Kyushu J. Math. **68** (2014), 359–376
doi:10.2206/kyushujm.68.359

SOME EXAMPLES OF FAB AND MILD PRO-p-GROUPS WITH TRIVIAL CUP-PRODUCT

Christian MAIRE

(Received 26 September 2013)

Abstract. Let G_S be the Galois group of the maximal pro-p-extension $\mathbb{Q}_S$ of $\mathbb{Q}$ unramified outside a finite set S of places of $\mathbb{Q}$ not containing the prime $p > 2$. In this work, we develop a method to produce some examples of mild (and thus FAB) pro-p-groups G_S for which some relations are of degree three (according to the Zassenhaus filtration). The key computation are done in some Heisenberg extensions of $\mathbb{Q}$ of degree p^3. With the help of GP-Pari we produce some examples for $p = 3$.

0. Introduction

Let $p > 2$ be an odd prime number. Let $S = \{\ell_1, \ldots, \ell_d\}$ be a finite set of prime numbers ℓ_i, with $\ell_i \equiv 1(\mathrm{mod\ p})$. Consider $\mathbb{Q}_S$ the maximal pro-p-extension of $\mathbb{Q}$ unramified outside S and put $\mathrm{G}_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

In the 1960s, Koch (see [**8**]) gave a description of the pro-p-group G_S by generators and relations. Thanks to this description, in 2006 Labute in [**9**] gave the first examples of pro-p-groups G_S with cohomological dimension two. By class field theory these groups have the FAB property: every open subgroup U of G_S has a finite abelianization. And then the strict cohomological dimension of these pro-p-groups G_S is three (see for example [**12**, Ch. III]). To produce such examples, Labute used a criteria for a pro-p-group to be *mild* (this one is related to a criterion of Anick [**1**]): in some favorable situations the initial terms of the relations satisfy some very special combinatorial properties such that the graded algebra built on the lower p-central series of G_S has a very nice description in terms of the corresponding free graded algebra. In the examples of Labute, the relations are of degree two according to the Zassenhaus filtration.

Very recently, the arithmetic aspect of the work of Labute has been improved by a series of papers of Schmidt [**14, 15**].

In [**16, 17**], when $p = 2$, Vogel has given a way to produce mild pro-2-groups G_S where the relations are of degree three. This method uses the Rédei symbol [**13**]. With this, Gärtner [**7**] has produced an arithmetic example of mild pro-2-group G where the relations are of degree three and such that, assuming that the Leopoldt conjecture holds, this group is FAB. The pro-2-group produced by Gärtner corresponds to the maximal pro-2-extension of $\mathbb{Q}$ unramified outside $S = \{2, 17, 7489, 15\,809\}$ in which the place 5 splits completely.

2010 Mathematics Subject Classification: Primary 11R21, 11Y40, 11R34, 20F05, 20F14, 20F40.
Keywords: mild pro-p-groups; restricted ramification; class field theory.

As the prime 2 is in S, it is necessary to force a place to split completely so as to rule out the $\mathbb{Z}_2$-cyclotomic extension.

In [**5**] Forré has developed the approach of mild pro-p-group by looking at the Zassenhaus filtration in the non-commutative ring of formal power series $\mathbb{F}_p[[X_1, \ldots, X_d]]^{nc}$ with coefficients in $\mathbb{F}_p$. It is this approach that we will use here.

By considering the arithmetic in some Heisenberg extension of degree 3^3 over $\mathbb{Q}$ we produce some mild pro-p-groups G_S for which some relations are of degree three. Moreover, these pro-3-groups are FAB (unconditionally). Here we do not have the Rédei symbols, but it will be interesting to explore the equality of Proposition 2.23 in this way.

In the next section, we recall the basic facts about mild pro-p-groups (according to the Zassenhaus filtration). In Section 2, we develop the arithmetic strategy and present the principle of the computation based on class field theory. In the last section we produce the two following examples.

Example 0.1. The pro-3-group $\mathrm{G}_S = \mathrm{G}_{\{19,9811,11\,863\}}$ can be described by the generators x_1, x_2 and x_3 and by the relations

$$\rho_1 \equiv [[x_1, x_2], x_1][[x_1, x_3], x_1][[x_2, x_3], x_1] \pmod{\mathrm{F}_{(4)}},$$

$$\rho_2 \equiv [[x_1, x_2], x_2]^{-1} \pmod{\mathrm{F}_{(4)}},$$

$$\rho_3 \equiv [[x_1, x_3], x_2]^{-1}[[x_1, x_3], x_3][[x_2, x_3], x_1] \pmod{\mathrm{F}_{(4)}}.$$

This pro-3-group G_S is mild and FAB. In particular:

(i) the pro-3-group G_S is of cohomological dimension two;

(ii) the Zassenhaus filtration of G_S has $1/(1 - 3t + 3t^3)$ as Poincaré series.

Example 0.2. Let $S = \{7, 13, 381, 11\,971\}$. The pro-3-group G_S is mild and FAB with two relations of degree two and two relations of degree three with $1/(1 - 4t + 2t^2 + 2t^3)$ as Poincaré series.

All of the computations have been done with GP-Pari [**2**].

Notation. For x, y in a group G, we denote by $[x, y] = x^{-1}y^{-1}xy$ the commutator of x and y.

1. Relations and mild pro-p-groups

For this section, we refer to [**4**], [**5**] and [**8**].

1.1. The Zassenhaus filtration

Let $\mathbb{F}_p^{nc}(d) := \mathbb{F}_p[[X_1, \ldots, X_d]]^{nc}$ be the non-commutative ring of formal power series in variables $X_1, \ldots, X_d$ over the finite field $\mathbb{F}_p$. Denote by $\mathscr{I}$ the two sided-ideal generated by the X_i: it is the augmentation ideal of $\mathbb{F}_p^{nc}(d)$, i.e. the kernel of the natural morphism $\mathbb{F}_p^{nc}(d) \twoheadrightarrow \mathbb{F}_p$:

$$\mathscr{I} = \ker(\mathbb{F}_p^{nc}(d) \longrightarrow \mathbb{F}_p).$$

The ring $\mathbb{F}_p^{nc}(d)$ is a topological local ring where the family $(\mathscr{I}^n)_n$ is a neighborhood basis of 0.

Now consider the free prop-p-group F of rank d generated by the elements $x_1, \ldots, x_d$. Denote by $\Lambda(\mathrm{F})$ the complete algebra

$$\Lambda(\mathrm{F}) := \varprojlim_{\mathrm{U} \subset \mathrm{F}} \mathbb{F}_p[\mathrm{F}/\mathrm{U}],$$

where U runs through open normal subgroups of F. Let

$$\mathrm{I}(\mathrm{F}) = \ker(\Lambda(\mathrm{F}) \to \mathbb{F}_p),$$

be the augmentation ideal of $\Lambda(\mathrm{F})$. Then it is well-known that the map (the Magnus expansion)

$$\varphi : \Lambda \to \mathbb{F}_p^{nc}(d)$$
$$x_i \mapsto 1 + X_i$$

is an isomorphism of topological rings. Remark that $\varphi(\mathrm{I}(\mathrm{F})) = \mathscr{I}$. Now consider the map ι from F to $\mathbb{F}_p^{nc}(d)$ defined by

$$\iota(x) = \varphi(x - 1),$$

and put $\mathrm{F}_{(n)} = \{x \in \mathrm{F},\ \iota(x) \in \mathscr{I}^n\}$. The sequence $(\mathrm{F}_{(n)})_n$ is a neighborhood basis of 1: it is the Zassenhaus filtration of F.

We recall some basic facts (see [**4, 16**]).

PROPOSITION 1.1. *We have the following.*

(i) *The elements* $[x_i, x_j]$, $i < j$, *form a* $\mathbb{F}_p$*-basis of* $\mathrm{F}_{(2)}/\mathrm{F}_{(3)}$.

(ii) *For* $p = 3$, *the elements*

$$x_i^3, \quad i = 1, \ldots, d$$
$$[[x_i, x_j], x_k], \quad i < j,\ k \leq j$$

form a $\mathbb{F}_p$*-basis of* $\mathrm{F}_{(3)}/\mathrm{F}_{(4)}$. *For* $p > 3$, *one has to omit the p-powers* x_i^p.

Example 1.2. Suppose that $p > 2$. When F is the free pro-p-group on two generators, then $\mathrm{F}/\mathrm{F}_{(3)}$ is a non-abelian group of order p^3 and of exponent p (because $\mathrm{F}^p \subset \mathrm{F}_{(3)}$): this quotient is isomorphic to the Heisenberg group

$$H_{p^3} = \langle x, y, x^p = 1, y^p = 1, [[x, y], x] = [[x, y], y] = 1 \rangle.$$

1.2. Strongly free sequence

Definition 1.3. Let $\mathcal{S} = \{P_1, \ldots, P_r\}$ be some series in $\mathscr{I} \subset \mathbb{F}_p^{nc}(d)$ and let $\mathscr{S}$ be the two-sided ideal generated by the elements $P_1, \ldots, P_r$. Then the family $\mathcal{S}$ is called strongly free if the quotient $\mathscr{S}/\mathscr{S}\mathscr{I}$ is a $\mathbb{F}_p^{nc}(d)/\mathscr{S}$-left-free module on the images of $P_1, \ldots, P_r$.

For $P \in \mathbb{F}_p^{nc}(d)$, $P \neq 0$, denote by P_i its term of degree i. If i_0 is the smallest integer such that $P_{i_0} \neq 0$, then P_{i_0} is called the initial form of P and is denoted by $\omega(P)$. The integer i_0 is the degree of P and is denoted by $i_0 := \deg(P)$. We put $\deg(0) = \infty$.

Definition 1.4. If $x \in \mathrm{F}$, the degree of x is the degree of $\iota(x)$ and is denoted by $\deg(x)$. For a subgroup H of F, the degree of H, denoted by $\deg(H)$, is the minimum of the degree of x, for all $x \in H$.

Definition 1.5. (Anick [**1**]) A family $M_1, \ldots, M_r$ of monomials in $\mathscr{I} \subset \mathbb{F}_p^{nc}(d)$, $M_i \neq 1$, is said to be combinatorially free if:

(1) no M_i is a submonomial of any M_j, $j \neq i$;

(2) for every i, j, the beginning of M_i is not the same as the ending of M_j.

Now let us fix a total order $<$ on the set $\{X_1, \ldots, X_d\}$ and then consider the lexicographic ordering on $\mathbb{F}_p^{nc}(d)$ deduced from $<$. If P is a sum of homogeneous monomials, we denote by $\mathscr{L}(P)$ the leading term of P.

Definition 1.6. A family $P_1, \ldots, P_r$ of series in $\mathscr{I} \subset \mathbb{F}_p^{nc}(d)$ is called combinatorially free (after ordering) if the family of monomials

$$\mathscr{L}(\omega(P_1)), \ldots, \mathscr{L}(\omega(P_r))$$

is combinatorially free.

THEOREM 1.7. (Forré [**5**]) *If the family $\mathcal{S} = \{P_1, \ldots, P_r\} \subset \mathbb{F}_p^{nc}(d)$ is combinatorially free then $\mathcal{S}$ is strongly free.*

1.3. Mild pro-p-groups

Let

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \longrightarrow \mathrm{G} \longrightarrow 1$$

be a minimal presentation of a finitely presented pro-p-group G. The p-rank of G is finite and equal to the p-rank of the free pro-p-group F and these two groups are topogically generated by d generators $x_1, \ldots, x_d$.

Let $\rho_1, \ldots, \rho_r \in \mathrm{R} \subset \mathrm{F}$ be a basis over $\mathbb{F}_p$ of $\mathrm{R}/\mathrm{R}^p[\mathrm{F}, \mathrm{R}] \simeq H_2(\mathrm{G}, \mathbb{F}_p)$ (the elements ρ_i are a basis of the relations of G).

The notion of a strongly free sequence will give us a sufficient condition for a pro-p-group to be of cohomological dimension two. The key criterion is the following.

THEOREM 1.8. (Brumer [**3**]) *The pro-p-group* G *is of cohomological dimension at most two if and only if the* $\mathbb{F}_p[[\mathrm{G}]]$*-module* $\mathrm{R}/\mathrm{R}^p[\mathrm{R}, \mathrm{R}]$ *is free.*

Now, with the previous theorem, it is possible to give criteria in the algebra $\mathbb{F}_p^{nc}(d)$ for a pro-p-group G to be of cohomological dimension at most two.

THEOREM 1.9. (Forré [**5**]) *The pro-p-group* G *is of cohomological dimension at most two if and only if $\mathscr{R}/\mathscr{R}\mathscr{I}$ is a free left $\mathbb{F}_p^{nc}(d)/\mathscr{R}$-module, where $\mathscr{R} = \iota(\mathrm{R})$.*

We can then define the notion of mild pro-p-group.

Definition 1.10. If a pro-p-group G has a presentation with relations $\rho_1, \ldots, \rho_r$, then G is called mild (following the Zassenhaus filtration) if the family $\iota(\rho_1), \ldots, \iota(\rho_r)$ is combinatorially free.

Thanks to the previous results, one obtains the following result.

THEOREM 1.11. *If* G *is mild then the cohomological dimension of* G *is at most two.*

Remark 1.12. (The Poincaré series) See **[5, 9]**. For $n \geq 1$, denote by $\mathrm{G}_{(n)}$ the quotient $\mathrm{F}_{(n)}\mathrm{R}/\mathrm{R}$ and put $a_n = \dim_{\mathbb{F}_p} \mathrm{G}_{(n)}/\mathrm{G}_{(n+1)}$. Then the Poincaré series $P(t)$ of G (associated with Zassenhauss filtration) is the formal series

$$P(t) = 1 + \sum_{n \geq 1} a_n t^n.$$

When the relations $\rho_1, \ldots, \rho_r$ of G are combinatorially free then the Poincaré series of G satisfies:

$$P(t) = \frac{1}{1 - dt + \sum_{i=1}^{r} t^{\deg(\rho_i)}}.$$

1.4. The relations in $\mathbb{F}_p^{nc}(d)$

Definition 1.13. Let $I = (i_1, \ldots, i_n)$ be a multi-index with $i_j \in \{1, \ldots, d\}$. One denotes by $n = \deg(I)$ the degree of I.

For $Z \in \mathbb{F}_p^{nc}(d)$, we denote by $\varepsilon_I(Z)$ to be the $X_{i_1} \cdots X_{i_n}$-coefficient of Z.

For $y \in \mathrm{F}$, let us denote, by abuse of notation, $\varepsilon_I(y)$ to be $\varepsilon_I(\iota(y))$.

PROPOSITION 1.14. *Let $x, y \in \mathrm{F}$. Write $\varphi(x) = 1 + X$ and $\varphi(y) = 1 + Y$, with $X, Y \in \mathbb{F}_p^{nc}(d)$. Then:*

(i) *if* $\deg(x) > \deg(I)$, *then* $\varepsilon_I(x) = 0$;

(ii) $\varepsilon_I(xy) = \sum_{JK=I} \varepsilon_J(x)\varepsilon_K(y)$, *where the sum is taken over all subsets J, K of I such that the concatenation JK of J and K is equal to I;*

(iii) *if* $\min(\deg(x), \deg(y)) > \deg(I)$, *then* $\varepsilon_I(xy) = 0$;

(iv) *if* $\max(\deg(x), \deg(y)) \geq \deg(I)$, *then* $\varepsilon_I(xy) = \varepsilon_I(x) + \varepsilon_I(y)$;

(v) $\varphi(x^{-1}) = 1 - X + X^2 - X^3 + \cdots$;

(vi) $\varphi([x, y]) = 1 + XY - YX +$ degree > 2;

(vii) *if* $\deg(y) \geq 2$, *then* $\varphi([x, y]) = 1 + XY - YX +$ degree > 3;

(viii) $\varphi([[x, y], z]) = 1 + XYZ - YXZ + -ZXY + ZYX +$ degree > 3.

Proof. Easy computation. □

Now, we are interested in the image in $\mathbb{F}_p^{nc}(d)$ of the relations of G. If $\rho_m \in \mathrm{F}$ is a such relation, then let us write (by Proposition 1.1)

$$\rho_m \equiv \prod_{i<j} [x_i, x_j]^{e_{i,j}(m)} \pmod{\mathrm{F}_{(3)}}, \tag{1}$$

and if moreover $\rho_m \in \mathrm{F}_{(3)}$:

$$\rho_m \equiv \prod_{j} x_j^{pa_j(m)} \prod_{i<j,k\leq j} [[x_i, x_j], x_k]^{e_{i,j,k}(m)} \pmod{\mathrm{F}_{(4)}}, \tag{2}$$

with $a_j, e_{i,j,k}(m) \in \mathbb{F}_p$.

PROPOSITION 1.15. *For $i < j < k$, we have*

$$e_{i,j}(m) = \varepsilon_{i,j}(\rho_m), \quad e_{i,j,i}(m) = -\varepsilon_{i,i,j}(\rho_m), \quad e_{i,j,j}(m) = \varepsilon_{i,j,j}(\rho_m),$$

$$a_j(m) = \varepsilon_{i,i,i}(\rho_m), \quad e_{i,j,k}(m) = -\varepsilon_{j,i,k}(\rho_m).$$

Remark 1.16. For $p > 3$, $a_j(m) = 0$.

Proof. By Proposition 1.14, we have

$$\iota([[x_i, x_j], x_j]) = X_i X_j X_j - X_j X_i X_j - X_j X_i X_j + X_j X_j X_i + \text{degree} > 3,$$

$$\iota([[x_i, x_j], x_i]) = X_i X_j X_i - X_j X_i X_i - X_i X_i X_j + X_i X_j X_i + \text{degree} > 3,$$

and for $i < k < j$:

$$\iota([[x_i, x_k], x_j]) = X_i X_k X_j - X_k X_i X_j - X_j X_i X_k + X_j X_k X_i + \text{degree} > 3,$$

$$\iota([[x_j, x_k], x_i]) = X_j X_k X_i - X_k X_j X_i - X_i X_j X_k + X_i X_k X_j + \text{degree} > 3.$$

Hence,

$$e_{i,j,j}(\rho_m) = \varepsilon_{i,j,j}(\rho_m) = \varepsilon_{j,j,i}(\rho_m) = -\tfrac{1}{2}\varepsilon_{j,i,j}(\rho_m),$$

$$e_{i,j,i}(m) = \tfrac{1}{2}\varepsilon_{i,j,i}(\rho_m) = -\varepsilon_{i,i,j}(\rho_m) = -\varepsilon_{j,i,i}(\rho_m),$$

$$e_{i,k,j}(m) = -\varepsilon_{k,i,j}(\rho_m) = -\varepsilon_{j,i,k}(\rho_m), \;\; e_{j,k,i}(m) = -\varepsilon_{k,j,i}(\rho_m) = -\varepsilon_{i,j,k}(\rho_m)$$

and

$$e_{i,k,j}(m) + e_{j,k,i}(m) = \varepsilon_{i,k,j}(\rho_m) = \varepsilon_{j,k,i}(\rho_m).$$

□

2. The principle of the computation

2.1. *The arithmetic context*

Let $p \geq 3$ be a prime number and let $S = \{\ell_1, \ldots, \ell_d\}$ be a set of primes such that $\ell_i \equiv 1 \pmod{p}$.

Let $\mathrm{G}_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, where $\mathbb{Q}_S$ is the maximal pro-p-extension of $\mathbb{Q}$ unramified outside S.

For $i = 1, \ldots, d$, denote by x_i a generator of the inertia group in G_S of a place $\mathfrak{l}_i | \ell_i$ along $\mathbb{Q}_S/\mathbb{Q}$ such that its restriction to the maximal abelian subextension $\mathbb{Q}_S^{ab}/\mathbb{Q}$ of $\mathbb{Q}_S$ corresponds, via class field theory, to the idèle where all components are 1 except the ℓ_i-component which is a primitive root of 1 modulo ℓ_i.

Then the pro-p-group G_S is topologically generated by the elements x_i, $i = 1, \ldots, d$.

Let

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \longrightarrow \mathrm{G}_S \longrightarrow 1,$$

be a minimal presentation of G_S on the elements x_i. For $i = 1, \ldots, d$, we identify x_i with one of its preimages in F. The free pro-p-group F is generated by the elements $x_1, \ldots, x_d$.

We also need some particular lifts of Frobenius elements. For $i = 1, \ldots, d$, let us fix a prime $\mathfrak{l}_i | \ell_i$ along $\mathbb{Q}_S/\mathbb{Q}$. Consider y_i a lift in G_S of the Frobenius of the place $\mathfrak{l}_i$ such that the restriction of y_i to $\mathbb{Q}_S^{ab}/\mathbb{Q}$ corresponds, via class field theory, to the idèle where all components are 1 except the ℓ_i-component which is ℓ_i.

As before, we identify y_i with one of its preimages in F.

Remark 2.1. By the choice of y_i, one has the following fact: if $\mathrm{L}/\mathbb{Q}$ is a p-elementary subextension of $\mathbb{Q}_S^{ab}/\mathbb{Q}$ in which the inertia degree of ℓ_i is trivial, then $y_{i|\mathrm{L}} = 1$.

Definition 2.2. Denote by $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$ the maximal elementary p-extension over $\mathbb{Q}$ unramified outside ℓ_i. This extension is of degree p in which ℓ_i is totally ramified.

Remark 2.3. As the maximal pro-p-extension of $\mathbb{Q}$ unramified outside ℓ_i is cyclic and totally ramified, then the p-class group of $\mathbb{Q}_{\ell_i}^{p,el}$ is trivial.

Remark 2.4. Let q be a prime such that:
(i) $q^{(\ell_i-1)/p} \in \mathbb{F}_{\ell_i}$ is of order p (or, equivalently, q is inert in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$);
(ii) for $j \neq i$, $q^{(\ell_j-1)/p} = 1$ in $\mathbb{F}_{\ell_j}$ (or, equivalently, q splits in $\mathbb{Q}_{\ell_j}^{p,el}/\mathbb{Q}$).
Then, we can choose x_i such that its restriction to the maximal p-elementary subextension $\mathbb{Q}_S^{p,el}/\mathbb{Q}$ of $\mathbb{Q}_S/\mathbb{Q}$ is equal to the restriction of the Frobenius $\mathfrak{f}_q$ of q. Indeed, the principal idèle q has only two non-trivial component via the Artin map in $\mathrm{Gal}(\mathbb{Q}_S^{p,el}/\mathbb{Q})$: the ℓ_i-component and the q-component.

2.2. *A first principle*

Let $I = (i_1, \ldots, i_n)$ be a multi-index, $i_j \in \{1, \ldots, d\}$. We want to estimate $\varepsilon_I(z)$ for some $z \in \mathrm{F}$. The strategy is the following: to look at the restriction of z to some quotients of G_S, i.e. in some p-extensions of $\mathbb{Q}$ unramified outside S.

Let Γ be a quotient of G_S. We can assume that Γ is generated by the images of the x_i, $i = 1, \ldots, d'$, with $d' \leq d$.

Denote by F' the free pro-p-groups on d'-generators $x_1, \ldots, x_{d'}$ and let $\alpha : \mathrm{F} \to \mathrm{F}'$ be the natural morphism sending $x_1, \ldots, x_{d'}$ to the generators of F' and such that $\alpha(x_i) = 1$ for $i > d'$.

By the universal property of F', there exists a section γ from F' to F such that $\alpha(\gamma(\alpha(x))) = \alpha(x)$, for all $x \in \mathrm{F}$. One then has the following natural commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{R} \arrow[r] \arrow[d] & \mathrm{F} \arrow[r] \arrow[d, "\alpha"] & \mathrm{G}_S \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{R}' \arrow[r] & \mathrm{F}' \arrow[r, "\beta"] \arrow[u, bend left, dotted, "\gamma"] & \Gamma \arrow[r] & 1
\end{tikzcd}$$

Here $\ker(\alpha)$ is the smallest normal subgroup of F generated by the elements $x_{d'+1}, \ldots, x_d$ and $\ker(\beta \circ \alpha) = \langle \gamma(\ker(\beta)), \ker(\alpha) \rangle$.

LEMMA 2.5. *If* $I \subset \{d' + 1, \ldots, d\}$ *and if* $\deg(I) < \deg(\ker(\beta))$*, then* $\varepsilon_I(z)$ *does not depend on the lift of* $\beta(\alpha(z))$ *in* F.

Proof. The section γ induces the injection

$$\mathbb{F}_p[[X_1, \ldots, X_{d'}]]^{nc} \hookrightarrow \mathbb{F}_p^{nc}(d)$$

and the degree of $\iota(\gamma(\ker(\beta))) \subset \mathbb{F}_p[[X_1, \ldots, X_{d'}]]^{nc}$ is the same as the degree of $\ker(\beta)$. Now, the kernel of α is the smallest normal subgroup containing $x_{d'+1}, \ldots, x_d$. Hence, $\iota(\ker(\alpha)) = (X_{d'+1}, \ldots, X_d)$, i.e. the two-sided ideal of $\mathbb{F}_p^{nc}(d)$ generated by the elements $X_{d'+1}, \ldots, X_d$.

In conclusion, for all $J \subset I$, $\varepsilon_J(\ker(\beta \circ \alpha)) = 0$. Hence for $z, z' \in \mathrm{F}$, such that $\beta(\alpha(z)) = \beta(\alpha(z'))$, one finally has $\varepsilon_I(z) = \varepsilon_I(z')$. □

Let us give two key examples useful for what will follow.

Example 2.6. Consider $\mathbb{Q}_{\ell_1}^{p,el}/\mathbb{Q}$ the maximal p-elementary extension of $\mathbb{Q}$ unramified outside ℓ_1. Put $\Gamma = \mathrm{Gal}(\mathbb{Q}_{\ell_1}^{p,el}/\mathbb{Q})$ and let F' be the free pro-p-group on x_1. Then, $\ker(\beta) = \langle x_1^p \rangle$.

Now, let $z \in \mathrm{F}$ such that $\beta(\alpha(z)) = x_1^a \in \Gamma$. Then $\varepsilon_1(z) = a$ and $\varepsilon_{1,1}(z) = a(a-1)/2$. In particular, $\varepsilon_{1,1}(z) = 0$ if $\beta(\alpha(z)) = 1$.

In this example, the computation of $\varepsilon_I(z)$ is reduced to look at the restriction of z to $\mathbb{Q}_{\ell_1}^{p,el}/\mathbb{Q}$.

Example 2.7. Let $T = \{\ell_1, \ell_2\}$ and let F' be the free-p-group generated by x_1 and x_2. Suppose that the relations of G_T are of degree three. Then, $\mathrm{G}_T/(\mathrm{G}_T)_{(3)} \simeq \mathrm{F}'/\mathrm{F}'_{(3)} \simeq H_{p^3}$, where H_{p^3} is the Heisenberg group. Then $\ker(\beta)$ is the smallest normal subgroup of F' generated by x_1^p, x_2^p, $[[x_1, x_2], x_1]$ and $[[x_1, x_2], x_2]$. Hence, $\ker(\beta) \subset \mathrm{F}'_{(3)}$. Hence, for $z \in \mathrm{F}$ such that $\beta(\alpha(z)) = [x_1, x_2]^a \in \Gamma$, one obtains $\varepsilon_{1,2}(z) = a$.

In this example, the computation of $\varepsilon_{1,2}(z)$ is reduced to look at the restriction of z to a Heisenberg extension of $\mathbb{Q}$.

For what will follow, we introduce the following notation.

Definition 2.8. Let $I = (i_1, \ldots, i_n)$. Put

$$\mu(I) = \varepsilon_{i_1,\ldots,i_{n-1}}(y_{i_n}),$$

where we identify y_{i_n} with one of its preimages in F.

The quantity $\mu(I)$ was first introduced as an arithmetic analogue of Milnor invariants of links by Morishita in [**10, 11**]. See also [**16**].

2.3. *The Koch computation*

One has the following description of G_S.

THEOREM 2.9. (Koch [**8**]) *The group* G_S *can be described by generators* $x_1, \ldots, x_d$ *and by the relations* $\rho_1, \ldots, \rho_r$ *where for* $m = 1, \ldots, d$:

$$\rho_m = x_m^{\ell_m - 1}[x_m^{-1}, y_m^{-1}].$$

This description comes from the fact that the relations are all local: they are coming from the maximal pro-p-extension of the local fields $\mathbb{Q}_{\ell_i}$. Let us be a little more precise.

PROPOSITION 2.10. *In the previous arithmetic situation:*

$$H^1(\mathrm{G}_S, \mathbb{F}_p) \simeq \bigoplus_{i=1}^{d} H^1(\Gamma_{\ell_i}, \mathbb{F}_p)$$

where $\Gamma_{\ell_i} = \mathrm{Gal}(\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q})$ *and the natural map*

$$H^2(\mathrm{G}_S, \mathbb{F}_p) \to \bigoplus_{i=1}^{d} H^2(\mathrm{G}_{\ell_i}, \mathbb{F}_p)$$

is an isomorphism, where $\mathrm{G}_{l_i} = \mathrm{Gal}(\overline{\mathbb{Q}_{\ell_i}}/\mathbb{Q}_{l_i})$ *and where* $\overline{\mathbb{Q}_{\ell_i}}$ *is the maximal pro-p-extension of the complete field* $\mathbb{Q}_{\ell_i}$.

For $i = 1, \dots, d$, let χ_i be a character such that $H^1(\Gamma_{\ell_i}, \mathbb{F}_p) = \langle \chi_i \rangle$.

Look at the cup product $\chi_i \cup \chi_j \in H^2(\mathrm{G}_S, \mathbb{F}_p)$. Then $\chi_i \cup \chi_i = 0$ and for k different from i and j, $\chi_i \cup \chi_j$ is zero in the ℓ_k-component $H^2(\mathrm{G}_{\ell_k}, \mathbb{F}_p)$ because χ_i and χ_j are unramified at ℓ_k.

LEMMA 2.11. *We have $\chi_i \cup \chi_j = 0$ in $H^2(\mathrm{G}_{\ell_i}, \mathbb{F}_p)$ if and only if ℓ_j splits in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$.*

Proof. This follows from a local computation. □

Hence, one obtains the following result.

COROLLARY 2.12. *The cup-product $H^1(\mathrm{G}_S, \mathbb{F}_p) \cup H^1(\mathrm{G}_S, \mathbb{F}_p)$ is zero if and only if for all i, j, the prime number ℓ_j splits in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$.*

Now, by using the principle of Section 2.2.

LEMMA 2.13. *One has $y_i \equiv x_j^{\mu(j,i)}$ in $\mathrm{Gal}(\mathbb{Q}_{\ell_j}^{p,el}/\mathbb{Q})$.*

Proof. This is an application of Example 2.6. □

With the notation of Section 1.4, one has the following result.

PROPOSITION 2.14. *Let $i < j$. One has $e_{i,j}(i) = \mu(j, i)$ and $e_{i,j}(j) = -\mu(i, j)$. In the other case, $e_{i,j}(k) = 0$.*

Proof. Let $I = (i, j)$. Then as $x_m^{\ell_m - 1}$ is at least of degree two:

$$\begin{aligned}\varepsilon_I(\rho_m) &= \varepsilon_I(x_m^{\ell_m-1}[x_m^{-1}, y_m^{-1}]) \\ &= \varepsilon_I(x_m^{-1}, y_m^{-1}]) \\ &= \varepsilon_I(X_m Y_m) - \varepsilon_I(Y_m X_m),\end{aligned}$$

where $Y_m = \varphi(y_m)$. The conclusion is then obvious. □

Finally, one obtains the two following lemmas.

COROLLARY 2.15. (Fröhlich [**6**]) *For $m = 1, \dots, r$, one has*

$$\rho_m = \prod_{i \neq m} [x_m, x_i]^{\mu(i,m)} \pmod{\mathrm{F}_{(3)}}.$$

COROLLARY 2.16. *The following are equivalent:*

(i) *the relation ρ_m is in $\mathrm{F}_{(3)}$;*

(ii) *for all i, ℓ_m splits in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$;*

(iii) *for all i, $\chi_m \cup \chi_i = 0$ in $H^2(\mathrm{G}_{\ell_i}, \mathbb{F}_p)$;*

(iv) *$\chi_m \cup H^1(\mathrm{G}_S, \mathbb{F}_p) \subset H^2(\mathrm{G}_S, \mathbb{F}_p)$ is zero.*

2.4. A key formula

For what will follow, we use the description of G_S by Koch: $\rho_m = x_m^{\ell_m-1}[x_m^{-1}, y_m^{-1}]$.

PROPOSITION 2.17. (Vogel [**16**, Theorem 2.1.7]) *Let $I = (i_1, i_2, i_3)$. Suppose that ℓ_m splits in $\mathbb{Q}_{\ell_{i_1}}^{p,el}/\mathbb{Q}$, $\mathbb{Q}_{\ell_{i_2}}^{p,el}/\mathbb{Q}$, and $\mathbb{Q}_{\ell_{i_3}}^{p,el}/\mathbb{Q}$. Then one has*

$$\varepsilon_I(\rho_m) = \alpha(p, I)\frac{(\ell_m - 1)}{p} + \delta_{i_1,m}\mu(i_2, i_3, m) - \delta_{i_3,m}\mu(i_1, i_2, m),$$

where $\alpha(p, I) = 0$ if $p > 3$ or if $I \neq (m, m, m)$, and is 1 otherwise.

Proof. Let $Y_m = \iota(y_m)$. The degree of $x_m^{\ell_m - 1}$ is at least three and by Example 2.6, the coefficients of Y_m in which appear at least one of the X_{i_1}, X_{i_2} and X_{i_3} are at least of degree two. Then (by using Proposition 1.14):

$$\begin{aligned}\varepsilon_I(\rho_m) &= \varepsilon_I(x_m^{\ell_m-1}[x_m^{-1}, y_m^{-1}])\\ &= \varepsilon_I(x_m^{\ell_m-1}) + \varepsilon_I[x_m^{-1}, y_m^{-1}]\\ &= \frac{(\ell_m - 1)}{p}\varepsilon_I(x_m^p) + \varepsilon_I(X_mY_m) - \varepsilon_I(Y_mX_m)\\ &= \frac{(\ell_m - 1)}{p}\varepsilon_I(x_m^p) + \delta_{i_1,m}\mu(i_2, i_3, m) - \delta_{i_3,m}\mu(i_1, i_2, m).\end{aligned}$$ □

Remark here that as an application of Example 2.6, we have the following result.

PROPOSITION 2.18. *One has $\mu(i, i, i) = 0$ and if ℓ_j splits in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$, then $\mu(i, i, j) = 0$.*

2.5. *Computation in some Heisenberg extensions*

Let $i \neq j$ be indices such that $\mu(i, j) = \mu(j, i) = 0$.

We want to compute the quantities $\mu(i, j, k)$ when k satisfies $\mu(i, k) = \mu(j, k) = 0$. To do this we use the principle of Example 2.7.

Put $T = \{\ell_i, \ell_j\} \subset S$. By Corollary 2.16, the conditions for the places of T imply that the relations of G_T are in $\mathrm{F}'_{(3)}$, where

$$1 \longrightarrow \mathrm{R}' \longrightarrow \mathrm{F}' \longrightarrow \mathrm{G}_T \longrightarrow 1$$

is a minimal presentation of G_T. Here F' is the free-pro-p-group generated by x_i and x_j: as usual, as $G_S \twoheadrightarrow G_T$, we identify the elements x_i and x_j in G_T with its preimages in G_S, F' and F. By hypothesis, $\mathrm{F}'_{(3)} \subset \mathrm{R}'$ and then

$$\mathrm{G}_T/(\mathrm{G}_T)_{(3)} \simeq \mathrm{F}'/\mathrm{F}'_{(3)} \simeq H_{p^3},$$

where $(\mathrm{G}_T)_{(n)} \simeq \mathrm{R}' \cap \mathrm{F}'_{(n)}/\mathrm{R}'$ and where

$$H_{p^3} = \langle x, y, x^p = 1, y^p = 1, [[x, y], x] = [[x, y], y] = 1\rangle$$

is the Heisenberg group of order p^3.

Let $\mathrm{K}_{i,j} = \mathbb{Q}_{(\ell_i,\ell_j)}^{(3)}$ be the p-extension associated by Galois theory to the group $(\mathrm{G}_T)_{(3)}$ and put $\mathrm{M}_{i,j} = \mathbb{Q}_{\ell_i}^{p,el}\mathbb{Q}_{\ell_j}^{p,el}$. Then $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathrm{M}_{i,j}) = \langle [x_i, x_j]\rangle$.

PROPOSITION 2.19. *One has $\mu(i, j, k) = -\mu(j, i, k)$. Moreover*

$$\mu(i, j, k) = 0 \Longleftrightarrow \mathfrak{l}_k \text{ splits in } \mathrm{K}_{i,j}/\mathrm{M}_{i,j},$$

where $\mathfrak{l}_k$ is a prime of $\mathrm{M}_{i,j}$ above ℓ_k.

Proof. This is an application of Example 2.7. Thanks to the conditions above ℓ_i, ℓ_j and ℓ_k, and Remark 2.1, the restriction of the element y_k to $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathbb{Q})$ is in the subgroup $\langle [x_i, x_j] \rangle$:

$$y_k \equiv [x_i, x_j]^a \pmod{\mathrm{Gal}(\mathbb{Q}_{\mathrm{S}}/\mathrm{K}_{\mathrm{i,j}})}.$$

Then $\varepsilon_{i,j}(y_k) = \varepsilon_{i,j}([x_i, x_j]^a) = a$ and $\varepsilon_{j,i}(y_k) = \varepsilon_{j,i}([x_i, x_j]^a) = -a$. □

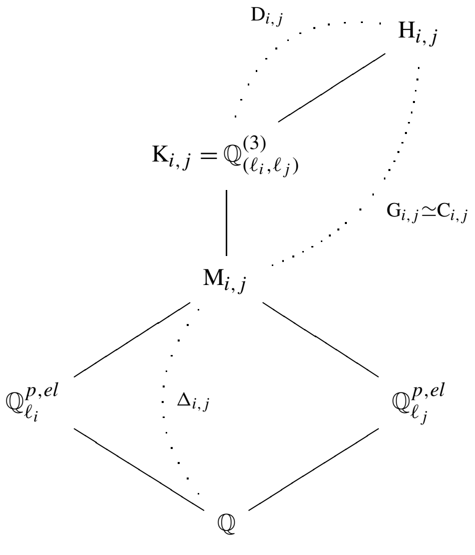
2.6. *The use of class field theory*

First, let us observe the following.

PROPOSITION 2.20. *The extension* $\mathrm{K}_{i,j}/\mathrm{M}_{i,j}$ *is unramified.*

Proof. The non-trivial elements of the Galois group of $\mathrm{K}_{i,j}/\mathbb{Q}$ are of order p. Hence, if a prime above ℓ_i is ramified in $\mathrm{K}_{i,j}/\mathrm{M}_{i,j}$, then $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathrm{M}_{i,j})$ is the inertia group in $\mathrm{K}_{i,j}/\mathbb{Q}$ of all primes above ℓ_i which contradicts the fact that $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$ is totally ramified at ℓ_i. □

Let $\mathrm{C}_{i,j} := \mathrm{Cl}_{\mathrm{M}_{i,j}}/(\mathrm{Cl}_{\mathrm{M}_{i,j}})^p$ be the elementary p-quotient of the class group of $\mathrm{M}_{i,j}$. By class field theory, $\mathrm{C}_{i,j}$ is isomorphic to the Galois group $\mathrm{G}_{i,j}$ of the maximal abelian unramified elementary p-extension $\mathrm{H}_{i,j}$ of $\mathrm{M}_{i,j}$. Put $\Delta_{i,j} = \mathrm{Gal}(\mathrm{M}_{i,j}/\mathbb{Q})$.


$\mathrm{D}_{i,j}$
$\mathrm{H}_{i,j}$
$\mathrm{K}_{i,j} = \mathbb{Q}^{(3)}_{(\ell_i,\ell_j)}$
$\mathrm{G}_{i,j} \simeq \mathrm{C}_{i,j}$
$\mathrm{M}_{i,j}$
$\mathbb{Q}_{\ell_i}^{p,el}$
$\Delta_{i,j}$
$\mathbb{Q}_{\ell_j}^{p,el}$
$\mathbb{Q}$

Then the extension $\mathrm{H}_{i,j}/\mathbb{Q}$ is Galois and $\Delta_{i,j}$ acts on $\mathrm{G}_{i,j}$ (and on $\mathrm{C}_{i,j}$) as follows

$$\tau \cdot (\mathfrak{a}, \mathrm{H}_{i,j}/\mathrm{M}_{i,j}) := \tau(\mathfrak{a}, \mathrm{H}_{i,j}/\mathrm{M}_{i,j})\tau^{-1} = (\mathfrak{a}^\tau, \mathrm{H}_{i,j}/\mathrm{M}_{i,j}),$$

where $(., \mathrm{H}_{i,j}/\mathrm{M}_{i,j}) : \mathrm{C}_{i,j} \to \mathrm{G}_{i,j} = \mathrm{Gal}(\mathrm{H}_{i,j}/\mathrm{M}_{i,j})$ is the Artin symbol.

As consequence of Proposition 2.19, one has the following result.

PROPOSITION 2.21. *We have*

$$\mu(i, j, k) = 0 \Longleftrightarrow \mathfrak{l}_k \text{ splits in } \mathrm{K}_{i,j}/\mathrm{M}_{i,j} \Longleftrightarrow (\mathfrak{l}_k, \mathrm{H}_{i,j}/\mathrm{M}_{i,j}) \in \mathrm{D}_{i,j},$$

where $\mathfrak{l}_k$ *is a prime of* $\mathrm{M}_{i,j}$ *above* ℓ_k.

We finish this part with the question of how to find the subgroup $\mathrm{D}_{i,j}$.

LEMMA 2.22. *There exists a unique subgroup* C *of* $\mathrm{C}_{i,j}$ *such that* C′ *is normal in* $\mathrm{Gal}(\mathrm{H}_{i,j}/\mathbb{Q})$ *and such that* $\mathrm{C}_{i,j}/\mathrm{C} \simeq \mathbb{Z}/p\mathbb{Z}$. *Hence,* $\mathrm{D}_{i,j}$ *is the unique subgroup of* $\mathrm{C}_{i,j}$ *of index p fixed by* $\Delta_{i,j}$.

Proof. If C′ is an another subgroup, then the quotient $\mathrm{Gal}(\mathrm{H}_{i,j}/\mathbb{Q})/\mathrm{C}'$ is a group of order p^3. Let K′ be the fixed field by C′. The extension $\mathrm{K}'/\mathrm{M}_{i,j}$ is unramified. First, it is obvious that the group $\mathrm{Gal}(\mathrm{K}'/\mathbb{Q})$ cannot be the group $(\mathbb{Z}/p\mathbb{Z})^3$. Now the groups $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and the non-abelian group of order p^3 different from H_{p^3} have the same particularity: all of the subgroups of order p^2 are cyclic, excepts one. Hence, if $\mathrm{Gal}(\mathrm{K}'/\mathbb{Q})$ is different from H_{p^3}, we can assume that $\mathrm{Gal}(\mathrm{K}'/\mathbb{Q}_{\ell_i}^{p,el})$ is cyclic. Then, as $\mathrm{K}'/\mathrm{M}_{i,j}$ is unramified, one deduces that $\mathrm{K}'/\mathbb{Q}_{\ell_i}^{p,el}$ is unramified. A contradiction. Hence, $\mathrm{Gal}(\mathrm{K}'/\mathbb{Q}) \simeq H_{p^3}$. The Galois group $\mathrm{Gal}(\mathrm{K}'/\mathbb{Q})$ is a quotient of F′, the relations of this quotient are in $\mathrm{F}_{(3)}$, and by comparing the indices, one obtains that C′ = C. □

2.7. *How to compute the relations modulo $F_{(4)}$*

Recall that $S = \{\ell_1, \ldots, \ell_d\}$. Following Remark 2.4, for $j = 1, \ldots, d$, let us choose some auxiliary primes q_j such that:

(i) the prime q_j is inert in $\mathbb{Q}_{\ell_j}^{p,el}/\mathbb{Q}$;

(ii) for all $i \neq j$, the prime q_j splits in $\mathbb{Q}_{\ell_i}^{p,el}/\mathbb{Q}$.

For $j = 1, \ldots, d$, there exist p^{d-1} primes $\mathfrak{Q}_j^{(*)}$ in $\mathbb{Q}_S^{p,el}$ above the auxiliary prime q_j. Then, for $j = 1, \ldots, d$, let us fix $\mathfrak{Q}_j | q_j$ one of these primes and then let us choose $x_j \in \mathrm{G}_S$ such that its restriction to $\mathrm{Gal}(\mathbb{Q}_S^{p,el}/\mathbb{Q})$ is equal to the inverse $\mathfrak{f}_{\mathfrak{Q}_j}^{-1}$ of the Frobenius $\mathfrak{f}_{\mathfrak{Q}_j}$ of $\mathfrak{Q}_j$.

Consider two primes ℓ_i and ℓ_j such that $\mu(i, j) = \mu(j, i) = 0$. Let ℓ_k be a third prime (eventually $\ell_k = \ell_i$), such that $\mu(i, k) = \mu(j, k) = 0$.

We want to compute $\mu(i, j, k)$ when it is non-zero.

We use the notation of Sections 2.5 and 2.6 for the primes ℓ_i and ℓ_j.

First, the extension $\mathrm{K}_{i,j}/\mathbb{Q}$ is a Heisenberg extension and we know that

$$y_k \equiv [x_i, x_j]^a \pmod{\mathrm{Gal}(\mathbb{Q}_\mathrm{S}/\mathrm{K}_{\mathrm{i,j}})}$$

and then $\mu(i, j, k) = a$.

The field $\mathbb{Q}_{\ell_i}^{p,el}$ contains p primes $\mathfrak{l}_j^{(1)}, \ldots, \mathfrak{l}_j^{(p)}$ above ℓ_j and p primes $\mathfrak{q}_j^{(1)}, \ldots, \mathfrak{q}_j^{(p)}$ above q_j. Now, in $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathbb{Q})$, fixing the subgroup generated by the Frobenius $\mathfrak{f}_{\mathfrak{q}_j^{(*)}}$ of a prime above q_j is equivalent to fixing the inertia group of a place $\mathfrak{l}_i^{(*)}$. For what follows, we assume that $\mathfrak{f}_{\mathfrak{q}_j^{(n)}}$ corresponds to $\mathfrak{l}_j^{(n)}$, $n = 1, \ldots, p$, and that moreover $\mathfrak{Q}_j \cap \mathrm{K}_{i,j} = \mathfrak{q}_j^{(1)} := \mathfrak{q}_j$. Then the restriction of x_j to $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathbb{Q})$ is equal to the inverse of the Frobenius $\mathfrak{f}_{\mathfrak{q}_j}$ of $\mathfrak{q}_j$.

Consider the subfield $\mathrm{N}_{i,j}$ of $\mathbb{Q}_{(\ell_i,\ell_j)}^{(p)}/\mathbb{Q}_{\ell_i}^{p,el}$ fixed by the Frobenius $\mathfrak{f}_{\mathfrak{q}_j}$ of $\mathfrak{q}_j$. Then

$$[x_i, x_j] \equiv (\mathfrak{f}_{\mathfrak{q}_j})^{x_i^{-1}} x_j \equiv \mathfrak{f}_{\mathfrak{q}_j^{x_i^{-1}}} x_j \pmod{\mathrm{Gal}(\mathbb{Q}_\mathrm{S}/\mathrm{K}_{\mathrm{i,j}})}.$$

Now the elements x_j and $\mathfrak{f}_{\mathfrak{q}_j^{x_i^{-1}}}$ are in $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{\ell_i}^{p,el})$, and then

$$[x_i, x_j] \equiv \mathfrak{f}_{\mathfrak{q}_j^{\mathfrak{f}_{q_i}}} \in \mathrm{Gal}(\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el}),$$

where $\mathfrak{f}_{q_i}$ is the Frobenius of the auxiliary prime q_i in $\mathrm{Gal}(\mathbb{Q}_{l_i}^{p,el}/\mathbb{Q})$.

Hence, as $\mathfrak{f}_{\mathfrak{q}_j^{\mathfrak{f}_{q_i}}}$ is not trivial in $\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el}$,

$$y_k \equiv [x_i, x_j]^a \pmod{\mathrm{Gal}(\mathbb{Q}_\mathrm{S}/\mathrm{K}_{\mathrm{i,j}})}$$

if and only if

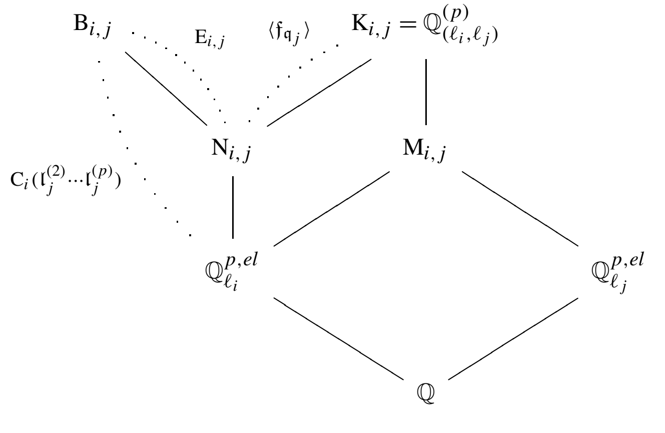
$$y_k \equiv \mathfrak{f}^a_{\mathfrak{q}_j^{\mathfrak{f}_{q_i}}} \in \mathrm{Gal}(\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el}),$$

which still makes sense because $y_k \in \mathrm{Gal}(\mathbb{Q}_S^{ab}/\mathbb{Q}_{\ell_i}^{p,el})$. Hence, to have $a \in \mathbb{F}_p$, it suffices to compare y_k with $\mathfrak{f}_{\mathfrak{q}_j^{\mathfrak{f}_{q_i}}}$ in $\mathrm{Gal}(\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el})$.

The question next is how to find $\mathrm{N}_{i,j}$?

The Frobenius $\mathfrak{f}_{\mathfrak{q}_j}$ is associated with the inertia group of the prime $\mathfrak{l}_{\ell_j}^{(1)}$ above ℓ_j. Hence, the extension $\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el}$ is of the conductor dividing $\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)}$.

Denote by $\mathrm{C}_i(\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)})$ the p-elementary quotient of the ray class group of $\mathbb{Q}_{\ell_i}^{p,el}$ of conductor $\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)}$. Let $\mathrm{B}_{i,j}$ be the p-elementary abelian extension of $\mathbb{Q}_{\ell_i}^{p,el}$ of conductor $\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)}$: by class field theory, $\mathrm{C}_i(\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)}) \simeq \mathrm{Gal}(\mathrm{B}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el})$. As the p-class group of $\mathbb{Q}_{\ell_i}^{p,el}$ is trivial, $\mathrm{Gal}(\mathrm{B}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el})$ is a quotient of $(\mathbb{Z}/p\mathbb{Z})^{p-1}$.



$\mathrm{B}_{i,j}$
$\mathrm{E}_{i,j}$
$\langle \mathfrak{f}_{\mathfrak{q}_j} \rangle$
$\mathrm{K}_{i,j} = \mathbb{Q}^{(p)}_{(\ell_i,\ell_j)}$
$\mathrm{N}_{i,j}$
$\mathrm{M}_{i,j}$
$\mathrm{C}_i(\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)})$
$\mathbb{Q}_{\ell_i}^{p,el}$
$\mathbb{Q}_{\ell_j}^{p,el}$
$\mathbb{Q}$

If $\mathrm{Gal}(\mathrm{B}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el})$ is cyclic, there is nothing to do: $\mathrm{B}_{i,j} = \mathrm{N}_{i,j}$.

Let $\mathfrak{A}$ be a prime for which the Frobenius $\mathfrak{f}_\mathfrak{A}$ generates $\mathrm{Gal}(\mathrm{K}_{i,j}/\mathrm{M}_{i,j})$. Then the extension $\mathrm{N}_{i,j}/\mathbb{Q}_{\ell_i}^{p,el}$ is such that:

(i) the restriction of $\mathfrak{f}_\mathfrak{A}$ is trivial;

(ii) the prime $\mathfrak{q}_j = \mathfrak{q}_j^{(1)}$ splits;

(iii) the primes $\mathfrak{q}_j^{(n)}$ are inert, $n = 2, \ldots, d$.

These properties characterize $\mathrm{N}_{i,j}$ (and then the subgroup $\mathrm{D}_{i,j}$) but also the primes $\mathfrak{l}_j^{(1)}$ associated with $\mathfrak{q}_j := \mathfrak{q}_j^{(1)}$. In conclusion, we have the following result.

PROPOSITION 2.23. *The quantity $\mu(i, j, k) \in \mathbb{F}_p$ is such that*

$$\mathfrak{l}_k \equiv \left(\mathfrak{q}_j^{\mathfrak{f}_{q_i}}\right)^{\mu(i,j,k)} \in \mathrm{C}_i(\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)})/\mathrm{E}_{i,j},$$

where $\mathfrak{l}_k | \ell_k$ is a prime ideal of $\mathbb{Q}_{\ell_i}^{p,el}$ above ℓ_k not dividing $\mathfrak{l}_j^{(2)} \cdots \mathfrak{l}_j^{(p)}$. In particular, when $k = j$, one has to take $\mathfrak{l}_k = \mathfrak{l}_j^{(1)}$.

3. Examples

3.1. Example

Take $p = 3$ and $S = \{\ell_1 = 11\,863, \ell_2 = 19, \ell_3 = 9811\}$.

First, we note that $\ell_i \equiv 1(p^2)$ and that for all $i \neq j$, the prime ℓ_i splits in $\mathbb{Q}_{\ell_j}^{p,el}/\mathbb{Q}$: $\mu(i, j) = 0$. Now, thanks to Propositions 1.15 and 2.17, the relations of G_S become:

	$e_{1,2,1}$	$e_{1,2,2}$	$e_{1,3,1}$	$e_{1,3,2}$
ρ_1	$-\mu(1, 2, 1)$	0	$-\mu(1, 3, 1)$	0
ρ_2	0	$-\mu(1, 2, 2)$	0	$-\mu(1, 3, 2)$
ρ_3	0	0	0	$-\mu(1, 2, 3)$

	$e_{1,3,3}$	$e_{2,3,1}$	$e_{2,3,2}$	$e_{2,3,3}$
ρ_1	0	$-\mu(2, 3, 1)$	0	0
ρ_2	0	0	$-\mu(2, 3, 2)$	0
ρ_3	$-\mu(1, 3, 3)$	$\mu(1, 2, 3)$	0	$-\mu(2, 3, 3)$

Notation. If ℓ_i and ℓ_j are two fixed primes, put $\mathrm{M}_{i,j} = \mathbb{Q}_{\ell_i}^{p,el}\mathbb{Q}_{\ell_j}^{p,el}$ and let $\mathrm{H}_{i,j}$ be the elementary unramified p-extension of $\mathrm{M}_{i,j}$.

If $\mathfrak{A}$ is an ideal of $\mathrm{M}_{i,j}$, denote by $\sigma_{\mathfrak{A}} := (\mathfrak{A}, \mathrm{H}_{i,j}/\mathrm{M}_{i,j})$ the Artin symbol of $\mathfrak{A}$ in $\mathrm{H}_{i,j}/\mathrm{M}_{i,j}$. If ℓ is a prime of $\mathbb{Q}$, then $\mathfrak{L}_\ell$ will be a prime of $\mathrm{M}_{i,j}$ above ℓ.

3.1.1. The extension $\mathbb{Q}_{\ell_1,\ell_2}^{3,el}/\mathbb{Q}$. The number field $\mathbb{Q}_{\ell_1}^{3,el} = \mathbb{Q}(\theta_1)$ is the unique subfield of $\mathbb{Q}(\zeta_{11863})$ of degree three over $\mathbb{Q}$. It is defined by a root θ_1 of the equation: $x^3 + x^2 - 3954x + 39\,104 = 0$. The field $\mathbb{Q}_{\ell_2}^{3,el} = \mathbb{Q}(\theta_2)$ is defined by a root θ_2 of the equation: $x^3 + x^2 - 6x - 7 = 0$. The compositum $\mathrm{M}_{1,2} = \mathbb{Q}_{\ell_1}^{3,el}\mathbb{Q}_{\ell_2}^{3,el}$ is generated by a root θ of the equation

$$\begin{aligned}
&x^9 - x^8 - 51\,408x^7 + 137\,525x^6 + 778\,957\,094x^5 + 583\,863\,320x^4 \\
&- 3\,310\,991\,579\,976x^3 - 29\,421\,274\,145\,536x^2 + 1\,777\,568\,574\,652\,416x \\
&+ 20\,509\,622\,778\,724\,352 = 0.
\end{aligned}$$

The 3-class group $\mathrm{C}_{1,2}$ of $\mathrm{M}_{1,2}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Gal}(\mathrm{K}_{1,2}/\mathrm{M}_{1,2}) = \langle\sigma_{\mathfrak{L}_{19}}\rangle = \langle\sigma_{\mathfrak{L}_{11\,863}}\rangle$. We remark that $\sigma_{\mathfrak{L}_{19}}^{-1} = \sigma_{\mathfrak{L}_{11\,863}}$. Hence, by Proposition 2.21, $\mu(1, 2, 1) \neq 0$ and $\mu(1, 2, 2) \neq 0$.

3.1.2. The extension $\mathbb{Q}^{3,el}_{\ell_1,\ell_3}/\mathbb{Q}$. The number field $\mathbb{Q}^{3,el}_{\ell_3}$ is defined by the equation $x^3 + x^2 - 3270x - 6904 = 0$. The compositum $\mathrm{M}_{1,3} = \mathbb{Q}^{3,el}_{\ell_1}\mathbb{Q}^{3,el}_{\ell_3}$ is generated by a root β of the equation:

$$\begin{aligned}&x^9 - x^8 - 25\,866\,384x^7 + 495\,245\,276x^6 + 166\,553\,813\,929\,280x^5\\&- 2\,186\,400\,407\,814\,976x^4 - 56\,279\,799\,218\,070\,071\,808x^3\\&+ 83\,890\,962\,452\,662\,796\,288x^2 + 942\,384\,971\,138\,013\,179\,412\,480x\\&+ 19\,677\,317\,846\,068\,743\,788\,036\,096 = 0.\end{aligned}$$

The class group of $\mathrm{M}_{1,3}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Gal}(\mathrm{K}_{1,3}/\mathrm{M}_{1,3}) = \langle\sigma_{\mathfrak{L}_{11\,863}}\rangle = \langle\sigma_{\mathfrak{L}_{9811}}\rangle$. Moreover, $\sigma_{\mathfrak{L}_{19}} = 1$. Hence, by Proposition 2.21, $\mu(1, 3, 2) = 0$, $\mu(1, 3, 1) \neq 0$ and $\mu(1, 3, 3) \neq 0$.

3.1.3. The extension $\mathbb{Q}^{3,el}_{\ell_2,\ell_3}/\mathbb{Q}$. The compositum $\mathrm{M}_{2,3} = \mathbb{Q}^{3,el}_{\ell_2}\mathbb{Q}^{3,el}_{\ell_3}$ is generated by a root γ of the equation:

$$\begin{aligned}&x^9 - x^8 - 42\,516x^7 + 35\,249x^6 + 535\,158\,074x^5 - 630\,338\,704x^4\\&- 1\,724\,988\,572\,520x^3 + 3\,634\,048\,124\,000x^2 + 45\,824\,385\,358\,080x\\&- 112\,874\,663\,383\,552 = 0.\end{aligned}$$

The class group of $\mathrm{M}_{2,3}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$. The p-group $\Delta_{2,3}$ acts trivially on $\sigma_{\mathfrak{L}_{19}}$ and on $\sigma_{\mathfrak{L}_{9811}}$ and then on $\langle\sigma_{\mathfrak{L}_{19}}, \sigma_{\mathfrak{L}_{9811}}\rangle \simeq (\mathbb{Z}/3\mathbb{Z})^2$. Hence, $\langle\sigma_{\mathfrak{L}_{19}}, \sigma_{\mathfrak{L}_{9811}}\rangle = \mathrm{D}_{2,3}$ and one verifies that $\mathrm{Gal}(\mathrm{K}_{2,3}/\mathrm{M}_{2,3}) = \langle\sigma_{\mathfrak{L}_{87|\mathrm{K}_{2,3}}}\rangle$. The primes $\mathfrak{L}_{19}$ and $\mathfrak{L}_{9811}$ split in $\mathrm{K}_{2,3}/\mathrm{M}_{2,3}$, and then $\mu(2, 3, 3) = \mu(2, 3, 2) = 0$. To finish, one has $\sigma_{\mathfrak{L}_{11863}} \notin \mathrm{D}_{2,3}$: $\mu(2, 3, 1) \neq 0$.

3.1.4. The ordering. Consider now the ordering $X_3 > X_2 > X_1$. Then by the above computation

$$\ell(\omega(\rho_1)) = X_3X_2X_1, \quad \ell(\omega(\rho_2)) = X_3X_2X_2, \quad \ell(\omega(\rho_3)) = X_3X_3X_1.$$

To conclude, the family $\{\rho_1, \rho_2, \rho_3\}$ is combinatorially free, the pro-p-group G_S is mild, and then by Theorem 1.11, the cohomological dimension of G_S is two.

3.1.5. The computation of the relations modulo $\mathrm{F}_{(4)}$. Recall that $p = 3$ and $S = \{\ell_1 = 11\,863, \ell_2 = 19, \ell_3 = 9811\}$.

First, we compute some auxiliary primes following Section 2.7: $q_1 = 31$, $q_2 = 2$, $q_3 = 191$.

The quantity $\mu(2, 3, 1)$. The computation will be done in the Heisenberg extension $\mathbb{Q}^{3,el}_{\ell_2,\ell_3}/\mathbb{Q}$. Following the notation of Section 2.7, we take $i = 2$ and $j = 3$.

Let $\mathcal{O}_2$ be the ring of integers of $\mathbb{Q}^{3,el}_{\ell_2} = \mathbb{Q}(\theta_2)$. One has the decompositions: $191\mathcal{O}_2 = \mathfrak{l}_{191}\mathfrak{l}'_{191}\mathfrak{l}''_{191}$, with $\mathfrak{l}_{191} = (191, 35 + \theta_2)$, $\mathfrak{l}'_{191} = (191, 75 + \theta_2)$, $\mathfrak{l}''_{191} = (191, 82 + \theta_2)$ and $9811\mathcal{O}_2 = \mathfrak{l}_{9811}\mathfrak{l}'_{9811}\mathfrak{l}''_{9811}$, with $\mathfrak{l}_{9811} = (9811, -3147 + \theta_2)$, $\mathfrak{l}'_{9811} = (9811, -1158 + \theta_2)$, $\mathfrak{l}''_{9811} = (9811, 4306 + \theta_2)$. The p-part of the ray class group of $\mathbb{Q}^{3,el}_{\ell_2}$ of conductor $\mathfrak{l}'_{9811}\mathfrak{l}''_{9811}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$: $\mathrm{C}_2(\mathfrak{l}'_{9811}\mathfrak{l}''_{9811}) = \langle(3), (\theta_2)\rangle$. The computation in this ray class group and conditions (i)–(iii) of Section 2.7 allow us to verify that $\mathfrak{l}_{9811}$ is associated with $\mathfrak{f}_{\mathfrak{l}_{191}}$: in $\mathrm{Gal}(\mathrm{K}_{2,3}/\mathbb{Q})$ the Frobenius $\mathfrak{f}_{\mathfrak{l}_{191}}$ generates the inertia group of $\mathfrak{l}_{9811}$. One verifies that $\mathfrak{f}_2 : \theta_2 \mapsto -\theta_2^2 + 4$ and that $\mathfrak{l}_{191}^{\mathfrak{f}_2} = \mathfrak{l}''_{191}$. Then, following the computation of Section 2.7:

$$[x_2, x_3] \equiv \mathfrak{f}_{\mathfrak{l}''_{191}} \in \mathrm{Gal}(\mathrm{N}_{2,3}/\mathbb{Q}_{\ell_2}^{p,el}). \tag{3}$$

To conclude, in the quotient $\mathrm{C}(\mathfrak{l}'_{9811}\mathfrak{l}''_{9811})/\mathrm{E}_{2,3}$, the ideals $\mathfrak{l}''_{191}$ and $\mathfrak{l}_{11863}$ are in the same class and then (thanks to (3)):

$$y_1 \equiv \mathfrak{f}_{\mathfrak{l}_{11863}} \equiv [x_2, x_3] (\mathrm{mod}\, \mathrm{Gal}(\mathbb{Q}_\mathrm{S}/\mathrm{K})),$$

and $\mu(2, 3, 1) = 1$.

The quantities $\mu(1, 2, 2)$ *and* $\mu(1, 2, 1)$. The computation will be done in the Heisenberg extension $\mathbb{Q}_{\ell_2,\ell_1}^{3,el}/\mathbb{Q}$ and following the notation of Section 2.7, we take $i = 2$ and $j = 1$. One has in $\mathbb{Q}_{\ell_2}^{3,el}$: $\mathfrak{l}'_{31} = (31, 4 + \theta_2)$, $\mathfrak{l}''_{31} = (31, 12 + \theta_2)$, and $11\,863\mathcal{O}_2 = \mathfrak{l}_{11\,863}\mathfrak{l}'_{11\,863}\mathfrak{l}''_{11\,863}$, where $\mathfrak{l}_{11\,863} = (11\,863, -3181 + \theta_2)$, $\mathfrak{l}'_{11\,863} = (11\,863, -382 + \theta_2)$, $\mathfrak{l}''_{11\,863} = (11\,863, 3564 + \theta_2)$. The ray class group of $\mathbb{Q}_{\ell_2}^{p,el}$ of conductor $\mathfrak{l}'_{11\,863}\mathfrak{l}''_{11\,863}$ is cyclic of degree three: $\mathrm{C}_2(\mathfrak{l}'_{11\,863}\mathfrak{l}''_{11\,863}) = \langle(\theta_2)\rangle$. The computation allow us to see that $\mathfrak{f}_{\mathfrak{l}_{31}}$ generates the inertia group of $\mathfrak{l}_{11863}$ and that $\mathfrak{l}'^{\mathfrak{f}_2}_{11\,863} = \mathfrak{l}''_{11\,863}$. Then

$$[x_1, x_2]^{-1} \equiv x_2^{-1}x_1^{-1}x_2x_1 \equiv \mathfrak{f}_{\mathfrak{l}''_{31}} \in \mathrm{Gal}(\mathrm{B}_{i,j}/\mathbb{Q}_{\ell_2}^{p,el}).$$

Now the restrictions of $\mathfrak{f}_{\mathfrak{l}_{19}}$ and of $\mathfrak{f}_{\mathfrak{l}''_{31}}$ in $\mathrm{B}'_{i,j}/\mathbb{Q}_{\ell_2}^{3,el}$ are the same. In conclusion:

$$y_2 \equiv \mathfrak{f}_{\mathfrak{l}_{19}} \equiv [x_1, x_2]^{-1} \quad (\mathrm{mod}\, \mathrm{Gal}(\mathbb{Q}_\mathrm{S}/\mathbb{Q}_{\ell_1,\ell_2}^{\mathrm{p,el}}))$$

i.e. $\mu(1, 2, 2) = -1$. By a similar computation:

(i) $\mathfrak{f}_{\mathfrak{l}_{11863}} = \mathfrak{f}_{\mathfrak{l}_{19}}^{-1}$ and then $\mu(1, 2, 1) = 1$;

(ii) $\mathfrak{f}_{\mathfrak{l}_{9811}} = \mathfrak{f}_{\mathfrak{l}_{19}}$ and then $\mu(1, 2, 3) = -1$.

The quantities $\mu(1, 3, 3)$ *and* $\mu(1, 3, 1)$. By a similar computation in the number field $\mathbb{Q}_{\ell_3}^{3,el}$, one also obtains $\mu(1, 3, 3) = \mu(1, 3, 1) = 1$.

To conclude, the computations above show the following.

Proposition 3.1. *The pro-3-group* $\mathrm{G}_{\{19,9811,11\,863\}}$ *can be defined by the generators* x_1, x_2 *and* x_3*, and by the relations*

$$\rho_1 \equiv [[x_1, x_2], x_1][[x_1, x_3], x_1][[x_2, x_3], x_1] \quad (\mathrm{mod}\, \mathrm{F}_{(4)}),$$

$$\rho_2 \equiv [[x_1, x_2], x_2]^{-1} \quad (\mathrm{mod}\, \mathrm{F}_{(4)}),$$

$$\rho_3 \equiv [[x_1, x_3], x_2]^{-1}[[x_1, x_3], x_3][[x_2, x_3], x_1] \quad (\mathrm{mod}\, \mathrm{F}_{(4)}).$$

3.2. A second example

Take $p = 3$, $S = \{\ell_1 = 13, \ell_2 = 7, \ell_3 = 11\,971, \ell_4 = 181\}$ and consider the ordering $X_4 > X_3 > X_2 > X_1$.

The relations ρ_1 and ρ_2 are of degree two. Indeed, as $\mu(4, 1) \neq 0$, thanks to Propositions 1.15 and 2.14, one has $\ell(\omega(\rho_1)) = X_4X_1$.

Moreover, $\mu(4, 2) = \mu(3, 2) = 0$ and $\mu(1, 2) \neq 0$, and then $\ell(\omega(\rho_2)) = X_2X_1$.

Now for all i, $\mu(i,3)=\mu(i,4)=0$, by Proposition 2.14, the relations ρ_3 and ρ_4 are in $\mathrm{F}_{(3)}$. Thanks to Proposition 2.17 and Example 2.6 the study of the relations ρ_3 and ρ_4 we will be done in some H_{p^3} extension of $\mathbb{Q}$.

First, let us remark that as $\ell_4 \equiv 1(\text{mod p}^2)$. Hence, $\varepsilon_{4,4,4}(\rho_4)=0$.

By a computation in the extension $\mathbb{Q}^{(3)}_{\ell_3,\ell_4}/\mathbb{Q}$, one obtains that $\mu(4,3,3)=0$ and that $\mu(3,4,4)\neq 0$. By a computation in the extension $\mathbb{Q}^{(3)}_{\ell_2,\ell_4}/\mathbb{Q}$, one obtains $\mu(2,4,3)\neq 0$. Recall that $\mu(4,4,3)=0$ (see Proposition 2.18).

Hence, $\varepsilon_{4,4,3}(\rho_3)=\mu(4,4,3)=0$, $\varepsilon_{4,3,3}(\rho_3)=\mu(4,3,3)=0$, and $\varepsilon_{4,2,3}(\rho_3)=\mu(4,2,3)\neq 0$. Then $\ell(\omega(\rho_3))=X_4X_2X_3$.

Moreover, $\varepsilon_{4,4,3}(\rho_4)=\mu(4,3,4)\neq 0$, and then $\ell(\omega(\rho_4))=X_4X_4X_3$.

We conclude that G_S is mild by noting that the family

$$\{X_4X_1,\ X_2X_1,\ X_4X_2X_3,\ X_4X_4X_3\}$$

is combinatorially free.

Acknowledgements. The author would like to thank Jan Minac and John Labute for making possible a visit to McGill and to the University of Western Ontario during summer 2012. The work of this paper started during these stays. He is also grateful to John Labute and to Jan Minac for many useful conversations and for their warm hospitality and their enthusiastic support.

He would also like to thank to Farshid Hajir and Jochen Gärtner for their interest in this work.

References

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

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier. GP-Pari. Available from http://pari.math.u-bordeaux.fr/.

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

[4] J.D. Dixon M. Du Sautoy, A. Mann and D. Segal. Analytic Pro-p-groups. Cambridge University Press, Cambridge, 1999.

[5] P. Forré. Strongly free sequences and pro-p-groups of cohomological dimension 2. J. Reine Angew. Math. **658** (2011), 173–192.

[6] A. Fröhlich. On fields of class two. Proc. London Math. Soc. (3) **4** (1954), 235–256.

[7] J. Gärtner. Mild Pro-p-groups with Trivial Cup-product. PhD Thesis, Heidelberg, 2011.

[8] H. Koch. Galois Theory of p-extensions. Springer, Berlin, 2002.

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

[10] M. Morishita. Milnor's link invariants attached to certain Galois groups over $\mathbb{Q}$. Proc. Japan Acad. Ser. A Math. Asci. **76**(2) (2000), 18–21.

[11] M. Morishita. On certain analogies between knots and primes. J. Reine Angew. Math. **550** (2002), 141–167.

[12] J. Neukirch, A. Schmidt and K. Wingberg. Cohomology of Number Fields (Grundlehren der Mathematischen Wissenschaften, 323). Springer, Berlin, 2008.

[13] L. Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie des quadratischen Zahlkörper I. J. Reine Angew. Math. **180** (1938), 1–43.

[14] A. Schmidt. Rings of integers of type $K(\pi,1)$. Doc. Math. **12** (2007), 441–471.

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

[16] D. Vogel. Massey Products in the Galois Cohomology of Number Fields. PhD Thesis, Heidelberg, 2004.

[17] D. Vogel. On the Galois group of 2-extensions with restricted ramification. J. Reine Angew. Math. **581** (2005), 117–150.

Christian Maire
Université de Franche-Comté
Laboratoire de Mathématiques
UMR CNRS 6623, UFR Sciences et Techniques
16 route de Gray
F-25030 Besançon
France
(E-mail: christian.maire@univ-fcomte.fr)