Mild pro-$p$-groups and $p$-extensions of imaginary quadratic fields with non-trivial $p$-class group

ZAKARIAE BOUAZZAOUI  ABDELAZIZ EL HABIBI

ABSTRACT. Let $k$ be an imaginary quadratic field and $p$ an odd prime number such that the $p$-rank of the class group of $k$ is one. Let $S$ be a finite set of places of $k$ distinct from $p$-adic places. We give sufficient conditions for the Galois group $G_S$, of the maximal pro-$p$-extension of $k$ which is unramified outside $S$, to be mild, hence of cohomological dimension 2.

1 Introduction

Let $p$ be a prime number, and let $k$ be a number field which is a finite extension of the field of rationals $\mathbb{Q}$. For a finite set $S$ of primes of $k$, consider the Galois group

$$G_S = \text{Gal}(k_S/k)$$

of the maximal pro-$p$-extension $k_S$ of $k$ which is unramified outside $S$. Galois extensions with ramification restricted to finite sets of primes arise naturally in algebraic number theory and arithmetic geometry, e.g., in terms of representations coming from the Galois action on the (étale) cohomology of algebraic varieties defined over number fields. A non-$p$-adic prime ideal $v$ of $k$ cannot ramify in any $p$-extensions over $k$ if the absolute norm $|O_k/v| \not\equiv 1 \pmod{p}$, where $O_k$ is the ring of algebraic integers in $k$. Since we consider only such pro-$p$-extensions over $k$ in the following, we assume that $S$ contains no archimedean primes if $p \neq 2$, and that $|O_k/v| \equiv 1 \pmod{p}$ for any prime ideal $v \in S$ which is not $p$-adic. The structure of $G_S$ reflects arithmetic properties of the field $k$ at the prime $p$. In particular when $S = \emptyset$, the derived series of $\text{Gal}(k_0/k)$ correspond to the $p$-class field tower of $k$, which is a classical object in algebraic number theory. If $S$ contains the places of $k$ lying above $p$, the group $G_S$ is fairly well understood. In particular it has been known that it is of cohomological dimension $\text{cd}(G_S)$ is at most 2 (assuming $k$ is totally imaginary if $p = 2$) and often a duality group (cf. [14]).

So far the structure of $G_S$ remains mysterious when $S$ is disjoint with the $p$-adic places. By celebrate theorems of Golod and Shafarevich, the group $G_S$ is infinite under some condition and it is a so-called $\text{fab}$ pro-$p$-group, i.e., the maximal abelian quotient of every open subgroup of $G_S$ is finite. However, the cohomological dimension of $G_S$ is not well understood.

J. Labute introduce mild pro-$p$-groups in [10] to give examples of groups $G_S$ with

2010 Mathematics Subject Classification: 11R32, (11R37).
Key words: Mild pro-$p$-groups, restricted ramification, class field theory.
\( \text{cd}(G_S) = 2 \) when \( S \) contains no \( p \)-adic places. These pro-\( p \)-groups are finitely generated and admits a presentation in terms of generators and defining relations, where the relations satisfy a condition of being free in a maximal possible way with respect to a suitable filtration. Equivalently, it is proved that \( G_S \) is mild if the Poincaré series associated to the filtration satisfies certain equality (e.g. [10]). Mild pro-\( p \)-groups are of cohomological dimension 2, which is one of the main reasons for their importance also from an arithmetic point of view. Furthermore, these groups are not \( p \)-adic analytic. This should holds for \( G_S \) as a consequence of tame Fontaine-Mazur conjecture, which asserts that \( G_S \) has no infinite \( p \)-adic analytic quotients (cf. [3]).

For the field \( \mathbb{Q} \), Labute came up with the first examples of finite sets \( S \) of primes of \( \mathbb{Q} \) such that \( S \) contains no \( p \)-adic places for an odd prime \( p \) and \( \text{cd}(G_S) = 2 \). For this, the author proves that \( G_S \) is mild for a suitable set of primes \( S \) such that the associated linking diagram \( \Gamma_S(p) \) forms a non-singular circuit in the sens of [10, Definition 1.4]. Later on, A. Schmidt [17], [18] extended the result of Labute by arithmetic methods and weakened Labute’s condition on \( S \). Schmidt’s results uses a cup product criterion on the first cohomology groups that has shown its effectiveness in the problem of producing mild pro-\( p \)-groups. In [11] Forré gave simple and direct proof for the algebraic criteria for mildness. Here we use the approach based on Koch theory to study mildness [9].

The property of mildness has been extensively studied in the last decades. Examples of groups \( G_S \) which are mild are known for the field of rationals \( \mathbb{Q} \), and for imaginary quadratic fields not containing \( p \)-roots of unity with prime to \( p \) class number [20]. We can also mention the papers [8], [10], [11], [5] and [6]. Recently, in [13] Minač et al. proved that if the maximal pro-\( p \) Galois group of a field is mild, then Positselski’s and Weigel’s Koszulity conjectures hold true for such a field.

The object of this paper is to study the property mild for the group \( G_S \) in the case when \( k \) is an imaginary quadratic number field with nontrivial \( p \)-class group, where \( p \) is an odd prime number. By tracing Koch’s theory, we first give in section 2 a Koch type presentation by generators and relations for \( G_S \) (Theorem 2.3):

\[
1 \longrightarrow R \longrightarrow F \overset{\pi}{\longrightarrow} G_S \longrightarrow 1,
\]

where \( F \) is a free pro-\( p \)-group and \( R \) is the relations group. This is done for certain set of primes of \( k \) whose norms are congruent to 1 modulo \( p \), where the relations modulo the third step of the lower central series are described by linking numbers \( \tilde{l}_{*,*} \) of primes.

In section 3 we describe an arithmetical sufficient condition for mildness of \( G_S \) (Theorem 3.1). These conditions are in terms of congruences modulo \( p \) of liking numbers appearing in Theorem 2.3. Furthermore, in Corollary 3.3 we give distinguished properties of the group \( G_S \), for example we obtain that \( G_S \) is a duality group with Euler
characteristic $\chi(G_S) = 1$. We obtain in Proposition 3.5 a sufficient conditions for mildness of $G_S$ with 4 generators. The assumption of $p$-rank equals 1 is to ease computations. However, by similar reasoning, we can obtain the same results in the case of fields for which the $p$-rank of the class group is less than $|S|$ (see Remark 2.4).

As an illustration, using PARI/GP we give the following example. Let $k$ be the quadratic field $\mathbb{Q}(\sqrt{-23})$ and $p = 3$. We consider the primes $\ell_0 = 13$, $\ell_1 = 211$, $\ell_2 = 67$ and $\ell_3 = 31$. For suitable choices of the places $v_i$ above the primes $\ell_i$, we prove that $G_S$ is a mild pro-$p$-group for $S = \{v_0, v_1, v_2, v_3\}$.

**Notations.** For a pro-$p$-group $G$, we denote by $[h, g] = h^{-1}g^{-1}hg$ the commutator of $g, h \in G$. For a closed subgroup $H$ of $G$, $[H, G]$ (resp. $H^p$) denote the minimal closed subgroup containing $\{[h, g] \mid h \in H, g \in G\}$ (resp. $\{h^p \mid h \in H\}$). Then $G^{ab} = G/[G, G]$. The $i$th cohomology group with coefficients in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is denoted by $H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$. For a set $Y$, $|Y|$ denote the cardinality. For objects $x$ and $y$, $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ otherwise.

2 Koch type presentation

Let $G$ be a finitely presented pro-$p$ group and let

$$1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$$

be a minimal presentation, where $F$ is the free pro-$p$ group on the generators $x_1, \ldots, x_d$ and $R = \langle \rho_1, \ldots, \rho_r \rangle$ is the normal subgroup of $F$ generated by the elements $\rho_i$, $i = 1, \ldots, r$.

**Definition 2.1.** The minimal presentation $\langle x_1, \ldots, x_d \mid \rho_1, \ldots, \rho_r \rangle$, of the pro-$p$-group $G$ is said to be of Koch type if $r \leq d$ and the relations $\rho_i$ satisfy a congruence of the form

$$\rho_i \equiv x_1^{a_{i1}} \prod_{i \neq j} \left[x_j, x_i\right]^{a_{ij}} \text{ mod } F_3,$$

with $a_i \in \mathbb{Z}_p$, $a_{ij} \in \mathbb{F}_p$, and $F_3$ is the third step of the descending $p$-central series of $F$. The group $G$ is of Koch type if it has a presentation of Koch type.

Given a Koch type presentation of $G_S$ for a set of places $S$ of a number field $k$, one can derive conditions for which the group $G_S$ is mild. Here we consider the following setting:

- $p > 2$ an odd prime number.
• $k$ an imaginary quadratic field such that the $\mathbb{F}_p$-rank of the class group $Cl_k$ is 1.

In the following, for each place $v$ of $k$, we denote $k_v$ for the completion of $k$ at $v$, and $U_v$ is the group of units of $k_v$. Let $S$ be a finite set of primes of $k$ whose norms is congruent to 1 modulo $p$. We define the group

$$V_S(k) = \{a \in k^\times \mid a \in (k_v^\times)^p \text{ for } v \in S \text{ and } a \in U_v k_v \text{ for } v \notin S\}.$$  

We can see that $(k^\times)^p \subset V_S(k)$. Thus we can put

$$B_S(k) = (V_S(k)/(k^\times)^p)^*,$$

where $(.)^*$ means the Pontryagin dual. We have the following exact sequence

$$0 \longrightarrow E_k/p \longrightarrow V_{\emptyset}(k)/(k^\times)^p \longrightarrow Cl_k \overset{\cdot \ p}{\longrightarrow} Cl_k,$$

where $E_k$ is the group of units of $k$. We are interested in the sets $S$ of places for which $V_S(k) = (k^\times)^p$. This is intimately related to the structure of the Galois group $G_S$. More precisely, it gives information about the generators and relations rank of $G_S$.

Shafarevich’s theorem [9, Theorem 11.8], tells us that the minimal number $d(G_S)$ of generators of $G_S$ (for our setting) is given by

$$d(G_S) = \dim_{\mathbb{F}_p} H^1(G_S) = |S| + \dim_{\mathbb{F}_p}(B_S(k)). \quad (2.1)$$

Furthermore, Theorem 11.5 of [9] gives that

$$r(G_S) = \dim_{\mathbb{F}_p} H^2(G_S) \leq |S| + \dim_{\mathbb{F}_p}(B_S(k)). \quad (2.2)$$

Let $a_1 \notin S$ be a prime ideal of $k$ such that $\{[a_1](Cl_k)^p\}$ is a basis of $Cl_k/p$. Then $Cl_k[p]$ is generated by $\{[a_1^{q_1/p}]\}$, where $q_1$ denotes the order of $[a_1]$. In particular, $a_1^{q_1} = a_1 O_k$ for some $a_1 \in V_{\emptyset}(k)$. The image of $a_1(k^\times)^p$, under the homomorphism $V_{\emptyset}(k)/(k^\times)^p \to Cl_k$, is $[a_1^{q_1/p}]$, thus we conclude that

$$\{a_1(k^\times)^p\} \text{ generates } V_{\emptyset}(k)/(k^\times)^p. \quad (2.3)$$

In the following, a set $S$ of places of $k$ is said to be singular at a finite place $v_0$ if:

$$v_0 \in S \text{ and } a_1^{(|O_k|/v_0|-1)/p} \not\equiv 1 \pmod{v_0}. $$

**Proposition 2.2.** ([2]) Let $S$ be a finite set of places of $k$. Suppose that $S$ is singular at $v_0$, then $B_S(k) = \{1\}$. It follows that

1. $d(G_S) = |S|$,
2. $r(G_S) \leq |S|$.

Proof. Since $V_0(k) = a_0^G(k^\times)^p$ (see (2.3)) and $a_1 \notin (k_{v_0})^p$ by assumption, we have $a_1 \notin V_S(k)$, and hence $V_S(k)/(k^\times)^p = \{1\}$. Thus $B_S(k) = \{1\}$. The assertion for minimal number of generators and relations of $G_S$ follows from (2.1) and (2.2). □

We would like to give an explicit description of the set of generators and relations in the group $G_S$ in our setting, while assuming that $S$ is singular and disjoint from the set of $p$-adic places of $k$. For this we will need some local notations:

For any prime $v$ of $k$, we let $\pi_v$ be a uniformizer of $v$ and $Frob_v$ is the corresponding Frobenius automorphism in the maximal subextension of $k_S/k$ in which a fixed prime of $k_S$ above $v$ is unramified.

If $\Sigma$ is a set of places of $k$, we put

$$U_\Sigma := \prod_{v \not\in \Sigma} U_v \times \prod_{v \in \Sigma} \{1\}.$$  

We set $\gamma_1 = (\gamma_1,v)_v$ where $\gamma_1,v = \pi_v$ if $v = a_1$ and $\gamma_1,v = 1$ otherwise. Then $\gamma_1 U k^\times$ correspond to the class $[a_1]$ under the isomorphism $J/U k^\times \simeq Cl_k$, where $U := U_0$ and $J$ is the group of ideles of $k$. We have in particular

$$\gamma_1^{-q_1} a_1 \in U \text{ and } q_1 \equiv 0 \pmod{p}. \quad (2.4)$$

Let $h$ be the order of the non-$p$-part of $Cl_k$. Let $w \in S$, then

$$[w]^h = [a_1]_w^{l_{w,1}}, \quad l_{w,1} \in \mathbb{Z}.$$  

Thus, $w^h = a_1^{l_{w,1}}(\varpi_w)$ for some $\varpi_w \in k^\times$. The idele element in $J$ corresponding to $\varpi_w$ is given by

$$(\varpi_w)_v \in \pi_v^h U_v \times \pi_1^{-l_{w,1}} U_{a_1} \times \prod_{v \not\in \{w,a_1\}} U_v.$$  

For $v \in S$, let $\alpha_v \in U_v$ be a primitive $|(\mathcal{O}_k/v)^\times|$-th root of unity, and consider the following elements of the group $G_S$:

- let $\sigma_v$ be an element of $G_S$ with the properties:
  1. $\sigma_v$ is a lift of $Frob_v$ to $G_S$,
  2. $(\sigma_v)^h|_{k_{S,v}} = (\varpi_v, k_{S,v}/k)$,

- let $\tau_v$ be an element of $G_S$ such that
  1. $\tau_v$ is an element of the inertia group $\mathcal{T}_v$ of $v$ in $k_S/k$,
2. \((\tau_v|_{k_S^g}) = (\alpha_v, k_S^{ab}/k)\),

- let \(\tau_1\) be a lift of \((\gamma_1, k_S^{ab}/k)\) to \(G_S\).

**Theorem 2.3.** Let \(S\) be a finite set of places of \(k\). Suppose that \(S\) is singular at \(v_0\). Then \(G_S\) has a minimal presentation

\[
1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S \longrightarrow 1,
\]

where \(F\) is a free pro-\(p\)-group with generators \(\{x_v\}_{v \in (S \setminus \{v_0\}) \cup \{1\}}\) such that \(\pi(x_v) = \tau_v\) for \(v \in (S \setminus \{v_0\}) \cup \{1\}\), and \(R\) is a normal subgroup of \(F\) normally generated by \(\{\rho_v\}_{v \in S}\) of the form

\[
\rho_v = x_v^{[O_{k,v}/v]^{-1}[x_v^{-1}, y_v^{-1}]}, \quad v \in S;
\]

(2.5)

where \(y_v \in F\) such that \(\pi(y_v) = \sigma_v\) and

\[
y_v \equiv \prod_{v \in (S \setminus \{v_0\}) \cup \{1\}} x_v^{\tilde{l}_{v,v}} \pmod{[F,F]},
\]

where, for every \(v \in (S \setminus \{v_0\}) \cup \{1\}\), \(\tilde{l}_{v,v}\) is some \(p\)-adic integer.

**Proof.** Recall the following exact sequence from class field theory:

\[
0 \to V_S/(k^x)^p \to V_{\emptyset}/(k^x)^p \to U/(U)^p U_S \to (G_S)^{ab}/p \to Cl_k/p \to 0.
\]

(2.6)

It follows that the set \(C = \{\tau_1, \tau_v, v \in S\}\) is a system of generators of \(G_S\). By Proposition 2.2, a minimal system of generators has cardinality \(|S|\), thus we have to omit one element of the set \(C\) to get a minimal system of generators.

Note that by Hasse principal we have \(k^x \cap J^p = (k^x)^p\). Thus, \(U \cap J^p = U^p\). We get the following isomorphisms

\[
V/(k^x)^p \simeq V J^p / J^p = (k^x J^p \cap U) J^p / J^p \simeq (k^x J^p \cap U) U^p / U^p,
\]

where \(V = V_{\emptyset}\). By (2.4) the maps are given by

\[
a_1(k^x)^p \longrightarrow a_1 J^p = \gamma_1^{-q_1 a_1} J^p \longrightarrow \gamma_1^{-q_1 a_1} U^p.
\]

Then, the set \(\{\gamma_1^{-q_1 a_1} U^p U_S\}\) is a basis of the image of the injective homomorphism

\[
V/(k^x)^p \longrightarrow U/U^p U_S.
\]

For \(v, w \in S\) such that \(v \neq w\), there are \(p\)-adic integers \(z_{1,v}, l_{w,v}\) satisfying

\[
\gamma_1^{-q_1 a_1} \equiv \alpha_{z_{1,v}} (\mod v),
\]

(2.7)

\[
\omega_w^{-1} \equiv \alpha_{l_{w,v}} (\mod v).
\]

(2.8)
We put \( l_{w,v} = 0 \) if we have \( v = w \).

The set \( \{ \alpha_v U^p U_S \} \) forms a basis of \( U/U^p U_S \). Then we have

\[
\prod_{v \in S} \alpha_{v}^{z_{1,v}} \equiv (\gamma_{1,v}^{-q_{1}} a_{1})_{v} \pmod{U^p U_S},
\]

hence

\[
\prod_{v \in S} \alpha_{v}^{z_{1,v}} \equiv \gamma_{1}^{-q_{1}} \pmod{J^p k^\times U_S}.
\]

Then, by class field theory we obtain

\[
\prod_{v \in S} \tau_{v}^{z_{1,v}} \equiv \tau_{1}^{-q_{1}} \pmod{[G_S,G_S]}.
\]  
(2.9)

Recall that \( \gamma_{1,v} = 1 \) if \( v \neq a_1 \). Since \( \gamma_{1,v}^{-q_{1}} a_{1} = a_{1} \equiv \alpha_{v}^{z_{1,v}} \pmod{v} \) for every \( v \in S \), we have \( z_{1,v} \neq 0 \pmod{p} \) because \( S \) is singular at \( v_0 \). Thus a minimal system of generators of \( G_S \) is given by \( C_0 = \{ \tau_1, \tau_v | v \in S \setminus \{ v_0 \} \} \). In particular, using (2.9) we have

\[
\tau_{v_0} \equiv \tau_{1}^{-q_{1} z_{1,v_0}} \prod_{v \in S \setminus \{ v_0 \}} \tau_{v}^{-z_{1,v} z_{1,v_0}} \pmod{[G_S,G_S]}.
\]  
(2.10)

For any \( w \in S \) we have

\[
\varpi_w = (\varpi_w, (1)_{v \neq w}) \equiv (1, (\varpi_w^{-1})_{v \neq w}) \pmod{k^\times}
\equiv (\gamma_{1,v}^{-1})(1)_{v \notin S \setminus \{ w \}}, (\varpi_w^{-1})_{v \in S \setminus \{ w \}} \pmod{U_S J^p k^\times}
\equiv \gamma_{1,v}^{-1} \prod_{v \in S} \alpha_{v}^{j_{w,v}} \pmod{U_S J^p k^\times}.
\]

By class field theory we obtain

\[
\sigma_w^h \equiv \tau_{1}^{-l_{w,v} h^{-1}} \prod_{v \in S} \tau_{v}^{l_{w,v} h^{-1}} \pmod{[G_S,G_S]}.
\]  
(2.11)

Since \( h \in \mathbb{Z} \setminus p\mathbb{Z} \), we have from (2.11):

\[
\sigma_w \equiv \tau_{1}^{-l_{w,v} h^{-1}} \prod_{v \in S} \tau_{v}^{l_{w,v} h^{-1}} \pmod{[G_S,G_S]},
\]  
(2.12)

where \( h^{-1} \) is the inverse of \( h \) modulo \( p \). Recall that \( C_0 = \{ \tau_1, \tau_v | v \in S \setminus \{ v_0 \} \} \) is a minimal system of generators of \( G_S \). Let \( F \) be a free pro-\( p \)-group on \( d = |S| \) generators. We define the surjective homomorphism \( \pi : F \to G_S \) by \( \pi(x_v) = \tau_v \) for \( v \in (S \setminus \{ v_0 \}) \cup \{1\} \) and let \( R = \ker(\pi) \). For each \( w \in S \), there exists \( y_w \in \pi^{-1}(\sigma_w) \) such that by (2.12) we have

\[
y_w \equiv x_{1}^{l_{w,v} h^{-1}} \prod_{v \in S} x_{v}^{l_{w,v} h^{-1}} \pmod{[F,F]}.
\]
Moreover, by (2.10) we have
\[ x_{v_0} \equiv x_1^{-q_1z_1^{-1}} \prod_{v \in S \setminus \{v_0\}} x_v^{-z_1,v z_1^{-1}} \pmod{[F,F]}. \] (2.13)

Thus, we find the congruence
\[ y_w \equiv \prod_{v \in (S \setminus \{v_0\}) \cup \{1\}} x_v^{\tilde{l}_w,v} \pmod{[F,F]}, \]

where
\[ \tilde{l}_w,v = (l_{w,v} - z_{l,v}z_{1,v0}^{-1}l_{w,v_0})h^{-1}, \]
for every \( v \in (S \setminus \{v_0\}) \cup \{1\} \), such that \( z_{1,1} = q_1 \).

Let \( v \in S \), we have a natural homomorphism \( G_v \to G_S \) where \( G_v \) is the Galois group of the compositum of all \( p \)-extensions of \( k_v \). Let \( F_v \) be a free pro-\( p \)-group on 2 generators \( s_v \) and \( t_v \). Define the homomorphism \( \phi_v : F_v \to F \) by \( \phi_v(s_v) = y_v \) and \( \phi_v(t_v) = x_v \). Then we have a surjective homomorphism \( F_v \to G_v \) whose kernel is the normal subgroup \( R_v \) generated by
\[ r_v = l_v^{\Omega_v/v} - 1[l_v^{-1}, s_v^{-1}]. \] (2.14)

We have the following commutative diagram
\[
\begin{array}{cccc}
1 & \longrightarrow & R & \longrightarrow & F & \xrightarrow{\pi} & G_S & \longrightarrow & 1 \\
& & \downarrow \phi_v & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & R_v & \longrightarrow & F_v & \longrightarrow & G_v & \longrightarrow & 1
\end{array}
\]

By assumption we have \( B_S(k) = \{1\} \), the morphism
\[ \text{loc} : H^2(G_S) \longrightarrow \bigoplus_{v \in S} H^2(G_v) \]
is injective. Then \( R \) is generated by \( \{\phi_v(r_v)\}_{v \in S} \) (see [9, Theorem 6.14]). Which complete the proof of the theorem. □

**Remark 2.4.** The vanishing of the quotient \( V_S(k)/(k^\times)^p \) is an important condition in the proof of the above result. However, this is not always true. For example if \( \dim_{F_p}(Cl_k/p) > |S| \) then \( V_S(k)/(k^\times)^p \neq \{1\} \). Indeed, if \( V_S(k)/(k^\times)^p = \{1\} \) then we have an injection
\[ V_0/(k^\times)^p \longrightarrow U/(U)^p U_S \]

However, we have \( U/(U)^p U_S \cong \prod_{v \in S} U_v/(U_v)^p \) and for any \( v \in S \) we have \( \dim_{F_p}(U_v/(U_v)^p) = 1 \). Thus, \( \dim_{F_p}(V_0(k)/(k^\times)^p) = \dim_{F_p}(Cl_k/p) \leq |S| \), which is absurd by assumption.

In the following section, we use the above theorem to give sufficient conditions for mildness of the group \( G_S \).
3 Mild pro-\(p\)-groups

Let us recall what is Zassenhaus filtration for pro-\(p\) groups. Let \(G\) be such a group and put \(G_1 = G\) and \(G_n = [G_{n-1}, G]\) for \(2 \leq n \leq n\) recursively. Then \(\{G_n\}_{n \geq 1}\) is the lower central series of \(G\). Put \(G_{(n)} = \{g \in G : g - 1 \in (I_G)^n\}\) for \(n \geq 1\), where \(I_G = \text{Ker}(\mathbb{F}_p[[G]] \to \mathbb{F}_p)\) is the augmentation ideal of \(\mathbb{F}_p[[G]]\). Then \(G_{(1)} = G\) and \(\{G_{(n)}\}_{n \geq 1}\) is the Zassenhaus filtration of \(G\).

A finitely presented pro-\(p\) group \(G\) is said to be mild (with respect to the Zassenhaus filtration) when \(G\) has a presentation \(F/R \cong G\) with a system of relations which make a strongly free sequence in the graded Lie algebra \(\text{gr}(F) = \bigoplus_{n \geq 1} F_{(n)}/F_{(n+1)}\) (see [10]).

In this section we give a condition for mildness of the pro-\(p\) groups \(G_S = \text{Gal}(k_S/k)\), where \(S\) is a singular set of places of \(k\).

Let \(S = \{v_0, ..., v_{d-1}\}\) be a finite set of finite places of \(k\) such that \(|\mathcal{O}_k/v_i| \equiv 1 \pmod{p}\) for every \(i \in \{0, ..., d-1\}\). Assume that \(S\) is singular at the place \(v_0\). Let \(I \coloneqq (S \setminus \{v_0\}) \cup \{1\}\) and recall that by Theorem 2.3, \(G_S \simeq F/R\) has generators \(\{x_{v_i}\}_{v_i \in I}\) and relations \(\{\rho_{v_i}\}_{1 \leq i \leq d-1}\). For \(f \in F\) and a multi-index \((v_1v_2\cdots v_n)\) with \(v_i \in I\), we put

\[
\varepsilon_{(v_1v_2\cdots v_n),p}(f) = \varepsilon_{Z_p[[F]]} \left( \frac{\partial^n f}{\partial x_{v_1}\partial x_{v_2}\cdots\partial x_{v_n}} \right) \mod p \in \mathbb{F}_p,
\]

which is called mod \(p\) Magnus coefficient, where \(\varepsilon_{Z_p[[F]]} : Z_p[[F]] \to Z_p\) is the augmentation map, and \(\frac{\partial}{\partial x_{v_i}}\) denotes the pro-\(p\) Fox derivative which is a continuous endomorphism of \(Z_p[[F]]\) ([7 §2]).

**Theorem 3.1.** Let \(S\) be singular at \(v_0\) and of cardinality \(4 \leq d \leq 2\mathbb{Z}\). Assume that \((S \setminus \{v_0\}) \cup \{1\}\) is a circular set, i.e. there exists a bijection \(\nu : \mathbb{Z}/d\mathbb{Z} \to (S \setminus \{v_0\}) \cup \{1\}\) such that \(\nu(0) = 1\) and which satisfies the following conditions:

1. \(l_{v_0, v_0(d-2)} \equiv l_{v_0, v_0(2)} \equiv 0 \pmod{p}\) and \(z_{1, v(1)} \equiv 0 \pmod{p}\) for all \(2 \leq j \leq d - 2\).

2. \(l_{v(2i), v(2j)} \equiv 0 \pmod{p}\) for any \(i, j\).

3. \(z_{1, v(1)}l_{v_0, 1} \prod_{i=1}^{d-1} l_{v(i), v(i+1)} \not\equiv z_{1, v(d-1)}l_{v_0, 1} \prod_{i=1}^{d-1} l_{v(i), v(i-1)} \pmod{p}\).

Then \(G_S\) is a mild pro-\(p\)-group of deficiency zero and hence of cohomological dimension \(2\).

**Proof.** To establish the result we use a criterion based on the cup-product (see [6]) yields that the pro-\(p\)-group \(G_S\) is mild if the \(\mathbb{F}_p\)-vector space \(H^1(G_S)\) has a decomposition \(H^1(G_S) = U \oplus V\) with the subspaces \(U\) and \(V\) such that...
\[ U \cup V = H^2(G_S) \quad \text{and} \quad V \cup V = \{0\}, \]

where \( U \cup V \) (resp. \( V \cup V \)) denote the image of \( U \otimes V \) (resp. \( V \otimes V \)) by the cup product

\[ \cup : H^1(G_S) \times H^1(G_S) \to H^2(G_S). \]

By Theorem 2.3 above, the group \( G_S \) has a minimal presentation

\[
1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S \longrightarrow 1,
\]

which we use to define the trace map associated to \( \rho \in R \):

\[ \text{tr}_\rho : H^2(G_S) \xrightarrow{\rho^{-1}} H^1(R)^{F/R} \to \mathbb{F}_p : \psi \mapsto \text{tg}^{-1}(\psi)(\rho), \]

where \( \text{tg} \) is the transgression isomorphism. The dual group \( H^2(G_S)^{\vee} \) is generated by \( \{\text{tr}_\rho \}_{\rho \in S} \) as an \( \mathbb{F}_p \)-vector space. Let \( \{\vchi_v\}_{v \in (S \setminus \{v_0\}) \cup \{1\}} \) be the dual basis of \( H^1(G_S) \simeq H^1(F) \) such that \( \vchi_v(\pi(x_v)) = \delta_{v_1,v_2}. \) Note that \( 4 \leq d \in 2\mathbb{Z}. \) Then \( H^1(G_S) = U \oplus V, \)

\[ \text{where } U = \bigoplus_{i=0}^{(d-2)/2} \mathbb{F}_p \vchi_v(2i+1) \text{ and } V = \bigoplus_{i=0}^{(d-2)/2} \mathbb{F}_p \vchi_v(2i). \]

For \( v \in S \) and \( v_1,v_2 \in (S \setminus \{v_0\}) \cup \{1\}, \) we have

\[ \text{tr}_{\rho_v}(\vchi_v \cup \vchi_{v_2}) = -\vchi_v(\vchi_{v_2}), \]

by the basic properties of mod \( p \) Magnus coefficients (cf. e.g., [5, Theorem 2.4] and [19, Proposition 2.18]).

By (1) and (2), we obtain \( \text{tr}_{\rho_v}(\vchi_v(2i) \cup \vchi_v(2j)) = 0 \) for any \( i,j,v. \) Since the pairing

\[ H^2(G_S) \times H^2(G_S)^{\vee} \to \mathbb{F}_p \]

is non-degenerate, \( V \cup V = \{0\}. \)

Put a \( d \times d \) matrix \( A = (a_{i,j})_{0 \leq i,j \leq d-1} \) with entries in \( \mathbb{F}_p \) such that

\[
a_{i,j} = \begin{cases} 
\text{tr}_{\rho_{v(i)}}(\vchi_v(j) \cup \vchi_v(j+1)) = -\delta_{\vchi_v(j),\vchi_v(j+1)} + \delta_{\vchi_v(j),\vchi_v(j+1)} \vchi_v(j+1) & \text{if } i \neq 0, \\
\text{tr}_{\rho_{v(0)}}(\vchi_v(j) \cup \vchi_v(j+1)) = (z_1, \vchi_v(j) \vchi_v(j+1) - z_1, \vchi_v(j+1) \vchi_v(j)) & \text{if } i = 0.
\end{cases}
\]

Suppose that \( \sum_{j=0}^{d-1} c_1(\vchi_v(j) \cup \vchi_v(j+1)) = 0 \) in \( U \cup V. \) Since

\[
a_{i,j} = \begin{cases} 
\text{tr}_{\rho_{v(i)}}(\vchi_v(j) \cup \vchi_v(j+1)) & \text{if } 1 \leq i \leq d-1, \\
\text{tr}_{\rho_{v(0)}}(\vchi_v(j) \cup \vchi_v(j+1)) & \text{if } i = 0.
\end{cases}
\]
Under the conditions (1) and (3) we have

\[
A = (a_{i,j})_{i,j} = h^{-d} \begin{pmatrix}
-z_{1,v(1)}l_{v(1),1}^{-1} & -l_{v(1),v(2)} & \cdots \\
-l_{v(2),v(1)} & \ddots & \ddots \\
\vdots & \ddots & \ddots & -l_{v(d-2),v(d-1)} & -l_{v(d-1),1}
\end{pmatrix}
\]

and

\[
\det(A) = z_{1,v_0}^{-1} h^{-d} \left( z_{1,v(1)}l_{v(1),1}^{-1} \prod_{i=1}^{d-1} l_{v(i),v(i+1)} - z_{1,v(d-1)}l_{v(1),v(d-1)} \prod_{i=1}^{d-1} l_{v(i),v(i-1)} \right).
\]

By the condition (3), we obtain \( \det(A) \not\equiv 0 \pmod{p} \).

We have

\[
(0,0,\ldots,0) = (\text{tr}_{\rho_{v_0}}(0), \text{tr}_{\rho_{v(1)}}(0), \ldots, \text{tr}_{\rho_{v(d-1)}}(0)) = (c_0, c_1, \ldots, c_{d-1})^t A,
\]

where \(^tA\) is the transpose of \( A \). Since \( \{\chi_{v(j)} \cup \chi_{v(j+1)}\}_{0 \leq j \leq d-1} \) is linearly independent, then \( U \cup V = H^2(G_S) \) and Therefore \( G_S \) is a mild pro-\( p \) group. In particular, \( \text{cd}(G_S) = 2 \).

Remark 3.2. The approach of this paper computes the cup product using Koch theory of minimal presentations and \( \pmod{p} \) Magnus coefficients. We note that another approach due to A. Schmidt gives a cup-product criterion by computing local components of the cup-product (see Section 5 of [18]).

Definition 3.3. A pro-\( p \)-group \( G \) is \textbf{fab} if for every open subgroup \( H \subseteq G \) the abelianization \( H^{ab} = H/[H,H] \) is finite. We call \( G \) fabulous if it is mild and fab.

Note that Labute gives a slightly different definition of what is a fabulous pro-\( p \)-group, where the group must satisfy an additional property called \textit{quadratic} (see [11, Definition 7]).

Corollary 3.4. Under the conditions of Theorem 3.1, the pro-\( p \)-group \( G_S \) satisfies the following properties:

1. \( G_S \) is fabulous.

2. \( G_S \) is a duality group.

3. The strict cohomological dimension is \( \text{scd}(G_S) = 3 \).

4. \( G_S \) is not \( p \)-adic analytic.
5. $\chi(G_S) = 1$ the Euler characteristic of $G_S$.

Proof. For the property (1), since $S$ is disjoint from the set $S_p$ of places lying above $p$, the extension $k_S/k$ does not contain any $\mathbb{Z}_p$ extensions, thus $G_S^{ab}$ is finite, hence $G_S$ is fabulous.

The second and the third properties follows from Proposition 1.3 of [21], and (4) follows from [3, Theorem 2.7].

Let $S$ be a finite set of places of $k$ of cardinality 4 such that $S = \{v_0, v_1, v_3, v_4\}$ where each $v_i$ is lying over a prime number $\ell_i$ satisfying $\ell_i \equiv 1 \pmod{p}$.

Proposition 3.5. The group $G_S$ is a mild pro-$p$-group with 4 generators if the following conditions are satisfied:

1. The places $v_0$, $v_1$ and $v_3$ have degree one, and $\ell_2$ is inert in $k$.
2. $a_1^{\frac{4}{p} - 1} \not\equiv 1 \pmod{v_0}$.
3. $\varpi_{v_0}^{\frac{\ell_2 - 1}{p}} \equiv 1 \pmod{\ell_2}$ and $a_1^{\frac{\ell_2 - 1}{p}} \equiv 1 \pmod{\ell_2}$.
4. $a_1^{\frac{4}{p} - 1} \not\equiv 1 \pmod{v_1}$, $\varpi_{v_1}^{\frac{\ell_2 - 1}{p}} \not\equiv 1 \pmod{\ell_2}$ and $\varpi_{v_2}^{\frac{\ell_4 - 1}{p}} \not\equiv 1 \pmod{v_3}$.
5. In the $p$-Hilbert class field of $k$, $v_0$ and $v_3$ are inert, and $v_1$ is split.

Proof. Let $\nu : \mathbb{Z}/4\mathbb{Z} \to (S \setminus \{v_0\}) \cup \{1\}$ be a bijection such that $\nu(0) = 1$ and $\nu(i) = v_i$ for every $i = 1, 2, 3$. The property (2) gives that $S$ is singular at $v_0$.

By (3) we obtain $l_{v_0,v_2} \equiv 0 \pmod{p}$ and $z_{1,v_2} \equiv 0 \pmod{p}$. Further, since $\ell_2$ is inert, we have $l_{v_2,1} \equiv 0 \pmod{p}$. The place $v_1$ splits in the $p$-Hilbert class field of $k$, then $l_{v_1,1} \equiv 0 \pmod{p}$.

Thus we have

$$z_{1,v(3)}l_{v_0,1} \prod_{i=1}^{3} l_{\nu(i),\nu(i-1)} \equiv 0 \pmod{p}.$$  

Moreover, by the properties (4) and the fact that $v_0$ and $v_3$ are inert in the $p$-Hilbert class field of $k$,

$$z_{1,v(1)}l_{v_0,1} \prod_{i=1}^{3} l_{\nu(i),\nu(i+1)} \not\equiv 0 \pmod{p}.$$  

Then Theorem [3, Theorem 2.7] gives that $G_S$ is a mild pro-$p$-group.

We end this section with the following computations performed using PARI/GP [15].
Example 3.6. Let $k$ be the quadratic field $\mathbb{Q}(\sqrt{-23})$ and $p = 3$. We consider the primes $\ell_0 = 13$, $\ell_1 = 211$, $\ell_2 = 67$ and $\ell_3 = 31$. Let $\mathcal{O}_k$ be the ring of integers of $k$. We have $Cl_k/p = \langle [a_1] \rangle$ where $a_1 = 3\mathcal{O}_k + (\sqrt{-23} - 1)\mathcal{O}_k$ and $v_0 = 13\mathcal{O}_k + (\sqrt{-23} - 4)\mathcal{O}_k$ a prime ideal over $\ell_0$. We set $v_1 = \varpi_{v_1}\mathcal{O}_k$ a prime ideal above $\ell_1$ such that $\varpi_{v_1} = -2 + 3\sqrt{-23}$ and we put $v_2 = \ell_2\mathcal{O}_k$. We have $a_1 = -2 - \sqrt{-23}$ such that $a_1^{v_1} = a_1\mathcal{O}_k$ and we obtain $a_1^{v_0} \equiv 9 \pmod{v_0}$, $a_1^{v_1} \equiv 1 \pmod{\ell_2}$, $a_1^{v_2} \equiv 14 \pmod{v_1}$. Moreover, $\varpi_{v_0} \equiv 1 \pmod{\ell_2}$, $\varpi_{v_1} \equiv 37 \pmod{\ell_2}$ and $\varpi_{v_2} \equiv 5 \pmod{v_3}$, where $v_3 = 31\mathcal{O}_k + (\sqrt{-23} - 15)\mathcal{O}_k$ and $\varpi_{v_3} = \ell_2$. Then Proposition 3.5 gives that $G_S$ is mild for $S = \{v_0, v_1, v_2, v_3\}$, hence it is of cohomological dimension 2.

Further comments
If the linking numbers $\tilde{\ell}_{s,s}$ in Theorem 2.3 all vanishes modulo $p$, then $F_{(3)}$ contains the relations modulo $R$. Thus the cup product is trivial. To study fabulous and mild pro-$p$-groups we need to compute relations modulo $F_{(4)}$. Examples are known for the field of rationals $\mathbb{Q}$ by the work of Vogel, Gärtner and Maire (e.g. [19], [5], [12]). It would be of interest to extend these results to imaginary quadratic fields with non trivial $p$-class group.

Acknowledgements. The authors thank Yasushi Mizusawa for reading an earlier version of this paper and for his valuable comments and suggestions. We also thank Christian Maire for his interest in this work.

References

[1] M.R. Bush, and J. Labute. Mild pro-$p$-groups with 4 generators. Journal of Algebra 308.2 (2007): 828-839.
[2] A. El Habibi and Y. Mizusawa, On pro-$p$-extensions of number fields with restricted ramification over intermediate $\mathbb{Z}_p$-extensions, J. Number Theory, 231, February (2022), Pages 214–238.
[3] J.-M. Fontaine, B. Mazur, Geometric Galois representations. In: Elliptic Curves, Modular Forms and Fermat’s Last Theorem, edited by J. Coates, and S.T. Yau. International Press, Boston (1995).
[4] P. Forré, Strongly free sequences and pro-$p$-groups of cohomological dimension 2, Journal für die Reine und Angewandte Mathematik (2011) (658).
[5] J. Gärtner, Rédei symbols and arithmetical mild pro-2-groups, Ann. Math. Qué. 38 (2014), no. 1, 13–36.
[6] J. Gärtner, Higher Massey products in the cohomology of mild pro-$p$-groups, J. Algebra 422 (2015), 788–820.
[7] Y. Ihara, On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. Invent. Math. 86 (1986), no. 3, 427–459.

[8] H. Koch, Uber Pro-$p$-Gruppen der kohomologischen Dimension 2, Math. Nachr. 78, 285-289 (1977)

[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 Angew. Math. 596 (2006), 155–182.

[11] J. Labute, Fabulous pro-$p$-groups. Ann. Sci. Math. Québec 32 (2008): 189-197.

[12] C. Maire, Some examples of fab and mild pro-$p$-groups with trivial cup-product. Kyushu J. Math. 68(2) (2014), 359–376.

[13] J. Minač, F. Pasini, C. Quadrelli, N. D. Tân, Mild pro-$p$ groups and the Koszulity conjectures. arXiv preprint arXiv:2106.03675 (2021).

[14] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields, Second edition, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, (2008).

[15] The PARI Group, PARI/GP version 2.7.4, Univ. Bordeaux, (2015). http://pari.math.u-bordeaux.fr/

[16] A. Schmidt, Circular sets of prime numbers and $p$-extensions of the rationals. Journal für die reine und angewandte Mathematik. (2006) 115–30.

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

[18] A. Schmidt, Über pro-$p$-fundamentalgruppen markierter arithmetischer kurven, J. reine u. ang. Math. 640 (2010), 203–235.

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

[20] D. Vogel, Circular sets of primes of imaginary quadratic number fields, der Forschergruppe Algebraische Zykel und L-Funktionen Regensburg/ Leipzig Nr. 5, (2006).

[21] K. Wingberg, Arithmetical Koch groups. (2007) preprint.

ZAKARIAE BOUAZZAOUI
Department of Mathematics, Faculty of Sciences of Meknès, Morocco.
z.bouazzaoui@edu.umi.ac.ma

ABDELAZIZ EL HABI BII
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
a.elhabibi@ump.ac.ma