J. Ramanujan Math. Soc. **37,** No.1 (2022) 63–85

Analytic Lie extensions of number fields with cyclic fixed points and tame ramification

Farshid Hajir[1] and Christian Maire[2]

[1]*Department of Mathematics & Statistics, University of Massachusetts, Amherst MA 01003, USA*
e-mail: hajir@math.umass.edu

[2]*Institut FEMTO-ST Université Bourgogne Franche-Comté, 15B Avenue des Montboucons, 25030 Besançon cedex, France*
e-mail: christian.maire@univ-fcomte.fr

Communicated by: Prof. Florian Herzig

Received: December 4, 2019

Abstract. Let p be a prime number and K an algebraic number field. What is the arithmetic structure of infinite Galois extensions L/K having p-adic analytic Galois group $\Gamma = \mathrm{Gal}(L/K)$? The celebrated Tame Fontaine-Mazur conjecture predicts that such extensions are either deeply ramified (at some prime dividing p) or ramified at an infinite number of primes. In this work, we take up a study (initiated by Boston) of this type of question under the assumption that L is Galois over some subfield k of K such that [K : k] is a prime $\ell \neq p$. Letting σ be a generator of Gal(K/k), we study the constraints posed on the arithmetic of L/K by the cyclic action of σ on Γ, focusing on the critical role played by the fixed points of this action, and their relation to the ramification in L/K. The method of Boston works only when there are no non-trivial fixed points for this action. We show that even in the presence of arbitrarily many fixed points, the action of σ places severe arithmetic conditions on the existence of finitely and tamely ramified uniform p-adic analytic extensions over K, which in some instances leads us to be able to deduce the non-existence of such extensions over K from their non-existence over k.

2000 Mathematics Subject Classification: 11R37, 22E20, 11R44.

1. Introduction

1.1 Background

Fix a prime p. The theory of pro-p groups has seen major advances in the last few decades. In particular, the monumental work [17] of Lazard on *p-adic analytic* groups (that is to say Lie groups over the field $\mathbb{Q}_p$ of p-adic numbers) has been simplified and reinterpreted beginning in the work of Lubotzky and Mann in the 1980s. An excellent treatment of this new viewpoint is given in the book [7] by Dixon, du Sautoy, Mann, and Segal and has made the subject more readily applied in many situations and much more accessible to a variety of non-experts. At the same time, the theory of Galois representations encodes vast amounts of arithmetic information via action of Galois groups on finite-dimensional p-adic vector spaces, giving rise to continuous homomorphisms from Galois groups to the p-adic Lie groups $\mathrm{Gl}_n(\mathbb{Q}_p)$. In this paper, we are interested in using group-theoretical information to derive consequences for *finitely and tamely* ramified Galois representations.

In [8], Fontaine and Mazur propose a characterization of all Galois representations which arise from the action of the absolute Galois group of K on Tate twists of étale cohomology groups of algebraic varieties defined over K: namely they predict that these are precisely the representations which are ramified at a finite number of primes of K and are potentially semistable at the primes dividing p. This is in essence, a vast "modularity" conjecture. If we restrict our attention to p-adic representations which are finitely and tamely ramified, we obtain the following consequence (Conjecture 5a of [8]) of this characterization (see Kisin-Wortmann [16] for the details).

Conjecture (Tame Fontaine-MazurConjecture). For a finite set S of primes of K of residue characteristic not equal to p, and $n \geq 1$, any continuous Galois representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gl}_n(\mathbb{Q}_p)$ which is unramified outside S has finite image.

The philosophy of this conjecture rests on the idea that the eigenvalues of Frobenius (under a finitely and tamely ramified p-adic representation ρ) ought to be roots of unity. Consequently, the image of such a representation is solvable, and hence finite by class field theory (because its open subgroups have finite abelianization). We refer the reader to [16] for further details.

One immediately checks the Conjecture for $n = 1$ by Class Field Theory. For $n > 1$, on the other hand, the Tame Fontaine-Mazur Conjecture in general appears to be completely out of reach, and the evidence for it for $n > 2$ is rather preliminary. However, for $K = \mathbb{Q}$, and $n = 2$, the pioneering methods of Wiles and Taylor-Wiles can be used to show that many types of 2-dimensional representations do come from algebraic geometry (in fact from weight one modular forms) and hence have finite image. As a partial list of such results, we refer the reader to Buzzard-Taylor [5], Buzzard [4], Kessaei [14], Kisin [15], Pilloni [21], Pilloni-Stroh [22].

We recall that a pro-p group Γ is called *uniform* if it is torsion-free and if moreover $\Gamma^{p^\varepsilon} = \langle x^{p^\varepsilon},\ x \in \Gamma \rangle$ contains the commutators $[\Gamma, \Gamma]$ of Γ where $\varepsilon = 1$ for $p > 2$ and $\varepsilon = 2$ for $p = 2$. By Lazard [17] (see also [7]), every finite-dimensional p-adic analytic group (closed subgroup of $\mathrm{Gl}_n(\mathbb{Q}_p)$ for some $n \geq 1$) has a finite-index (open) uniform subgroup. Moreover, a uniform group of dimension 1 or 2 has a quotient isomorphic to $\mathbb{Z}_p$. Thus, the Tame Fontaine-Mazur conjecture can be rephrased as follows.

Conjecture (Tame Fontaine-Mazur Conjecture – Uniform Version). Suppose K is a number field, and Γ is a uniform pro-p group of dimension $d > 2$, hence infinite. Then there does not exist a finitely and tamely ramified Galois extension L/K with Galois group $\Gamma = \mathrm{Gal}(L/K)$.

Our aim in this paper is to provide some evidence for the above conjecture. The first such evidence, in the case of unramified extensions, was provided by Boston (see [2] and [3]). In this paper, we extend Boston's ideas to the tamely ramified case.

1.2 Boston's Theorem

In [2] and [3], Boston initiated the study of the following situation (see also Wingberg [24] and Maire [19]). We fix a uniform pro-p group Γ and assume that Γ is realized as the Galois group of a *finitely and tamely ramified* extension L/K, i.e. $\Gamma = \mathrm{Gal}(L/K)$, and we assume, moreover, that Γ is equipped with a semi-simple Galois action. To be more explicit, from now on we assume that:

- K is a finite Galois extension of a number field k with Galois group $\Delta = \mathrm{Gal}(K/k)$
- Δ is a cyclic group of prime order ℓ dividing $p - 1$, and we fix a generator σ of Δ
- L/K is a finitely and tamely ramified Galois extension which is Galois over k
- $\Gamma = \mathrm{Gal}(L/K)$ is a uniform pro-p group of finite dimension d (as p-adic manifold).

Theorem (Boston). Under the above assumptions, if in addition

- p does not divide the order of the class group of k, and
- L/K is everywhere unramified,

then Γ is trivial.

Boston's theorem gave the first substantive corroboration of the conjecture of Fontaine and Mazur in that it precludes the existence of certain (non-abelian) uniform unramified Galois extensions. Here's the strategy of Boston's proof of the above result. The assumptions made in the theorem imply that σ acts without non-trivial fixed points on Γ^{ab} (to simplify the terminology, we say by way of shorthand that the action of σ is "FPF (fixed-point-free)"). By the uniformity of Γ the action of σ is fixed-point-free also on Γ. The existence of this fixed-point-free cyclic action on Γ implies that Γ is nilpotent (see Proposition 3.4). We recall that a group is called FAb if for all open subgroups U, the abelianization U^{ab} is finite. Since L/K is tamely ramified, Γ is FAb. Since Γ is both nilpotent and FAb, it is finite; but as a uniform group, it is torsion-free, hence must be trivial.

In this work, we attempt to extend Boston's strategy from the unramified case to the case of (tamely) ramified L/K. The key challenge is to handle the fixed points introduced by ramification because Boston's proof relies heavily on the fact the σ-action in the unramified case is fixed-point-free. We refer to [11] for a different application of this phenomenon in the context of Iwasawa theory where one allows wild ramification in L/K.

In order to state our results, we need to introduce some more notation and hypotheses. Let S be a finite set of places of K all of which are prime to p (we say that the set S is tame and indicate this by writing $(S, p) = 1$). Since we will be working with p-extensions in which the primes in S are allowed to ramify, we further assume that for finite places $\mathfrak{p} \in S$, we have $\#\mathcal{O}_{\mathrm{K}}/\mathfrak{p} \equiv 1 (\mathrm{mod}\ p)$. We let K_S be the maximal pro-p extension of K unramified outside S and we put $\mathrm{G}_S = \mathrm{G}_S(\mathrm{K}) = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.

Let us also take an auxiliary finite set T of places of K, disjoint from S, and define K_S^T to be the maximal pro-p extension of K unramified outside S and in which the places in T split completely. We put $\mathrm{G}_S^T = \mathrm{G}_S^T(\mathrm{K}) = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$. We note then that $\mathrm{K}_S^T \subset \mathrm{K}_S$, that $\mathrm{G}_S \twoheadrightarrow \mathrm{G}_S^T$ and that $\mathrm{K}_S^{\emptyset} = \mathrm{K}_S$.

Recall that K is a number field admitting a non-trivial automorphism σ of prime order ℓ dividing $p - 1$, and $\mathrm{k} = \mathrm{K}^{\sigma}$ is the fixed field of $\Delta = \langle \sigma \rangle$. We will assume that the sets S and T described above are stable under the action of σ. Thus, the extension $\mathrm{K}_S^T/\mathrm{k}$ is Galois and σ acts on $\mathrm{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.

Definition 1.1. *Consider a continuous Galois representation* $\rho : \mathrm{G}_S^T(\mathrm{K}) \to \mathrm{Gl}_n(\mathbb{Q}_p)$*, and let* L *be the subfield of* K_S^T *fixed by* $\ker(\rho)$ *so that the image* Γ *of* ρ *is naturally identified with* $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$*. We say that* ρ *(or* Γ*) is* σ-uniform *if we have (i)* $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *is uniform; and (ii)* L/k *is Galois, i.e. the action of* σ *on* $\mathrm{G}_S^T(\mathrm{K})$ *induces an action on* Γ*.*

For a finitely generated pro-p group G, recall that a closed subgroup generated by pth powers and commutators, $\Phi(G) = G^p[G, G]$, is the *Frattini subgroup* of G; it is a characteristic subgroup of finite index. The *Frattini quotient* $G^{p,\mathrm{el}} := G/\Phi(G)$ is the maximal abelian exponent p quotient of G. The method of Boston described in §1.1 in the unramified case carries over to G_S^T without any trouble only if the action of σ on Γ is FPF. More precisely, if the action of σ on $\mathrm{G}_S^T/\Phi(\mathrm{G}_S^T)$ is fixed-point-free, then any σ-uniform representation of G_S^T has trivial image. As indicated above, we try to extend the method by introducing fixed points that result from allowing tame ramification. We show that even in the presence of non-trivial fixed points, all σ-uniform quotients of G_S^T are trivial as long as the "new" ramification is restricted to the subgroup generated by the fixed points. In §2, we will present our results in greater generality, but we first illustrate them by presenting a special case for the well-known uniform and FAb pro-p group $\mathrm{Sl}_2^1(\mathbb{Z}_p) := \ker\big(\mathrm{Sl}_2(\mathbb{Z}_p) \to \mathrm{Sl}_2(\mathbb{Z}/p\mathbb{Z})\big)$ of dimension 3 (p odd).

Theorem A. *Suppose* K/k *is a quadratic extension with Galois group* $\Delta = \langle \sigma \rangle$ *such that the odd prime* p *does not divide the class number of* k*. Then there exist infinitely many disjoint finite sets* S *and* T *of primes of* K*, with* $(S, p) = 1$ *and* $|S|$ *arbitrarily large, such that*

(i) $\mathrm{G}_S^T(\mathrm{K})$ *is infinite,*

(ii) *under the action of* σ*, there are* $|S|$ *independent fixed points in* $\mathrm{G}_S^T(\mathrm{K})^{p,\mathrm{el}}$*,*

(iii) *all continuous* σ*-uniform representations* $\rho : \mathrm{G}_S^T \twoheadrightarrow \mathrm{Sl}_2^1(\mathbb{Z}_p)$ *come from* k *by compositum from* K*.*

As corollary of Theorem A, one has:

Corollary B. *Under the conditions of Theorem A, if the Tame Fontaine-Mazur conjecture holds for* k *then there is no continuous* σ*-uniform representation* $\rho : \mathrm{G}_S^T(\mathrm{K}) \twoheadrightarrow \mathrm{Sl}_2^1(\mathbb{Z}_p)$*.*

In the simplest open case of the above conjecture, one can take $\mathrm{K} = \mathbb{Q}$ and $\Gamma = \mathrm{Sl}_2^1(\mathbb{Z}_p)$. We must then show that $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ cannot be realized as the Galois group of a finitely and tamely ramified Galois extension over $\mathbb{Q}$. Given the recent spectacular breakthroughs coming from the Taylor-Wiles method, perhaps the current methods will one day prove sufficient to establish this special case of the Tame Fontaine-Mazur conjecture, but at the moment the theory of even Galois representations is still under-developed by comparison with odd ones. We should emphasize that in this work, we rely exclusively on group-theoretical methods. However, as automorphic methods approach a full proof of the tame Fontaine-Mazur conjecture (for 2-dimensional representations at least) over $\mathbb{Q}$, one would be apply to use the group-theoretical techniques discussed here to deduce some cases of the Tame Fontaine-Mazur conjecture over quadratic fields from known cases over $\mathbb{Q}$.

2. Presentation of results

2.1 A key definition

Recall that Γ is a uniform pro-p group equipped with the action of an automorphism σ of prime order $\ell \mid p-1$. We denote by

$$\Gamma_\sigma^\circ = \langle \gamma \in \Gamma, \sigma(\gamma) = \gamma \rangle,$$

the closed subgroup of Γ generated by the fixed points of Γ under the action of σ, and let Γ_σ be its normal closure in Γ. Let $G := \Gamma/\Gamma_\sigma$.

Definition 2.1. *With the above assumptions, the action of σ on Γ is said to be* fixed-point-mixing modulo Frattini *(*FPMF*) if $G = \Gamma/\Gamma_\sigma$ acts non-trivially on $\Gamma_\sigma/\Phi(\Gamma_\sigma)$.*

This notion will be essential for our work; its relevance is explained at the end of §2.3. Let us give two examples that we will study in section 3.4 and will be important to illustrate our results.

Example 2.2 (See §3.4.1). *If a FAb and uniform pro-p group of dimension 3 admits non-trivial action by an automorphism σ of order 2, then this action is fixed-point-mixing modulo Frattini. Thus, any involution which acts non-trivially on the linear group $\mathrm{Sl}_2^1(\mathbb{Z}_p) := \ker\big(\mathrm{Sl}_2(\mathbb{Z}_p) \to \mathrm{Sl}_2(\mathbb{Z}/p\mathbb{Z})\big)$ is fixed-point-mixing modulo Frattini.*

Example 2.3 (See §3.4.2). *More generally, for the FAb pro-p group*

$$\mathrm{Sl}_n^1(\mathbb{Z}_p) := \ker\big(\mathrm{Sl}_n(\mathbb{Z}_p) \to \mathrm{Sl}_n(\mathbb{Z}/p\mathbb{Z})\big) \qquad n \geq 2,$$

and the automorphism σ_A coming from conjugation by a matrix $A \in \mathrm{Gl}_n(\mathbb{Z}_p)$ of order 2, the action of σ_A is fixed-point-mixing modulo Frattini.

2.2 When σ is of order 2

The case where the automorphism σ is an involution, i.e. $\ell = 2$, is particularly interesting. Let us begin with a definition.

Definition 2.4. *Let Γ be a uniform group of dimension d, which also then equals the p-rank of Γ, i.e. $\Gamma/\Phi(\Gamma)$ is a d-dimensional vector space over $\mathbb{F}_p$. Suppose $\sigma \in \mathrm{Aut}(\Gamma)$ has order 2. If the multiplicity of the trivial character in the action of σ on $\Gamma/\Phi(\Gamma)$ is r, we say that the action of σ on Γ is of type $(r, d-r)$ and write $t_\sigma(\Gamma) = (r, d-r)$.*

Under our blanket assumption that σ is non-trivial, it is easy to see that $t_\sigma(\Gamma) \neq (d, 0)$. In [2] and [3], the assumption is always that $t_\sigma(\Gamma) = (0, d)$. In this work, we consider the more general intermediate types $t_\sigma(\Gamma) = (r, d-r)$ with $0 < r < d$, by allowing tame ramification.

The result we want to present will involve the Hilbert p-class field K^H of K so we recall this concept. Recalling that the prime p has been throughout fixed, we let $\mathrm{Cl}(\mathrm{K})$ be the p-Sylow subgroup of the ideal class group of K and K^H the maximal abelian unramified p-extension of K. The Artin map gives a canonical isomorphism $\mathrm{Cl}(\mathrm{K}) \to \mathrm{Gal}(\mathrm{K}^H/\mathrm{K})$. More generally, if S is a finite tame set of places of K and T is another finite set of places disjoint from S, Cl_S^T will be the p-Sylow subgroup of the T-ray class group of K mod S, which corresponds via the Artin map to $\mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})^{ab}$. As before, put $\mathrm{G}_S^T = \mathrm{G}_S^T(\mathrm{K}) = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.

Theorem C. *Let $p > 2$ and let $s \in \mathbb{N}$. Let K/k be a quadratic extension with Galois group $\Delta = \langle\sigma\rangle$ such that p does not divide $|\mathrm{Cl}(\mathrm{k})|$. Let T be a finite set of places of k that totally splits in K^H/K of large enough cardinality (see Theorem 4.1 for a more exact statement), and such that $\mathrm{Cl}_\emptyset^T(\mathrm{K}^H)$ is trivial. Then there exist s pairwise disjoint positive-density sets $\mathcal{S}_i$, $i = 1, \ldots, s$ of prime ideals $\mathfrak{p} \subset \mathcal{O}_\mathrm{k}$ of k such that for finite sets $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathcal{S}_i$, we have*

(i) *under the action of σ, there are s independent fixed points in $\mathrm{G}_S^T/\Phi(\mathrm{G}_S^T)$;*
(ii) *there is no continuous representation $\rho : \mathrm{G}_S^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image Γ which is fixed-point-mixing modulo Frattini.*

We can apply Theorem C to the groups $\mathrm{Sl}_n^1(\mathbb{Z}_p) = \ker\big(\mathrm{Sl}_n(\mathbb{Z}_p) \to \mathrm{Sl}_n(\mathbb{Z}/p\mathbb{Z})\big)$, $n \geq 2$. For all $n \geq 2$, $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ is a uniform FAb group of dimension $n^2 - 1$. We consider automorphisms σ_A of order 2 obtained via conjugation by a diagonalizable matrix $A \in \mathrm{Gl}_n(\mathbb{Z}_p)$.

Corollary D. *Under the conditions of Theorem C, there exist s positive-density sets $\mathcal{S}_i$, $i = 1, \ldots, s$ of prime ideals $\mathfrak{p} \subset \mathcal{O}_\mathrm{k}$ of* k*, such that for all finite sets $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathcal{S}_i$, and all $n \geq 2$, there does not exist a continuous representation $\rho : \mathrm{G}_S^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ where the involution $\sigma = \sigma_A$ is conjugation by a diagonalizable matrix $A \in \mathrm{Gl}_n(\mathbb{Z}_p)$.*

2.3 Strategy of the proofs and outline of the rest of the paper

Our main results combine a number of ingredients: the effect of a semisimple cyclic action with fixed points on group structure, the rigid structure of uniform groups, arithmetic properties of the arithmetic fundamental groups G_S^T, existence of Minkowski units, etc. In this subsection, we will give an outline of how these ingredients are combined together.

- *Criteria for infinitude of* G_S^T. Let us consider the context of Theorem C. In the statement of that theorem, we refer to the need for T to be "large enough" and here we wish to explain this a bit more. In order to arrange to have enough fixed points, we want to take

$$|T| \geq \alpha s + \beta, \tag{1}$$

with α and β depending on K. On the other hand, by the theorem of Golod-Shafarevich, the group G_S^T is infinite when the p-rank of G_S^T is sufficiently large. To be more exact, if

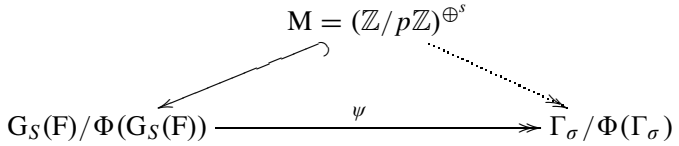
$$d_p\mathrm{G}_S^T \geq 2 + 2\sqrt{|T| + r_1 + r_2 + 1}, \tag{2}$$

where (r_1, r_2) is the signature of K, the pro-p group G_S^T is infinite (see for example [18]). Moreover, the p-rank of G_S^T is at least s (because of the choice of S and T). Hence, by (1) and (2), one can guarantee the infiniteness of G_S^T by taking s sufficiently large, *i.e.* by introducing sufficiently many fixed points.
- *Uniform groups* (Section 3). Next we turn to the situation where a cyclic group $\langle\sigma\rangle$ of order ℓ, with $\ell \mid p-1$, acts on a uniform group Γ. In particular we focus on the subgroup Γ_σ° generated by the fixed points and its normal closure in Γ, denoted Γ_σ. Here, the key result is Proposition 3.7: it specifies generators for Γ_σ and is crucial for the rest of our work. When Γ is FAb, the quotient group $G := \Gamma/\Gamma_\sigma$, is a finite p-group. Moreover, when σ is of order 2, G is abelian.
- *The choice of the prime ideals* (§4). We fix K and consider varying sets S, T where $\mathrm{L} \subseteq \mathrm{K}_S^T$ has Galois group $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. We now assume σ has order 2. Since G is abelian, the field F fixed by Γ_σ is abelian over K. Moreover we will see that F is contained in the p-Hilbert class field K^H. To simplify further, let us assume $\mathrm{F} = \mathrm{K}^H$. The choice of prime ideals $\mathfrak{p}$ of S is based on the following desired outcomes: (i) to create enough fixed points for the action of σ; (ii) to control the generators of $\mathrm{G}_S(\mathrm{F})$ via their inertia groups. Typically, the group G, acts trivially on the new ramification in $(G_S(\mathrm{F}))^{p,el}$.
  To show the existence of such prime ideals, one uses Kummer theory and the Chebotarev density Theorem. In order to do this, we require information about the units of the number field F, namely we need F to contain "Minkowski units". To be more precise, let $\mathcal{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{k})$; we say that F has a Minkowski unit if the quotient $\mathcal{O}_\mathrm{F}^\times/(\mathcal{O}_\mathrm{F}^\times)^p$ contains a non-trivial $\mathbb{F}_p[\mathcal{G}]$-free module. Note that we are not in the semisimple case as $p \mid |\mathcal{G}|$. This delicate and interesting question has been studied in recent work of Ozaki [20]: to estimate the rank of the maximal free $\mathbb{F}_p[\mathcal{G}]$-module of $\mathcal{O}_\mathrm{F}^\times/(\mathcal{O}_\mathrm{F}^\times)^p$. Our idea here is to introduce a set T and control the $\mathbb{F}_p[\mathcal{G}]$-structure of T-units of F.

- *The strategy* (§5). There exists a morphism of $\mathbb{F}_p[G]$-modules

$$\psi : \mathrm{G}_S(\mathrm{F})/\Phi(\mathrm{G}_S(\mathrm{F})) \twoheadrightarrow \Gamma_\sigma/\Phi(\Gamma_\sigma).$$

The map ψ dictates the compatibility of two $\mathbb{F}_p[G]$-modules, one of which comes from arithmetic considerations, and the other from group-theoretical ones. We suspect that the exploitation of this kind of compatibility can be useful in many other contexts.
We now give some examples for which the structures of $\mathrm{G}_S(\mathrm{F})/\Phi(\mathrm{G}_S(\mathrm{F}))$ and of $\Gamma_\sigma/\Phi(\Gamma_\sigma)$ as $\mathbb{F}_p[G]$-modules are not compatible. Typically, the given situations are those for which the morphism ψ is deduced from a $\mathbb{F}_p[G]$-module M on which G acts trivially, namely we have a diagram as follows:



From the above diagram, one obtains a contradiction since $G = \Gamma/\Gamma_\sigma$ does not act trivially on $\Gamma_\sigma/\Phi(\Gamma_\sigma)$. This explains the relevance of the notion of the action of σ being "fixed-point-mixing modulo Frattini" that was introduced in Definition 2.1.

3. Uniform groups and Fixed Points

Let p be a prime number and let Γ be a finitely generated pro-p group.

- For two elements x, y of Γ, denote by $x^y := y^{-1}xy$ the conjugate of x by y, and by $[x, y] = x^{-1}x^y$ the commutator of x and y. Put $[\Gamma, \Gamma] = \langle [x, y], x, y \in \Gamma \rangle$ and $\Phi(\Gamma) = [\Gamma, \Gamma]\Gamma^p$;
- Let $\Gamma^{ab} := \Gamma/[\Gamma, \Gamma]$ be the maximal abelian quotient of Γ;
- The Frattini quotient $\Gamma^{p,\mathrm{el}} := \Gamma/\Phi(\Gamma)$ is the maximal abelian p-elementary quotient of Γ;
- Denote by $d_p(\Gamma) = \dim_{\mathbb{F}_p} H^1(\Gamma, \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} \Gamma^{p,\mathrm{el}}$ the p-rank of Γ: by the Burnside Basis Theorem, it is the minimal number of generators of Γ.

3.1 Schur-Zassenhaus

For this paragraph our reference is the book of Ribes and Zalesskii [23, Chapter 4].

If Γ is a finitely generated pro-p group of p-rank d, denote by $\mathrm{Aut}(\Gamma)$ the group of automorphisms (always continous) of Γ. Recall that the kernel of the morphism $\ker\big(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma^{p,\mathrm{el}})\big)$is a pro-$p$ group and that $\mathrm{Aut}(\Gamma^{p,\mathrm{el}}) \simeq \mathrm{Gl}_d(\mathbb{F}_p)$. Let us start with the following well-known result which is crucial in our context:

Theorem 3.1 (Schur-Zassenhaus). *Let* $1 \longrightarrow \Gamma \longrightarrow \mathcal{G} \longrightarrow \mathcal{G}/\Gamma \longrightarrow 1$ *be an exact sequence of profinite groups, where* Γ *is a finitely generated pro-*p *group and where* $\mathcal{G}/\Gamma$ *is finite of order coprime to* p*. Then the group* $\mathcal{G}$ *has a subgroup* Δ_0 *isomorphic to the quotient* $\Delta = \mathcal{G}/\Gamma$ *and* Δ_0 *is unique up to conjugation in* $\mathcal{G}$*. In particular:* $\mathcal{G} = \Gamma \rtimes \Delta_0 \simeq \Gamma \rtimes \Delta$*. In other words, the pointed set* $H^1(\Delta, \Gamma)$ *is reduced to* $\{[0]\}$*.*

Proof. See for example Theorem 2.3.15, [23]. □

Let us now consider a finitely generated pro-p group Γ equipped with an automorphism $\sigma \in \mathrm{Aut}(\Gamma)$ of order a prime number ℓ different from p.

Definition 3.2. *Denote by* $\Gamma_\sigma^\circ := \langle \gamma \in \Gamma, \sigma(\gamma) = \gamma \rangle$ *the closed subgroup generated by the fixed point of* Γ *and by*

$$\Gamma_\sigma := \Gamma_\sigma^{\circ\,\mathrm{Norm}},$$

the normal closure of Γ_σ° *in* Γ*.*

Of course, σ acts trivially on Γ_σ° and $\sigma \in \mathrm{Aut}(\Gamma_\sigma)$.

Definition 3.3. *We say that the action of σ on Γ is* Fixed-Point-Free (FPF) *if $\Gamma_\sigma^\circ = \{e\}$.*

Recall first a well-known result that shows the rigidity of the FPF-notion.

Proposition 3.4. *Let Γ be a pro-p group and let $\sigma \in \mathrm{Aut}(\Gamma)$ of order coprime to p. If the action of σ on Γ is FPF, then Γ is nilpotent. Moreover if σ is of order $\ell = 2$, then Γ is abelian.*

Proof. See Corollary 4.6.10, [23]. □

Now we may present the first step of our work.

Proposition 3.5. *Let Γ be a finitely generated pro-p group and $\sigma \in \mathrm{Aut}(\Gamma)$ of order ℓ coprime to p. Put $G := \Gamma/\Gamma_\sigma$. Then the action of σ on G is FPF, so G is nilpotent. If moreover Γ is FAb then G is a finite group.*

Proof. Consider the non-abelian Galois $\langle\sigma\rangle$-cohomology of the sequence:

$$1 \longrightarrow \Gamma_\sigma \longrightarrow \Gamma \longrightarrow G \longrightarrow 1,$$

to obtain the sequence of pointed sets:

$$0 \longrightarrow H^0(\langle\sigma\rangle, \Gamma_\sigma) \longrightarrow H^0(\langle\sigma\rangle, \Gamma) \longrightarrow H^0(\langle\sigma\rangle, G) \longrightarrow H^1(\langle\sigma\rangle, \Gamma_\sigma) \longrightarrow \cdots$$

By the Schur-Zassenhaus Theorem 3.1, $H^1(\langle\sigma\rangle, \Gamma_\sigma) = \{[0]\}$ and then as $\Gamma_\sigma^\circ = H^0(\langle\sigma\rangle, \Gamma) = H^0(\langle\sigma\rangle, \Gamma_\sigma)$, one obtains $H^0(\langle\sigma\rangle, G) = \{[0]\}$: in other words, the action of σ on G is FPF. Then by Proposition 3.4 the pro-p group G is nilpotent. Moreover if Γ is FAb, the pro-p group G is also FAb, one concludes that G is finite. □

3.2 Uniform pro-p groups

We first recall some basic facts about p-adic analytic groups (Lie groups over $\mathbb{Q}_p$). The main references for this section are [7] and [17].

For $i \geq 1$, denote by $\Gamma_{i+1} = \Gamma_i^p[\Gamma, \Gamma_i]$ where $\Gamma_1 = \Gamma$: it is the p-central descending series of the finitely generated pro-p group Γ. The pro-p group Γ is said *uniform* if and only if for $i \geq 1$, the map $x \mapsto x^{p^{i-1}}$ induces an isomorphism between Γ_i/Γ_{i+1} and Γ/Γ_2 and $[G, G] \subset \Gamma^{2p}$.

Let Γ be a uniform pro-p group, and let $\{x_1, \ldots, x_d\}$ be a minimal system of (topological) generators of Γ. The group Γ being uniform, the map $x \mapsto x^{p^n}$ induces a homeomorphism ψ_n between Γ and Γ_{n+1}. By taking the limit on the p^nth roots, the group Γ can be equipped with an additive law (and we denote by Γ_+ this "new" group). More precisely, put $x +_n y = \psi_n^{-1}(x^{p^n} y^{p^n})$ and

$$x + y := \lim_{n\to\infty} (x +_n y).$$

Then $\Gamma_+ := \mathbb{Z}_p x_1 \oplus \cdots \oplus \mathbb{Z}_p x_d$ is a group isomorphic to $\mathbb{Z}_p^d$.

In fact $\Gamma = \overline{\langle x_1\rangle} \cdots \overline{\langle x_d\rangle}$: for every $x \in \Gamma$, there exists a unique d-tuple $(a_1, \ldots, a_d) \in \mathbb{Z}_p^d$ such that $x = x_1^{a_1} \cdots x_n^{a_n}$. Moreover the map

$$\begin{array}{rcl} \varphi : \Gamma & \longrightarrow & \Gamma_+ \\ x = x_1^{a_1} \cdots x_d^{a_d} & \mapsto & a_1 x_1 \oplus \cdots \oplus a_n x_n \end{array}$$

is a homeomorphism (see [7], Theorem 4.9).

Let us fix $\sigma \in \mathrm{Aut}(\Gamma)$. It is not difficult to see that $\sigma(x) +_n \sigma(y) = \sigma(x +_n y)$. Hence, by passing to the limit, the action of σ becomes a linear action on Γ_+, *i.e.* $\sigma \in \mathrm{Gl}_d(\mathbb{Z}_p)$ (see §4.3 of [7]). One needs more to determine the Galois structure.

Theorem 3.6. *The map φ induces an isomorphism of $\mathbb{F}_p[\langle\sigma\rangle]$-modules between $\Gamma^{p,\mathrm{el}}$ and Γ_+/p.*

Proof. It suffices to note that φ induces an isomorphism of groups between $\Gamma^{p,\mathrm{el}}$ and Γ_+/p: it is exactly Corollary 4.15 of [7]. □

3.2.1 Semisimple action and fixed points

Recall the assumption that $\sigma \in \mathrm{Aut}(\Gamma)$ is of finite order ℓ, a prime number different from p.

The action σ on Γ_+ is semisimple, and the $\mathbb{Z}_p[\langle\sigma\rangle]$-module Γ_+ is projective. Hence the action of σ on Γ_+/p lifts uniquely (up to isomorphism) to Γ_+ and then, one can find a family of generators of Γ respecting this action, or that respects the decomposition of Γ_+ as projective modules.

Set $r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma$. The integer r corresponds to the dimension of the $\mathbb{F}_p$-vector subspace of $\Gamma^{p,\mathrm{el}}$ consisting of fixed points of $\Gamma^{p,\mathrm{el}}$.

Now let us fix a basis $\{x_1, \ldots, x_d\}$ of Γ respecting the decomposition into irreducible characters following the action of σ such that $\{x_1, \ldots, x_r\}$ corresponds to a basis of $(\Gamma^{p,\mathrm{el}})_\sigma$ *i.e.* $\sigma(x_i) = x_i$ for $i = 1, \ldots, r$. Clearly $\overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle} \subseteq \Gamma_\sigma^\circ$.

In the rest of this section, we will rely heavily on the following result.

Proposition 3.7. *Let Γ be a uniform pro-p group and let $\sigma \in \mathrm{Aut}(\Gamma)$ be of order ℓ. Suppose that $\ell \mid (p-1)$. Then, with the notation introduced above, we have*

$$\Gamma_\sigma^\circ = \overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle} = \langle x_1, \ldots, x_r\rangle\cdot$$

Proof. As ℓ divides $p-1$, the $\mathbb{Q}_p$-irreducible characters of $\langle\sigma\rangle$ are all of degree 1. In particular, by the choice of the x_i, we get that for $i > r$, $\sigma(x_i) = x_i^{\lambda_i}$, where $\lambda_i \in \mathbb{Z}_p\backslash\{1\}$.

Take $x \in \Gamma_\sigma^\circ$ and let us write $x = x_1^{a_1} \cdots x_d^{a_d}$. Then $x = \sigma(x)$, if and only if,

$$\prod_{i=1}^{d} x_i^{a_i} = \prod_{i=1}^{d} \sigma(x_i)^{a_i}\cdot$$

Thanks to the uniqueness of the product, one deduces that for $i > r$, $\lambda_i a_i = a_i$, *i.e.*, $a_i = 0$ because $\lambda_i \neq 1$. One has proven that $\Gamma_\sigma^\circ = \overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle}$. On the other hand, trivially $\langle x_1, \ldots, x_r\rangle \subset \Gamma_\sigma^\circ$ and $\overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle} \subset \langle x_1, \ldots, x_r\rangle$, which prove the desired equalities. □

We recover here, with a weaker hypothesis, *i.e.* $\ell \mid (p-1)$, the following corollary used in [11]:

Corollary 3.8. *Let Γ be a uniform pro-p group. Under previous conditions, $\Gamma_\sigma^\circ = \{e\}$ if and only if $(\Gamma^{p,\mathrm{el}})_\sigma = \{\overline{e}\}$.*

Corollary 3.9. *Suppose that σ is of order 2, then $d_p(\Gamma/\Gamma_\sigma) = d - r$ where $d = d_p\Gamma$ and $r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma$.*

Proof. Put $G = \Gamma/\Gamma_\sigma$. Consider the minimal system of generators $(x_i)_{i=1,\ldots,d}$ of Γ introduced above, satisfying in particular that $\sigma(x_i) = x_i$ for $i = 1, \ldots, r$. The group Γ_σ contains the elements $x_1, \ldots, x_r$. The quotient G is topologically generated by the classes $x_i\Gamma_\sigma$, $i > r$, so $d_pG \leq d - r$. In fact, the classes $(x_i\Gamma_\sigma)_{i>r}$ form a minimal system of generators of G: indeed, if not it would show that (possibly after renumbering) the class $x_{r+1}\Gamma_\sigma$ can be expressed in terms of the classes $x_i\Gamma_\sigma$, $i \geq r+2$, which would imply that the class $x_{r+1}[\Gamma, \Gamma]$ could be written in terms of the classes $\big(x_j[\Gamma, \Gamma]\big)_{j\neq r+1}$ since Γ/Γ_σ is abelian, which contradicts the minimality of $\{x_1, \ldots, x_d\}$. Hence $d_pG = d - r$. □

3.2.2 On the group Γ_σ

Let us conserve the notations and assumptions of the preceding subsection; in particular Γ is uniform, $\sigma \in \mathrm{Aut}(\Gamma)$ is of prime order ℓ and $\ell \mid (p-1)$. Recall that $\Gamma_\sigma^\circ = \langle x_1 \cdots x_r\rangle$ and put $G = \Gamma/\Gamma_\sigma$.

By Proposition 3.5, if Γ is FAb, the group Γ_σ is open in Γ, the quotient $G = \Gamma/\Gamma_\sigma$ is finite and $\mathbb{Z}_p[[G]] \simeq \mathbb{Z}_p[G]$.

Recall now as G is a pro-p group, the ring $\mathbb{Z}_p[[G]]$ (resp. $\mathbb{F}_p[[G]]$) is a local ring, with maximal ideal the augmentation ideal $\ker(\mathbb{Z}_p[[G]] \to \mathbb{F}_p)$ (resp. $\ker(\mathbb{F}_p[[G]] \to \mathbb{F}_p)$). The ring $\mathbb{Z}_p[[G]]$ (resp. $\mathbb{F}_p[[G]]$) acts by conjugation on $\Gamma_\sigma/[\Gamma_\sigma, \Gamma_\sigma]$ (resp. $\Gamma_\sigma^{p,el}$). The following proposition gives a system of minimal generators of this action.

Proposition 3.10.

(i) *The automorphism σ acts trivially on $\left(\Gamma_\sigma^{ab}\right)_G$.*

(ii) *The cosets $x_1\Phi(\Gamma_\sigma), \ldots, x_r\Phi(\Gamma_\sigma)$ form a minimal system of generators of the quotient $\Gamma_\sigma^{p,el}$ of Γ_σ seen as $\mathbb{F}_p[[G]]$-module. In particular $d_p\Gamma_\sigma \geq r$.*

Proof.

(i) As $\Gamma_\sigma^{p,el}$ is generated by the G-conjuguates of the classes of the x_i, $i = 1, \ldots, r$, one gets that σ acts trivially on $\left(\Gamma_\sigma^{p,el}\right)_G$, and then on $\left(\Gamma_\sigma^{ab}\right)_G$.

(ii) Consider now the exact sequence

$$\cdots H_2(\Gamma, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H_2(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \left(\Gamma_\sigma^{p,el}\right)_G \longrightarrow \Gamma^{p,\mathrm{el}} \twoheadrightarrow G^{p,\mathrm{el}},$$

coming from the short exact sequence $1 \longrightarrow \Gamma_\sigma \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$. The automorphism σ acts ont these exact sequences. As the group Γ_σ contains the elements $x_1, \ldots, x_r$, the action of σ on $G^{p,\mathrm{el}}$ has no non-trivial fixed points. By comparing the character of the action of σ on the initial exact sequence, one obtains that $d_p\left(\Gamma_\sigma^{p,el}\right)_G = r$. Thus by Nakayama's lemma, the classes $x_1\Phi(\Gamma_\sigma), \ldots, x_r\Phi(\Gamma_\sigma)$ form a minimal system of generators of the $\mathbb{F}_p[[G]]$-module $\Gamma_\sigma^{p,el}$. In conclusion we get $d_p\Gamma_\sigma \geq r$.

□

We now recall a notion introduced in Definition 2.1: the action of σ on the group Γ is called fixed-point-mixing modulo Frattini (FPMF) if $G = \Gamma/\Gamma_\sigma$ does not act trivially on $\Gamma_\sigma/\Phi(\Gamma_\sigma) = \Gamma_\sigma^{p,el}$.

Proposition 3.11. *If the action of σ on Γ is not fixed-point-mixing modulo Frattini (i.e. G acts trivially on $\Gamma_\sigma/\Phi(\Gamma_\sigma)$), then $\Gamma_\sigma = \Gamma_\sigma^\circ$ and $d_p\Gamma_\sigma = r$.*

Proof. It is a consequence of Proposition 3.10. □

Proposition 3.12. *Let Γ be a FAb uniform group of dimension $d > 1$. Suppose $\sigma \in \mathrm{Aut}(\Gamma)$ of order $\ell = 2$. If $t_\sigma(\Gamma) = (1, d-1)$, then the action of σ on Γ is fixed-point-mixing modulo Frattini.*

Proof. If $d_p\Gamma_\sigma = 1$, the group Γ_σ is generated by only one element and then is procyclic. Since Γ is FAb, the group Γ_σ is open by Proposition 3.5, the quotient Γ/Γ_σ is finite and then the p-adic analytic group Γ is of dimension 1 which is a contradiction. Thus, $d_p\Gamma_\sigma > 1$ and the action of σ on Γ is fixed-point-mixing modulo Frattini thanks to Proposition 3.11. □

Remark 3.13. We will see in Proposition 3.23 that when Γ is FAb and uniform of dimension d, $t_\sigma(\Gamma) \neq (d-1, 1)$.

3.3 Uniform groups and Lie algebras

3.3.1 The correspondence

Consider a uniform group Γ of dimension d. We have seen how to associate to Γ a uniform abelian group $\Gamma_+ \simeq \mathbb{Z}_p^d$. In fact, this group is naturally equipped with more algebraic structure, as we now explain.

For $x, y \in \Gamma$, put $(x, y)_n := \psi_{2n}^{-1}([x^{p^n}, y^{p^n}])$ and define

$$(x, y) = \lim_{n\to\infty} (x, y)_n.$$

The $\mathbb{Z}_p$-module Γ_+ equipped with the bracket $(\cdot, \cdot)$ is a $\mathbb{Z}_p$-Lie algebra of dimension d ([7],Theorem 4.30). Denote by $\mathcal{L}_\Gamma$ this new Lie algebra. Recall that each $\sigma \in \mathrm{Aut}(\Gamma)$ induces an automorphism of Γ_+. By noting that $\sigma((x, y)_n) = (\sigma(x), \sigma(y))_n$, we see that $\sigma(x, y) = (\sigma(x), \sigma(y))$, so σ becomes an automorphism of the $\mathbb{Z}_p$-Lie algebra $\mathcal{L}_\Gamma$.

We remark that as Γ is uniform, thus $[\Gamma, \Gamma] \subset \Gamma^{2p}$ and $(x, y)_n \in \Gamma^{2p}$; by passing to the limit, one obtains: $(\mathcal{L}_\Gamma, \mathcal{L}_\Gamma) \subset 2p\,\mathcal{L}_\Gamma$.

Definition 3.14. *A $\mathbb{Z}_p$-Lie algebra $\mathcal{L}$ is called powerful if $(\mathcal{L}, \mathcal{L}) \subset 2p\mathcal{L}$.*

Recall now the correspondence.

Theorem 3.15 ([7], Theorem 9.10). *There exists a bijective correspondence between the category of uniform groups of dimension d and the category of powerful $\mathbb{Z}_p$-Lie algebras of dimension d.*

Given a uniform group of dimension d, we have already seen how to associate to it a $\mathbb{Z}_p$-Lie algebra of dimension d. The inverse map is obtained by using the development of Campbell-Hausdorff Φ (see section 9.4 of [7]).

Theorem 3.16 ([7], Theorem 9.8 and Theorem 9.10). *Let $\mathcal{L}$ be a powerful $\mathbb{Z}_p$-Lie algebra of dimension d. Let $\{x_1, \ldots, x_d\}$ be a $\mathbb{Z}_p$-basis of $\mathcal{L}$. The law $x * y = \Phi(x, y)$ makes $\mathcal{L}$ into a uniform group $\Gamma_{\mathcal{L}}$ of dimension d, topologically generated by $\{x_1, \ldots, x_d\}$. Moreover $\mathcal{L}_{\Gamma_{\mathcal{L}}} \simeq \mathcal{L}$ and $\Gamma_{\mathcal{L}_\Gamma} \simeq \Gamma$.*

Remark 3.17. Let us examine carefully the case where $\mathcal{L}$ is a powerful sub-Lie-algebra of the Lie algebra $\mathcal{M}_n(\mathbb{Q}_p)$ of p-adic $n \times n$ matrices equipped with the bracket $(A, B) = AB - BA$. Consider the map "exponential" exp and "logarithm" log of matrices well-defined in our context (see §6.3 of [7]): $\mathcal{L} \underset{\log}{\overset{\exp}{\rightleftarrows}} \exp(\mathcal{L})$. Thus for $A, B \in \mathcal{L}$, we get $\exp(A)\exp(B) = \exp(\Phi(A, B))$, where Φ is the Campbell-Hausdorff series (see Proposition 6.27 of [7]) and then $\exp(\mathcal{L})$ is isomorphic to the uniform group $\Gamma_{\mathcal{L}}$ (see Corollary 6.25 of [7]).

Since we are especially interested in uniform groups which are FAb, we give a characterization of such groups, which is probably well-known to specialists.

Proposition 3.18. *A uniform group Γ is FAb if and only if*

$$\mathcal{L}_\Gamma(\mathbb{Q}_p) = (\mathcal{L}_\Gamma(\mathbb{Q}_p), \mathcal{L}_\Gamma(\mathbb{Q}_p)),$$

where $\mathcal{L}(\mathbb{Q}_p)$ is the $\mathbb{Q}_p$-Lie algebra obtained from $\mathcal{L}$ by extending the scalars to $\mathbb{Q}_p$.

Proof. For every open subgroup H of the uniform group Γ, $\mathcal{L}_H(\mathbb{Q}_p) = \mathcal{L}_\Gamma(\mathbb{Q}_p)$. Hence, one has to prove that Γ^{ab} is finite if and only if, $\mathcal{L}_\Gamma(\mathbb{Q}_p) = (\mathcal{L}_\Gamma(\mathbb{Q}_p), \mathcal{L}_\Gamma(\mathbb{Q}_p))$. Suppose Γ^{ab} infinite. There exists a closed and normal subgroup H of Γ such that $\Gamma/H \simeq \mathbb{Z}_p$. By Proposition 4.31 of [7], the subgroup H is uniform, the $\mathbb{Z}_p$-Lie algebra $\mathcal{L}_H$ is an ideal of $\mathcal{L}_\Gamma$, and $\mathcal{L}_{\Gamma/H} \simeq \mathcal{L}_\Gamma/\mathcal{L}_H$. As Γ/H is abelian, the Lie algebra $\mathcal{L}_{\Gamma/H}$ is commtutative (corollary 7.16 of [7]). In fact, $\mathcal{L}_{\Gamma/H} = \mathbb{Z}_p$. Then $\mathcal{L}_H$ contains $[\mathcal{L}_\Gamma, \mathcal{L}_\Gamma]$; thus $\mathcal{L}_\Gamma/(\mathcal{L}_\Gamma, \mathcal{L}_\Gamma) \twoheadrightarrow \mathcal{L}_\Gamma/\mathcal{L}_H \simeq \mathbb{Z}_p$ and therefore $(\mathcal{L}_\Gamma(\mathbb{Q}_p), \mathcal{L}_\Gamma(\mathbb{Q}_p)) \subsetneq \mathcal{L}_\Gamma(\mathbb{Q}_p)$.

In the other direction, suppose that $(\mathcal{L}_\Gamma(\mathbb{Q}_p), \mathcal{L}_\Gamma(\mathbb{Q}_p)) \subsetneq \mathcal{L}_\Gamma(\mathbb{Q}_p)$, or equivalently that the $\mathbb{Z}_p$-rank of $\mathcal{L}_\Gamma/(\mathcal{L}_\Gamma, \mathcal{L}_\Gamma)$ is not trivial. Put $\mathcal{L}_1 = \mathcal{L}_\Gamma/(\mathcal{L}_\Gamma, \mathcal{L}_\Gamma)$. As $\mathbb{Z}_p$-modules, let us write $\mathcal{L}_1 = \mathcal{L}_0 \oplus \mathrm{Tor}(\mathcal{L}_1)$. It is then easy to see that $\mathrm{Tor}(\mathcal{L}_1)$ is an ideal of the Lie algebra $\mathcal{L}_1$. Thus consider the quotient $\mathcal{L}_0 := \mathcal{L}_1/\mathrm{Tor}(\mathcal{L}_1)$: it is a non trivial, commutative and torsion-free $\mathbb{Z}_p$-Lie algebra. By the correspondence of Theorem 3.15, the algebra $\mathcal{L}_0$ corresponds to a uniform abelian group Γ_0 (by Corollary 7.16 of [7]). In fact, as $\mathcal{L}_0 \simeq \mathbb{Z}_p^t$, with $t > 0$, on has $\Gamma_0 \simeq \mathbb{Z}_p^t$. The algebra $\mathcal{L}_0$ is also the quotient of $\mathcal{L}_\Gamma$ by the ideal $\mathcal{L}_2$ generated by $(\mathcal{L}_\Gamma, \mathcal{L}_\Gamma)$ and the lifts of $\mathrm{Tor}(\mathcal{L}_1)$. By Proposition 7.15 of [7], under the correspondence of Theorem 3.15, the algebra $\mathcal{L}_2$ corresponds to a uniform closed subgroup H of Γ; moreover Γ/H is uniform. Therefore as for the previous implication, we get $\mathcal{L}_{\Gamma/H} \simeq \mathcal{L}_\Gamma/\mathcal{L}_2 \simeq \mathcal{L}_0 \simeq \mathbb{Z}_p^t$ and then $\Gamma/H \simeq \Gamma_0 \simeq \mathbb{Z}_p^t$. □

The proof has shown the following result:

Corollary 3.19. *A uniform group Γ is FAb if and only if Γ^{ab} is finite.*

In this subsection, we have seen the relevance of powerful $\mathbb{Z}_p$-Lie algebras and their automorphisms in our study. If moreover we restrict attention to FAb and uniform groups, one sees the importance of simple algebras. Indeed, it follows from definitions that every $\mathbb{Z}_p$-Lie algebra $\mathcal{L}$ which is simple or even semisimple (after extending scalars) produces a uniform FAb group by Proposition 3.18.

3.3.2 Lie algebras and fixed points

We now further explore the Lie algebra $\mathcal{L}$ over $\mathbb{Q}_p$. Denote by $(\cdot,\cdot)$ the Lie bracket of $\mathcal{L}$.

Definition 3.20. *Let $\mathcal{L}$ be a Lie algebra and let $\sigma \in \mathrm{Aut}(\mathcal{L})$. Put $\mathcal{L}_\sigma = \{x \in \mathcal{L}, \sigma(x) = x\}$.*

Let us introduce the notion of FAb algebra.

Definition 3.21. *A Lie algebra $\mathcal{L}$ over $\mathbb{Q}_p$ is called FAb if $(\mathcal{L},\mathcal{L}) = \mathcal{L}$. In particular a semisimple Lie algebra is FAb.*

As for pro-p groups having a FPF automorphism σ of order $\ell \neq p$, the same phenomenon occurs for Lie algebras. Indeed as a consequence of a result of Borel and Serre [1] (cf the remark of Jacobson [13], page 281), we have the following Proposition.

Proposition 3.22. *Let $\mathcal{L}$ be a* FAb *Lie algebra and let $\sigma \in \mathrm{Aut}(\mathcal{L})$ of order ℓ. Then $\mathcal{L}_\sigma \neq \{0\}$.*

Proof. Indeed, by Proposition 4 of [1], if $\mathcal{L}_\sigma = \{0\}$ then $\mathcal{L}$ is nilpotent and the conclusion is obvious. □

An automorphism of order ℓ of a FAb $\mathbb{Q}_p$-Lie algebra must have a non-trivial fixed point. One finds again Proposition 3.4 in the context of uniform groups. If $\sigma \in \mathrm{Aut}(\mathcal{L})$ is of order 2, as for pro-p groups, one define the σ-type of $\mathcal{L}$ as $t_\sigma(\mathcal{L}) = (a,b)$, where $a = \dim\ker(\sigma - \iota)$ and $b = \dim\ker(\sigma + \iota)$, ι being the trivial automorphism. We have $a = \dim \mathcal{L}_\sigma$ and $b = d - a$ where $d = \dim \mathcal{L}$.

Proposition 3.23. *Let $\mathcal{L}$ be a FAb $\mathbb{Q}_p$-Lie algebra of dimension d and let $\sigma \in \mathrm{Aut}(\mathcal{L})$ be of order 2. Let $t_\sigma(\mathcal{L}) = (a,b)$ be the σ-type of $\mathcal{L}$. Then $a \neq 0$ and $b > 1$.*

Proof. Observe that since $\mathcal{L}$ is FAb then $d \geq 3$. By Proposition 3.22, the type $(0,d)$ is excluded. Suppose $\mathcal{L}$ of type $(d-1,1)$. Take a $\mathbb{Q}_p$-basis $\{e_1, e_2, \ldots, e_{d-1}, \varepsilon\}$ of $\mathcal{L}$ respecting the action σ, *i.e.* for $i = 1,\ldots,d-1$, $\sigma(e_i) = e_i$ and $\sigma(\varepsilon) = -\varepsilon$. One then remarks that σ acts by $+1$ on (e_i,e_j) and by -1 on (e_i,ε): therefore $(e_i,e_j) \in \langle e_1,\ldots,e_{d-1}\rangle$ and $(e_i,\varepsilon) \in \langle\varepsilon\rangle$. Hence, for $i \neq j$, $(e_i,e_j) = \sum_{k=1}^{d-1} a_k(i,j)e_k$, with $a_k \in \mathbb{Q}_p$, and also for $i = 1,\ldots,d-1$, $(e_i,\varepsilon) = \lambda_i\varepsilon$. As the Lie algebra is FAb, the matrix $(a_k(i,j))_{((i,j),k)}$ of size $\frac{(d-1)(d-2)}{2} \times (d-1)$ must be of maximal rank, *i.e.* $d-1$. Also the vector $(\lambda_1,\ldots,\lambda_{d-1})$ is non zero.

Now the elements $(e_i)_i$ and ε must verify the Jacobi identity; in particular one should have for $i \neq j$:

$$(e_i,(e_j,\varepsilon)) + (e_j,(\varepsilon,e_i)) + (\varepsilon,(e_i,e_j)) = 0\cdot$$

Thus one gets

$$\begin{aligned}(e_i,(e_j,\varepsilon)) + (e_j,(\varepsilon,e_i)) + (\varepsilon,(e_i,e_j)) &= \lambda_j(e_i,\varepsilon) - \lambda_i(e_j,\varepsilon) + \sum_{k=1}^{d-1} a_k(i,j)(\varepsilon,e_k)\\ &= \lambda_j\lambda_i\varepsilon - \lambda_i\lambda_j\varepsilon - \sum_{k=1}^{d-1} a_k(i,j)\lambda_k\varepsilon\end{aligned}$$

and then

$$\sum_{k=1}^{d-1} a_k(i,j)\lambda_k = 0\cdot$$

If the matrix $(a_k(i,j))_{((i,j),k)}$ is of maximal rank, then $\lambda_k = 0$ for all k and $\mathcal{L}$ is not FAb. □

Applying the correspondence of uniform groups/Lie algebras, this proposition allows us to obtain the following corollary:

Corollary 3.24. *Let Γ be a FAb uniform group of dimension d and let $\sigma \in \mathrm{Aut}(\Gamma)$ be of order 2. Then $t_\sigma(\Gamma) = (d-k, k)$ with $k \geq 2$. Therefore for a FAb uniform group of dimension 3 the type of every automorphism σ of order 2 satisfies $t_\sigma(\Gamma) = (1, 2)$.*

On other hand, look at Lie algebras $\mathcal{L}$ having few fixed points. Consider, say, a Lie algebra $\mathcal{L}$ of dimension 4 such that $\mathcal{L}_\sigma$ is of dimension 1. Let $\{e_1, e_2, e_3, \varepsilon\}$ be a $\mathbb{Q}_p$-basis of $\mathcal{L}$ respecting the action if σ, *i.e.* here $\sigma(e_i) = -e_i$ and $\sigma(\varepsilon) = \varepsilon$. Then $(e_i, e_j) \in \langle\varepsilon\rangle$ and $(e_i, \varepsilon) \in \langle e_1, \ldots, e_3\rangle$. A linear algebra computation similar to those of Proposition 3.23 shows that $\mathcal{L}$ can not be FAb: necessarily, $\mathcal{L}/(\mathcal{L}, \mathcal{L}) \twoheadrightarrow \mathbb{Q}_p$. The same holds for the dimension 5. In fact, it is a general and well-known phenomenon for semisimple Lie algebras $\mathcal{L}$. Indeed dimension of $\mathcal{L}_\sigma$ grows with the dimension of $\mathcal{L}$ (see Theorem 10 and Theorem 8 of [13]).

3.4 Examples

3.4.1 The group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$

We assume that $p > 2$. Let us start with the $\mathbb{Z}_p$-Lie algebra $\mathfrak{sl}_2$ of dimension 3 generated by the matrices

$$x = \begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix},\ y = \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix},\ z = \begin{pmatrix} p & 0 \\ 0 & -p \end{pmatrix}.$$

The algebra $\mathfrak{sl}_2$ is the subalgebra of the trace zero matrices for which the reduction modulo p is trivial. One has the relations $[x, y] = pz$, $[x, z] = -2px$ and $[y, z] = 2py$. As $[\mathfrak{sl}_2, \mathfrak{sl}_2] \subset p \cdot \mathfrak{sl}_2$, the algebra $\mathfrak{sl}_2$ is FAb and powerful. Put

$$X = \exp(x) = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix},\ Y = \exp(y) = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix},\ Z = \exp(z) = \begin{pmatrix} e^p & 0 \\ 0 & e^{-p} \end{pmatrix}.$$

Let $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ be the subgroup of $\mathrm{Sl}_2(\mathbb{Z}_p)$ generated by the X, Y, Z; it is the kernel of the reduction morphism $\mathrm{Sl}_2(\mathbb{Z}_p) \to \mathrm{Sl}_2(\mathbb{Z}/p\mathbb{Z})$. The group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ is FAb, uniform and of dimension 3.

Proposition 3.25. *For every involution σ of the uniform pro-p group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$, the action of σ is fixed-point-mixing modulo Frattini.*

Proof. The uniform pro-p group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ is FAb and of dimension 3: by Corollary 3.24, every automorphism σ of order 2 is of type $(1, 2)$. One concludes with Proposition 3.12. □

3.4.2 The group $\mathrm{Sl}_n^1(\mathbb{Z}_p)$

Let $\mathfrak{sl}_n(\mathbb{Q}_p)$ be the $\mathbb{Q}_p$-Lie algebra constituted by the square matrices $n \times n$ with coefficients in $\mathbb{Q}_p$ and of zero trace. It is a simple algebra of dimension $n^2 - 1$. Recall a natural basis of it:

(a) for $i \neq j$, $E_{i,j} = (e_{k,l})_{k,l}$ for which all the coefficient are zero excepted $e_{i,j}$ that takes value p;
(b) for $i > 1$, $D_i = (d_{k,l})_{k,l}$ which is the diagonal matrix $D_i = (p, 0, \ldots, 0, -p, 0, \ldots, 0)$, where $d_{i,i} = -p$.

Let $\mathfrak{sl}_n$ be the $\mathbb{Z}_p$-Lie algebra generated by the $E_{i,j}$ and the D_i. The algebra $\mathfrak{sl}_n$ is FAb and powerful.

Put $X_{i,j} = \exp E_{i,j}$ and $Y_i = \exp D_i$. Denote by $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ the subgroup of $\mathrm{Sl}_n(\mathbb{Z}_p)$ generated by the matrices $X_{i,j}$ and Y_i. The group $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ is FAb, uniform and of dimension $n^2 - 1$. It is also the kernel of the reduction map of $\mathrm{Sl}_n(\mathbb{Z}_p)$ modulo p. Put $\Gamma = \mathrm{Sl}_n^1(\mathbb{Z}_p)$.

We now examine the inner automorphisms σ_A. More precisely let us assume that A is of order 2. Denote by $k = \dim\ker(A - I)$, *i.e.* the number of $+1$s on the diagonal. We can simplify to the case where $A = (a_{i,j})$ is diagonal with $a_{i,i} = 1$ for $i \leq k$, and $a_{i,i} = -1$ for $i > k$.

Lemma 3.26. *With the above assumptions, the vector subspace $\left(\mathfrak{sl}_n\right)_{\sigma_A}$ of the fixed points of the algebra $\mathfrak{sl}_n$ under conjugation by A is generated by the diagonal matrices and by the matrices $E_{i,j}$ for $\{i, j\} \subset \{1, \ldots, k\}$ or for $\{i, j\} \subset \{k+1, \ldots, n\}$. The matrices $E_{i,j}$ and $E_{j,i}$, with $i \leq k$ and $j > k$, form a basis of the subspace of the eigenvalue -1.*

Proof. It is a simple computation. □

Denote by H the subgroup of Γ generated by the matrices $X_{i,j}$ for $\{i,j\} \subset \{1,\dots,k\}$ and for $\{i,j\} \subset \{k+1,\dots,n\}$.

Lemma 3.27. *Under the above conditions, one has*

(i) $\Gamma_\sigma^\circ = \langle X_{i,j}, \{i,j\} \subset \{1,\dots,k\}, \{i,j\} \subset \{k+1,\dots,n\}, Y_l, i \neq j, l > 1\rangle$.
(ii) $H \lhd \Gamma_\sigma^\circ$;
(iii) $H \subset \left(\begin{array}{c|c} A_{k,k} & 0 \\ \hline 0 & B_{n-k,n-k} \end{array}\right)$

Proof.

(i) is a consequence of Proposition 3.7.
(ii) is an easy computation, and (iii) is obvious.

□

We finally obtain:

Proposition 3.28. *Let $n \geq 2$ and let $\sigma = \sigma_A$ with $\mathrm{A} \in \mathrm{Gl}_n(\mathbb{Z}_p)$ of order 2. Then*

(i) *The action of σ on $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ is fixed-point-mixing modulo Frattini;*
(ii) $\mathrm{Sl}_n^1(\mathbb{Z}_p)/\mathrm{Sl}_n^1(\mathbb{Z}_p)_\sigma \simeq (\mathbb{Z}/p\mathbb{Z})^{2k(n-k)}$.

Proof. We can simplify to the case where $A = (a_{i,j})$ is diagonal with $a_{i,i} = 1$ for $i \leq 1$, and $a_{i,i} = -1$ for $i > k$.

(i) By Lemma 3.27, the subgroup H is of dimension (as variety over $\mathbb{Q}_p$) at most $k^2 + (n-k)^2$ which is strictly smaller than $n^2 - 1$. On the other hand, the quotient Γ_σ° / H is generated by the diagonal matrices, and is hence abelian; it will be finite if the subgroup Γ_σ° is open in Γ, because Γ is FAb. Therefore Γ, which is of dimension $n^2 - 1$, is of the same dimension as Γ_σ, which can not be of the same dimension as H. Then $\Gamma_\sigma^\circ \subsetneq \Gamma_\sigma$, which proves that the action of σ on Γ is fixed-point-mixing modulo Frattini by Proposition 3.11.
(ii) For $i \neq j$, set $Y_{i,j} = Y_i^{-1} Y_j = \exp(D_i - D_j)$. Here $D_i - D_j = (d_{k,l})$ is the diagonal matrix with $d_{i,i} = -p$, $d_{j,j} = +p$, and 0 otherwise. Observe now

$$Y_{i,j} X_{i,j} Y_{i,j}^{-1} X_{i,j}^{-1} = X_{i,j}^{\exp(2p)-1},$$

which shows that $G := \Gamma/\Gamma_\sigma$ is of exponent p. Then thanks to Lemma 3.9, one has $G \simeq (\mathbb{Z}/p\mathbb{Z})^{2k(n-k)}$; here $r = n^2 - 1 - 2k(n-k)$.

□

4. Ramification with prescribed Galois action

First, let us recall some notations.

- p is a prime number.
- If K is a fixed number field, and if S and T are two finite and disjoints sets of primes ideals of $\mathcal{O}_K$, denote by K_S^T the maximal pro-p extension of K unramified outside S and totally split at T; $\mathrm{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.
- *We assume throughout that S contains no primes above p* and that for finite places $\mathfrak{p} \in S$, we have $\#\mathcal{O}_\mathrm{K}/\mathfrak{p} \equiv 1 (\mathrm{mod}\ p)$. Hence, by class field theory, the pro-p group G_S^T is FAb.
- Put $\mathrm{Cl}_S^T(\mathrm{K}) := (\mathrm{G}_S^T)^{ab}$. It is the p-Sylow of the S-ray T-class class group of K. In particular, $\mathrm{Cl}(\mathrm{K}) := \mathrm{Cl}_\emptyset^\emptyset(\mathrm{K})$ is the p-Sylow of the class group of K.
- Let $\mathcal{O}_\mathrm{K}^T$ be the group of T-units of K.
- If L/K is an extension of K, we still denote by abuse, $S = S(\mathrm{L})$ be the set of primes of $\mathcal{O}_\mathrm{L}$ above the primes $\mathfrak{p} \in S$.

4.1 Preparation

Let us set the context.

- Let us start with a number field k with two finite and disjoints sets S and T of primes of k.
- Let L/k be a finite Galois extension with Galois group $\mathcal{G}$. We assume that $\mathcal{G}$ has only one p-Sylow subgroup G; put $\Delta := \mathcal{G}/G$. Hence Δ is a finite group of prime order $\ell \neq p$. Put $\mathrm{K} = \mathrm{L}^G$.
- Let T be a finite set of primes of $\mathcal{O}_\mathrm{k}$ *all of which split completely in* L, and consider

$$\mathrm{V}^T = \{\alpha \in \mathrm{L}^\times,\ v_{\mathfrak{P}}(\alpha) \equiv 0 \ (\mathrm{mod}\, p), \forall \mathcal{O}_\mathrm{L}\text{-primes } \mathfrak{P} | \mathfrak{p} \notin T\}.$$

- Consider now the governing field $\mathrm{F}^T := \mathrm{L}'(\sqrt[p]{\mathrm{V}^T})$, where $\mathrm{L}' = \mathrm{L}(\zeta_p)$. The Kummer extension F^T/L' is unramified outside $T \cup S_p(\mathrm{L}')$.
- We also define analogous objects over k, namely:

$$\mathrm{V}_\mathrm{k}^T = \{\alpha \in \mathrm{k}^\times,\ v_{\mathfrak{p}}(\alpha) \equiv 0 \ (\mathrm{mod}\, p), \forall \mathfrak{p} \notin T\},$$

  and the governing field $\mathrm{F}_\mathrm{k}^T := \mathrm{k}(\zeta_p, \sqrt[p]{\mathrm{V}_\mathrm{k}^T})$.
- Henceforth, we assume that the extension L/K is unramified everywhere, in particular the archimedean places of K split completely in L.

4.1.1 On free sub-$\mathcal{G}$-modules of $\mathrm{V}^T/(\mathrm{L}^\times)^p$

We will be interested in finding some free sub-$\mathbb{F}_p[\mathcal{G}]$-modules of $\mathrm{V}^T/(\mathrm{L}^\times)^p$: they will appear thanks to control over the group of T-units, indeed one easily sees that $\mathbb{F}_p \otimes \mathcal{O}_\mathrm{L}^T \hookrightarrow \mathrm{V}^T/(\mathrm{L}^\times)^p$.

The following result, crucial for us, is a consequence of an adapted version of Lemma 2 of [20].

Theorem 4.1. *We assume that the archimedean places of* K *split completely in* L. *There exists a constant* $\mathrm{A} = \mathrm{A}(\mathrm{L}/\mathrm{K}) \in \mathbb{Z}$ *such that if* m *is any given positive integer, there exists a choice of a set* T *of size* $|T| \leq m + A$ *consisting of finite places of* k *that split completely in* L/k, *such that the* $\mathbb{F}_p[\mathcal{G}]$*-module* $\mathbb{F}_p \otimes \mathcal{O}_\mathrm{L}^T$ *contains a submodule isomorphic to* $\mathbb{F}_p[\mathcal{G}]^m$.

We now give an explicit formula for A(L/K) where the proof can be found in [12, §6.1].

Let us introduce a bit more notation. Let us write d_∞ for the number of archimedean places of k that split completely in K/k and r_∞ the number of ramified archimedean places (*i.e.* those that are real in k and not real in K).

- When μ_p is not contained in $\mathcal{O}_\mathrm{L}^T$, take

$$\mathrm{A} = -\left[d_\infty + \frac{1}{2}r_\infty - (|\mathcal{G}| - 1)\left(r_1 + r_2 - d_\infty - \frac{1}{2}r_\infty + d_p\mathrm{Cl}(\mathrm{K})\right) - 1\right].$$

- When $\mu_p \subset \mathcal{O}_\mathrm{L}^T$, take

$$\mathrm{A} = -\left[d_\infty + \frac{1}{2}r_\infty - (|\mathcal{G}| - 1)\left(r_1 + r_2 + 1 - d_\infty - \frac{1}{2}r_\infty + d_p\mathrm{Cl}(\mathrm{K}) + d_p H^2(G, \mathbb{Z}/p\mathbb{Z})\right)\right].$$

4.1.2 Kummer Theory and applications

Denote by $\chi_p = \mathbb{F}_p(1)$ the cyclotomic character resulting from the action on the pth roots of unity. For a $\mathbb{F}_p[\mathcal{G}]$-module M, put $M(1) = M \otimes_{\mathbb{F}_p} \mathbb{F}_p(1)$, and M^* the Pontryagin dual of M.

Put $\mathcal{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$; the group $\mathcal{G}$ acts on $\mathrm{V}^T/(\mathrm{L}^\times)^p$ and then on $\mathcal{H}$. After noting that $(L')^p \cap L = L^p$, recall that the bilinear form

$$\begin{array}{rccc} b : & \mathrm{V}^T/(\mathrm{L}^\times)^p \times \mathcal{H} & \longrightarrow & \mu_p \\ & (x, h) & \mapsto & \sqrt[p]{x}^{h-1} \end{array}$$

is non-degenerate and functorial with respect to the action of $\mathcal{G}$:

$$b(g(x),h) = b(x, g^{-1}(h)^{\chi_p(g)}), g \in \mathcal{G}, x \in \mathrm{V}^T, h \in \mathcal{H}.$$

This bilinear form induces an isomorphism of $\mathcal{G}$-modules :

$$\Theta : \left(\mathrm{V}^T/(\mathrm{L}^\times)^p\right)^*(1) \xrightarrow{\approx} \mathcal{H} \cdot \tag{3}$$

Proposition 4.2. *If the $\mathbb{F}_p[\mathcal{G}]$-module $\mathrm{V}^T/(\mathrm{L}^\times)^p$ contains a free submodule $\langle\varepsilon\rangle_{\mathcal{G}}$ generated by some element ε, then $\mathcal{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains, as a direct factor, a free sub-$\mathbb{F}_p[\mathcal{G}]$-module $\mathcal{H}_\varepsilon$ of rank 1, i.e. $\left(\langle\varepsilon\rangle_{\mathcal{G}}\right)^*(1)$, the latter being isomorphic to $\mathrm{Gal}(\mathrm{L}'(\sqrt[p]{\langle\varepsilon\rangle_{\mathcal{G}}})/\mathrm{L}')$.*

Proof. As $\mathbb{F}_p[\mathcal{G}]$ is a Frobenius ring, the free submodule $\langle\varepsilon\rangle_{\mathcal{G}}$ is a direct factor in $\mathrm{V}^T/(\mathrm{L}^\times)^p$. By passing to the dual, the module $\left(\langle\varepsilon\rangle_{\mathcal{G}}\right)^*(1)$ is free and is in direct factor in $\left(\mathrm{V}^T/(\mathrm{L}^\times)^p\right)^*(1) \underset{\sim}{\overset{\Theta}{\to}} \mathcal{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$. Finally by Kummer theory, $\left(\langle\varepsilon\rangle_{\mathcal{G}}\right)^*(1) \simeq \mathrm{Gal}(\mathrm{L}'(\sqrt[p]{\langle\varepsilon\rangle_{\mathcal{G}}})/\mathrm{L}')$. □

Definition 4.3. *Under the hypothesis of Proposition 4.2, denote by x_ε a generator of the free $\mathbb{F}_p[\mathcal{G}]$-module $\mathcal{H}_\varepsilon$.*

4.1.3 The Theorem of Gras-Munnier

Definition 4.4. *Let* K *be a number field and S a finite set of prime ideals of $\mathcal{O}_\mathrm{K}$. We say the extension* F/K *is S-ramified if it is unramified outside S and S-totally ramified if it is S-ramified and moreover all primes in S are totally ramified in* F/K.

Let us conserve the notation introduced in the beginning of this section 4.1: $\mathrm{L}' = \mathrm{L}(\zeta_p)$ and $\mathrm{F}^T = \mathrm{L}'(\sqrt[p]{\mathrm{V}^T})$. Let us recall the Theorem of Gras-Munnier (see [10], [9]) that will be extremely useful to us.

Theorem 4.5 (Gras-Munnier [10]). *Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ and T be two finite sets of prime ideals of $\mathcal{O}_\mathrm{L}$, such that $S \cap T = \emptyset$, and such that for all $\mathfrak{p}_i \in S$, $\mathrm{N}\mathfrak{p}_i \equiv 1 (\mathrm{mod}\, p)$. For each $i = 1, \ldots, m$, let $\mathfrak{P}_i$ be a prime of $\mathcal{O}_{\mathrm{L}'}$ above $\mathfrak{p}_i$. Then, there exists a T-split, S-totally ramified cyclic extension* F/L *of degree p if and only if, for $i = 1, \ldots, m$, there exists $a_i \in \mathbb{F}_p^\times$, such that*

$$\prod_{i=1}^{m} \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}_i}\right)^{a_i} = 1 \ \in \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}'),$$

where $\left(\frac{\mathrm{F}^T/\mathrm{L}'}{\bullet}\right)$ is the Artin symbol in the extension F^T/L'.

Note that the condition does not depend on the choice of the primes $\mathfrak{P}_i$ above $\mathfrak{p}_i$ (which merely causes a shift in the exponents a_i).

4.1.4 Chebotarev density Theorem and applications

The Chebotarev density Theorem allows us to give a relationship between the Theorem of Gras-Munnier and the section about Kummer Theory. We continue to conserve the notations and the context of section 4.1.

Definition 4.6. *Let U, S and T be three pairwise finite disjoint sets of prime ideals of $\mathcal{O}_\mathrm{L}$. Put $\Sigma = S \cup U$ and assume that Σ is tame, i.e. $(\Sigma, p) = 1$. Denote by $\mathrm{I}_S^T(U, \mathrm{L})$ the subgroup of $\mathrm{G}_\Sigma^T(\mathrm{L})/\Phi(\mathrm{G}_\Sigma^T(\mathrm{L}))$ generated by the inertia groups of the prime ideals of U.*

Lemma 4.7. *With notation as above, the following conditions are equivalent.*

- $\mathrm{I}_S^T(U, \mathrm{L}) = \{1\}$
- *Every T-split Σ-ramified cyclic degree p extension of* L *is S-ramified*

– *For every non-empty subset U' of U, there does not exist a cyclic degree p T-split $U' \cup S$-ramified extension of* L *where all primes of U' are totally ramified.*

Proof. Obvious. □

Denote by $\mathrm{F}(S)$ the subgroup of $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ generated by the Frobenius of the ideals of S (with an abuse of notation); here the primes in S are unramified in F^T/L'.

Corollary 4.8. *Suppose that the $\mathbb{F}_p[\mathcal{G}]$-module $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains a free submodule $\mathcal{H}_\varepsilon = \langle x_\varepsilon \rangle_\mathcal{G}$ of rank 1 such that*

$$\mathcal{H}_\varepsilon \bigcap \mathrm{F}(S) = \{0\}.$$

By Chebotarev density Theorem, choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathrm{L}$ such that $\left\langle \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}} \right) \right\rangle = \langle x_\varepsilon \rangle$, for any $\mathfrak{P}|\mathfrak{p}$. Put $U = \{g(\mathfrak{P}) = \mathfrak{P}^g,\ g \in \mathcal{G}\}$. Then $\mathrm{I}_S^T(U, \mathrm{L}) = \{1\}$.

Proof. Let L_0/L be a T-split, $S \cup U$-ramified, degree p cyclic extension of L. As the free $\mathbb{F}_p[\mathcal{G}]$-module $\left\langle \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}} \right) \right\rangle_\mathcal{G}$ intersects trivially $\mathrm{F}(S)$, one has thanks to Theorem 4.5 that the extension L_0/L is unramified at U (by hypothesis there does not exist a non-trivial relation between the elements of U). By Lemma 4.7, one concludes that $\mathrm{I}_S^T(U, \mathrm{L}) = \{1\}$. □

4.2 The set $\mathcal{S}$

We are now going to give a non free situation that will be used in the proof of Theorem 5.4. It is essential for the definition of the sets $\mathcal{S}$.

4.2.1 On some special sub-modules

Let us start from the existence of a free submodule $\mathbb{F}_p[\mathcal{G}]^{|\mathcal{G}|}$ of $\mathrm{V}^T/(\mathrm{L}^\times)^p$, of rank $|\mathcal{G}|$.

Let $(\varepsilon_g)_g$ be a basis of $\mathbb{F}_p[\mathcal{G}]^{|\mathcal{G}|}$ indexed by the elements of $\mathcal{G}$. As $\mathbb{F}_p[\mathcal{G}]$ is a Frobenius ring, the free module $\bigoplus_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon_g$ is a direct factor in $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$; put then

$$\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p = \bigoplus_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon_g \oplus M,$$

as the sum of $\mathcal{G}$-modules.

Let $N = \sum_{h\in\mathcal{G}} h$ be the algebraic norm. Let us mention an easy lemma:

Lemma 4.9. *The module $\mathbb{F}_p N$ is a sub-$\mathbb{F}_p[\mathcal{G}]$-module of $\mathbb{F}_p[\mathcal{G}]$ generated by N. In other words, $\langle N \rangle_\mathcal{G} = \langle N \rangle$. It is also the only sub-$\mathcal{G}$-module of $\mathbb{F}_p[\mathcal{G}]$ on which $\mathcal{G}$ acts trivially.*

Proof. Put $\sum_{g\in\mathcal{G}} a_g g \in \mathbb{F}_p[\mathcal{G}]$, $a_g \in \mathbb{F}_p$. Then

$$\sum_{g\in\mathcal{G}} a_g g \left(\sum_{h\in\mathcal{G}} h \right) = \sum_{g\in\mathcal{G}} a_g \sum_{h\in\mathcal{G}} gh = \sum_{g\in\mathcal{G}} a_g N \in \mathbb{F}_p N,$$

which proves the first part. Now clearly $\mathcal{G}$ acts trivially on N and moreover if we start with an element $\sum_{g\in\mathcal{G}} a_g g$ on which $\mathcal{G}$ acts trivially, then obviously, a_g is constant. □

Take $z_0 \in \mathrm{V}_{\mathrm{k}}^T(\mathrm{L}^\times)^p/(\mathrm{L}^\times)^p$ and write $z_0 = \big(\sum_{g\in\mathcal{G}} y_g\big) + z$, with $y_g \in \mathbb{F}_p[\mathcal{G}]\varepsilon_g$ and $z \in M$. As $\mathcal{G}$ acts trivially on z_0, then $\mathcal{G}$ acts trivially on the elements y_g and Lemma 4.9 shows that $y_g \in \mathbb{F}_p N \cdot \varepsilon_g$. Denote by abuse, $\langle N\rangle := \mathbb{F}_p N \cdot \varepsilon_g$.

The morphism of $\mathbb{F}_p[\mathcal{G}]$-modules

$$\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p \twoheadrightarrow \bigoplus_{g\in\mathcal{G}} \big(\mathbb{F}_p[\mathcal{G}]\varepsilon_g/\langle N\rangle\big)$$

factors through $\mathrm{V}_{\mathrm{k}}^T(\mathrm{L}^\times)^p/(\mathrm{L}^\times)^p$. Passing to the dual, on obtains:

$$\left(\bigoplus_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon_g/\langle N\rangle\right)^*(1) \hookrightarrow \big(\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p\mathrm{V}_{\mathrm{k}}^T\big)^*(1)$$

where

$$\big(\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p\mathrm{V}_{\mathrm{k}}^T\big)^*(1) = \ker\Big[\big(\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p\big)^*(1) \twoheadrightarrow \big(\mathrm{V}_{\mathrm{k}}^T(\mathrm{L}^\times)^p/(\mathrm{L}^\times)^p\big)^*(1)\Big].$$

By passing to Kummer theory and by using the isomorphism Θ of (3), we get:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \big(\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p\mathrm{V}_k^T\big)^*(1) & \longrightarrow & \big(\mathrm{V}_{\mathrm{L}}^T/(\mathrm{L}^\times)^p\big)^*(1) & \longrightarrow & \big(\mathrm{V}_{\mathrm{k}}^T(\mathrm{L}^\times)^p/(\mathrm{L}^\times)^p\big)^*(1) & \longrightarrow & 0 \\
 & & \downarrow\wr & & \Theta\downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \mathrm{Gal}(\mathrm{F}^T/\mathrm{F}_{\mathrm{k}}^T\mathrm{L}') & \longrightarrow & \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}') & \longrightarrow & \mathrm{Gal}(\mathrm{F}_{\mathrm{k}}^T\mathrm{L}'/\mathrm{L}') & \longrightarrow & 0
\end{array}$$

Put

$$\mathcal{H}' := \Theta\left(\left(\bigoplus_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon_g/\langle N\rangle\right)^*(1)\right); \tag{4}$$

then $\mathcal{H}' \subset \mathrm{Gal}(\mathrm{F}^T/\mathrm{F}_{\mathrm{k}}^T\mathrm{L}')$.

Let us study more carefully $\mathcal{H}'$. We will continue to denote by $(\varepsilon_g)_g$ the dual basis of ε_g.

Let us fix an element ε_g. Then $\big(\mathbb{F}_p[\mathcal{G}]/\langle N\rangle\big)^* \simeq \{f \in \mathrm{Hom}(\mathbb{F}_p[\mathcal{G}], \mathbb{F}_p),\ f(N) = 0\}$, see for example [6], §60, chapter IX. Let

$$\mathrm{I} = \ker\big(\mathbb{F}_p[\mathcal{G}] \to \mathbb{F}_p\big)$$

be the augmentation ideal of the algebra $\mathbb{F}_p[\mathcal{G}]$. Obviously, *via* the isomorphism between $\mathbb{F}_p[\mathcal{G}]^*$ and $\mathbb{F}_p[\mathcal{G}]$, one has $\mathrm{I} \subset \{f \in \mathrm{Hom}(\mathbb{F}_p[\mathcal{G}], \mathbb{F}_p),\ f(N) = 0\}$; these two $\mathbb{F}_p$-spaces vector have the same dimension, *i.e.* $|\mathcal{G}| - 1$, and then finally $\mathrm{I} = \{f \in \mathrm{Hom}(\mathbb{F}_p[\mathcal{G}], \mathbb{F}_p),\ f(N) = 0\}$. The exact sequences

$$1 \longrightarrow \langle N\rangle \longrightarrow \mathbb{F}_p[\mathcal{G}] \longrightarrow \mathbb{F}_p[\mathcal{G}]/\langle N\rangle \longrightarrow 1$$

and

$$1 \longrightarrow \mathrm{I} \longrightarrow \mathbb{F}_p[\mathcal{G}] \longrightarrow \mathbb{F}_p \longrightarrow 1$$

are dual to each other, and the same holds after tensoring by μ_p.

Put $x_g = \varepsilon_g \otimes \zeta_p$: it is a generator of the free module $\big(\mathbb{F}_p[\mathcal{G}]\varepsilon_g\big)(1)$. In the sum $\bigoplus_{g\in\mathcal{G}} \mathrm{I}\cdot x_g \hookrightarrow \bigoplus_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]x_g$, let us choose the particular element x defined by

$$x := \left(\sum_{g\in\mathcal{G}} (g-1)x_g\right). \tag{5}$$

Obviously the algebraic norm kills each component $g - 1$ of x_g and then $N(x) = 0$. Let $\mathrm{Ann}(x)$ be the annihilator of x.

Lemma 4.10. *The relation $N(x) = 0$ is the unique non trivial relation of x,* i.e *if $\sum_{h\in\mathcal{G}} a_h h \cdot x = 0$ then $a_h = a_e$ for all $h \in \mathcal{G}$. Equivalently,* $\mathrm{Ann}(x) = \mathbb{F}_p N$.

Proof. Write $\lambda = \sum_{h\in\mathcal{G}} a_h h \in \mathbb{F}_p[\mathcal{G}]$ such that $\lambda \cdot x = 0$. Then

$$0 = \lambda x = \sum_{g\in\mathcal{G}} \lambda(g-1)x_g.$$

As the modules $\langle x_g\rangle$ are in direct sum, one has for every $g \in \mathcal{G}$, $\lambda(g-1)x_g = 0$. The modules $\langle x_g\rangle$ being moreover free, one gets $\lambda(g-1) = 0$. Thus $\lambda \in \bigcap_{g\in\mathcal{G}} \mathrm{Ann}(g-1) \in \mathbb{F}_p[\mathcal{G}]$. To conclude, it suffices to remark that the intersection is reduced to $\mathbb{F}_p N$. Indeed, when g is fixed, we get $\sum_{h\in\mathcal{G}} a_h h(g-1) = 0$ if and only if, $a_{hg^{-1}} = a_g$ for all h. When varying g, one obtains $a_{hg} = a_h$ for all h and g, implying $a_g = a_e$ for all $g \in \mathcal{G}$. □

4.2.2 Some consequences

Let us start now with x given by Definition (5).

Recall that $x \in \bigoplus_{g\in\mathcal{G}} \mathrm{I}x_g$, where $\mathrm{I} = \{f \in \mathrm{Hom}(\mathbb{F}_p[\mathcal{G}], \mathbb{F}_p),\ f(N) = 0\}$.

Put $x_0 = \Theta(x) \in \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$, where Θ is the isomorphism coming from Kummer theory, see (3). The element x_0 is in $\mathcal{H}'$ and then $x_0 \in \mathrm{Gal}(\mathrm{F}^T/\mathrm{F}_k^T\mathrm{L}')$.

By Chebotarev density Theorem, let us choose a prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathrm{L}$ which splits totally in L'/k and such that $\left\langle \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right)\right\rangle = \langle x_0\rangle$.

Let $\mathfrak{p}_\mathrm{k} = \mathrm{N}_{\mathrm{L}/\mathrm{k}}(\mathfrak{P})$ be the unique prime ideal of $\mathcal{O}_\mathrm{k}$ under $\mathfrak{p}$. Put $U = \{\mathfrak{p}_\mathrm{k}\}$ and still denote by abuse $U = U(\mathrm{F}) = \{\mathfrak{P} \subset \mathcal{O}_\mathrm{F},\ \mathfrak{P}|\mathfrak{p}_\mathrm{k}\}$ when F/k is a finite extension.

Remark 4.11. When $s = 1$, in the main theorem (Theorem C) the set $\mathcal{S}$ considered is composed of such prime ideals. The set $\mathcal{S}$ is of positive density. This density depends on the size of $\mathrm{Gal}(\mathrm{F}^T/\mathbb{Q})$; the size of $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ depends on the p-class group of K, on the signature of K and on the size of $|T|$.

Proposition 4.12. *With the previous notations and conditions (especially the choice of $\mathfrak{P}$), we get the isomorphism of $\mathcal{G}$-modules:* $\mathrm{I}^T(U,\mathrm{L}) \simeq \mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof. Suppose that there exists a non-trivial relation between the conjugates $\left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right)^g$, $g \in \mathcal{G}$, of $\left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right)$: $\left(\sum_{g\in\mathcal{G}} a_g g\right) \cdot \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right) = 0$, with $a_{g_0} \neq 0$ for at least one $g_0 \in \mathcal{G}$. Then, as $\left\langle \left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right)\right\rangle = \langle x_0\rangle$, by Lemma 4.10, one gets $a_g = a_{g_0} \neq 0$ for all $g \in \mathcal{G}$. Thus by Theorem 4.5, every T-split degree p cyclic extension of L which is ramified at one prime $\mathfrak{P}_0|\mathfrak{p}$ is totally ramified at all $\mathfrak{P}_0^g$, $g \in \mathcal{G}$. That means that $d_p\mathrm{I}^T(U) \leq 1$ (it is an easy generalization of Lemma 4.7).

We now show that the number field k has a T-split, $\{\mathfrak{p}_\mathrm{k}\}$-totally ramified, degree p cyclic extension. Indeed, by the choice of $\mathfrak{P}$, one knows that $\left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right) \in \langle x_0\rangle \subset \mathcal{H}'$ and consequently, $\left(\frac{\mathrm{L}'\mathrm{F}_\mathrm{k}^T/\mathrm{L}'}{\mathfrak{P}}\right) = 1$. By the properties of the Artin symbol, one gets

$$\left(\frac{\mathrm{L}'\mathrm{F}_\mathrm{k}^T/\mathrm{k}'}{\mathrm{N}_{\mathrm{L}'/\mathrm{k}'}(\mathfrak{P})}\right) = \left(\frac{\mathrm{L}'\mathrm{F}_\mathrm{k}^T/\mathrm{L}'}{\mathfrak{P}}\right) = 1,$$

where $\left(\frac{\mathrm{F}_\mathrm{k}^T/\mathrm{k}'}{\mathrm{N}_{\mathrm{L}'/\mathrm{k}'}(\mathfrak{P})}\right) = 1$. We then remark that $\mathrm{N}_{\mathrm{L}'/\mathrm{k}'}(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_{\mathrm{k}'}$ above $\mathfrak{p}$. By Theorem 4.5, it proves the existence of a T-split, $\{\mathfrak{p}_\mathrm{k}\}$-totally ramified, degree p cyclic extension of k. Then, $\mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{Z}/p\mathbb{Z}$ as $\mathcal{G}$-modules. But one still has $\mathrm{I}^T(U,\mathrm{L}) \twoheadrightarrow_\mathcal{G} \mathrm{I}^T(U,\mathrm{k})$, because $\mathfrak{p}_\mathrm{k}$ splits totally in L/k. By comparing the p-rank, one finally obtains: $\mathrm{I}^T(U,\mathrm{L}) \simeq \mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{Z}/p\mathbb{Z}$. □

To finish this part, we present a result of avoidance.

Proposition 4.13. *Suppose that the* $\mathbb{F}_p[\mathcal{G}]$*-module* $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ *contains a free sub-module* $\mathcal{H}'$ *of rank* $|\mathcal{G}|$ *with basis* $(x_g)_{g\in\mathcal{G}}$*. Put* $x_0 = \sum_{g\in\mathcal{G}}(g-1)x_g \in \mathcal{H}'$*. By Chebotarev density Theorem, take a prime ideal* $\mathfrak{P}$ *of* $\mathcal{O}_\mathrm{L}$ *such that* $\left\langle\left(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\right)\right\rangle = \langle x_0\rangle$*. Suppose moreover that* $\mathcal{H}' \bigcap \mathrm{F}(S) = \{0\}$*, where* $\mathrm{F}(S)$ *is the subgroup of* $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ *generated by the Frobenius of a* $\mathcal{G}$*-stable set* S *of ideals of* $\mathcal{O}_\mathrm{L}$*. Then, as* $\mathcal{G}$*-modules,* $\mathrm{I}_S^T(U,\mathrm{L}) \simeq \mathrm{I}_S^T(U,\mathrm{k}) \simeq \mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{Z}/p\mathbb{Z}$*, where* $U = \{\mathfrak{P}^g,\ g\in\mathcal{G}\}$*. Moreover* $\mathrm{I}_S^T(U,\mathrm{L}) \cap \mathrm{I}_U^T(S,\mathrm{L}) = \{e\}$.

Proof. As $x_0 \in \mathcal{H}'$, the module $\langle x_0\rangle_\mathcal{G}$ intersects $\mathrm{F}(S)$ trivially. As for Proposition 4.12, it implies that any T-split cyclic degree p extension of L, S-ramified and totally ramified at $\mathfrak{P}_0|\mathfrak{p}$ is totally ramified at all $\mathfrak{P}_0^g$, $g\in\mathcal{G}$. Hence, $d_p\mathrm{I}_S^T(U,\mathrm{L}) \leq 1$. But by Proposition 4.12, one knows that $d_p\mathrm{I}^T(U,\mathrm{L}) \geq 1$. As $\mathrm{I}_S^T(U,\mathrm{L}) \twoheadrightarrow \mathrm{I}^T(U,\mathrm{L})$ one obtains $\mathrm{I}_S^T(U,\mathrm{L}) \simeq_\mathcal{G} \mathbb{Z}/p\mathbb{Z}$.

Suppose now $\mathrm{I}_S^T(U,\mathrm{L}) \cap \mathrm{I}_U^T(S,\mathrm{L}) \neq \{e\}$. As $\mathrm{I}_S^T(U,\mathrm{L})$ is of order p, it implies that $\mathrm{I}_S^T(U,\mathrm{L}) \subset \mathrm{I}_U^T(S,\mathrm{L})$ and then every T-split, U-ramified, cyclic degree p extension of L, is in fact everywhere unramified, which contradicts $\mathrm{I}^T(U,\mathrm{L}) \simeq \mathbb{Z}/p\mathbb{Z}$. □

5. Proof of the main results

5.1 The strategy

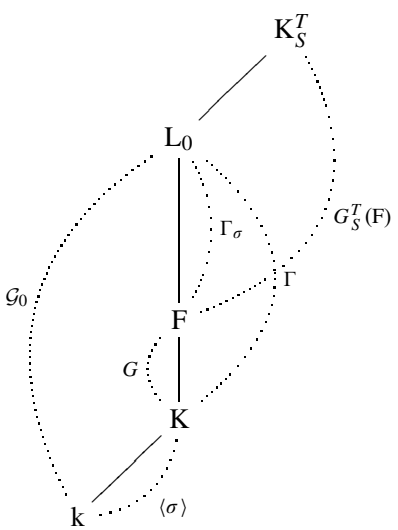
5.1.1

Let $\mathrm{L}_0/\mathrm{K}/\mathrm{k}$ be a σ-uniform tower; put $\Gamma = \mathrm{Gal}(\mathrm{L}_0/\mathrm{K})$, $\mathcal{G}_0 = \mathrm{Gal}(\mathrm{L}_0/\mathrm{k})$ and $\Delta = \langle\sigma\rangle$. We still assume that σ is of order $\ell \mid (p-1)$.

Denote by d the p-rank of Γ and by r the p-rank of the fixed points of σ acting on $\Gamma^{p,\mathrm{el}} = \Gamma/\Phi(\Gamma)$. Let $x_1,\ldots,x_n \in \Gamma$ be some lifts of some generators of $\Gamma^{p,\mathrm{el}}$ respecting the action of σ (see §3.2.1). We fix $x_1\ldots,x_r$ the lifts of the fixed points. Hence, by Proposition 3.7, $\Gamma_\sigma^\circ = \langle x_1,\ldots,x_r\rangle$, the pro-$p$ group Γ_σ is topologically generated by the conjuguates x_i^g, $i=1,\ldots,r$, $g\in G := \Gamma/\Gamma_\sigma$ of the x_i. Moreover by Proposition 3.10, $\Gamma_\sigma^{p,el}$ is minimally generated as $\mathbb{F}_p[[G]]$-module by the family $\{x_1\Phi(\Gamma_\sigma),\ldots,x_r\Phi(\Gamma_\sigma)\}$.

5.1.2

Now assume that Γ is the Galois group of a pro-p extension unramified outside S and totally split at T, *i.e.* a quotient of $\mathrm{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$. Suppose moreover that the places in S are coprime to p, in other words, S is tame. Then G_S^T and Γ are FAb. Put $\mathrm{F} := \mathrm{L}_0^{\Gamma_\sigma}$, $G := \mathrm{Gal}(\mathrm{F}/\mathrm{K})$ and $\mathcal{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{k})$. The situation is summarized in the diagram below.



By Proposition 3.5: $[\mathrm{F} : \mathrm{K}] < \infty$, and by maximality of K_S^T, one has $\mathrm{K}_S^T = \mathrm{F}_S^T$; put $\mathrm{G}_S^T(\mathrm{F}) := \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{F})$.

Then the natural map $\mathrm{G}_S^T(\mathrm{F}) \twoheadrightarrow \Gamma_\sigma$ factors through $\psi : \mathrm{G}_S^{T,ab}(\mathrm{F}) \twoheadrightarrow (\Gamma_\sigma)^{ab}$.

Of course, G acts on $\mathrm{G}_S^T(\mathrm{F})$ and on Γ_σ and then ψ is a G-morphism of abelian groups.

We recall that $x_1 \ldots, x_r$ are in Γ, they can be lifted to G_S^T. In fact, by construction, the elements $x_1 \ldots, x_r$ are in $\mathrm{G}_S^T(\mathrm{F})$ and by Proposition 3.10, their classes generate $\Gamma_\sigma^{p,el}$ as a $\mathbb{F}_p[G]$-module. Put $\mathrm{M} := \langle G \cdot x_i \Phi(\mathrm{G}_S^T(\mathrm{F})), i = 1, \ldots, r\rangle \subset \left(\mathrm{G}_S^T(\mathrm{F})\right)^{p,\mathrm{el}}$.

Proposition 5.1. *The morphism ψ induces a surjective G-morphism from* M *to* $\Gamma_\sigma^{p,el}$.

Now, we make our key observation: the group M is a subgroup of $\left(\mathrm{G}_S^T(\mathrm{F})\right)^{p,\mathrm{el}}$, it may be described by class field theory, and the G-structure of $\Gamma_\sigma^{p,el}$ depends only on the pro-p group Γ.

As we have mentioned in the beginning of this work, the goal is to find some situations where the G-structures of M *and of* Γ_σ^{ab} *are not compatible.*

5.2 When σ is of order 2

Suppose now that K/k is a quadratic extension such that $p \nmid |\mathrm{Cl}(\mathrm{k})|$; put $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = \langle\sigma\rangle$. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be a finite set of prime ideals of $\mathcal{O}_\mathrm{k}$ such that

$$(\mathrm{G}_S(\mathrm{K}))^{p,\mathrm{el}} \simeq_{\mathcal{G}} (\mathrm{G}_\emptyset(\mathrm{K}))^{p,\mathrm{el}} \bigoplus (\mathbb{Z}/p\mathbb{Z})^{\oplus^s}.$$

Let $\mathrm{I}(S)$ be the subgroup of $\mathrm{G}_S^{ab}(\mathrm{K})$ generated by the inertia groups of the primes in S. One then has $1 \longrightarrow \mathrm{I}(S) \longrightarrow \mathrm{G}_S^{ab}(\mathrm{K}) \longrightarrow \mathrm{G}_\emptyset^{ab}(\mathrm{K}) \longrightarrow 1$.

Take a minimal set of generators $\{x_1, \ldots, x_r, y_1, \ldots, y_r\}$ of $\mathrm{G}_S^{ab} = \mathrm{G}_S^{ab}(\mathrm{K})$ as follows: the elements $x_1, \ldots, x_s$ satisfy $\sigma(x_i) = x_i^{-1}$ and the elements $y_1, \ldots, y_r$ satisfy $\sigma(y_i) = y_i$.

Let $\mathrm{L}_0/\mathrm{K}/\mathrm{k}$ be a σ-uniform tower in K_S/k. Put $\mathrm{F} := \mathrm{L}_0^{\Gamma_\sigma}$. Let us recall that $\mathrm{Gal}(\mathrm{F}/\mathrm{K})$ is fixed point free under the action of σ of order 2: hence F/K is an abelian subextension of K_S^{ab}.

Recall that K^H denotes the Hilbert p-class field of K.

Lemma 5.2. *The extension* F/K *is unramified. Moreover,* $\mathrm{F} = \mathrm{L}_0 \cap \mathrm{K}^H$.

Proof. First observe that σ acts trivially on $I(S)$. As σ acts without non-trivial fixed point on $G = \Gamma/\Gamma_\sigma$ and that $G_S^{ab} \overset{f}{\twoheadrightarrow} G$, one then gets $f(\mathrm{I}(S)) = \{1\}$, meaning exactly that F/K is unramified, *i.e.* $\mathrm{F} \subset \mathrm{K}^H$. Put $\mathrm{F}_1 = \mathrm{L}_0 \cap \mathrm{K}^H$. Obviously, $\mathrm{F} \subset \mathrm{F}_1$. As σ acts by -1 on Cl(K), σ acts by -1 on $\mathrm{Gal}(\mathrm{F}_1/\mathrm{F})$. On the other hand, as F_1/K is abelian, one still has $\left(\Gamma_\sigma^{ab}\right)_G \twoheadrightarrow \mathrm{Gal}(\mathrm{F}_1/\mathrm{F})$. But by Proposition 3.10, the involution σ acts trivially on $\left(\Gamma_\sigma^{ab}\right)_G$, which implies that σ acts trivially on $\mathrm{Gal}(\mathrm{F}_1/\mathrm{F})$. To conclude: σ acts at a time by -1 and by $+1$ on $\mathrm{Gal}(\mathrm{F}_1/\mathrm{F})$, consequently $\mathrm{F}_1 = \mathrm{F}$. □

Proposition 5.3. *Let us conserve the notations and the conditions of this section. Suppose that T is a finite set of prime ideals of $\mathcal{O}_\mathrm{k}$, disjoint from S, such that:*

- *each prime ideal of T totally splits in* K^H/k*;*
- $\mathrm{Cl}_\emptyset^T(\mathrm{K}^H)$ *is trivial.*

Let $\rho : \mathrm{G}_S^T(\mathrm{K}) \to \mathrm{Gl}_m(\mathbb{Q}_p)$ be a continuous representation with σ-uniform image Γ. Then Γ_σ is supported at S, meaning the inertia groups of the prime ideals of S generate the group Γ_σ.

Proof. The σ-uniform tower $\mathrm{L}_0/\mathrm{K}/\mathrm{k}$ is in $\mathrm{K}_S^T/\mathrm{k}$. By Lemma 5.2 the inertia groups of $\mathfrak{p} \in S$ are in Γ_σ. Denote by L_1 the subfield of L_0 fixed by these inertia groups: the extension L_1/F is T-split and unramified everywhere. Suppose that L_1/F is not trivial. Then one can assume that L_1/F is of degree p. Then by Lemma 5.2, we get that $\mathrm{L}_1\mathrm{K}^H/\mathrm{K}^H$ is T-split and unramified, cyclic degree p extension. But by hypothesis $\mathrm{Cl}_\emptyset^T(\mathrm{K}^H)$ is trivial, and then, by class field theory, one obtains a contradiction. □

5.3 Proof of Theorem C

We are now able to prove Theorem C of the section 2.

Theorem 5.4 (Theorem C). *Let $p > 2$ and let $s \in \mathbb{N}$. Let K/k be a quadratic extension and suppose that p does not divide $|\mathrm{Cl}(\mathrm{k})|$. Let T be a finite set of places of k that totally splits in K^H/K, such that $|T| \geq \mathrm{A} + s|\mathcal{G}|$, where $\mathrm{A} = \mathrm{A}(\mathrm{K}^H/\mathrm{K})$ (see Theorem 4.1 for a more exact statement), and such that $\mathrm{Cl}^T_\emptyset(\mathrm{K}^H)$ is trivial. Then there exists s sets $\mathcal{S}_1, \ldots, \mathcal{S}_s$, of ideal primes of $\mathcal{O}_\mathrm{k}$, all of positive density, such that for $\Sigma = S \cup S'$ with $S' = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, where $\mathfrak{p}_i \in \mathcal{S}_i$, $i = 1, \ldots, s$, one has:*

(i) $(\mathrm{G}^T_S)^{p,\mathrm{el}} \simeq_\mathcal{G} \mathrm{Cl}(\mathrm{K})/p \bigoplus (\mathbb{Z}/p\mathbb{Z})^{\oplus^s}$;
(ii) *there is no continuous representation $\rho : \mathrm{G}^T_S \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image Γ which is fixed-point-mixing modulo Frattini.*

Proof. The proof is a combination of the previous results.

Let us conserve the notations of §4.1. Put $\mathrm{L} := \mathrm{K}^H$.

Let us take a finite set T of tame places of k such that:

- $|T| \geq \mathrm{A} + s|\mathcal{G}|$,
- each prime ideal of T totally splits in K^H/k,
- $\mathrm{Cl}^T_\emptyset(\mathrm{K}^H) = 1$.

□

Lemma 5.5. *There exists $s|\mathcal{G}|$ elements $\varepsilon^i_g \in \mathrm{V}^T_\mathrm{L}$, $g \in \mathcal{G}$, $i = 1, \ldots, s$, such that*

(i) *for every $i = 1, \ldots, s$, the $\mathbb{F}_p[\mathcal{G}]$-module $\sum_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon^i_g$ is free of rank $|\mathcal{G}|$, with basis $\{\varepsilon^i_g,\ g \in \mathcal{G}\}$;*
(ii) *the $\mathbb{F}_p[\mathcal{G}]$-modules $\sum_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon^i_g$ are in direct factors:*

$$\sum_{i=1}^{s} \sum_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon^i_g = \bigoplus_{i=1}^{s} \left(\sum_{g\in\mathcal{G}} \mathbb{F}_p[\mathcal{G}]\varepsilon^i_g \right).$$

Proof. This is a consequence of Theorem 4.1 and Proposition 4.2. □

Let us adapt the Proposition 4.13 in our context. For $i = 1, \ldots, s$, let $\mathcal{H}_i \subset \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ be the free $\mathbb{F}_p[\mathcal{G}]$-modules of basis $\{x^i_g,\ g \in \mathcal{G}\}$. Recall that these modules are obtained by Kummer duality from the elements of Lemma 5.5. Put also $x^i_0 := \sum_{g\in\mathcal{G}}(g-1)x^i_g \in \mathcal{H}'$. By Chebotarev density Theorem, let $\mathcal{S}_i$ be the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_\mathrm{K}$, such that the (class of) Frobenius of $\mathfrak{p}$ in F^T/k corresponds to x^i_0: the $\mathcal{S}_i$ is of positive density.

Then consider $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ a set of prime ideals of $\mathcal{O}_\mathrm{k}$, with $\mathfrak{p}_i \in \mathcal{S}_i$.

For $i = 1, \ldots, s$, choose a prime ideal $\mathfrak{P}_i|\mathfrak{p}_i$ of $\mathcal{O}_\mathrm{L}$ above $\mathfrak{p}_i$. Put $U_i = \{\mathfrak{P}^g_i, g \in G\}$.

Let us fix $i \in \{1, \ldots, s\}$, and put

$$S_i = U_1 \cup \cdots \cup U_{i-1} \cup U_{i+1} \cup \cdots \cup U_r,$$

here, we drop U_i.

Lemma 5.6.

(i) *Let R'/k be a Galois subextension of L/k of Galois group G'. Then as $\mathbb{F}_p[G']$-modules:*

$$\mathrm{I}^T(S, \mathrm{R}') \simeq \bigoplus_{i=1}^{s} \mathrm{I}^T_{S_i}(U_i, \mathrm{R}') \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus^s}.$$

(ii) *At the level of K, one has:*

$$\left(\mathrm{G}^T_S(\mathrm{K})\right)^{p,\mathrm{el}} \simeq_\mathcal{G} \left(\mathrm{G}^T_\emptyset(\mathrm{K})\right)^{p,\mathrm{el}} \bigoplus \left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus^s} \simeq_\mathcal{G} \left(\mathrm{G}_\emptyset(\mathrm{K})\right)^{p,\mathrm{el}} \bigoplus \left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus^s}.$$

Proof.

(i) First, take $\mathrm{R}' = \mathrm{L}$ and fix i. By Lemma 5.5, $\mathcal{H}_i \cap \mathrm{F}(S_i) = \{0\}$. Proposition 4.13 applied to U_i and to S_i allows us to get: $\mathrm{I}^T_{S_i}(U_i, \mathrm{L}) \simeq \mathrm{I}^T_{S_i}(U_i, \mathrm{K}) \simeq \mathrm{I}^T(U_i, \mathrm{k}) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{I}^T_{S_i}(U_i, \mathrm{L}) \cap \mathrm{I}^T_{U_i}(S_i, \mathrm{L}) = \{e\}$. Hence when i varies, the groups $\mathrm{I}^T_{S_i}(U_i, \mathrm{L})$ are in direct factors in $\big(\mathrm{G}^T_S(\mathrm{L})\big)^{p,\mathrm{el}}$.
Take now R' in L/k. As L/K is ramified, one has $\mathrm{I}^T_{S_i}(U_i, \mathrm{L}) \twoheadrightarrow \mathrm{I}^T_{S_i}(U_i, \mathrm{R}') \twoheadrightarrow \mathrm{I}^T_{S_i}(U_i, \mathrm{k})$ and one concludes thanks to $\mathrm{I}^T_{S_i}(U_i, \mathrm{L}) \simeq \mathrm{I}^T_{S_i}(U_i, \mathrm{k})$.

(ii) comes from the exact sequence of $\mathbb{F}_p[\langle\sigma\rangle]$-modules (which splits by semisimplicity):

$$1 \longrightarrow \bigoplus_{i=1}^{s} \mathrm{I}^T_{S_i}(U_i, \mathrm{K}) \longrightarrow \big(\mathrm{G}^T_S(\mathrm{K})\big)^{p,\mathrm{el}} \longrightarrow \big(\mathrm{G}^T_\emptyset(\mathrm{K})\big)^{p,\mathrm{el}} \longrightarrow 1$$

and by the choice of T: $\big(\mathrm{G}^T_\emptyset(\mathrm{K})\big)^{p,\mathrm{el}} \simeq \big(\mathrm{G}_\emptyset(\mathrm{K})\big)^{p,\mathrm{el}}$.

Let us start with a σ-uniform extension $\mathrm{L}_0/\mathrm{K}/\mathrm{k}$ such that $\mathrm{Gal}(\mathrm{L}_0/\mathrm{K})$ is a uniform quotient of $\mathrm{G}^T_S(\mathrm{K})$. Put $\Gamma = \mathrm{Gal}(\mathrm{L}_0/\mathrm{K})$ and assume that $d \geq 1$.

As $(\mathrm{G}^T_S(\mathrm{K}))^{p,\mathrm{el}} \twoheadrightarrow \Gamma^{p,\mathrm{el}}$, the action of σ on $\Gamma^{p,\mathrm{el}}$ has at most s "fixed points". Moreover by Boston [2] and [3], this action must have at least one non-trivial fixed point. Hence, here as Γ is supposed to be non trivial, we get $1 \leq r \leq s$, where $r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma$. Put $G := \Gamma/\Gamma_\sigma$.

If we denote by F the subfield of L_0 fixed by Γ_σ, then by Lemma 5.2 the extension F/K is unramified at S, $\mathrm{F} \subset \mathrm{K}^T_\emptyset$ and $\mathrm{G}^T_\emptyset(\mathrm{K}) \twoheadrightarrow \mathrm{Gal}(\mathrm{F}/\mathrm{K})$.

By Proposition 5.3, observe now that the fixed points in $(\mathrm{G}^T_S(\mathrm{F}))^{p,\mathrm{el}}$ come from the ramification at S.

By Lemma 5.6, the $\mathbb{F}_p$-vector space $\mathrm{I}^T(S, \mathrm{F})$ is of dimension s and the action of $G := \mathrm{Gal}(\mathrm{F}/\mathrm{K})$ on it is trivial: indeed, $\mathrm{I}^T(S, \mathrm{F}) \simeq_{\mathcal{G}} (\mathbb{Z}/p\mathbb{Z})^{\oplus^s}$. But, by Proposition 5.1 and by the condition above the ramification at the prime ideals $\mathfrak{p}_i \in S$, $\mathrm{I}^T S, \mathrm{F}) \twoheadrightarrow (\Gamma_\sigma)^{p,\mathrm{el}}$ and then G acts trivially on $(\Gamma_\sigma)^{p,\mathrm{el}}$. At this point, one uses the condition fixed-point-mixing modulo Frattini to obtain a contradiction: indeed in this case G should act non trivially on $(\Gamma_\sigma)^{p,\mathrm{el}}$. □

We can now say few words about the proofs of the results of §1 and §2.

– Theorem A of the subsection 1.1 comes from the fact that every involution σ on $\mathrm{Sl}^1_2(\mathbb{Z}_p)$ is of type $t_\sigma(\Gamma) = (1, b)$ and then is fixed-point-mixing modulo Frattini by Proposition 3.25. (Here T sufficiently large means also that $\mathrm{Cl}^T(\mathrm{K}^H)$) is trivial.) Hence the action of σ on Γ should be trivial. Thus $\mathrm{Im}(\rho)$ comes from k by compositum from K.
– Corollary D can be deduced from Theorem C and Proposition 3.28.

References

[1] A. Borel and J.-P. Serre, Sur certains sous-groupes des groupes de Lie compacts, *Comment. Math. Helv.*, **27** (1953) 128–139.
[2] N. Boston, Some cases of the Fontaine-Mazur conjecture, *J. Number Theory*, **42** no. 3, (1992) 285–291.
[3] N. Boston, Some cases of the Fontaine-Mazur conjecture II, *J. Number Theory*, **75** no. 2, (1999) 161–169.
[4] K. Buzzard, Analytic continuation of overconvergent eigenforms, *Jour. Am. Math. Soc.*, **16** (2002) 29–55.
[5] K. Buzzard and R. Taylor, Companion forms and weight 1 forms, *Annals of Math.*, **149** (1999) 905–919.
[6] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, *John Wiley and Sons, coll. "Pure and Applied Mathematics"*, no. 11 (1988).
[7] J. D. Dixon, M. P. F. Du Sautoy, A. Mann and D. Segal, Analytic pro-p-groups, *Cambridge studies in advances mathematics*, Cambridge University Press, **61** (1999).
[8] J.-M. Fontaine and B. Mazur, Geometric Galois representations, In Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA (1995).
[9] G. Gras, Class Field Theory, SMM, Springer (2003).
[10] G. Gras and A. Munnier, Extensions cycliques T-totalement ramifiées, *Publ. Math. Besançon* (1997/98).
[11] F. Hajir and C. Maire, Prime decomposition and the Iwasawa mu-invariant, *Mathematical Proceedings of the Cambridge Philosophical Society*, **166** (2019) 599–617.
[12] F. Hajir and C. Maire, Analytic Lie extensions of number fields with cyclic fixed points and tame ramification, arXiv:1710.09214 (2017).
[13] N. Jacobson, A note on automorphisms and derivations of Lie algebras, *Pacific J. Math.*, **12** (1962) 281–283.

[14] Kassaei, Payman L., Modularity lifting in parallel weight one, *J. Amer. Math. Soc.*, **26** no. 1, (2013) 199–225.
[15] M. Kisin, Modularity of 2-adic representations, *Invent. Math.*, **178(3)** (2009) 587–634.
[16] M. Kisin and S. Wortmann, A note on Artin motives, *Math. Res. Letters*, **10** no. 2–3 (2003), 375–389.
[17] M. Lazard, Groupes analytiques p-adiques, *IHES, Publ. Math.*, **26** (1965) 389–603.
[18] C. Maire, Finitude de tours et p-tours T-ramifiées modérées, S-décomposées, *J. Th. des Nombres de Bordeaux*, **8** (1996) 47–73.
[19] C. Maire, Some new evidence for the Fontaine-Mazur conjecture, *Mathematical Research Letters*, **14** (2007) 673–680.
[20] M. Ozaki, Construction of maximal unramified p-extensions with prescribed Galois groups, *Invent. Math.*, **183** no. 3, (2011) 649–680.
[21] V. Pilloni, Formes modulaires p-adiques de Hilbert de poids 1, *Invent. Math.*, **208** no. 2, (2017) 633–676.
[22] V. Pilloni and B. Stroh, Surconvergence, ramification et modularité, *Astérisque*, **382** (2016) 195–266.
[23] L. Ribes and P. Zalesskii, Profinite Groups, EMG 40, Springer (2010). Dedicated to Yuri I. Manin on the occasion of his 65th birthday, *Mosc. Math. J.*, **2** no. 2, (2002) 329–402.
[24] K. Wingberg, On the Fontaine-Mazur Conjecture for CM-Fields, *Compositio Math.*, **131** (2002) 341–354.