ANALYTIC LIE EXTENSIONS OF NUMBER FIELDS WITH CYCLIC FIXED POINTS AND TAME RAMIFICATION

by

Farshid Hajir & Christian Maire

Abstract. — Let p be a prime number and K an algebraic number field. What is the arithmetic structure of Galois extensions L/K having p-adic analytic Galois group $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$? 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.

Contents

2000 *Mathematics Subject Classification.* — 11R37, 22E20, 11R44.

Key words and phrases. — Uniform p-adic Lie groups, fixed points, tame Fontaine-Mazur conjecture, class field theory.

Acknowledgements. The second author would like to thank the Department of Mathematics & Statistics at UMass Amherst for its hospitality during several visits.

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 [**28**] 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 in the book [**9**] 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, which is to say creates 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.

We recall that a pro-p group Γ is called *uniform* if $\Gamma^p = \langle x^p,\ x \in \Gamma\rangle$ contains the commutators $[\Gamma,\Gamma]$ of Γ and if moreover Γ is torsion-free. By Lazard [**28**] (see also [**9**]), 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.
In [**4**] and [**5**], Boston initiated the study of the following situation (see also Wingberg [**41**] and Maire [**32**]). We fix a uniform pro-p group Γ and assume that Γ is realized as the Galois group of a *tamely ramified* extension L/K, i.e. $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, 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 $\Delta = \mathrm{Gal}(\mathrm{K}/\mathrm{k})$
- 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
- $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ is a uniform pro-p group of finite dimension d

***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.*

Here's the strategy of Boston's proof of this 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 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 [**18**] for a different application of this phenomenon in the context of Iwasawa theory where one allows wild ramification in L/K.

1.2. A sample result. — 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 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 $\#\mathscr{O}_{\mathrm{K}}/\mathfrak{p}\equiv 1 (\mathrm{mod}\ p)$. 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 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 $\mathrm{Sl}_2^1(\mathbb{Z}_p):=\ker\Big(\mathrm{Sl}_2(\mathbb{Z}_p)\to\mathrm{Sl}_2(\mathbb{F}_p)\Big)$ of dimension 3.

Theorem. — *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*. Let* $\Gamma=\mathrm{Sl}_2^1(\mathbb{Z}_p)$*. Suppose for all finite sets* Σ *of places of* k *with* $(\Sigma,p)=1$*, there is no continuous Galois representation* $G_\Sigma(\mathrm{k})\twoheadrightarrow\Gamma$*. 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) $\mathrm{G}_S^T(\mathrm{K})^{p,\mathrm{el}}$ *has* $|S|$ *independent fixed points under the action of* σ*,*

(iii) *there is no continuous* σ*-uniform representation* $\rho:\mathrm{G}_S^T(\mathrm{K})\twoheadrightarrow\Gamma$*.*

Remark 1.2. — The above theorem holds with $\Gamma = \mathrm{Sl}_n^1(\mathbb{Z}_p)$ for arbitrary n, under the additional assumption that the action of the automorphism σ on Γ corresponds to conjugation by a matrix of order 2 in $\mathrm{Gl}_n(\mathbb{Z}_p)$. For more details, see §5.3.

1.3. Motivation. — An important and vast "modularity" conjecture forms the motivation for the study begun by Boston and continued here. In [**10**], 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. If we restrict our attention to p-adic representations which are finitely and tamely ramified, we obtain the following consequence (Conjecture 5a of [**10**]) of this characterization (see Kisin-Wortmann [**25**] for the details).

Conjecture **(Tame Fontaine-Mazur Conjecture)**. — *For a finite set S of primes of* K *of residue characteristic not equal to p, and $n \geq 1$, any continuous Galois representation $\rho : \mathrm{G}_S \longrightarrow \mathrm{Gl}_n(\mathbb{Q}_p)$ 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 it is also FAb). We refer the reader to [**25**] 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 $\mathrm{K} = \mathbb{Q}$, 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 [**7**], Buzzard [**6**], Kessaei [**23**], Kisin [**24**], Pilloni [**35**], Pilloni-Stroh [**36**].

Recalling that every finitely generated p-adic analytic group has a uniform open subgroup, and that a uniform group of dimension 1 or 2 has quotient isomorphic to $\mathbb{Z}_p$, 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* $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$.

In the simplest non-trivial case, 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 listed above, 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 can 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 §2.5. Let us give two examples that we will study in section 5 and will be important to illustrate our results.

***Example 2.2* (See §5.2).** — 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 $\mathrm{Sl}_2^1(\mathbb{Z}_p) := \ker\Big(\mathrm{Sl}_2(\mathbb{Z}_p) \to \mathrm{Sl}_2(\mathbb{F}_p)\Big)$ is fixed-point-mixing modulo Frattini.

***Example 2.3* (See §5.3).** — More generally, for the FAb pro-p group

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

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 $t_\sigma(\Gamma) = (r, d-r)$. We will say that the type of action of automorphisms of order 2 on Γ is constant if for all $\sigma, \tau \in \mathrm{Aut}(\Gamma)$ of order 2, $t_\sigma(\Gamma) = t_\tau(\Gamma)$.

Under our blanket assumption that σ is non-trivial, it is easy to see that $t_\sigma(\Gamma) \neq (d, 0)$. In [**4**] and [**5**], 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 $\mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.
As before, put $\mathrm{G}_S^T = \mathrm{G}_S^T(\mathrm{K}) = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.

Theorem A. — *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 *totally split in K^H/K of large enough cardinality (see Theorem 6.7 for a more exact statement), and such that $\mathrm{Cl}^T(\mathrm{K}^H)$ is trivial. Then there exist s pairwise disjoint positive-density sets $\mathscr{S}_i$, $i = 1, \cdots, s$ of prime ideals $\mathfrak{p} \subset \mathscr{O}_\mathrm{k}$ of* k *such that for finite sets $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, 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.*

Remark 2.5. — The key point for obtaining (ii) above is as follows. The choices of S and T are made so that $(\mathrm{G}_S)^{p,\mathrm{el}} = (\mathrm{G}_S^T)^{p,\mathrm{el}}$. The action of σ on G_S^T has type $(s, d_p\mathrm{Cl}(\mathrm{K}))$, so we can rule out the existence of ρ with σ-uniform image Γ if $t_\sigma(\Gamma)$ is not compatible with $t_\sigma(\mathrm{G}_S^T)$. Such incompatibility can be caused at the level of the subgroup generated by the fixed points of σ. Typically, condition (i) of Theorem A assures an incompatibility for certain automorphisms of order 2. We will see that when σ has order 2, the contradiction can be detected already at the level of the Hilbert p-class field of K.

When Γ has constant type for all order 2 automorphisms, the following interesting situation arises.

Corollary 2.6. — *If the uniform group Γ of dimension $d > 0$ is such that for all $\sigma \in \mathrm{Aut}(\Gamma)$ of order 2, σ is fixed-point-mixing modulo Frattini, then under the conditions of Theorem A, all continuous representations $\rho : \mathrm{G}_S^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image Γ come from* k. *In particular, such a representation does not exist if either*

- *The Tame Fontaine-Mazur conjecture holds for* k, *or*
- *$d > |S|$.*

We can apply Theorem A to the groups $\mathrm{Sl}_n^1(\mathbb{Z}_p) = \ker\Big(\mathrm{Sl}_n(\mathbb{Z}_p) \to \mathrm{Sl}_n(\mathbb{F}_p)\Big)$, $n \geq 2$. 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 $A \in \mathrm{Gl}_n(\mathbb{Z}_p)$. According to [**39**], all automorphisms σ which act trivially on the Cartan subalgebra are of the form σ_A for some $A \in \mathrm{Gl}_n(\mathbb{Z}_p)$. We thus obtain the theorem of §1.2 and the remark following it.

Corollary 2.7. — *Under the conditions of Theorem A, there exist s positive-density sets $\mathscr{S}_i$, $i = 1, \ldots, s$ of prime ideals $\mathfrak{p} \subset \mathscr{O}_\mathrm{k}$ of* k, *such that for all finite sets $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, 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. When σ is of order $\ell \mid p-1$.— The results of the previous section for involutions can be generalized for other automorphisms. When σ has order $\ell > 2$, we need to introduce a notion of ramification in relation to the normal subgroup Γ_σ of Γ.

Definition 2.8. — Let $\rho : \mathrm{G}_\Sigma^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with image Γ be a σ-uniform representation for some $\sigma \in \mathrm{Aut}(\Gamma)$ of order prime to p. For a subset $S' \subset \Sigma$, we say that Γ_σ is supported at S' if the inertia groups at the places in S' generate Γ_σ.

For a positive integer n, let $\mathrm{K}_S^{(n)}/\mathrm{K}$ be the nth stage of the p-tower K_S/K, i.e. $\mathrm{K}_S^{(n)}$ is the fixed field of the nth term of the central series of $\mathrm{G}_S = \mathrm{G}_S(\mathrm{K})$. Since S does not contain primes dividing p, by class field theory, $\mathrm{K}_S^{(n)}/\mathrm{K}$ is a finite extension.

For a prime $\ell > 3$, we put

$$m(\ell) = 1 + \lceil 2^{\ell-1}\log_2(\ell-1) - \log_2(\ell-1)(\ell-2)\rceil; \tag{1}$$

we also define $m(2) = 1$ and $m(3) = 2$ – see remark 4.11 for an explanation of the motivation for this definition.

Theorem B. — *Let* K *be a number field admitting an automorphism σ of order $\ell \mid p-1$ with fixed field* $\mathrm{k} = \mathrm{K}^\sigma$. *Let S be a finite set of primes of* k *not dividing p such that the action of σ on G_S^{ab} has no non-trivial fixed-points. Let $s \in \mathbb{Z}_{>0}$. Then there is an integer A depending only on $[\mathrm{K}_S^{(m(\ell))} : \mathrm{K}]$, s and $|S|$ such that if T is a finite set of places of* k *that split completely in $\mathrm{K}_S^{(m(\ell))}/\mathrm{k}$ satisfying $|T| \geq \mathrm{A}$, then there exist s positive-density sets $\mathscr{S}_i$, $i = 1, \cdots, s$, of prime ideals $\mathfrak{p} \subset \mathscr{O}_\mathrm{k}$ of* k, *with the property that for all finite sets $S' = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, we have:*

(i) *the action of σ on $\mathrm{G}_\Sigma^T/\Phi(\mathrm{G}_\Sigma^T)$ has s independent fixed points, where $\Sigma = S \cup S'$;*
(ii) *there is no FPMF σ-uniform continuous representation $\rho : \mathrm{G}_\Sigma^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ such that Γ_σ is supported at S', where Γ is the image of ρ.*

2.4. Along the cyclotomic $\mathbb{Z}_p$-extension. — The realm of $\mathbb{Z}_p$-extensions is particularly rich for providing situations where we can take T (in the consideration of previous sections) as small as possible. Let $\mathrm{k}_\infty = \bigcup_n \mathrm{k}_n$ (resp. $\mathrm{K}_\infty = \bigcup_n \mathrm{K}_n$) be the cyclotomic $\mathbb{Z}_p$-extension of k (resp. of K), where as before K/k is a cyclic degree $\ell \mid p-1$ extension with Galois group $\langle\sigma\rangle$. Let us assume that all along $\mathrm{k}_\infty/\mathrm{k}$, the p-class groups of the fields k_n are trivial. Then σ acts without fixed-points on the p-class groups $\mathrm{Cl}(\mathrm{K}_n)$ of the fields K_n. On the other hand, the growth of $[\mathrm{K}_n : \mathrm{K}] = p^n$ allows us to apply Theorem B with $T = \emptyset$ as long as n is sufficiently large (when $\ell = 2$, we have to assume in addition that the real infinite places of k do not complexify in K/k).

Theorem C. — *Let $s \in \mathbb{Z}_{>0}$. Let* K/$\mathbb{Q}$ *be a real quadratic field and* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle\sigma\rangle$. *Let $\mathrm{K}_\infty = \bigcup_n \mathrm{K}_n$ (resp. $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$) be the cyclotomic $\mathbb{Z}_p$-extension of* K *(resp. of $\mathbb{Q}$). We assume that Greenberg Conjecture holds for* K *(the invariants μ and λ vanish). Then for $n_0 \gg 0$, there exist s positive density sets $\mathscr{S}_i$, $i = 1, \cdots, s$, of places $\mathfrak{p} \subset \mathscr{O}_{\mathbb{Q}_{n_0}}$, such that for all finite sets $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, and for all $n \geq n_0$,*

(i) *the action of σ on $\mathrm{G}_S(\mathrm{K}_n)/\Phi(\mathrm{G}_S(\mathrm{K}_n))$ has s independent fixed points;*
(ii) *there is no FPMF continuous σ-uniform $\rho : \mathrm{G}_S(\mathrm{K}_n) \longrightarrow \mathrm{Gl}_m(\mathbb{Q}_p)$ such that Γ_σ is supported at S, where Γ is the image of ρ.*

Remark 2.9. — We note that the pro-p group $\mathrm{G}_\emptyset(\mathrm{K})$ is infinite as soon as the p-rank of $\mathrm{Cl}(\mathrm{K})$ is at least 3 (Schoof [**38**]).

2.5. 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. To simplify, let us consider the context of Theorem A. 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

$$|T| \geq \alpha s + \beta, \tag{2}$$

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

$$d_p \mathrm{G}_S^T \geq 2 + 2\sqrt{|T| + r_1 + r_2 + 1}, \tag{3}$$

where (r_1, r_2) is the signature of K, the pro-p group G_S^T is infinite (see for example [**31**]). Moreover, the p-rank of G_S^T is at least s (because of the choice of S and T). Hence, by (2) and (3), one can guarantee the infiniteness of G_S^T by taking s sufficiently large, *i.e.* by introducing sufficiently many fixed points.

• *Uniform groups* (Part I). 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 4.6: 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* (Part II.) We fix K and consider varying sets S, T where $\mathrm{L} \subseteq \mathrm{K}_S^T$ has Galois group $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. To simplify the exposition, we now assume σ has order 2. Since G is abelian, the field F fixed by Γ_σ is abelian over K. If morevoer Γ_σ is supported at S then 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 $G_S^{ab}(\mathrm{F})$.

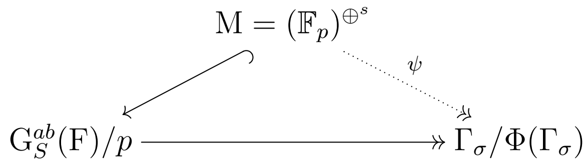
To show the existence of such prime ideals, one uses Kummer theory and the Chebotarev density Theorem. In order to do this, we require information about the units of the number field F, namely we need F to contain "Minkowski units". To be more precise, let $\mathscr{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{k})$; we say that F has a Minkowski unit if the quotient $\mathscr{O}_\mathrm{F}^\times/(\mathscr{O}_\mathrm{F}^\times)^p$ contains a non-trivial $\mathbb{F}_p[\mathscr{G}]$-free module. Note that we are not in the semisimple case as $p \mid |\mathscr{G}|$! This delicate and interesting question has been studied in recent work of Ozaki [**33**]: to estimate the rank of the maximal free $\mathbb{F}_p[\mathscr{G}]$-module of $\mathscr{O}_\mathrm{F}^\times/(\mathscr{O}_\mathrm{F}^\times)^p$. Our idea here is to introduce a set T and control the $\mathbb{F}_p[\mathscr{G}]$-structure of T-units of F.

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

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

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 $\mathrm{G}_S^{ab}(\mathrm{F})/p$ 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.

PART I
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 $d_p(\Gamma) = \dim_{\mathbb{F}_p} H^1(\Gamma, \mathbb{F}_p) = \dim_{\mathbb{F}_p} \Gamma^{p,\mathrm{el}}$ the p-rank of Γ: by the Burnside Basis Theorem, it is the minimal number of generators of Γ.

3. Schur-Zassenhaus

For this paragraph our reference is the book of Ribes and Zalesskii [**37**, 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* $1 \longrightarrow \Gamma \longrightarrow \mathscr{G} \longrightarrow \mathscr{G}/\Gamma \longrightarrow 1$ *be an exact sequence of profinite groups, where* Γ *is a pro-p group finitely generated and where* $\mathscr{G}/\Gamma$ *is finite of order coprime to p. Then the group* $\mathscr{G}$ *has a subgroup* Δ_0 *isomorphic* *to the quotient $\Delta = \mathscr{G}/\Gamma$ and Δ_0 is unique up to conjugation in $\mathscr{G}$. In particular: $\mathscr{G} = \Gamma \rtimes \Delta_0 \simeq \Gamma \rtimes \Delta$. In other words, the pointed set $H^1(\Delta, \Gamma)$ is reduced to $\{[0]\}$.*

Proof. — See for example Theorem 2.3.15, [**37**]. □

Let us now consider a finitely generated pro-p group Γ equipped with an automorphism $\sigma \in \mathrm{Aut}(\Gamma)$ of order coprime to p. To simplify, we moreover assume here that the order of σ is a prime number ℓ.

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 and if σ is of order 3 then Γ is nilpotent of class at most 2. For $\ell \geq 5$, the nilpotency class of Γ is at most $n(\ell) := \dfrac{(\ell-1)^{2^{\ell-1}-1}-1}{\ell-2}$.*

Proof. — See Corollary 4.6.10, [**37**]. □

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 of class at most $n(\ell)$. Moreover if Γ is FAb, the pro-p group G is also FAb, one concludes that G is finite. □

4. 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 [**9**] and [**28**].
Let Γ be a p-adic analytic pro-p group: the profinite group Γ is a closed subgroup of $\mathrm{Gl}_m(\mathbb{Z}_p)$ for some integer m. The group Γ is called *powerful* if $[\Gamma,\Gamma]\subset\Gamma^p$ ($[\Gamma,\Gamma]\subset\Gamma^4$ when $p=2$); a powerful pro-p group Γ is said *uniform* if it is torsion free. Let $\dim(\Gamma)$ be the dimension of Γ as analytic variety.

Theorem 4.1. — *Every p-adic analytic pro-p group contains an open uniform subgroup.*

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 pro-p group Γ.

Theorem 4.2. — *A powerful pro-p group Γ is uniform if and only if for $i\geq 1$, the map $x\mapsto x^p$ induces an isomorphism between Γ_i/Γ_{i+1} and Γ/Γ_2.*

Remark 4.3. — It is conjectured that a torsion-free p-adic analytic pro-p group satisfying $d_p(\Gamma)=\dim(\Gamma)$ must be uniform. This is known to be the case when $\dim(\Gamma)<p$, see [**26**].

4.1. Additive law and automorphisms. — Let Γ be a uniform pro-p group. If $\{x_1,\cdots,x_d\}$ is a minimal system of (topological) generators of Γ, then $\{x_1\Phi(\Gamma),\cdots,x_d\Phi(\Gamma\}$ forms a basis of $\Gamma^{p,\mathrm{el}}=\Gamma/\Phi(\Gamma)$. The group Γ being uniform, the morphism $x\mapsto x^{p^n}$ induces an isomorphism 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 $\mathbb{Z}_p^d$.

Theorem 4.4 **([9], Theorem 4.9)**. — *Let Γ be a uniform pro-p group. Then $\Gamma=\overline{\langle x_1\rangle}\cdots\overline{\langle x_d\rangle}$. In other words, for every $x\in\Gamma$, there exists a unique d-tuple $(a_1,\cdots,a_d)\in\mathbb{Z}_p^d$ such that $x=x_1^{a_1}\cdots x_n^{a_n}$. Moreover the map*

$$\begin{array}{rcl}\varphi:\Gamma & \longrightarrow & \Gamma_+\\ x=x_1^{a_1}\cdots x_d^{a_d} & \mapsto & a_1x_1\oplus\cdots\oplus a_nx_n\end{array}$$

is a homeomorphism (not necessarily of groups).

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 [**9**]). One needs more to determine the Galois structure.

Theorem 4.5. — *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 [**9**]. $\square$

4.2. 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. We first recall a result which is valid in a more general context (not only for uniform groups), for $\ell = 2$, see [**19**] ; for larger ℓ coprime to p, see [**3**], [**42**] and [**16**].

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. If the action of σ on the generators $x_1, \cdots, x_d$ of Γ_+ has $(a_{i,j})_{i,j}$ for matrix with coefficients in $\mathbb{Z}_p$, we get $\sigma(x_i) = \sum_{j=1}^{d} a_{i,j}x_j \in \Gamma_+$, which becomes in Γ: $\sigma(x_i) = \prod_{j=1}^{d} x_j^{a_{i,j}}$.

Put

$$r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma.$$

The integer r corresponds to the dimension of the $\mathbb{F}_p$-vector subspace of $\Gamma^{p,\mathrm{el}}$ consisting of fixed points of $\Gamma^{p,\mathrm{el}}$. The integer r is the number of times that the trivial character appears in the decomposition of the $\mathbb{F}_p[\langle\sigma\rangle]$-module $\Gamma^{p,\mathrm{el}}$.

Now let us fix a basis $\{x_1, \cdots, x_d\}$ of Γ respecting the decomposition into irreducible characters following the action of Γ. Suppose moreover that the set $\{x_1 \cdots, x_r\}$ corresponds to a basis of $(\Gamma^{p,\mathrm{el}})_\sigma$. In particular, $\sigma(x_i) = x_i$ for $i = 1, \cdots, r$. Clearly $\overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle} \subseteq \Gamma_\sigma^\circ$. For the reverse inclusion, one supposes moreover that ℓ divides $p-1$.

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

Proposition 4.6. — *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*

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

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,

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

As for $i = 1, \cdots, r$, one has $\sigma(x_i) = x_i$, we get

$$\prod_{i>r}^{d} x_i^{a_i} = \prod_{i>r} x_i^{\lambda_i a_i}.$$

Thanks to the uniqueness of the product in Theorem 4.4, 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 $\langle x_1, \cdots, x_r\rangle \subset \Gamma_\sigma^\circ$ and $\overline{\langle x_1\rangle} \cdots \overline{\langle x_r\rangle} \subset \langle x_1, \cdots, x_r\rangle$, which prove the desired equalities. □

Remark 4.7. — In the above considerations, the uniform property of Γ is essential. By Proposition 4.6 and when $\ell \mid (p-1)$, the group Γ_σ is the normal subgroup of Γ generated by the conjugates of the $x_1, \cdots, x_r$.

Remark 4.8. — The condition $\ell \mid (p-1)$ implies that the irreducible characters of σ are of degree 1 and then $\varphi \circ \sigma = \sigma \circ \varphi$. The existence of fixed points of σ can be detected in Γ or in Γ_+. Let us remark that we can omit the condition "$\ell \mid (p-1)$" when for all irreducible representations of $\mathbb{Z}_p$-basis $\{x_{i_1}, \cdots, x_{i_t}\}$, one has $x_{i_j} x_{i_k} = x_{i_k} x_{i_j}$. If the group Γ is obtained by a certain exponential of a $\mathbb{Z}_p$-Lie algebra $\mathfrak{L}$ (see §4.4), the condition on the commutativity can be tested in $\mathfrak{L}$: this remark should open some other perspectives.

We recover here, with a weaker hypothesis, *i.e.* $\ell \mid (p-1)$, the following corollary used in [**18**]:

Corollary 4.9. — *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 4.10. — *Under the conditions of Proposition 4.6, we have $d_p(\Gamma/\Gamma_\sigma) = d - r$ 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 $(x_i)_{i=1,\cdots,d}$ of Γ introduced above, satisfying in particular that $\sigma(x_i) = x_i$ for $i = 1, \cdots, r$. The group Γ_σ contains the elements $x_1, \cdots, x_r$. 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 $x_{r+1}\Phi(\Gamma)$ could be written in terms of the classes $\big(x_j\Phi(\Gamma)\big)_{j \neq r+1}$, which contradicts the minimality of $\{x_1, \cdots, x_d\}$. Hence $d_pG = d - r$. □

4.3. 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 $\mathbb{Z}_p[[G]] \simeq \mathbb{Z}_p[G]$.

Remark 4.11. — If Γ is FAb, the group $G = \Gamma/\Gamma_\sigma$ is a finite p-group of p-rank at most d and having an automorphism σ acting without non-trivial fixed points. By Shalev [**40**], it is possible to give an upper bound for the solvability length $\mathrm{dl}(G)$ of G which depends only on d: $\mathrm{dl}(G) \leq 2^{d+1} - d - 4 + \lceil \log_2 d \rceil$. By taking the proof of Shalev (lemma 4.4, lemma 4.5 and Proposition 4.6 of [**40**]), we remark that a key point is the number of distinct eigenvalues of σ. We note that in [**40**], a slightly different notion of G being "uniform" is used: in Shalev's terminology, for a such group G, one has $\mathrm{dl}(G) \leq 2^{\ell-1} - 1$. If we remove the condition of G being uniform in the sense of Shalev, we have a weaker bound $\mathrm{dl}(G) \leq d(2^{\ell-1} - 1) + \lceil \log_2(d) \rceil$. One should compare these bounds to the bounds $m(\ell)$ coming from [**37**], Corollary 4.6.10 (see Proposition 3.4) and given in the introduction (by recalling that $\mathrm{dl}(G) \leq \log_2(n(\ell) + 1)$).

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 4.12. — (i) *The cosets $x_1\Phi(\Gamma_\sigma), \cdots, x_r\Phi(\Gamma_\sigma)$ 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 $d_p\Gamma_\sigma \geq r$.*

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

Proof. — (i) By Proposition 4.6, the group Γ_σ° is topologically generated by the elements $x_1, \cdots, x_r$: they form a minimal system of generators. Thus the quotient $\Gamma_\sigma^{p,el}$ is topologically generated by the G-conjuguates $G \cdot x_i\Phi(\Gamma_\sigma)$ of the classes of the x_i, $i = 1, \cdots, r$, in $\Gamma_\sigma^{p,el}$. Consider now the exact sequence

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

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 $x_1, \cdots, x_r$, the action of σ on $G^{p,\mathrm{el}}$ has no non-trivial fixed points. Moreover as $\Gamma_\sigma^{p,el}$ is generated by the G-conjuguates of the classes of the x_i, $i = 1, \cdots, r$, one gets that σ acts trivially on $\left(\Gamma_\sigma^{p,el}\right)_G$. 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 $x_1\Phi(\Gamma_\sigma), \cdots, x_r\Phi(\Gamma_\sigma)$ form a minimal system of generators of the $\mathbb{F}_p[[G]]$-module $\Gamma_\sigma^{p,el}$. In conclusion we get $d_p\Gamma_\sigma \geq r$. Now (ii) is obvious: the group Γ_σ^{ab} is generated by the G-conjuguates of the classes of the $x_i\Phi(\Gamma_\sigma)$, $i = 1, \cdots, r$, hence σ acts trivially on $\left(\Gamma_\sigma^{ab}\right)_G$. □

Remark 4.13. — As consequence of the proof, we get an exact sequence:

$$1 \longrightarrow \left(\Gamma_\sigma^{p,el}\right)_G \longrightarrow \Gamma^{p,\mathrm{el}} \longrightarrow G^{p,\mathrm{el}} \longrightarrow 1,$$

and then $H_2(\Gamma, \mathbb{F}_p) \twoheadrightarrow H_2(G, \mathbb{F}_p)$.

Recall that for a uniform group Γ of dimension d, for all closed subgroup U of Γ, one has $d_p\mathrm{U} \leq d$.

Remark 4.14. — Assume G finite. On can define its maximal free sub-$\mathbb{F}_p[G]$-module $\left(\Gamma_\sigma^{p,el}\right)_0$ of $\Gamma_\sigma^{p,el}$. As the p-rank of Γ_σ is smaller than d, one sees that $\left(\Gamma_\sigma^{p,el}\right)_0$ is trivial as soon as $|G| > d$.

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 4.15. — *If the action of σ on Γ is not fixed-point-mixing modulo Frattini, then $\Gamma_\sigma = \Gamma_\sigma^\circ$ and $d_p\Gamma_\sigma = r$.*

Proof. — It is a consequence of Proposition 4.12. □

Proposition 4.16. — *Let Γ be a uniform group of dimension dimension $d > 1$. Suppose $\sigma \in \mathrm{Aut}(\Gamma)$ of order $\ell = 2$. Recall that $r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma$.*

(i) *If $t_\sigma(\Gamma) = (1, d-1)$ and if Γ_σ is open (which is the case if Γ is FAb), then the action of σ on Γ is fixed-point-mixing modulo Frattini.*
(ii) *If $t_\sigma(\Gamma) = (d-1, 1)$ and if $d_p\Gamma_\sigma > r$, then Γ_σ is uniform.*

Proof. — (i) If $d_p\Gamma_\sigma = 1$, the group Γ_σ is generated by only one element and then is procyclic. If Γ_σ is open, 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 4.15.
(ii) Here $d_p\Gamma_\sigma = d$ which is equivalent to Γ_σ being a uniform group (of dimension d). □

Remark 4.17. — We will see in Proposition 4.30 that when Γ is FAb and uniform of dimension d, $t_\sigma(\Gamma) \neq (d-1,1)$.

***Remark 4.18* (See [29])**. — For every uniform group Γ, there exists an open subgroup Γ_0 such that for all open subgroup U of Γ_0, one has $d_p\mathrm{U} \geq \dim(\mathfrak{L}(\Gamma))$, where $\dim(\mathfrak{L}(\Gamma))$ is the dimension of the Lie algebra associated to Γ (see the next section). If moreover Γ is FAb, one has also $\dim(\mathfrak{L}(\Gamma)) < \dim(\Gamma) = d_p\Gamma$.

4.4. Uniform groups and Lie algebras. —

4.4.1. 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 $(x,y)_n := \psi_{2n}([x^{p^n}, y^{p^n}])$ and define

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

***Theorem 4.19* ([9],Theorem 4.30)**. — *The $\mathbb{Z}_p$-module Γ_+ equipped with the bracket $(\cdot,\cdot)$ is a $\mathbb{Z}_p$-Lie algebra of dimension d. Denote by $\mathscr{L}_\Gamma$ this new Lie algebra.*

Remark 4.20. — 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 $\mathscr{L}_\Gamma$.

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: $(\mathscr{L}_\Gamma,\mathscr{L}_\Gamma) \subset 2p\ \mathscr{L}_\Gamma$.

Definition 4.21. — A $\mathbb{Z}_p$-Lie algebra $\mathscr{L}$ is called powerful if $(\mathscr{L},\mathscr{L}) \subset 2p\mathscr{L}$.

Recall now the following correspondence.

***Theorem 4.22* ([9], 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 [**9**]), which we now sketch. Using the formal series of $\mathbb{Q}_p[[X]]$

$$E(X) = \sum_{n\geq 0}\frac{1}{n!}X^n \quad \text{and} \quad L(X) = \sum_{n\geq 1}\frac{(-1)^{n+1}}{n}X^n,$$

we define

$$\Phi(X,Y) = L(E(X)E(Y)-1)\cdot$$

We consider the series Φ in the Lie algebra $\mathbb{Q}_p((X,Y))$ equipped with the bracket $[X,Y] = XY - YX$. For $U_1,\cdots,U_t \in \mathbb{Q}_p((X,Y))$, let us define by induction $[U_1,\cdots,U_t] = [[U_1,\cdots,U_{t-1}],U_t]$. If e is the multiset $e = (e_1,\cdots,e_s)$, $e_i \geq 1$ for all i, put $[X,Y]_e = [X, X(e_1), Y(e_2),\cdots]$, where $X(e_i)$ (resp. $Y(e_j)$) denotes the constant e_i-tuple $X(e_i) = (X,\cdots,X)$ (resp. the e_j-tuple $Y(e_j) = (Y,\cdots,Y)$). Hence $[X,Y]_e$ is a bracket of length $\langle e\rangle := 1 + e_1 + \cdots + e_s$.

In $\mathbb{Q}_p((X,Y))$, let us write $\Phi = \sum_n u_n(X,Y)$, where u_n denote the elements of degree n which can be expressed as a sum

$$u_n(X,Y) = \sum_{\langle e\rangle = n-1} q_e[X,Y]_e,$$

where $q_e \in \mathbb{Q}$. One translate these formulas to the $\mathbb{Z}_p$-Lie algebras $\mathscr{L}$ equipped with the bracket $(\cdot,\cdot)$. Suppose $\mathscr{L}$ powerful. Then for all $x,y \in \mathscr{L}$, the specialization of Φ at the bracket (x,y) converges in $\mathscr{L}$ (see Corollary 6.38 of [**9**]). Concretely, in the formulas one has replaced $[X,Y]$ by (x,y).

Theorem 4.23 **([9], Theorem 9.8 and Theorem 9.10)**. — *Let $\mathscr{L}$ be a powerful $\mathbb{Z}_p$-Lie algebra of dimension d. Let $\{x_1,\cdots,x_d\}$ be a $\mathbb{Z}_p$-basis of $\mathscr{L}$. The law $x*y = \Phi(x,y)$ makes $\mathscr{L}$ into a uniform group $\Gamma_{\mathscr{L}}$ of dimension d, topologically generated by $\{x_1,\cdots,x_d\}$. Moreover $\mathscr{L}_{\Gamma_{\mathscr{L}}} \simeq \mathscr{L}$ and $\Gamma_{\mathscr{L}_\Gamma} \simeq \Gamma$.*

Remark 4.24. — Let us examine carefully the case where $\mathscr{L}$ is a powerful sub-Lie-algebra of the Lie algebra $\mathscr{M}_n(\mathbb{Q}_p)$ 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 [**9**]): $\mathscr{L} \underset{\log}{\overset{\exp}{\rightleftarrows}} \exp(\mathscr{L})$. Thus for $A,B\in\mathscr{L}$, we get $\exp(A)\exp(B) = \exp(\Phi(A,B))$, where Φ is the Campbell-Hausdorff series (see Proposition 6.27) and then $\exp(\mathscr{L})$ is isomorphic to the uniform group $\Gamma_{\mathscr{L}}$ (see Corollary 6.25 of [**9**]).

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 4.25. — *A uniform group Γ is FAb if and only if*

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

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

Proof. — For every open subgroup H of the uniform group Γ, $\mathscr{L}_H(\mathbb{Q}_p) = \mathscr{L}_\Gamma(\mathbb{Q}_p)$. Hence, one has to prove that Γ^{ab} is finite if and only if, $\mathscr{L}_\Gamma(\mathbb{Q}_p) = (\mathscr{L}_\Gamma(\mathbb{Q}_p), \mathscr{L}_\Gamma(\mathbb{Q}_p))$. 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 [**9**], the subgroup H is uniform, the $\mathbb{Z}_p$-Lie algebra $\mathscr{L}_H$ is an ideal of $\mathscr{L}_\Gamma$, and $\mathscr{L}_{\Gamma/H} \simeq \mathscr{L}_\Gamma/\mathscr{L}_H$. As Γ/H is abelian, the Lie algebra $\mathscr{L}_{\Gamma/H}$ is commtutative (corollary 7.16 of [**9**]). In fact, $\mathscr{L}_{\Gamma/H} = \mathbb{Z}_p$. Then $\mathscr{L}_H$ contains $[\mathscr{L}_\Gamma, \mathscr{L}_\Gamma]$; thus $\mathscr{L}_\Gamma/(\mathscr{L}_\Gamma,\mathscr{L}_\Gamma) \twoheadrightarrow \mathscr{L}_\Gamma/\mathscr{L}_H \simeq \mathbb{Z}_p$ and therefore $(\mathscr{L}_\Gamma(\mathbb{Q}_p), \mathscr{L}_\Gamma(\mathbb{Q}_p)) \subsetneq \mathscr{L}_\Gamma(\mathbb{Q}_p)$.

In the other direction, suppose that $(\mathscr{L}_\Gamma(\mathbb{Q}_p), \mathscr{L}_\Gamma(\mathbb{Q}_p)) \subsetneq \mathscr{L}_\Gamma(\mathbb{Q}_p)$, or equivalently that the $\mathbb{Z}_p$-rank of $\mathscr{L}_\Gamma/(\mathscr{L}_\Gamma,\mathscr{L}_\Gamma)$ is not trivial. Put $\mathscr{L}_1 = \mathscr{L}_\Gamma/(\mathscr{L}_\Gamma,\mathscr{L}_\Gamma)$. As $\mathbb{Z}_p$-modules, let us write $\mathscr{L}_1 = \mathscr{L}_0 \oplus \mathrm{Tor}(\mathscr{L}_1)$. It is then easy to see that $\mathrm{Tor}(\mathscr{L}_1)$ is an ideal of the Lie algebra $\mathscr{L}_1$. Thus consider the quotient $\mathscr{L}_0 := \mathscr{L}_1/\mathrm{Tor}(\mathscr{L}_1)$: it is a non trivial, commutative and torsion-free $\mathbb{Z}_p$-Lie algebra! By the correspondence of Theorem 4.22, the algebra $\mathscr{L}_0$ corresponds to a uniform abelian group Γ_0 (by Corollary 7.16 of [**9**]). In fact, as $\mathscr{L}_0 \simeq \mathbb{Z}_p^t$, with $t>0$, on has $\Gamma_0 \simeq \mathbb{Z}_p^t$. The algebra $\mathscr{L}_0$ is also the quotient of $\mathscr{L}_\Gamma$ by the ideal $\mathscr{L}_2$ generated by $(\mathscr{L}_\Gamma,\mathscr{L}_\Gamma)$ and the lifts of $\mathrm{Tor}(\mathscr{L}_1)$. By Proposition

7.15 of [**9**], under the correspondence of Theorem 4.22, the algebra $\mathscr{L}_2$ corresponds to a uniform closed subgroup H of Γ; moreover Γ/H is uniform. Therefore as for the previous implication, we get $\mathscr{L}_{\Gamma/H} \simeq \mathscr{L}_\Gamma/\mathscr{L}_2 \simeq \mathscr{L}_0 \simeq \mathbb{Z}_p^t$ and then $\Gamma/H \simeq \Gamma_0 \simeq \mathbb{Z}_p^t$. □

The proof has shown the following result:

Corollary 4.26. — *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 $\mathscr{L}$ which is simple or even semisimple (after extending scalars) produces a uniform FAb group by Proposition 4.25.

4.4.2. Lie algebras and fixed points. — We now further explore the Lie algebra $\mathscr{L}$ over $\mathbb{Q}_p$. Denote by $(\cdot,\cdot)$ the Lie bracket of $\mathscr{L}$. For algebras of dimension 2 or 3, see for example [**22**], §I.4.

Definition 4.27. — Let $\mathscr{L}$ be a Lie algebra and let $\sigma \in \mathrm{Aut}(\mathscr{L})$. Put $\mathscr{L}_\sigma = \{x \in \mathscr{L}, \sigma(x) = x\}$.

Let us introduce the notion of FAb algebra.

Definition 4.28. — A Lie algebra $\mathscr{L}$ over $\mathbb{Q}_p$ is called FAb if $(\mathscr{L},\mathscr{L}) = \mathscr{L}$. 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 [**2**] (cf the remark of Jacobson [**21**], page 281), we have the following Proposition.

Proposition 4.29. — *Let $\mathscr{L}$ be a* FAb *Lie algebra and let $\sigma \in \mathrm{Aut}(\mathscr{L})$ of order ℓ. Then $\mathscr{L}_\sigma \neq \{0\}$.*

Proof. — Indeed, by Proposition 4 of [**2**], if $\mathscr{L}_\sigma = \{0\}$ then $\mathscr{L}$ 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 $\sigma \in \mathrm{Aut}(\mathscr{L})$ is of order 2, as for pro-p groups, one define the σ-type of $\mathscr{L}$ as $t_\sigma(\mathscr{L}) = (a,b)$, where $a = \dim\ker(\sigma - \iota)$ and $b = \dim\ker(\sigma + \iota)$, ι being the trivial automorphism. We have $a = \dim \mathscr{L}_\sigma$ and $b = d - a$ where $d = \dim \mathscr{L}$.

Proposition 4.30. — *Let $\mathscr{L}$ be a FAb $\mathbb{Q}_p$-Lie algebra of dimension d and let $\sigma \in$* $\mathrm{Aut}(\mathscr{L})$ *be of order* 2. *Let $t_\sigma(\mathscr{L}) = (a,b)$ be the σ-type of $\mathscr{L}$. Then $a \neq 0$ and $b > 1$.*

Proof. — By Proposition 4.29, the type $(0,d)$ is excluded. Suppose $\mathscr{L}$ of type $(d-1,1)$. Take a $\mathbb{Q}_p$-basis $\{e_1, e_2, \cdots, e_{d-1}, \varepsilon\}$ of $\mathscr{L}$ respecting the action σ, *i.e.* for $i = 1,\cdots,d-1$, $\sigma(e_i) = e_i$ 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 $(e_i,e_j) \in \langle e_1,\cdots,e_{d-1}\rangle$ 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 $i = 1,\cdots,d-1$, $(e_i,\varepsilon) = \lambda_i\varepsilon$. As the Lie algebra is FAb, the matrix $(a_k(i,j))_{((i,j),k)}$ of size $\dfrac{(d-1)(d-2)}{2} \times (d-1)$ must be of maximal rank, *i.e.* $d-1$. Also the vector $(\lambda_1,\cdots,\lambda_{d-1})$ are non zero.

Now the elements $(e_i)_i$ and ε should 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 $\mathscr{L}$ is not FAb. □

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

Corollary 4.31. — *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 is constant and equal to $t_\sigma(\Gamma) = (1, 2)$.*

On other hand, look at Lie algebras $\mathscr{L}$ having few fixed points. Consider, say, a Lie algebra $\mathscr{L}$ of dimension 4 such that $\mathscr{L}_\sigma$ is of dimension 1. Let $\{e_1, e_2, e_3, \varepsilon\}$ be a $\mathbb{Q}_p$-basis of $\mathscr{L}$ 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 $(e_i, \varepsilon) \in \langle e_1, \cdots, e_3 \rangle$. A linear algebra computation similar to those of Proposition 4.30 shows that $\mathscr{L}$ can not be FAb: necessarily, $\mathscr{L}/(\mathscr{L}, \mathscr{L}) \twoheadrightarrow \mathbb{Q}_p$. The same holds for the dimension 5. In fact, it is a general and well-known phenomenon for semisimple Lie algebras $\mathscr{L}$. Indeed dimension of $\mathscr{L}_\sigma$ grows with the dimension of $\mathscr{L}$ (see Theorem 10 and Theorem 8 of [**21**]).

5. Examples

5.1. First examples. — We first give examples of non FAb uniform groups having an automorphism σ of order 2 with fixed points. We assume that $p > 2$.

5.1.1. Direct product. — Consider $\mathbb{Z}_p \times \mathbb{Z}_p = \langle x \rangle \times \langle y \rangle$ with $\sigma(x) = x$ and $\sigma(y) = y^{-1}$; $t_\sigma(\Gamma) = (1,1)$. Then $\Gamma_\sigma = \Gamma_\sigma^\circ = \langle x \rangle$ and $G = \Gamma/\Gamma_\sigma = \langle y \rangle \simeq \mathbb{Z}_p$. Here $\mathbb{Z}_p[[G]] \simeq \mathbb{Z}_p[[T]]$ and the action of y on x is trivial.

5.1.2. Semidirect product. — For $a \in \mathbb{Z}_p^\times$, Consider

$$\Gamma = \Gamma(a) = \langle x, y \mid y^x = y^a \rangle$$

which can be realized concretely as $\Gamma = \langle \xi, \eta \rangle \subset \mathrm{Gl}_2(\mathbb{Z}_p)$ where

$$\xi = \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}, \ \eta = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

Without loss of generality, we may take $a = 1 + p^k$. Let $\sigma \in \mathrm{Aut}(\Gamma)$ of order 2 such that $\sigma(x) = x$ and $\sigma(y) = y^{-1}$. Here, $t_\sigma(\Gamma) = (1, 1)$. One then has $\Gamma_\sigma = \langle x, y^{a-1}\rangle$ and $G \simeq \mathbb{Z}/p^k\mathbb{Z}$, where k is the p-adic valuation of $a - 1$: the subgroup Γ_σ is open. One has $[x, y] = y^{p^k}$, therefore $[x, y^n] = y^{np^k}$. Put $x_i = \sigma^i(x)$ and let us use the additive notation. For $2 \leq n \leq p^k - 1$, one has the relation $x_n = (1 - n)x_0 + nx_1$. Thus $(\Gamma_\sigma)^{p,\mathrm{el}} = \mathbb{F}_p[G] \cdot x = \langle x_0, x_1\rangle$ which is of p-rank 2. The action of σ on Γ is fixed-point-mixing modulo Frattini (see also Proposition 4.16).

If we consider the decomposition of $(\Gamma_\sigma)^{p,\mathrm{el}}$ as the sum of indecomposable modules (see [**8**], lemma 64.2), one necessarily obtains $(\Gamma_\sigma)^{p,\mathrm{el}} \simeq_G I^{p^k-2}$, where $I := \ker\Big(\mathbb{F}_p[G] \to \mathbb{F}_p\Big)$ is the augmentation ideal of $\mathbb{F}_p[G]$.

5.1.3. The Heisenberg group. — Let $\mathscr{L}$ be the $\mathbb{Z}_p$-Lie algebra of dimension 3 generated by the matrices $x = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix}$, $z = \begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix}$, with bracket $[A, B] = AB - BA$. Hence $[x, y] = 0$, $[x, z] = pz$ and $[y, z] = -pz$. Moreover $\mathscr{L}$ is powerful but not FAb because $[\mathscr{L}(\mathbb{Q}_p), \mathscr{L}(\mathbb{Q}_p)] = \mathbb{Q}_p z$. Denote by Γ the uniform group generated by the exponentials of x, y and z:

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

under the correspondence of Theorem 4.23 (see remark 4.24). The $\mathbb{Z}_p$-rank of Γ^{ab} is equal to 2 and $\Gamma^{ab} \simeq \mathbb{Z}_p^2 \times \mathbb{Z}/p\mathbb{Z}$. Let $\sigma = \sigma_A \in \mathrm{Aut}(\Gamma)$ be the automorphism of order 2 corresponding to conjugation by the matrix $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$: $\sigma(M) = A^{-1}MA$. Then $\Gamma_\sigma^\circ = \langle X, Y\rangle \simeq \mathbb{Z}_p^2$ and $G := \Gamma/\Gamma_\sigma = \langle Z\Gamma_\sigma\rangle \simeq \mathbb{Z}/p\mathbb{Z}$. As here G is finite and as Γ_σ° is of analytic dimension 2, necessarily $\Gamma_\sigma^\circ \subsetneq \Gamma_\sigma$ and then G does not act trivially on $(\Gamma_\sigma)^{p,\mathrm{el}}$.

5.2. The group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$. — As before, we assume $p > 2$. 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 $\mathrm{Sl}_2(\mathbb{Z}_p) \to \mathrm{Sl}_2(\mathbb{F}_p)$. The group $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ is FAb, uniform and of dimension 3.

Proposition 5.1. — *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 4.31, every automorphism σ of order 2 is of type $(1, 2)$. One concludes with Proposition 4.16. □

By using the correspondence of Section 4.4.1, one can say more. Consider the homomorphisms "exponential" and "logarithm" of matrices: $\mathfrak{sl}_2 \underset{\log}{\overset{\exp}{\rightleftarrows}} \mathrm{Sl}_2^1(\mathbb{Z}_p)$.

Given $A \in \mathrm{Gl}_2(\mathbb{Z}_p)$ and $B \in \mathfrak{sl}_2$, one has $\exp(\sigma_A(B)) = \sigma_A(\exp B)$, where $\sigma = \sigma_A$ is the conjugation by A, providing the passage from $\mathrm{Aut}(\mathrm{Sl}_2^1(\mathbb{Z}_p))$ to $\mathrm{Aut}(\mathfrak{sl}_2)$, and *vice versa*. Let τ be an involution of $\mathrm{Sl}_2^1(\mathbb{Z}_p)$. The automorphism τ induces an involution on $\mathfrak{sl}_2$ and then on $\mathfrak{sl}_2(\mathbb{Q}_p)$. The key point comes from the fact that every automorphism of $\mathfrak{sl}_2(\mathbb{Q}_p)$ is the automorphism σ_A of conjugation by a certain matrix $A \in \mathrm{Gl}_2(\mathbb{Q}_p)$ (see [**39**], Theorem 1); thus $\tau(T) = \sigma_A(T) = A^{-1}TA$. Now, one can assume that the coefficients of A are in $\mathbb{Z}_p$. Then, as σ is of order 2 and acts on $\mathfrak{sl}_2$, the minimal polynomial of A is $X^2 - 1$ or $X^2 - \varepsilon$, for $\varepsilon \in \mathbb{Z}_p^\times \backslash (\mathbb{Z}_p^\times)^2$. And, at the end, one can assume that $A \in \mathrm{Gl}_2(\mathbb{Z}_p)$. Hence the matrix A is similar in $\mathrm{Gl}_2(\mathbb{Z}_p)$ to $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or to $D_\varepsilon = \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}$ (see [**34**]).
Let $\sigma = \sigma_D$ and $\sigma_\varepsilon = \sigma_{D_\varepsilon}$ be the two involutions of $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ corresponding to the conjugation by D or by D_ϵ respectively. They are defined by

- $\sigma(X) = X^{-1}$, $\sigma(Y) = Y^{-1}$ and $\sigma(Z) = Z$;
- $\sigma_\varepsilon(X) = Y^{1/\varepsilon}$, $\sigma_\varepsilon(Y) = X^\varepsilon$ and $\sigma_\varepsilon(Z) = Z^{-1}$.

Hence there exists $M \in \mathrm{Gl}_2(\mathbb{Z}_p)$ such that $MAM^{-1} = D$ or D_ε. Thus $\tau = \sigma_A = \sigma_M^{-1}\sigma\sigma_M$ or $\tau = \sigma_M^{-1}\sigma_\varepsilon\sigma_M$. As the matrices M and A are in $\mathrm{Gl}_2(\mathbb{Z}_p)$, σ_M and σ_A are in $\mathrm{Aut}(\mathrm{Sl}_2^1(\mathbb{Z}_p))$: the correspondence gives that the identity $\tau = \sigma_M^{-1}\sigma\sigma_M$ can be seen to be in $\mathrm{Aut}(\mathrm{Sl}_2^1(\mathbb{Z}_p))$ showing that τ is conjuguate to σ or to σ_ε in $\mathrm{Aut}(\mathrm{Sl}_2^1(\mathbb{Z}_p))$. Lastly, let us remark that for σ, the situation is easy to describe: one has $\Gamma_\sigma^\circ = \langle Z \rangle$. Let $\Gamma_\sigma = \langle Z \rangle^{\mathrm{Norm}}$ be the normal subgroup of $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ generated by the conjuguates of Z and put $G := \Gamma/\Gamma_\sigma$. As $XZX^{-1}Z^{-1} = \begin{pmatrix} 1 & p(1-e^{2p}) \\ 0 & 1 \end{pmatrix}$ becomes trivial in G, one has that X^p is trivial in G. Then thanks to Proposition 4.10, one has: $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

5.3. The group $\mathrm{Sl}_n^1(\mathbb{Z}_p)$. — Let $\mathfrak{sl}_n(\mathbb{Q}_p)$ be the $\mathbb{Q}_p$-Lie algebra constitued 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 $t > 1$, $D_i = (d_{k,l})_{k,l}$ which is the diagonal matrix $D_i = (p, 0, \cdots, 0, -p, 0, \cdots, 0)$, 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 powerful and uniform.
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.

By Seligman [**39**], one knows that the automorphisms of the algebra $\mathfrak{sl}_n(\mathbb{Q}_p)$ are generated by those of two types, namely those of the form $\sigma_A(X) = X^{-1}AX$ with $A \in \mathrm{Gl}_n(\mathbb{Q}_p)$, or of the form $X \mapsto \sigma_A(-X')$, where X' corresponds to the transposition of X.

We now examine the inner automorphisms σ_A. Put $\Gamma = \mathrm{Sl}_n^1(\mathbb{Z}_p)$ and take an automorphism σ of order 2. The automorphism σ induces an automorphism of order 2 on $\mathfrak{sl}_n(\mathbb{Q}_p)$

that we assume of the form σ_A. As for $\mathrm{Sl}_2^1(\mathbb{Z}_p)$, one reduces to the case where A has X^2-1 or $X^2-\varepsilon$ as minimal polynomial, for some $\varepsilon \in \mathbb{Z}_p^\times \backslash (\mathbb{Z}_p^\times)^2$. In particular, when n is odd, this polynomial is X^2-1. It is also the case if we have:

$$\Gamma \rtimes \langle \sigma \rangle \simeq \Gamma \rtimes \langle A \rangle \hookrightarrow \mathrm{Gl}_n(\mathbb{Z}_p),$$

where A is a matrix of order 2 that acts by conjugation. Let us assume that A is of order 2. As with the case of $\mathrm{Sl}_2^1(\mathbb{Z}_p)$, we can simplify to the case where A is diagonal with ± 1 eigenvalues. Denote by $k = \dim \ker(A-I)$, *i.e.* the number of $+1$s on the diagonal.

Lemma 5.2. — *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 $\{i,j\} \subset \{1,\cdots,k\}$ or for $\{i,j\} \subset \{k+1,\cdots,n\}$. 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 $\{i,j\} \subset \{1,\cdots,k\}$ and for $\{i,j\} \subset \{k+1,\cdots,n\}$.

Proposition 5.3. — *Under the above conditions, one has*
(i) $\Gamma_\sigma^\circ = \langle X_{i,j}, \{i,j\} \subset \{1,\cdots,k\}, \{i,j\} \subset \{k+1,\cdots,n\},\ D_l, i \neq j, l > 1\rangle\cdot$
(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 4.6.
(ii) is an easy computation. □

Hence one sees that 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.

Proposition 5.4. — *Let $n \geq 2$ and let $\sigma = \sigma_A$ with* $\mathrm{A} \in \mathrm{Gl}_n(\mathbb{Z}_p)$ *of order* 2. *Then*
(i) $\mathrm{Sl}_n^1(\mathbb{Z}_p)/\mathrm{Sl}_n^1(\mathbb{Z}_p)_\sigma \simeq (\mathbb{Z}/p\mathbb{Z})^{2k(n-k)}$;
(ii) *The action of σ on* $\mathrm{Sl}_n^1(\mathbb{Z}_p)$ *is fixed-point-mixing modulo Frattini.*

Proof. — One only has to verify (i): it is a computation as for $\mathrm{Sl}_2^1(\mathbb{Z}_p)$. □

PART II
ARITHMETIC RESULTS

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 $\mathscr{O}_K$, 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 $\#\mathscr{O}_\mathrm{K}/\mathfrak{p} \equiv 1 (\mathrm{mod}\ p)$. 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.
– Let $\mathscr{O}_\mathrm{K}^T$ be the group of T-units of K.
– Let $\mathscr{O}_{\mathrm{K},S}^T$ be the subgroup of $\mathscr{O}_\mathrm{K}^T$ defined as the kernel of the natural map

$$\mathscr{O}_\mathrm{K}^T \to \prod_{v\in S} \mathbb{F}(\mathrm{K},v)^\times,$$

where $\mathbb{F}(\mathrm{K},v)$ denote the residue field of K at v; in other words, $\mathscr{O}_{\mathrm{K},S}^T$ is the group of T-units of K congruent to 1 modulo $\mathfrak{p}$, for all $\mathfrak{p} \in S$.
– If L/K is an extension of K, we still denote by abuse, $S = S(\mathrm{L})$ be the set of primes of $\mathscr{O}_\mathrm{L}$ above the primes $\mathfrak{p} \in S$.

6. On the freeness of T-units in the non-semisimple case

6.1. 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 $\mathscr{G}$. We assume that $\mathscr{G}$ has only one p-Sylow subgroup G; put $\Delta := \mathscr{G}/G$. Hence Δ is a finite group of order coprime to p. Put $\mathrm{K} = \mathrm{L}^G$. The group $\mathscr{O}_\mathrm{L}^T$ of T-units of L has a structure of $\mathbb{Z}[\mathscr{G}]$-module.
– Put $\mathscr{E} := \mathscr{O}_\mathrm{L}^T/(\mathscr{O}_\mathrm{L}^T)^p = \mathbb{F}_p \otimes \mathscr{O}_\mathrm{L}^T$.
– Henceforth, we assume that:
  – the archimedean places of K split completely in L,
  – the primes of T split completely in L/k,
  – the extension L/K is unramified outside S.
– Denote by S_{ram} the set of primes of primes of $\mathscr{O}_\mathrm{K}$ in S that are ramified in L/K.

We are interested in finding some arithmetic situations for which the $\mathbb{F}_p[\mathscr{G}]$-module $\mathscr{E}$ contains a non-trivial free $\mathscr{G}$-module. To this end, we are going to use and extend an idea of Ozaki [**33**].

Let us first recall the semisimple version of Dirichlet's unit theorem that will be of interest to us.

Theorem 6.1 **(Dirichlet's unit theorem - see [14])**. — *With all the notation and assumptions as listed above, let $D_1, \cdots, D_m$ be the decomposition groups of the archimedean places of* k *in* K/k. *Then one has the isomorphism of $\mathbb{F}_p[\Delta]$-modules:*

$$\mathbf{1} \oplus \mathscr{O}_\mathrm{K}^T/(\mathscr{O}_\mathrm{K}^T)^p \simeq \mathrm{Ind}_{D_1}^\Delta \mathbb{F}_p \oplus \cdots \oplus \mathrm{Ind}_{D_m}^\Delta \mathbb{F}_p \oplus \mathbb{F}_p[\Delta]^{|T|} \oplus \chi_p,$$

where χ_p is the cyclotomic character corresponding to the action of Δ on the pth roots of the unity in K.

6.2. Technical results. —

6.2.1. On some structural elements. — Let Δ be a finite group of order coprime to p.

Definition 6.2. — If M is a finitely generated $\mathbb{F}_p[\Delta]$-module, denote by $r_\Delta(M)$ its minimal number of generators.

Remark 6.3. — The semisimplicity of $\mathbb{F}_p[\Delta]$ allows us to study $r_\Delta(M)$. First, let us recall that an $\mathbb{F}_p[\Delta]$-module M is monogenic if and only if its character χ_M is contained in the regular character Reg of $\mathbb{F}_p[\Delta]$ (we write this as $\chi_M \leq \mathrm{Reg}$). Hence, given an $\mathbb{F}_p[\Delta]$-module M, to determine $r_\Delta(M)$ is equivalent to resolving the decomposition of χ_M into characters, all of them being in the regular representation.

Denote by $(\cdot)^*$ the Pontryagin dual $\mathrm{Hom}(\,\cdot\,, \mathbb{Q}_p/\mathbb{Z}_p)$. From now on, all the $\mathbb{F}_p[\Delta]$-modules under consideration are assumed finitely generated.

Lemma 6.4. — *(i)If $A \twoheadrightarrow B$ is a surjective $\mathbb{F}_p[\Delta]$-morphism, then $r_\Delta(A) \geq r_\Delta(B)$.*
(ii) If A is an $\mathbb{F}_p[\Delta]$-module, then $r_\Delta(A) = r_\Delta(A^*)$.
(iii) If A and B are $\mathbb{F}_p[\Delta]$-modules such that $A \hookrightarrow B$, then $r_\Delta(A) \leq r_\Delta(B)$.
(iv) Let $\cdots \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow \cdots$ be an exact sequence of $\mathbb{F}_p[\Delta]$-modules. Then

$$r_\Delta(B) \leq r_\Delta(A) + r_\Delta(C) \;\cdot$$

(v) If A and B are two $\mathbb{F}_p[\Delta]$-modules such that $B \simeq \mathbb{F}_p[\Delta]^t \oplus A$, then $r_\Delta(B) = t + r_\Delta(A)$.
(vi) If A and B are two Δ-modules such that $pA = 0$ and $A \hookrightarrow B$, then $r_\Delta(A) \leq d_pB$.

Proof. — (i) is obvious.
For (ii), let us write $\chi_A = \chi_1 + \cdots + \chi_s$ with $s = r_\Delta(A)$ and $\chi_i \leq \mathrm{Reg}$, $i = 1, \cdots, s$. Then $\chi_{A^*} = \chi_A^* = \chi_1^* + \cdots + \chi_s^*$, where χ_i^* is the dual character of χ_i defined by $\chi^*(s) = \chi(s^{-1})$. But trivially, $\chi_i^* \leq \mathrm{Reg}$ and then $r_\Delta(A^*) \leq r_\Delta(A)$. It then implies, $r_\Delta(A^{**}) \leq r_\Delta(A^*)$ and the conclusion holds by using the Δ-isomorphism $A \simeq A^{**}$.
(iii) is a consequence of (i) and (ii), after passing to the dual.
(iv) is consequence of (i) and (iii).
For (v): it suffices to prove the equality for $t = 1$. First of all, one has $r_\Delta(B) \leq 1 + r_\Delta(A)$, *i.e.* $r_\Delta(A) \geq r_\Delta(B) - 1$. Then let us write $\chi_B = \chi_1 + \cdots \chi_s$, with $s = r_\Delta(B)$ and $\chi_i \leq \mathrm{Reg}$, $i = 1, \cdots, s$. As χ_B contains the regular representation Reg, one may complete for example the character χ_1 with some irreducible characters coming from the other characters χ_i, $i > 1$, to obtain Reg. Then we get $\chi_B = \mathrm{Reg} + \chi_2' + \cdots + \chi_s'$, with for $i = 2, \cdots, s$, $\chi_i' \leq \chi_i \leq \mathrm{Reg}$. It implies that $\mathrm{Reg} + \chi_A = \chi_B = \mathrm{Reg} + \chi_2' + \cdots + \chi_s'$ showing $\chi_A = \chi_2' + \cdots + \chi_s'$ and then $r_\Delta(A) \leq s - 1 = r_\Delta(B) - 1$. In conclusion, one has the desired equality: $r_\Delta(B) = r_\Delta(A) + 1$.
(vi) It is a trivial estimation. It is clear that $r_\Delta(A) \leq d_pA$; the conclusion follows from the fact that $d_pA \leq d_pB$. $\square$

6.2.2. Semilocal rings and a lower bound. — We first recall some classical results about semilocal rings; for more details see [**27**, Chapter 2].

Let us conserve the arithmetic context of the previous section 6.1: we start with $\mathscr{G} \simeq G \rtimes \Delta$, where G is the unique p-Sylow G of $\mathscr{G}$.

The group algebra $\mathbb{F}_p[\mathscr{G}]$ is a semilocal ring of radical $R := \langle g - 1,\ g \in G\rangle$; the quotient $\mathbb{F}_p[\mathscr{G}]/R$ is isomorphic to the semisimple algebra $\mathbb{F}_p[\Delta]$ (see [**8**], §64, exercice).

The algebra $\mathbb{F}_p[\mathscr{G}]$ is also Frobenius: one has the $\mathbb{F}_p[\mathscr{G}]$-modules isomorphism $\mathbb{F}_p[\mathscr{G}] \simeq \Big(\mathbb{F}_p[\mathscr{G}]\Big)^*$, coming from the symmetric non-degenerate bilinear form $(f,g) = \sum_{g\in\mathscr{G}} f(h)g(h^{-1})$, for $f = \sum_h f(h)h$ and $g = \sum_h g(h)h \in \mathbb{F}_p[\mathscr{G}]$. Thus, every free submodule M_0 of a finitely generated $\mathbb{F}_p[G]$-module M is in direct factor in M: indeed, if $\mathbb{F}_p[\mathscr{G}] \hookrightarrow M$ then by duality $M^* \twoheadrightarrow \mathbb{F}_p[\mathscr{G}]^*$; by projectivity of $\mathbb{F}_p[\mathscr{G}]$, the free module can be lifted in direct factor in M^*, and it suffices to take the dual again.

In conclusion, every finitely generated $\mathbb{F}_p[\mathscr{G}]$-module M has a free maximal submodule (in direct factor): there exists an integer $t = t(M)$ such that

$$M \simeq \mathbb{F}_p[\mathscr{G}]^t \oplus N,$$

where N is of torsion (for all $x \in N$, there exists $\lambda \in \mathbb{F}_p[\mathscr{G}]$, $\lambda \neq 0$, such that $\lambda \cdot x = 0$). The integer t is unique. We deduce a first relation:

$$d_p M = |\mathscr{G}|t + d_p N,$$

where here d_p means as usual the p-rank.
On the other hand, as $\mathbb{F}_p[\mathscr{G}]^G \simeq \mathbb{F}_p[\Delta]$, we get $M^G \simeq \mathbb{F}_p[\Delta]^t \oplus N^G$, and then by 6.4 (iv), $r_\Delta(M^G) = t + r_\Delta(N^G)$.

Recall that for a finitely generated $\mathbb{F}_p[\mathscr{G}]$-module A, one has a Δ-isomorphism: $(A^*)_G \simeq (A^G)^*$.

Recall now Nakayama's Lemma (see [**27**, Chapter 2 §4]).

Lemma 6.5. — *The $\mathbb{F}_p[\mathscr{G}]$-module A is generated by $m_1, \cdots, m_s$ if and only if, the $\mathbb{F}_p[\Delta]$-module $A/(RA) = A_G$ is generated by $m_1RA, \cdots, m_sRA$. In particular, one can take $s = r_\Delta(A_G)$.*

Let us come back to our context and start with $M = \mathbb{F}_p[\mathscr{G}]^t \oplus N$. By Lemma 6.4 (ii), $r_\Delta(N^G) = r_\Delta((N^G)^*)$. By Nakayama's Lemma 6.5, the $\mathbb{F}_p[\mathscr{G}]$-module N^* can be generated by $r_\Delta((N^*)_G) = r_\Delta((N^G)^*) = r_\Delta(N^G) = r_\Delta(M^G) - t$ elements. Then, let us remark that:

$$d_p N^* \leq (|\mathscr{G}| - 1)\Big(r_\Delta(M^G) - t\Big)\cdot$$

Indeed, as N^* is of torsion (because N is), for every element $x \in N\backslash\{0\}$, we have $\mathbb{F}_p[\mathscr{G}] \cdot x \simeq \mathbb{F}_p[\mathscr{G}]/\mathrm{Ann}(x)$, where $\mathrm{Ann}(x)$ is the annulator of x, it is a non zero ideal of $\mathbb{F}_p[\mathscr{G}]$, and then $d_p\mathbb{F}_p[\mathscr{G}] \cdot x = |\mathscr{G}| - d_p\mathrm{Ann}(x) \leq |\mathscr{G}| - 1$. Then

$$d_p N = d_p N^* \leq \Big(|\mathscr{G}| - 1\Big) r_\Delta(N^*),$$

by Lemma 6.5.

Proposition 6.6. — *Let M be a finitely generated $\mathbb{F}_p[\mathscr{G}]$-module. Then there is a well-defined non-negative integer $t = t(M)$ such that $M \simeq \mathbb{F}_p[\mathscr{G}]^t \oplus N$, with N of torsion. For this t, we have the following lower bound:*

$$t \geq d_p M - \Big(|\mathscr{G}| - 1\Big) \cdot r_\Delta(M^G)\cdot$$

Proof. — Note that $d_p N = d_p M - t|\mathscr{G}|$ and that $d_p N \leq (|\mathscr{G}| - 1)\Big(r_\Delta(\mathrm{M}^G) - t\Big)$: the conclusion is obvious. □

6.3. Cohomology of units. — We are going to apply Proposition 6.6 to the $\mathbb{F}_p[\mathscr{G}]$-module $M = \mathscr{E} = \mathbb{F}_p \otimes \mathscr{O}_{\mathrm{L}}^T$. Our arithmetic context will allow us to give some situations where, in the notation of the preceding proposition, t may be as big as possible (thanks to the choice of T). To do this, we need to give a sharp estimate of $r_\Delta(\mathscr{E}^G)$. More precisely, we propose to show the following result in this direction.

Theorem 6.7. — *As introduced at the beginning of this section, let* L/k *be a finite Galois extension with Galois group* $\mathscr{G}$*. We assume that* $\mathscr{G}$ *has only one* p*-Sylow subgroup* G*; put* $\Delta := \mathscr{G}/G$*. Hence* Δ *is a finite group of order coprime to* p*. Put* $\mathrm{K} = \mathrm{L}^G$*. We assume that the archimedean places of* K *split completely in* L*. There exists a constant* $\mathrm{A} = \mathrm{A}(\mathrm{L}/\mathrm{K}) \in \mathbb{Z}$ *(depending on the "arithmetic" in* L/K*) 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* $\mathbb{F}_p[\mathscr{G}]$*-module* $\mathscr{E} = \mathbb{F}_p \otimes \mathscr{O}_{\mathrm{L}}^T$ *contains a submodule isomorphic to* $\mathbb{F}_p[\mathscr{G}]^m$*.*

This theorem will be proved in two stages (Theorem 6.10 and Theorem 6.13) which will give an explicit formula for $\mathrm{A}(\mathrm{L}/\mathrm{K})$ depending on whether L contains a primitve pth root of unity or not. The proofs will occupy us in the next two subsections.

Remark 6.8. — We will see that when $[\mathrm{K} : \mathbb{Q}]$ is small with respect to $|\mathscr{G}|$ then $\mathrm{A} > 0$. But, as we will see too, the context of the cyclotomic $\mathbb{Z}_p$-extension produces some situations where A is negative.

Remark 6.9. — When the arithmetic context L/k is fixed, the growth of T allows us to assure that the T-units admit an arbitrarily large free $\mathbb{F}_p[\mathscr{G}]$-submodule. This explains the appearance of the constant A in Theorems A and B.

To achieve our goal, we are going to develop an idea of Ozaki [**33**]. 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). We let (r_1, r_2) be the signature of k. We also let $\mu_p = \langle \zeta_p \rangle$ be the group of pth roots of unity. The proof will very much depend on whether non-trivial pth roots of unity are present in L.

6.3.1. When $\mathscr{O}_{\mathrm{L}}^T$ *does not contain* μ_p*.* — We prove

Theorem 6.10. — *Let* L/K *be a Galois extension with Galois group* $\mathscr{G} \simeq G \rtimes \Delta$*, where the order of* Δ *is coprime to the* p*-Sylow* G *of* $\mathscr{G}$*.* Suppose that L does not containt μ_p. *Let us decompose the* $\mathbb{F}_p[\mathscr{G}]$*-module* $\mathscr{E} := \mathbb{F}_p \otimes \mathscr{O}_{\mathrm{L}}^T$ *as* $\mathbb{F}_p[\mathscr{G}]^t \oplus N$*, where* N *is of torsion. Under the arithmetic conditions of section 6.1, one has*

$$t \geq |T| + d_\infty + \frac{1}{2}r_\infty - (|\mathscr{G}| - 1)\Big(r_1 + r_2 - d_\infty - \frac{1}{2}r_\infty + d_p\mathrm{Cl}_S^T(\mathrm{K}) + |\mathscr{G}||S| + |S_{ram}|\Big) - 1\cdot$$

Remark 6.11. — When μ_p is not contained in $\mathscr{O}_{\mathrm{L}}^T$, put

$$\mathrm{A} = -\Big(d_\infty + \frac{1}{2}r_\infty - (|\mathscr{G}| - 1)\Big(r_1 + r_2 - d_\infty - \frac{1}{2}r_\infty + d_p\mathrm{Cl}_S(\mathrm{K}) + |\mathscr{G}||S| + |S_{ram}|\Big) - 1\Big).$$

We note that $d_p\mathrm{Cl}_S^T(\mathrm{K}) \leq d_p\mathrm{Cl}_S(\mathrm{K})$.

The goal of the end of this section is to prove Theorem 6.10.

First of all, let us remark that all the cohomology groups $H^\bullet(G, \cdot)$ are finite Δ-modules.

Let us start with the exact sequence of G-modules corresponding to raising to the pth-power :

$$\mathbf{1} \longrightarrow \mathscr{O}_{\mathrm{L}}^T \xrightarrow{p} \mathscr{O}_{\mathrm{L}}^T \longrightarrow \mathscr{E} \longrightarrow 1\cdot$$

We then have

$$\mathbb{F}_p \otimes \mathscr{O}_{\mathrm{K}}^T \hookrightarrow \mathscr{E}^G \twoheadrightarrow H^1(G, \mathscr{O}_{\mathrm{L}}^T)[p]\cdot \tag{4}$$

Thanks to Lemma 6.4 (iv), this exact sequence of $\mathbb{F}_p[\Delta]$-module gives the inequality

$$r_\Delta(\mathscr{E}^G) \leq r_\Delta(H^1(G, \mathscr{O}_{\mathrm{L}}^T)[p]) + r_\Delta(\mathbb{F}_p \otimes \mathscr{O}_{\mathrm{K}}^T)\cdot \tag{5}$$

We want to bound the quantities $r_\Delta(H^1(G, \mathscr{O}_{\mathrm{L}}^T)[p])$ and $r_\Delta(\mathbb{F}_p \otimes \mathscr{O}_{\mathrm{K}}^T)$.

As the extension L/K is unramified outside S, it is possible to control the cohomology group $H^1(G, \mathscr{O}_{\mathrm{L}}^T)$. Indeed put $j_{\mathrm{L/K},S}^T : \mathrm{Cl}_S^T(\mathrm{K}) \to \mathrm{Cl}_S^T(\mathrm{L})$ for the natural "conorm" morphism of ideal classes. The following proposition, that is a generalization of a result of Iwasawa [**20**] when $T = S = \emptyset$, has been proved in Maire [**30**]:

Proposition 6.12. — *Let* L/K *be a finite Galois extension unramified outside S and tamely ramified at S. Put* $G = \mathrm{Gal}(\mathrm{L/K})$. *Then* $H^1(G, \mathscr{O}_{L,S}^T) \simeq_\Delta \ker(j_{L/K,S}^T)$.

Proof. — See [**30**]. □

Let us estimate the difference between $\mathscr{O}_{\mathrm{L}}^T$ and $\mathscr{O}_{L,S}^T$. Start with the exact sequence

$$1 \longrightarrow \mathscr{O}_{L,S}^T \longrightarrow \mathscr{O}_{\mathrm{L}}^T \longrightarrow B \longrightarrow 1,$$

where $\varphi : B \hookrightarrow \prod_{v \in S} \mathbb{F}(\mathrm{L}, v)^\times$ and where $\mathbb{F}(\mathrm{L}, v)$ is the residue field of L at v. One has

$$\cdots \longrightarrow H^1(G, \mathscr{O}_{\mathrm{L},S}^T) \longrightarrow H^1(G, \mathscr{O}_{\mathrm{L}}^T) \longrightarrow H^1(G, B) \longrightarrow \cdots$$

and

$$\cdots \longrightarrow H^0(G, \mathrm{coker}\varphi) \longrightarrow H^1(G, B) \longrightarrow H^1(G, \prod_{v \in S} \mathbb{F}(\mathrm{L}, v)^\times) \longrightarrow \cdots$$

Denote by α the morphism $\alpha : H^1(G, \mathscr{O}_{\mathrm{L}}^T)[p] \longrightarrow H^1(G, B)[p]$. Then, one has the exact sequence of $\mathbb{F}_p[\Delta]$-modules:

$$1 \longrightarrow \ker(\alpha) \longrightarrow H^1(G, \mathscr{O}_{\mathrm{L}}^T)[p] \longrightarrow \mathrm{Im}(\alpha) \longrightarrow 1\cdot$$

By Lemma 6.4 (iv), one has

$$r_\Delta(H^1(G, \mathscr{O}_L^T)[p]) \leq r_\Delta(\mathrm{Im}(\alpha)) + r_\Delta(\ker(\alpha)). \tag{6}$$

By Lemma 6.4 (iii), as $\mathrm{Im}(\alpha) \hookrightarrow H^1(G, B)[p]$, one obtains

$$r_\Delta(\mathrm{Im}(\alpha)) \leq r_\Delta(H^1(G, B)[p]). \tag{7}$$

Moreover, if we denote $B' := \mathrm{Im}\Big(B^G \to H^1(G, \mathscr{O}_{\mathrm{L},S}^T)\Big)$, then

$$\ker(\alpha) \simeq \Big(H^1(G, \mathscr{O}_{\mathrm{L},S}^T)/B'\Big)[p] \hookrightarrow H^1(G, \mathscr{O}_{\mathrm{L},S}^T)/B' \twoheadleftarrow H^1(G, \mathscr{O}_{\mathrm{L},S}^T)$$

and then, by Proposition 6.12 and Lemma 6.4 (vi), one obtains the upper bound:

$$r_\Delta(\ker(\alpha)) \leq d_p \mathrm{Cl}_S^T(\mathrm{K}). \tag{8}$$

Using (6), (7) and (8), one obtains:

$$r_\Delta(H^1(G,\mathscr{O}_{\mathrm{L}}^T)[p]) \leq r_\Delta(H^1(G,B)[p]) + d_p\mathrm{Cl}_S^T(\mathrm{K})\cdot \tag{9}$$

To estimate $r_\Delta(H^1(G,B)[p])$, let β be the morphism

$$\beta : H^1(G,B)[p] \longrightarrow \Big(H^1(G,\prod_{v\in S}\mathbb{F}(\mathrm{L},v)^\times)\Big)[p].$$

One has

$$r_\Delta(H^1(G,B)[p]) \leq r_\Delta(\mathrm{Im}(\beta)) + r_\Delta(\ker(\beta)). \tag{10}$$

As before, the evaluation of $r_\Delta(\mathrm{Im}(\beta))$ is made thanks to the estimation of

$$r_\Delta(H^1(G,\prod_{v\in S}\mathbb{F}(\mathrm{L},v)^\times)[p]).$$

By Shapiro's Lemma, one has the Δ-isomorphism

$$H^1(G,\prod_{v\in S}\mathbb{F}(\mathrm{L},v)^\times) \simeq \bigoplus_{v\in S} H^1(G_v,\mathbb{F}(\mathrm{L},v)^\times)\cdot$$

Let us fix $v\in S$. Let $G_v = \mathrm{Gal}(\mathrm{L}_v/\mathrm{K}_v)$ be the decomposition group in L/K of a place of L above v; put I_v the inertia group I_v associated to G_v. The quotient G_v/I_v corresponds to the Galois group of the local maximal unramified extension $\mathrm{L}_v^{nr}/\mathrm{K}_v$ in $\mathrm{L}_v/\mathrm{K}_v$. The quotient G_v/I_v is isomorphic to the Galois group of the associated residual extensions; as $\mathbb{F}(\mathrm{L},v)$ is isomorphic to the residual field of L_v^{nr}, By Hilbert Theorem 90, one has: $H^1(G_v/I_v,\mathbb{F}(\mathrm{L},v)^\times)=0$. Hence the exact sequence $1\longrightarrow I_v\longrightarrow G_v\longrightarrow G_v/I_v\longrightarrow 1$ induces

$$1\longrightarrow H^1(G_v,\mathbb{F}(\mathrm{L},v)^\times)\longrightarrow H^1(I_v,\mathbb{F}(\mathrm{L},v)^\times)^{G_v/I_v}\longrightarrow\cdots$$

The finite group I_v acts trivially on the cyclic group $\mathbb{F}(\mathrm{L},v)^\times$, then $H^1(I_v,\mathbb{F}(\mathrm{L},v)^\times)$ is cyclic because the ramification of v is tame. To resume,

$$H^1(G,\prod_{v\in S}\mathbb{F}(\mathrm{L},v)^\times) \simeq \bigoplus_{v\in S_{ram}(\mathrm{K})} C_v,$$

where $S_{ram}(\mathrm{K})$ is the set of places of $S(\mathrm{K})$ that are ramified in L/K and where C_v is a cyclic group with $C_v := \ker\Big(H^1(I_v,\mathbb{F}(\mathrm{L},v)^\times)\to H^2(G_v/I_v,\mathbb{F}(\mathrm{L},v)^\times)\Big)$.

For $v_0\in S(\mathrm{k})$, the group Δ acts transitively on $\prod_{v|v_0} C_v$, where the produce is on the places v of K above v_0. Then

$$r_\Delta(H^1(G,\prod_{v\in S}\mathbb{F}(\mathrm{L},v)^\times)[p]) \leq \sum_{v_0\in S_{ram(\mathrm{k})}} r_\Delta(\prod_{v|v_0} C_v[p]) \leq |S_{ram}|,$$

where here $S_{ram}=S_{ram}(\mathrm{k})$ is the subset of places of S $(=S(\mathrm{k}))$ ramified in L/K. Finally

$$r_\Delta(\mathrm{Im}(\beta)) \leq |S_{ram}|. \tag{11}$$

To control $\ker(\beta)$, as before, one uses the estimation of Lemma 6.4 (vi) to obtain $r_\Delta(\ker(\beta)) \leq d_p\Big(\mathrm{coker}\varphi\Big)^G$ and then:

$$d_p\Big(\mathrm{coker}\varphi\Big)^G \leq d_p\mathrm{coker}\varphi \leq d_p\Big(\prod_{v\in S(\mathrm{L})}\mathbb{F}(\mathrm{L},v)^\times\Big) \leq |S(\mathrm{L})| \leq |S||\mathscr{G}|\cdot \tag{12}$$

By using (9), (10), (11), and (12):

$$\begin{aligned} r_\Delta(H^1(G,\mathscr{O}_{\mathrm{L}}^T)[p]) &\leq r_\Delta(H^1(G,B)[p]) + d_p\mathrm{Cl}_S^T(\mathrm{K}) \\ &\leq |S||\mathscr{G}| + |S_{ram}| + d_p\mathrm{Cl}_S^T(\mathrm{K}), \end{aligned}$$

where we put $S = S(\mathrm{k})$ and $S_{ram} = S_{ram}(\mathrm{k})$. Now it suffices to use Dirichlet's unit Theorem 6.1 to obtain:

$$r_\Delta(\mathscr{E}^G) \leq r_\Delta(H^1(G,\mathscr{O}_{\mathrm{L}}^T)[p]) + r_\Delta(\mathbb{F}_p\otimes\mathscr{O}_{\mathrm{K}}^T) \leq |\mathscr{G}||S| + |S_{ram}| + d_p\mathrm{Cl}_S^T(\mathrm{K}) + r_1 + r_2 - 1 + |T|\cdot$$

We finish the proof of Theorem 6.10 thanks to Proposition 6.6 and to the fact that

$$d_p\mathscr{E} = |\mathscr{G}|\Big(\frac{1}{2}r_\infty + d_\infty + |T|\Big) - 1\cdot$$

6.3.2. When $\mathscr{O}_{\mathrm{L}}^T$ contains μ_p. — As for the previous section, let us write the $\mathbb{F}_p[\mathscr{G}]$-module $\mathscr{E} := \mathbb{F}_p\otimes\mathscr{O}_{\mathrm{L}}^T$ as $\mathbb{F}_p[\mathscr{G}]^t\oplus N$, where N is of torsion.

Theorem 6.13. — *Let us consider the same context as for Theorem 6.10, with the exception that* L *contains μ_p. Let us decompose the $\mathbb{F}_p[\mathscr{G}]$-module $\mathscr{E} := \mathbb{F}_p\otimes\mathscr{O}_{\mathrm{L}}^T$ as $\mathbb{F}_p[\mathscr{G}]^t\oplus N$, where N is of torsion. Then*

$$t \geq |T| + d_\infty + \frac{1}{2}r_\infty - (|\mathscr{G}|-1)\Big(r_1+r_2+1-d_\infty-\frac{1}{2}r_\infty + d_p\mathrm{Cl}_S^T(\mathrm{K}) + |\mathscr{G}||S| + |\mathscr{G}||S_{ram}| + d_pH^2(G,\mathbb{F}_p)\Big)\cdot$$

Remark 6.14. — When $\mu_p\subset\mathscr{O}_{\mathrm{L}}^T$, put

$$\mathrm{A} = -\Big[d_\infty + \frac{1}{2}r_\infty - (|\mathscr{G}|-1)\Big(r_1+r_2+1-d_\infty-\frac{1}{2}r_\infty + d_p\mathrm{Cl}_S(\mathrm{K}) + |\mathscr{G}||S| + |\mathscr{G}||S_{ram}| + d_pH^2(G,\mathbb{F}_p)\Big)\Big].$$

As before, we note that $d_p\mathrm{Cl}_S^T(\mathrm{K}) \leq d_p\mathrm{Cl}_S(\mathrm{K})$.

Let us start with the following sequence of G-modules

$$1 \longrightarrow \mathscr{O}_{\mathrm{L}}^T/\mu_p \xrightarrow{p} \mathscr{O}_{\mathrm{L}}^T \longrightarrow \mathscr{E} \longrightarrow 1\ \cdot \tag{13}$$

Then (13) becomes

$$\mathbb{F}_p\otimes\mathscr{O}_{\mathrm{K}}^T \hookrightarrow \mathscr{E}^G \longrightarrow H^1(G,\mathscr{O}_K^T/\mu_p) \longrightarrow \cdots \tag{14}$$

Consider

$$1 \longrightarrow \mu_p \longrightarrow \mathscr{O}_{\mathrm{L}}^T \longrightarrow \mathscr{O}_{\mathrm{L}}^T/\mu_p \longrightarrow 1$$

which gives

$$\cdots \longrightarrow H^1(G,\mu_p) \longrightarrow H^1(G,\mathscr{O}_{\mathrm{L}}^T) \longrightarrow H^1(G,\mathscr{O}_{\mathrm{L}}^T/\mu_p) \longrightarrow H^2(G,\mu_p) \longrightarrow H^2(G,\mathscr{O}_{\mathrm{L}}^T) \longrightarrow \cdots$$

Let us remark here that the p-group G acts trivially on μ_p. Thus for $i=1,2$, the groups $H^i(G,\mu_p)$ describe generators and relations of G.
One then has

$$d_pH^1(G,\mathscr{O}_{\mathrm{L}}^T/\mu_p) \leq d_pH^2(G,\mathbb{F}_p) + d_pH^1(G,\mathscr{O}_{\mathrm{L},S}^T)\cdot$$

and

$$\begin{aligned} r_\Delta(\mathscr{E}^G) &\leq r_\Delta(\mathbb{F}_p\otimes\mathscr{O}_{\mathrm{K}}^T) + d_pH^1(G,\mathscr{O}_{\mathrm{L}}^T/\mu_p) \\ &\leq r_\Delta(\mathbb{F}_p\otimes\mathscr{O}_K^T) + d_pH^1(G,\mathscr{O}_{\mathrm{L}}^T) + d_pH^2(G,\mathbb{F}_p) \\ &\leq r_\Delta(\mathbb{F}_p\otimes\mathscr{O}_K^T) + |\mathscr{G}||S| + |\mathscr{G}||S_{ram}| + d_p\mathrm{Cl}_S^T(\mathrm{K}) + d_pH^2(G,\mathbb{F}_p) \end{aligned}$$

where for the last inequality, one takes the previous computation concerning $H^1(G,\mathscr{O}_{\mathrm{L}}^T)$ to obtain an upper bound for $d_pH^1(G,\mathscr{O}_{\mathrm{L}}^T)$. The conclusion may be deduced from Proposition 6.6.

7. Ramification with prescribed Galois action

7.1. Preparation. —

7.1.1. Kummer Theory. — Our reference here is the book of Gras [**13**], §6, chapter I. Let us start with a Galois extension L/k of Galois group $\mathscr{G}$ and recall some notations.

- Denote by $\chi_p = \mathbb{F}_p(1)$ the cyclotomic character resulting from the action on the pth roots of unity. For a $\mathbb{F}_p[\mathscr{G}]$-module M, put $M(1) = M \otimes_{\mathbb{F}_p} \mathbb{F}_p(1)$.
- Let T be a finite set of primes of $\mathscr{O}_{\mathrm{k}}$ *all of which split completely in* L, and consider

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

- 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:

$$\mathrm{V}^T_{\mathrm{k}} = \{\alpha \in k^\times,\ v_{\mathfrak{P}}(\alpha) \equiv 0 \ (\mathrm{mod} p), \forall \mathscr{O}_L\text{-primes } \mathfrak{P}|\mathfrak{p} \notin T\}\},$$

  and the governing field $\mathrm{F}^T_{\mathrm{k}} := \mathrm{k}(\zeta_p, \sqrt[p]{\mathrm{V}^T_{\mathrm{k}}})$.

Remark 7.1. — One easily see that $\mathbb{F}_p \otimes \mathscr{O}^T_{\mathrm{L}} \hookrightarrow \mathrm{V}^T/(\mathrm{L}^\times)^p$. We will be interested in finding some free sub-$\mathbb{F}_p[\mathscr{G}]$-modules of $\mathrm{V}^T/(\mathrm{L}^\times)^p$: they will appear thanks to control over the group of T-units $\mathbb{F}_p \otimes \mathscr{O}^T_{\mathrm{L}}$ in conjunction with Theorem 6.7.

Put $\mathscr{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$; the group $\mathscr{G}$ acts on $\mathrm{V}^T/(\mathrm{L}^*)^p$ and then on $\mathscr{H}$. Recall that the bilinear form

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

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

$$b(g(x), h) = b(x, g^{-1}(h)^{\chi_p(g)}).$$

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

$$\Theta : \left(\mathrm{V}^T/(\mathrm{L}^\times)^p\right)^*(1) \xrightarrow{\cong} \mathscr{H} \cdot \tag{15}$$

Proposition 7.2. — *If the $\mathbb{F}_p[\mathscr{G}]$-module $\mathbb{F}_p \otimes \mathscr{O}^T_{\mathrm{L}}$ contains a free submodule $\langle\varepsilon\rangle_{\mathscr{G}}$ generated by the unit ε, then $\mathscr{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains, as a direct factor, a free sub-$\mathbb{F}_p[\mathscr{G}]$-module $\mathscr{H}_\varepsilon$ of rank 1, isomorphic to $\left(\langle\varepsilon\rangle_{\mathscr{G}}\right)^*(1)$, the latter being isomorphic to $\mathscr{H}_\varepsilon := \mathrm{Gal}(\mathrm{L}'(\sqrt[p]{\langle\varepsilon\rangle})/\mathrm{L}')$.*

Proof. — As $\langle\varepsilon\rangle_{\mathscr{G}}$ is free, it is a direct factor in $\mathrm{V}^T/(\mathrm{L}^\times)^p$. By passing to the dual, the module $\left(\langle\varepsilon\rangle_{\mathscr{G}}\right)^*(1)$ is free and is in direct factor in $\left(\mathrm{V}^T/(\mathrm{L}^\times)^p\right)^*(1) \overset{\Theta}{\rightsquigarrow} \mathscr{H} = \mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$. Finally by Kummer theory, $\left(\langle\varepsilon\rangle_{\mathscr{G}}\right)^*(1) \simeq \mathscr{H}_\varepsilon$. □

Definition 7.3. — Under the hypothesis of Proposition 7.2, denote by x_ε a generator of the free module $\mathscr{H}_\varepsilon$.

7.1.2. The Theorem of Gras-Munnier. —

Definition 7.4. — Let K be a number field and S a finite set of prime ideals of $\mathscr{O}_{\mathrm{K}}$. We say the extension L/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 L/K.

Let us conserve the notation introduced in the beginning of this section 7.1: $\mathrm{L}' = \mathrm{L}(\zeta_p)$ and $\mathrm{F}^T = \mathrm{L}'(\sqrt[p]{\mathrm{V}^T})$. Let us recall the Theorem of Gras-Munnier (see [**15**], [**13**]) that will be extremely useful to us.

Theorem 7.5 **(Gras-Munnier [15]).** — *Let $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_m\}$ and T be two finite sets of prime ideals of $\mathscr{O}_{\mathrm{L}}$, such that $S \cap T = \emptyset$, and such that for all $\mathfrak{p}_i \in S$, $\mathrm{N}\mathfrak{p}_i \equiv 1 (\bmod p)$. For each $i = 1, \cdots, m$, let $\mathfrak{P}_i$ be a prime of $\mathscr{O}_{\mathrm{L}'}$ 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 $i = 1, \cdots, m$, there exists $a_i \in \mathbb{F}_p^\times$, such that*

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

where $\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\bullet}\Big)$ 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).

7.1.3. 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 7.1.

Definition 7.6. — Let U, S and T be three pairwise disjoint sets of prime ideals of $\mathscr{O}_{\mathrm{L}}$. 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 7.7. — *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. □

Corollary 7.8. — *Suppose that the $\mathbb{F}_p[\mathscr{G}]$-module $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains a free submodule $\mathscr{H}_\varepsilon = \langle x_\varepsilon \rangle_{\mathscr{G}}$ of rank 1. By Chebotarev density Theorem, choose a prime ideal $\mathfrak{p}$ of $\mathscr{O}_{\mathrm{L}}$ such that $\langle \Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big) \rangle = \langle x_\varepsilon \rangle$, where $\mathfrak{P} | \mathfrak{p}$. Then for $U = \{g(\mathfrak{P}) = \mathfrak{P}^g,\ g \in \mathscr{G}\}$, we have $\mathrm{I}^T(U, \mathrm{L}) = \{1\}$.*

Proof. — Let first recall the property of the Artin symbol: for $g \in \mathscr{G}$ and $\mathfrak{P} \subset \mathscr{O}_{\mathrm{L}}$, one has:

$$\Big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}^g}\Big) = g\Big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)g^{-1} = \Big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)^{g^{-1}}.$$

By hypothesis there does not exist a non-trivial relation between the conjugates of $\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)^g$ with $g \in \mathscr{G}$. Then by Theorem 7.5, there exists no T-split, U'-totally ramified, cyclic degree p extension of K, for every non empty set U' of S, meaning that $\mathrm{I}^T(U, \mathrm{L})$ is trivial (thanks to Lemma 7.7 with $S = \emptyset$). $\square$

In fact, we want to say more. For a finite set S, $\mathscr{G}$-stable, of tame ideal primes of $\mathscr{O}_\mathrm{L}$ with $S \cap T = \emptyset$, 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 7.9. — *Suppose that the $\mathbb{F}_p[\mathscr{G}]$-module $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains a free submodule $\mathscr{H}_\varepsilon = \langle x_\varepsilon \rangle_\mathscr{G}$ of rank 1 such that*

$$\mathscr{H}_\varepsilon \bigcap \mathrm{F}(S) = \{0\}\cdot$$

By Chebotarev density Theorem, choose a prime ideal $\mathfrak{p}$ of $\mathscr{O}_\mathrm{L}$ such that $\langle \Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big) \rangle = \langle x_\varepsilon \rangle$, for any $\mathfrak{P}|\mathfrak{p}$. Put $U = \{g(\mathfrak{P}) = \mathfrak{P}^g,\ g \in \mathscr{G}\}$. 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 $\mathbb{F}_p[\mathscr{G}]$-module $\langle \Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big) \rangle_\mathscr{G}$ intersects trivially $\mathrm{F}(S)$, one has thanks to Theorem 7.5 that the extension L_0/L is unramified at U. By Lemma 7.7, one concludes that $\mathrm{I}_S^T(U, \mathrm{L}) = \{1\}$. $\square$

7.2. The set $\mathscr{S}$. — We are now going to give a non free situation that will be used in the proof of Theorem 9.2. It is essential for the definition of the sets $\mathscr{S}$.
Let us start from the existence of a free submodule $\mathbb{F}_p[\mathscr{G}]^{|\mathscr{G}|}$ of $\mathrm{V}^T/(\mathrm{L}^\times)^p$, of rank $|\mathscr{G}|$.
Let $(\varepsilon_g)_g$ be a basis of $\mathbb{F}_p[\mathscr{G}]^{|\mathscr{G}|}$ indexed by the elements of $\mathscr{G}$.
As $\mathbb{F}_p[\mathscr{G}]$ is a Frobenius ring, the free module $\bigoplus_{g \in \mathscr{G}} \mathbb{F}_p[\mathscr{G}]\varepsilon_g$ is a direct factor in $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$; put then

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

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

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

Lemma 7.10. — *The module $\mathbb{F}_p N$ is a sub-$\mathbb{F}_p[\mathscr{G}]$-module of $\mathbb{F}_p[\mathscr{G}]$ generated by N. In other words, $\langle N \rangle_\mathscr{G} = \langle N \rangle$. It is also the only sub-$\mathscr{G}$-module of $\mathbb{F}_p[\mathscr{G}]$ on which $\mathscr{G}$ acts trivially.*

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

$$\sum_{g \in \mathscr{G}} a_g g\Big(\sum_{h \in \mathscr{G}} h\Big) = \sum_{g \in \mathscr{G}} a_g \sum_{h \in \mathscr{G}} gh = \sum_{g \in \mathscr{G}} a_g N \in \mathbb{F}_p N,$$

which proves the first part. Now clearly $\mathscr{G}$ acts trivially on N and moreover if we start with an element $\sum_{g \in \mathscr{G}} a_g g$ on which $\mathscr{G}$ acts trivially, then obviously, a_g is constant (not depending on $g \in \mathscr{G}$). $\square$

Take $\varepsilon_0 \in \mathrm{V}_{\mathrm{k}}^T(\mathrm{L}^\times)^p/(\mathrm{L}^\times)^p$ and write $\varepsilon_0 = \Big(\sum_{g\in\mathscr{G}} y_g\Big) + z$, with $y_g \in \mathbb{F}_p[\mathscr{G}]\varepsilon_g$ and $z \in W$. As $\mathscr{G}$ acts trivially on ε_0, then $\mathscr{G}$ acts trivially on the elements y_g and Lemma 7.10 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 $\mathbb{F}_p[\mathscr{G}]$-modules

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

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

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

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 (15), we get:

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

Put

$$\mathscr{H}' := \Theta\Big(\Big(\bigoplus_{g\in\mathscr{G}} \mathbb{F}_p[\mathscr{G}]\varepsilon_g/\langle N\rangle\Big)^*(1)\Big); \tag{16}$$

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

Let us study more carefully $\mathscr{H}'$. First, by Kummer duality, one has

$$\bigoplus_{g\in\mathscr{G}} \Big(\mathbb{F}_p[\mathscr{G}]\varepsilon_g/\langle \mathrm{N}\rangle\Big)^* \hookrightarrow \bigoplus_{g\in\mathscr{G}} \Big(\mathbb{F}_p[\mathscr{G}]\varepsilon_g\Big)^* \twoheadrightarrow \bigoplus_{g\in\mathscr{G}} \langle N\rangle^*.$$

We will continue to denote by $(\varepsilon_g)_g$ the dual basis of ε_g.

Let us fix an element ε_g. Then $\Big(\mathbb{F}_p[\mathscr{G}]/\langle N\rangle\Big)^* \simeq \{f \in \mathrm{Hom}(\mathbb{F}_p[\mathscr{G}],\mathbb{F}_p),\ f(N)=0\}$, see for example [**8**], §60, chapter IX. Let

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

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

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

and

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

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 $\Big(\mathbb{F}_p[\mathscr{G}]\varepsilon_g\Big)(1)$. In the sum $\bigoplus_{g\in\mathscr{G}} \mathrm{I}\cdot x_g \hookrightarrow \bigoplus_{g\in\mathscr{G}} \mathbb{F}_p[\mathscr{G}]x_g$, let us choose the particular element x defined by

$$x := \Big(\sum_{g\in\mathscr{G}}(g-1)x_g\Big)\cdot \tag{17}$$

Obviously the algebraic norm kills each component $g-1$ of x_g and then $N(x)=0$. In fact:

Lemma 7.11. — *The relation $N(x)=0$ is the unique non trivial relation of x,* i.e *if $\sum_{h\in\mathscr{G}} a_h h\cdot x = 0$ then $a_h = a_e$ for all $h\in\mathscr{G}$. Equivalently,* $\mathrm{Ann}(x) = \mathbb{F}_p N$.

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

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

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

7.3. Some consequences. — Let us start now with x given by Definition (17). Recall that $x\in\bigoplus_{g\in\mathscr{G}}\mathrm{I}x_g$, where $\mathrm{I} = \{f\in\mathrm{Hom}(\mathbb{F}_p[\mathscr{G}],\mathbb{F}_p), f(N)=0\}$.

Put $x_0 = \Theta(x)\in\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$, where Θ is the isomorphism coming from Kummer theory, see (15). The element x_0 is in $\mathscr{H}'$ 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 $\mathscr{O}_\mathrm{L}$ which splits totally in L/k and such that $\langle\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)\rangle = \langle x_0\rangle$.

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

Remark 7.12. — When $S=\emptyset$ and $s=1$, in the main theorems (Theorems A and B) the set $\mathscr{S}$ considered is composed of such prime ideals. The set $\mathscr{S}$ is of positive density. This density depends on the discriminant of $\mathrm{F}^T/\mathbb{Q}$ and on the size of $\mathrm{Gal}(\mathrm{F}^T/\mathbb{Q})$. The discriminant of $\mathrm{L}'/\mathbb{Q}$ is related to the number field K; the discriminant of F^T/L' depends on the wild ramification in F^T/L' and on the tame ramification at T; and the size of $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ depends the p-class group of K, on the signature of K and on the size of $|T|$.

Proposition 7.13. — *With the previous notations and conditions (especially the choice of $\mathfrak{P}$), we get the isomorphism of $\mathscr{G}$-modules:* $\mathrm{I}^T(U,\mathrm{L})\simeq\mathrm{I}^T(U,\mathrm{k})\simeq\mathbb{F}_p$.

Proof. — Suppose that there exists a non-trivial relation between the conjuguates $\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)^g$, $g\in\mathscr{G}$, of $\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)$: $\Big(\sum_{g\in\mathscr{G}} a_g g\Big)\cdot\Big(\dfrac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\Big)=0$, with $a_{g_0}\neq 0$ for at least one

$g_0 \in \mathscr{G}$. Then, as $\langle\big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\big)\rangle = \langle x_0\rangle$, by Lemma 7.11, one gets $a_g = a_{g_0} \neq 0$ for all $g \in \mathscr{G}$. Thus by Theorem 7.5, 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 $\mathfrak{P}_0^g$, $g \in \mathscr{G}$. That means that $d_p\mathrm{I}^T(U) \leq 1$ (it is an easy generalization of Lemma 7.7).
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 $\big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\big) \in \langle x_0\rangle \subset \mathscr{H}'$ and consequently, $\big(\frac{\mathrm{L}'\mathrm{F}_\mathrm{k}^T/\mathrm{L}'}{\mathfrak{P}}\big) = 1$. By the properties of the Artin symbol, one gets

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

where $\Big(\frac{\mathrm{F}_\mathrm{k}^T/\mathrm{k}'}{\mathrm{N}_{\mathrm{L}'/\mathrm{k}'}(\mathfrak{P})}\Big) = 1$. We then remark that $\mathrm{N}_{\mathrm{L}'/\mathrm{k}'}(\mathfrak{P})$ is a prime ideal of $\mathscr{O}_\mathrm{k}$ above $\mathfrak{p}$. By Theorem 7.5, it proves the existence of a T-split, $\{\mathfrak{p}_\mathrm{k}\}$-totally ramified, degree p cyclic extension of k. Then, $\mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{F}_p$ as $\mathscr{G}$-modules. But one still has $\mathrm{I}^T(U,\mathrm{L}) \twoheadrightarrow_{\mathscr{G}} \mathrm{I}^T(U,\mathrm{k})$, because $\mathfrak{p}_\mathrm{k}$ splits totally in L/k. By comparing the p-rank, one finally obtains: $\mathrm{I}^T(U,\mathrm{L}) \simeq \mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{F}_p$. □

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

Proposition 7.14. — *Suppose that the* $\mathbb{F}_p[\mathscr{G}]$*-module* $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ *contains a free submodule* $\mathscr{H}'$ *of rank* $|\mathscr{G}|$ *with basis* $(x_g)_{g\in\mathscr{G}}$. *Put* $x_0 = \sum_{g\in\mathscr{G}}(g-1)x_g \in \mathscr{H}'$. *By Chebotarev density Theorem, take a prime ideal* $\mathfrak{P}$ *of* $\mathscr{O}_\mathrm{L}$ *such that* $\langle\big(\frac{\mathrm{F}^T/\mathrm{L}'}{\mathfrak{P}}\big)\rangle = \langle x_0\rangle$. *Suppose moreover that*

$$\mathscr{H}' \bigcap \mathrm{F}(S) = \{0\},$$

where $\mathrm{F}(S)$ *is the subgroup of* $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ *generated by the Frobenius of a* $\mathscr{G}$*-stable set* S *of ideals of* $\mathscr{O}_\mathrm{L}$. *Then, as* $\mathscr{G}$*-modules,* $\mathrm{I}_S^T(U,\mathrm{L}) \simeq \mathrm{I}_S^T(U,\mathrm{k}) \simeq \mathrm{I}^T(U,\mathrm{k}) \simeq \mathbb{F}_p$*, where* $U = \{\mathfrak{P}^g,\ g\in\mathscr{G}\}$. *Moreover* $\mathrm{I}_S^T(U,\mathrm{L}) \cap \mathrm{I}_U^T(S,\mathrm{L}) = \{e\}$.

Proof. — As $x_0 \in \mathscr{H}'$, the module $\langle x_0\rangle_{\mathscr{G}}$ intersects $\mathrm{F}(S)$ trivially. As for Proposition 7.13, 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 $\mathfrak{P}_0^g$, $g \in \mathscr{G}$. Hence, $d_p\mathrm{I}_S^T(U,\mathrm{L}) \leq 1$. But by Proposition 7.13, 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 $\mathrm{I}_S^T(U,\mathrm{L}) \simeq_{\mathscr{G}} \mathbb{F}_p$.
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 $\mathrm{I}^T(U,\mathrm{L}) \simeq \mathbb{F}_p$. □

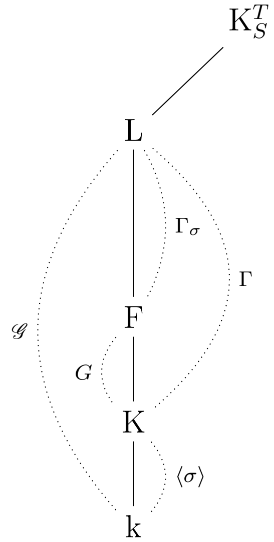
Remark 7.15. — The main question it to find an element x in $\big(\mathrm{V}^T/(\mathrm{L}^\times)^p\big)^*$ such that $\mathrm{Ann}(x) = \mathbb{F}_pN$. In some cases, one can find a such element in a free module of rank 1. Typically if $\mathscr{G} = \langle x\rangle$ is cyclic, it suffices to take $x = g-1$. Or, in the semisimple case, *i.e.* when the order of $\mathscr{G}$ is coprime to p, take $x = \sum_{g\in\mathscr{G}}(g-1)$.

PART III
PROOF OF THE MAIN RESULTS

8. The strategy

8.1. — Let L/K/k be a σ-uniform tower; put $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, $\mathscr{G} = \mathrm{Gal}(\mathrm{L}/\mathrm{k})$ 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 $x_1, \cdots, x_n \in \Gamma$ be some lifts of some generators of $\Gamma^{p,\mathrm{el}}$ respecting the action of σ (see §4.2). We fix $x_1 \cdots, x_r$ the lifts of the fixed points. Hence, by Proposition 4.6, $\Gamma_\sigma^\circ = \langle x_1, \cdots, x_r\rangle$, the pro-$p$ group Γ_σ is topologically generated by the conjuguates $x_i^g, i = 1, \cdots, r$, $g \in \mathrm{G} := \Gamma/\Gamma_\sigma$ of the x_i. Moreover by proposition 4.12, $\Gamma_\sigma^{p,el}$ is minimaly generated as $\mathbb{F}_p[[G]]$-module by the family $\{x_1\Phi(\Gamma_\sigma), \cdots, x_r\Phi(\Gamma_\sigma)\}$.

8.2. — 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 and Γ are FAb. Put $\mathrm{F} := \mathrm{L}^{\Gamma_\sigma}$ and $\mathrm{G} := \mathrm{Gal}(\mathrm{F}/\mathrm{K})$. 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 $x_1 \cdots, x_r$ are in Γ, they can be lifted to G_S^T. In fact, by construction, the elements $x_1 \cdots, x_r$ are in $\mathrm{G}_S^T(\mathrm{F})$ and by Proposition 4.12, their classes generate $\Gamma_\sigma^{p,el}$ as $\mathbb{F}_p[\mathrm{G}]$-modules. Put $\mathrm{M} := \langle \mathrm{G} \cdot x_i\Phi(\mathrm{G}_S^T(\mathrm{F})),\ i = 1, \cdots, r\rangle \subset \Big(\mathrm{G}_S(\mathrm{F})\Big)^{p,\mathrm{el}}$.

Proposition 8.1. — *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.*

9. Proof of Theorem B

Let us start with a notation. For a finitely generated pro-p-group G, denote by $(G_n)_n$ the central series of G: $G_0 = G$, and for $n \geq 0$, $G_{n+1} = [G_n, G_n]$. Put $G^n = G/G_n$.

Definition 9.1. — Let $n \geq 1$. Denote by $\mathrm{K}_S^{(n)}$ the subfield of K_S fixed by $(\mathrm{G}_S)_n$, whose Galois group over K is thus G_S^n. It is also the nth step of the p-tower K_S/K of K, unramified outside S.

Recall the integer $m(\ell)$ defined in (1): it is an upper bound of the solvability length of the quotient $G := \Gamma/\Gamma_\sigma$. See also remark 4.11.

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

***Theorem 9.2* (Theorem B)**. — *Let* K *be a number field equipped with an automorphism* σ *of order* $\ell \mid (p-1)$*; put* $\mathrm{k} = \mathrm{K}^\sigma$*. Suppose that there exists a finite set* S *of tame primes of* $\mathscr{O}_\mathrm{k}$ *such that the action of* σ *on* G_S^{ab} *is fixed point free. Fix* $s \in \mathbb{Z}_{>0}$*.*
Let T *be a finite set of prime ideals of* $\mathscr{O}_\mathrm{k}$ *that totally split in* $\mathrm{K}_S^{(m(\ell))}/\mathrm{k}$ *and such that* $|T| \geq \mathrm{A} + s|\mathscr{G}|(|S||\mathscr{G}|+1)$*, where* $\mathrm{A} = \mathrm{A}(\mathrm{K}_S^{(m(\ell))}/\mathrm{K})$ *(see remarks 6.11 and 6.14). Then there exists* s *sets* $\mathscr{S}_1, \cdots, \mathscr{S}_s$*, of ideal primes of* $\mathscr{O}_\mathrm{k}$*, all of positive density, such that for* $\Sigma = S \cup S'$ *with* $S' = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$*, where* $\mathfrak{p}_i \in \mathscr{S}_i$*,* $i = 1, \cdots, s$*, one has:*

- (i) $(\mathrm{G}_\Sigma^T)^{p,\mathrm{el}} \simeq_{\mathscr{G}} (\mathrm{G}_S)^{p,\mathrm{el}} \bigoplus (\mathbb{F}_p)^{\oplus s}$*;*
- (ii) *there is no continuous Galois representation* $\rho : \mathrm{G}_\Sigma^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ *which is fixed-point-mixing modulo Frattini and* Γ_σ *is supported at* S'*, where* Γ *is the image of* ρ*.*

Proof. — The proof is a combination of the previous results. First, the extension $\mathrm{K}^{(m(\ell))}/\mathrm{k}$ is a Galois extension. Put $\mathrm{L}_0 = \mathrm{K}_S^{(m(\ell))}$ and $\mathscr{G} = \mathrm{Gal}(\mathrm{L}_0/\mathrm{k})$. Consider the $\mathbb{F}_p[\mathscr{G}]$-module $\mathbb{F}_p \otimes \mathscr{O}_{\mathrm{L}_0}^T$ and let $\mathbb{F}_p[\mathscr{G}]^t \oplus N$ be its decomposition as $\mathbb{F}_p[\mathscr{G}]$-modules where N is of torsion (see §6.2.2). Thanks to Theorem 6.7, as T is sufficiently large, one gets $t \geq s|\mathscr{G}|(|S||\mathscr{G}|+1)$.

Let us conserve the notations of §7.1. Let $\mathrm{F}(S)$ be the sub-$\mathbb{F}_p[\mathscr{G}]$-module of $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ generated by the Frobenius of the prime ideals of S (see §7.1.3).

Lemma 9.3. — *Suppose that* $t \geq s|\mathscr{G}|(|S||\mathscr{G}|+1)$*. Then there exists* $s|\mathscr{G}|$ T*-units* $\varepsilon_g^i \in \mathscr{O}_{\mathrm{L}_0}^T$*,* $g \in \mathscr{G}$*,* $i = 1, \cdots, s$*, such that*

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

$$\sum_{i=1}^{s} \sum_{g \in \mathscr{G}} \mathbb{F}_p[\mathscr{G}]\varepsilon_g^i = \bigoplus_{i=1}^{s} \Big(\sum_{g \in \mathscr{G}} \mathbb{F}_p[\mathscr{G}]\varepsilon_g^i \Big);$$

(iii) *following the notations of Section 7.1, for* $i = 1, \cdots, s$,

$$\Theta\Big(\Big(\sum_{g\in\mathscr{G}} \mathbb{F}_p[\mathscr{G}]\varepsilon_g^i\Big)^*(1)\Big) \cap \mathrm{F}(S) = \{0\}.$$

Proof. — Let us start with $\mathbb{F}_p \otimes \mathscr{O}_{\mathrm{L}_0}^T \simeq \mathbb{F}_p[\mathscr{G}]^t \oplus N$. By Kummer duality, $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$ contains $\mathbb{F}_p[\mathscr{G}]^t$ in direct factor, the free modules coming from the image of the dual of T-units by Θ (see §7.2). As $d_p\mathrm{F}(S) \leq |S||\mathscr{G}|$, the $\mathbb{F}_p[\mathscr{G}]$-module $\mathrm{F}(S)$ intersects at most $|S||\mathscr{G}|$ modules each one isomorphic to $\mathbb{F}_p[\mathscr{G}]^{s|\mathscr{G}|}$. Hence as $t \geq s|\mathscr{G}|(|S||\mathscr{G}|+1)$, there exists at least one module isomorphic to $\mathbb{F}_p[\mathscr{G}]^{s|\mathscr{G}|}$ that does not intersect $\mathrm{F}(S)$, in other words, there exists $s|\mathscr{G}|$ free submodules M_i of $\mathrm{Gal}(\mathrm{F}^T/\mathrm{L}')$, $i = 1, \cdots, s|\mathscr{G}|$, all in direct factors, such that $\mathrm{F}(S) \cap \Big(\sum_i \mathrm{M}_i\Big) = \{0\}$. Then the T-units given by $\Theta^{-1}(\mathrm{M}_i)$ satisfy (i), (ii) and (iii) of the Lemma. □

Let us adapt the Proposition 7.14 in our context. For $i = 1, \cdots, s$, let $\mathscr{H}^i$ be the free $\mathbb{F}_p[\mathscr{G}]$-modules of basis $\{x_g^i,\ g \in \mathscr{G}\}$. Recall that these modules are obtained by Kummer duality from the T-units of Lemma 9.3. Put also $x_0^i := \sum_{g\in\mathscr{G}}(g-1)x_g^i \in \mathscr{H}'$. By Chebotarev density Theorem, let $\mathscr{S}_i$ be the set of prime ideals $\mathfrak{p}$ of $\mathscr{O}_{\mathrm{K}}$, such that the (class of) Frobenius of $\mathfrak{p}$ in F^T/k corresponds to x_0^i: the $\mathscr{S}_i$ is of positive density.

Then consider $S' = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ a set of prime ideals of $\mathscr{O}_{\mathrm{k}}$, with $\mathfrak{p}_i \in \mathscr{S}_i$; put $\Sigma = S \cup S'$.

For $i = 1, \cdots, s$, choose a prime ideal $\mathfrak{P}_i|\mathfrak{p}_i$ of $\mathscr{O}_{\mathrm{L}_0}$ above $\mathfrak{p}_i$. Put $U_i = \{\mathfrak{P}_i^g, g \in \mathrm{G}\}$.

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

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

here, we drop U_i.

Lemma 9.4. — (i) *Let* R'/k *be a Galois subextension of* L_0/k *of Galois group* G'. *Then as* $\mathbb{F}_p[G']$*-modules:*

$$\mathrm{I}_S^T(S', \mathrm{R}') \simeq \bigoplus_{i=1}^s \mathrm{I}_{S_i}^T(U_i, \mathrm{R}') \simeq \Big(\mathbb{F}_p\Big)^{\oplus s}.$$

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

$$\Big(\mathrm{G}_\Sigma^T(\mathrm{K})\Big)^{p,\mathrm{el}} \simeq_{\mathscr{G}} \Big(\mathrm{G}_S^T(\mathrm{K})\Big)^{p,\mathrm{el}} \bigoplus \Big(\mathbb{F}_p\Big)^{\oplus s} \simeq_{\mathscr{G}} \Big(\mathrm{G}_S(\mathrm{K})\Big)^{p,\mathrm{el}} \bigoplus \Big(\mathbb{F}_p\Big)^{\oplus s}.$$

Proof. — (i) First, take $R' = \mathrm{L}_0$ and fix i. By Lemma 9.3, $\mathscr{H}_i \cap \mathrm{F}(S_i) = \{0\}$. The proposition 7.14 applied to U_i and to S_i allows us to get: $\mathrm{I}_{S_i}^T(U_i, \mathrm{L}_0) \simeq \mathrm{I}_{S_i}^T(U_i, \mathrm{K}) \simeq \mathrm{I}^T(U_i, \mathrm{k}) \simeq \mathbb{F}_p$ and $\mathrm{I}_{S_i}^T(U_i, \mathrm{L}_0) \cap \mathrm{I}_{U_i}^T(S_i, \mathrm{L}_0) = \{1\}$. Hence when i varies, the groups $\mathrm{I}_{S_i}^T(U_i, \mathrm{L}_0)$ are in direct factors in $\Big(\mathrm{G}_\Sigma^T(\mathrm{L}_0)\Big)^{p,\mathrm{el}}$.

Take now R' in L_0/k. As L_0 is S'-ramified, one has $\mathrm{I}_S^T(S', \mathrm{L}_0) \twoheadrightarrow \mathrm{I}_S^T(S', \mathrm{R}') \twoheadrightarrow \mathrm{I}_S^T(S', \mathrm{k})$ and one concludes thanks to $\mathrm{I}_S^T(S', \mathrm{L}_0) \simeq \mathrm{I}_S^T(S', \mathrm{k})$.

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

$$1 \longrightarrow \bigoplus_{i=1}^s \mathrm{I}_{S_i}^T(U_i, \mathrm{K}) \longrightarrow \Big(\mathrm{G}_\Sigma^T(\mathrm{K})\Big)^{p,\mathrm{el}} \longrightarrow \Big(\mathrm{G}_S^T(\mathrm{K})\Big)^{p,\mathrm{el}} \longrightarrow 1\cdot$$

and by the choice of T: $\Big(\mathrm{G}_S^T(\mathrm{K})\Big)^{p,\mathrm{el}} \simeq \Big(\mathrm{G}_S(\mathrm{K})\Big)^{p,\mathrm{el}}$. □

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

As $(\mathrm{G}_\Sigma^T(\mathrm{K}))^{p,\mathrm{el}} \twoheadrightarrow \Gamma^{p,\mathrm{el}}$, the action of σ on $\Gamma^{p,\mathrm{el}}$ has at most s "fixed points". Moreover by Boston [**4**] and [**5**], 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 $r = \dim_{\mathbb{F}_p}(\Gamma^{p,\mathrm{el}})_\sigma$. Denote by $x_1, \cdots, x_n \in \Gamma$ the element of Γ that respect the action of σ, with the choice: $\sigma(x_i) = x_i$, for $i = 1, \cdots, r$ (see section 4.2).
By Lemma 4.6 and Proposition 4.12, one knows that Γ_σ is topologically generated by the G-conjuguates of the x_i, $i = 1, \cdots, r$, where $\mathrm{G} := \Gamma/\Gamma_\sigma$. It is the notion of fixed-point-mixing modulo Frattini that will give us some information about the x_i, $i = 1, \cdots, r$.

For $i = 1, \cdots, s$, and $\mathfrak{p}_i \in S'$, let y_i be a generator of the inertia group $I_{\mathfrak{p}_i}$ of a ideal prime $\mathfrak{p}_i$ in L_0: $I_{\mathfrak{p}_i} = \langle y_i \rangle$.

It is clear that $I_{\mathfrak{p}_i}$ intersects non trivially Γ_σ. The fixed-point-mixing modulo Frattini impose then

$$\langle y_1, \cdots, y_s \rangle^{\mathrm{Norm}} = \Gamma_\sigma.$$

In particular

(i) if we note by F the subfield of L fixed by Γ_σ, then the extension F/K is unramified at S', $\mathrm{F} \subset \mathrm{K}_S^T$ and $\mathrm{G}_S^T(\mathrm{K}) \twoheadrightarrow \mathrm{Gal}(\mathrm{F}/\mathrm{K})$;
(ii) the pro-p group Γ_σ is generated by the G-conjuguates of the y_i, $i = 1, \cdots, s$.

On the other hand, the action of σ on $G = \Gamma/\Gamma_\sigma$ is fixed point free, hence G is nilpotent of length at most $n(\ell)$ (see remark 4.11). Consequently, we get: $\mathrm{F} \subset (\mathrm{K}_S^T)^{(m(\ell))} = \mathrm{K}_S^{(m(\ell))} = \mathrm{L}_0$ by the choice of T.

By Lemma 9.4, the $\mathbb{F}_p$-vector space $\mathrm{I}_S^T(S', \mathrm{F})$ is of dimension s and the action of $G := \mathrm{Gal}(\mathrm{F}/\mathrm{K})$ on it is trivial: indeed, $\mathrm{I}_S^T(S', \mathrm{F}) \simeq_{\mathscr{G}} (\mathbb{F}_p)^{\oplus^s}$. But, by Proposition 8.1 and by the condition above the ramification at the prime ideals $\mathfrak{p}_i \in S'$, $\mathrm{I}_S^T(S', \mathrm{F}) \twoheadrightarrow (\Gamma_\sigma)^{p,\mathrm{el}}$ 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 $(\Gamma_\sigma)^{p,\mathrm{el}}$! $\square$

10. Applications

10.1. When σ is of order 2. — Theorem A gives a context where the condition about the ramification is automatically satisfied. Lets us give a proof.

We still conserve the main notations of Theorem 9.2: let K/k be a quadratic extension; put $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = \langle \sigma \rangle$. Let S be a finite set of ideal primes of $\mathscr{O}_\mathrm{k}$ such that $p \nmid |\mathrm{Cl}_S(\mathrm{k})|$. Let $S' = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ be a finite set of prime ideals of $\mathscr{O}_\mathrm{k}$ such that

$$(\mathrm{G}_\Sigma(\mathrm{K}))^{p,\mathrm{el}} \simeq (\mathrm{G}_S(\mathrm{K}))^{p,\mathrm{el}} \bigoplus (\mathbb{F}_p)^{\oplus^s},$$

where $\Sigma = S \cup S'$, with a slight abuse of notation. Let $\mathrm{I}(S')$ be the subgroup of $\mathrm{G}_\Sigma^{ab}(\mathrm{K})$ generated by the inertia groups of the primes in S'. One then has $1 \longrightarrow \mathrm{I}(S') \longrightarrow \mathrm{G}_\Sigma^{ab}(\mathrm{K}) \longrightarrow \mathrm{G}_S^{ab}(\mathrm{K}) \longrightarrow 1$.

Take a minimal set of generators $\{x_1, \cdots, x_s, y_1, \cdots, y_t\}$ of $\mathrm{G}_\Sigma^{ab} = \mathrm{G}_\Sigma^{ab}(\mathrm{K})$ as follows: the elements $x_1, \cdots, x_s$ satisfy $\sigma(x_i) = x_i^{-1}$ and the elements $y_1, \cdots, y_t$ satisfy $\sigma(y_i) = y_i$ (see for example [**19**], Theorem 2.3).

Lemma 10.1. — *Under the conditions of this section, one has* $\mathrm{I}(S') = \langle y_1, \cdots, y_t\rangle$.

Proof. — As $\mathrm{I}(S')\left(\mathrm{G}_\Sigma^{ab}\right)^p/\left(\mathrm{G}_\Sigma^{ab}\right)^p \simeq \ker\left(\mathrm{G}_\Sigma^{p,\mathrm{el}} \to \mathrm{G}_S^{p,\mathrm{el}}\right)$,

$$t = d_p\left[\mathrm{I}(S')\left(\mathrm{G}_\Sigma^{ab}\right)^p/\left(\mathrm{G}_\Sigma^{ab}\right)^p\right] \leq d_p\mathrm{I}(S') \leq |S'| = t,$$

hence, $d_p\mathrm{I}(S') = |S'|$.

As σ acts by -1 on G_S^{ab}, we get $\langle y_1, \cdots, y_t\rangle \subset \mathrm{I}(S')$. Suppose $\langle y_1, \cdots, y_t\rangle \subsetneq \mathrm{I}(S')$. Put $x \in \mathrm{I}(S')\backslash\langle y_1, \cdots, y_t\rangle$. Then there exists $y \in \langle y_1, \cdots, y_t\rangle$ such that $xy \in \langle x_1, \cdots, x_s\rangle$ with $xy \neq e$. As $\mathrm{G}_\Sigma^{ab} = \langle y_1, \cdots, y_t\rangle \oplus \langle x_1, \cdots, x_s\rangle$, one gets $d_p\mathrm{I}(S') \geq d_p\langle y_1, \cdots, y_t\rangle + 1$, and so a contradiction. □

Let $\mathrm{L}/\mathrm{K}/\mathrm{k}$ be a σ-uniform tower in $\mathrm{K}_\Sigma/\mathrm{k}$. Put $\mathrm{F} := \mathrm{L}^{\Gamma_\sigma}$.
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_Σ^{ab}.

Lemma 10.2. — *The extension* F/K *is* S*-ramified. Moreover,* $\mathrm{F} = \mathrm{L} \cap \mathrm{K}_S^{ab}$.

Proof. — By Lemma 10.1, the involution σ acts trivially on $\mathrm{I}(S')$. As σ acts without non-trivial fixed point fixed on $G = \Gamma/\Gamma_\sigma$ and that $G_\Sigma^{ab} \overset{\theta}{\twoheadrightarrow} G$, one then gets $\theta(\mathrm{I}(S')) = \{1\}$, meaning exactly that F/K is S-ramified, *i.e.* $\mathrm{F} \subset \mathrm{K}_S^{ab}$. Put $\mathrm{F}_1 = \mathrm{L} \cap \mathrm{K}_S^{ab}$. Obviously, $\mathrm{F} \subset \mathrm{F}_1$. As σ acts by -1 on $\mathrm{Cl}_S(\mathrm{K})$, σ acts by -1 on $\mathrm{Gal}(\mathrm{F}_1/\mathrm{F})$: indeed if not, $\mathrm{Gal}(\mathrm{K}_S^{ab}/\mathrm{F})$ would have a fixed point (see the proof of Proposition 3.5). 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 4.12, 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 $\mathrm{F}_1 = \mathrm{F}$. □

Remark 10.3. — Lemma 10.2 shows that the inertia groups of the prime ideals $\mathfrak{p} \in S_0$ are in Γ_σ.

Proposition 10.4. — *Let us conserve the notations and the conditions of this section. By Chebotarev density Theorem, choose a finite set* T *of prime ideals of* $\mathscr{O}_\mathrm{k}$*, disjoint from* S*, such that:*

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

Let $\rho : \mathrm{G}_\Sigma^T \to \mathrm{Gl}_m(\mathbb{Q}_p)$ *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 $\mathrm{L}/\mathrm{K}/\mathrm{k}$ is in $\mathrm{K}_\Sigma^T/\mathrm{k}$ and then in $\mathrm{K}_\Sigma/\mathrm{k}$: one can apply Lemma 10.2 to this situation. By Lemma 10.2 the inertia groups of $\mathfrak{p} \in S'$ are in Γ_σ. Denote by L_1 the subfield of L fixed by these inertia groups: the extension L_1/F is T-split and S-ramified. Suppose that L_1/F is not trivial. Then one can assume that L_1/F is of degree p. Then by Lemma 10.2, we get that $\mathrm{L}_1\mathrm{K}_S^{ab}/\mathrm{K}_S^{ab}$ is T-split and S-ramified, cyclic degree p extension. But by hypothesis $\mathrm{Cl}_S^T(\mathrm{K}_S^{ab})$ is trivial, and then, by class field theory, one obtains a contradiction. □

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

- Theorem A can be deduced from Theorem 9.2 and from Proposition 10.4.
- Theorem of the subsection 1.2 comes from the fact that every involution σ on $\mathrm{Sl}_2^1(\mathbb{Z}_p)$ is of type $t_\sigma(\Gamma) = (1, b)$ and then is fixed-point-mixing modulo Frattini by Proposition 5.1. (Here T sufficiently large means also that $\mathrm{Cl}^T(\mathrm{K}^H))$ is trivial.)
- Corollary 2.6 comes from the fact that the action of σ on Γ should be trivial. Thus $\mathrm{Im}(\rho)$ comes from k by compositum and then it suffices to remark that $d_p\mathrm{Cl}_S(\mathrm{k}) \leq |S|$. (Here, as previous, T sufficiently large means also that $\mathrm{Cl}^T(\mathrm{K}^H))$ is trivial.)
- Corollary 2.7 can be deduced from Theorem A and Proposition 5.4.

10.2. Along a $\mathbb{Z}_p$-extension. — The context of the cyclotomic $\mathbb{Z}_p$-extension allows one to take T as small as possible.

10.2.1. When $\ell = 2$. — Take $p > 2$. Let K/k be a quadratic extension such that:

(i) K is totally real. Put $r_1 = [\mathrm{k} : \mathbb{Q}]$;
(ii) the p-class group along the $\mathbb{Z}_p$-cyclotomic extension of k is trivial;
(iii) the number field K satisfies the Greenberg's conjecture.

For $n \geq 0$, put K_n (resp. k_n) for the nth steps of the $\mathbb{Z}_p$-cyclotomic extension K_∞ of K (resp. of k): $[\mathrm{K}_n : \mathrm{K}] = [\mathrm{k}_n : \mathrm{k}] = p^n$.

We are going to apply Theorem A to the σ-uniform extensions of $\mathrm{K}_n/\mathrm{k}_n$.

Take n_0 sufficiently large such that

- for all $n \geq n_0$, $\mathrm{Cl}(\mathrm{K}_{n+1}) \simeq \mathrm{Cl}(\mathrm{K}_n)$, which is always possible by condition (iii);
- all prime ideals above p are totally ramified in $\mathrm{k}_\infty/\mathrm{k}_{n_0}$.

Let us fix $s \in \mathbb{Z}_{>0}$.

Put $\mathrm{C}_0 \simeq \mathrm{Cl}(\mathrm{K}_n)$ and $\mathrm{C} := \mathrm{Gal}(\mathrm{L}_{n+1}/\mathrm{k}_n) \simeq \Big(\mathrm{C}_0 \times \mathbb{Z}/p\mathbb{Z}\Big) \rtimes \langle\sigma\rangle$. Let us apply the strategy developped in part II in order to find free $\mathbb{F}_p[\mathrm{C}]$-modules in $\mathscr{O}_{\mathrm{L}_n}^\times/(\mathscr{O}_{\mathrm{L}_n}^\times)^p$. Let us write $\mathscr{O}_{\mathrm{L}_n}^\times/(\mathscr{O}_{\mathrm{L}_n}^\times)^p = \mathbb{F}_p[\mathrm{C}]^{t_n} \oplus N_n$, with N_n of torsion. Following Theorem 6.10, we get $t_n \geq r_1 p^n - (|\mathrm{C}| - 1)d_p C - 1$. Hence for large n, we are guarantee that $t_n \geq s|\mathrm{C}|$, and then the method developed in the proof of Theorem 9.2 can apply with $T = \emptyset$! Hence, there exists s set $\mathscr{S}_i$, $i = 1, \ldots, s$ of prime ideals of $\mathscr{O}_{\mathrm{k}_n}$, all of positive density, such that for all set $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, one gets:

$$\Big(\mathrm{G}_S(\mathrm{K}_{n+1})\Big)^{p,\mathrm{el}} \simeq \Big(\mathrm{G}_S(\mathrm{K}_n)\Big)^{p,\mathrm{el}} \simeq \mathrm{C}_0/p \bigoplus \Big(\mathbb{F}_p\Big)^{\oplus^s}.$$

Consequently the groups $(\mathrm{G}_S(\mathrm{K}_n)^{p,\mathrm{el}})_n$ stabilize in two consecutive steps: by a classical argument in Iwasawa theory (see for example [**11**], theorem 1), one obtains that for $n \geq m$, with m sufficiently large: $\mathrm{G}_S(\mathrm{K}_n)^{p,\mathrm{el}} \simeq \mathrm{C}_0/p \oplus \Big(\mathbb{F}_p\Big)^{\oplus^s}$. Applying the strategy of the proof of Theorem A, one obtains the following corollary:

***Corollary 10.5* (Theorem C).** — *Under the conditions of this section, for sufficiently large $m \in \mathbb{Z}_{>0}$, there exists s set $\mathscr{S}_i$, $i = 1, \cdots, s$, of prime ideals of $\mathscr{O}_{\mathrm{k}_m}$, all of positive density, such that for all set $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, and for all $n \geq m$, one has:*

(i) $\Big(\mathrm{G}_S(\mathrm{K}_n)\Big)^{p,\mathrm{el}} \simeq \mathrm{C}_0/p \oplus \Big(\mathbb{F}_p\Big)^{\oplus^s}$ *;*
(ii) *the non existence of continuous representation $\rho : \mathrm{G}_S(\mathrm{K}_n) \to \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image fixed-point-mixing modulo Frattini and Γ_σ supported at S.*

One can say more. Indeed, let us choose moreover a set T of prime ideals of k_m, such that

- each ideal prime of T splits totally in $\mathrm{K}^{(1)}_{m+1}/\mathrm{k}_m$;
- $\mathrm{Cl}^T(\mathrm{K}^{(1)}_{m+1})$ is trivial.

Then, $\mathrm{Cl}^T(\mathrm{K}^{(1)}_n)$ is trivial for all $n \geq m$. Proposition 10.4 shows that the ramification will be supported by the fixed points.

Corollary 10.6. — *With the conditions and notations of this section, for m sufficiently large, there exists s sets $\mathscr{S}_i$, $i=1,\cdots,s$, of prime ideals of $\mathscr{O}_{\mathrm{k}_m}$, all of positive density, such that for all set $S=\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, and for all $n \geq m$, one gets:*

(i) $\left(\mathrm{G}^T_S(\mathrm{K}_n)\right)^{p,\mathrm{el}} \simeq \mathrm{C}_0/p \bigoplus \left(\mathbb{F}_p\right)^{\oplus^s}$;
(ii) *the non existence of continuous representation $\rho : \mathrm{G}^T_S(\mathrm{K}_n) \rightarrow \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image fixed-point-mixing modulo Frattini.*

To conclude this section, let us give an example.
Take $p=3$ and $\mathrm{K}=\mathbb{Q}(\sqrt{32009})$.
Let $\mathrm{K}_\infty = \bigcup_n \mathrm{K}_n$ be the $\mathbb{Z}_p$- cyclotomic extension of K. Put $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle\sigma\rangle$. A computation with Pari-GP [**1**] shows that for all $n \geq 1$, $\mathrm{Cl}(\mathrm{K}_n) \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Following Theorem 6.7, remark 6.11 and Theorem 9.2, take n such that

$$r_1 3^n - (|C|-1)d_3C - 1 \geq s|C|,$$

where $|C| = 2\times 3^4$, $r_1 = 2$ and where s is the number of fixed points that we want to introduce. Hence $n \geq n_0 = \lceil \log_3(2+s)+4 \rceil$ holds. If moreover we take a set T of ideal primes of $\mathscr{O}_{\mathrm{k}_{n_0}}$ all totally splits in $\mathrm{K}^H_{n_0+1}/\mathbb{Q}_{n_0}$ and such that $\mathrm{Cl}^T(\mathrm{K}_{n_0+1})$ is trivial, one then gets:

Corollary 10.7. — *Let $\mathrm{K}=\mathbb{Q}(\sqrt{32009})$ and let $s \in \mathbb{Z}_{>0}$. Take T as before. There exists s sets $\mathscr{S}_i$, $i=1,\cdots,s$,of prime ideals of $\mathscr{O}_{\mathbb{Q}_{n_0}}$, all of positive density, such that for all set $S=\{\mathfrak{p}_1,\cdots,\mathfrak{p}_s\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, and for $n \geq \log_3(2+s)+4$, one has:*

(i) $\mathrm{G}^T_S(\mathrm{K}_n)^{p,\mathrm{el}}$ *has s independant fixed points under the action of σ;*
(ii) *there exists no continuous representation $\rho : \mathrm{G}^T_S(\mathrm{K}_n) \longrightarrow \mathrm{Gl}_m(\mathbb{Q}_p)$ with σ-uniform image fixed-point-mixing modulo Frattini.*

Remark 10.8. — If we start with a situation where the p-class group is cyclic along the $\mathbb{Z}_p$-cyclotomic extension, then $\mathrm{Cl}(\mathrm{K}^H_n)$ is trivial: and then one can take $T=\emptyset$. But in this case, the group G_S is of type $(1,b)$, and one has seen in Proposition 4.30 (or Corollary 4.31) that this type is not compatible with the type of FAb uniform groups. And in this case, the expected conclusion is obvious!

10.2.2. When ℓ is odd. — Let K/k be a cyclic extension of prime degree $\ell > 2$. Assume that $\ell \mid (p-1)$. Suppose that

(i) the extension K/k is totally real;
(ii) the p-class group along the $\mathbb{Z}_p$-cyclotomic extension of k is trivial.

Let us take the notation of the beginning of section 8. One has seen that $\mathrm{K}^{(m)}$ is the key number field, where $\mathrm{K}^{(m)}$is the mth step of the Hilbert p-class field tower of K and where $m = \log_2(n(\ell)+1)$.

Thus by the Greenberg's conjecture, for $n_0 \gg 0$ and for $n \geq n_0$, on has $[\mathrm{K}_{n_0}^{(1)} : \mathrm{K}_{n_0}] = [\mathrm{K}_n^{(1)} : \mathrm{K}_{n_0}]$. If moreover, one assumes the Greenberg's conjecture for all the fields K_n, there exists an integer $n_1 \geq n_0$ such that $n \geq n_1$, $[(\mathrm{K}_{n_1})^{(1)} : \mathrm{K}_{n_1}^{(1)}] = [(\mathrm{K}_n^1)^{(1)} : \mathrm{K}_n^{(1)}]$ and then $[\mathrm{K}_n^{(2)} : \mathrm{K}_n] = [\mathrm{K}_{n_1}^{(2)} : \mathrm{K}_{n_1}]$. By following this process, one gets the existence of $n_m \in \mathbb{Z}_{>0}$ such that for all $n \geq n_m$, we get $[\mathrm{K}_n^{(m)} : \mathrm{K}_n] = [\mathrm{K}_{n_m}^{(m)} : \mathrm{K}_{n_m}]$ when supposing the Greenberg's conjecture for the number fields K_{n_i}, $i = 0, \cdots, m$. One can then apply the strategy of the section 10.2.1 to obtain:

Corollary 10.9. — *Under the conditions of this section, in particular by assuming the Greenberg's conjecture for totally real number fields, for sufficiently large $m \in \mathbb{Z}_{>0}$, there exists s sets $\mathscr{S}_i$, $i = 1, \cdots, s$ of prime ideals of $\mathscr{O}_{\mathrm{k}_m}$, all of positive density, such that for all set $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$, with $\mathfrak{p}_i \in \mathscr{S}_i$, and for all $n \geq m$, one has:*

(i) $\Big(\mathrm{G}_S(\mathrm{K}_n)\Big)^{p,\mathrm{el}}$ *has s independant fixed points under the action of σ;*

(ii) *there is no continuous representation $\rho : \mathrm{G}_S(\mathrm{K}_n) \to \mathrm{Gl}_r(\mathbb{Q}_p)$ of σ-uniform image fixed-point-mixing modulo Frattini and where Γ_σ is supported at S.*

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, GP-Pari. Available from http://pari.math.u-bordeaux.fr/.

[2] A. Borel and J.-P. Serre, *Sur certains sous-groupes des groupes de Lie compacts*, Comment. Math. Helv. **27** (1953), 128-139.

[3] N. Boston, *Explicit Deformation of Galois Representations*, Inventiones Math. **103** (1991), 181-196.

[4] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory **42** (1992), no. 3, 285-291.

[5] N. Boston, *Some cases of the Fontaine-Mazur conjecture II.* J. Number Theory **75** (1999), no. 2, 161-169.

[6] K. Buzzard, *Analytic continuation of overconvergent eigenforms*, Jour. Am. Math. Soc. **16** (2002), 29-55.

[7] K. Buzzard and R. Taylor, *Companion forms and weight* 1 *forms*, Annals of Math. **149** (1999), 905-919.

[8] 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.

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

[10] 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.

[11] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of Number Fields*, Proc. Japan Acad. **70** Ser. A (1994), 264-266.

[12] D. Gildenhuysn W. Herfort and L. Ribes, *Profinite Frobenius group*, Arch. Math. **33** (1979/80), no. 6, 518–528.

[13] G. Gras, *Class Field Theory*, SMM, Springer, 2003.

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

[15] G. Gras and A. Munnier, *Extensions cycliques T-totalement ramifiées*, Publ. Math. Besançon, 1997/98.

[16] R. Greenberg, *Galois representations with open images*, Annales Math. Québec **40** (2016), Issue 1, p 83-119.

[17] F. Hajir and C. Maire, *Unramified subextensions of ray class fields towers*, Journal of Algebra **249** (2002), 528-543.

[18] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, preprint 2016.

[19] W.N. Herfort and L. Ribes, *On Automorphisms of Free Pro-p-Groups I*, Proc. Amer. Math. Soc. **108** (1990), no. 2, 287–295. J. Math. Soc. Japan **35** (1983), no. 4, 693–709.

[20] K. Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures et Appl. **35** (1956), 180-192.

[21] N. Jacobson, *A note on automorphisms and derivations of Lie algebras*, Pacific J. Math. **12** (1962), 281-283.

[22] N. Jacobson, *Lie Algebras*, Dover, 1979.

[23] Kassaei, Payman L. *Modularity lifting in parallel weight one*, J. Amer. Math. Soc. **26** (2013), no. 1, 199-225.

[24] M. Kisin, *Modularity of 2-adic representations*, Invent. Math. **178** (3) (2009), 587-634.

[25] M. Kisin and S. Wortmann, *A note on Artin motives*, Math. Res. Letters **10** (2003), no. 2-3, 375-389.

[26] B. Klopsch and I. Snopce, *A characterization of uniform pro-p groups*, Q. J. Math. **65** (2014), no. 4, 1277–1291.

[27] T.Y. Lam, *A first course in noncommutative rings*, GTM 131, Springer, 2001

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

[29] A. Lubotzky and A. Mann, *Powerful p-groups II. p-adic Analytic Groups*, J. of Algebra **105** (1987), 506-515.

[30] C. Maire, *T-S-capitulation*, Publ. Math. Besançon, 1996.

[31] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées, S-décomposées*, J. Th. des Nombres de Bordeaux **8** (1996), 47-73.

[32] C. Maire, *Some new evidence for the Fontaine-Mazur conjecture*, Mathematical Research Letters **14** (2007), 673-680.

[33] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math. **183** (2011), no. 3, 649–680.

[34] J. Pomfret, *Similarity of matrices over finite rings*, Proc. of the AMS **37** (1973), no. 2, 421-422.

[35] V. Pilloni, *Formes modulaires p-adiques de Hilbert de poids* 1, Invent. Math., to appear.

[36] V. Pilloni and B. Stroh, *Surconvergence, ramification et modularité*, Astérisque **382** (2016), 195-266.

[37] L. Ribes and P. Zalesskii, Profinite Groups, EMG 40, Springer, 2010.

[38] R. Schoof, *Infinite class field towers of quadratic fields*, J. Reine Angew. Math. **372** (1986), 209–220.

[39] G.B. Seligman, *On automorphisms of Lie algebras of classical type. II*, Trans. Amer. Math. Soc. **94** (1960), 452 - 482.

[40] A. Shalev, *Automorphisms of finite groups of bounded ranks*, Israel Jour. of Math. **82** (1993), 395-404. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. Mosc. Math. J.**2** (2002), no. 2, 329–402.

[41] K. Wingberg, *On the Fontaine-Mazur Conjecture for CM-Fields*, Compositio Math. **131** (2002), 341-354.

[42] K. Wingberg, *Free quotients of Demuskin groups with operators*, Preprint 2004.

June 7, 2018

Farshid Hajir, Department of Mathematics & Statistics, University of Massachusetts, Amherst MA 01003, USA.

Christian Maire, Laboratoire de Mathématiques de Besançon, Université Bourgogne Franche-Comté et CNRS (UMR 6623), 16 route de Gray, 25030 Besançon cédex, France.