1\}$. □

Remark 3.4. — Observe that $H \rtimes \Delta' \hookrightarrow Gl_m(\mathbb{Z}_p)$. 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 or the map Pr_M 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-adic analytic group G for which the Lie algebra is semisimple, there exist a continuous Galois representation $\rho : Gal(\overline{k}/k) \to Gl_m(\mathbb{Z}_p)$ with image commensurable with G.*

Proof. — Our hypotheses imply the pro-p group $G_{k,p}$ is free of p-rank $r_2 + 1 \geqslant 2$. Let $U \subset G$ be a uniform subgroup of G. The group U is commensurable with a subgroup H generated by 2 elements (Corollary 2.12). We conclude by noting that H is a quotient of $G_{K,p}$, thanks to the universal property of free groups. □

When k is totally real (and p is odd), 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. — The principle proposed is the one developed by Greenberg [**11**], with a generalization based on Theorem 3.3 when the field of the residue image is not p-rational.

- 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 $\Gamma = Gal(K_p/k) \simeq G_{K,p} \rtimes \Delta$.

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 1.6.

- 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.
- Let $\rho_0 : \Delta \hookrightarrow Gl_m(\mathbb{Z}_p)$ be a Galois representation of $Gal(K/k)$. Set $\Delta' := \rho_0(\Delta)$.
- Let $G \subset Gl_m^1$ be a uniform group, and let H be a closed subgroup of G as in Section 3.2.

We suppose now that Δ' acts by conjugation on H, such that there exists a Δ-isomorphism $\beta : H^{p,el} \to M$.

Hence, we also get $Gal(L/K) \rtimes \Delta \simeq H^{p,el} \rtimes \Delta'$. We then have a continuous Galois representation

$$\rho_1 : Gal(K_p/k) \to H^{p,el} \rtimes \Delta'$$

such that:

(i) $(\rho_1)_{|Gal(K_p/K)} = \beta^{-1} \circ Pr_M$,

(ii) $\rho_{1|_\Delta} = \rho_0$.

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

If K is p-rational, which is the context of [**11**], one can apply Proposition 1.4 to obtain:

Corollary 4.2. — *If $G_{K,p}$ is free, 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.*

If K is not p-rational, we use Theorem 3.3.

- As 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 4.3. — *If $\ker(\iota_{K,p}) = 1$ and $\mathscr{T}_{K,p}[p] \perp \mathfrak{g}_p$, then 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.*

By Proposition 1.9 observe that $\ker(\iota_{K,p}) = 1$ and $\mathscr{T}_{K,p}[p] = 1$ imply that K is p-rational.

Remark 4.4. — Let $\rho' : Gal(K_p/k) \to Gl_m(\mathbb{Z}_p)$ be a Galois representation having image commensurable with $Sl_m(\mathbb{Z}_p)$, and unramified outside a finite set S that contain all p-adic places. 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 $Gl_m(\mathbb{Z}_p)$. Observe also that ρ is unramified outside S.

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 $G_{K,p}$ is free pro-p. By Proposition 1.15, $\chi(G_{K,p}^{p,el}) = \mathbf{1} + \varphi$. 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 the 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 commensurable.

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

Proof. — Apply Corollary 4.2: there exists a continuous Galois representation $\rho' : Gal(K_p/\mathbb{Q}) \to Sl_m^1 \rtimes \rho_0(\Delta) \hookrightarrow Gl_m(\mathbb{Z}_p)$ with image containing Sl_m^k for some $k \gg 0$, as open subgroup. We conclude with Remark 4.4. □

As a corollary, we obtain:

Corollary 4.6 **(Theorem A)**. — *There exist continuous Galois representations ρ : $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ 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 [**18**]), $p \nmid |Cl_K|$, and therefore K is p-rational (see Example 1.10). For $p = 3$, the number field $\mathbb{Q}(\sqrt{-3})$ is 3-rational. Apply Theorem 4.5. □

Remark 4.7. — Observe that ramification at 2 only occurs in $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$.

4.3. Galois representations via $\mathbb{Q}(\zeta_p)$. —

4.3.1. When the maximal 2-subextension of $\mathbb{Q}(\zeta_p)$ is p-rational. — Let a be the odd part of $p-1$; in other words, $p - 1 = a2^\lambda$ with $2 \nmid a$; so $\lambda = v_2(p-1)$.

Take $k = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_p)$ and let K/k be the maximal 2-extension in L. Let s be a generator of $\Delta = Gal(K/\mathbb{Q})$. Recall that $\iota_{K,p}$ is injective, and by Proposition 1.15,

$$\chi(\mathscr{F}_{K,p}/p) = \mathbf{1} + \omega^a + \omega^{3a} + \cdots + \omega^{(p-2)a},$$

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 $H = \langle g_1, g_2 \rangle \subset Sl_m^1$.

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.

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 $v_2(m-2) \geqslant v_2(p-1)$.

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

Let us start with a character ω^{k_i} that appears in $\chi(Cl_L[p])$, that is equivalent to say that ω^{1-k_i} appears in $\chi(\mathscr{T}_{L,p}[p])$. The characters of $\mathscr{T}_{L,p}[p]$ are ω^{1-k_i}, and such a character becomes a character of $\mathscr{T}_{K,p}[p]$ if and only if a divides $k_i - 1$.

Hence K is p-rational if and only if $a \nmid k_i - 1$ for every i. By using Corollary 4.2 and Remark 4.4, we obtain:

Corollary 4.8. — *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.*

Example 4.9. — For $p \leqslant 4 \cdot 10^5$, there are only six cases for which (ii) fails, and the index of irregularity e_p is 1 for all of them:

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

.

4.3.2. Open image in T_m. — Let $T_m \subset Gl_m(\mathbb{Z}_p)$ be the group of upper triangular matrices with diagonal entries equal to 1.

In this part we propose to give a strategy to produce Galois representations $\rho : G_\mathbb{Q} \to Gl_m(\mathbb{Z}_p)$ with open image in T_m and unramified outside $\{p, \infty\}$.

Let $\mathfrak{t}_m \subset \mathfrak{gl}_m$ be the $\mathbb{Z}_p$-lie algebra generated by the matrices $E_{i,j}(p)$, $i < j$. The algebra $\mathfrak{t}_m$ is powerful. Let $T_m^1 := exp(\mathfrak{t}_m)$ be the exponential of $\mathfrak{t}_m$. Then $T_m^1 = T_m \cap Gl_m^1$, T_m^1 is uniform and open in T_m.

Let us consider the following elements $z_1 := E_{1,2}(p), \cdots, z_{m-1} := E_{m-1,m}(p)$. It is not difficult to see that the z_i, $i = 1, \cdots, m-1$, generate the Lie algebra $\mathfrak{t}_m(\mathbb{Q}_p)$.

Let H be the closed subgroup of T_m^1 generated by the $g_i := exp(z_i)$'s, $i = 1, \cdots, m-1$. The pro-p group H is of p-rank $m-1$ and commensurable with T_m^1.

Set $\lambda = (p-1)/2$. We assume first that $m \leqslant \lambda$.

We are still using $L = \mathbb{Q}(\zeta_p)$ as in the previous section. Let s be a generator of $\Delta = Gal(L/\mathbb{Q})$. Recall that $\iota_{L,p}$ is injective, and

$$\chi(\mathscr{F}_{L,p}/p) = \mathbf{1} + \omega + \omega^3 + \cdots + \omega^{(p-2)}.$$

Let ω^{k_i} be the characters that appear in Cl_L, $i = 1, \cdots, e_p$.

Let b be an (odd) integer coprime to $p-1$. Set $B_b(s) = \sum_{i=1}^{m} \omega^{ba_i}(s) E_{i,i}$, where $a_i = 0$ for i odd, and $a_i = i-1$ for i even.
Consider the Galois representation $\rho_0 : Gal(L/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ defined by $\rho_0(s) = B_b(s)$. Then for $1 \leqslant i < m$,

$$B_b(s) \cdot z_i = \begin{cases} \omega^{-bi}(s)\ z_i & i \text{ odd}, \\ \omega^{b(i-1)}(s)\ z_i & i \text{ even}. \end{cases}$$

Of course $B_b(s)$ acts also on T_m^1, and the characters that appear in the decomposition of $\chi(\mathfrak{t}_m)$ are like $\omega^{b(j-l)}$ with $1 \leqslant j, l \leqslant m$.
By the choice of b, observe that the action of Δ on $H/H^{p,el}$ is compatible with the action on $\mathscr{F}_{L,p}$. Hence by Theorem 3.3 the realization of $H \rtimes \Delta$ as Galois extension of $\mathbb{Q}$ can be done when $b(j-l) \not\equiv k_i - 1 \bmod p-1$, for every $1 \leqslant j, l \leqslant m$ and $i = 1, \cdots, e_p$: in this case the characters appearing in $\chi(\mathfrak{t}_m)$ and in $\chi(\mathscr{T}_{L,p})$ are distinct, giving us orthogonality. Of course this is automatic when $e_p = 0$.

Let us give an explicit criteria. To simplify, one assumes that the index of irregularity e_p of p is equal to 1. Let $0 \leqslant n_b < p-1$ be the representant of $b^{-1}(k_1 - 1)$ modulo $p-1$. Set $N_p = max_b\big(min(n_b, p-1-n_b)\big)$, and observe that for every $1 \leqslant j, l \leqslant N_p$, one has $b(j-l) \not\equiv k_1 - 1$ modulo $p-1$. We have proven (with Remark 4.4):

Corollary 4.10. — *Suppose that $e_p = 1$. There exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$ and with open image in T_m, for every $m \leqslant N_p$.*

Example 4.11. — • Take $p = 37$. Then $e_p = 1$, $k_1 = 5$, and $N_p = 16$.
• Take $p = 257$. Then $e_p = 1$, $k_1 = 93$, and $N_p = 124$.

It is possible to give some asymptotic estimate.

***Corollary 4.12* (Corollary C)**. — *Let $e \geqslant 0$, and let p be a prime number such that $e_p \leqslant e$. There is a constant c_e depending on e such that for every $m \leqslant c_e(p-1)^{1/(e+1)}$, there exist continuous Galois representations $\rho : G_{\mathbb{Q}} \to Gl_m(\mathbb{Z}_p)$ unramified outside $\{p, \infty\}$ and with open image in T_m. One can take $c_0 = 1/2$ and $c_1 = 1/4$.*

Proof. — When $e = 0$, L is p-rational, and the only condition is $m \leqslant \lambda = \dfrac{p-1}{2}$.
More generally we study the equation

$$b(j-l) \equiv k_i - 1 \pmod{p-1}, \tag{3}$$

$1 \leqslant j, l \leqslant m$ and $i = 1, \cdots, e_p$. One can assume $1 \leqslant k_i - 1 \leqslant \lambda$, and observe that $j \neq l$.

Let $q > 1$ be an integer coprime to $p-1$. Suppose that $q^e \leqslant \lambda$. Among the $e+1$ intervals $[1, q), [q, q^2), \cdots, [q^j, q^{j+1}), \cdots, [q^e, \lambda]$, at least one interval I contains no $k_i - 1$; write $I = [q^{i_0}, q^{i_0+1})$ or $I = [q^e, \lambda]$.
Set $b = q^{i_0}$, and consider the Galois representation $\rho_0 : Gal(K/\mathbb{Q}) \to Gl_m(\mathbb{Z}_p)$ defined as before by $\rho_0(s) = B_b(s)$. Observe now that $q^{i_0}(j-l) \in I$ if $m \leqslant q$ and $m \leqslant \lambda/q^e$; the last condition corresponds to the case where $I = [q^e, \lambda]$. In other words, the equation (3) has no solution: the characters of the action of Δ on $H^{p,el}$ avoid the ω^{k_i-1}'s. When $q = o(\lambda^{e+1})$ these two bounds are essentially the same; and in this case $m \ll_e q^{1/(e+1)}$ is suitable. For this, observe now that one can find an integer q coprime to $p-1$ between $\lambda^{1/(e+1)}$ and $\lambda^{1/(e+1)} + c(log(p))^2$, where c is an absolute constant: this is the bound of Iwaniec [**14**] for the Jacobsthal's function; we then have $\lambda^{1/(e+1)} < q < c'_e \lambda^{1/(e+1)}$. Set $c_e = \left((c'_e)^e 2^{1/(e+1)}\right)^{-1}$; observe that $m \leqslant c_e(p-1)^{1/(e+1)}$ implies $m \leqslant q$ and $q^e m \leqslant \lambda$ (the existence of a such positive integer m implies $q^e \leqslant \lambda$ which is a condition above).
When $e = 1$: by Bertrand's postulate one knows that there exists a prime q coprime to $p-1$ such that $\sqrt{2\lambda} < q < 2\sqrt{2\lambda}$. Here $m \leqslant \dfrac{1}{4}\sqrt{p-1}$ implies $m \leqslant q$ and $qm \leqslant \lambda$.
The end of the proof is an application of Theorem 3.3 with Remark 4.4. □

4.4. Other perspectives: Galois representations partially ramified at p. — Let K be a number field, let S be a finite set of primes of K, and let K_S be the maximal pro-p extension of K unramified outside S; set $G_S = Gal(K_S/K)$. A part of the results of Section 1.2 can be adapted to G_S; this section has been written with this idea in mind. A key result to apply Theorem 3.3 is Proposition 1.6. As noted in [**19**, §3], one may have $H^2(G_S, \mathbb{Q}/\mathbb{Z}) = 0$, and eventually G_S free, even if S does not contain all places above p. Hence, clearly our strategy can produce Galois representations $\rho : G_S \to Gl_m(\mathbb{Z}_p)$ with open image, and for which the ramification at p is partial.

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] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, Mathematical Proceedings of the Cambridge Philosophical Society **166** (2019), 599-617.

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

[14] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Mathematica **11** (1978), no. 1, 225–231.

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

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

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

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

[19] C. Maire, *Sur la dimension cohomologique des pro-p-extensions des corps de nombres*, J. Th. des Nombres de Bordeaux **17** fasc. 2 (2005), 575-606.

[20] 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.

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

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

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

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

[25] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. **15** (1972), no. 4, 259-331.

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

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

[28] I.R. Shafarevich, *Extensions with given ramification points*, Publ. Math. IHES **18** (1964), 295-319.

[29] S. Tang, *A note on Galois representations valued in reductive groups with open image*, Journal of Number Theory, to appear.

[30] K. Wingberg, *Free pro-p-extensions of number fields*, preprint 2005.

March 17, 2023

Christian Maire, Université de Franche-Comté, CNRS, Institut FEMTO-ST, 15B avenue des Montboucons, 25000 Besançon, FRANCE • *E-mail :* `christian.maire@univ-fcomte.fr`