PRIME DECOMPOSITION AND THE IWASAWA MU-INVARIANT

by

Farshid Hajir & Christian Maire

Abstract. — For $\Gamma = \mathbb{Z}_p$, Iwasawa was the first to construct Γ-extensions over number fields with arbitrarily large μ-invariants. In this work, we investigate other uniform pro-p groups which are realizable as Galois groups of towers of number fields with arbitrarily large μ-invariant. For instance, we prove that this is the case if p is a regular prime and Γ is a uniform pro-p group admitting a fixed-point-free automorphism of odd order dividing $p-1$. Both in Iwasawa's work, and in the present one, the size of the μ-invariant appears to be intimately related to the existence of primes that split completely in the tower.

Contents

Introduction

Let p be a prime number. Let K be a number field and let L/K be a uniform p-extension: L/K is a normal extension whose Galois group $\Gamma := \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ is a uniform pro-p group (see section 1.1.1). We suppose moreover that *the set of places of* K *that are ramified in* L/K *is finite.*

2000 ***Mathematics Subject Classification.*** — 11R23, 11R29, 11R37.

Key words and phrases. — Ideal class groups, uniform pro-p groups, Iwasawa theory, μ-invariant, prime decomposition.

Acknowledgements. The second author would like to thank the Department of Mathematics & Statistics at UMass Amherst for its hospitality during several visits. He also thanks UMI CNRS 3457 at Montréal for providing a stimulating research atmosphere on a "Délégation" there. The authors are grateful to Georges Gras for helpful correspondence regarding p-rational fields.

If F/K is a finite subextension of L/K, let us denote by A(F) the p-Sylow subgroup of the class group of F and put

$$\mathscr{X} := \varprojlim_{\mathrm{F}} \mathrm{A}(\mathrm{F}),$$

where the limit is taken over all number fields F in L/K with respect the norm map. Then $\mathscr{X}$ is a $\mathbb{Z}_p[[\Gamma]]$-module and, thanks to a structure theorem (see section 1.1.2), one attaches a μ-invariant to $\mathscr{X}$, generalizing the well-known μ-invariant introduced by Iwasawa in the classical case $\Gamma \simeq \mathbb{Z}_p$. Iwasawa showed that the size of the μ-invariant is related to the rate of growth of p-ranks of p-class groups in the tower. For the simplest $\mathbb{Z}_p$-extensions, i.e. the cyclotomic ones, he conjectured that $\mu = 0$; this was verified for base fields which are abelian over $\mathbb{Q}$ by Ferrero and Washington [**9**] but remains an outstanding problem for more general base fields. Iwasawa initially suspected that his μ-invariant vanishes for all $\mathbb{Z}_p$-extensions, but later was the first to construct $\mathbb{Z}_p$-extensions with non-zero (indeed arbitrarily large) μ-invariants. It is natural to ask what other p-adic groups enjoy this property. Our present work leads us to the following conjecture:

Conjecture 0.1. — *Let Γ be a uniform pro-p group having a non-trivial fixed-point-free automorphism σ of order m co-prime to p (in particular if $m = \ell$ is prime, Γ is nilpotent). Then Γ has arithmetic realizations with arbitrarily large μ-invariant, i.e. for all $n \geq 0$, there exists a number field* K *and an extension* L/K *with Galois group isomorphic to Γ such that $\mu_{\mathrm{L/K}} \geq n$.*

Our approach for realizing Γ as a Galois group is to make use of the existence of so-called p-rational fields. See below for the definition, but for now let us just say that the critical property of p-rational fields is that in terms of certain maximal p-extensions with restricted ramification, they behave especially well, almost as well as the base field of rational numbers. As we will show, Conjecture 0.1 can be reduced to finding a p-rational field with a fixed-point-free automorphism of order m co-prime to p. These considerations lead us to formulate the following conjecture about p-rational fields.

Conjecture 0.2. — *Given a prime p and an integer $m \geq 1$ co-prime to p, there exist a totally imaginary field K_0 and a degree m cyclic extension K/K_0 such that* K *is p-rational.*

Although we will not need it, we believe K_0 in the conjecture may be taken to be imaginary quadratic; see Conjecture 4.16 below. Our key result is:

Theorem 0.3. — *Conjecture 0.2 for the pair (p, m) implies Conjecture 0.1 for any uniform pro-p group Γ having a fixed-point-free automorphism of order m.*

One knows that if m is an odd divisor of $p-1$, where p is a regular prime, then for any $n \geq 1$, the cyclotomic field $\mathbb{Q}(\zeta_{p^n})$ provides a positive answer to the previous question. We therefore have

Corollary 0.4. — *Assume p is a regular prime and that the uniform group Γ has a fixed-point-free automorphism σ of odd order m dividing $p-1$. Then Conjecture 0.1 is true for Γ.*

This circle of ideas is closely related to the recent work of Greenberg [**15**] in which he constructs analytic extensions of number fields having a Galois group isomorphic to an open subgroup of $\mathrm{Gl}_k(\mathbb{Z}_p)$. The idea of studying pro-p towers equipped with a fixed-point-free action of a finite group of order prime to p occurs also in Boston's papers [**2**] and [**3**].

Our work raises the following purely group-theoretical question.

Question 0.5. — *Let Γ be a nilpotent uniform pro-p group. Does there exist a uniform nilpotent pro-p group Γ' having a fixed-point-free automorphism of prime order $\ell \neq p$ such that $\Gamma' \twoheadrightarrow \Gamma$?*

A positive answer to this question would imply that for all nilpotent uniform pro-p groups Γ, there exist arithmetic realizations with arbitrarily large μ-invariant.

In his recent work [**12**], Gras gave some conjectures about the p-adic regulator in a fixed number field K when p varies. In our context, one obtains:

Theorem 0.6. — *Let $\mathbb{P}$ be an infinite set of prime numbers and let m be an integer co-prime to all $p \in \mathbb{P}$. Let $(\Gamma_p)_{p\in\mathbb{P}}$ be a family of uniform pro-p groups of fixed dimension d, all having a fixed-point-free automorphism σ of order m. Assuming the Conjecture of Gras (see Conjecture 4.13), there exists a constant p_0, such that for all $p \geq p_0$, there exist Γ_p-extensions of number fields with arbitrarily large μ-invariants.*

In another direction, a conjecture in the spirit of the heuristics of Cohen-Lenstra concerning the p-rationality of the families $\mathscr{F}_{\mathrm{G}}$ of number fields K Galois over $\mathbb{Q}$, all having Galois group isomorphic to a single finite group G, seems to be reasonable (see [**31**]). When the prime $p \nmid |\mathrm{G}|$, the philosophy here is that the density of p-rational number fields in $\mathscr{F}_{\mathrm{G}}$ is positive. This type of heuristic lends further evidence for conjecture 0.1.

Notations

Let $\mathscr{G}$ be a finitely generated pro-p group. For two elements x, y of $\mathscr{G}$, we denote by $x^y := y^{-1}xy$ the conjugate of x by y and by $[x,y] := x^{-1}y^{-1}xy = x^{-1}x^y$ the commutator of x and y. For closed subgroups $\mathscr{H}_1, \mathscr{H}_2$ of $\mathscr{G}$, let $[\mathscr{H}_1, \mathscr{H}_2]$ be the *closed* subgroup generated by all commutators $[x_1, x_2]$ with $x_i \in \mathscr{H}_i$. Let $\mathscr{G}^{\mathrm{ab}} := \mathscr{G}/[\mathscr{G},\mathscr{G}]$ be the maximal abelian quotient of $\mathscr{G}$, and let $d(\mathscr{G}) := \dim_{\mathbb{F}_p} \mathscr{G}^{\mathrm{ab}}$ be its p-rank.

Denote by $(\mathscr{G}_n)$ the p-central descending series of $\mathscr{G}$:

$$\mathscr{G}_1 = \mathscr{G},\ \mathscr{G}_2 = \mathscr{G}^p[\mathscr{G},\mathscr{G}], \cdots,\ \mathscr{G}_{n+1} = \mathscr{G}_n^p[\mathscr{G},\mathscr{G}_n].$$

The sequence $(\mathscr{G}_n)_n$ forms a base of open neighborhoods of the unit element e of $\mathscr{G}$.

If K is a number field, let A(K) be the p-Sylow subgroup of the class group of K. Let $S_p := \{\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}} : \mathfrak{p}|p\}$ be the set of primes of K of residue characteristic p. If S is any finite set of places of K, denote by K_S the maximal pro-p extension of K unramified outside S and put $\mathscr{G}_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ as well as $\mathrm{A}_S := \mathscr{G}_S^{\mathrm{ab}}$.

1. Arithmetic background

1.1. Formulas in non-commutative Iwasawa Theory. —

1.1.1. Algebraic tools. — Two standard references concerning p-adic analytic and in particular, uniform, pro-p groups are the long article of Lazard [**25**] and the book of Dixon, Du Sautoy, Mann and Segal [**8**].

Let Γ be an analytic pro-p group: we can think of Γ as a closed subgroup of $\mathrm{Gl}_m(\mathbb{Z}_p)$ for a certain integer m. The group Γ is said *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 has no torsion.
Let us recall two important facts.

Theorem 1.1. — *Every p-adic analytic pro-p group contains an open uniform subgroup.*

Theorem 1.2. — *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 $\Gamma_{i+1}/\Gamma_{i+2}$.*

Let us make some remarks.

Remark 1.3. — Let $\dim(\Gamma)$ be the dimension of Γ as analytic variety.
1) If Γ is uniform then $d_p\Gamma=\dim(\Gamma)=\mathrm{cd}_p(\Gamma)$, where $\mathrm{cd}_p(\Gamma)$ is the p-cohomological dimension of Γ.
2) [**24**, Corollary 1.8] Suppose Γ is a torsion-free p-adic analytic group, $p\geq\dim(\Gamma)$ and $d(\Gamma)=\dim(\Gamma)$. Then the group Γ is uniform.
3) For $p\geq 2$, the pro-p-group $\mathbb{1}_n+\mathscr{M}_n(\mathbb{Z}_p)$ is uniform, where $\mathscr{M}_n(\mathbb{Z}_p)$ is the the set of $n\times n$ matrices with coefficients in $\mathbb{Z}_p$.

Now let us fix a uniform pro-p group Γ of dimension d. Recall that (Γ_n) is the p-descending central series of Γ. By Theorem 1.2, one has $[\Gamma:\Gamma_n]=p^{dn}$, for all n.

Let $\mathbb{Z}_p[[\Gamma]]:=\varprojlim_{\mathscr{U}\lhd_O\Gamma}\mathbb{Z}_p[\Gamma/\mathscr{U}]$ be the complete Iwasawa algebra, where $\mathscr{U}$ runs along the open normal subgroups of Γ. Put $\Omega:=\mathbb{F}_p[[\Gamma]]=\mathbb{Z}_p[[\Gamma]]/p$. The rings Ω and $\mathbb{Z}_p[[\Gamma]]$ are local, noetherien and without zero divisor [**8**, §7.4]: each of them has a fractional skew field. Denote by $Q(\Omega)$ the fractional skew field of Ω. If $\mathscr{X}$ is a finitely generated Ω-module, the *rank* $\mathrm{rk}_\Omega(\mathscr{X})$ of $\mathscr{X}$ is the $Q(\Omega)$-dimension of $\mathscr{X}\otimes_\Omega Q(\Omega)$. For more details, we refer the reader to Howson [**19**] and Venjakob [**34**].

Definition 1.4. — Let $\mathscr{X}$ be a finitely generated $\mathbb{Z}_p[[\Gamma]]$-module. Put

$$r(\mathscr{X})=\mathrm{rk}_\Omega\mathscr{X}[p]\ \text{ and }\ \mu(\mathscr{X})=\sum_{i\geq 0}\mathrm{rk}_\Omega\mathscr{X}[p^{i+1}]/\mathscr{X}[p^i].$$

Remark 1.5. — One has $\mu(\mathscr{X})\geq r(\mathscr{X})$ and, $r(\mathscr{X})=0$ if and only if $\mu(\mathscr{X})=0$.

There is a large and growing literature on the study of $\mathbb{Z}_p[[\Gamma]]$-modules in the context of Iwasawa theory. We recall a result of Perbet [**30**], where, by making use of the work of Harris [**17**], Venjakob [**34**] and Coates-Schneider-Sujatha [**5**], among others, he manages to estimate the size of the coinvariants $(\mathscr{X}_{\Gamma_n})_n$ of $\mathscr{X}$. Recall that $\mathscr{X}_{\Gamma_n}$ is the largest quotient of $\mathscr{X}$ on which Γ_n, the nth element of the p-central series, acts trivially.

***Theorem 1.6* (Perbet, [30])**. — *Suppose that $\mathscr{X}$ is a torsion $\mathbb{Z}_p[[\Gamma]]$-module where Γ is a uniform pro-p group of dimension d. Then for $n\gg 0$:*

$$\dim_{\mathbb{F}_p}\mathscr{X}_{\Gamma_n}=r(\mathscr{X})p^{dn}+O\Big(p^{n(d-1)}\Big),$$

and

$$\#(\mathscr{X}_{\Gamma_n}/p^n) = p^{\mu(\mathscr{X})p^{dn}+O\left(np^{n(d-1)}\right)}.$$

We now turn to applying these formulas in the arithmetic context.

1.1.2. Arithmetic. — Let L/K be a Galois extension of number fields with Galois group Γ, where Γ is a uniform pro-p group. We assume that *the set of primes of* K *ramified in* L/K *is finite*. Let $(\Gamma_n)_n$ be the p-central descending series of Γ and put $\mathrm{K}_n := \mathrm{L}^{\Gamma_n}$ for the corresponding tower of fixed fields.

Now let $\mathscr{X}$ be the projective limit along L/K of the p-class group $\mathrm{A}(\mathrm{K}_n)$ of the fields K_n. Then, $\mathscr{X}$ is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module. For the remainder of this work, $\mathscr{X}$ will denote this module built up from the p-class groups of the intermediate number fields in L/K. In particular, we put $\mu_{\mathrm{L/K}} = \mu(\mathscr{X})$ and $r_{\mathrm{L/K}} = r(\mathscr{X})$. For this module, by classical descent, Perbet proved:

***Theorem 1.7* (Perbet [30]).** — *For $n \gg 0$, one has:*

$$\log|\mathrm{A}(\mathrm{K}_n)/p^n| = \mu_{\mathrm{L/K}} p^{dn}\log p + O\left(np^{d(n-1)}\right)$$

and

$$d_p\mathrm{A}(\mathrm{K}_n) = r_{\mathrm{L/K}} p^{dn} + O\left(p^{n(d-1)}\right).$$

One then obtains immediately the following corollary:

***Corollary 1.8*.** — (*i*) *Along the extension* L/K*, the p-rank of* $\mathrm{A}(\mathrm{K}_n)$ *grows linearly with respect to the degree* $[\mathrm{K}_n : \mathrm{K}]$ *if and only if* $\mu_{\mathrm{L/K}} \neq 0$.
(*ii*) *If there exists a constant α such that for all $n \gg 0$, $d_p\mathrm{A}(\mathrm{K}_n) \geq \alpha p^{dn}$, i.e. $d_p\mathrm{A}(\mathrm{K}_n) \geq \alpha[\mathrm{K}_n : \mathrm{K}]$, then $\mu_{\mathrm{L/K}} \geq \alpha$.*

At this point, we should recall some standard facts from commutative Iawasawa theory. First, for the cyclotomic $\mathbb{Z}_p$-extension, Iwasawa conjectured that the μ-invariant is 0 for all base fields, and this has been shown to be the case when the based field is abelian over $\mathbb{Q}$. When the base field K contains a primitive pth root of unity, the reflection principle allows one to give some estimates on the μ-invariant [**30**].

1.2. On the p-rational number fields. — A number field K is called *p-rational* if the Galois group $\mathscr{G}_{S_p}$ of the maximal pro-p-extension of K unramified outside p is pro-p free. From the extensive literature on p-rational fields, we refer in particular to Jaulent-Nguyen Quang Do [**22**], Movahhedi-Nguyen Quang Do [**27**], Movahhedi [**28**], and Gras-Jaulent[**14**]. A good general reference is the book of Gras [**11**].

***Definition 1.9*.** — If $\mathscr{G}$ is a pro-p group, let us denote by $\mathscr{T}(\mathscr{G})$ the torsion of $\mathscr{G}^{\mathrm{ab}}$. When $\mathscr{G} = \mathscr{G}_S$, put $\mathscr{T}_S := \mathscr{T}(\mathscr{G}_S)$; when $S = S_p$, put $\mathscr{T}_p := \mathscr{T}_{S_p}$.

A standard argument in pro-p group theory shows the following:

***Proposition 1.10*.** — *A pro-p group $\mathscr{G}$ is free if and only if $\mathscr{T}(\mathscr{G})$ and $H^2(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p)$ are trivial.*

Proof. — Indeed, the exact sequence $0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ gives the sequence

$$0 \longrightarrow H_2(\mathscr{G}, \mathbb{Z})/p \longrightarrow H_2(\mathscr{G}, \mathbb{F}_p) \longrightarrow H_1(\mathscr{G}, \mathbb{Z})[p] \longrightarrow 0,$$

and to conclude, recall that $H_1(\mathscr{G}, \mathbb{Z}) \simeq \mathscr{G}^{ab}$ and $H_2(\mathscr{G}, \mathbb{Z}) \simeq H^2(\mathscr{G}, \mathbb{Q}/\mathbb{Z})^*$. □

Remark that if $\mathscr{G}$ is pro-p free then $\mathscr{G}^{\mathrm{ab}} \simeq \mathbb{Z}_p^d$, where d is the p-rank of $\mathscr{G}$. This observation shows in particular that if the group $\mathscr{G}$ corresponds to the Galois group of a pro-p extension of number fields, then necessarily this extension is wildly ramified.

We now explain how the Schur multiplier of $\mathscr{G}_S$ is related to the Leopoldt Conjecture.

Proposition 1.11. — *Let S be a set of places of* K, *and for $v \in S$, let $\mathscr{U}_v$ be the pro-p completion of the local units at v. If the $\mathbb{Z}_p$-rank of the diagonal image of $\mathscr{O}_{\mathrm{K}}^\times$ in $\prod_{v\in S} \mathscr{U}_v$ is maximal, namely $r_1 + r_2 - 1$, then $H^2(\mathscr{G}_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Moreover if $S_p \subseteq S$, these conditions are equivalent. In particular, assuming the Leopoldt Conjecture for* K *at p, $\mathscr{G}_{S_p}$ is free if and only if $\mathscr{T}_p$ is trivial.*

Proof. — For the case of restricted ramification, see [**26**]. For the general case, see [**29**, Corollaire 1.5]. □

Remark 1.12. — Some examples of free quotients of $\mathscr{G}_S$ with splitting conditions are given in §4.3 below.

***Proposition 1.13* (A 'numerical' p-rationality criterion)**
Let $\mathrm{A}_{\mathfrak{m}}$ be the p-Sylow subgroup of the ray class group of modulus $\mathfrak{m} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{a_{\mathfrak{p}}}$ of K, *where $a_{\mathfrak{p}} = 2e_{\mathfrak{p}} + 1$, and $e_{\mathfrak{p}}$ is the absolute index of ramification of $\mathfrak{p}$ (in* K/$\mathbb{Q}$*). Assume that* K *verifies the Leopoldt Conjecture at p. Then* K *is p-rational if and only if $d_p\mathrm{A}_{\mathfrak{m}} = r_2 + 1$.*

Proof. — First, as one assumes Leopoldt Conjecture for K at p, then the $\mathbb{Z}_p$-rank of $\mathrm{A}_{S_p} = \mathscr{G}_{S_p}^{\mathrm{ab}}$ is exactly r_2+1. Hence $\mathscr{G}_{S_p}$ is free if and only if $\mathscr{T}_p = \{1\}$, which is equivalent to $d_p\mathrm{A}_{S_p} = r_2 + 1$. Now, by Hensel's lemma, every unit $\varepsilon \equiv 1(\mathrm{mod}\pi_{\mathfrak{p}}^{a_{\mathfrak{p}}})$ is a p-power in $\mathrm{K}_{\mathfrak{p}}^\times$ and so $d_p\mathrm{A}_{\mathfrak{m}} = d_p\mathrm{A}_{S_p}$. □

Example 1.14. — Take $\mathrm{K} = \mathbb{Q}(\zeta_7)$ and $p = 37$. Then, p is not ramified in K/$\mathbb{Q}$ and $a_{\mathfrak{p}} = 3$. A simple computation gives $\mathrm{d}_p\mathrm{A}_{S_p} = 4 = r_2 + 1$, so K is 37-rational.

Example 1.15. — One can check easily that $\mathbb{Q}(\zeta_7)$ is not 2-rational but $\mathbb{Q}(\zeta_{13})$ is 2-rational.

Here is a very well-known case of the situation.

***Proposition 1.16* (A 'theoretical' p-rationality criterion)**
Suppose that the number field K *contains a primitive pth root of unity. Then* K *is p-rational if and only if there exists exactly one prime of* K *above p and the p-class group of* K *(in the narrow sense if $p = 2$) is generated by the unique prime dividing p.*

Proof. — See for example Theorem 3.5 of [**11**]. □

Remark 1.17. — In particular, when p is regular, $\mathbb{Q}(\zeta_{p^n})$ is p-rational for all $n \geq 1$.

Now we will give some more precise statements by considering some Galois action. Let K/K_0 be a Galois extension of degree m, with $p \nmid m$. Put $\Delta = \mathrm{Gal}(\mathrm{K}/\mathrm{K}_0)$. Let $r = r_1(\mathrm{K}_0) + r_2(\mathrm{K}_0)$ be the number of archimedean places of K_0. Let S be a finite set of places of K_0. The arithmetic objects that will use have a structure of $\mathbb{F}_p[\Delta]$-modules. Then for a such module M, one notes by $\chi(M)$ its character. Let ω be the Teichmüller character, let $\mathbf{1}$ be the trivial character and let χ_{reg} be the regular character of Δ.

Proposition 1.18. — *Suppose the field* K *is* p*-rational and that the real infinite places of* K_0 *stay real in* K *(this is always the case when* m *is odd). Then*

$$\chi(\mathrm{A}_{S_p}) = r_2(\mathrm{K}_0)\chi_{\mathrm{reg}} + \mathbf{1}\cdot$$

Proof. — It is well-known. The character of the Δ-module $\prod_{v\in S_p}\left(\mathscr{U}_v/\mu_{p^\infty}(\mathrm{K}_v)\right)$ is equal to $[\mathrm{K}_0 : \mathbb{Q}]\chi_{\mathrm{reg}}$ and by Dirichlet's Unit Theorem, the character of $\mathscr{O}_{\mathrm{K}}^{\times}/\mu(\mathrm{K})$ is equal to $\left(r_1(\mathrm{K}_0) + r_2(\mathrm{K}_0)\right)\chi_{\mathrm{reg}} - \mathbf{1}$. Then, as K is p-rational,

$$\chi(\mathrm{A}_{S_p}) = [\mathrm{K}_0 : \mathbb{Q}]\chi_{\mathrm{reg}} - \left(\left(r_1(\mathrm{K}_0) + r_2(\mathrm{K}_0)\right)\chi_{\mathrm{reg}} - \mathbf{1}\right) = r_2(\mathrm{K}_0)\chi_{\mathrm{reg}} + \mathbf{1}\cdot$$

□

1.3. Genus Theory. — The literature on Genus Theory is rich. The book of Gras [**11**, Chapter IV, §4] is a good source for its modern aspects. All we will need in this work is the following simplified version of the main result.

***Theorem 1.19* (Genus Theory)**. — *Let* F/K *be a Galois degree* p *extension of number fields* L/K. *Let* S *be the set of places of* K *ramified in* F/K *(including the infinite places). Then*

$$d_p\mathrm{A}(\mathrm{L}) \geq |S| - 1 + d_p\mathscr{O}_K^{\times}.$$

We will also need the following elementary fact.

Proposition 1.20. — *Let* K *be a number field containing a primitive pth root of unity, and let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *be distinct prime ideals of* $\mathscr{O}_{\mathrm{K}}$. *Then there exists a cyclic extension* F/K *of degree* p *in which the primes* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *all ramify.*

Proof. — Choose a prime ideal $\mathfrak{p}_0$ of $\mathscr{O}_{\mathrm{K}}$ in the inverse of the ideal class of the product $\mathfrak{p}_1 \cdots \mathfrak{p}_t$, so that $\mathfrak{p}_0\mathfrak{p}_1 \ldots \mathfrak{p}_t$ is a principal ideal in $\mathscr{O}_{\mathrm{K}}$, generated by some algebraic integer α, say. Then $\mathrm{F} = \mathrm{K}(\alpha^{1/p})$ is a cyclic degree p extension of K totally ramified at all the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. □

2. Background on automorphisms of pro-p groups

For this section, our main reference is the book of Ribes and Zalesskii [**32**, Chapter 2 and Chapter 4]. If Γ is a finitely generated pro-p group, denote by $\mathrm{Aut}(\Gamma)$ the group of continuous automorphisms of Γ. Recall that the kernel of $g_\Gamma : \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2)$ is a pro-p group and that $\mathrm{Aut}(\Gamma/\Gamma_2) \simeq \mathrm{Gl}_d(\mathbb{F}_p)$, where d is the p-rank of Γ.

2.1. Fixed points. —

Definition 2.1. — Let Γ be a finitely generated pro-p group and let $\sigma \in \mathrm{Aut}(\Gamma)$. Put $\mathrm{Fix}(\Gamma,\sigma) := \{x \in \Gamma : \sigma(x) = x\}$.

Remark 2.2. — (i) Obviously, $\mathrm{Fix}(\Gamma,\sigma)$ is a closed subgroup of Γ.
(ii) For integers n, $\mathrm{Fix}(\Gamma,\sigma) \subset \mathrm{Fix}(\Gamma,\sigma^n)$ with equality when n is co-prime to the order of σ.

Definition 2.3. — For $\sigma \in \mathrm{Aut}(\Gamma)$, $\sigma \neq e$, one says that $\Gamma^{\circlearrowleft \sigma}$ is fixed-point-free if $\mathrm{Fix}(\Gamma,\sigma) = \{e\}$. More generally, if Δ is a subgroup of $\mathrm{Aut}(\Gamma)$, one says that the action $\Gamma^{\circlearrowleft \Delta}$ of Δ on Γ is fixed-point-free if and only if

$$\bigcup_{\substack{\sigma\neq e\\ \sigma\in\Delta}} \mathrm{Fix}(\Gamma,\sigma) = \{e\}.$$

In others words, Δ is fixed-point-free if and only if, for all non-trivial $\sigma \in \Delta$, $\Gamma^{\circlearrowleft \sigma}$ is fixed-point-free.

Remark 2.4. — Clearly if $\Gamma^{\circlearrowleft \langle\sigma\rangle}$ is fixed-point-free then $\Gamma^{\circlearrowleft \sigma}$ is fixed-point-free; it is an equivalence when σ is of prime order ℓ.

We are interested in instances of groups with fixed-point-free action that arise in arithmetic contexts. Let us recall the Schur-Zassenhaus Theorem for a profinite group $\mathscr{G}$:

***Theorem 2.5* (Schur-Zassenhaus).** — *Let Γ be a closed normal pro-p subgroup of a profinite group $\mathscr{G}$. Assume that the quotient $\Delta := \mathscr{G}/\Gamma$ is of order co-prime to p. Then the profinite group $\mathscr{G}$ contains a subgroup Δ_0 isomorphic to Δ. Two such groups are conjugated by an element of Γ and $\mathscr{G} = \Gamma \rtimes \Delta_0$.*

Proof. — See Theorem 2.3.15 of [**32**] or proposition 1.1 of [**10**]. □

As first consequence, one has the following:

Proposition 2.6. — *Let Γ be a finitely generated pro-p group and let $\Delta \subset \mathrm{Aut}(\Gamma)$ of order m, $p \nmid m$. If $\Gamma^{\circlearrowleft \Delta}$ is fixed-point-free then $\Big(\Gamma/\Gamma_2\Big)^{\circlearrowleft \Delta}$ is fixed-point-free, where we recall that Γ_2, the 2nd step in the p-central series of Γ, is the Frattini subgroup.*

Proof. — Let $\sigma \in \Delta$. The group $\langle\sigma\rangle$ acts on Γ, on Γ_2 and on Γ/Γ_2. By the Schur-Zassenhaus Theorem (applied to $\Gamma_2 \rtimes \langle\sigma\rangle$), the non-abelian cohomology group $H^1(\langle\sigma\rangle,\Gamma_2)$ is trivial and then the nonabelian cohomology of the exact sequence $1 \longrightarrow \Gamma \longrightarrow \Gamma \rtimes \langle\sigma\rangle \longrightarrow \langle\sigma\rangle \longrightarrow 1$ allows us to obtain:

$$H^0(\langle\sigma\rangle,\Gamma) \twoheadrightarrow H^0(\langle\sigma\rangle,\Gamma/\Gamma_2),$$

which is exactly the assertion of the Proposition. See also [**4**], [**15**], [**35**]. □

A main observation for our paper is the converse of the previous proposition when Γ is uniform:

Proposition 2.7. — *Let Γ be a uniform pro-p group. Let $\sigma \in \mathrm{Aut}(\Gamma)$ of order m co-prime to p. Then $(\Gamma/\Gamma_2)^{\circlearrowleft \sigma}$ is fixed-point-free if and only if $\Gamma^{\circlearrowleft \sigma}$ is fixed-point-free.*

Proof. — One direction is taken care of by Proposition 2.6. For the other direction, we first note that

$$\begin{array}{rcl}\varphi : \Gamma_{n-1}/\Gamma_n & \to & \Gamma_n/\Gamma_{n+1} \\ x & \mapsto & x^p\end{array}$$

is a $\langle\sigma\rangle$-isomorphism for $n \geq 2$. We thus obtain a $\langle\sigma\rangle$-isomorphism from Γ/Γ_2 to Γ_n/Γ_{n+1}. If $(\Gamma/\Gamma_2)^{\circlearrowleft\sigma}$ is fixed-point-free, then $(\Gamma_n/\Gamma_{n+1})^{\circlearrowleft\sigma}$ is fixed-point-free for all $n \geq 1$. Suppose $y \in \Gamma$ satisfies $\sigma(y) = y$. As the action of Γ/Γ_2 is fixed-point-free, we have $y(\mathrm{mod}\Gamma_2) \in \Gamma/\Gamma_2$ is trivial, so $y \in \Gamma_2$. Continuing in this way, we in fact conclude that $y \in \bigcap_n \Gamma_n = \{e\}$. □

Corollary 2.8. — *Let Γ be a uniform pro-p group and let $\sigma \in \mathrm{Aut}(\Gamma)$ of order m co-prime to p. Denote by χ the character of the semi-simple action of $\langle\sigma\rangle$ on Γ/Γ_2. Then $\Gamma^{\circlearrowleft\sigma}$ is fixed-point-free if and only, $\langle\chi, \mathbf{1}\rangle = 0$.*

Proof. — Indeed, one has seen (Proposition 2.7) that $\Gamma^{\circlearrowleft\sigma}$ is fixed-point-free if and only $\Big(\Gamma/\Gamma_2\Big)^{\circlearrowleft\sigma}$ is fixed-point-free, which is equivalent to $\langle\chi, \mathbf{1}\rangle = 0$. □

Remark 2.9. — Suppose that Γ is uniform of dimension d. The restriction of $\sigma \in \mathrm{Aut}(\Gamma)$ to $\Gamma/\Gamma_2 \simeq \mathbb{F}_p^d$ is an element of $\mathrm{Gl}_d(\mathbb{F}_p)$. Denote by $P_\sigma \in \mathbb{F}_p[X]$ its characteristic polynomial. Then the action $\Gamma^{\circlearrowleft\sigma}$ is fixed-point-free if and only if $P_\sigma(1) \neq 0$.

Remark 2.10. — When Γ is uniform and $\Delta \subset \mathrm{Aut}(\Gamma)$ is of order m co-prime to p, testing that the action of Δ is fixed-point-free on Γ is equivalent to testing this condition on the quotient $\mathrm{M} := \Gamma/\Gamma_2$. Let χ be the character resulting from the action of Δ on M. Then $\Gamma^{\circlearrowleft\Delta}$ is fixed point-free on M if and only if, for all $e \neq \sigma \in \Delta$, $\mathrm{Res}_{|\langle\sigma\rangle}(\chi)$ does not contain the trivial character, where here $\mathrm{Res}_{|\langle\sigma\rangle}$ is the restriction to $\langle\sigma\rangle$. By Frobenius Reciprocity, this condition is equivalent to $\langle\chi, \mathrm{Ind}_{\langle\sigma\rangle}^{\Delta}\mathbf{1}\rangle = 0$, where $\mathrm{Ind}_{\langle\sigma\rangle}^{\Delta}$ is the induction from $\langle\sigma\rangle$ to Δ.

We need also of the following proposition which will be crucial for our main result.

Proposition 2.11. — *Let Γ be a finitely generated pro-p group. Let σ and τ be two elements in $\mathrm{Aut}(\Gamma)$ of order m co-prime to p. If $\sigma = \tau$ on Γ/Γ_2, then $\Gamma^{\circlearrowleft\sigma}$ is fixed-point-free if and only if, $\Gamma^{\circlearrowleft\tau}$ is fixed-point-free. More precisely, $\mathrm{Fix}(\Gamma, \sigma) = g \cdot \mathrm{Fix}(\Gamma, \tau)$ for a certain element $g \in \ker\Big(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2)\Big)$.*

One needs the following lemma:

Lemma 2.12. — *Let Γ be a finitely generated pro-p group. Let σ and τ be two elements of $\mathrm{Aut}(\Gamma)$ of order m, $p \nmid m$, satisfying $\sigma = \tau$ on Γ/Γ_2. Then there exists $g \in \mathrm{Aut}(\Gamma)$ such that $\tau = \sigma^g$.*

Proof. — This is to be found in Lemma 3.1 of [**18**]. Since σ and τ coincide as elements of $\mathrm{Aut}(\Gamma/\Gamma_2)$, there exists γ in the pro-p group $\ker\Big(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2)\Big)$ such that $\sigma = \gamma\tau$. Consider the group $\langle\tau, \gamma\rangle : \langle\gamma, \gamma^\tau, \cdots, \gamma^{\tau^{m-1}}\rangle \rtimes \langle\tau\rangle$. Since $\langle\gamma, \gamma^\tau, \cdots, \gamma^{\tau^{m-1}}\rangle \subset \ker\Big(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2)\Big)$, $\langle\tau, \gamma\rangle$ is a semi-direct product of a pro-p-group and a group of order m. As τ and σ are both in $\langle\tau, \gamma\rangle$, the subgroups $\langle\tau\rangle$ and $\langle\sigma\rangle$ are conjugate to each other (by the Schur-Zassenahus Theorem 2.5): there exists $g \in \langle\gamma, \gamma^\tau, \cdots, \gamma^{\tau^{m-1}}\rangle$

such that $\tau^k = \sigma^g$ for a certain integer k, $(k,m)=1$, since σ and τ have the same order. Moreover, in Γ/Γ_2, $\overline{\tau}^k = \overline{\sigma^g} = \overline{\sigma} = \overline{\tau}$, and so we can take $k=1$. □

Proof of Proposition 2.11. — By the previous lemma, $\tau = \sigma^g$, for some g in $\ker(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2))$. We have that y is a fixed point of τ if and only if $g(y)$ is a fixed point of σ. □

2.2. Lifts. — Given a uniform pro-p group Γ equipped with an automorphism σ of order m prime to p, the central question of this subsection is to realize $\Gamma \rtimes \langle\sigma\rangle$ as a Galois extension over a number field.

Proposition 2.13. — *Let* F *be a free pro-p-group on d generators, and let g_{F} be the natural map* $\mathrm{Aut}(\mathrm{F}) \to \mathrm{Aut}(\mathrm{F}/\mathrm{F}_2)$*. Consider a subgroup* $\Delta \subset \mathrm{Aut}(\mathrm{F}/\mathrm{F}^p[\mathrm{F},\mathrm{F}])$ *of order m co-prime to p. Then there exists a subgroup* $\Delta_0 \subset \mathrm{Aut}(\mathrm{F})$ *isomorphic to Δ such that $g_{\mathrm{F}}(\Delta_0) = \Delta$. Moreover, any two such subgroups are conjugated by an element* $g \in \ker\Big(\mathrm{Aut}(\mathrm{F}) \to \mathrm{Aut}(\mathrm{F}/\mathrm{F}_2)\Big)$.

Proof. — First of all the natural map $g_{\mathrm{F}} : \mathrm{Aut}(\mathrm{F}) \to \mathrm{Aut}(\mathrm{F}/\mathrm{F}_2)$ is onto (Proposition 4.5.4 of [**32**]). Put $\widetilde{\Delta} = g_{\mathrm{F}}^{-1}(\Delta)$ and recall that $\ker(g_{\mathrm{F}})$ is a pro-p group. Then, $\Delta \simeq \widetilde{\Delta}/\ker(g_F)$ which has order co-prime to p. By the Schur-Zassenhaus Theorem 2.5, there exists a subgroup $\Delta_0 \subset \mathrm{Aut}(\mathrm{F})$, such that $(\Delta_0 \ker g_{\mathrm{F}})/\ker(g_{\mathrm{F}}) \simeq \Delta$. Moreover, two such subgroups are conjugate to each other. □

In fact, one needs a little bit more. The following proposition can be found in a recent paper of Greenberg [**15**] and partially in an unpublished paper of Wingberg [**35**].

***Proposition 2.14* (Greenberg, [15], Proposition 2.3.1)**. — *Let* $\mathscr{G} = \mathrm{F} \rtimes \Delta$ *be a profinite group where* F *is free pro-p on d' generators and where Δ is a finite group of order m co-prime to p. Let Γ be a finitely generated pro-p group on d generators, with $d' \geq d$. Suppose that there exists* $\Delta' \subset \mathrm{Aut}(\Gamma)$*, with $\Delta' \simeq \Delta$, such that the module* $\Delta'_{|\Gamma/\Gamma_2}$ *is isomorphic to a submodule of* $\Delta_{|\mathrm{F}/\mathrm{F}_2}$*. Then there exists a normal subgroup* N *of* F*, stable under Δ, such that* F/N *is Δ-isomorphic to Γ and so we have a surjection*

$$\mathscr{G} \twoheadrightarrow \Gamma \rtimes \Delta \simeq \Gamma \rtimes \Delta'.$$

Since this result is essential for our construction, we include a proof.

***Lemma 2.15* (Wingberg, [35], lemma 1.3)**. — *Let* F *be a free pro-p-group on d generators and let Γ be a pro-p groups generated by d generators. Let φ be a morphism on pro-p groups* $\varphi : \mathrm{F} \twoheadrightarrow \Gamma$*. Assume that there exists a finite group* $\Delta \subset \mathrm{Aut}(\Gamma)$ *of order m co-prime to p. Then the action of Δ lift to* F *such that φ becomes a Δ-morphism.*

Proof following [**35**]. — For a finitely generated pro-p group N, denote by g_{N} the natural map $g_{\mathrm{N}} : \mathrm{Aut}(\mathrm{N}) \to \mathrm{Aut}(\mathrm{N}/\mathrm{N}_2)$. Recall that $\ker(g_{\mathrm{N}})$ is a pro-p group.
Let $1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \longrightarrow \Gamma \longrightarrow 1$ be a minimal presentation of Γ. Denote by $\mathrm{Aut}_{\mathrm{R}}(\mathrm{F}) := \{\sigma \in \mathrm{Aut}(\mathrm{F}) : \sigma(\mathrm{R}) \subset (\mathrm{R})\}$. The natural morphism $f : \mathrm{Aut}_{\mathrm{R}}(\mathrm{F}) \to \mathrm{Aut}(\Gamma)$ is onto (see [**32**, Proposition 4.5.4]). Put $\widetilde{\Delta} := f^{-1}(\Delta) \subset \mathrm{Aut}_{\mathrm{R}}(\mathrm{F})$. Then $f(\widetilde{\Delta}) = \Delta$. Now the isomorphism between F/F_2 and Γ/Γ_2 induces an isomorphism f' between $\mathrm{Aut}(\mathrm{F}/\mathrm{F}_2)$ and $\mathrm{Aut}(\Gamma/\Gamma_2)$. Hence on $\mathrm{Aut}_{\mathrm{R}}(\mathrm{F}) \subset \mathrm{Aut}(\mathrm{F})$, one has: $g_\Gamma \circ f = f' \circ g_{\mathrm{F}}$. In particular $\ker\Big(\mathrm{Aut}_{\mathrm{R}}(\mathrm{F}) \to \mathrm{Aut}(\Gamma/\Gamma_2)\Big)$ is a pro-p group. Now let $\widetilde{f} : \widetilde{\Delta} \to \Delta$. Then: (i) $\ker(\widetilde{f})$

is a pro-p group and (ii) $\widetilde{\Delta}/\ker(\widetilde{f}) \simeq \Delta$ which has order co-prime to p. By the Schur-Zassenhaus Theorem 2.5, there exists $\Delta_0 \subset \mathrm{Aut}_{\mathrm{R}}(\mathrm{F})$ such that $\Delta_0 \cap \ker(\widetilde{f})$, *i.e.* $f(\Delta_0) = \Delta$ and we are done. ☐

Proof of Proposition 2.14. — As $d' \geq d$, let φ be a surjective morphism $\mathrm{F} \twoheadrightarrow \Gamma$. Put $\mathrm{R} = \ker(\varphi)$. As $p \nmid m$, the action of Δ on F/F_2 is semi-simple. Let us complete the $\mathbb{F}_p[\Delta]$-module Γ/Γ_2 with a submodule M such that $\Gamma/\Gamma_2 \oplus \mathrm{M} \simeq \mathrm{F}/\mathrm{F}_2$ as Δ-module. Let Γ' be the pro-p group $\Gamma' = \Gamma \times \Gamma_0$, where $\Gamma_0 \simeq (\mathbb{Z}_p/p\mathbb{Z}_p)^{d'-d}$ is generated by an $\mathbb{F}_p$-basis of M. By Lemma 2.15, there exists $\Delta_0 \subset \mathrm{Aut}_{\mathrm{R}}(\mathrm{F})$ isomorphic to Δ, such that the morphism $\varphi : \mathrm{F} \twoheadrightarrow \Gamma'$ is a Δ_0-morphism. By Proposition 2.13, there exists $g \in \mathrm{Aut}(\Gamma)$ such that $\Delta_0 = \Delta^g$. We note that $\Delta_0 \subset \mathrm{Aut}_{\mathrm{R}}(\mathrm{F})$ is equivalent to $\Delta \subset \mathrm{Aut}_{g(\mathrm{R})}(\mathrm{F})$. Then we take $\mathrm{N} = \langle g(\mathrm{R}), g(\mathrm{M})\rangle$ and observe that F/N is Δ-isomorphic to Γ. ☐

2.3. Frobenius groups. — We now review a group-theoretic notion that we need for our study of the μ-invariant.

Definition 2.16. — Let $\mathscr{G}$ be a profinite group. One says that $\mathscr{G}$ is a Frobenius group if $\mathscr{G} = \Gamma \rtimes \Delta$, where Γ is a finitely generated pro-p group, Δ is of order m co-prime to p, and such that the conjugation action of Δ on Γ is fixed-point-free.

The notion of a Frobenius group is a very restrictive one, as illustrated in the following Theorem:

***Theorem 2.17* (Ribes-Zalesskii, [32], corollary 4.6.10)**. — *Let $\mathscr{G} = \Gamma \rtimes \Delta$ be a Frobenius profinite group. Then the subgroup Γ of $\mathscr{G}$ is nilpotent. Moreover if $2 \mid |\Delta|$, Γ is abelian, if $3 \mid |\Delta|$, Γ is nilpotent of class at most 2, and more generaly of class at most* $\dfrac{(\ell-1)^{2^{\ell-1}-1}-1}{\ell-2}$ *if the prime number ℓ divides $|\Delta|$.*

Proposition 2.18. — *Let $\mathscr{G} = \Gamma \rtimes \Delta$, where Γ is a uniform pro-p group and such that $p \nmid |\Delta|$. Then $\mathscr{G}$ is a Frobenius group if and only if the action of Δ is fixed-point-free on Γ/Γ_2.*

Proof. — It is a consequence of Proposition 2.7. ☐

3. Proof of the main result

Let us recall the motivating question of this paper. Given a uniform group Γ of dimension d, equipped with a fixed-point-free automorphism of finite order co-prime to p, can one realize an arithmetic context for Γ as Galois group with arbitrarily large associated μ-invariant?

3.1. The principle. — Here we develop our strategy, which is simply to emulate Iwasawa's original construction for $\Gamma = \mathbb{Z}_p$. Given a uniform pro-p group Γ, our claim is that it suffices to produce a Galois extension L of a number field K such that

(i) Gal(L/K) is isomorphic to Γ;
(ii) there are only finitely many primes that are ramified in L/K;
(iii) there exist infinitely many primes of K which split completely in L/K.

We now explain why such a construction suffices to answer our key question for Γ.

Proposition 3.1. — *Suppose* Γ *is a uniform pro-*p *group and* L *is a Galois extension of a number field* K *such that:*

(i) Gal(L/K) *is isomorphic to* Γ*;*

(ii) *there are only finitely many primes that are ramified in* L/K*;*

(iii) *there exist infinitely many primes of* K *that split completely in* L/K.

Then there exist Γ*-extensions of number fields with arbitrarily large associated* μ*-invariant.*

Proof. — We may assume, without loss of generality, that K contains ζ_p, a primitive pth root of unity, for if we replace K by $\mathrm{K}(\zeta_p)$ and L by $\mathrm{L}(\zeta_p)$, then conditions (i), (ii), (iii) still hold – we merely observe that $\mathrm{K}(\zeta_p)/\mathrm{K}$ has degree co-prime to p whereas L/K is a pro-p extension. Choose an integer $t \geq 1$, as well as distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of $\mathscr{O}_{\mathrm{K}}$ which split completely in L. Let K'/K a cyclic degree p extension in which each of the primes $\mathfrak{p}_i$ ramifies for $i = 1, \ldots, t$ (see Proposition 1.20). Letting $\mathrm{L}' = \mathrm{K}'\mathrm{K}$, we see immediately that L'/K' is a Galois extension with Galois group isomorphic to Γ. Put $\mathrm{K}_n = \mathrm{L}^{\Gamma_n}$ where Γ_n is the nth term in the p-central series of $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Let $\mathrm{K}'_n : \mathrm{K}'\mathrm{K}_n$. Then using the genus theory estimate Theorem 1.19 to the cyclic degree p extension $\mathrm{K}'_n/\mathrm{K}_n$, we get the following lower bound for the p-rank of the p-class group of K'_n:

$$d_p\mathrm{A}(\mathrm{K}'_n) \geq [\mathrm{K}'_n : \mathrm{K}]\,(t - r_2(\mathrm{K}') - 1)\,.$$

We conclude from Corollary 1.8 that $\mu_{\mathrm{L}'/\mathrm{K}'} \geq t - r_2(\mathrm{K}') - 1$. Since we can take t to be as large as desired, and noting of course that $r_2(\mathrm{K}')$ is fixed as $t \to \infty$, we have shown that Γ-extensions with arbitrarily large μ-invariant can be constructed over base fields which are cyclic of degree p over K (if K contains ζ_p), and over $\mathrm{K}(\zeta_p)$ otherwise. □

To produce a tower L/K satisfying the hypotheses of the Proposition, we realize Γ, along with its fixed-point-free automorphism, inside the maximal pro-p extension $\mathrm{K}_{S_p}/\mathrm{K}$ of a p-rational field K; in particular the condition (ii) will be automatically satisfied in our situation as the ramification in the tower will be restricted to the primes dividing p.

3.2. The case $\Gamma = \mathbb{Z}_p$. — We now review Iwasawa's strategy in [**21**] (see also Serre [**33**, §4.5]) for finding arithmetic situations with large μ-invariant.

Let $\mathrm{K}/\mathbb{Q}$ be an imaginary quadratic field. Let us denote by σ the generator of $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. Suppose p is a rational prime which splits in $\mathscr{O}_{\mathrm{K}}$ into two distinct primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Let us suppose further that p does not divide the class number of K. Then for $i = 1, 2$, the maximal pro-p extension $\mathrm{K}_{\{\mathfrak{p}_i\}}$ of K unramified outside $\mathfrak{p}_i$ has Galois group Γ_i isomorphic to $\mathbb{Z}_p$. The automorphism σ permutes the fields $\mathrm{K}_{\{\mathfrak{p}_i\}}$. Thus inside the compositum of these two $\mathbb{Z}_p$-extensions, if we denote by $\langle e_i \rangle$ the subgroup fixing the field $\mathrm{K}_{\{\mathfrak{p}_i\}}$, then the subfield L fixed by $\langle e_1 + e_2 \rangle$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_p$, and the action $\sigma(e_1) = e_2 \equiv -e_1 (\mathrm{mod} \langle e_1 + e_2 \rangle)$ is dihedral.

Corollary 3.2. — *Under the preceding conditions,* $\mathrm{Gal}(\mathrm{L}/\mathbb{Q}) = \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \rtimes \langle \sigma \rangle \simeq \mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z}$*, where the action of* σ *satisfies* $x^\sigma = x^{-1}$*,* x *denoting a generator of* Gal(L/K)*. Thus, all primes* ℓ *of* $\mathbb{Q}$ *which remain inert in* $\mathrm{K}/\mathbb{Q}$ *subsequently split completely in* L/K.

Proof. — The first part of the corollary follows from the observations preceding it. For the second part, remark that the non-trivial cyclic subgroups of $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ are of the form $\langle x^{p^k} \rangle \simeq \mathbb{Z}_p$, $k \in \mathbb{N}$, or of the form $\langle \sigma x^{p^k} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Hence let ℓ be a prime which is unramified in L/$\mathbb{Q}$. If ℓ is inert in K/$\mathbb{Q}$, then the Frobenius automorphism σ_ℓ of ℓ in L/$\mathbb{Q}$ is of the form σx^{p^k}. As σ_ℓ is of order 2 (or equivalently, $\langle\sigma_\ell\rangle \cap \mathrm{Gal}(\mathrm{L}/\mathrm{K}) = \{e\}$), the prime ℓ splits totally in L/K. □

By applying Proposition 3.1 to the extension L/K, this construction allows us to produce $\mathbb{Z}_p$-extensions with μ-invariant as large as desired.

Remark 3.3. — We can say a bit more in the example 3.2. Let us show that a place of K above a prime ℓ splits totally in L/K if and only if ℓ is inert in K/$\mathbb{Q}$. For a prime $\mathfrak{q} \nmid p$, denote by $\sigma_\mathfrak{q}$ the Frobenius of $\mathfrak{q}$ in the compositum of the $\mathbb{Z}_p$-extensions of K. Let ℓ a prime that splits in K/$\mathbb{Q}$; let us write $\ell\mathscr{O}_\mathrm{K} = \mathscr{L}\mathscr{L}'$. If we write $\sigma_\mathscr{L} = ae_1 + be_2$, then by conjugation, $\sigma_{\mathscr{L}'} = be_1 + ae_2$. The key point is that the maximal pro-p extension of K unramified outside p and totally split at $\mathscr{L}$ and $\mathscr{L}'$ is finite, see [**11**]. Then $a^2 \neq b^2$. Note that when ℓ is inert in K/$\mathbb{Q}$ then $\sigma_\ell = a(e_1 + be_2)$. By reducing the Frobenius modulo $\langle e_1 + e_2\rangle$, we note that in the case when ℓ is inert, $\sigma_\ell \equiv 0 \pmod{\langle e_1 + e_2\rangle}$ but when ℓ splits in K/$\mathbb{Q}$, $\sigma_\mathscr{L} \equiv (a-b)e_1 \pmod{\langle e_1 + e_2\rangle} \neq 0 \pmod{\langle e_1 + e_2\rangle}$.

Remark 3.4. — One can generalize the above discussion for $\Gamma = \mathbb{Z}_p^r$, by considering a large CM-extension abelian over $\mathbb{Q}$. See Cuoco [**7**, Theorem 5.2])

Remark 3.5. — We observe that the basic principle in the constructions above is that there is a positive density of primes of a field K_0 which are inert in K, and that all of these subsequently split (thanks to the fact that the action $\Gamma^{\circlearrowleft\sigma}$ is fixed-point-free) in the Γ-extension. This is the starting point for the general case.

3.3. The general case. — We will consider a uniform pro-p group Γ of dimension d having a fixed-point-free automorphism σ of order m co-prime to p. We assume that $m \geq 3$; indeed for $m = 2$, $\Gamma \simeq \mathbb{Z}_p^d$ (by Theorem 2.17 of Ribes and Zaleskii).

Proposition 3.6. — *Let Γ be a uniform pro-p group of dimension d having an automorphism τ of order m with fixed-point-free action, where $m \geq 3$ is co-prime to p. Suppose* F_0 *is a totally imaginary number field admitting a cyclic extension* F/F_0 *of degree m such that* F *is p-rational. Let n be an integer such that $p^n[\mathrm{F}_0 : \mathbb{Q}]\cdot \geq 2d$, and let* K_0, *respectively* K *be the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of* F_0, *respectively* F. *Then there exists an intermediate field* $\mathrm{K} \subset \mathrm{L} \subset \mathrm{K}_{S_p}$ *such that* L *is Galois over* K_0 *with Galois group isomorphic to $\Gamma \rtimes \langle\tau\rangle$. In particular, if τ acts fixed-point-freely on* Γ/Γ_2 *and if $m = \ell$ is prime, then* $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_0)$ *is a Frobenius group.*

Proof. — The extension K/K_0 is cyclic of degree m and the number field K is p-rational, hence $\mathscr{G} := \mathrm{Gal}(\mathrm{K}_{S_p}/\mathrm{K})$ is a free pro-p group on $r_2(\mathrm{K}) + 1 \geq d$ generators. Put $\mathrm{Gal}(\mathrm{K}/\mathrm{K}_0) = \langle\sigma\rangle$ The extension $\mathrm{K}_{S_p}/\mathrm{K}_0$ is a Galois extension with Galois group $\mathscr{G}_0 = \mathrm{Gal}(\mathrm{K}_{S_p}/\mathrm{K}_0)$ isomorphic to $\mathscr{G} \rtimes \langle\sigma\rangle$. By Proposition 1.18, the character of the action of σ on $\mathscr{G}/\mathscr{G}_2$ is $p^n([\mathrm{F}_0 : \mathbb{Q}]/2)\cdot\chi_{\mathrm{reg}} + \mathbf{1}$. Now let $\chi(\Gamma/\Gamma_2) = \sum_{\chi\in\mathrm{Irr}(\langle\sigma\rangle)} \lambda_\chi\chi$ be the character of the action of τ on Γ/Γ_2. Then $\sum_\chi \chi(1)\lambda_\chi = d$ and, for all χ, $\lambda_\chi \leq d/\chi(1) \leq d$. In particular since $[\mathrm{F}_0 : \mathbb{Q}]\cdot p^n \geq 2d$, then necessarily, the $\langle\tau\rangle$-module Γ/Γ_2 is isomorphic to a submodule of $\mathscr{G}/\mathscr{G}_2$. By Proposition 2.14, there exists a normal subgroup N of $\mathscr{G}$, stable under σ, such that $\mathscr{G}/\mathrm{N}$ is $\langle\sigma\rangle$-isomorphic to Γ, and we have a surjection $\mathscr{G}_0 \twoheadrightarrow \Gamma \rtimes \langle\sigma\rangle \simeq \Gamma \rtimes \langle\tau\rangle$. □

We now state the key arithmetic proposition we need.

Proposition 3.7. — *Let* L/K_0 *be a Galois extension of Galois group* $\Gamma \rtimes \langle\sigma\rangle$*, where* Γ *is a uniform group of dimension* d *and where* σ *is of order* m *co-prime to* p*. Suppose that* $\Gamma^{\circlearrowleft^\sigma}$ *is fixed-point-free. Then every place* $\mathfrak{p}$ *which is (totally) inert in* K/K_0 *and is not ramified in* L/K *splits completely in* L/K*.*

Proof. — Let $\mathfrak{p}$ a prime of K inert in K/K_0 which is not ramified in L/K. Let us fix a prime $\mathfrak{P}|\mathfrak{p}$ of L (see $\mathfrak{P}$ as a system of coherent primes in L/K). Denote by $\widetilde{\sigma_\mathfrak{p}}$ be the Frobenius of $\mathfrak{p}$ in K/K_0 and let $\sigma_\mathfrak{P} \in \mathrm{Gal}(\mathrm{L}/\mathrm{K}_0)$ be an element of order m of the decomposition group of $\mathfrak{P}$ in L/K_0 lifting $\widetilde{\sigma_\mathfrak{p}}$. Then $\sigma_\mathfrak{P} = \sigma^i$ in $\mathrm{Aut}(\Gamma/\Gamma_2)$, for an integer i, $(i,m)=1$. By Proposition 2.11, there exists $g \in \ker\Big(\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Gamma_2)\Big)$ such that $\mathrm{Fix}(\Gamma, \sigma_\mathfrak{P}) = g \cdot \mathrm{Fix}(\Gamma, \sigma^i) = \{e\}$, the last equality coming from Remark 2.2. Let $\widehat{\sigma_\mathfrak{P}} := \mathrm{Frob}_\mathfrak{P}(\mathrm{L}/\mathrm{K})$. As $\mathfrak{p} \in \Sigma$, the prime $\mathfrak{P}$ is unramified in K/K_0 and then the decomposition group of $\mathfrak{P}$ in L/K_0 is cyclic: the elements $\sigma_\mathfrak{P}$ and $\widehat{\sigma_\mathfrak{P}}$ commute or, equivalently, $\widehat{\sigma_\mathfrak{P}}^{\sigma_\mathfrak{P}} = \widehat{\sigma_\mathfrak{P}}$. Hence if $\widehat{\sigma_\mathfrak{P}} \neq e$, the element $\sigma_\mathfrak{P} \in \mathrm{Aut}(\Gamma)$ has a fixed-point. Contradiction, and then $\widehat{\sigma_\mathfrak{P}} = e$. □

Assembling our forces, we can now formulate our main theorem.

Theorem 3.8. — *Let* Γ *be a uniform pro-p group having an automorphism* τ *of order* m *with fixed-point-free action, where* $m \geq 3$ *is co-prime to* p*. Suppose* F_0 *is a totally imaginary number field admitting a cyclic extension* F/F_0 *of degree* m *such that* F *is* p*-rational. Then there exists a finite* p*-extension* K/F *unramified outside* p *and a* Γ*-extension* L/K *with the following property: for any given integer* μ_0*, there exists a cyclic degree* p *extension* K' *over* $\mathrm{K}(\zeta_p)$ *such that* $\mathrm{L}' = \mathrm{LK}'$ *is a* Γ*-extension of* K' *whose* μ*-invariant satisfies* $\mu_{\mathrm{L}'/\mathrm{K}'} \geq \mu_0$*.*

Proof. — We simply follow the rubric of Proposition 3.6. Choose an integer n large enough so that $p^n[\mathrm{F}_0 : \mathbb{Q}] \geq 2\dim(\Gamma)$, then let K_0 and K by the nth layer of the cyclotomic $\mathbb{Z}_p$-extensions of F_0 and F respectively. Since F is p-rational, so is K. By Proposition 3.6, we are guaranteed of the existence of a Galois extension L/K_0 with Galois group $\Gamma \rtimes \langle\tau\rangle$ and $\mathrm{K} = \mathrm{L}^\Gamma$. By Proposition 3.7, every inert place in K/K_0 splits completely in L/K. Now we simply apply the construction described in the proof of Proposition 3.1. □

Remark 3.9. — Let us remark that in the construction of Theorem 3.8 (in fact of Proposition 3.6), we start with a p-rational field F and pass to another p-rational field K whose maximal p-ramified p-extension is of large enough rank to have Γ as a quotient. However, the cyclic degree p extension K' of $\mathrm{K}(\zeta_p)$ over which we construct a tower with large μ-invariant is not itself p-rational (see [**11**, Chapter IV, §3]).

Remark 3.10. — In his original treatment [**21**], Iwasawa was able to treat the case $p = 2$ alongside odd primes p. The elements of finite order of $\mathrm{Aut}(\mathbb{Z}_2)$ are of order 2. Then the Question 0.5 is essential for applying our previous "co-prime to p" strategy for $\mathbb{Z}_2$. Indeed, let us consider the uniform pro-2 group $\Gamma := \mathbb{Z}_2^2$ instead of $\mathbb{Z}_2$ by noting that $\mathrm{Aut}(\mathbb{Z}_2^2)$ has a fixed-point-free automorphism τ of order 3. By example 1.15, one knows that the field $\mathrm{K} = \mathbb{Q}(\zeta_{13})$ is 2-rational; the Galois group G_{S_2} is free on 7 generators. Moreover, G_{S_2} has an automorphism of order 3 coming from the unique cyclic sub-extension K/K_0 of degree 3. The character of this action contains the character of the action of τ on Γ/Γ_2. Hence by Proposition 3.6, there exists a Galois extension L/K with $\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \simeq \Gamma = \mathbb{Z}_2^2$ in which every odd inert place $\mathfrak{p}$ in K/K_0 splits completely in L/K. In particular every such place splits in every $\mathbb{Z}_2$-quotient of Γ and then the Proposition 3.1 apply for $\mathbb{Z}_2$.

4. Complements

4.1. A non-commutative example. — Assume $p > 3$. The nilpotent uniform groups of dimension ≤ 2 are all commutative. In dimension 3 they are parametrized, up to isomorphism, by $s \in \mathbb{N}$ and represented (see [**23**, §7 Theorem 7.4]) by:

$$\Gamma(s) = \langle x, y, z \mid [x, z] = [y, z] = 1, [x, y] = z^{p^s} \rangle.$$

Here the center of $\Gamma(s)$ is the procyclic group $\langle z \rangle$ and one has the sequence:

$$1 \longrightarrow \mathbb{Z}_p \longrightarrow \Gamma(s) \longrightarrow \mathbb{Z}_p^2 \longrightarrow 1.$$

Proposition 4.1. — *Let $s \in \mathbb{N}$ and let $p \equiv 1 (\mathrm{mod}\ 3)$. The group of automorphisms of $\Gamma(s)$ contains an element σ of order 3 for which the action is fixed-point-free.*

Proof. — To simplify the notation, put $\Gamma = \Gamma(s)$. First, let us remark that for $a, b \in \mathbb{N}$, one has $x^a y^b = z^{abp^s} y^b x^a$. Indeed,

$$x^a y = x^{a-1} z^{p^s} yx = z^{p^s} x^{a-1} yx = z^{ap^s} yx^a,$$

and the same holds for xy^b.
Let ζ be a primitive third root of the unity and let $\zeta^{(n)} \in \mathbb{N}$ be the truncation at level n of the p-adic expansion of ζ: $\zeta^{(n)} \equiv \zeta (\mathrm{mod}\ p^n)$. Let us consider σ defined by:

$$\begin{array}{rcl} \sigma : \Gamma & \rightarrow & \Gamma \\ x & \mapsto & x^{\zeta} \\ y & \mapsto & y^{\zeta} \\ z & \mapsto & z^{\zeta^2} \end{array}$$

Then $\sigma \in \mathrm{Aut}(\Gamma)$. Indeed one has to show that the relations defining Γ are stable under the action of σ, which is obvious for the relations $[x, z] = 1$ and $[y, z] = 1$. Let us look at the last relation. First, as Γ is uniform, let us recall that $\Gamma_{n+1} = \Gamma^{p^n}$. We have:

$$\sigma([x, y]) = \sigma(xyx^{-1}y^{-1}) \equiv x^{\zeta^{(n)}} y^{\zeta^{(n)}} x^{-\zeta^{(n)}} y^{-\zeta^{(n)}} (\mathrm{mod}\ \Gamma_n) \equiv z^{\left(\zeta^{(n)}\right)^2 p^s} (\mathrm{mod}\ \Gamma_n) \longrightarrow_n z^{\zeta^2 p^s}.$$

To finish, let us show that the automorphism σ is fixed-point-free. Indeed the eigenvalues of the action of σ on the $\mathbb{F}_p$-vector space $\Gamma/\Gamma_2 \simeq \mathbb{F}_p^3$ are ζ (with multiplicity 2) and ζ^2, so $\Gamma/\Gamma_2^{\circlearrowleft^{\sigma}}$ is fixed-point-free and we conclude with Proposition 2.7. □

Remark 4.2. — If $p \not\equiv 1 (\mathrm{mod}\ 3)$, there is no element $\sigma \in \mathrm{Aut}(\Gamma(s))$ of order 3 with fixed-point-free action. Indeed, let $\sigma \in \mathrm{Aut}(\Gamma(s)/\Gamma(s)_2) \simeq \mathrm{Gl}_3(\mathbb{F}_p)$, and suppose that σ is fixed-point-free. The eigenvalues of σ in $\overline{\mathbb{F}_p}$ are ζ and/or ζ^2 with multiplicity. But, as the trace of σ is in $\mathbb{F}_p$, then necessarily $\zeta \in \mathbb{F}_p$ and $3 \mid p - 1$.

Corollary 4.3. — *Assume $p \equiv 1 (\mathrm{mod}\ 3)$ and p regular. For each $s \in \mathbb{N}$, there exist $\Gamma(s)$-extensions of numbers fields with arbitrarily large μ-invariant.*

Remark 4.4. — For $p = 37$, which is the smallest irregular prime, we may not resort to the construction above with $\mathrm{F} = \mathbb{Q}(\zeta_{37})$, but we can still realize $\Gamma(s)$-extensions with arbitrarily large μ-invariant by applying Theorem 3.8 for $\mathrm{F}/\mathrm{F}_0 = \mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7})$.

4.2. Counting the split primes in uniform extensions. — Let L/K be a Galois extension with p-adic analytic Galois group Γ of dimension d. Denote by Σ the set of primes of $\mathscr{O}_{\mathrm{K}}$ unramified in L/K. Assume Σ finite. For $\mathfrak{p} \in \Sigma$, let $\mathscr{C}_{\mathfrak{p}}$ be the conjugacy class of the Frobenius of $\mathfrak{p}$ in L/K and put

$$\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) = \Big|\{\mathfrak{p} \in \Sigma,\ \mathscr{C}_{\mathfrak{p}} = \{1\}, \mathrm{N}(\mathfrak{p}) \leq x\}\Big|,$$

where $\mathrm{N}(\mathfrak{p}) := \Big|\mathscr{O}_{\mathrm{K}}/\mathfrak{p}\Big|$.

In [**33**, Corollary 1 of Theorem 10], under GRH, Serre shows that for all $\varepsilon > 0$, $\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) = O\Big(x^{\frac{1}{2}+\varepsilon}\Big)$. Without assuming GRH, $\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) = O\Big(x/\log^{2-\varepsilon}(x)\Big)$.

Proposition 4.5. — *Let p be a regular prime and let Γ be a uniform pro-p group having a non-trivial fixed-point-free automorphism σ of prime order $\ell \mid p-1$. Then there exists a constant $C > 0$ and a Γ-extension* L *over a number field* K *such that*

$$\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) \geq C\frac{x^{1/\ell}}{\log x}, \qquad x \gg 0.$$

Proof. — One use the construction of section 3.3. Put $\mathrm{K} = \mathbb{Q}(\zeta_{p^n})$ where n is the smallest integer such that $p^n(p-1) \geq 2\ell d$. Let K/K_0 be the unique cyclic extension of degree ℓ; $\mathrm{Gal}(\mathrm{K}/\mathrm{K}_0) = \langle\sigma\rangle$. Let L/K be a uniform Galois extension with group Γ constructed by the method of Proposition 3.6. Let $\mathscr{E}(\mathrm{L/K})$ be the set of conjugacy classes of $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ of the elements σ^i with $(i,\ell) = 1$. By Proposition 3.7, a prime $\mathfrak{q}$ of K for which the Frobenius conjugacy class $\sigma_{\mathfrak{q}} \in \mathrm{K}/\mathbb{Q}$ is in $\mathscr{E}(\mathrm{L/K})$, splits totally in L/K. Hence

$$\begin{aligned} \pi_{\mathrm{L/K}}^{\mathrm{split}}(x) &\geq \Big|\{\mathfrak{q} \in \Sigma,\ \sigma_{\mathfrak{q}} \in \mathscr{E}(\mathrm{L/K}),\ \mathrm{N}(\mathfrak{q}) \leq x\}\Big| \\ &= \Big|\{\mathfrak{q} \in \Sigma, \exists (i,\ell) = 1,\ \mathscr{C}_q(\mathrm{K}/\mathbb{Q}) = \sigma^i,\ q^\ell \leq x\} \\ &= \Big|\{\mathfrak{q} \in \Sigma, \exists (i,\ell) = 1,\ \mathscr{C}_q(\mathrm{K}/\mathbb{Q}) = \sigma^i,\ q \leq x^{1/\ell}\}\Big| \end{aligned}$$

where $\mathscr{C}_q(\mathrm{K}/\mathbb{Q})$ is the conjugacy class of the Frobenius of q in $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. By using Chebotarev Density Theorem, one concludes that

$$\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) \gg \frac{x^{1/\ell}}{\log x}.$$

□

Example 4.6. — For the uniform group $\Gamma(s)$ of dimension 3 discussed in §4.1, one obtains $\Gamma(s)$-extensions L/K with $\pi_{\mathrm{L/K}}^{\mathrm{split}}(x) \gg \dfrac{x^{1/3}}{\log x}$.

4.3. On p-rational fields with splitting. — For all this section, assume that $p > 2$. By making use of fixed-point-free automorphisms, we have produced some uniform extensions with infinitely many totally split primes. Using Class Field Theory it is also possible to produce some free-pro-p extensions with some splitting phenomena, but *we do not know if it is possible to construct free pro-p extensions in which infinitely many primes of the base field split completely.* In fact this question is related to the work of Ihara [**20**] and the recent work of the authors [**16**].

Let us show how to produce some free pro-p extensions with some splitting. Let S and T be two finite sets of places of number field K such that $S \cap T = \emptyset$. Recall that $S_p = \{\mathfrak{p} \in \mathrm{K} : \mathfrak{p}|p\}$. Let (r_1, r_2) be the signature of K. Let K_S^T be the maximal pro-p

extension of K unramified outside S and totally decomposed at T. Put $\mathscr{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$; $\mathrm{A}_S^T := \mathscr{G}_S^{T\,\mathrm{ab}}$ and $\mathrm{A}_S^T/p := \mathscr{G}_S^{T\,\mathrm{ab}}/\mathscr{G}_S^{T\,ab,p}$. Of course, one has $d_p\mathrm{A}_S^T = d_p\mathscr{G}_S^T$ and for $S = T = \emptyset$, $\mathrm{A}_\emptyset^\emptyset(\mathrm{K}) = \mathrm{A}(K)$.

We are interested in constructing an example where the group $\mathscr{G}_S^T$ is a free pro-p group and T is not empty.

The following is a fundamental and classical result about the Euler characteristics of $\mathscr{G}_S^T$.

***Proposition 4.7* (Shafarevich and Koch).** — *Suppose that* K *contains the p-roots of the unity. Then,*

$$\mathrm{d}_p H^2(\mathscr{G}_S^T, \mathbb{F}_p) \leq d_p\mathrm{A}_T^S + |S| - 1$$

and

$$d_p\mathscr{G}_S^T = d_p\mathrm{A}_T^S + |S| - |T| - (r_1 + r_2) + \sum_{v \in S \cap S_p} [\mathrm{K}_v : \mathbb{Q}_p]\cdot$$

Proof. — See for example [**11**, Corollary 3.7.2, Appendix] for the bound for the H^2 and [**11**, Theorem 4.6, Chapter I, §4] for the H^1. □

The first inequality of the previous proposition would allow us to produce a free pro-p extension with complete splitting at the primes in T if $d_pA_T^S + |S| - 1 = 0$. On the other hand, if we apply the second line , let us read the second of Proposition 4.7 with the role of S and T reversed, we find that

$$d_p\mathrm{A}_T^S \geq |T| - (r_1 + r_2 + |S|).$$

We conclude that, under this strategy, $|T| \leq r_1 + r_2 + 1$, so this method is rather limited in scope.

Let us take $\mathrm{K} = \mathbb{Q}(\zeta_p)$ when p is regular and $S = S_p$. Then the group $\mathscr{G}_S^T$ will be pro-p free when A_T^S is trivial. As the p-class group of K is trivial, one has:

$$\mathrm{A}_T^S \simeq (\prod_{v \in T} \mathscr{U}_v)/\mathscr{O}_\mathrm{K}^S,$$

where $\mathscr{U}_v$ is the pro-p completion of the local units at v and where $\mathscr{O}_K^S$ is the group of S-units of K. Now, there are several types of scenarios where the quotient $(\prod_{v\in T} \mathscr{U}_v)/\mathscr{O}_\mathrm{K}^S$ is trivial. Let us give one. Suppose that $T = \{\ell\}$ where ℓ is inert in $\mathrm{K}/\mathbb{Q}$. Then $\mathscr{U}_\ell$ is isomorphic to the p-part of $\mathbb{F}_\ell^\times$. Hence, the global pth roots of unity will kill this part when $|\mathscr{U}_\ell| = p$ i.e. when $\ell^{p-1} - 1$ is exactly divisible by p. When this is the case, the group $\mathscr{G}_S^T$ is free on $(p-3)/2$ generators.

4.4. Incorporating the Galois action. — We can take these ideas a bit further by studying the Galois action. Throughout this subsection, we fix the following notation and assumptions (we still assume $p > 2$). Let K_0 be a number field, K/K_0 a cyclic extension of integer m co-prime to p. Put $\Delta = \mathrm{Gal}(\mathrm{K}/\mathrm{K}_0)$. Let $r = r_1(\mathrm{K}_0) + r_2(\mathrm{K}_0)$ be the number of archimedean places of K_0. Let S and T be two finite sets of places of K_0 such that $S \cap T = \emptyset$ and S contains S_p. By abuse of notation, the set of places of K above S and T are again called S and T respectively. Denote by S_{split} (resp. T_{split}) the set of places of S (resp. of T) splitting in K/K_0 an by S_{inert} (resp. T_{inert}) the set of places of S (resp. of T) not splitting in K/K_0. As in §1.2, the arithmetic objects of interest have a structure as $\mathbb{F}_p[\Delta]$-modules. We recall the following mirror identity from the book of Gras [**13**, Chapter II, §5.4.2]:

Theorem 4.8. — *Assume that $S_p \subset S$ and that* K *contains a primitive pth root of unity. Then:*

$$\omega\chi^{-1}(\mathrm{A}_S^T) - \chi(\mathrm{A}_T^S) = r\chi_{\mathrm{reg}} + \omega - \mathbf{1} + |S_{\mathrm{inert}}|\mathbf{1} + |S_{\mathrm{split}}|\chi_{\mathrm{reg}} - |T_{\mathrm{split}}|\chi_{\mathrm{reg}} - |T_{\mathrm{inert}}|\omega.$$

Proposition 4.9. — *Suppose that* K*, which is a cyclic degree p extension of* K_0*, contains a primitive pth root of unity and is p-rational. Then K_0, as well as every number field* K_n *in the cyclotomic extension* K_∞ *of* K *is also p-rational.*

Proof. — It is an obvious extension of Proposition 1.16. □

Now we assume that K_0 is totally imaginary and we take $S = S_p$.
By hypothesis, there is no abelian unramified p-extension of K in which p splits completely. Then for $T = \emptyset$, by Theorem 4.8, one has:

$$\omega\chi^{-1}(\mathrm{A}_S) = r\chi_{\mathrm{reg}} + \omega.$$

The group $\mathrm{A}_S(\mathrm{K}_0)$ corresponds by Class Field Theory to the Galois group of the maximal *abelian* pro-p extension of K_0 unramified outside S. The Galois group $\mathscr{G}_S(\mathrm{K}_0)$ is free on $r+1$ generators. The action of Δ on A_S/p being semi-simple, the $\mathbb{F}_p[\Delta]$-module $\mathrm{A}_S(\mathrm{K}_0)/p$ is isomorphic to A_S^T/p on which the Δ action is trivial.

By the Chebotarev Density Theorem, we can choose a set $T := \{\mathfrak{p}_0, \cdots, \mathfrak{p}_r\}$ of places of K_0 all inert in K/K_0, with $|T| = d_p A_S(\mathrm{K}_0) = r+1$, such that the Frobenius symbols $\sigma_{\mathfrak{p}_i}$, $i = 0, \cdots, r$, generate the p-group $\mathrm{A}_S(\mathrm{K}_0) \otimes \mathbb{F}_p$. By the choice of T, one has $\chi(\mathrm{A}_S^T) = \chi(\mathrm{A}_S) - |T|\mathbf{1}$. Thanks to Theorem 4.8 one then obtains:

$$\chi(\mathrm{A}_T^S) = \omega\chi^{-1}(\mathrm{A}_S^T) - \omega\chi^{-1}(\mathrm{A}_S) - |T|\omega = 0.$$

Then the maximal pro-p-extension of K unramified outside T and splitting at S, is trivial. One then uses Proposition 4.7 to obtain:

Proposition 4.10. — *Under the conditions of Proposition 4.9, and with $S = S_p$ and T as above, the pro-p-group $\mathscr{G}_S^T$ is free on $r(\ell-1)$ generators and*

$$\chi(\mathrm{A}_S^T) = r(\chi_{\mathrm{reg}} - \mathbf{1}).$$

Remark 4.11. — (*i*) The main point of Proposition 4.10 is that the action of σ on A_S^T is fixed-point-free, where $\Delta = \langle\sigma\rangle$.
(*ii*) By Proposition 4.9, the degree r can be taken arbitrarily large.

As corollary, one obtains:

Corollary 4.12. — *Assume the conditions of Proposition 4.10. Let* L/K_0 *be a sub-extension of* $\mathrm{K}_S^T/\mathrm{K}_0$ *such that* $\Gamma = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *is a uniform pro-p group. Then every (totally) inert (odd) prime* $\mathfrak{p} \subset \mathscr{O}_\mathrm{K}$ *in* K/K_0 *splits completely in* L/K*.*

4.5. Some heuristics on p-rationality. — Here we exploit some conjectures on p-rationality to get further heuristic evidence in direction of Conjecture 0.1. These are of two types. The first is in the spirit of the Leopoldt Conjecture – in a certain sense this is a transcendantal topic; the main reference is the recent work of Gras [**12**]. The second one is inspired by the heuristics of Cohen-Lenstra [**6**].

***Conjecture 4.13* (Gras, Conjecture 8.11 of [12])**. — *Let* K *be a number field. Then for* $p \gg 0$*, the field* K *is* p*-rational.*

Proposition 4.14. — *Let* $\mathbb{P}$ *be an infinite set of prime numbers and* m *an integer coprime to all* $p \in \mathbb{P}$*. Let* $(\Gamma_p)_{p\in\mathbb{P}}$ *be a family of uniform pro-*p *groups all of dimension* d *and all having a fixed-point-free automorphism of order* m*. If Conjecture 4.13 is true for some number field* K *of degree* mn*, then for all but finitely many primes* $p \in \mathbb{P}$*, the groups* Γ_p *have arithmetic realizations as Galois groups with arbitrarily large* μ*-invariant.*

Proof. — Let us take K_0 be a totally imaginary abelian number field of degree n over $\mathbb{Q}$ and let $\mathrm{K}_1/\mathbb{Q}$ be a degree m cyclic extension with $\mathrm{K}_0 \cap \mathrm{K}_1 = \emptyset$. Let $\mathrm{K} = \mathrm{K}_0\mathrm{K}_1$ be the compositum. Put $\langle\sigma\rangle = \mathrm{Gal}(\mathrm{K}/\mathrm{K}_0)$. Under Conjecture 4.13, one knows that for large p depending only on K, the field K is p-rational. One then applies Theorem 3.8. □

Example 4.15. — Let us fix $s \in \mathbb{N}$ and let $\mathbb{P}$ be the set of primes $p \equiv 1 \bmod 3$. Let $\Gamma(s,p)$ be the pro-p group $\Gamma(s)$ of dimension 3 introduced in §4.1. One can apply Proposition 4.14 to the family of groups $(\Gamma(s,p))_{p\in\mathbb{P}}$.

Let us consider another idea for studying p-rationality, in the spirit of the Cohen-Lenstra Heuristics [**6**]. For a prime number $p \geq 5$ and an integer $m > 1$ not divisible by p, let us consider the family $\mathscr{F}_m(\mathrm{K}_0)$ of cyclic extensions of degree m over a fixed p-rational number field K_0. Following the idea of Pitoun and Varescon [**31**], it seems reasonable to make the following conjecture:

Conjecture 4.16. — *Let us fix* p *and* m *as above. If* K_0 *is a* p*-rational quadratic imaginary field, the proportion of number fields* K *in* $\mathscr{F}_m(\mathrm{K}_0)$ *which are* p*-rational (counted according to increasing absolute value of the discriminant) is positive.*

Obviously, Conjecture 4.16 implies Conjecture 0.1.

References

[1] E.D. Bolker, *Inverse limits of solvable groups*, Proc. Amer. Math. Soc. **14** (1963), 147–152.

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

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

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

[5] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2**:1 (2003), 73–108.

[6] H. Cohen and H.W. Lenstra, Jr, *Heuristics on Class groups on Number Fields*, Number Theory, Noordwijkerhout 1983, Lecture Notes in Math., Vol. 1068, Springer 1984, 33-62.

[7] A.A. Cuoco, *Generalized Iwasawa invariants in a family*, Compositio Math. **51** (1984), 89-103.

[8] 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.

[9] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Annals of Mathematics. Second Series **109** (1979), no. 2, 377–395.

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

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

[12] G. Gras, *Les θ-régulateurs locaux d'un nombre algébrique – Conjectures p-adiques*, Canadian J. Math. **68** (2016), no. 3, 571-624.

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

[14] G. Gras and J.-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. **202** (1989), 343-365.

[15] R. Greenberg, *Galois representations with open image*, Ann. Math. Québec **40** (2016), no. 1, 83-119.

[16] F. Hajir and C. Maire, *On the invariant factors of class groups in towers of number fields*, Canadian J. Math. (2017).

[17] M. Harris, *p-adic representations arising from descent on abelian varieties*, Compositio Math. **39**:2 (1979), 177-245. With Correction: Compositio Math. **121**:1 (2000), 105-108.

[18] W.N. Herfort and L. Ribes,*On Automorphisms of Free Pro-p-Groups I*, Proc. Amer. Math. Soc. **108** (1990), no. 2, 287–295.

[19] S. Howson, *Euler Characteristics as invariants of Iwasawa modules*, Proc. London Math. Society **85** (2002) no. 3, 634-658.

[20] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japan **35** (1983), no. 4, 693-709.

[21] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions.* Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, pp. 1–11. Kinokuniya, Tokyo, 1973.

[22] J.-F. Jaulent and T. Nguyen Quang Do, *Corps p-réguliers, corps p-rationnels et ramification restreinte*, J. Théor. Nombres Bordeaux **5** (1993), 343-363.

[23] J. Gonzálo-Sánchez and B. Klopsch, *Analytic pro-p groups of small dimensions*, J. Group Theory **12** (2009), no. 5, 711–734.

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

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

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

[27] A. Movahhedi and T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, 155–200, Progr. Math., 81, Birkhäuser Boston, Boston, MA, 1990.

[28] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nachr. **149** (1990), 163–176.

[29] T. Nguyen Quang Do, *Formations de classes et modules d'Iwasawa*, Noordwijkerhout 1983, Lecture Notes in Math., Vol. 1068, Springer 1984, 167-185.

[30] G. Perbet, *Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques* (French) [On Iwasawa invariants in p-adic Lie extensions] Algebra Number Theory **5** (2011), no. 6, 819–848.

[31] F. Pitoun and F. Varescon, *Computing the torsion of the p-ramified module of a number field.* (English summary) Math. Comp. **84** (2015), no. 291, 371–383.

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

[33] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES, vol. **54** (1981), 123-201.

[34] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. **4**: (2002), 271–311.

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

September 14, 2018

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

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