A NOTE ON ASYMPTOTICALLY GOOD EXTENSIONS IN WHICH INFINITELY MANY PRIMES SPLIT COMPLETELY

by

Oussama Hamza & Christian Maire

Abstract. — Let p be a prime number, and let K be a number field. For $p = 2$, assume moreover K totally imaginary. In this note we prove the existence of asymptotically good extensions L/K of cohomological dimension 2 in which infinitely many primes split completely. Our result is inspired by a recent work of Hajir, Maire, and Ramakrishna.

Let K be a number field, and let L/K be an infinite unramified extension. Denote by $\mathscr{S}_{L/K}$ the set of prime ideals of K that split completely in L/K. In [**8**] Ihara proved that $\displaystyle\sum_{\mathfrak{p}\in\mathscr{S}_{L/K}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} < \infty$, where $N(\mathfrak{p}) := |\mathscr{O}_K/\mathfrak{p}|$; and this result raised the following interesting question: are there L/K for which $\mathscr{S}_{L/K}$ is infinite? This question was recently answered in the positive by Hajir, Maire, and Ramakrishna in [**7**]. Infinite unramified extensions L/K are special cases of infinite extensions for which the root discriminants $rd_F := |Disc_F|^{1/[F:\mathbb{Q}]}$ are bounded, where the field F ranges over the finite-dimensional subextensions of L/K, and $Disc_F$ is the discriminant of F. Such extensions are called *asymptotically good*, and it is now well-known that in such extensions the inequality of Ihara involving $\mathscr{S}_{L/K}$ still holds (see for example [**16**], [**13**]).

Pro-p extensions of number fields with restricted ramification allow us to exhibit asymptotically good extensions. Let p be a prime number, and let S be a finite set of prime ideals of K coprime to p (more precisely each $\mathfrak{p} \in S$ is such that $N(\mathfrak{p}) \equiv 1 (\bmod\ p)$); the set S is called *tame*. Let K_S be the maximal pro-p extension of K unramified outside S, put $G_S := Gal(K_S/K)$. In K_S/K the root discriminants are bounded by some constant depending on the discriminant of K and the norm of the places of S (see for example [**6**, Lemma 5]). Moreover thanks to the Golod-Shafarevich criterion, it is well-known that K_S/K is infinite when $|S|$ is large in comparison to $[K : \mathbb{Q}]$ (see for example [**14**, Chapter X, §10, Theorem 10.10.1]), and therefore asymptotically good. For instance, if $p > 2$, $\mathbb{Q}_S/\mathbb{Q}$ is infinite when $|S| \geqslant 4$. In [**7**] the authors showed that when S is large, there exists

2000 ***Mathematics Subject Classification.*** — 11R37, 11R29.
Key words and phrases. — Pro-p extensions with restricted ramification, asymptotically good extensions, mild pro-p extensions.

The authors thank Karim Belabas, Farshid Hajir and Alexander Schmidt for useful comments; and Philippe Lebacque and Jan Mináč for their interests in this work. They also want to thank the anonymous referee for its careful reading of the paper. CM was partially supported by the ANR project FLAIR (ANR-17-CE40-0012), and by the EIPHI Graduate School (ANR-17-EURE-0002).

infinite subextension L/K of K_S/K for which the set $\mathscr{S}_{L/K}$ is infinite, without providing any information on $Gal(L/K)$. Here we prove:

Theorem A. — *Let p be a prime number, and let K be a number field. For $p = 2$ assume K totally imaginary. Let T and S_0 be two disjoint finite sets of prime ideals of K, where S_0 is tame. Then for infinitely many finite sets S of tame prime ideals of K containing S_0, there exists an infinite pro-p extension L/K in K_S/K such that*

(i) the set $\mathscr{S}_{L/K}$ of places that split completely in L/K is infinite and contains T;
(ii) the pro-p group $G = Gal(L/K)$ is of cohomological dimension 2;
(iii) the minimal number of relations of G is infinite, i.e. $\dim H^2(G, \mathbb{F}_p) = \infty$;
(iv) for each $\mathfrak{p} \in S$, the local extension $L_\mathfrak{p}/K_\mathfrak{p}$ is maximal, i.e. isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$;
(v) the Poincaré series of the algebra $\mathbb{F}_p[\![G]\!]$ is equal to $\left(1 - dt + rt^2 + t^3 \sum_{n\geqslant 0} t^n\right)^{-1}$, where $d = d_pG_S$, and where r is explicit, depending on K, S, T.

Remark 1. — *We will see that the pro-p group G of Theorem A is mild in the terminology of Anick* [**2**]. *See also Labute* [**10**] *for arithmetic contexts.*

Remark 2. — *Let L/K be an asymptotically good Galois extension. Set $\mathscr{T}_{L/K} := \{\mathfrak{p} \subset \mathscr{O}_K, f(\mathfrak{p}) < \infty\}$, where $f(\mathfrak{p})$ is the residue extension degree of $\mathfrak{p}$ in L/K. Then one actually has $\displaystyle\sum_{\mathfrak{p}\in\mathscr{T}_{L/K}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} < \infty$ (see* [**8**], [**16**], *etc.). But observe that $\mathscr{S}_{L/K} = \mathscr{T}_{L/K}$ in the context of Theorem A. To be complete, also note that for $X \geqslant 2$ one has (assuming the GRH): $|\{\mathfrak{p} \in \mathscr{S}_{L/K},\ N(\mathfrak{p}) \leqslant X\}| \leqslant cX^{1/2}\big([K:\mathbb{Q}]\log X + b\big)$, where c is an absolute constant, and where b is an upper bound for the sequence of the root discriminants in L/K; in particular one can take $b = \log|Disc_K|$ when L/K is unramified (see* [**7**]*).*

The proof follows the strategy developed by Labute [**10**] (see also [**11**], [**15**], [**4**] etc.) for studying the cohomological dimension of a pro-p group G, through the notion of strongly free sets introduced by Anick [**1**]. By following the approach of Forré [**4**], we adapt this idea to the setting where the minimal number of relations of G is infinite. This key idea is associated to a result of Schmidt [**15**] that shows that the pro-p group G_S is of cohomological dimension 2 for some well-chosen S; the proof of Schmidt involves the cup-product $H^1(G_S, \mathbb{F}_p) \cup H^1(G_S, \mathbb{F}_p)$. Here we use the translation of this cup-product to the polynomial algebras, due to Forré [**4**]. In particular, this allows us to choose infinitely many Frobenius elements in G_S such that the family of the highest terms of these plus the highest terms of the relations of G_S, is combinatorially free (see §1.1.2 and Definition 1.2). We conclude by cutting the tower K_S/K by all these Frobenius elements: this is the strategy of [**7**].

This note contains two sections. In §1 we recall the results we need regarding pro-p groups, graded algebras, and arithmetic of pro-p extensions with restricted ramification. In §2 we start with an example involving $K = \mathbb{Q}$, and prove the main result.

Notations.
Let p be a prime number.
• If V is a $\mathbb{F}_p$-vector space we denote by $\dim V$ its dimension over $\mathbb{F}_p$.
• For a pro-p group G, we denote by $H^i(G)$ the cohomology group $H^i(G, \mathbb{F}_p)$. The p-rank of G, which is equal to $\dim H^1(G)$, is noted d_pG.

1. The results we need

1.1. On pro-p groups. — For this section we refer to [**3**], [**9**, Chapters 5, 6 and 7], and [**4**]. Take a prime number p.
Let G be a pro-p group of finite p-rank d, and let $1 \to R \to F \to G \to 1$ be a minimal presentation of G by a free pro-p group F; the algebra $\Lambda_G := \mathbb{F}_p[\![G]\!]$ acts continuously on $R/R^p[R,R]$. The cohomological dimension $cd(G)$ of G is the smallest integer n (possibly $n = \infty$) such that $H^i(G) = 0$ for every $i \geqslant n+1$.

Theorem 1.1. — *One has* $cd(G) \leqslant 2$ *if and only if* $R/R^p[R,R] \simeq \prod_I \Lambda_G$. *Moreover* $\dim H^2(G) = |I|$.

Proof. — See [**3**, Corollary 5.3] or [**9**, Chapter 7, §7.3, Theorem 7.7]. □

We are going to translate conditions of Theorem 1.1 into the algebra $\mathbb{F}_p^{nc}[\![X_1, \cdots, X_d]\!]$.

1.1.1. Filtred and graded algebras. — The results of this section can be found in [**1**].
• Let $E := \mathbb{F}_p^{nc}[\![X_1, \cdots, X_d]\!]$ be the algebra of series in noncommuting variables $X_1, \cdots, X_d$ with coefficients in $\mathbb{F}_p$. We consider now non-commutative multi-indices $\alpha = (\alpha_1, \cdots, \alpha_n)$, with $\alpha_i \in \{1, \cdots, d\}$, and we denote by X_α the monomial element of the form $X_\alpha := X_{\alpha_1} \cdots X_{\alpha_n}$. We endow each X_i with degree 1; and we denote by $\deg(X_\alpha)$ the degree of X_α which is $|\alpha|$.
For $Z = \sum_\alpha a_\alpha X_\alpha$, the quantity $\omega(Z) := \min_{a_\alpha \neq 0}\{\deg(X_\alpha)\}$ is the valuation of Z, with the convention that $\omega(0) = \infty$. For $n \geqslant 0$, put $E_n := \{Z \in E, \omega(Z) \geqslant n\}$. Observe that E_1 is the augmentation ideal of E: this is the two-sided ideal of E topologically generated by the X_i's. The algebra E is filtered by the E_n's and its graded algebra $\mathrm{Grad}(E)$ is then:

$$\mathrm{Grad}(E) := \bigoplus_{n \in \mathbb{Z}_{\geqslant 0}} E_n/E_{n+1} \simeq \mathbb{F}_p^{nc}[X_1, \ldots, X_d].$$

In other words, $\mathrm{Grad}(E)$ is isomorphic to the non-commutative polynomial algebra $A := \mathbb{F}_p^{nc}[X_1, \ldots, X_d]$, where each X_i is endowed with formal degree 1. Let $A_n := \{z \in A, \omega(z) \geqslant n\}$ be the filtration of A; observe that A_1 is the augmentation ideal of A.

• Let $X_\alpha, X_{\alpha'}$ be two monomials (viewed in E or in A). The element X_α is said to be a *submonomial* of $X_{\alpha'}$, if $X_{\alpha'} = X_\beta X_\alpha X_{\beta'}$, with $X_\beta, X_{\beta'}$ two monomials of A.

Definition 1.2. — A family $\mathscr{F} = \{X_{\alpha(i)}\}_{i \in I}$ of monomials of A is combinatorially free if for all $i \neq j$:

(i) $X_{\alpha(i)}$ is not a submonomial of $X_{\alpha(j)}$,
(ii) if $X_{\alpha(i)} = X_\alpha X_\beta$ and $X_{\alpha(j)} = X_{\alpha'} X_{\beta'}$, then $X_\alpha \neq X_{\beta'}$, with $X_\alpha, X_\beta, X_{\alpha'}, X_{\beta'}$ nontrivial monomials, *i.e.* different from 1.

The monomials may be endowed with a total order $<$ as follows. First let us consider the natural ordering $<'$ defined by: $X_1 <' X_2 <' \cdots <' X_d$.

Definition 1.3. — Let X_α and X_β be two monomials. We say that $X_\alpha > X_\beta$, if $\omega(X_\alpha) < \omega(X_\beta)$. If X_α and X_β have the same valuation, we use the lexicographic order induced by $<'$.

Now, let $Z = \sum_\alpha a_\alpha X_\alpha$ be a nonzero element of E, with $a_\alpha \in \mathbb{F}_p$. Then $\widehat{Z} := \max\{X_\alpha,\ a_\alpha \neq 0\}$ is the *highest term* respecting the order $<$. Observe that $\widehat{Z} \in A$.

• Let $C = A\mathscr{F}A$ be the two-sided A-ideal generated by $\mathscr{F} := \{Z_i\}_{i\in I}$, where $\mathscr{F}$ is a locally finite graded subset of A_1; in particular I is countable. Let $B := A/C$ be the quotient endowed with the quotient filtration; we denote by $P_B(t) := \sum_{n\in\mathbb{Z}_{\geqslant 0}} \dim(B_n/B_{n+1}) \cdot t^n$ the Poincaré series of B. Observe that the family $\mathscr{F}$ generates the B-module C/CA_1.

***Theorem 1.4* (Anick).** — *If the family $\{\widehat{Z}\}_{i\in I}$ is combinatorially free, then*

(i) C/CA_1 is a free B-module over the Z_i's, and

(ii) $P_B(t) = \big(1 - dt + \sum_{i\in I} t^{n_i}\big)^{-1}$, where $n_i := \omega(Z_i)$.

Proof. — See [**1**, Theorems 2.6 and 3.2]. □

If C/CA_1 is a free B-module over the Z_i's, we say that the family $\mathscr{F} = \{Z_i\}_{i\in I}$ is *strongly free* (see [**1**]).

Example 1.5. — Take $d = 5$. Let $a_n \geqslant 1$ be an increasing sequence, and consider the family $\mathscr{F} = \{X_5X_3, X_4X_2, X_4X_3, X_5X_2, X_5X_1, X_5X_4^{a_n}X_1, n \geqslant 1\}$. Put $B := A/A\mathscr{F}A$. Then $\mathscr{F}$ is combinatorially free, and $P_B(t) = \big(1 - 5t + t^2 \sum_{n\geqslant 1} t^{a_n}\big)^{-1}$.

1.1.2. Pro-p groups of cohomological dimension $\leqslant 2$ and polynomial algebras. — Let F be a free pro-p group on d generators $x_1, \cdots, x_d$. Let $\Lambda_F := \mathbb{F}_p[\![F]\!]$ be the complete group algebra over F. Recall that Λ_F is isomorphic to the Magnus algebra E; this isomorphism φ is given by $x_i \mapsto X_i + 1$ (see for example [**9**, Chapter 7, §7.6, Theorem 7.16]). Let us endow E with the filtration and the ordering of §1.1.1. So $\varphi : \Lambda_F \xrightarrow{\simeq} E$ becomes a filtered isomorphism, and consequently one can endow Λ_F with the valuation ω_F defined as follows: $\omega_F(z) := \omega(\varphi(z))$. Observe that $E_1 \simeq I_F := \ker(\Lambda_F \to \mathbb{F}_p)$; that is, E_1 is isomorphic to the augmentation ideal of Λ_F.

Take $x \in F$, nontrivial. Then the degree $\deg(x)$ of x is defined as $\deg(x) := \omega_F(x-1) = \omega(\varphi(x-1))$. We denote by $\widehat{x} \in A$ the highest term of $\varphi(x-1) \in E$; we say that $\widehat{x}$ is the highest term of x.

Example 1.6. — Take $d \geqslant 3$ with the lexicographic ordering $X_1 < X_2 < X_3 < \cdots < X_d$.

(i) The highest term of $[x_1, [x_2^{p^n}, x_3]]$ is $X_3X_2^{p^n}X_1$, $n \geqslant 1$.

(ii) Given $x, y \in F$, let us write $f_x(y) = [x, y] \in F$. Then the highest term of $f_{x_1} \circ f_{x_2}^{\circ n}(x_3)$ is $X_3X_2^nX_1$, $n \geqslant 1$.

Let G be a pro-p group of p-rank d, and let $1 \to R \to F \to G \to 1$ be a minimal presentation of G by F; this induces a filtered morphism $\theta : \Lambda_F \to \Lambda_G$. We now endow Λ_G with the induced valuation ω_G of ω_F as follows: for $z \in \Lambda_G$, let us define

$$\omega_G(z) := \max\{\omega_F(z'), z' \in \Lambda_F, \theta(z') = z\}.$$

Put $E_{G,n} := \{z \in \Lambda_G, \omega_G(z) \geqslant n\}$, the filtration of Λ_G. Then $\mathrm{Grad}(\Lambda_G) := \bigoplus_n E_{G,n}/E_{G,n+1}$ is the graded algebra of $\mathbb{F}_p[\![G]\!]$ respecting the quotient filtration with $P_G(t) := \sum_{n\geqslant 0} \dim E_{G,n}/E_{G,n+1} \cdot t^n$ as Poincaré series.

For $n \geqslant 1$, put $F_n := \{x \in F, \varphi(x-1) \in E_n\}$, and $G_n := F_nR/R$. The sequences (F_n) and (G_n) are the Zassenhaus filtrations of F and G. The filtration $(E_{G,n})$ also corresponds to the filtration coming from the augmentation ideal of Λ_G (see [**12**, Appendice A.3, Théorème 3.5]).

Theorem 1.7. — *Let $\mathscr{F} = \{\rho_i\}_{i\in I}$ be a family of elements of R which generates R as closed normal subgroup of F. If $\{\widehat{\rho_i}\}_{i\in I}$ is combinatorially free, then*

(i) $R/R^p[R,R] \simeq \prod_{i\in I} \Lambda_G$, $cd(G) \leqslant 2$, *and* $\dim H^2(G) = |I|$;

(ii) $P_G(t) = \big(1 - dt + \sum_{i\in I} t^{n_i}\big)^{-1}$, *where* $d = d_pG$, *and* $n_i := \deg(\rho_i) = \omega(\widehat{\rho_i})$.

Proof. — When the set of indices I is finite, this version can be found in [**4**]. We show here that the result also holds when I is infinite. First, observe that as $\{\widehat{\rho_i}\}_{i\in I}$ is combinatorially free then I is countable infinite, and $\mathscr{F}$ is a convergent family.

For $i \in I$, put $Y_i := \varphi(\rho_i - 1) \in E_1$; $n_i = \omega(Y_i)$. Let $I(R) \subset E_1$ be the closed two-sided ideal of E_1 topologically generated by the Y_i's, $i \in I$; one has $\ker(\theta) \simeq I(R)$ (see for example [**9**, Chapter 7, §7.6, Theorem 7.17]). Let us recall now that one has the topological G-isomorphism $R/R^p[R,R] \simeq I(R)/I(R)E_1$ (see for example [**4**, Proposition 4.3]). We want some informations on the G-module $R/R^p[R,R]$, and then on $I(R)/I(R)E_1$.

For $i \in I$, let $Z_i \in A$ be the initial form of $Y_i \in E_1$ defined as follows: let us write $Y_i = Z_{i,n_i} + Z_{i,n_i+1} + \cdots$, where $n_i = \omega(Y_i)$ and where $Z_{i,j}$ are homogeneous polynomials of degree j (possibly $Z_{i,j} = 0$); then put $Z_i := Z_{i,n_i}$. Observe that $\widehat{\rho_i} = \widehat{Y_i} = \widehat{Z_i}$.

Let C be the closed two-sided ideal of A generated by the family $\{Z_i\}_{i\in I}$. Since the family $\{\widehat{\rho_i}\}_{i\in I}$ is combinatorially free then by Theorem 1.4 the family $\{Z_i\}_{i\in I}$ is strongly free. Put $B := A/C$.

Proposition 1.8. — *One has $C = \mathrm{Grad}(I(R)) \subset A$. In particular, as graded A-modules, one gets $\mathrm{Grad}(\Lambda_G) \simeq B$, and*

$$\mathrm{Grad}(I(R)/I(R)E_1) \simeq C/CA_1 \simeq \bigoplus_{i\in I} BZ_i \simeq \bigoplus_{i\in I} B[n_i],$$

where $B[n_i]$ means B as A-module with an n_i-shift filtration.

Proof. — This is only a slight generalization of the case I finite; see proof of [**4**, Theorem 3.7]. □

Then by Theorem 1.4 and Proposition 1.8 we first get

$$P_G(t) = P_B(t) = \big(1 - dt + \sum_{i\in I} t^{n_i}\big)^{-1}.$$

Consider now the continuous morphism

$$\Psi : \prod_{i\in I} \Lambda_G \to I(R)/I(R)E_1 \simeq R/R^p[R,R],$$

which sends (a_i) to $\sum_i a_i Y_i \pmod{I(R)E_1}$. Since $n_i \to \infty$ with i, the morphism Ψ is well-defined. Remember that $\Lambda_G \simeq E/I(R)$.

Lemma 1.9. — *The map Ψ is surjective.*

Proof. — Put $W := \{\sum_{i\in I} a_i Y_i, a_i \in E\} \subset I(R)$. Then

$$I(R) = WE = W\mathbb{F}_p + WE_1 = W + WE_1.$$

We conclude by noticing that $WE_1 \subset I(R)E_1$. □

Set $N := \ker(\Psi)$. Therefore one gets a sequence of filtered G-modules:

$$1 \to N \to \prod_{i\in I} \Lambda_G[n_i] \xrightarrow{\Psi} I(R)/I(R)E_1 \to 1.$$

This one induces the following sequence of graded A-modules:

$$0 \to \mathrm{Grad}(N) \to \mathrm{Grad}(\prod_{i\in I} \Lambda_G[n_i]) \to \mathrm{Grad}(I(R)/I(R)E_1) \to 0.$$

For the surjectivity, use the fact that I is countable. Now since $n_i \to \infty$ with i, then

$$\mathrm{Grad}\big(\prod_{i\in I} \Lambda_G[n_i]\big) = \mathrm{Grad}\big(\bigoplus_{i\in I} \Lambda_G[n_i]\big) \simeq \bigoplus_{i\in I} B[n_i].$$

By Proposition 1.8, we finally get that Ψ induces an isomorphism between $\mathrm{Grad}\big(\prod_{i\in I} \Lambda_G[n_i]\big)$ and $\mathrm{Grad}\big(I(R)/I(R)E_1\big)$, which implies $\mathrm{Grad}(N) = 0$, then $N = 0$. Hence, as G-modules, $\prod_{i\in I} \Lambda_G \simeq I(R)/I(R)E_1 \simeq R/R^p[R,R]$. One concludes by applying Theorem 1.1. □

Remark 1.10. — The conclusions of Theorem 1.7 also hold if $\{\widehat{\rho}_i\}_{i\in I}$ is strongly free.

1.1.3. Cup-products and cohomological dimension. — Here we assume $p > 2$.
Let G be a pro-p group of p-rank d which is not free pro-p. Recall that the cup product maps $H^1(G) \otimes H^1(G)$ to $H^2(G)$. Labute in [**10**] gave a criterion involving cup-products so that $cd(G) = 2$. This point of view has been developed by Forré in [**4**].

***Theorem 1.11* (Forré)**. — *Let $p > 2$ be a prime number. Let G be a finitely presented pro-p group which is not free pro-p. Suppose that $H^1(G) = U \oplus V$ with U and V such that $U \cup U = 0$ and $U \cup V = H^2(G)$. Then $cd(G) = 2$, and G can be described by d generators and r relations $\rho_1, \cdots, \rho_r$ such that the highest term of each ρ_i is of the form $X_{t(i)}X_{s(i)}$ for some $s(i), t(i)$ such that $s(i) \leqslant \dim V < t(i)$, and $(s(i), t(i)) \neq (s(j), t(j))$ for $i \neq j$.*

Proof. — See the proof of [**4**, Theorem 6.4, Corollary 6.6] with the choice of the ordering $X_1 < X_2 < \cdots < X_d$. □

Let us make the following observation: given $n \geqslant 1$, according to Example 1.6 one can find some $x \in F$ for which the highest term is of the form $X_k X_j^n X_i$, for $i < j < k$.

Corollary 1.12. — *Under the assumptions of Theorem 1.11, suppose $c := \dim V \geqslant 2$. For some fixed $1 < i_0 \leqslant c < j_0 \leqslant d$, and $n \geqslant 1$, let $x_n \in F$ with highest term $X_{j_0}X_{i_0}^n X_1$. Suppose moreover that $r < (d-c)(c-1)$. Then there exists (i_0, j_0) such that the family $\{\widehat{\rho_1}, \cdots, \widehat{\rho_r}, \widehat{x_n}, n \geqslant 1\}$ is combinatorially free. In particular, for such (i_0, j_0) one has:*

- *(i) the cohomological dimension of the quotient $\Gamma := F/\langle \rho, \cdots, \rho_r, x_n, n \in \mathbb{Z}_{>0}\rangle^{Nor}$ of G is smaller than 2;*
- *(ii) $\dim H^2(\Gamma) = \infty$;*
- *(iii) $P_\Gamma(t) = \big(1 - dt + rt^2 + t^3 \sum_{n\geqslant 0} t^n\big)^{-1}$.*

Proof. — According to Theorem 1.11, for $i = 1, \cdots, r$, the highest term of ρ_i is of the form $X_{t(i)}X_{s(i)}$ for some $s(i) \leqslant c < t(i)$, and the family $\mathscr{E} := \{X_{t(1)}X_{s(1)}, \cdots, X_{t(r)}X_{s(r)}\}$ is combinatorially free. Now, since $r < (d-c)(c-1)$ and $c \geqslant 2$, we can find (i_0, j_0) such that $X_{j_0}X_{i_0}$ is not in $\mathscr{E}$; therefore $\mathscr{E} \cup \{X_{j_0}X_{i_0}^n X_1, n \in \mathbb{Z}_{>0}\}$ is combinatorially free. And we can apply Theorem 1.7. □

Remark 1.13. — In fact $r \leqslant (d-c)c-2$ is enough. Indeed, with such a condition one has $X_{j_0}X_{i_0} \notin \mathscr{E}$ for some $(i_0,j_0) \neq (1,r)$, $i_0 \leqslant c < j_0 \leqslant r$. Hence if $i_0 \neq 1$, the family $\mathscr{E} \cup \{X_{j_0}X_{i_0}^n X_1, n \in \mathbb{Z}_{>0}\}$ is combinatorially free. Otherwise $j_0 \neq r$, and take $\mathscr{E} \cup \{X_r X_{j_0}^n X_{i_0}, n \in \mathbb{Z}_{>0}\}$.

1.2. Arithmetic background. — Let p be a prime number, and let K be a number field. For $p=2$, assume K totally imaginary. Let S and T be two disjoint finite sets of K. We assume moreover S tame. We denote by $Cl_K^T(p)$ the p-Sylow of the T-class group of K. Let K_S^T/K be the maximal pro-p extension of K unramified outside S where each $\mathfrak{p} \in T$ splits completely; put $G_S^T := Gal(K_S^T/K)$. Let us recall Shafarevich's formula (see for example [**5**, Chapter I, §4, Theorem 4.6]):

$$d_p G_S^T = |S| - (r_1+r_2) + 1 - |T| - \delta_{K,p} + \dim V_S^T/(K^\times)^p,$$

where

$$V_S^T = \{x \in K^\times,\ x \in (K_\mathfrak{p}^\times)^p U_\mathfrak{p}\ \forall x \notin S \cup T,\ x \in (K_\mathfrak{p}^\times)^p\ \forall \mathfrak{p} \in S\},$$

and where $\delta_{K,p} = 1$ if K contains μ_p (the p-roots of 1), 0 otherwise. Here as usual, $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$, and $U_\mathfrak{p}$ is the group of local units of $K_\mathfrak{p}$. Observe that if there is no p-extension of $K(\mu_p)$ unramified outside T and p in which each prime of S splits completely, then $V_S^T/(K^\times)^p$ is trivial: this is a Chebotarev condition type.

Schmidt in [**15**] showed that G_S^T may be *mild* following the terminology of Labute [**10**]. More precisely, he proved:

***Theorem 1.14* (Schmidt).** — *Let K be a number field and let p be a prime number. For $p=2$ suppose K totally imaginary. Let S_0 and T be two disjoint finite sets of prime ideals of K with S_0 tame. Assume T sufficiently large so that $Cl_K^T(p)$ is trivial; when $\mu_p \subset K$, assume moreover that T contains all prime ideals above p. Then there exist infinitely many finite tame sets S containing S_0 such that $H^1(G_S^T) = U \oplus V$, where the subspaces U and V satisfy: (i) $U \cup U = 0$; (ii) $U \cup V = H^2(G_S^T)$. Moreover, one has* $\dim H^2(G_S^T) = \dim H^1(G_S^T) + r_1 + r_2 + |T| - 1$.

Theorem 1.14 is not in this form in [**15**]: the result presented here can be found in the proof of Theorem 6.1 of [**15**].

At this level, following [**15**] let us compute the value of $c = \dim V$.

When $\mu_p \not\subset K$, we expand S_0 so that for every $\mathfrak{p} \in S_0$, $d_p G_{S_0\backslash\{\mathfrak{p}\}}^T = |S_0| - r_1 - r_2 - |T|$, which is equivalent by Shafarevich's formula to the triviality of $V_{S_0\backslash\{\mathfrak{p}\}}^T/(K^\times)^p$.

When $\mu_p \subset K$, we expand S_0 so that the set of the Frobenius elements at $\mathfrak{p}$ in G_T^{el} when $\mathfrak{p}$ ranges over S_0, corresponds to the set of the nontrivial elements of G_T^{el}; here $G_T^{el} = Gal(K_T^{el}/K)$, where K_T^{el} is the maximal elementary abelian p-extension of K inside K_T. One also has $V_{S_0\backslash\{\mathfrak{p}\}}^T/(K^\times)^p = \{1\}$.

The set S of Theorem 1.14 contains S_0, and is of size $2|S_0|$; the prime ideals $\mathfrak{p} \in S - S_0$ are choosen with respect to some local conditions, according to Chebotarev density theorem. Moreover $U = H^1(G_{S_0}^T, \mathbb{F}_p)$, and the subspace V is such that $\dim V = c = |S_0|$. See [**15**, Proof of Theorem 6.1] for more details.

Lemma 1.15. — *Under the previous assumptions, each prime $\mathfrak{p} \in S$ is ramified in the maximal elementary abelian p-extension $K_S^{T,el}/K$ inside K_S^T.*

Proof. — Observe first that if $S'' \subset S'$, then $V_{S'}^T/(K^\times)^p \hookrightarrow V_{S''}^T/(K^\times)^p$. Hence afforded by the choice of S_0, one has: for every $\mathfrak{p} \in S$, $V_{S\backslash\{\mathfrak{p}\}}^T/(K^\times)^p$ is trivial. Then by Shafarevich's formula, one gets $d_pG_S^T = 1 + d_pG_{S\backslash\{\mathfrak{p}\}}^T$, showing that $\mathfrak{p}$ is ramified in $K_S^{T,el}/K$. □

Put $\alpha_{K,T} = 3 + 2\sqrt{2 + r_1 + r_2 + |T|}$. By obvious arguments one finds:

Lemma 1.16. — *If $d_pG_S^T > \alpha_{K,T}$, then $d_pG_S^T + r_1 + r_2 + |T| - 1 < (d-c)(c-1)$ for every $c \in [2, d]$.*

Let us finish this part with an obvious observation.

Remark 1.17. — If G_S^T is not trivial and such that $cd(G_S^T) \leqslant 2$, then $cd(G_S^T) = 2$.

2. Example and proof

2.1. Example. — • Take $p > 2$, and $K = \mathbb{Q}$. In this case the relations of the pro-p groups G_S are all local: this is the description due to Koch [**9**, Chapter 11, §11.4, Example 11.11]. Let ℓ be a prime number such that $p|\ell - 1$. Denote by $\mathbb{Q}_\ell$ the (unique) cyclic extension of $\mathbb{Q}$ of degree p unramified outside ℓ.
Let $S = \{\ell_1, \cdots, \ell_d\}$ be a set of d different primes such that $\ell_i \equiv 1 (\mathrm{mod}\ p)$. The pro-$p$ group G_S can be described by generators $x_1, \cdots, x_d$, and relations $\rho_1, \cdots, \rho_d$ such that

$$\rho_i \equiv \prod_{j \neq i} [x_i, x_j]^{a_j(i)} \ (\mathrm{mod}\ F_3), \tag{1}$$

where $a_j(i) \in \mathbb{Z}/p\mathbb{Z}$, and where each x_i is a generator of the inertia group of ℓ_i. The element $a_j(i)$ is zero if and only if the prime ℓ_i splits in $\mathbb{Q}_{\ell_j}/\mathbb{Q}$, which is equivalent to $\ell_i^{(\ell_j-1)/p} \equiv 1 (\mathrm{mod}\ \ell_j)$.
• Take $p = 3$, $S_0 = \{7, 13\}$, and $T = \emptyset$. Put $S = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5\}$ with $\ell_1 = 31, \ell_2 = 19, \ell_3 = 13, \ell_4 = 337, \ell_5 = 7$. Then the highest terms of the relations (1), viewed in $\mathbb{F}_p^{nc}[X_1, \cdots, X_5]$, are: $\widehat{\rho_1} = X_1X_3$, $\widehat{\rho_2} = X_2X_4$, $\widehat{\rho_3} = X_2X_3$, $\widehat{\rho_4} = X_1X_4$, $\widehat{\rho_5} = X_1X_5$. Since the $\widehat{\rho_i}$'s are combinatorially free, G_S is of cohomological dimension 2 by Theorem 1.7.
Now for each $n > 0$, let us choose a prime number ℓ_n of $\mathbb{Z}$ such that the highest term of a lift x_n in F of its Frobenius element $\sigma_n \in G_S$, is of the form $X_5X_4^nX_1$ (which is possible by Example 1.6, see next section). Next consider the maximal Galois subextension $L/\mathbb{Q}$ of $\mathbb{Q}_S/\mathbb{Q}$ fixed by all the conjuguates of the σ_n's (this is the "cutting towers" strategy of [**7**]). Put $G := Gal(L/\mathbb{Q})$. Then the pro-3 group G can be described by generators $x_1, \cdots, x_5$, and relations $\{\rho_1, \cdots, \rho_5, x_n, n \in \mathbb{Z}_{>0}\}$ (which is not *a priori* a minimal set). By construction, the ℓ_n's split totally in $L/\mathbb{Q}$. Observe now that

$$\{\widehat{\rho_1}, \cdots, \widehat{\rho_5}, \widehat{x_n}, n \geqslant 1\} = \{X_5X_1, X_5X_2, X_4X_3, X_4X_2, X_5X_3, X_5X_4^nX_1, n \in \mathbb{Z}_{>0}\},$$

which is combinatorially free. By Theorem 1.7 the pro-3-group G is of cohomological dimension 2, $H^2(G)$ is infinite, and $P_G(t) = \big(1 - 5t + 5t^2 + t^3(1 + t + t^2 + \cdots)\big)^{-1}$.

2.2. Proof of the main result. — • Take $p > 2$. Let S_0 and T be two finite disjoint sets of prime ideals of K, where S_0 is tame. Take T sufficiently large so that $Cl_K^T(p)$ is trivial. When K contains μ_p, assume moreover that T contains all p-adic prime ideals.

First take S containing S_0 as in Theorem 1.14, and sufficiently large so that $d := d_pG_S^T > \alpha_{K,T}$. Put $G = G_S^T$. Here $r = \dim H^2(G) = d + r_1 + r_2 - 1 + |T|$.

Let us start with a minimal presentation of G:

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1.$$

By Theorem 1.14 and Theorem 1.11, the subgroup R can be generated as normal subgroup by some relations $\rho_1, \cdots, \rho_r$ such that the highest terms $\widehat{\rho_k}$ are of the form X_iX_j for some $i \leqslant c < j$, where $c = \dim V$. Observe that since G is FAb then $c \in [2, d-2]$.
Given $n \geqslant 1$, the quotient G/G_{n+1} is finite. Put $K_{(n+1)} := (K_S^T)^{G_{n+1}}$. For $n \geqslant 1$, take $x_n \in F_{n+2} \backslash F_{n+3}$. By Chebotarev density theorem there exists some prime ideal $\mathfrak{p}_n \subset \mathscr{O}_K$ such that $\sigma_{\mathfrak{p}_n}$ is conjuguate to x_n in $Gal(K_{(n+3)}/K)$; here $\sigma_{\mathfrak{p}_n} \in G$ denotes the Frobenius element of $\mathfrak{p}_n$. Now take $z_n \in F$ such that $\varphi(z_n) = \sigma_{\mathfrak{p}_n}$. Then $z_n \equiv \sigma_{\mathfrak{p}_n} \pmod{RF_{n+3}}$. In other words, there exists $y_n \in F_{n+3}$, $\alpha_n \in F$, and $r_n \in R$ such that $\alpha_n z_n \alpha_n^{-1} = x_n y_n r_n$.
Set $\Sigma := T \cup \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots\}$, and consider K_S^Σ the maximal pro-p extension of K unramified oustide S and where each primes $\mathfrak{p}$ of Σ splits completely. Put $G_S^\Sigma := Gal(K_S^\Sigma/K)$. Then

$$G_S^\Sigma \simeq G/\langle \sigma_{\mathfrak{p}_n}, n \in \mathbb{Z}_{>0} \rangle^{Nor}.$$

Here $\langle \sigma_{\mathfrak{p}_n}, n \in \mathbb{Z}_{>0} \rangle^{Nor}$ is the normal closure of $\langle \sigma_{\mathfrak{p}_n}, n \in \mathbb{Z}_{>0} \rangle$ in G. Therefore K_S^Σ/K satisfies (i) of Theorem A. But observe now that

$$G/\langle \sigma_{\mathfrak{p}_n}, n \in \mathbb{Z}_{>0} \rangle^{Nor} \simeq F/\langle \rho_1, \cdots, \rho_r, z_n, n \in \mathbb{Z}_{>0} \rangle^{Nor} = F/\langle \rho_1, \cdots, \rho_r, x_n y_n, n \in \mathbb{Z}_{>0} \rangle^{Nor}.$$

For $n \geqslant 1$, the highest term of $x_n y_n$ is equal to the highest term of x_n; therefore it is enough to choose the x_n's as in Corollary 1.12 which is possible: indeed since $d > \alpha_{K,T}$, by Lemma 1.16, one has $r < (c-1)(d-c)$ for every $c \in [1, d-1]$. Afforded by Corollary 1.12, one gets (ii), (iii), and (v) of Theorem A.

Let us proof (iv). By Lemma 1.15 each prime ideal $\mathfrak{p} \in S$ is ramified in $K_S^{T,el}/K$, showing that $\tau_\mathfrak{p} \in G$ is not in $RF^p[F,F]$, where $\tau_\mathfrak{p} \in G$ is a generator of the inertia group at $\mathfrak{p}$. Therefore $d_p G_S^\Sigma = d_p G$, and then every prime $\mathfrak{p} \in S$ is ramified in K_S^Σ/K. But since G is torsion-free (because $cd(G) = 2$), then $\langle \tau_\mathfrak{p} \rangle \simeq \mathbb{Z}_p$, and the local extension $(K_S^\Sigma)_\mathfrak{p}/K_\mathfrak{p}$ must be maximal.

• Assume $p = 2$, and suppose K totally imaginary. Then Theorem 1.14 holds, but Theorem 1.11 does not. As explained by Forré in [**4**, Proof Theorem 6.4], one has to take two orderings to show that the highest terms of the relations $\rho_1, \cdots, \rho_r$ are strongly free. Now in this context the strategy of the approximation of the x_n's by some Frobenius elements as in Corollary 1.12 also applies. Along the same lines as in the proof of Theorem 6.4 in [**4**], and by choosing the x_n's as for $p \neq 2$, we observe that the initial forms of the new relations $\{\rho_1, \cdots, \rho_r, x_n, n \geqslant 1\}$ are still strongly free. We conclude by invoking Remark 1.10. □

References

[1] D. J. Anick, *Non-commutative graded algebras and their Hilbert series*, J. of Algebra **78** n1 (1982), 120-140.

[2] D. J. Anick, *Inert sets and the Lie algebra associated to a group*, J. Algebra **111** (1987), 154-165.

[3] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. of Algebra **4** (1966), 442-470

[4] P. Forré, *Strongly free sequences and pro-p-groups of cohomological dimension* 2, J. reine u. angew. Math **658** (2011), 173-192.

[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, C. Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), 35-53.

[7] F. Hajir, C. Maire, R. Ramakrishna, *Cutting towers of number fields*, 2019, arXiv:1901.04354.

[8] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japon **35** (1983), no4, 693-709.

[9] H. Koch, Galois Theory of p-Extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

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

[11] J. Labute, J. Mináč, *Mild pro-2-groups and 2-extensions of* $\mathbb{Q}$ *with restricted ramification*, J. Algebra **332** (2011), 136–158.

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

[13] P. Lebacque, *Quelques résultats effectifs concernant les invariants de Tsfasman-Vladut*, Ann. Inst. Fourier **65** (2015), no. 1, 63–99.

[14] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, GMW 323, corr. 2nd ed., Springer-Verlag Berlin Heidelberg, 2013.

[15] A. Schmidt, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010), 203-235.

[16] M. Tsfasman and S. Vladut, *Infinite global fields and the generalized Brauer-Siegel theorem.* Dedicated to Yuri I. Manin on the occasion of his 65th birthday, Mosc. Math. J. **2** (2002), no 2, 329-402.

June 22, 2020

Oussama Hamza, Ecole Normale Supérieure de Lyon, Université de Lyon, 15 parvis René Descartes, 69342 Lyon Cedex 07, France • *E-mail :* `oussama.hamza@ens-lyon.fr`

Christian Maire, Institut FEMTO-ST, Université Bourgogne Franche-Comté, 15B Avenue des Montboucons, 25030 Besançon Cedex, France • *E-mail :* `christian.maire@univ-fcomte.fr`