# ON THE ANALYTICITY OF THE MAXIMAL EXTENSION OF A NUMBER FIELD WITH PRESCRIBED RAMIFICATION AND SPLITTING

*by*

Donghyeok Lim & Christian Maire

***Abstract.*** — We determine all the $p$-adic analytic groups that are realizable as Galois groups of the maximal pro-$p$ extensions of number fields with prescribed ramification and splitting under an assumption which allows us to move away from the Tame Fontaine-Mazur conjecture.

## Introduction

For a number field $K$, its absolute Galois group $G_K$ is a fundamental object of study. The last decades have shown that (continuous) Galois representations

$$\rho : G_K \to Gl_n(\mathbb{Q}_p)$$

occupy a central position in arithmetic geometry, serving as a fundamental tool to provide a bridge between the geometric and arithmetic aspects of number theory. A governing philosophy is the conjecture of Fontaine and Mazur [**3**, Conjecture 1] that an irreducible $p$-adic Galois representation of $G_K$ comes from a geometric object if it is unramified outside a finite set of primes and its restrictions to the decomposition subgroups at primes above $p$ are potentially semi-stable. A variation of the conjecture is the 'Tame Fontaine-Mazur conjecture' that if $S$ is a finite set of non-$p$ primes of $K$, then a $p$-adic analytic quotient of $G_K$ that is unramified outside $S$ is always finite ([**3**, Conjecture 5a]). This variation of

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

***Key words and phrases.*** — Pro-$p$ extensions of number fields, restricted ramification, Galois representations, $p$-adic analytic groups.

This work has been started during a visiting position for the second author at Ewha Womans University, and finished during a visiting fellow at the Western Academic for Advanced Research (WAFAR) of Western University; CM thanks the Department of Mathematics at Ewha University and the WAFAR for providing a beautiful research atmosphere. We would like to thank Bill Allombert for his help with PARI/GP, and Cécile Armana for useful remarks. We also would like to express our gratitude to the referees for their comments. The first author was supported by the Core Research Institute Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177) and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. NRF-2022R1I1A1A01071431). The second author was also partially supported by the EIPHI Graduate School (ANR-17-EURE-0002).

the conjecture has also been actively studied by using group-theoretic methods and has led to the development of the theory of pro-$p$ extensions of number fields.
A pro-$p$ group $G$ is isomorphic to a closed subgroup of $Gl_n(\mathbb{Z}_p)$ if and only if $G$ is analytic. Therefore, it is natural to study which $p$-adic analytic groups can be realized as $G_S^T$, which is a Galois group naturally defined in terms of ramification and splitting of places of number fields.

Let us be more precise. Let $S$ and $T$ be two finite and disjoint sets of places of $K$. Let $\bar{K}_S^T$ (resp. $K_S^T$) be the maximal (resp. the maximal pro-$p$) extension of $K$ unramified outside $S$ and completely decomposed at $T$. We put $\bar{G}_S^T := \bar{G}_{K,S}^T := Gal(\bar{K}_S^T/K)$ (resp. $G_S^T := G_{K,S}^T := Gal(K_S^T/K)$).
In this paper, we are interested in Galois representations $\rho : \bar{G}_{K,S}^T \to Gl_n(\mathbb{Q}_p)$ with $p$-closed image in $\bar{K}_S^T$, *i.e.* such that $H^1(ker(\rho), \mathbb{Z}/p) = 1$. More precisely, we want to characterize the possible $\mathbb{Q}_p$-Lie algebra $\mathscr{L}(\rho)$ of the image of $\rho$. For example, when $K = \mathbb{Q}$, $S = T = \varnothing$ then $\mathscr{L}(\rho) = \{0\}$ for every Galois representation $\rho$ of $\bar{G}_{K,\varnothing}^{\varnothing}$ since this Galois group is trivial.

Every *compact* $p$-adic analytic group contains a torsion free pro-$p$ group as an open subgroup. Hence by base change, one can assume that $S$ contains only finite places, and we can focus on $G_{K',S}^T$ for some finite extension $K'/K$ in $\bar{K}_S^T$.

In general, this question is difficult because it is not easy to determine whether $G_S^T$ is a FAb group *i.e.* if its open subgroups have finite abelianization. If $G_S^T$ is FAb, then the problem of determining the analyticity of $G_S^T$ shares many difficulties with the (Tame) Fontaine-Mazur conjecture mentioned before.
Thus to make the study more accessible, we assume the following condition $(C)$

$$1 + \delta_S > |T| + r_1 + r_2,$$

where $\delta_S$ denotes the sum $\sum_{\mathfrak{p}\in S'_p} [K_\mathfrak{p} : \mathbb{Q}_p]$ for $S'_p = \{\text{prime } \mathfrak{p} \in S, \mathfrak{p}|p\}$, and $r_1$ (resp. $r_2$) is the number of real (resp. complex) places of $K$. By the assumption $(C)$, the pro-$p$ group $G_S^T$ has $\mathbb{Z}_p$ as a quotient by class field theory (cf. [**5**, Chapter III, Theorem 1.6]). In particular, we move away from the Tame Fontaine-Mazur conjecture.

We first prove:

***Theorem A***. — *Assuming $(C)$, the pro-$p$ group $G_S^T$ is a $p$-adic analytic group if and only if, it is virtually isomorphic to:*

*(i)* $\mathbb{Z}_p$, *or*

*(ii)* $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ *(noncommutative), or*

*(iii)* $\mathbb{Z}_p \times \mathbb{Z}_p$.

*Moreover, we have* $\delta_S = r_1 + r_2 + |T|$.

Observe that when $G_S^T \simeq \mathbb{Z}_p$, then $G_S^T$ is potentially of local type. Here, *potentially of local type* means that there exists a prime $\mathfrak{p}|p$ of $K_S^T$ above a prime in $S$ such that the decomposition subgroup of $G_S^T$ at $\mathfrak{p}$ is open. This notion was studied by Wingberg in [**16**]. We will observe that if $\zeta_p \in K$, then $G_S^T$ is also potentially of local type in the cases $(ii)$ and $(iii)$.

Back to the original question: let $\rho : \bar{G}_{K,S}^T \to Gl_n(\mathbb{Q}_p)$ be a Galois representation with $p$-closed image in $\bar{K}_S^T$. Then in $(i)$ (resp. in $(iii)$) the Lie algebra $\mathscr{L}(\rho)$ is the abelian $\mathbb{Q}_p$-algebra of dimension 1 (resp. of dimension 2). In $(ii)$, $\mathscr{L}(\rho)$ is the noncommutative Lie algebra of dimension 2; $\mathscr{L}(\rho)$ can be generated by $x$ and $y$ satisfying the relation $[x, y] = x$.

It is easy to produce examples of type $(i)$ (namely when $K = \mathbb{Q}$ and $S = S_p$, the set of primes of $K$ that are $p$-adic). The examples of type $(ii)$ were studied by Wingberg [**16**] when $S_p \subset S$ and $T = \varnothing$. However, no example of type $(iii)$ was known. As the second result, one obtains:

***Theorem B***. — *Let $p$ be an odd prime. There is a number field $K$ and a finite set $T$ of primes of $K$ such that $G_{K,S_p}^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. The set $T$ is given by the Chebotarev density theorem.*

We remark that $\mathbb{Z}_p \times \mathbb{Z}_p$ cannot be realized as $G_S$ when $S$ contains $S_p$ because $G_S$ has Euler-Poincaré characteristic $-r_2$ whereas $\mathbb{Z}_p \times \mathbb{Z}_p$ has Euler-Poincaré characteristic 0. Hence, if $G_S$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, then $K$ is totally real. In that case, the $\mathbb{Z}_p$-rank of $G_S$ is 1 by Leopoldt conjecture.

By a numerical computation, we also find an example for $p = 2$ for which $G_S^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

***Example***. — *Take $K = \mathbb{Q}(\zeta_8)$. Let $\mathfrak{p}$ (resp. $\mathfrak{q}$) be the prime ideal $(2 + \zeta_8 + 2\zeta_8^2)$ (resp. $(6 - \zeta_8 + 6\zeta_8^2)$) of $K$ above 7 (resp. 71). Then, $G_{K,S_2}^{\{\mathfrak{p},\mathfrak{q}\}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.*

The paper contains three sections. In Section 1, we recall basic facts about pro-$p$ groups and arithmetic in pro-$p$-extensions of a number field. In Section 2, we prove Theorems A and B. The last section is devoted to some remarks. In particular, the proof of Theorem B allows us to compute a lower bound for the number of sets $T = \{\mathfrak{p}, \mathfrak{q}\}$ of primes of $K$ such that $N\mathfrak{p}, N\mathfrak{q} \leqslant X$, $G_{K,S_p}^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ which holds for generic pairs $(K, p)$ of an imaginary biquadratic field $K$ and an odd prime $p$ under the recent conjecture of Gras on $p$-rationality of number fields.

All calculations were performed using PARI/GP [**14**].

**Notations.** Throughout this article $p$ is a prime number.

- If $M$ is a finitely generated $\mathbb{Z}_p$-module, set $d_pM := dim_{\mathbb{F}_p} M/M^p$, $M[p] := \{m \in M, pm = 0\}$, and $\mathrm{rk}_{\mathbb{Z}_p} M = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$.
- Let $G$ be a finitely generated pro-$p$ group. Set $G^{ab} := G/[G, G]$, $G^{p,el} := G^{ab}/(G^{ab})^p$, and $d_pG := dim_{\mathbb{F}_p} G^{p,el}$. For $n \geqslant 1$, $(G_n)$ denotes the Zassenhaus filtration of $G$ (cf. [**8**, Chapter 7]).

## 1. Generalities on pro-$p$ groups and Galois groups with restricted ramification

In this section, we briefly recall basic facts that are necessary in this paper.

**1.1. The partial Euler-Poincaré characteristic of pro-$p$ groups.** — Let $G$ be a finitely generated pro-$p$ group. Recall that the cohomological dimension $cd(G)$ of a pro-$p$ group $G$ is defined to be the smallest integer $k$ such that $H^k(G,\mathbb{Z}/p) \neq 0$ and $H^{k+1}(G,\mathbb{Z}/p) = 0$.
Suppose that the groups $H^i(G,\mathbb{Z}/p)$ are finite for $i = 1, \cdots, n$. Then the $n$-th partial Euler-Poincaré characteristic $\chi_n(G)$ is defined to be

$$\chi_n(G) = \sum_{i=0}^{n} (-1)^i d_p H^i(G,\mathbb{Z}/p).$$

The cohomological dimension of a pro-$p$ group can be studied by the partial Euler-Poincaré characteristic according to the following theorem of Schmidt [**15**].

***Proposition 1.1***. — *Let $G$ be a pro-$p$ group such that $H^i(G,\mathbb{Z}/p)$ is finite for $0 \leqslant i \leqslant n$. Suppose that there is an integer $N$ such that $(-1)^n\chi_n(U) + N \geqslant (-1)^n(G:U)\chi_n(G)$ for all open subgroups $U$ of $G$. Then either $G$ is finite or $cd(G) \leqslant n$.*

We will apply Proposition 1.1 for $n = 2$. In that case, $\chi_2(G)$ is intimately related to the $\mathbb{Z}_p$-rank of $G^{ab}$. Let us write

$$G^{ab} \simeq \mathbb{Z}_p^t \oplus \mathscr{T},$$

where $\mathscr{T}$ is the torsion subgroup of $G^{ab}$. Recall the following well-known result.

***Proposition 1.2***. — *One has*

$$\chi_2(G) = 1 + d_p H_2(G,\mathbb{Z}_p) - t.$$

*Moreover, the group $G$ is free pro-$p$ if and only if $H^2(G,\mathbb{Q}/\mathbb{Z}) = 0$ and $\mathscr{T} = 1$.*

*Proof.* — By taking the $G$-homology of the exact sequence $0 \longrightarrow \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \longrightarrow \mathbb{Z}/p \longrightarrow 0$, we obtain the following exact sequence

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

Both claims follow from the isomorphism $H_1(G,\mathbb{Z}_p) \simeq G^{ab}$ and the duality between cohomology and homology groups. □

**1.2. On the pro-$p$ groups $G_S^T$.** — Let $K$ be a number field, and $S, T$ be two finite disjoint sets of primes of $K$. In this work, we will assume that $S$ consists only of finite places. Set

- $S_p$ : the set of primes of $K$ above $p$, $S'_p = S \cap S_p$, and $\delta_S := \delta_{S'_p} := \sum_{\mathfrak{p}\in S'_p} [K_\mathfrak{p} : \mathbb{Q}_p]$,
- $E^T := E_K^T$ the *pro-$p$ completion* of the group of $T$-units of $K$,
- $K_\mathfrak{p}$ the completion of $K$ at $\mathfrak{p}|p$, $U_\mathfrak{p}$ the group of units of $K_\mathfrak{p}$,
- $\mathscr{U}_S := \prod_{\mathfrak{p}\in S'_p} \mathscr{U}_\mathfrak{p}$, and $\mathscr{U}_\mathfrak{p} := \varprojlim_n U_\mathfrak{p}/U_\mathfrak{p}^{p^n}$ the pro-$p$ completion of $U_\mathfrak{p}$,
- $\delta := \delta_{K,p} = 1$ (resp. $\delta_\mathfrak{p} = 1$) if $\zeta_p \in K$ (resp. $\zeta_p \in K_\mathfrak{p}$), 0 otherwise,
- For every $\mathfrak{p} \in S\backslash S_p$, we assume that $\delta_\mathfrak{p} = 1$,
- $\varphi := \varphi_S^T : E^T \to \mathscr{U}_S$ the diagonal embedding of $E^T$ into $\mathscr{U}_S$,
- $V_S^T = \{x \in K^\times \mid v_\mathfrak{p}(x) \equiv 0 \mod p\ \forall \mathfrak{p} \notin T \ \&\ x \in K_\mathfrak{p}^{\times p}\ \forall \mathfrak{p} \in S\}$ where $v_\mathfrak{p}(x)$ denotes the discrete valuation of $x$ at $\mathfrak{p}$,
- $K_S^T/K$ the maximal pro-$p$ extension of $K$ unramified outside $S$ and completely decomposed at $T$; $G_S^T := G_{K,S}^T := Gal(K_S^T/K)$,

- $\mathscr{T}_S$ the torsion part of $G_S^{ab}$ (here $T = \varnothing$),
- If $L/K$ is a finite extension, by abuse we still denote $S := S_L := \{\mathfrak{P}|\mathfrak{p}, \mathfrak{p} \in S\}$.

The pro-$p$ group $G_S^T$ is well-known to be finitely presented. More precisely, one has

$$d_p G_S^T = 1 + \sum_{\mathfrak{p}\in S} \delta_{\mathfrak{p}} - \delta + d_p V_S^T / K^{\times p} + \delta_S - (r_1 + r_2 + |T|)$$

and

$$d_p H^2(G_S^T, \mathbb{Z}/p) \leqslant \sum_{\mathfrak{p}\in S} \delta_{\mathfrak{p}} - \delta + d_p V_S^T / K^{\times p} + \theta,$$

where $\theta$ is equal to 1 if $\zeta_p \in K$ and $S = \varnothing$, and zero in all other cases. (See [**13**, Chapter X, Theorem 10.7.10].)

Therefore, we have the inequality

$$\chi_2(G_S^T) \leqslant \theta + r_1 + r_2 + |T| - \delta_S.$$

In particular, assuming $(C)$, $\delta_S$ is positive. Thus, $S$ is non-empty and $\theta$ is zero, implying

$$\chi_2(G_S^T) \leqslant 0. \tag{1}$$

From the above explicit formulae of Shafarevich and Koch, we also have the following fact on the Schur multiplicator $H_2(G_S^T, \mathbb{Z}_p)$ of $G_S^T$ (cf. Lemme 3.1 of [**11**]).

***Lemma 1.3***. — *The $p$-rank of $H_2(G_S^T, \mathbb{Z}_p)$ is bounded above by $\theta + \mathrm{rk}_{\mathbb{Z}_p} ker(\varphi_S^T)$.*

*Proof.* — By Proposition 1.2 and the formulae of Shafarevich and Koch, we have the inequality

$$d_p H_2(G_S^T, \mathbb{Z}_p) = \chi_2(G_S^T) - 1 + \mathrm{rk}_{\mathbb{Z}_p} G_S^{T,ab} \leqslant -1 - \delta_S + r_1 + r_2 + |T| + \theta + \mathrm{rk}_{\mathbb{Z}_p} G_S^{T,ab}.$$

The claim follows from the equality $\mathrm{rk}_{\mathbb{Z}_p} G_S^{T,ab} = \delta_S - (r_1 + r_2 + |T| - 1) + \mathrm{rk}_{\mathbb{Z}_p} ker(\varphi_S^T)$. □

We study $G_{S_p}^T$ by considering it as a quotient of $G_{S_p}$ by the (normal subgroup generated by the) Frobenius automorphisms at the primes of $K_{S_p}$ above $T$. The key idea of the proof of Theorem B is as follows: for any finite quotient $G$ of $G_{S_p}$, we can use the Chebotarev density theorem to find some primes whose Frobenius restrict to any prescribed elements of $G$. Let us recall relatively strong properties of $G_{S_p}$. See [**13**, Proposition 8.3.18, Corollary 8.7.5, and Corollary 10.4.8].

***Theorem 1.4***. — *Suppose that $S$ contains $S_p$ and assume that $K$ totally imaginary if $p = 2$. The pro-$p$ group $G_S$ has cohomological dimension* 1 *or* 2*. Moreover, we have $\chi_2(G_S) = -r_2$.*

To make our strategy of using the Chebotarev density theorem as easy as possible, it is nice to consider the case when $G_S$ is free pro-$p$. Observe that if $G_S$ is free pro-$p$ then there is no tame ramification in $K_S/K$.

***Proposition 1.5***. — *Let $K$ be a number field and $S$ a finite set of places of $K$. If $ker(\varphi_S) = 1$ and $\mathscr{T}_S = 1$, then $G_S$ is free pro-$p$. The converse is also true if $S = S_p$. Furthermore, we have $d_p G_S = 1 + \delta_S - (r_1 + r_2)$.*

*Proof.* — This is a consequence of Proposition 1.2 and Lemma 1.3. Moreover when $S = S_p$, we have $\chi_2(G_{S_p}) = -r_2$ (see Theorem 1.4) which implies

$$d_p H_2(G_{S_p}, \mathbb{Z}_p) = \mathrm{rk}_{\mathbb{Z}_p} ker(\varphi_S).$$

Hence in this case, if $G_S$ is free pro-$p$, then we have $ker(\varphi_S) = 1$. □

Under the Leopoldt conjecture, $G_{S_p}$ is free pro-$p$ if and only if $\mathscr{T}_{S_p} = 1$. Even though the freeness of $G_{S_p}$ seems to be strong, it is believed to be a common phenomenon. In particular, we have the following conjecture.

***Conjecture 1.6* (Gras [4]).** — *Given a number field $K$, then $\mathscr{T}_{S_p} = 1$ for $p \gg 0$.*

To be complete, let us recall that when $G_{S_p}$ is free pro-$p$, then $K$ is said to be *$p$-rational* ([**12**]).

We finish this subsection with a well-known fact on the $\mathbb{Z}_p$-rank of $G_S^T$ [**5**]. By class field theory, the $\mathbb{Z}_p$-rank of the abelianization of $G_{K,S}^T$ is equal to the $\mathbb{Z}_p$-rank of the cokernel of the diagonal map $\varphi : E^T \to \mathscr{U}_S$. If $K/\mathbb{Q}$ is Galois, then considering Galois actions of $Gal(K/\mathbb{Q})$ is useful as in the following lemma which will be important in Theorem B.

***Lemma 1.7.*** — *Let $K/\mathbb{Q}$ be an imaginary biquadratic field. Let $K^+$ be its real quadratic subfield. Let $T$ be a non-empty finite set of non-$p$ primes of $K$. If the primes of $T$ are fixed by $Gal(K/K^+)$, then the $\mathbb{Z}_p$-rank of $G_{K,S_p}^T$ is 2.*

*Proof.* — Let $\mathbf{1}$ be the trivial $\mathbb{Q}_p$-character of $Gal(K/K^+)$, and $\chi$ be the nontrivial character. The character of the $\mathbb{Q}_p$-representation $\mathscr{U}_{S_p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is equal to $\mathbf{1} + \mathbf{1} + 2\chi$. On the other hand, the character of the $T$-units is $(|T| + 1)\mathbf{1}$. Hence, the character of the image of $\varphi_{S_p}^T$ is contained in the isotypic component at $\mathbf{1}$. It is precisely $\mathbf{1} + \mathbf{1}$ because for any non-$p$ prime $\mathfrak{p}$ of $K$, the $\mathbb{Z}_p$-rank of $G_{K,S_p}^{\{\mathfrak{p}\}}$ is strictly smaller than $G_{K,S_p}$; $\mathfrak{p}$ does not split completely in the cyclotomic $\mathbb{Z}_p$-extension of $K$. □

## 2. Proof of the main results

In this section, we prove the main theorems of this work. They completely give answer to the question of the realizability of analytic groups as $G_{K,S}^T$ under the assumption $(C)$.

### 2.1. Proof of Theorem A. —

***Theorem 2.1.*** — *Assuming $(C)$, the pro-$p$ group $G_S^T$ is a $p$-adic analytic group if and only if it is virtually isomorphic to one of $\mathbb{Z}_p$, $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ (noncommutative), and $\mathbb{Z}_p \times \mathbb{Z}_p$. In particular, we have $\delta_S = r_1 + r_2 + |T|$.*

*Proof.* — The proof combines the argument of Proposition 3.3 of [**11**] and properties of $p$-adic analytic groups ([**2**]). Suppose that $G_S^T$ is $p$-adic analytic, then the $p$-rank of open subgroups $U$ of $G_S^T$ are uniformly bounded. Hence, the $\mathbb{Z}_p$-ranks of $U$ are also uniformly bounded. If $L$ is the subfield of $K_S^T$ fixed by an open subgroup $U$, then we have the following equality

$$rk_{\mathbb{Z}_p} U^{ab} = [L : K](\delta_S - (r_1 + r_2 + |T|)) + 1 + rk_{\mathbb{Z}_p} ker(\varphi_{L,S}^T). \tag{2}$$

Hence, if $G_S^T$ is $p$-adic analytic, then necessarily we have

(*a*) $\delta_S = r_1 + r_2 + |T|$ and,

($b$) the rank of the kernel of $\varphi_S^T$ is bounded along $K_S^T/K$.

By Lemma 1.3, ($b$) implies that the $p$-rank of $H_2(U, \mathbb{Z}_p)$ is uniformly bounded for all open subgroups $U$ of $G_S^T$. By Proposition 1.2, $|\chi_2(U)|$ for open subgroups $U$ of $G_S^T$ are uniformly bounded. Since $\chi_2(G)$ is non-positive by the assumption ($C$) (see (1)), for some sufficiently large integer $N$, we have $\chi_2(U) + N \geqslant (G : U)\chi_2(G)$ for all $U$. Therefore, either $G_S^T$ is finite or $cd(G_S^T) \leqslant 2$ by Proposition 1.1. By the assumption ($C$), the pro-$p$ group $G_S^T$ is never finite. One concludes thanks to the classification of the $p$-adic analytic groups of dimension 2 (see [**10**, §7]). □

Observe that when $G_S^T \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$, whether it is commutative or not is related to the behavior of $\ker(\varphi_{L,S}^T)$ for number fields $L$ in $K_S^T/K$.

***Proposition 2.2***. — *Suppose that $G_S^T$ is a uniform pro-p group of dimension 2. Then $\mathrm{rk}_{\mathbb{Z}_p} \ker(\varphi_{L,S}^T) \in \{0, 1\}$ is constant along $K_S^T/K$. Moreover, $\mathrm{rk}_{\mathbb{Z}_p} \ker(\varphi_{L,S}^T) = 1$ if and only if $G_S^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

*Proof.* — The claim follows from the classification of uniform pro-$p$ groups of rank 2, the formula (2), and the conclusion (a) in the proof of Theorem A. □

**2.2. Proof of Theorem B.** — Now, let us prove that $\mathbb{Z}_p \times \mathbb{Z}_p$ can be realized as a Galois group $G_{K,S_p}^T$ for a number field $K$ and a finite set $T$ of primes of $K$. We use the $p$-rational number fields.

Take $p$ odd. Let $K$ be an imaginary biquadratic $p$-rational field. The existence of such a number field is already known from the works [**1, 9**]. We will take $S = S_p$. Then, $T$ is necessarily equal to $\{\mathfrak{p}, \mathfrak{q}\}$ for some non-$p$ primes of $K$ by the conclusion ($a$) of Theorem A. Suppose that $\mathfrak{p}$ is a non-$p$ prime of $K$ whose Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p}}$ in $G_{S_p} := G_{K,S_p}$ represents a non-trivial element in the vector space $(G_{S_p})^{p,el} \simeq \mathbb{F}_p^3$. Then we have the following easy lemma.

***Lemma 2.3***. — *The pro-p group $G_{S_p}^{\{\mathfrak{p}\}}$ is free pro-p on 2 generators.*

If $\mathfrak{q}$ is a non-$p$ prime of $K$ distinct from $\mathfrak{p}$, then for the set $T = \{\mathfrak{p}, \mathfrak{q}\}$, $G_{S_p}^T$ is a one relator pro-$p$ group of rank 2 unless it is isomorphic to $\mathbb{Z}_p$.

A main difficulty in proving $G_{S_p}^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ is that we cannot apply the Chebotarev density theorem in an infinite Galois extension. However, if $G_{S_p}^T$ is already known to be a one relator pro-$p$ group, then we can use the Chebotarev density theorem for $\mathfrak{q}$ in a finite quotient of $G_{S_p}^{\{\mathfrak{p}\}}$ to guarantee that $G_{S_p}^T$ is a Demushkin pro-$p$ group.

***Proposition 2.4***. — *Let $S$ and $T$ be disjoint and finite sets of primes of $K$ such that $\delta_S = r_1 + r_2 + |T|$. Suppose that $(G_{K,S}^T)^{ab} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Let $K_1, \cdots, K_{p+1}$ be the $p+1$ degree-p extensions of $K$ in $K_S^T/K$. Then $G_{K,S}^T \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ if and only if*

$$d_p G_{K_1,S}^T = \cdots = d_p G_{K_{p+1},S}^T = 2.$$

*Proof.* — One direction is obvious.

Suppose now that $d_p G_{K_1,S}^T = \cdots = d_p G_{K_{p+1},S}^T = 2$. Then by Schreier's formula, the pro-$p$ group $G_{K,S}^T$ is not free. Moreover by hypothesis and (1), one has $d_p H^2(G_S^T, \mathbb{F}_p) \leqslant 1$. Therefore, $G_{K,S}^T$ is a pro-$p$-group with one relator. By the assumption on $d_p G_{K_i,S}^T$ and [**13**, Chapter III, Theorem 3.9.15], $G_{K,S}^T$ is a Demushkin group (on two generators). We are done since Demushkin pro-$p$ groups are uniquely determined by their abelianizations. □

Proposition 2.4 provides us a simple criterion to check numerically whether $G^T_{K,S}$ is Demushkin with existing algorithms. It also implies that whether $G^T_{K,S}$ is Demushkin is determined by the class of the Frobenius at $\mathfrak{q}$ in the quotient of $G^{\{\mathfrak{p}\}}_{K,S}$ by the Frattini subgroup of the Frattini subgroup of $G^{\{\mathfrak{p}\}}_{K,S}$ which is *finite*. We can understand this also in the following way.

***Proposition 2.5***. — *Let $F$ be a free pro-$p$ group of generator rank 2 with generators $x, y \in F$. Let $r$ be an element of $F_2 = F^p(F, F)$. Set $R$ to be the smallest normal closed subgroup of $F$ generated by $r$. Then the quotient group $F/R$ is Demushkin if and only if $r$ is congruent to $[x, y]^i$ modulo $F_3$ for an $i \in \mathbb{Z}$ prime to $p$.*

*Proof.* — The group $G = F/R$ is an one-relator pro-$p$ group of rank 2. Observe that $i \in (\mathbb{Z}/p)^\times$ if and only if the cup-product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is non-trivial (cf. [**13**, Chapter III, Proposition 3.9.13 (ii)], [**8**, Theorem 7.23]). Since $H^1(G, \mathbb{F}_p)$ has $p$-rank 2, this is equivalent to the non-degeneracy of the cup-product. □

Theorem B is implied by the following theorem.

***Theorem 2.6***. — *Let $p$ be an odd prime and let $K$ be an imaginary biquadratic $p$-rational field. Then there are infinitely many sets $T$ of primes of $K$ with $|T| = 2$ such that $G^T_{K,S_p}$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.*

*Proof.* — Let $K$ be an imaginary biquadratic field that is $p$-rational [**1, 9**]: the pro-$p$ group $G_{K,S_p}$ is free pro-$p$ of rank 3 (see Proposition 1.5). Let $K^+$ be the real quadratic subfield of $K$; we put $\Delta = Gal(K/K^+)$ and $s$ the generator of $\Delta$. Let $\mathfrak{p}$ be a prime of $K^+$ which is inert in $K^+_\infty K/K^+$ where $K^+_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $K^+$. Then $G^{\{\mathfrak{p}\}}_{K,S_p}$ is free pro-$p$ of rank 2 by Lemma 2.3. We remark that $(G^{\{\mathfrak{p}\}}_{K,S_p})^{p,el}$ is isomorphic to $\mathbb{F}_p^- \oplus \mathbb{F}_p^-$ as $\mathbb{F}_p[\Delta]$-modules.

Set $F := G^{\{\mathfrak{p}\}}_{K,S_p}$. Let $x, y$ be a system of minimal topological generators of $F$. By [**7**] the elements $x$ and $y$ can be chosen such that $x^s = x^{-1}$ and $y^s = y^{-1}$, where $x^s$ and $y^s$ denote the image of the conjugate action of $s$ on $x$ and $y$ respectively. Denote by $(F_n)$ the Zassenhaus filtration of $F$.

Set $T = \{\mathfrak{p}, \mathfrak{q}\}$. If $G^T_{K,S_p}$ is not isomorphic to $\mathbb{Z}_p$, then it is a one relator pro-$p$ group of rank 2. Suppose that a finite prime $\mathfrak{q}$ of $K$ satisfies the following two conditions:

- $(a)$ $\mathfrak{q}$ is lying over a prime of $K^+$ that is inert in $K/K^+$, and
- $(b)$ the Frobenius automorphism in $F$ corresponding to a prime of $K^{\{\mathfrak{p}\}}_{S_p}$ above $\mathfrak{q}$ is congruent to $[x, y]^i$ modulo $F_3$ for some $i \in \mathbb{Z}$ that is coprime to $p$.

The condition $(b)$ implies that $G^T_{K,S_p}$ is Demushkin by Proposition 2.5. On the other hand, the $\mathbb{Z}_p$-rank of $(G^T_{K,S_p})^{ab}$ is 2 by $(a)$ and Lemma 1.7. Hence, $G^T_{K,S_p}$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Let us now prove the existence of such a prime $\mathfrak{q}$. By the choice of $\mathfrak{p}$, the extension $K^{\{\mathfrak{p}\}}_{S_p}/K^+$ is Galois with Galois group isomorphic to $F \rtimes \Delta$ by the Schur-Zassenhaus theorem. Let $M$ be the subfield of $K^{\{\mathfrak{p}\}}_{S_p}$ fixed by $F_3$: the field $M$ is still Galois over $K^+$ and we have $Gal(M/K^+) \simeq Gal(M/K) \rtimes \Delta$. Let us use $x, y$ to denote also their images in $Gal(M/K)$. Take $j \in \mathbb{Z}$ coprime to $p$. By the Chebotarev density theorem, there is a prime $\mathfrak{q}$ of $K^+$ such that the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{Q}}$ in $Gal(M/K^+)$ at a prime

$\mathfrak{Q}$ of $M$ above $\mathfrak{q}$ is in the conjugacy class of $([x,y]^j, s) \in Gal(M/K^+)$. The restriction of $\mathrm{Frob}_{\mathfrak{Q}}$ to $K$ is $s \in \Delta$. Therefore, the prime $\mathfrak{q}$ is inert in $K/K^+$. By definition, $(\mathrm{Frob}_{\mathfrak{Q}})^2$ is the Frobenius automorphism of $Gal(M/K)$ at $\mathfrak{Q}$, and this Frobenius automorphism is equal to $([x,y]^{j(1+s)}, 1) = (([x,y][x^{-1}, y^{-1}])^j, 1) \in Gal(M/K)$. An easy computation in the Magnus algebra of $F$ shows that $[x^{-1}, y^{-1}] \equiv [x,y]$ modulo $F_3$. Therefore, $(\mathrm{Frob}_{\mathfrak{Q}})^2$ satisfies the condition $(b)$. If we take $T = \{\mathfrak{p}, \mathfrak{q}\}$, then $G^T_{K,S_p}$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. □

***Remark 2.7***. — Take $K/K^+$, $S$ and $T$ as before. Let $T_0$ be any set of primes $\mathfrak{p}$ of $K^+$ inert in $K/K^+$: by [**6**, Corollary 3.2] these primes split completely in $K^T_S/K$. Then $G^{T\cup T_0}_S \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Hence, the assumption $(C)$ is not absolutely necessary.

***Example 2.8***. — Let $K$ be the number field $\mathbb{Q}(\zeta_8)$, and let $\theta$ be a fixed primitive 8th root of unity. Then $K$ is 2-rational. Let $\mathfrak{p}_7$ (resp. $\mathfrak{p}_{71}$) be the prime ideal $(2+\theta+2\theta^2)$ (resp. $(6-\theta+6\theta^2)$) of $K$ above 7 (resp. 71). Set $T = \{\mathfrak{p}_7, \mathfrak{p}_{71}\}$. By Lemma 1.7, $(G^T_{S_2})^{ab}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
We can check that $K_1 = K(\sqrt{\theta})$, $K_2 = K(\sqrt{\theta^3-\theta^2+1})$, and $K_3 = K(\sqrt{-\theta^3+\theta-1})$ are the three quadratic extensions of $K$ in $K^T_{S_2}/K$. A computation shows that $d_2 G^T_{K_i,S_2} = 2$, for $i = 1,2,3$. Hence, $\mathfrak{p}_{71}$ does not split completely in $K^{\{\mathfrak{p}_7\}}_{S_2}$, and the pro-2 group $G^T_{S_2}$ is defined by two generators and one relation. By Proposition 2.4, one concludes that $G^T_{S_2} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

## 3. Some remarks

**3.1. When $G^T_S$ is of local type.** — When $G^T_S \simeq \mathbb{Z}_p$, $G^T_S$ must be potentially of local type by the finiteness of the class group. We can generalize this to all $p$-adic analytic $G^T_S$ under some hypothesis.

***Proposition 3.1***. — *Suppose that the assumption $(C)$ is true and $G^T_S$ is $p$-adic analytic. If $\zeta_p \in K$, then $G^T_S$ is of local type if $p > 2$ and potentially of local type if $p = 2$.*

*Proof.* — Let $L$ be a finite extension of $K$ in $K^T_S$. There is a finite extension $K'$ of $K$ containing $L$ such that $Gal(K^T_S/K')$ is a uniformly powerful open subgroup of $G^T_S$. By Theorem A, we have $d_p Gal(K^T_S/K') \leqslant 2$. By the formulae of Shafarevich and Koch and the conclusion $(a)$ of Theorem A, we have the inequality

$$\sum_{\mathfrak{p}\in S'_K} \delta_{\mathfrak{p}} + d_p V^T_{K',S}/K'^{\times p} \leqslant 2.$$

Therefore, $|S_L \cap S_p| \leqslant |S_{K'} \cap S_p|$ is at most 2. Since $L$ is arbitrary, each $p$-adic prime $\mathfrak{p}_0 \in S$ of $K$ splits into at most two primes in $K^T_S$. Hence, the decomposition group $G_{\mathfrak{p}_0}$ of $\mathfrak{p}_0$ in $K^T_S/K$ is exactly $G^T_S$ if $p$ is odd, and an open subgroup of $G^T_S$ if $p = 2$. □

**3.2. Quantities on $T$ with $G^T_{S_p} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.** — Let $K$ be an imaginary biquadratic number field and $p$ an odd prime. Let $K^+$ be the real quadratic subfield of $K$; we put $\Delta = Gal(K/K^+)$. For $X \geqslant 2$, set

$$A(X) = \left\{\{\mathfrak{p}, \mathfrak{q}\} \text{ a set of primes of } K \;\middle|\; N_{K/\mathbb{Q}}\mathfrak{p}, N_{K/\mathbb{Q}}\mathfrak{q} \leqslant X,\ G^{\{\mathfrak{p},\mathfrak{q}\}}_{K,S_p} \simeq \mathbb{Z}_p \times \mathbb{Z}_p\right\}.$$

By the conjecture of Gras, the proof of Theorem B gives us the following statistics of $|A(X)|$ for generic couples $(K, p)$.

***Proposition 3.2.*** — *Let $p$ be an odd prime and $K$ an imaginary biquadratic $p$-rational number field. Then as $X \to \infty$*

$$|A(X)| \geqslant c_p \frac{X}{(\log X)^2},$$

*where $c_p$ is some constant depending on $p$.*

It is easy to understand that $|A(X)|$ is very small compared to $(X/\log X)^2$ because the primes $\mathfrak{p}$ and $\mathfrak{q}$ have residue class degrees larger than 1.

*Proof.* — We will compute a lower bound for the number of $T$ in the proof of Theorem B. Let $K'$ be the first layer of the cyclotomic $\mathbb{Z}_p$-extension of $K$. Let $K_2 := K_p^{p,el}$ be the maximal elementary abelian $p$-extension of $K$ that is unramified outside $p$ ; $Gal(K_2/K) \simeq G_{K,S_p}^{p,el}$. Following the proof of Theorem B, observe that the prime $\mathfrak{p}$ is inert in $K'/K$. Let $M$ be as in the proof of Theorem B. Set $M' = MK'$. Observe that $Gal(M'/K) \simeq Gal(K'/K) \times Gal(M/K)$. Let us choose a prime $\mathfrak{q}$ such that its Frobenius automorphism in $Gal(M'/K)$ has trivial component at $Gal(K'/K)$ and its restriction to $M$ is as in the proof of Theorem B. By this choice, $\mathfrak{q}$ splits completely in $K_2/K$, and there is no symmetry between $\mathfrak{p}$ and $\mathfrak{q}$.

By using the argument of the proof of Theorem B, we can check that the number of $\mathfrak{p}$ that is inert in $K/K^+$ such that $G_{K,S_p}^{\{\mathfrak{p}\}}$ is free pro-$p$ of rank 2 and $N_{K/\mathbb{Q}}\mathfrak{p} \leqslant X$ is asymptotically

$$\frac{(p-1)\sqrt{X}}{p \log X} \tag{3}$$

as $X \to \infty$ by applying the Chebotarev density theorem in $K_2/K^+$. For each aforementioned $\mathfrak{p}$, let $N_{\mathfrak{p}}(X)$ be the number of primes $\mathfrak{q}$ of $K$ with $N_{K/\mathbb{Q}}\mathfrak{q} \leqslant X$ such that $\mathfrak{q}$ splits in $K'$, $\mathfrak{q}$ is equal to its conjugate over $K^+$, and its Frobenius automorphism is in the conjugacy class of $([x,y]^j, s) \in Gal(M/K^+)$ for some $j$ coprime to $p$. If $F$ is free pro-$p$ of rank 2, then we have $(F : F_3) = p^3$ and $(M' : K^+) = 2p^4$. Therefore, $N_{\mathfrak{p}}(X)$ is asymptotically

$$\frac{(p-1)\sqrt{X}}{p^4 \log X} \tag{4}$$

as $X \to \infty$ by applying the Chebotarev density theorem in $M'/K^+$. We conclude thanks to the proof of Theorem B, (3), and (4). In particular, $c_p$ is bounded below by $(p-1)^2/p^5$. □

**3.3. Other pro-$p$ groups of the form $G_S^T$.** — Using a similar argument, we can study the statistics of the sets $T = \{\mathfrak{p}, \mathfrak{q}\}$ of primes of imaginary biquadratic $p$-rational fields $K$ such that $G_{S_p}^T$ is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ (noncommutative). The number of the sets $T = \{\mathfrak{p}, \mathfrak{q}\}$ with $G_{S_p}^T \simeq \mathbb{Z}_p$ and $N_{K/\mathbb{Q}}\mathfrak{p}, N_{K/\mathbb{Q}}\mathfrak{q} \leqslant X$ is asymptotically equal to

$$\frac{(p^3-1)(p^2-1)}{2p^5} \frac{X^2}{(logX)^2}$$

as $X \to \infty$. On the other hand, the number of the sets $T = \{\mathfrak{p}, \mathfrak{q}\}$ with $G_{S_p}^T \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ (noncommutative) and $N_{K/\mathbb{Q}}\mathfrak{p}, N_{K/\mathbb{Q}}\mathfrak{q} \leqslant X$ is asymptotically equal to

$$\frac{(p^3-1)(p^2-1)}{2p^7} \frac{X^2}{(logX)^2}$$

as $X \to \infty$. The statistics for $\mathbb{Z}_p$ come from the fact that a quotient of the free pro-$p$ group of rank 3 by two elements is isomorphic to $\mathbb{Z}_p$ if and only if the classes of two elements in the maximal elementary abelian quotient are linearly independent. The statistics for $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ (noncommutative) can be computed by noting that at least one of $\mathfrak{p}$ and $\mathfrak{q}$ does not belong to the Frattini subgroup of $G_{S_p}$ and applying Proposition 2.5. We can disregard the possibility of $G_{S_p}^T \simeq \mathbb{Z}_p^2$ because the number in Section 3.2 is negligible.

## References


[1] Y. Benmerieme, and A. Movahhedi. *Multi-quadratic p-rational number fields*, Journal of Pure and Applied Algebra **225** (2021), n9, 106657.

[2] 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.

[3] 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.

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

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

[6] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, Math. Proc. of the Cambridge Philosophical Soc. **166** (2019), 599-617.

[7] W. N. Herfort and L. Ribes, *On Automorphisms of Free Pro-p-Groups I*, Proceedings of the American Mathematical Society, **108** (1990), No. 2, 287-295.

[8] H. Koch, Galois Theory of $p$-extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin 2002.

[9] J. Koperecz, *Triquadratic p-rational fields*, Journal of Number Theory **242** (2023), 402-408.

[10] J. González-Sánchez, B. Klopsch, *Analytic pro-p groups of small dimensions*, Journal of Group Theory **12** (2009), no.5, 711-734.

[11] 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.

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

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

[14] The PARI Group, PARI/GP-2.15.3, Univ. Bordeaux, 2023, http://pari.math.u-bordeaux.fr/.

[15] A. Schmidt, *Bounded defect in partial Euler characteristics*, Bull. London Math. Soc. **28** (1996), 463-464.

[16] K. Wingberg, *Galois groups of local and global type*, J. Reine Angew. Math. **517** (1999), 223–239.



*May 1, 2024*



Donghyeok Lim, Institute of Mathematical Sciences, Ewha Womans University, Seoul 03760, Republic of Korea • *E-mail :* donghyeokklim@gmail.com

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