MASSEY PRODUCTS AND UNIPOTENT EXTENSIONS WITH RESTRICTED RAMIFICATION

by

Oussama Hamza, Donghyeok Lim & Christian Maire

Dedicated to Ján Mináč on his 71st birthday

Abstract. — We fix a prime p and construct new cases of pro-p extensions of number fields with restricted ramification and splitting, whose Galois groups decompose as coproducts of pro-p absolute Galois groups of local fields. As a consequence, these pro-p extensions satisfy the strong Massey vanishing property and thus admit large unipotent quotients.

Introduction

Context. — The absolute Galois group of a field is a fundamental object in algebra and arithmetic. A natural and longstanding question is:

Which profinite groups can be realized as absolute Galois groups of fields?

In general, fully understanding the structure of absolute Galois groups is highly mysterious and notoriously difficult. A common approach is therefore to fix a prime p and study the maximal pro-p quotient, known as the pro-p absolute Galois group. For number fields, it is common to consider further quotients of the pro-p absolute Galois group by restricting the ramification. In this context, presentations of pro-p groups in terms of generators and relations play a central role. A pioneering result was given by Golod and Shafarevich in the 1960s [**4**], who used the idea of presentation to construct the first examples of infinite p-class field towers. Their method was systematically extended to the setting of pro-p absolute Galois groups unramified outside finite sets S of primes, which we denote by G_S (a detailed introduction to these Galois groups can be found in [**12**]).

2000 ***Mathematics Subject Classification.*** — 55S30, 11R32, 12G05, 20E06, 20F05.
Key words and phrases. — Pro-p extensions with restricted ramification and splitting, Mild presentations, Massey products, Unipotent representations.

The first and third authors gratefully acknowledge the support of the Western Academy for Advanced Research (WAFAR) in Western University, during the year 2022/23 and the Institute for Advanced Studies in Mathematics (IASM) in Harbin Institute of Technology, during the summer 2025. The third author is grateful to WAFAR and IASM for support during visits in summers 2023 and 2025. The third author was partially supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne Franche-Comté Region. The second author was supported by the National Research Foundation of Korea (NRF) grants No. RS-2024-00462910. The authors thank Elyes Boughattas for his comments and interest in this paper.

When S contains all p-adic places (i.e. in the wildly ramified case), the study of G_S motivated the development of the Poitou–Tate duality theory. Further study of these wildly ramified pro-p extensions, often guided by analogies with the theory of Riemann surfaces, produced explicit presentations of G_S in various cases.
In the early 2000s, Labute [**13**] introduced the notion of *mild* pro-p groups (see §1.2 for definition) for odd primes p to provide examples of tamely ramified G_S of cohomological dimension 2. These pro-p groups are infinite and FAB (i.e. every open subgroup has finite abelianization), a property that follows from class field theory. This result was later extended to the case $p = 2$ by Labute and Mináč in [**14**]. Labute's idea has since inspired a range of further developments. Notably, Schmidt [**34**] proved a general result showing that, by suitably enlarging the set S to allow additional tame ramification, the Galois groups G_S become mild.

Massey products, originally introduced in a geometrical context (see [**19**]) as finer group invariants than cohomology algebras, were independantly used by Morishita [**28**] and Vogel [**37**] to extract information about the presentations of G_S. Gärtner [**3**] further connected these results with mild presentations. Building on Dwyer's works [**2**], which established a connection between Massey products and unipotent representations, Mináč and Tân conjectured the following two necessary conditions for pro-p groups to be isomorphic to the pro-p absolute Galois group G_K of a field K.

(i) The Kernel Unipotent Conjecture [**23**, Conjecture 1.3] predicts that the Zassenhaus filtration of G_K, when K contains a primitive p-th root of the unity ζ_p, is given by the kernels of unipotent representations.

(ii) The Massey vanishing conjecture, which is the main focus of this paper, was first formulated in [**25**] under the assumption $\zeta_p \in K^\times$, and later extended to a more general form in [**24**]. The conjecture can be formally stated as follows:

***Conjecture* (Mináč-Tân).** — *Let G_K be a pro-p absolute Galois group of a field K. Then G_K satisfies the Massey vanishing property.*

We refer the reader to §1.1.1 for the relevant definitions. This conjecture has been the subject of active research over a wide range of base fields (see, for example [**21**] for a detailed overview of known results). In the arithmetic context, Mináč and Tân [**25**, Theorem 4.3] showed the conjecture for G_K, when K is a local field. Subsequently, Guillot, Mináč, Topaz and Wittenberg [**8**] verified the Massey vanishing property in the case $n = 4$ and $p = 2$, for G_K when K is a number field. Finally, Harpaz and Wittenberg [**10**] completely resolved the conjecture for number fields.

Let G be a pro-p group, and let $n \geqslant 3$ be an integer. For an n-tuple $(\chi_1, \ldots, \chi_n)$ of homomorphisms from G to $\mathbb{F}_p$, if the Massey product $\langle \chi_1, \ldots, \chi_n \rangle$ is defined (see § 1.1.1 for definition), then the cup products $\chi_j \cup \chi_{j+1}$ vanish for all $1 \leqslant j \leqslant n-1$. This motivates the following properties on G, known as the strong Massey vanishing property:

If $\chi_j \cup \chi_{j+1} = 0$ for all $1 \leqslant j \leqslant n-1$, then the Massey product $\langle \chi_1, \ldots \chi_n \rangle$ vanishes.

Mináč and Tân [**26**] studied this property for pro-p absolute Galois groups. However, its validity turns out to be more delicate. Harpaz and Wittenberg showed that the strong Massey vanishing property does not hold for G_K, when K is a number field containing an 8-th primitive root of the unity [**8**, Appendix]. Merkurjev and Scavia [**20**] generalized the previous argument for several other fields.

By contrast, the third author, together with Mináč, Ramakrishna, and Tân [**18**] verified the strong Massey vanishing property for G_K, when K is a number field not containing the p-th roots of unity, and its tame absolute quotient. These contrasting results illustrate the increased complexity that the presence of the p-th roots of unity in K may bring to the study of G_K.

Results. — In this work, we study the strong Massey vanishing property in the context of restricted ramification, and we use it to construct unipotent extensions of number fields with small number of ramified primes. By a unipotent extension, we mean a Galois extension whose Galois group is isomorphic to $\mathbb{U}_n \coloneqq \mathbb{U}_n(\mathbb{F}_p)$, the group of $n \times n$ upper triangular unipotent matrices over $\mathbb{F}_p$.

It has been observed that realizing a finite group as a Galois group comes at the cost of introducing significant ramification. If K does not contain ζ_p, the generalization of the Scholz-Reichardt method from $\mathbb{Q}$ to K already requires a nontrivial amount of ramification. When $\zeta_p \in K$, the situation becomes considerably more difficult. For example, for general fields K, no general reasonable upper bound is known for the number of ramified primes needed to realize arbitrary 2-groups (see, for instance, [**33**]). This again shows that the presence of ζ_p in the base field K affects the complexity of studying G_K.

On the other hand, wild ramification enables the construction of a variety of finite p-groups G as Galois groups over number fields unramified outside p. Specifically, for a prime p and a number field K with r_2 complex places, the Galois group of the maximal pro-p extension of K unramified outside p is often a free pro-p group of rank $r_2 + 1$ (see p-rationality in §2.3). By the universal property of free pro-p groups, any finite p-group G with generator rank at most r_2+1 can then be realized as a Galois group over K, unramified outside p. In particular, we can easily demonstrate that any finite p-group G can be realized as a Galois group $Gal(L/K')$ over some number field K' such that the extension L/K' is unramified outside p.

However, using only wild ramification has limitations when the base field is fixed, as the generator rank of such Galois groups is bounded by $r_2 + 1$. To go beyond this, it is necessary to allow tame ramification. Inspired by Wingberg [**38**], Movahhedi [**29**] and, Jaulent and Sauzet [**11**], we study new situations where pro-p extensions with restricted ramification and splitting condition is a coproduct of free and Demushkin components. These groups check the strong Massey vanishing property, which allows us in the best situation to infer unipotent quotients with generator rank $2r_2 + 2$, which is twice the maximal generator rank allowed in the purely wild case.

Let us introduce notations before stating our results. Let K be a number field of signature (r_1, r_2). Let S and T be finite sets of primes of K such that T is disjoint from S, and let S_p denote the set of primes of K lying above p. Define

$$\delta_S \coloneqq \sum_{\mathfrak{p} \in S \cap S_p} [K_{\mathfrak{p}} : \mathbb{Q}_p], \quad r_S^T \coloneqq \delta_S - (r_1 + r_2 - 1 + |T|).$$

Let K_S^T be the maximal pro-p extension of K unramified outside S and totally decomposed at T, and set $G_S^T \coloneqq Gal(K_S^T/K)$ and $G_S^{T,ab} \coloneqq G_S^T/[G_S^T, G_S^T]$. For the definition of the strong Massey vanishing property, see Definition 1.2 in §1.1.1.

Theorem A. — *Suppose that $G_S^{T,ab} \simeq \mathbb{Z}_p^{r_S^T}$. Then there exist infinitely many sets N of tame primes of K with $|N| = r_S^T$ such that $G_{S\cup N}^T$ satisfies the strong Massey vanishing property. As a consequence, if $r_S^T \geqslant 2$, then there exists a surjective homorphism*

$$\rho_S : G_{S\cup N}^T \twoheadrightarrow \mathbb{U}_{2r_S^T+1},$$

where $\mathbb{U}_{2r_S^T+1}$ denotes the group of upper-unitriangular matrices of size $2r_S^T+1$ over $\mathbb{F}_p$.

As initiated in [**18**] and inspired by [**1**], we can lift the coefficients of the map $G_{S\cup N}^T \twoheadrightarrow \mathbb{U}_{2r_S^T+1}$ to $\mathbb{Z}/p^m \coloneqq \mathbb{Z}/p^m\mathbb{Z}$, provided that the set N of primes and the integer m are suitably chosen. Furthermore, if the matrix is not required to be of maximal size $2r_S^T+1$, one can work over $\mathbb{Z}/p^m$ for any m. For instance:

Theorem B. — *Let K be a number field with $r_2 \geqslant 2$, and assume the Gras and Leopoldt Conjectures. Fix an integer $m \geqslant 1$. Then, for all sufficiently large primes p, there exist infinitely many sets N of r_2 tame primes such that there exists a surjective homomorphism $G_{S_p\cup N} \twoheadrightarrow \mathbb{U}_{2r_2+2}(\mathbb{Z}/p^m)$.*

Here $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ denotes the group of upper-triangular unipotent $(n+1)\times(n+1)$-matrices with entries in $\mathbb{Z}/p^m$. A more general version that incorporates splitting conditions is given in Heuristic 2 in §2.6.2.

Gras's Conjecture is central in this kind of study, and we refer the reader to Conjecture 2.9 in §2.3 for a more precise formulation.

This paper is organised in two parts. The first part focuses on group-theoretic results on the strong Massey vanishing property and unipotent representations. The second part studies arithmetic applications and proves our results. For the computations, we have used the program PARI/GP [**36**].

Notations. — We fix a prime number p.
• For a $\mathbb{Z}_p$-module A, the number d_pA refers to the dimension of A/A^p over $\mathbb{F}_p$, and $\mathrm{rk}_{\mathbb{Z}_p}A$ denotes the $\mathbb{Z}_p$-rank of A, which is the dimension over $\mathbb{Q}_p$ of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A$.
• If X is a set, we denote by $|X|$ its cardinality.
• We denote by Γ a finitely presented pro-p group.
• Almost all cohomology groups $H^i(\Gamma, \mathbb{F}_p)$ have $\mathbb{F}_p$-coefficients with trivial action so in those cases we simply write $H^i(\Gamma)$. We denote by $d_p\Gamma \coloneqq h^1(\Gamma)$ the generator rank of Γ, and by $h^2(\Gamma)$ its relation rank.
• Set $\mathrm{Frat}(\Gamma) \coloneqq \Gamma^p[\Gamma,\Gamma]$ to be the Frattini subgroup of Γ. For every homomorphism $\rho\colon \Gamma \to \Gamma'$ of finitely generated pro-p groups, we denote by $\rho^{\mathrm{Frat}}\colon \Gamma/\mathrm{Frat}(\Gamma) \to \Gamma'/\mathrm{Frat}(\Gamma')$ the induced homomorphism.

1. Group Theory

1.1. Massey vanishing property and liftings. — Let $n \geqslant 3$ be an integer, and let $\mathbb{U}_{n+1}$ be the group of all upper-triangular unipotent $(n+1)\times(n+1)$-matrices with entries in $\mathbb{F}_p$. We denote by Z_{n+1} the subgroup of $\mathbb{U}_{n+1}$ with all off-diagonal entries 0 except at position $(1, n+1)$. This subgroup is the center of $\mathbb{U}_{n+1}$ and is isomorphic to $\mathbb{F}_p$. We define the quotient group $\overline{\mathbb{U}_{n+1}} \coloneqq \mathbb{U}_{n+1}/Z_{n+1}$, which can be seen as the class of matrices where the $(1, n+1)$-entry is formally removed.

Let $\psi\colon \mathbb{U}_{n+1} \to \overline{\mathbb{U}_{n+1}}$ be the canonical surjection, and define the maps

$\varphi\colon \mathbb{U}_{n+1} \to \mathbb{F}_p^n, \quad M \mapsto (M_{1,2}, \dots, M_{n,n+1}), \quad \overline{\varphi}\colon \overline{\mathbb{U}_{n+1}} \to \mathbb{F}_p^n, \quad \overline{M} \mapsto (\overline{M}_{1,2}, \dots, \overline{M}_{n,n+1}).$

For each continuous group homomorphism $\rho : \Gamma \to \mathbb{U}_{n+1}$ and each $1 \leqslant i < j \leqslant n+1$, we denote by $\rho_{i,j}$ the (i,j)-th coordinate function :

$$\rho_{i,j} : \Gamma \to \mathbb{F}_p, \quad g \mapsto \rho(g)_{i,j}.$$

We use similar notation for homomorphisms $\overline{\rho} : \Gamma \to \overline{\mathbb{U}_{n+1}}$. Note that $\rho_{i,i+1}$ (resp. $\overline{\rho}_{i,i+1}$) is a group homomorphism for each $1 \leqslant i \leqslant n-1$.

By definition, we have the commutative diagram of groups:

$$\begin{array}{ccccccc} 1 & \longrightarrow & Z_{n+1} & \longrightarrow & \mathbb{U}_{n+1} & \xrightarrow{\psi} & \overline{\mathbb{U}}_{n+1} \longrightarrow 1 \\ & & & & & \searrow^{\varphi} & \downarrow \overline{\varphi} \\ & & & & & & \mathbb{F}_p^n \end{array}$$

1.1.1. Massey vanishing properties. — For each n-tuple $\chi := (\chi_1, \dots, \chi_n)$ of elements in $H^1(\Gamma)$, we denote by θ_χ the map :

$$\theta_\chi\colon \Gamma \to \mathbb{F}_p^n, \quad g \mapsto (\chi_1(g), \dots, \chi_n(g)).$$

Definition 1.1. — We say that:

- The Massey product $\langle \chi_1, \dots, \chi_n \rangle$ is *defined* if θ_χ lifts to $\overline{\mathbb{U}_{n+1}}$, i.e. there exists a morphism $\overline{\rho}_\chi\colon \Gamma \to \overline{\mathbb{U}_{n+1}}$ such that $\theta_\chi := \overline{\varphi} \circ \overline{\rho}_\chi$.
- The Massey product $\langle \chi_1, \dots, \chi_n \rangle$ *vanishes* if θ_χ lifts to $\mathbb{U}_{n+1}$, i.e. there exists a morphism $\rho_\chi\colon \Gamma \to \mathbb{U}_{n+1}$ such that $\theta_\chi = \varphi \circ \rho_\chi$.

The existence of a homomorphic lift of θ_χ to $\overline{\mathbb{U}_{n+1}}$ (which is the definition of the Massey product) is related to the existence of a subset of $H^2(\Gamma)$ (see [**2**, Theorem 2.4]), which is called the Massey product and denoted by $\langle \chi_1, \dots, \chi_n \rangle$. Observe that if a Massey product $\langle \chi_1, \dots, \chi_n \rangle$ vanishes, then it is necessarily defined. If the Massey product is defined, then an easy cohomological computation shows that $\chi_u \cup \chi_{u+1} = 0$ for every $1 \leqslant u \leqslant n-1$.

***Definition 1.2* (Massey vanishing property)**. — We say that a pro-p group Γ

- satisfies the Massey vanishing property if every defined Massey product vanishes,
- satisfies the strong Massey vanishing property if for every n-tuple $(\chi_1, \dots, \chi_n)$ of elements in $H^1(\Gamma)$ satisfying $\chi_u \cup \chi_{u+1} = 0$ for each $1 \leqslant u \leqslant n-1$, the Massey product $\langle \chi_1, \dots, \chi_n \rangle$ vanishes.

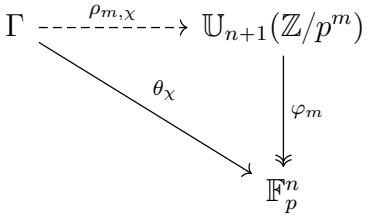
1.1.2. Liftings and m-strong Massey vanishing property. — For every integer $m \geqslant 1$, set $\mathbb{Z}/p^m := \mathbb{Z}/p^m\mathbb{Z}$. Let $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ be the group of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries in $\mathbb{Z}/p^m$. We define the surjective morphism

$$\varphi_m\colon \mathbb{U}_{n+1}(\mathbb{Z}/p^m) \to \mathbb{F}_p^n; \quad M \mapsto (\overline{M_{1,2}}; \dots; \overline{M_{n-1,n}}),$$

where $\overline{M_{i,j}}$ is the image of $M_{i,j}$ modulo $p\mathbb{Z}/p^m$. Note that when $m = 1$, the map φ_1 coincides with φ defined previously.

Building on ideas from [**1**], the third author, together with Mináč, Ramakrishna and Tân [**18**], also introduced the following group-theoretic property, which they studied in the context of (tame) absolute Galois groups:

***Definition 1.3* (m-strong Massey vanishing property).** — We say that a pro-p group Γ satisfies the m-strong Massey vanishing property if, for every n-tuple $(\chi_1, \dots, \chi_n)$ of elements in $H^1(\Gamma)^n$ satisfying $\chi_i \cup \chi_{i+1} = 0$ for each $1 \leqslant i \leqslant n-1$, there exists a morphism $\rho_{m,\chi} \colon \Gamma \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ such that the following diagram commutes:



We also say that $\rho_{m,\chi}$ is a lifting of θ_χ (over $\mathbb{Z}/p^m$).

If $m = 1$, this is the usual strong Massey vanishing property.
We now use the m-strong Massey vanishing property to lift unipotent surjections with coefficients in $\mathbb{F}_p$ to unipotent surjections with coefficients in $\mathbb{Z}/p^m$.

***Lemma 1.4*.** — *For every integer $m \geqslant 1$, the morphism induced by φ_m denoted by*

$$\varphi_m^{\mathrm{Frat}} \colon \mathbb{U}_{n+1}(\mathbb{Z}/p^m)/\mathrm{Frat}(\mathbb{U}_{n+1}(\mathbb{Z}/p^m)) \to \mathbb{F}_p^n$$

is an isomorphism.

Proof. — Clearly $\mathrm{Frat}(\mathbb{F}_p^n) = 0$. Let us denote by I_{n+1} the identity matrix and by $\epsilon_{i,j}$ the elementary $(n+1) \times (n+1)$-matrix whose entry is equal to one in (i,j), and zero everywhere else. An easy computation shows that:

$$[\mathbb{U}_{n+1}(\mathbb{Z}/p^m), \mathbb{U}_{n+1}(\mathbb{Z}/p^m)] = \langle \mathrm{I}_{n+1} + a\epsilon_{i,j}; \quad a \in \mathbb{Z}/p^m \text{ and } j - i \geqslant 2 \rangle.$$

Furthermore,

$$\mathbb{U}_{n+1}(\mathbb{Z}/p^m)^p \cdot [\mathbb{U}_{n+1}(\mathbb{Z}/p^m), \mathbb{U}_{n+1}(\mathbb{Z}/p^m)] = P + [\mathbb{U}_{n+1}(\mathbb{Z}/p^m), \mathbb{U}_{n+1}(\mathbb{Z}/p^m)],$$

where P is the additive subgroup generated by $\{pb\epsilon_{i,j}; \quad b \in \mathbb{Z}/p^m, j - i = 1\}$.
This implies that the kernel of φ_m is exactly $\mathrm{Frat}(\mathbb{U}_{n+1}(\mathbb{Z}/p^m))$. Thus $\varphi_m^{\mathrm{Frat}}$ is an isomorphism. □

As an application, we infer:

***Proposition 1.5*.** — *Assume that Γ satisfies the m-strong Massey vanishing property. Suppose moreover that there exists an n-tuple $\chi \coloneqq (\chi_1, \dots, \chi_n)$ in $H^1(\Gamma)^n$ satisfying the following conditions:*

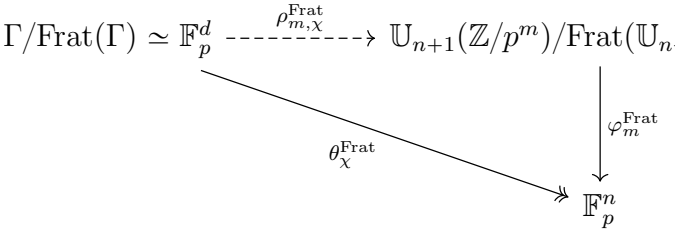
- *the map $\theta_\chi \colon \Gamma \to \mathbb{F}_p^n$ is surjective,*
- *for every $1 \leqslant u \leqslant n-1$, we have $\chi_u \cup \chi_{u+1} = 0$.*

Then there exists a surjective homomorphism $\rho_{m,\chi} \colon \Gamma \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ lifting θ_χ. Moreover, all such liftings are surjective.

Proof. — From the m-strong Massey vanishing property, there exists $\rho_{m,\chi} \colon \Gamma \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ which lifts θ_χ in $\mathbb{Z}/p^m$. Let us recall from Lemma 1.4 that we have the isomorphism

$$\varphi_m^{\mathrm{Frat}} \colon \mathbb{U}_{n+1}(\mathbb{Z}/p^m)/\mathrm{Frat}(\mathbb{U}_{n+1}(\mathbb{Z}/p^m)) \simeq \mathbb{F}_p^n.$$

Thus we infer the commutative diagram:



Since θ_χ is surjective and $\varphi_m^{\mathrm{Frat}}$ is an isomorphism, the map $\rho_{m,\chi}^{\mathrm{Frat}}$ is surjective. By Burnside Lemma, we conclude that the map $\rho_{m,\chi}$ is also surjective. □

1.2. Mildness. — Let us consider a finitely presented pro-p group Γ with a presentation (not necessarily minimal):

$$(P_\Gamma) \coloneqq \langle x_1, \dots x_d \mid l_1, \dots, l_r \rangle.$$

Alternatively, we have a presentation $1 \to R \to F \to \Gamma \to 1$, where F is pro-p free on d generators and R is the closed normal subgroup of F generated by the l_i's.
We denote by $E(\Gamma)$ the completed group ring of Γ over $\mathbb{F}_p$ filtered by $E_n(\Gamma)$, the n-th power of the augmentation ideal.
The Magnus isomorphism (see [**15**, Chapitre II, 3.1.4 and Appendice A.3]) provides an isomorphism ϕ of filtered algebras between $E(F)$ and $E \coloneqq \mathbb{F}_p\langle\langle X_1, \dots, X_d \rangle\rangle$, the algebra of noncommutative series in $X_1, \dots X_d$ over $\mathbb{F}_p$, where every X_i is assigned degree 1. The isomorphism ϕ is characterized by $\phi(x_i) \coloneqq X_i + 1$.
Let us choose an order $\succ_X$ on $\{X_1, \dots, X_d\}$, and extend it to an order on monomials on E. To fix the ideas, we take the order $X_d \succ_X X_{d-1} \succ_X \cdots \succ_X X_1$. This is always possible after relabeling the X_i's.
We define $\widehat{l_i}$ as the leading monomial of the series $\phi(l_i) - 1$.

Definition 1.6 **(Mild groups)**. — In this paper, we say that the presentation (P_Γ) is (quadratic) mild (for an order $\succ_X$) if for every i, we have $\widehat{l_i} \coloneqq X_{i_2}X_{i_1}$ (with $i_2 > i_1$), and for every i, j, we have $X_{i_2} \neq X_{j_1}$.

This is (a special case of) the notion used by Labute in [**13**, §1] to produce examples of pro-p group G_S of cohomological dimension 2.

Proposition 1.7. — *If (P_Γ) is mild, then the presentation is minimal and Γ has cohomological dimension 2.*

Proof. — See [**13**, Theorem 5.1]. □

Remark 1.8 **(Koszulity and Mildness)**. — Following our definition, using [**13**, Theorem 5.1] and [**9**, Proposition 1], we can easily show that if the group Γ admits a mild presentation, then the algebra $H^\bullet(\Gamma)$ is Koszul. Positselski [**31**] conjectured that pro-p absolute Galois groups of fields containing the p-th roots of the unity has Koszul cohomology ring, which is a stronger property than the Bloch-Kato conjecture. This conjecture was investigated by Mináč and his collaborators in [**22**] and [**27**].

1.3. The property $(\mathscr{P}_m)$ and the class $\mathscr{D}_m$. — Set $m \geqslant 1$. We define the property $(\mathscr{P}_m)$ that we study for the rest of the paper:

Definition 1.9. — We say that a group Γ satisfies the property $(\mathscr{P}_m)$ if:

(i) the group Γ checks the m-strong Massey vanishing property,

(*ii*) the group Γ admits a mild quadratic presentation or is free,
(*iii*) every open subgroup of Γ checks (*i*) and (*ii*).

We now define the class $\mathscr{D}_m$ of pro-p absolute Galois groups Γ of local fields with characteristic of residue fields different from p, which either:
– do not contain the p-th roots of the unity, so $\Gamma \simeq \mathbb{Z}_p$ [**12**, Theorem 10.1],
– contain the p^m-th roots of the unity, so Γ is Demushkin of rank 2 [**12**, Theorem 10.2].

Unipotent representations on this class were studied by Conti, Demarche and Florence in [**1**]. We easily observe that if $m \geqslant m'$ then $\mathscr{D}_m$ is a subclass of $\mathscr{D}_{m'}$.

Proposition 1.10. — *The class $\mathscr{D}_m$ checks the property $(\mathscr{P}_m)$.*

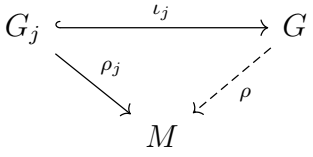
Proof. — Take Γ in $\mathscr{D}_m$. We check (*i*), (*ii*) and (*iii*). If $\Gamma \simeq \mathbb{Z}_p$, this is clear. So we assume that $\Gamma \neq \mathbb{Z}_p$.
(*i*) From [**26**, Proposition 4.1], we observe that every group in $\mathscr{D}_m$ checks the strong Massey vanishing property. Let $(\chi_1, \dots \chi_n)$ be an n-tuple in $H^1(\Gamma)^n$ satisfying $\chi_u \cup \chi_{u+1} = 0$. By the strong Massey vanishing property, there exists $\rho_\chi \colon \Gamma \to \mathbb{U}_{n+1}$ lifting θ_χ. Using [**1**, Corollary], we infer a morphism $\rho_{m,\chi} \colon \Gamma \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ which lifts ρ_χ, thus lifts θ_χ. Consequently Γ satisfies the m-strong Massey vanishing property.
(*ii*) Using [**12**, Theorem 10.2], we observe that Γ admits a presentation with two generators x_2, x_1 and one relation l_1 which checks $\widehat{l_1} = X_2X_1$, for the order $X_2 > X_1$, so it is mild.
(*iii*) Every open subgroup H of Γ is in $\mathscr{D}_m$ (see for example [**30**, Proposition 7.5.9, Chapter VII]), so satisfies (*i*) and (*ii*). □

1.4. Coproducts and the class $\overline{\mathscr{D}_m}$. — We denote by $\coprod$ the coproduct in the category of pro-p groups. This is the pro-p completion of the abstract free product in groups. For further details, we refer the reader to [**32**, Chapter 9] and [**30**, Chapter IV].
Let $\{G_1, \dots, G_k\}$ be a family of finitely generated pro-p groups, and set $G \coloneqq \coprod_{i=1}^k G_i$. We observe that we have natural injective morphisms $\iota_j \colon G_j \to G$ for every $1 \leqslant j \leqslant k$, and we infer:

Proposition 1.11 **(Universal property)**. — *For every pro-p group M and family of maps $\{\rho_j \colon G_i \to M\}_{1 \leqslant j \leqslant k}$, there exists a unique map:*

$$\rho \colon G \to M,$$

that we denote by $\rho \coloneqq \coprod_{i=1}^k \rho_i$, such that for each j the following diagram commutes:



Proof. — See [**32**, Proposition 9.1.2]. □

Let us observe that we have a map

$$\mathrm{Res}_1 \colon H^1(G) \to \bigoplus_{i=1}^k H^1(G_i), \quad \chi_u \mapsto (\chi_u \circ \iota_1, \dots, \chi_u \circ \iota_k).$$

By Proposition 1.11 this map is bijective, and we identify every element χ in $H^1(G_i)$ with an element $\widetilde{\chi}$ in $H^1(G)$ verifying $\widetilde{\chi}(\iota_i(g)) = \chi(g)$ for every $g \in G_i$, and $\widetilde{\chi}(\iota_j(G_j)) = 0$ for $j \neq i$.

Proposition 1.12. — *For every integer $n \geqslant 1$, we have an isomorphism*

$$\mathrm{Res}_n \colon H^n(G) \simeq \bigoplus_{i=1}^{k} H^n(G_i)$$

Furthermore for every pair $i \neq j$, the image of the following map is trivial:

$$\cup \colon H^1(G_i) \times H^1(G_j) \to H^2(G), \quad (\chi_1, \chi_2) \mapsto \widetilde{\chi_1} \cup \widetilde{\chi_2}.$$

Proof. — The isomorphism comes from [**30**, Theorem (4.1.4)] and the previous discussion. The computation on the coproduct is also well known, but let us propose an alternative proof using unipotent representations, inspired by [**26**, Lemma 4.7]. The proof follows easily by induction from the case $G \coloneqq G_1 \coprod G_2$. Take χ_1 in $H^1(G_1)$ and χ_2 in $H^1(G_2)$. We define morphisms $\rho_1 \colon G_1 \to \mathbb{U}_3$ and $\rho_2 \colon G_2 \to \mathbb{U}_3$ by:

$$\rho_1 \colon g_1 \mapsto \begin{bmatrix} 1 & \chi_1(g_1) & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \rho_2 \colon g_2 \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \chi_2(g_2) \\ 0 & 0 & 1 \end{bmatrix}$$

Then using the universal property, we infer a morphism $\rho \coloneqq (\rho_1 \coprod \rho_2) \colon G \to \mathbb{U}_3$ which satisfies $\rho_{1,2} = \widetilde{\chi_1}$ and $\rho_{2,3} = \widetilde{\chi_2}$. Furthermore, an easy computation implies $\widetilde{\chi_1} \cup \widetilde{\chi_2} = 0$. □

1.4.1. Mildness. — Now let us assume that, for each $i = 1, \ldots, k$, the group G_i is either free or admits a mild presentation (P_{G_i}). In this case, the universal property implies the following:

Corollary 1.13. — *The group $G \coloneqq \coprod_{i=1}^{k} G_i$ either admits a mild presentation, or is pro-p free.*

Proof. — If every $G_i \simeq \mathbb{Z}_p$, then G is pro-p free. Now to simplify the notations, we assume that for every i, the pro-p group G_i is not free (the mixed case is very similar). Thus for every i the group G_i admits a mild presentation:

$$(P_{G_i}) \coloneqq \langle x_{i,1}, \ldots, x_{i,d_i} \mid l_{i,1}, \ldots, l_{i,r_i} \rangle,$$

and we have $\widehat{l_{i,j}} \coloneqq X_{i,j_2} X_{i,j_1}$, where $X_{i,j_2} > X_{i,j_1}$ and $j_2 > j_1$.
By Proposition 1.11, the group G admits a presentation:

$$(P_G) \coloneqq \langle x_{1,1}, \ldots, x_{1,d_1}, \ldots, x_{k,d_k} \mid l_{1,1}, \ldots, l_{1,r_1}, \ldots, l_{k,r_k} \rangle.$$

Considering the order: $X_{k,d_k} \succ_X X_{k,d_k-1} \succ_X \cdots \succ_X X_{k,1} \succ_X \cdots \succ_X X_{1,1}$, we conclude that the presentation (P_G) is mild. □

1.4.2. Open subgroups and the class $\overline{\mathscr{D}_m}$. — We define $\overline{\mathscr{D}_m}$ as the closure of $\mathscr{D}_m$ with respect to finite coproducts. Concretely, the pro-p groups in $\overline{\mathscr{D}_m}$ are described by pro-p groups $G \coloneqq \coprod_{i=1}^{k} G_i$, where $\{G_1, \ldots, G_k\}$ is a family of pro-p groups in $\mathscr{D}_m$. A profinite version of the Kurosh subgroup Theorem [**30**, Theorem (4.2.1)] allows us to show the following result:

Corollary 1.14. — *Suppose that the pro-p groups $G_1, \cdots, G_k$ are in $\mathscr{D}_m$. Set $G = \coprod_{i=1}^{k} G_i$. Then every open subgroup H of G is a coproduct of groups in $\mathscr{D}_m$.*

Proof. — By [**30**, Theorem (4.2.1)], the group H is a coproduct of groups that are either isomorphic to an open subgroup of some G_i, or to a free pro-p group. We conclude by applying Proposition 1.10. □

1.4.3. The property $(\mathscr{P}_m)$ and the class $\overline{\mathscr{D}_m}$. — We show here that the class $\overline{\mathscr{D}_m}$ satisfies the property $(\mathscr{P}_m)$

Theorem 1.15. — *Assume that G is a pro-p group in $\overline{\mathscr{D}_m}$, then G satisfies $(\mathscr{P}_m)$.*

Proof. — If G is free, the proof is easy. Let us consider a family $G_1, \dots, G_k$ such that $G \coloneqq \coprod_{i=1}^{k} G_i$, and assume that every G_i is mild (the proof of the mixed case is very similar). We observe from Corollary 1.13 that G is mild, so checks (ii). Furthermore, from Corollary 1.14, every open subgroup of G is in $\overline{\mathscr{D}_m}$. To conclude, we only need to show that G satisfies the m-strong Massey vanishing property. This is a well-known result, but let us give a proof.
From Proposition 1.12, we observe that

$$H^1(G) \simeq \bigoplus_{i=1}^{k} H^1(G_i), \text{ and } \widetilde{\chi_{i,a}} \cup \widetilde{\chi_{j,b}} = 0 \text{ for } i \neq j$$

for every $\chi_{i,a} \in H^1(G_i)$ and $\chi_{j,b} \in H^1(G_j)$.
Let us consider $(\chi_1, \dots, \chi_n)$ an n-tuple of elements in $H^1(G)$ such that $\chi_u \cup \chi_{u+1} = 0$. We construct a morphism $\rho\colon G \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ such that $\rho_{u,u+1} \equiv \chi_u \pmod p$ for each $1 \leqslant u \leqslant n$. For this purpose, we write

$$\chi_u \coloneqq \sum_{j=1}^{k} \widetilde{\chi_{j,u}}, \quad \text{where } \chi_{j,u} \coloneqq \chi_u \circ \iota_j \text{ is in } H^1(G_j).$$

As Res_2 is an isomorphism that satisfies $\mathrm{Res}_2(a \cup b) = \mathrm{Res}_1(a) \cup \mathrm{Res}_1(b)$, we infer that:

$$\chi_u \cup \chi_{u+1} \coloneqq \sum_{j=1}^{k} \widetilde{\chi_{j,u}} \cup \widetilde{\chi_{j,u+1}} = 0 \implies \widetilde{\chi_{j,u}} \cup \widetilde{\chi_{j,u+1}} = 0, \text{ for every } j.$$

Since G_j satisfies the m-strong Massey vanishing property, we can construct $\rho_j\colon G_j \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ such that $(\rho_j)_{u,u+1} \equiv \chi_{j,u} \pmod p$.
By the universal property, we infer a map $\rho\colon G \to \mathbb{U}_{n+1}(\mathbb{Z}/p^m)$, which satisfies $\rho_{u,u+1} \equiv \sum_j \widetilde{\chi_{j,u}} \coloneqq \chi_u \pmod p$. □

Let us give consequences on unipotent quotients of G.

Proposition 1.16. — *Assume that G is in $\overline{\mathscr{D}_m} \backslash \mathscr{D}_m$, i.e., G is a coproduct of at least two factors. Then the group $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ is a quotient of G if and only if $n \leqslant h^1(G)$.*

Proof. — If $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ is a quotient of G, then we infer a surjection $G/\mathrm{Frat}(G) \simeq \mathbb{F}_p^{h^1(G)}$ to $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)/\mathrm{Frat}(\mathbb{U}_{n+1}(\mathbb{Z}/p^m)) \simeq \mathbb{F}_p^n$. Thus, we obtain $h^1(G) \geqslant n$.
Conversely, we assume that $h^1(G) \geqslant n$, and let us write $G \coloneqq G_1 \coprod \dots \coprod G_k$ where $k \geqslant 2$ and each G_i lies in $\mathscr{D}_m$. By Theorem 1.15, the pro-p group G satisfies the m-strong Massey vanishing property. Using Proposition 1.12, we can construct an n-tuple $(\chi_1, \dots, \chi_n)$ of characters of G such that $\chi_u \cup \chi_{u+1} = 0$ for every $1 \leqslant u \leqslant n-1$.
To simplify the discussion, let us assume that none of the groups G_i is isomorphic to $\mathbb{Z}_p$. For each $1 \leqslant i \leqslant k$ we choose $\{\chi_{i,1}, \chi_{i,2}\}$ a basis of $H^1(G_i)$, and we define $\chi_i \coloneqq \chi_{i,1}$

if $i \leqslant k$ and $\chi_i \coloneqq \chi_{i-k,2}$ if $i > k$. This family is well defined since $h^1(G) \coloneqq 2k \geqslant n$, and the associated map $\theta_\chi \colon G \to \mathbb{F}_p^n$ is surjective. We conclude using Proposition 1.5. □

Remark 1.17. — Assume that $G \in \overline{\mathscr{D}_m} \backslash \mathscr{D}_m$, and is given in the form:

$$G \coloneqq \Big(\coprod_{i=1}^{k_1} G_i \Big) \coprod \Big(\coprod_{j=1}^{k_2} H_j \Big),$$

where each G_i is a Demushkin group of rank 2 in $\mathscr{D}_m$, and each H_j is isomorphic to $\mathbb{Z}_p$. In particular, we have $h^1(G) = 2k_1 + k_2$. The pro-p group G admits a free quotient of rank $k_1 + k_2$. Using Lemma 1.4, we infer that for every integer l, the pro-p group G admits $\mathbb{U}_{n+1}(\mathbb{Z}/p^l)$ as a quotient, whenever $n \leqslant k_1 + k_2$. However, thanks to the property $(\mathscr{P}_m)$, we can go beyond this bound: more precisely, we can construct a surjection from G onto $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ for any $n \leqslant 2k_1 + k_2$.

2. Arithmetic applications

2.1. Notations. — Let K be a number field. Denote by

- $(r_1, r_2) \coloneqq (r_{1,K}, r_{2,K})$ the signature of K,
- S_p the set of p-adic places of K,
- S a finite set of places of K; set $S'_p \coloneqq S \cap S_p$,
- K_v the completion of K at each place v of K, and U_v the group of units of K_v,
- $\mathscr{G}_v$ the Galois group of the maximal pro-p extension of K_v; $\mathscr{I}_v$ its inertia subgroup, and $\mathscr{F}_v = \mathscr{G}_v/\mathscr{I}_v$,
- $\delta_S \coloneqq \sum_{v \in S'_p} [K_v : \mathbb{Q}_p]$, so that $\delta_S = \delta_{S'_p}$,
- A finite prime $\mathfrak{q}$ of K is called tame if $N(\mathfrak{q}) \equiv 1 \pmod{p}$, and more generally, m-tame if $N(\mathfrak{q}) \equiv 1 \pmod{p^m}$ for some integer $m \geqslant 1$,
- For a set $N = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_n\}$ of tame primes, we write $m_N \coloneqq min\{v_p(N(\mathfrak{q}) - 1), \mathfrak{q} \in N\}$, where v_p is the discrete p-adic valuation on $\mathbb{Z}$,
- For each place v, let $\mathscr{U}_v \coloneqq \varprojlim_n U_v/U_v^{p^n}$ be the pro-p completion of U_v. Then define $\mathscr{U}_S \coloneqq \prod_{v \in S} \mathscr{U}_v$,
- T a finite set of places of K, disjoint from S; set $E^T \coloneqq E_K^T$ the *pro-p completion* of the group of T-units of K,
- $\varphi_S^T : E^T \to \mathscr{U}_S$ the diagonal embedding of E^T into $\mathscr{U}_S$,
- K_S^T/K the maximal pro-p extension of K unramified outside S and totally decomposed at T; $G_S^T \coloneqq G_{K,S}^T \coloneqq Gal(K_S^T/K)$, and $G_S \coloneqq G_S^\varnothing$,
- $K_S^{T,ab}$ is the maximal abelian extension of K in K_S^T; set $G_S^{T,ab} \coloneqq Gal(K_S^{T,ab}/K)$,
- $K_S^{T,p,el}$ is the maximal elementary abelian extension of K in K_S^T; set $(G_S^T)^{p,el} \coloneqq Gal(K_S^{T,p,el}/K)$,
- $\mathscr{T}_S^T$ the $\mathbb{Z}_p$-torsion part of $G_S^{T,ab}$,
- $r_S^T \coloneqq \mathrm{rk}_{\mathbb{Z}_p} G_S^{T,ab}$, $r_S \coloneqq r_S^\varnothing$,

In our work, infinite places play a limited role in arguments. We focus on finite places and distinguish them by notation according to their roles: $\mathfrak{p}$ denotes a p-adic place, $\mathfrak{q}$ a non-p-adic (tame) place where ramification may occur (see Remark 2.7), and $\mathfrak{l}$ a place at which splitting conditions are imposed.

2.2. Classical results. — Most of the results in this section are well-known; see for example [**16**, §1], [**30**, Chapter X]. Since Shafarevich and Koch, we know that G_S^T is finitely presented as in the following theorem.

Theorem 2.1. — *Suppose that S is not empty. Then, we have*

$$1 - h^1(G_S^T) + h^2(G_S^T) \leqslant r_1 + r_2 + |T| - \delta_S.$$

When $S_p' = \varnothing$, the pro-p group G_S^T is FAB. More generally, we have

Proposition 2.2. — *One has $r_S^T = \mathrm{rk}_{\mathbb{Z}_p}\big(\mathrm{coker}(\varphi_S^T)\big)$. Thus if φ_S^T is injective then*

$$r_S^T = \delta_S - (r_1 + r_2 - 1 + |T|).$$

Conversely, if T is disjoint from S and we have the previous equality, then φ_S^T is injective.

As a consequence, we have (see. [**16**, Lemma 1.3]):

Corollary 2.3. — *Suppose that $S \neq \varnothing$. Then $\mathrm{rk}_{\mathbb{Z}_p} H_2(G_S^T, \mathbb{Z}_p) \leqslant \mathrm{rk}_{\mathbb{Z}_p}\big(\ker(\varphi_S^T)\big)$, where H_2 denotes the second group homology.*

By duality, we have an isomorphism $H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H_2(G, \mathbb{Z}_p)$ for a pro-p group G. Corollary 2.3 allows us to find many instances where the following lemma is particularly useful.

Lemma 2.4. — *Let $\psi : \Gamma \twoheadrightarrow G$ be a surjective morphism of pro-p groups. Suppose moreover that $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. Then ψ is an isomorphism if and only if ψ induces an isomorphism between Γ^{ab} and G^{ab}.*

Proof. — See [**29**, Lemma 2]. □

In particular, we have the following practical criterion for determining when G_S^T is free.

Proposition 2.5. — *A pro-p group G is free if and only if G^{ab} is torsion-free and $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. In particular, if $\ker(\varphi_S^T) = 1$ and $\mathscr{T}_S^T = 1$, then G_S^T is free pro-p. Furthermore, we have $h^1(G_S^T) = 1 + \delta_S - (r_1 + r_2 + |T|)$.*

Proof. — Consider a minimal presentation

$$1 \to R \to F \to G \to 1.$$

Since G^{ab} is torsion free, we have $G^{ab} \simeq F^{ab}$. Therefore, by Lemma 2.4, we conclude that $F \simeq G$. Now, let K, S, and T be as in the statement of Proposition 2.5. In this setting, the vanishing of $H^2(G_S^T, \mathbb{Q}/\mathbb{Z})$ follows from Corollary 2.3. Lastly, the formula for $h^1(G_S^T)$ follows from the assumption $\mathscr{T}_S^T = 1$, together with the Burnside Basis lemma and Proposition 2.2. □

Remark 2.6. — A non-p-adic place is not ramified in a free pro-p extension. Hence, if G_S^T is free, then we have $K_S^T = K_{S_p'}^T$.

Remark 2.7. — (see [**12**, §10]) A finite non-p-adic prime $\mathfrak{q}$ ramifies in a pro-p extension if and only if its norm $N(\mathfrak{q})$ in $\mathbb{N}$ satisfies $N(\mathfrak{q}) \equiv 1 \pmod{p}$. It is well known that the following conditions are equivalent:

- $\mathfrak{q}$ is m-tame;
- $\mathscr{G}_\mathfrak{q}$ belongs to the class $\mathscr{D}_m \backslash \mathscr{D}_{m-1}$;
- $\mathfrak{q}$ splits completely in $K(\zeta_{p^m})/K$.

Remark 2.8. — When $S = S_p$ and $T = \varnothing$, the conditions $\ker(\varphi_{S_p}) = 1$ and $\mathscr{T}_{S_p} = 1$ together are equivalent to the freeness of G_{S_p} by Euler-Poincaré characteristic formula (see [**30**, Corollary 8.7.5]).

2.3. The coproduct decomposition of G_S. — In this subsection we explain that in many cases the Galois group G_S belongs to the class $\overline{\mathscr{D}_m}$ for some integer $m \geqslant 1$.
One important guiding principle in the study of G_S has been to use presentations of $\mathscr{G}_v$ at the places $v \in S$, which are well-known as explained in § 1.3.

For each place v we have a natural restriction map $\mathscr{G}_v \to G_S$ corresponding to a fixed embedding $k_S \hookrightarrow \overline{k_v}$. When $v \notin S$, this map factors through the quotient $\mathscr{G}_v \to \mathscr{G}_v/\mathscr{I}_v \cong \mathscr{F}_v$. Using Proposition 1.11, for each subset S_0 of S we obtain a canonical morphism

$$\psi_{S,S_0} : \coprod_{v \in S_0} \mathscr{G}_v \longrightarrow G_S.$$

By the Burnside Basis theorem the map ψ_{S,S_0} is surjective if and only if $G_{S\setminus S_0}^{S_0}$ is trivial. If ψ_{S,S_0} is not surjective, we choose a finite set W of primes of K disjoint from S such that $G_{S\setminus S_0}^{S_0 \cup W}$ is trivial. Then, we obtain a surjective map

$$\psi_{S,S_0,W} : \left(\coprod_{v \in S_0} \mathscr{G}_v \right) \coprod \left(\coprod_{w \in W} \mathscr{F}_w \right) \twoheadrightarrow G_S.$$

Inspired by the theory of Riemann surfaces, several studies have investigated the problem of finding conditions under which the map $\psi_{S,S_0,W}$ is an isomorphism (see [**30**, Chapter X, §5 and §9]). This situation serves as a starting point for our study of G_S^T.
To illustrate the relevance of such cases, suppose that the map $\psi_{S,S_0,W}$ is an isomorphism. Assume moreover that S_0 contains at least one tame prime and that each local Galois group $\mathscr{G}_v$ with $v \in S_0 \cap S_p$ is free. Then G_S belongs to the class $\overline{\mathscr{D}_m}$, where $m = m_{S_0'}$ for the maximal subset $S_0' \subseteq S_0$ consisting of tame primes. By Theorem 1.15, it follows that G_S satisfies the property $(\mathscr{P}_m)$.

The notion of p-rationality naturally emerges in this context and will play a central role in what follows. Throughout, we make the additional assumption that K is totally imaginary when $p = 2$. Then, the cohomological dimension of G_{S_p} is always less than or equal 2. Following [**29**, Definition 1], we say that a number field K is p-rational if G_{S_p} is free. While this condition may seem technical, the case $\mathbb{Q}(\zeta_p)$ with p regular provides a classical example (see [**35**, §4]). In recent years, there has been growing interest in p-rationality for multiquadratic fields. Additionally, we recall the following fundamental conjecture due to Gras.

Conjecture 2.9 **(Gras [7], Conjecture** 8.11**)**. — *Given a number field K, we have $\mathscr{T}_{S_p} = 1$ for $p \gg 0$, and so from Leopoldt Conjecture the field K is p-rational for $p \gg 0$.*

The role of p-rationality is highlighted in the following theorem.

Theorem 2.10 **(Satz** 3.1 **of [38], Théorème** 2 **of [29])**. — *Assume that S contains S_p. The following conditions are equivalent:*
(i) The field K is p-rational and the Frobenius automorphisms at the places of $S\setminus S_p$ form a basis of $(G_{S_p})^{p,el}$.

(*ii*) *The map*

$$\psi_{S,S\setminus S_p,\varnothing} : \coprod_{\mathfrak{q}\in S\setminus S_p} \mathscr{G}_{\mathfrak{q}} \longrightarrow G_S$$

is an isomorphism.

As a result, once a number field is p-rational, we can find many sets N of tame primes such that $G_{S_p\cup N}$ belongs to $\overline{\mathscr{D}}$. We explore this idea further with G_S^T in the next section.

Remark 2.11. — In [**39**], Wingberg established the necessary and sufficient condition on (K, S) for the free pro-p product decomposition of G_S in a more general setting. Theorem 6 of [**39**], whose proof does not require $\zeta_p \in K$, recovers Theorem 2.10. The free pro-p product decomposition of G_{S_p} into a free pro-p group and Demushkin groups of rank greater than 2, corresponding to the absolute pro-p Galois group of a p-adic local field containing ζ_p [**30**, Theorem 7.5.14], is in principle possible. This was studied further in [**11**] through explicit examples.

2.4. On the freeness of G_S^T. — We now aim to extend Theorem 2.10, originally stated for G_S, to the setting of G_S^T, while also allowing the set S not to contain S_p. Generally, the difficulty in studying (pro-p) Galois groups comes from the absence of a general theory of Galois cohomology. We use Corollary 2.3 and Lemma 2.4, which offer a more heuristic and direct approach, thereby avoiding the need for deep cohomological machinery. In this respect, our approach differs from that of [**29, 39**], which used the Poitou–Tate duality. In particular, we proceed under the assumption that G_S^T is free.
Nevertheless, proving the freeness of G_S^T is a highly non-trivial and transcendental problem. Rather than pursuing a direct proof, we provide a heuristic argument which suggests that G_S^T is free in many cases. As shown in Proposition 2.5, two properties would be essential: the injectivity of φ_S^T and the triviality of $\mathscr{T}_S^T$.
The relationship between the injectivity of φ_S^T and the Schanuel Conjecture is well-known. For instance, we have:

Proposition 2.12. — *Let K be a Galois extension over an imaginary quadratic field k with Galois group G. Let p be a prime that splits in k, and fix a prime $\mathfrak{p}$ of k above p. Let $S_\mathfrak{p}$ denote the set of primes of K lying above $\mathfrak{p}$, and let S be a finite set of primes of K containing $S_\mathfrak{p}$. If G is abelian, then φ_S^T is injective for $T = \{\mathfrak{l}\}$, where $\mathfrak{l}$ is any non-p-adic prime of K. Moreover, assuming Schanuel's Conjecture, the injectivity of $\varphi_S^{\{\mathfrak{l}\}}$ holds for arbitrary Galois extension K/k.*

Proof. — See [**17**, §3] and [**5**, Chapter III, Corollary 3.6.5] □

In [**7**], Gras introduced a heuristic argument for Conjecture 2.9. Building on his approach, we anticipate the following heuristic:

Heuristic 1. — *Let K be a number field, and let T be a fixed finite set of primes of K such that for each $\mathfrak{l} \in T$, the completion $K_\mathfrak{l}$ is equal to $\mathbb{Q}_\ell$ for ℓ lying below $\mathfrak{l}$. Assume that $|T|\leqslant r_2$. Then, under Conjecture 2.9, the number of p for which $\ker(\varphi_{S_p}^T) \neq 1$ or $\mathscr{T}_{S_p}^T \neq 1$ is expected to be finite.*

In fact, if G_S is known to be free, it becomes straightforward to obtain a sufficient condition for the freeness of G_S^T. To streamline our discussion, we introduce the following definition.

Definition 2.13. — Let S and T be two finite disjoint sets of places of K. A set of places W, disjoint with $S \cup T$, is said to be (S,T)-primitive if the Frobenius automorphisms in $(G_S^T)^{p,el}$ at W are linearly independent over $\mathbb{F}_p$. If the Frobenius automorphisms in $(G_S^T)^{p,el}$ at W are a basis over $\mathbb{F}_p$, we say that W is maximal (S,T)-primitive. In the special case $T = \varnothing$, we simply call such a set S-primitive.

We note that in **[29]**, the term *primitivity* was used to refer to S_p-primitivity in the context of p-rational fields. We have the following proposition.

Proposition 2.14. — *Suppose that G_S is a free pro-p group. For any S-primitive set T, the group G_S^T is also free pro-p. Moreover, if* $\ker(\varphi_S) = 1$, *then we also have* $\ker(\varphi_S^T) = 1$.

Proof. — Let R be the normal subgroup of G_S generated by the Frobenius automorphisms at T. By the freeness of G_S, we have the exact sequence

$$0 \to H^1(G_S^T) \to H^1(G_S) \to H^1(R)^{G_S^T} \to H^2(G_S^T) \to 0.$$

From the S-primitivity of T, we deduce that $h^1(G_S^T) = h^1(G_S) - |T|$. Moreover, since R is the closed normal subgroup generated by the Frobenius automorphisms at T, we have $d_p H^1(R)^{G_S^T} \leqslant |T|$. Thus, equality must hold: $d_p H^1(R)^{G_S^T} = |T|$, which implies that $h^2(G_S^T) = 0$. Hence G_S^T is free. The second claim follows from the chain of equalities

$$|T| = d_p G_S - d_p G_S^T = r_S - r_S^T = \mathrm{rk}_{\mathbb{Z}_p} \ker(\varphi_S) - \mathrm{rk}_{\mathbb{Z}_p} \ker(\varphi_S^T) + |T|,$$

which shows that $\ker(\varphi_S^T) = 1$, since by hypothesis we have $\ker(\varphi_S) = 1$. □

As a consequence of the Chebotarev density theorem, once the freeness of G_S is established, one can find many sets T such that G_S^T is also free. In contrast, the heuristic we employ takes a different perspective: it fixes K and T, and studies the freeness of $G_{S_p}^T$ as p varies.

Supporting argument for Heuristic 1. — By the Gras conjecture, we can assume without loss of generality that G_{S_p} is free of rank $r_2 + 1$. According to the Chebotarev density theorem, for each *fixed* p, the Frobenius automorphism of primes $\mathfrak{l}$ in $(G_{S_p})^{p,el}$ is equidistributed as $\mathfrak{l}$ *varies*. Since the Dirichlet density of the set of primes $\mathfrak{l}$ with $K_\mathfrak{l} \neq \mathbb{Q}_\ell$ is zero, the equidistribution still holds when restricting to primes with $K_\mathfrak{l} = \mathbb{Q}_\ell$. Hence, for a fixed $\mathfrak{l} \in T$, it is reasonable to heuristically expect the Frobenius automorphism in $G_{S_p}^{p,\mathrm{el}}$ at $\mathfrak{l}$ to be equidistributed as p varies. The group $G_{S_p}^T$ is free of rank $r_2 + 1 - |T|$ unless the Frobenius automorphisms in $(G_{S_p})^{p,el}$ associated to the places in T are linearly dependent. Hence, the probability $\mathbb{P}(p, K, T)$ that $G_{S_p}^T$ is not free of rank $r_2 + 1 - |T|$ is equal to

$$1 - \prod_{i=1}^{|T|} \left(1 - \frac{1}{p^{r_2 - i + 2}}\right).$$

One can check that the infinite sum $\sum_p \mathbb{P}(p, K, T)$ is bounded above. The claim about finiteness then follows from the Borel-Cantelli lemma (see the beginning of **[7**, §4.1**]**). □

Remark 2.15. — (i) While our heuristic is formulated under the assumption of the Gras Conjecture, it is worth noting that the argument in **[7]** can be used to heuristically recover both the conjecture on G_{S_p} and the same expectation on $G_{S_p}^T$, simultaneously and from the same reasoning. Unlike our heuristic, **[7]** uses the equidistribution of the generalized Fermat quotient (ex. **[7**, §4.2.1.(ii)**]**) and the heuristic on

the existence of a binomial probability law ([**6**, §4.4], [**7**, §7]), as observed through numerical experiments.

(ii) Our assumption that $K_{\mathfrak{l}} = \mathbb{Q}_\ell$ was made mainly for simplicity. For example, if K is a Galois number field and the decomposition subgroup $D_{\mathfrak{l}}$ of $G := G(K/\mathbb{Q})$ at $\mathfrak{l}$ is nontrivial, then the Frobenius automorphism at $\mathfrak{l}$ lies in the sub-$\mathbb{F}_p[Gal(K/\mathbb{Q})]$-module of $(G_{S_p})^{p,el}$ on which $D_{\mathfrak{l}}$ acts trivially. The presence of such a non-trivial Galois action can create an obstruction to deducing the finiteness of the set of primes as predicted in Heuristic 1. Nevertheless, the overall heuristic suggests that such primes, though possibly infinite, are still very rare.

Remark 2.16. — We may attempt to apply the idea from the proof of Proposition 2.14 to obtain a free quotient $G_{S_p}^T$ from a non-free pro-p group G_{S_p}. However, this is not straightforward. Controlling the Frobenius elements in G_S^{ab} at T is subtle, and for $G_{S_p}^{T,ab}$ to be torsion-free, the map $\varphi_{S_p}^T$ must fail to be injective. As a consequence, under the Leopoldt Conjecture, for any non-p-adic prime $\mathfrak{l}$, the group $G_{S_p}^{\{\mathfrak{l}\}}$ is not free unless G_{S_p} is.

2.5. Proof of Theorem A. — We now prove Theorem A, beginning with the following result:

Proposition 2.17. — *Assume that φ_S^T is injective. Let $N = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_s\}$ be a finite set of tame primes. Then*

$$Gal(K_{S\cup N}^{T,ab}/K_S^{T,ab}) \simeq \mathbb{Z}/p^{n_1} \times \cdots \times \mathbb{Z}/p^{n_r},$$

where $n_i = v_p(N(\mathfrak{q}_i) - 1)$. If moreover $\mathscr{T}_S^T = 1$, then we have

$$G_{S\cup N}^{T,ab} \simeq \mathbb{Z}_p^{r_S^T} \times \mathbb{Z}/p^{n_1} \times \cdots \times \mathbb{Z}/p^{n_r}.$$

Proof. — From the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E^T & \longrightarrow & \mathscr{U}_{S\cup N} & \longrightarrow & (G_{S\cup N}^T)^{ab} & \longrightarrow & \mathrm{Cl}_T & \longrightarrow & 0 \\ & & \| & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \| & & \\ 0 & \longrightarrow & E^T & \longrightarrow & \mathscr{U}_S & \longrightarrow & (G_S^T)^{ab} & \longrightarrow & \mathrm{Cl}_T & \longrightarrow & 0 \end{array}$$

and the Snake lemma, we infer that $Gal(K_{S\cup N}^{T,ab}/K_S^{T,ab})$ is isomorphic to the kernel of the map $\mathscr{U}_{S\cup N}/\varphi_{S\cup N}(E^T) \to \mathscr{U}_S/\varphi_S(E^T)$. Here, Cl_T denotes the quotient of the p-class group of K by the subgroup generated the ideal classes of the primes in T. We deduce the claim by applying the Snake lemma once more to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E^T & \longrightarrow & \mathscr{U}_{S\cup N} & \longrightarrow & \mathscr{U}_{S\cup N}/\varphi_{S\cup N}(E^T) & \longrightarrow & 0 \\ & & \| & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \\ 0 & \longrightarrow & E^T & \longrightarrow & \mathscr{U}_S & \longrightarrow & \mathscr{U}_S/\varphi_S(E^T) & \longrightarrow & 0 \end{array}$$

The second claim follows from the first one by the $\mathbb{Z}_p$-freeness of $(G_S^T)^{ab}$. □

The following result corresponds to Theorem A in the introduction. For additional explanation, see also Remark 2.19.

Theorem 2.18 **(Theorem A)**. — *Let S, T, $N \subset M$ be four sets of primes of K such that*

(*i*) *the map* φ_S^T *is injective,*
(*ii*) *the torsion part* $\mathscr{T}_S^T$ *of* $(G_S^T)^{ab}$ *is trival,*
(*iii*) *the primes* $\mathfrak{q}$ *in* N *are tame,*
(*iv*) *the set* M *is maximal* (S,T)*-primitive.*

Then the natural map $\psi^T_{S\cup N,N,M\setminus N} : \left(\coprod_{\mathfrak{q}\in N}\mathscr{G}_\mathfrak{q}\right)\coprod\left(\coprod_{\mathfrak{l}\in M\setminus N}\mathscr{F}_\mathfrak{l}\right)\longrightarrow G^T_{S\cup N}$ *is an isomorphism. In particular, the pro-p group* $G^T_{S\cup N}$ *satisfies* $(\mathscr{P}_{m_N})$*, and consequently the* m_N*-strong Massey vanishing property, where* $m_N \coloneqq min\{v_p(N(\mathfrak{q})-1), \mathfrak{q}\in N\}$.

Proof. — By Proposition 2.5 and the assumptions (i) and (ii), the group G_S^T is free of rank r_S^T. Consider the natural map

$$\psi^T_{S\cup N,N,M\setminus N} : \left(\coprod_{\mathfrak{q}\in N}\mathscr{G}_\mathfrak{q}\right)\coprod\left(\coprod_{\mathfrak{l}\in M\setminus N}\mathscr{F}_\mathfrak{l}\right)\longrightarrow G^T_{S\cup N}.$$

By assumption (iv), the map $\psi^T_{S\cup N,N,M\setminus N}$ is surjective. Hence, by Proposition 2.17, it induces an epimorphism on the abelianizations between isomorphic finitely generated $\mathbb{Z}_p$-modules. By the structure theorem for finitely generated modules over $\mathbb{Z}_p$, it follows that the map on the abelianizations is an isomorphism.
Moreover, assumption (i) and Corollary 2.3 together imply that $H^2(G_S^T,\mathbb{Q}/\mathbb{Z}) = 0$. Therefore by Lemma 2.4, the map $\psi^T_{S\cup N,N,M\setminus N}$ is an isomorphism. As a consequence, the group $G^T_{S\cup N}$ belongs to the class $\overline{\mathscr{D}_{m_N}}$ and, by Theorem 1.15, it satisfies the property $(\mathscr{P}_{m_N})$. □

Remark 2.19. — The hypothesis $(G_S^T)^{ab}\simeq\mathbb{Z}_p^{r_S^T}$ in Theorem A immediately yields (ii) in Theorem 2.18. Furthermore, if T is disjoint from S, then by Proposition 2.2, condition (i) also holds. Applying the arguments from the previous proof and using the Chebotarev density theorem, we can find infinitely many sets N of size r_S^T such that

$$\psi^T_{S\cup N,N,\varnothing} : \left(\coprod_{\mathfrak{q}\in N}\mathscr{G}_\mathfrak{q}\right)\longrightarrow G^T_{S\cup N}$$

is an isomorphism. By using Proposition 1.16 (and Remark 1.17 with $k_2 = 0$), this establishes Theorem A as stated in the introduction.

Example 2.20. — Consider the multiquadratic field $K = \mathbb{Q}(\sqrt{-1},\sqrt{2},\sqrt{7},\sqrt{19})$, and take $p = 3$. Let N be a set consisting of one prime of K lying over each of the rational primes $19, 31, 199$, and let T be a set consisting of one prime of K lying over each of 53 and 89. Then, we have

$$G^T_{S_3\cup N}\cong\left(\coprod_{v\in N}\mathscr{G}_v\right)\coprod\mathscr{F}$$

where $\mathscr{F}$ is the free pro-3 group of rank 4.

Corollary 2.21. — *Let* K *be a number field, and* $S\subset S_p$ *such that:*
(*i*) *the map* φ_S *is injective,*
(*ii*) $\mathscr{T}_S = 1$.

Assume moreover that $r_S \geqslant 2$. Then there exists infinitely many sets N of tame primes, with $|N| = r_S$, such that

$$G_{S\cup N} \twoheadrightarrow \mathbb{U}_{2r_S+1}.$$

As a consequence, there exists a $\mathbb{U}_{2r_S+1}$-extension of K unramified outside $S \cup N$.

Remark 2.22. — Corollary 2.21 is a direct consequence of Theorem 2.18 and Proposition 1.16. Observe that if $r_S = 1$ then, for $N = \{\mathfrak{q}\}$, the group $G_{S\cup N}$ is a Demushkin group of rank 2. Thus $\mathbb{U}_3$ is not a quotient of $G_{S\cup N}$.

2.6. Lifting Massey Products to $\mathbb{Z}/p^m$. — In this subsection, we enlarge S to construct surjective unipotent representations $G^T_{S\cup N} \to \mathbb{U}_n(\mathbb{Z}/p^m)$ for $m > 1$. Theorem 2.18 provides situations where $G^T_{S\cup N}$ lies in $\overline{\mathscr{D}_{m_N}}$ and satisfies $(\mathscr{P}_{m_N})$. By Proposition 1.16, this leads to a surjective homomorphism $G^T_{S\cup N} \to \mathbb{U}_{2r_S^T+1}(\mathbb{Z}/p^{m_N})$. However, in certain cases, the conditions (iii) and (iv) of Theorem 2.18 may be incompatible, creating an obstruction to constructing unipotent representations with both rank $n = 2r_S^T + 1$ and large m.

2.6.1. Obstruction to full rank with large coefficients. — Let ν be the largest integer $\geqslant 0$ such that $K(\zeta_{p^\nu}) = K(\zeta_p)$. Let $K_{1,p}$ be the $\mathbb{F}_p$-extension of K contained in $K(\zeta_{p^{\nu+1}})$. For simplicity of notation, we write K_1 for $K_{1,p}$ throughout, except in the supporting argument of Heuristic 2. We note that $K_1(\zeta_p) = K_1(\zeta_{p^{\nu+1}})$.

Proposition 2.23. — *Let K be a number field and let S and T be finite sets of primes of K such that $\ker(\varphi_S^T) = 1$ and $\mathscr{T}_S^T = 1$. There exist infinitely many sets N of tame primes of size r_S^T such that*

$$G^T_{S\cup N} \cong \coprod_{\mathfrak{q}\in N} \mathscr{G}_\mathfrak{q},$$

where each $\mathscr{G}_\mathfrak{q}$ is a Demushkin group in $\mathscr{D}_\nu$. As a consequence, if $r_S^T \geqslant 2$, there exists a surjective homomorphism

$$G^T_{S\cup N} \twoheadrightarrow \mathbb{U}_{2r_S^T+1}(\mathbb{Z}/p^\nu).$$

Proof. — By Chebotarev density theorem, we can find a finite set N of primes whose Frobenius at $Gal(K_S^{T,p,el}(\zeta_p)/K)$ form a basis of the subgroup $Gal(K_S^{T,p,el}(\zeta_p)/K(\zeta_p))$. Via the isomorphism

$$Gal(K_S^{T,p,el}(\zeta_p)/K(\zeta_p)) \cong (G_S^T)^{p,el},$$

this implies that N is (S,T)-primitive. Moreover, since the Frobenius automorphism at each $\mathfrak{q} \in N$ fixes $K(\zeta_p) = K(\zeta_{p^\nu})$, it follows from Remark 2.7 that each $\mathfrak{q}$ is ν-tame. Therefore, by Theorem 2.18, the group $G^T_{S\cup N}$ satisfies the property $(\mathscr{P}_\nu)$. The conclusion then follows from Proposition 1.16. □

Proposition 2.24. — *Let K be a number field, and let S and T be finite sets of primes of K such that $\ker(\varphi_S^T) = 1$ and $\mathscr{T}_S^T = 1$. Let $m > \nu$ be an integer.*

(1) *If K_1 is not contained in $K_S^{T,p,el}$, then there exist infinitely many sets N of tame primes such that $G^T_{S\cup N}$ is isomorphic to the coproduct of r_S^T Demushkin groups, each belonging to the class $\mathscr{D}_m$. As a consequence, if $r_S^T \geqslant 2$, there is a surjective homomorphism $G^T_{S\cup N} \to \mathbb{U}_{2r_S^T+1}(\mathbb{Z}/p^m)$.*

(2) *If $K_1 \subseteq K_S^{T,p,el}$, then no such set N of size r_S^T exists. However, there exist sets N_0 with $|N_0| = r_S^T - 1$ such that, for any $M \supseteq N_0$, the group $G_{S\cup M}^T$ is a coproduct of the form*

$$\Big(\coprod_{\mathfrak{q}\in N_0} \mathscr{G}_{\mathfrak{q}}\Big) \coprod G',$$

where each $\mathscr{G}_{\mathfrak{q}}$ for $\mathfrak{q} \in N_0$ belongs to $\mathscr{D}_m$, and G' is either isomorphic to $\mathbb{Z}_p$ or a Demushkin group in the class $\mathscr{D}_\nu$ but not in $\mathscr{D}_{\nu+1}$. As a consequence, if $r_S^T \geqslant 2$, there is a surjective homomorphism $G_{S\cup N'}^T \to \mathbb{U}_{2r_S^T}(\mathbb{Z}/p^m)$.

Proof. — If the intersection $K(\zeta_{p^m}) \cap K_S^{T,p,el}$ is strictly larger than K, then it must coincide with K_1. Therefore, the first claim follows directly from the proof of Proposition 2.23. Assume now that $K_1 \subseteq K_S^T$. In this case, we can construct a set N_0 of size $r_S^T - 1$ satisfying the desired property, by using the same argument as in Proposition 2.23 to the isomorphism

$$Gal(K_S^{T,p,el}(\zeta_{p^m})/K(\zeta_{p^m})) \cong Gal(K_S^{T,p,el}/K_1).$$

Let $N_0 \cup \{\mathfrak{q}'\}$ be a maximal (S,T)-primitive set. If $\mathfrak{q}'$ is not tame, then $G_{S\cup M}^T = G_{S\cup N_0}^T$ by Remark 2.7. If $\mathfrak{q}'$ is tame, then it is not m-tame. Otherwise, the Frobenius at $\mathfrak{q}'$ would fix $K(\zeta_{p^m}) \cap K_S^{T,p,el} = K_1$, which contradicts $|N_0| = \dim_p Gal(K_S^{T,p,el}/K_1)$. Hence, in this case, the pro-p group $G_{S\cup M}^T$ is a coproduct of $\coprod_{\mathfrak{q}\in N_0} \mathscr{G}_{\mathfrak{q}} \in \overline{\mathscr{D}_m}$ and $\mathscr{G}_{\mathfrak{q}'} \in \mathscr{D}_\nu$. In both cases, $\coprod_{\mathfrak{q}\in N_0} \mathscr{G}_{\mathfrak{q}} \coprod \mathbb{Z}_p$ is a quotient of $G_{S\cup M}^T$, and the claim on the unipotent representation follows. □

Remark 2.25. — As shown in the proof of the above proposition, the inclusion $K_1 \subseteq K_S^T$ can be viewed as an obstruction to constructing a set N for which $G_{S\cup N}^T$ becomes the coproduct of the maximal number of Demushkin groups in $\mathscr{D}_m$ for $m > \nu$.

As a complement to Corollary 2.21, we now state the following result, which corresponds to Theorem B in the introduction. Note that $K_1 \subset K_{S_p}$.

Corollary 2.26 **(Theorem B)**. — *Let K be a number field with $r_2 \geqslant 2$, and assume the Gras and Leopoldt Conjectures. Then there exists a constant p_0 such that for all primes $p > p_0$, and for any integer $m \geqslant 1$, there exists a Galois extension L/K with Galois group*

$$Gal(L/K) \cong \mathbb{U}_{2r_2+2}(\mathbb{Z}/p^m),$$

which is unramified outside $S_p \cup N$, where N is a set of r_2 tame primes.
More precisely, for each such p and m, there exist infinitely many sets N of r_2 tame primes such that there exists a surjective group homomorphism

$$G_{S_p\cup N} \twoheadrightarrow \mathbb{U}_{2r_2+2}(\mathbb{Z}/p^m).$$

Remark 2.27. — When K does not contain the p-th roots of the unity, the theorem of Scholz and Reichardt demonstrates the existence of a Galois extension L/K with Galois group isomorphic to $\mathbb{U}_{n+1}(\mathbb{Z}/p^m)$ which is unramified outside a set N_0 of tame primes of size

$$|N_0| = (d_p Cl_K + d_p E_K) + n + (nm-1)(nm-2),$$

where Cl_K is the class group of K. This shows that constructing unipotent Galois extensions using only tame ramification requires a significantly large amount of ramification.

2.6.2. Splitting and Obstructions. — As discussed earlier, the obstruction to constructing a unipotent representation $G^T_{S\cup N} \to \mathbb{U}_{2r_S^T+1}(\mathbb{Z}/p^m)$ for $m > \nu$, lies entirely in the relationship between K_1 and K_S^T. We now continue the discussion, with particular focus on the role of T.
If there is a prime $\mathfrak{l} \in T$ which does not split in K_1, then $K_1 \nsubseteq K_S^T$. We can always find this situation by enlarging T by one element.

Proposition 2.28. — *Let K, S, and T be such that $\ker(\varphi_S^T) = 1$ and $\mathscr{T}_S^T = 1$. Then there exists a Chebotarev density set of primes $\mathfrak{l} \notin T \cup S$ such that $\{\mathfrak{l}\}$ is (S,T)-primitive and $K_1 \nsubseteq K_S^{T\cup\{\mathfrak{l}\}}$.*

Proof. — It suffices to take $\mathfrak{l}$ that is inert in K_1. □

In the same spirit as § 2.4, we study the inclusion $K_{1,p} \subset K_{S_p}^T$ for fixed K and T, for varying prime numbers p. For a fixed integer a, a prime p is called a Wieferich prime to the base a if

$$a^{p-1} \equiv 1 \pmod{p^2}.$$

According to the Gras's heuristic involving a binomial probability law, the number of Wieferich primes to a fixed base a is expected to be finite ([**6**, Théorème 4.9]). This perspective is closely connected to Gras Conjecture and motivates the following heuristic.

Heuristic 2. — *Let K be a number field, and let $T \neq \varnothing$ be a fixed set of primes as in Heuristic 1. Then, it is expected that there exists an integer $p_0 \in \mathbb{N}$ such that for every prime $p > p_0$ and every integer $m \geqslant 1$, there exist infinitely many sets N of tame primes for which the group $G^T_{S_p\cup N}$ is the coproduct of r_S^T Demushkin groups in the class $\mathscr{D}_m$.*
As a consequence, there exist Galois extensions of K with Galois group isomorphic to $\mathbb{U}_{2r_S^T+1}(\mathbb{Z}/p^m)$, unramified outside $S_p \cup N$ and totally decomposed at T.

Supporting argument. — According to Heuristic 1, it is expected that $\ker(\varphi_{S_p}^T) = 1$ and $\mathscr{T}_{S_p}^T = 1$ for all but finitely many primes p. Let $\mathfrak{l} \in T$ be fixed, and let l be the rational prime below $\mathfrak{l}$. For all but finitely many primes p, the field $K_{1,p}$ is the compositum of K and $\mathbb{Q}_{1,p}$. The prime $\mathfrak{l}$ splits in $K_{1,p}$ if and only if $\mathbb{Q}_{1,p} \subseteq K_{\mathfrak{l}}$, which in turn holds if and only if l splits in $\mathbb{Q}_{1,p}$ for $p > [K : \mathbb{Q}]$. This is equivalent to p being a Wieferich prime to the base l. By [**6**, Théorème 4.9], the number of such primes p is expected to be finite. □

We conclude this paper with a numerical example that illustrates our results.

Example 2.29. — Let $K = \mathbb{Q}(i, \sqrt{2}, \sqrt{7})$, which is the splitting field of the polynomial

$$f(x) = x^8 - 32x^6 + 344x^4 - 512x^2 + 1936.$$

Fix a root θ of $f(x)$, and consider the following prime ideals in $\mathscr{O}_K$:

$$\mathfrak{q}_1 = (163, \theta^2 + 10), \quad \mathfrak{q}_2 = (37, \theta^2 - 6\theta + 7),$$
$$\mathfrak{q}_3 = (2341, \theta^2 + 306\theta - 551), \quad \mathfrak{q}_4 = (73, \theta^2 - 10\theta + 18),$$
$$\mathfrak{l} = \left(241, \frac{-241\theta^7}{5280} + \frac{10363\theta^5}{5280} - \frac{39283\theta^3}{1320} + \theta^2 + \frac{212821\theta}{1320} - 82\right).$$

Let $N = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$ and $T = \{\mathfrak{l}\}$. Then the union $N \cup T$ is S_3-primitive, and the Galois group $G^T_{S_3\cup N}$ is isomorphic to the coproduct $\coprod_{1\leqslant i\leqslant 4} \mathscr{G}_{\mathfrak{q}_i}$, and hence belongs to the

class $\overline{\mathscr{D}_2}$. As a consequence, there exists a $\mathbb{U}_9(\mathbb{Z}/9)$-extension of K which is unramified outside $S_3 \cup N$ and totally splitting at $\mathfrak{l}$.

References

[1] A. Conti, C. Demarche, and M. Florence, *Lifting Galois representations via Kummer flags*, arXiv preprint arXiv:2403.08888 (2024).

[2] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), no. 2, 177–190.

[3] J. Gärtner, *Higher Massey products in the cohomology of mild pro-p-groups*, J. Algebra **422** (2015), 788–820.

[4] E. Golod and I. R. Shafarevich, *On the class field tower*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **28** (1964), no. 2, 261–272.

[5] G. Gras, *Class field theory: from theory to practice, corr. 2nd ed.*, Springer Monographs in Mathematics, (2005).

[6] ———, *Étude probabiliste des quotients de Fermat*, Funct. Approx. Comment. Math. **54** (2016), no. 1, 115–140. MR 3477738

[7] ———, *Les θ-régulateurs locaux d'un nombre algébrique: Conjectures p-adiques*, Canad. J. Math. **68** (2016), no. 3, 571–624.

[8] P. Guillot, J. Mináč, and A. Topaz, *Four-fold Massey products in Galois cohomology*, Compos. Math. **154** (2018), no. 9, 1921–1959.

[9] O. Hamza, *On extensions of number fields with given quadratic algebras and cohomology*, Manuscripta Math. **176** (2025), no. 1, Paper No. 8, 21. MR 4848855

[10] Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J. **172** (2023), no. 1, 1 – 41.

[11] J-F. Jaulent and O. Sauzet, *Pro-ℓ-extensions de corps de nombres $\mathfrak{l}$-rationnels*, J. Number Theory **65** (1997), no. 2, 240–267. MR 1462840

[12] H. Koch, *Galois theory of p-extensions*, Springer Science & Business Media, 2002.

[13] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$*, J. Reine Angew. Math. **596** (2006), 155–182.

[14] J. Labute and J. Mináč, *Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification*, J. Algebra **332** (2011), no. 1, 136–158.

[15] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHÉS **26** (1965), 5–219.

[16] D. Lim and C. Maire, *On the analyticity of the maximal extension of a number field with prescribed ramification and splitting*, Proc. Am. Math. Soc. **152** (2024), no. 12, 5013–5024.

[17] C. Maire, *On the $\mathbb{Z}_\ell$-rank of abelian extensions with restricted ramification*, J. Number Theory **92** (2002), no. 2, 376–404.

[18] C. Maire, J. Mináč, R. Ramakrishna, and N. D. Tân, *On the strong Massey property for number fields*, arXiv preprint arXiv:2409.01028 (2024).

[19] W. S. Massey, *Higher order linking numbers*, J. Knot Theory Ramifications **7** (1998), 393–414.

[20] A. Merkurjev and F. Scavia, *Degenerate fourfold Massey products over arbitrary fields*, J. Eur. Math. Soc. (2024).

[21] ———, *Lectures on the Massey vanishing conjecture*, (2024).

[22] J. Mináč, F. Pasini, C. Quadrelli, and N. D. Tân, *Koszul algebras and quadratic duals in Galois cohomology*, Adv. Math. **380** (2021), 107569.

[23] J. Mináč and N. D. Tân, *The Kernel Unipotent Conjecture and the vanishing of Massey products for odd rigid fields*, Adv. Math. **273** (2015), 242–270.

[24] ———, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. **94** (2016), no. 3, 909–932.

[25] ———, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. **19** (2016), no. 1, 255–284.

[26] ———, *Counting Galois $\mathbb{U}_4(\mathbb{F}_p)$-extensions using Massey products*, J. Number Theory **176** (2017), 76–112.

[27] J. Mináč, F. W. Pasini, C. Quadrelli, and N. D. Tân, *Mild pro-p groups and the Koszulity conjectures*, Expo. Math. **40** (2022), no. 3, 432–455. MR 4475389

[28] M. Morishita, *Milnor invariants and Massey products for prime numbers*, Compos. Math. **140** (2004), no. 1, 69–83.

[29] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nachr. **149** (1990), 163–176. MR 1124802

[30] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, vol. 323, Springer Science & Business Media, 2013.

[31] L. Positselski, *Galois cohomology of a number field is Koszul*, J. Number Theory **145** (2014), 126–152.

[32] L. Ribes and P. Zalesskii, *Profinite groups*, vol. 40, Springer Science & Business Media, 2010.

[33] P. Schmid, *Realizing 2-groups as Galois groups following Shafarevich and Serre*, Algebra Number Theory **12** (2018), no. 10, 2387–2401. MR 3911134

[34] A. Schmidt, *Über pro-p-fundamentalgruppen markierter arithmetischer kurven*, J. Reine Angew. Math. **640** (2010), 203–235. MR 2629694

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

[36] The PARI Group, Univ. Bordeaux, *PARI/GP version `2.15.3`*, 2023, available from `http://pari.math.u-bordeaux.fr/`.

[37] D. Vogel, *Massey products in the galois cohomology of number fields*, Ph.D. thesis, 2004.

[38] K. Wingberg, *Freie Produktzerlegungen von Galoisgruppen und Iwasawa-Invarianten für p-Erweiterungen von* **Q**, J. Reine Angew. Math. **341** (1983), 111–129. MR 697311

[39] ———, *On Galois groups of p-closed algebraic number fields with restricted ramification*, J. Reine Angew. Math. **400** (1989), 185–202. MR 1013730

February 13, 2026

Oussama Hamza, Institute for Advanced Studies in Mathematics, Harbin Institute of Technology, Harbin, China 150001 • *E-mail :* `ohamza3@uwo.ca`

Donghyeok Lim, Department of Mathematics Education, Korea National University of Education, Cheongju 28173, South Korea • *E-mail :* `donghyeokklim@gmail.com`

Christian Maire, Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, F-25000 Besançon, France • *E-mail :* `christian.maire@univ-fcomte.fr`