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

Oussama Hamza, Christian Maire

To cite this version:

Oussama Hamza, Christian Maire. A NOTE ON ASYMPTOTICALLY GOOD EXTENSIONS IN WHICH INFINITELY MANY PRIMES SPLIT COMPLETELY. 2020. hal-02489967

HAL Id: hal-02489967
https://hal.science/hal-02489967
Preprint submitted on 24 Feb 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 [7].

Let $K$ be a number field, and let $L/K$ be an infinite unramified extension. Denote by $\mathcal{S}_{L/K}$ the set of prime ideals of $K$ that split completely in $L/K$. In [8] Ihara proved that $\sum_{p \in \mathcal{S}_{L/K}} \log N(p)/N(p) < \infty$, and raised the following interesting question: are there $L/K$ for which $\mathcal{S}_{L/K}$ is infinite? This question was recently answered in the positive by Hajir, Maire, and Ramakrishna in [7]. In fact, infinite unramified extensions $L/K$ are some special cases of infinite extensions for which the root discriminants $\text{rd}_F := |\text{Disc}_F|^{1/[F:Q]}$ are bounded, where the number fields $F$ vary in $L/K$, and $\text{Disc}_F$ 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 $\mathcal{S}_{L/K}$ still holds (see for example [16], or [13] for the study of such extensions).

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 $p \in S$ is such that $|\mathcal{O}_K/p| \equiv 1 \pmod{p}$); the set $S$ is called tame. Let $K_S$ be the maximal pro-$p$ extension of $K$ unramified outside $S$, put $G_S = \text{Gal}(K_S/K)$. 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 Golod-Shafarevich criterion, it is well-known that $K_S/K$ is infinite when $|S|$ is large as compared to $[K:Q]$ (see for example [14, Chapter X, §10, Theorem 10.10.1]), and then asymptotically good. E.g. for $p > 2$, $\mathbb{Q}_S/\mathbb{Q}$ is infinite when $|S| \geq 4$. In [7] the authors showed that when $S$ is large, there exist infinite subextension

\textbf{2000 Mathematics Subject Classification.} — 11R37, 11R29.

\textbf{Key words and phrases.} — Pro-$p$ extensions with restricted ramification, asymptotically good extensions, mild pro-$p$ extensions.

The authors thank Farshid Hajir for useful comments, and Philippe Lebacque for his interest in this work. CM was partially supported by the ANR project FLAIR (ANR-17-CE40-0012), and by the EIPHI Graduate School (ANR-17-EURE-0002).
L/K of K_S/K for which the set \( \mathcal{A}_{L/K} \) is infinite. But they give no information about the structure of \( \text{Gal}(L/K) \). 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 exist an infinite pro-\( p \) extension \( L/K \) such that

(i) the set \( \mathcal{A}_{L/K} \) of places that split completely in \( L/K \) contains \( T \);
(ii) the set \( \mathcal{A}_{L/K} \) is infinite;
(iii) the pro-\( p \) group \( G = \text{Gal}(L/K) \) is of cohomological dimension 2;
(iv) the minimal number of relations of \( G \) is infinite, i.e. \( \dim H^2(G, \mathbb{F}_p) = \infty \);
(v) for each \( p \in S \), the local extension \( L_p/K_p \) is maximal, i.e. isomorphic to \( \mathbb{Z}_p \times \mathbb{Z}_p \);
(vi) the Poincaré series of the algebra \( \mathbb{F}_p[G] \), endowed with the graduation from the ideal of augmentation, is equal to \( (1 - dt + rt^2 + t^3 \sum_{n \geq 0} t^n)^{-1} \), where \( d = \dim G_S \), 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.

The proof uses various tools. The first one is the strategy developed initially by Labute [10], then by Labute-Mináč [11], Schmidt [15], Forré [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 refine this idea when 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 in the polynomial algebra, due to Forré. In particular, this allows us to choose infinitely many Frobenius 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 §1.1.3 and Definition 1.2).

We conclude by cutting the tower \( K_S/K \) by all these Frobenius: 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 when \( K = \mathbb{Q} \), 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 \( H^1(G) \) the cohomology group \( H^1(G, \mathbb{F}_p) \). The \( p \)-rank of \( G \), which is equal to \( \dim H^1(G) \), is noted \( d_p G \).

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 \( p \).
1.1.1. Minimal presentation and cohomological dimension. — Let $G$ be a pro-$p$ group of finite 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 $F$. Let $\mathcal{F} := \{\rho_i\}_{i \in I}$ be an $F_p$-basis of $R/R^p[F,F]$; observe that $I$ is not necessarily finite. The algebra $\Lambda_G := F_p[G]$ acts on $R/R^p[R,R]$, and by Nakayama’s lemma the $\rho_i$’s generate topologically $R/R^p[R,R]$ as $\Lambda_G$-module (see for example [3, Corollary 1.5]).

Let us recall the definition of the cohomological dimension $\text{cd}(G)$ of $G$: it is the smallest integer $n$ (eventually $n = \infty$) such that $H^i(G) = 0$ for every $i \geq n + 1$.

**Theorem 1.1.** — The following assertions are equivalent:

1. $\text{cd}(G) \leq 2$;
2. $R/R^p[R,R]$ is a free compact $\Lambda_G$-module;
3. $R/R^p[R,R] \cong \prod_I \Lambda_G$.

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 in the algebra $F_p^n[X_1, \ldots, X_d]$.

1.1.2. Filtered and graded algebras. — The results of this section can be found in [1].

- Let $E = F_p^n[X_1, \ldots, X_d]$ be the algebra of noncommutative series in $X_1, \ldots, X_d$ with coefficients in $F_p$. We consider now noncommutative multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n)$, with $\alpha_i \in \{1, \ldots, d\}$, and we denote by $X_\alpha$ the monomial element of the form $X_\alpha = X_{\alpha_1} \cdots X_{\alpha_n}$. We endow each $X_i$ with the degree 1; the degree $\deg(X_\alpha)$ of $X_\alpha$ is $|\alpha|$.

For $Z = \sum_\alpha a_\alpha X_\alpha$, the quantity $\omega(Z) = \min_{\alpha \neq 0} (\deg(X_\alpha))$ is the valuation of $Z$, with the convention that $\omega(0) = \infty$. For $n \geq 0$, put $E_n = \{Z \in E, \omega(Z) \geq n\}$. 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 $\text{Grad}(E)$ is then:

$$\text{Grad}(E) = \bigoplus_{n \in \mathbb{Z}_{\geq 0}} E_n/E_{n+1} \cong F_p^n[X_1, \ldots, X_d].$$

In other words $\text{Grad}(E)$ is isomorphic to the noncommutative polynomial algebra $A := F_p^n[X_1, \ldots, X_d]$, where each $X_i$ is endowed with the formal degree 1. Let $A_n = \{z \in A, \omega(z) \geq n\}$ be the gradation of $A$; observe that $A_1$ is the augmentation ideal of $A$.

- Let $X_\alpha, X_{\beta'}$ be two monomials (viewed in $E$ or in $A$). The element $X_\alpha$ is 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 $\mathcal{F} = \{X_{\alpha(i)}\}_{i \in I}$ of monomials of $A$ is combinatorially free if for all $i \neq j$:

1. $X_{\alpha(i)}$ is not a submonomial of $X_{\alpha(j)}$;
2. if $X_{\alpha(i)} = X_\alpha X_\beta$ and $X_{\alpha(j)} = X_\alpha' X_\beta'$, then $X_\alpha \neq X_\alpha'$, with $X_\alpha, X_\beta, X_\alpha', X_{\beta'}$ non-trivial monomials, i.e. $\neq 1$.

The monomials may be endowed with a total order $<$ as follows.

First let us consider the natural ordering $<'$ defined by: $X_1 <' X_2 <' \cdots <' X_d$. 


Let $X_\alpha$ and $X_\beta$ two monomials, we say that $X_\alpha > X_\beta$, if $\omega(X_\alpha) < \omega(X_\beta)$; if $X_\alpha$ and $X_\beta$ have the same valuation, we use the lexicographic order induced by $<^\prime$.

Now, let $Z = \sum a_\alpha X_\alpha$ be a nonzero element of $E$, with $a_\alpha \in F_p$. Then $\hat{Z} := \max\{X_\alpha, a_\alpha \neq 0\}$ is the highest term respecting the order $<$.

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

**Theorem 1.3 (Anick).** — Let $\mathcal{F} = \{Z_i\}_{i \in I}$ be a locally finite graded subset of $A_1$, and let $C$ be a two-sided ideal of $A$ generated by the $Z_i$’s; put $B = A/C$. For each $i$, let $X_{\alpha(i)} := \hat{Z}_i$ be the highest term of $Z_i$. If the family $\{X_{\alpha(i)}\}_{i \in I}$ is combinatorially free, then

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

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

**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 $\mathcal{F} = \{Z_i\}_{i \in I}$ is strongly free (see [1]).

**Example 1.4.** — Take $d = 5$, and the lexicographic ordering $X_1 < X_2 < \cdots < X_5$. Let $a_n \geq 1$ be an increasing sequence, $n \geq 0$, and consider the family $\mathcal{F} = \{X_5X_3, X_4X_3, X_4X_2, X_5X_2, X_5X_1, X_5X^nX_1, n \geq 1\}$. Put $B = A/A \mathcal{F} A$. Then $\mathcal{F}$ is combinatorially free, and $P_B(t) = \left(1 - 5t + t^2 \sum_{n \geq 1} t^{n_1}\right)^{-1}$.

### 1.1.3. Pro-$p$ groups of cohomological dimension $\leq 2$ and polynomial algebra. — Let us conserve the notations of §1.1.1.

Let $F$ be a free pro-$p$ group on $d$ generators $x_1, \ldots , x_d$. Let $\Lambda_F := F_p[F]$ be the complete algebra associated to $F$. Recall that $F_p[F]$ is isomorphic to the Magnus algebra $E = F_{p^c}[X_1, \ldots , X_d]$; this isomorphism $\varphi$ 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 §1.1.2. The filtered isomorphism $\varphi : \Lambda_F \cong E$ allows us to endow $\Lambda_F$ with the valuation $\omega_F$ defined as follows: $\omega_F(z) = \omega(\varphi(z))$. Observe that $E_1 \cong F_p : \ker(\Lambda_F \rightarrow F_p)$, that is $E_1$ is isomorphic to the augmentation ideal of $\Lambda_F$.

Take $x \in F$, $x \neq 1$. Then the degree $\deg(x)$ of $x$ is defined as $\deg(x) := \omega_F(x - 1) = \omega(\varphi(x - 1))$. We denote by $\hat{x}$ the highest term of $\varphi(x - 1) \in E$. Hence $\hat{x}$ is a monomial.

**Example 1.5.** — Take $d \geq 3$ with the lexicographic ordering $X_1 < X_2 < X_3 < \cdots < X_d$.

(i) The highest term of $[x_1, [x_2^n, x_3]]$ is $X_3X_2^nX_1$.

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

Let $G$ be a pro-$p$ group of $p$-rank $d$, and let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a minimal presentation of $G$ by $F$; this induces a filtered morphism $\theta : \Lambda_F \rightarrow \Lambda_G$. We now endow $\Lambda_G$ with the induced valuation $\omega_G$ of $\omega_F$ as follows: for $z \in \Lambda_G$, let us define $\omega_G(z) = \max\{\omega_F(z'), z' \in \Lambda_F, \theta(z') = z\}$. 

4
Put $E_{G,n} = \{ z \in \Lambda_G, \omega_G(z) \geq n \}$, the filtration of $\Lambda_G$. Then $\text{Grad}(\Lambda_G) = \bigoplus_{n \geq 0} E_{G,n}/E_{G,n+1}$ is the graded algebra of $\mathbb{F}_p[[G]]$ respecting the quotient gradation with $P_G(t) = \sum_{n \geq 0} \dim E_{G,n}/E_{G,n+1} \cdot t^n$ as Poincaré series.

For $n \geq 1$, 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 $(E_{G,n})$ corresponds also to the filtration coming from the augmentation ideal of $\Lambda_G$ (see for example [12, Appendice A.3, Théorème 3.5]).

**Theorem 1.6.** — Let $\mathcal{F} = \{ \rho_i \}_{i \in I}$ be a family of generators $R/R^p[R,R]$. For each $i \in I$, let $X_{a(i)} = (\rho_i)_{i \in I} \in A$ be the highest term of $\rho_i$. If $\{ X_{a(i)} \}_{i \in I}$ is combinatorially free, then

1. $R/R^p[R,R] \simeq \bigoplus_{i \in I} \Lambda_G, \text{ and } \deg(G) \leq 2$;
2. $P_G(t) = (1 - dt + \sum_{i \in I} t^{n_i})^{-1}$, where $d = d_pG$, and $n_i = \deg(\rho_i) = \omega(X_{a(i)})$.

**Proof.** — When the set of indexes $I$ 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 $\{ X_{a(i)} \}_{i \in I}$ is combinatorially free then $I$ is countable infinite.

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 the topological $G$-isomorphism between $R/R^p[R,R]$ and $I(R)/I(R)E_1$ (see for example [4, Proposition 4.3]). We want to see 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 $Z_i$ are homogeneous polynomial of degree $j$ (eventually $Z_i = 0$); then put $Z_i = Z_i, n_i$. Observe that $\hat{\rho}_i = \hat{Y}_i = \hat{Z}_i$.

Let $C$ be the closed ideal of $A = \mathbb{F}_p[[X_1, \cdots, X_d]]$ generated by the family $\{ Z_i \}_{i \in I}$. As the family $\{ \hat{\rho}_i \}_{i \in I}$ is combinatorially free then by Theorem 1.3 the family $\{ Z_i \}_{i \in I}$ is strongly free. Put $B = A/C$.

**Proposition 1.7.** — One has $C = \text{Grad}(I(R)) \subset A$. In particular, as graded $A$-modules, one gets $\text{Grad}(\Lambda_G) \simeq B$, and

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

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

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

Then by Theorem 1.3 and Proposition 1.7 we firstly get

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

Consider now the continuous morphism

$$\Psi : \bigoplus_{i \in I} \Lambda_G \rightarrow I(R)/I(R)E_1 \simeq R/R^p[R,R],$$
sendind \((a_i)\) to \(\sum_i a_i Y_i \pmod{I(E)}\); as \(n_i \to \infty\) with \(i\), it is well-defined. Remember that \(\Lambda G \cong E/I(R)\). Put \(N = \ker(\Psi)\).

**Lemma 1.8.** — The map \(\Psi\) is surjective.

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

\[
I(R) = WE = W_F + WE_1 = W + WE_1.
\]

We conclude by observing that \(WE_1 \subset I(E)\).

Therefore one gets a sequence of filtered \(G\)-modules:

\[
1 \to N \to \prod_{i \in I} \Lambda G[n_i] \to I(R)/I(E) \to 1.
\]

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

\[
0 \to \text{Grad}(N) \to \text{Grad}(\prod_{i \in I} \Lambda G[n_i]) \to \text{Grad}(I(R)/I(E)) \to 0.
\]

For the surjectivity, use the fact that \(I\) is countable. Now as \(n_i \to \infty\) with \(i\), then

\[
\text{Grad}(\prod_{i \in I} \Lambda G[n_i]) = \text{Grad}(\bigoplus_{i \in I} \Lambda G[n_i]) \cong \bigoplus_{i \in I} B[n_i].
\]

By Proposition 1.7, we finally get that \(\Psi\) induces an isomorphism between \(\text{Grad}(\prod_{i \in I} \Lambda G[n_i])\) and \(\text{Grad}(I(R)/I(E))\), which implies \(\text{Grad}(N) = 0\), then \(N = 0\). Hence, as \(G\)-modules, \(\prod_{i \in I} \Lambda G \cong I(R)/I(E) \cong R/R_P[G,R]\), and we conclude with Theorem 1.1. 

**Remark 1.9.** — Conclusions of Theorem 1.6 also hold if \(\{P_i\}_{i \in I}\) is strongly free.

**Remark 1.10.** — For references on graded and filtered modules, see also [12, Chapter I and II].

1.1.4. *Cup-products and cohomological dimension.* — Here we suppose now \(p > 2\).

Let \(G\) be a pro-\(p\) group of \(p\)-rank \(d\) which is not pro-\(p\) free. Recall that the cup product sends \(H^1(G) \otimes H^1(G)\) to \(H^2(G)\). Labute in [10] gave a criterion involving cup-products so that cd\((G) = 2\). This point of view has been developped by Forrée in [4]. Let us recall it.

**Theorem 1.11 (Forrée).** — Let \(p > 2\) be a prime number. Let \(G\) be a finitely presented pro-\(p\) group which is not pro-\(p\) free. Suppose that \(H^1(G) = U \oplus V\) such that \(U \cup U = 0\) and \(U \cup V = H^2(G)\). Put \(c = \dim V\). Then cd\((G) = 2\), and \(G\) can be described by some relations \(\rho_1, \ldots, \rho_r\) such that the highest term of each \(\rho_i\) can be written as \(X_{s(i)} X_{t(i)}\) for some \(s(i), t(i)\) such that \(s(i) \leq c < t(i)\), and such that \((s(i), t(i)) \neq (s(j), t(j))\) for \(i \neq j\).

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

**Remark 1.12.** — Observe that the family \(\{X_{s(i)} X_{t(i)}\}_i\) of Theorem 1.11 is combinatorially free.
Before to present a corollary, let us make the following observation: given \( n \geq 1 \), thanks to Example 1.5, one may find some \( x \in F \) such that the highest term of \( x \) is like \( X_kX^n_i \) for \( i < j < k \).

**Corollary 1.13.** — Consider the situation of Theorem 1.11. Suppose \( c \geq 2 \). For some fixed \( 1 < i_0 \leq c < j_0 \leq d \), and \( n \geq 1 \), let \( x_n \in F \) of highest term \( X_{j_0}X^n_{i_0}X_1 \). Suppose moreover that \( r < (d - c)(c - 1) \). Then there exists \((i_0, j_0)\) such that the family \( \{\hat{\rho}_1, \ldots, \hat{\rho}_r, \hat{x}_n, n \geq 1\} \) is combinatorially free. In particular for such \((i_0, j_0)\):

1. the group quotient \( \Gamma := F/\langle \rho, \ldots, \rho_r, x_n, n \in \mathbb{Z}_{>0}\rangle \) of \( G \) is of cohomological dimension 2;
2. \( \dim H^2(\Gamma, \mathbb{F}_p) = \infty \);
3. The Poincaré series of \( \Lambda_{\Gamma} \) is \((1 - dt + rt^2 + t^3 \sum_{n \geq 0} t^n)^{-1}\).

**Proof.** — Thanks to Theorem 1.11, for \( i = 1, \ldots, r \), the highest term of \( \rho_i \) is of the form \( X_{i(i)}X_{s(i)} \) for some \( s(i) \leq c < t(i) \), and the family \( \mathcal{E} := \{X_{i(1)}X_{s(1)}, \ldots, X_{i(r)}X_{s(r)}\} \) is combinatorially free. Now, as \( r < (d - c)(c - 1) \) and \( c \geq 2 \), we can find \((i_0, j_0)\) such that \( X_{j_0}X_{i_0} \) is not in \( \mathcal{E} \), and then \( \mathcal{E} \cup \{X_{j_0}X^n_{i_0}X_1, n \in \mathbb{Z}_{>0}\} \) is combinatorially free. Then apply Theorem 1.6.

**Remark 1.14.** — In fact \( r \leq (d - c)2 - 1 \) is sufficient. Indeed, with such condition one has \( X_{j_0}X^n_{i_0} \notin \mathcal{E} \) for some \((i_0, j_0) \neq (1, r), i_0 \leq c < j_0 \leq r \). Hence, if \( i_0 \neq 1 \) the family \( \mathcal{E} \cup \{X_{j_0}X^n_{i_0}X_1, n \in \mathbb{Z}_{>0}\} \) is combinatorially free. Otherwise \( j_0 \neq r \), and take \( \mathcal{E} \cup \{X_rX^n_{j_0}X_{i_0}, n \in \mathbb{Z}_{>0}\} \).

### 1.2. Arithmetic backgrounds.

Let \( p \) be a prime number, and let \( K \) be a number field. For \( p = 2 \), assume \( K \) totally imaginary. Let \( S \) and \( T \) two disjoint finite sets of prime ideals of the ring of integers \( \mathcal{O}_K \) of \( K \). We assume moreover that each \( \mathfrak{p} \in S \) is such that \( \mathcal{O}_{K/\mathfrak{p}} = \mathbb{Z}_p \), the set \( S \) is called tame. We denote by \( \text{Cl}^T_\mathfrak{p}(K) \) the \( p \)-Sylow of the \( T \)-class group of \( K \).

Let \( K_{\mathfrak{p}}^T/K \) be the maximal pro-\( p \) extension of \( K \) unramified outside \( S \) and where each \( \mathfrak{p} \in T \) splits completely in \( K_{\mathfrak{p}}^T/K \); put \( G^T_{\mathfrak{p}} = \text{Gal}(K_{\mathfrak{p}}^T/K) \). As we recalled it in Introduction, when \( G^T_{\mathfrak{p}} \) is infinite, the extension \( K_{\mathfrak{p}}^T/K \) is asymptotically good. Recall Shafarevich’s formula (see for example [5, Chapter I, §, Theorem 4.6]):

\[
d_p G^T_{S} = |S| - (r_1 + r_2) - 1 - |T| + \delta_{K,p} + d_p V^T_{S}/K^x_p,
\]

where

\[
V^T_{S} = \{x \in K^x, x \in K_p^x U_p \forall x \notin S \cup T, x \in K_p^x \forall p \in S\},
\]

and where \(\delta_{K,p} = 1\) if \( K \) contains \( \mu_p \) (the \( p \)-roots of 1), 0 otherwise. Here as usual, \( K_p \) is the completion of \( K \) at \( p \), and \( U_p \) is the group of the local units at \( p \). 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 \( V^T_{S}/K^x_p \) is trivial: this is a Chebotarev condition type.

Schmidt in [15] showed that \( G^T_{S} \) may be mild following the terminology of Labute [10]. More precisely, he proved:

**Theorem 1.15 (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 \( T \) two disjoint finite sets of prime ideals of \( K \) with \( S_0 \) tame. Assume \( T \) sufficiently large such that \( \text{Cl}^T_\mathfrak{p}(p) \) is trivial; when \( \mu_p \subset K \), assume moreover that \( T \) contains all prime ideals above \( p \). Then there exist
Remark 1.18. — If infinitely finite tame sets $S$ containing $S_0$ such that $H^1(G_S^T) = U \oplus V$ where the two subspaces $U$ and $V$ satisfy: (i) $U \cup U = 0$; (ii) $U \cup V = H^2(G_S^T)$. Moreover, for such $S$ and $T$ one has $\dim H^2(G_S^T) = \dim H^1(G_S^T) + r_1 + r_2 + |T| - 1$.

Theorem 1.15 is not presented in this form in [15], here we give the form we need: the result presented here can be found in the proof of Theorem 6.1 of [15].

At this level, let us compute the value of $c = \dim V$ of Theorem 1.15, following [15]. When $\mu_p \in K$ let us choose first a finite set $S_0$ of prime ideals of $K$, tame and disjoint from $T$, such that for every $p \in S_0$, one has

$$d_p G_{S_0 \setminus \{p\}}^T = |S_0| - r_1 - r_2 - |T| + \delta_{K,p},$$

which is equivalent by Shafarevich’s formula to the triviality of $V_{S_0 \setminus \{p\}}^T/K^{xp}$.

When $\mu_p \subset K$ let us choose $S_0$, finite, tame and disjoint from $T$, such that the set of the Frobenius at $p$ in $G_T^{p-el}$ when $p$ varies in $S_0$, corresponds to the nontrivial elements of $G_T^{p-el}$, where $G_T^{p-el}$ is the Galois group of the $p$-elementary abelian extension $K_T^{p-el}/K$ of $K_T/K$. Here one has also the triviality of $V_{S_0 \setminus \{p\}}^T/K^{xp}$.

The set $S$ of Theorem 1.15 contains $S_0$, and is of size $2|S_0|$; the prime ideals $p \in S - S_0$ are chosen by respecting some global conditions, thanks to Chebotarev density theorem. Moreover $U = H^1(G_S^T, \mathbb{F}_p)$, and the subspace $V$ is such that $\dim V = c = |S_0|$. See [15, Proof of Theorem 6.1] for more details.

Now observe the following:

Lemma 1.16. — Above the previous conditions, each prime $p \in S$ is ramified in the $p$-elementary abelian extension $K_S^{T,p^{el}}/K$ of $K_S^T/K$.

Proof. — Observe first that if $S'' \subset S'$, then $V_{S'}^{T}/K^{xp} \hookrightarrow V_{S''}^{T}/K^{xp}$.

Hence thanks to the choice of $S_0$, it is not difficult to see the following: for every $p \in S$, $V_{S_0 \setminus \{p\}}^T/K^{xp}$ is trivial. Then by Shafarevich’s formula, we get that

$$d_p G_S^T = 1 + d_p G_{S_0 \setminus \{p\}}^T,$$

showing that $p$ is ramified in $K_S^{T,p^{el}}/K$.

Put $\alpha_{K,T} = 3 + 2\sqrt{2 + r_1 + r_2 + |T|}$. In Theorem 1.15 one may take $S$ sufficiently large so that $d = \dim H^1(G_S^T, \mathbb{F}_p) > \alpha_{K,T}$.

Lemma 1.17. — If $d > \alpha_{K,T}$, then $d - r_1 - r_2 + |T| - 1 < (d - c)(c - 1)$ for every $c \in [2, d]$.

Proof. — Easy computation.

Let us finish this part with an obvious observation thanks to class field theory.

Remark 1.18. — If $G_S^T$ is not trivial and of cohomological dimension at most 2, then $cd(G_S^T) = 2$. 

8
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, and then not difficult to describe: this is the description due to Koch [9, Chapter 11, §11.4, Example 11.11].

Let $\ell$ be a prime number such that $p|\ell - 1$. Denote by $\mathbb{Q}_{\ell}$ the (unique) cyclic degree $p$-extension of $\mathbb{Q}$ unramified outside $\ell$; the extension $\mathbb{Q}_{\ell}/\mathbb{Q}$ is totally ramified at $\ell$.

Let $S = \{\ell_1, \ldots, \ell_d\}$ be $d$ different prime numbers such that $p$ divides each $\ell_i - 1$. The pro-$p$ group $G_S$ can be described by $x_1, \ldots, x_d$ generators, and $\rho_1, \ldots, \rho_d$ relations verifying:

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

where $a_j(i) \in \mathbb{Z}/p\mathbb{Z}$; moreover the element $x_i$ can be chosen such that it is a generator of the inertia group of $\ell_i$. The element $a_j(i)$ is zero if and only the prime $\ell_i$ splits in $\mathbb{Q}_{\ell_j}/\mathbb{Q}$, which is equivalent to

\[
\ell_i^{(\ell_j - 1)/p} \equiv 1 \pmod{\ell_j}.
\]

• Typically take $p = 3$, and $S_0 = \{7, 13\}$, $T = \emptyset$. Then put $S = \{p_1, p_2, p_3, p_4, p_5\}$ with $p_1 = 31, p_2 = 19, p_3 = 13, p_4 = 337, p_5 = 7$. Then the highest terms of the relations (1), viewed in $\mathbb{F}_p^c[X_1, \ldots, X_5]$, are $\hat{\rho}_1 = X_1X_3$, $\hat{\rho}_2 = X_2X_4$, $\hat{\rho}_3 = X_2X_3$, $\hat{\rho}_4 = X_1X_4$, $\hat{\rho}_5 = X_1X_5$. Hence as the $\hat{\rho}_i$’s are combinatorially free, then $G_S$ is of cohomological dimension 2 by Theorem 1.6.

Now for each $n \in \mathbb{Z}_{>0}$, let us choose a prime number $p_n$ of $\mathbb{Z}$ such that the highest term in $\mathbb{F}_p^c[X_1, \ldots, X_5]$ of its Frobenius $\sigma_n \in G_S$ is like $X_5X_4^nX_1$ (which is possible by Example 1.5 or Corollary 1.13, see next section). Then consider the maximal Galois subextension $L/\mathbb{Q}$ of $Q_S/\mathbb{Q}$ fixed by all the conjugates of the $\tau_n$’s (this is the “cutting towers” strategy of [7]). Put $G = \text{Gal}(L/\mathbb{Q})$. Then the pro-$3$ group $G$ can be described by the generators $x_1, \ldots, x_5$, and the relations $\{\rho_1, \ldots, \rho_5, \tau_n, n \in \mathbb{Z}_{>0}\}$ (which is not a priori a minimal set). By construction all the $p_n$ split totally in $L/\mathbb{Q}$. Observe now that

\[
\{\hat{\rho}_1, \ldots, \hat{\rho}_5, \tau_n, n \geq 1\} = \{X_5X_1, X_5X_2, X_4X_3, X_4X_2, X_5X_3, X_5X_4^nX_1, n \in \mathbb{Z}_{>0}\},
\]

which is combinatorially free. By Theorem 1.6 the pro-$3$-group $G$ is of cohomological dimension 2, $H^2(G)$ is infinite, and $\mathbb{F}_3[[G]]$ has $\left(1 - 5t + 5t^2 + t^3(1 + t + t^2 + \cdots)\right)^{-1}$ as Poincaré series.

2.2. Proof of the main result. — • Let $p > 2$ be a prime number, and let $K$ be a number field. Let $S_0$ and $T$ two finite disjoint sets of prime ideals of $K$, where $S_0$ is tame. Take $T$ sufficiently large such that $\text{Cl}_K^T(p)$ is trivial. When $K$ contains $\mu_p$, assume moreover that $T$ contains all $p$-adic prime ideals.

First take $S$ containing $S_0$ as in Theorem 1.15, and sufficiently large such that $d > \alpha_{K,T}$. 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 1.15 and Theorem 1.11 the quotient $R/R^p[F, R]$ may be generated as $\mathbb{F}_p^c$ vector spaces by some relations $\rho_1, \ldots, \rho_c$ such that the highest terms $\hat{\rho}_k$ are like $X_iX_j$ for some $i \leq c < j$, where $c = \dim V$. Observe that as $G$ is $F$Ab then $c \in [2, d - 2]$. 

Given \( n \geq 1 \), then the quotient \( G/G_{n+1} \) is finite. Put \( K_{(n+1)} = (K_S^T)^{G_{n+1}} \). Let \( a_n \in \mathbb{Z}_{>0} \) be an increasing sequence. Let \( x_n \in F_{an} \setminus F_{an+1} \). By Chebotarev density theorem there exists some prime ideal \( p_n \subset \mathcal{O}_K \) such that \( \sigma_{p_n} \) is conjugate to \( x_n \) in \( \text{Gal}(K_{(n+1)}/K) \). Here \( \sigma_{p_n} \in G \) denotes the Frobenius of \( p_n \) in \( K_S^T/K \). Now take \( z_n \in F \) such that \( \varphi(z_n) = \sigma_{p_n} \).

Hence

\[
\text{z}_n \equiv \sigma_{p_n} \pmod{RF_{an+1}}.
\]

In other words, there exists \( y_n \in F_{an+1} \) and \( r_n \in R \) such that \( z_n = \sigma_{p_n} y_n r_n \).

Let \( \Sigma = T \cup \{ p_1, p_2, \ldots \} \), and consider \( K_S^\Sigma \) the maximal pro-\( p \) extension of \( K \) unramified outside \( S \) and where each primes \( p \) of \( \Sigma \) splits completely. Put \( G_S^\Sigma = \text{Gal}(K_S^\Sigma/K) \). Then

\[
G_S^\Sigma \cong G/\langle \sigma_{p_n}, n \in \mathbb{Z}_{>0} \rangle^{\text{Nor}}.
\]

Here \( \langle \sigma_{p_n}, n \in \mathbb{Z}_{>0} \rangle^{\text{Nor}} \) is the normal closure of \( \langle \sigma_{p_n}, n \in \mathbb{Z}_{>0} \rangle \) in \( G_S^\Sigma \). Hence \( K_S^\Sigma \) satisfies (i) and (ii) of Theorem A. But observe now that

\[
G/\langle \sigma_{p_n}, n \in \mathbb{Z}_{>0} \rangle^{\text{Nor}} \cong F/\langle \sigma_{p}, \ell \rangle^{\text{Nor}} = F/\langle \rho_1, \cdots, \rho_r, x_n y_n, n \in \mathbb{Z}_{>0} \rangle^{\text{Nor}},
\]

as \( \sigma_{p_n} \) and \( x_n \) are conjugate.

Since the highest term of each \( x_n y_n \) in \( E = \mathbb{F}_p[[X_1, \ldots, X_d]] \) is the same as the highest term of \( x_n \), it suffices to choose the \( x_n \)'s as in Corollary 1.13 which is possible: indeed as \( d > \alpha_{K,T} \) then by Lemma 1.17 \( r < (c - 1)(d - c) \), for every \( c \in [1, d - 1] \). Thanks to Corollary 1.13, one gets (iii), (iv), and (vi) of Theorem A.

(v): by Lemma 1.16 each prime ideal \( p \in S \) is ramified in \( K_S^{T, p - q}/K \), showing that \( \tau_p \in G \) is not in \( RF_p[F, F] \), where \( \tau_p \) is a generator of the inertia group at \( p \) in \( G \). As the \( p \)-rank of \( G_S^\Sigma \) is the same as the \( p \)-rank of \( G \), each prime \( p \in S \) is ramified in \( K_S^\Sigma \). But as \( G \) is without torsion (because \( cd(G) = 2 \)), necessarily \( \langle \tau_p \rangle \cong \mathbb{Z}_p \), and the structure of local extensions forces \( (K_S^\Sigma)_p/K_p \) to be maximal.

- Assume \( p = 2 \), and \( K \) be totally imaginary. Then Theorem 1.15 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 elements \( x_n \) by some Frobenius as in Corollary 1.13 also applies. Then by following the proof of Theorem 6.4 in [4], and by choosing the \( x_n \)'s as in the case \( p = 2 \), we observe that the initial forms of the new relations \( \{ \rho_1, \cdots, \rho_r, x_n, n \geq 1 \} \) are still strongly free. We conclude by using Remark 1.9 of Theorem 1.6.

\[\square\]

References

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

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

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

[4] P. Forré, Strongly free sequences and pro-\( p \)-groups of cohomological dimension 2, J. reine u. angew. Math \textbf{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 Q, J. reine u. angew. Math. 596 (2006), 155–182.

[11] J. Labute, J. Mináč, Mild pro-2-groups and 2-extensions of 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, Springer-Verlag Berlin Heidelberg, 2000.

[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.

February 24, 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, FEMTO-ST Institute, Université Bourgogne Franche-Comté, 15B Avenue des Montboucons, 25030 Besançon Cedex, France  •  E-mail : christian.maire@univ-fcomte.fr