p-EXTENSIONS WITH RESTRICTED RAMIFICATION – THE MIXED CASE

DENIS VOGEL

Abstract. Let p be an odd prime number, k a number field and S a set of primes of k containing some, but not all primes of k above p. We study under which conditions $G_S(k)(p)$ is a mild pro-p-group of deficiency one, and apply our results to the case of imaginary quadratic number fields.

1. Introduction

Let k be a number field, p an odd prime number and S a finite set of primes of k. The pro-p-group $G_S(k)(p) = \mathrm{Gal}(k_S(p)/k)$, i.e. the Galois group of the maximal p-extension of k unramified outside S contains interesting information on the arithmetic of k. Let S_p denote the set of primes of k above p. There are three cases that have to be distinguished:

- the wild case: $S_p \subset S$,
- the tame case: $S \cap S_p = \varnothing$,
- the mixed case: $\varnothing \neq S_p \cap S \subsetneqq S_p$.

In the wild case, it is known that $G_S(k)(p)$ is of cohomological dimension less or equal to 2, and it is often a duality group, see [NSW], Ch. X, §7. The strict cohomological dimension of $G_S(k)(p)$ is conjecturally 2 (Leopoldt's conjecture). In the tame case, only little had been known on the structure of $G_S(k)(p)$ until recently. Labute([L]) showed that pro-p-groups whose presentation in terms of generators and relations is of a certain type, so-called mild pro-p-groups, are of cohomological dimension 2. Then he used results of Koch to show that $G_S(\mathbb{Q})(p)$ is a mild pro-p-group if S is a strictly circular set of prime numbers. In [V], Labute's techniques were applied to the case where k is an imaginary quadratic number field. Schmidt([S1],[S2]) extended the results of Labute by arithmetic methods and could show that, under some conditions on k and p, for any given finite set S' of primes of k of norm $\equiv 1 \mod p$, there exists a finite set $S \supset S'$ of primes of k of norm $\equiv 1$ mod p, such that $G_S(k)(p)$ is mild. In the tame case, if the group $G_S(k)(p)$ is mild, then it is a duality group of strict cohomological dimension 3. The mixed case has been studied in papers of Wingberg([W]) and Maire([M]) using the theory of elliptic curves and Iwasawa theory. In particular it is shown that if K/k is an abelian extension of an imaginary quadratic number field and S is a non-empty subset of $S_p(K)$ stable under $\mathrm{Gal}(K/k)$, then the cohomological dimension of $G_S(K)(p)$ is less or equal to 2, see [M], Prop. 3.5.

Date: July 18, 2007.

The objective of this paper is the study of the mixed case, making use of Labute's results on mild groups. In §2 we study under which conditions the group $G_S(k)(p)$ is a mild pro-p-group of deficiency one. In §3 the result is applied to the following situation. Let k be an imaginary quadratic number field whose class number is not divisible by p, and assume furthermore that p splits in k, $p\mathcal{O}_k = \mathfrak{p}\bar{\mathfrak{p}}$. Let S' be a set of primes of k of norm $\equiv 1 \mod p$, and let $S = S' \cup \{\mathfrak{p}\}$. We will prove criterions for $G_S(k)(p)$ to be a mild pro-p-group and hence, of cohomological dimension 2. Explicit examples will be given as well.

I would like to thank Alexander Schmidt and Kay Wingberg for interesting discussions on the subject and valuable suggestions.

2. Mild pro-p-groups of deficiency one in the mixed case

Let p be an odd prime number and let k be a number field. For a prime $\mathfrak{q}$ of k, let $k_\mathfrak{q}$ denote the completion of k with respect to $\mathfrak{q}$ and $U_\mathfrak{q}$ its group of units. We put

$$n_\mathfrak{q} = \dim_{\mathbb{F}_p} U_\mathfrak{q}/U_\mathfrak{q}^p.$$

Let S be a finite set of primes of k. Let $\text{Б}_S(k)$ denote the dual of the Kummer group

$$V_S(k) = \{a \in k^\times \mid a \in k_\mathfrak{q}^{\times p} \text{ for } \mathfrak{q} \in S \text{ and } a \in U_\mathfrak{q} k_\mathfrak{q}^{\times p} \text{ for } \mathfrak{q} \notin S\}.$$

We remark that we have an exact sequence

$$(1) \qquad 0 \longrightarrow \mathcal{O}_k^\times/p \longrightarrow V_\varnothing(k) \longrightarrow {}_p\,\mathrm{Cl}(k) \longrightarrow 0,$$

and for each subset $T \subset S$ we have an exact sequence

$$(2) \qquad 0 \longrightarrow V_T(k) \longrightarrow V_\varnothing(k) \longrightarrow \textstyle\prod_{\mathfrak{q}\in T} U_\mathfrak{q}/U_\mathfrak{q}^p,$$

see [K], §11.3. We let $h(k)$ denote the class number of k, and we set

$$\delta_\mathfrak{q} = \begin{cases} 1 & \text{if } \mu_p \subset k_\mathfrak{q}, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.1. *We say that the triple (k, S, p) has the property $(*)$ if the following holds:*

- $p \nmid h(k)$,
- $\delta_\mathfrak{q} = 1$ *for* $\mathfrak{q} \in S, \mathfrak{q} \notin S_p$,
- $\delta_\mathfrak{q} = 0$ *for* $\mathfrak{q} \in S \cap S_p$,
- $\text{Б}_S(k) = 0$,
- $\sum_{\mathfrak{q}\in S\cap S_p} [k_\mathfrak{q} : \mathbb{Q}_p] = r$, *where $r = r_1 + r_2$ is the number of archimedean primes of k.*

We remark that in this case $\mu_p \not\subset k$ and

$$n_\mathfrak{q} = \begin{cases} 1 & \text{if } \mathfrak{q} \in S, \mathfrak{q} \notin S_p, \\ [k_\mathfrak{p} : \mathbb{Q}_p] & \text{if } \mathfrak{q} \in S \cap S_p. \end{cases}$$

We denote the maximal p-extension of k unramified outside S by $k_S(p)$, and we put $G_S(k)(p) = G(k_S(p)/k)$. For $\mathfrak{q} \in S$, let $\{\alpha_{\mathfrak{q},1}, \ldots, \alpha_{\mathfrak{q},n_\mathfrak{q}}\}$ be a basis of the $\mathbb{F}_p$-vector space $U_\mathfrak{q}/U_\mathfrak{q}^p$, and let $\pi_\mathfrak{q}$ be a uniformizer of $k_\mathfrak{q}$. Let $\mathfrak{Q}$ be an extension of $\mathfrak{q}$ to $k_S(p)$. We let $\sigma_\mathfrak{q}$ be an element of $G_S(k)(p)$ with the following properties:

(i) $\sigma_{\mathfrak{q}}$ is a lift of the Frobenius automorphism of $\mathfrak{Q}$;

(ii) the restriction of $\sigma_{\mathfrak{q}}$ to the maximal abelian subextension $\tilde{k}/k$ of $k_S(p)/k$ is equal to $(\hat{\pi}_{\mathfrak{q}}, \tilde{k}/k)$, where $\hat{\pi}_{\mathfrak{q}}$ denotes the idèle whose $\mathfrak{q}$-component equals $\pi_{\mathfrak{q}}$ and all other components are 1.

For $i = 1, \ldots, n_{\mathfrak{q}}$, let $\tau_{\mathfrak{q},i}$ denote an element of $G_S(p)$ such that

(i) $\tau_{\mathfrak{q},i}$ is an element of the inertia group $T_{\mathfrak{Q}}$ of $\mathfrak{Q}$ in $k_S(p)/k$;

(ii) the restriction of $\tau_{\mathfrak{q},i}$ to $\tilde{k}/k$ equals $(\hat{\alpha}_{\mathfrak{q},i}, \tilde{k}/k)$, where $\hat{\alpha}_{\mathfrak{q},i}$ denotes the idèle whose $\mathfrak{q}$-component equals $\alpha_{\mathfrak{q},i}$ and all other components are equal to 1.

We set

$$h^i(G_S(k)(p)) = \dim_{\mathbb{F}_p}(H^i(G_S(k)(p), \mathbb{Z}/p\mathbb{Z}), \qquad i = 1, 2.$$

We say that a finitely presented pro-p-group G is of *deficiency one* if $h^1(G) - h^2(G) = 1$.

Proposition 2.2. *Assume that the triple (k, S, p) satisfies the property $(*)$. Let $S \setminus S_p = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$. Then*

$$h^1(G_S(k)(p)) = 1 + n$$

and

$$h^2(G_S(k)(p)) \leq n.$$

If $Б_{S\cap S_p}(k) = 0$, then the group $G_S(k)(p)$ has a presentation $G_S(k)(p) = F/R$ where F is the free pro-p-group on generators $x_1, \ldots, x_{n+1}$, and R is generated as a normal subgroup of F by relations $r_1, \ldots, r_n$ which are given modulo F_3 by

$$r_i \equiv x_i^{\mathrm{N}(\mathfrak{q}_i)-1} \prod_{\substack{j=1\\ j\neq i}}^{n+1} [x_i, x_j]^{a_{ij}} \mod F_3,\ i = 1, \ldots, n.$$

Here F_3 denotes the third step of the descending p-central series of F.

Proof. Since (k, S, p) satisfies $(*)$, we have by [NSW], Thm. 8.7.11,

$$\begin{aligned} h^1(G_S(k)(p)) &= 1 + \sum_{\mathfrak{q}\in S} \delta_{\mathfrak{q}} + \dim_{\mathbb{F}_p} Б_S(k) + \sum_{i=1}^{m} [k_{\mathfrak{p}_i} : \mathbb{Q}_p] - r \\ &= 1 + n \end{aligned}$$

and

$$h^2(G_S(k)(p)) \leq \sum_{\mathfrak{q}\in S} \delta_{\mathfrak{q}} + \dim_{\mathbb{F}_p} Б_S(k) = n$$

An explicit construction of a presentation of $G_S(k)(p)$ in terms of generators and relations is carried out in [K],§11.4. We sketch it here. The set of $n + r$ automorphisms $\mathcal{M} = \{\tau_{\mathfrak{q},i} \mid \mathfrak{q} \in S, i = 1, \ldots, n_{\mathfrak{q}}\}$ constitutes a system of generators of $G_S(k)(p)$ which is not minimal unless $r = 1$. In order obtain a minimal generating set, we have to remove $r-1$ elements from the above set. Which generators can be omitted is determined by the following method: By construction, the set $\mathcal{N} = \{\alpha_{\mathfrak{q},i} \mid \mathfrak{q} \in S, i = 1, \ldots, n_{\mathfrak{q}}\}$ is a basis of the $\mathbb{F}_p$-vector space $\prod_{\mathfrak{q}\in S} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. Let $\epsilon_1, \ldots, \epsilon_{r-1}$ be a system of fundamental units of k. Since $Б_S(k) = 0$, the elements $\epsilon_1, \ldots, \epsilon_{r-1}$ are linearly independent in

$\prod_{\mathfrak{q}\in S} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. We have to omit elements from $\mathcal{N}$ such that the remaining elements, together with $\epsilon_1,\dots,\epsilon_{r-1}$, form a basis of $\prod_{\mathfrak{q}\in S} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. In this way, we arrive at a subset $\mathcal{N}_0 \subset \mathcal{N}$ of cardinality $n+1$. A minimal system of generators of $G_S(k)(p)$ is then given by the subset $\mathcal{M}_0 \subset \mathcal{M}$ corresponding to $\mathcal{N}_0$.

Assume that $Б_{S\cap S_p}(k) = 0$. Then $\epsilon_1,\dots,\epsilon_{r-1}$ are linearly independent in the $r-$ dimensional $\mathbb{F}_p$-vector space $\prod_{\mathfrak{q}\in S\cap S_p} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. This implies that there exists a prime $\mathfrak{p} \in S\cap S_p$ and $k \in \{1,\dots,n_{\mathfrak{p}}\}$ such that $\{\epsilon_1,\dots,\epsilon_{r-1},\alpha_{\mathfrak{p},k}\}$ is a basis of $\prod_{\mathfrak{q}\in S\cap S_p} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. Then $\{\epsilon_1,\dots,\epsilon_{r-1},\alpha_{\mathfrak{p},k},\alpha_{q_1,1},\dots,\alpha_{\mathfrak{q}_n,1}\}$ is a basis of $\prod_{\mathfrak{q}\in S} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. Therefore $\{\tau_{\mathfrak{q}_1,1},\dots,\tau_{\mathfrak{q}_n,1},\tau_{\mathfrak{p},k}\}$ is a minimal system of generators of $G_S(k)(p)$. Let F be the free pro-p-group on generators $x_1,\dots,x_{n+1}$. We define a presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\psi} G_S(k)(p) \longrightarrow 1$$

by $\psi(x_i) = \tau_{\mathfrak{q}_i,1}, i = 1,\dots,n$, $\psi(x_{n+1}) = \tau_{\mathfrak{p},k}$. Let y_i be a preimage of $\sigma_{\mathfrak{q}_i}$ for $i = 1,\dots,n$. Then

$$y_i \equiv \prod_{\substack{j=1\\ j\neq i}}^{n+1} x_j^{a_{ij}} \mod F_2.$$

for $a_{ij} \in \mathbb{Z}/p\mathbb{Z}$. The relation subgroup R is generated as a normal subgroup of F by the relations

$$r_i = x_i^{\mathrm{N}(\mathfrak{q}_i)-1}[x_i^{-1}, y_i^{-1}], \quad i = 1,\dots,n,$$

We obtain

$$r_i \equiv x_i^{\mathrm{N}(\mathfrak{q}_i)-1}[x_i,y_i] \equiv x_i^{\mathrm{N}(\mathfrak{q}_i)-1}[x_i, \prod_{\substack{j=1\\ j\neq i}}^{n+1} x_j^{a_{ij}}] \equiv x_i^{\mathrm{N}(\mathfrak{q}_i)-1}\prod_{\substack{j=1\\ j\neq i}}^{n+1}[x_i,x_j]^{a_{ij}} \mod F_3,$$

which finishes the proof. □

By applying Thm. 3.10, Thm. 3.18 and Thm. 3.19 of [L], we immediately obtain:

Theorem 2.3. *Let p be an odd prime number, k a number field and S a set of primes of K. Assume that (k,S,p) satisfies $(*)$ and $Б_{S\cap S_p}(k) = 0$. Assume that a presentation of $G_S(k)(p)$ as obtained in 2.2 is given: $G_S(k)(p) = F/R$, where F is the free pro-p-group on generators $x_1,\dots,x_{n+1}$, $n = \#(S\setminus S_p)$, R is the normal subgroup of F generated by relations $r_1,\dots,r_n$ which satisfy a congruence of the form*

$$r_i \equiv x_i^{pa_i}\prod_{\substack{j=1\\ j\neq i}}^{n+1}[x_i,x_j]^{a_{ij}} \mod F_3,\ i = 1,\dots,n.$$

with $a_i, a_{ij} \in \mathbb{Z}/p\mathbb{Z}$. Assume that one of the following conditions is fulfilled:

(i) *$a_{i,n+1} \neq 0$ for $1 \le i \le n$*

(ii) *$a_{n,n+1} \neq 0$ and $a_{i,n} \neq 0$ for $i < n$.*

Then $G_S(k)(p)$ is a mild pro-p-group of deficiency one. In particular, we have $\operatorname{cd} G_S(k)(p) = 2$.

An interesting example in which (k, S, p) fulfills $(*)$ and $\text{Б}_{S\cap S_p}(k) = 0$ can be obtained if k is an imaginary quadratic number field. This case will be studied in more detail in §3. Here we are going to point out another situation in which the above conditions are fulfilled.

Proposition 2.4. *Let p be a prime and k a CM-field with maximal real subfield k^+ such that*

- *p is inert in $k^+/\mathbb{Q}$,*
- *p splits in k/k^+, $p\mathcal{O}_k = \mathfrak{p}\bar{\mathfrak{p}}$,*
- *$\delta_\mathfrak{p} = 0$,*
- *$p \nmid h(k)$,*

and one of the following two conditions holds:

(i) *$p \nmid h(k(\mu_p))$,*
(ii) *$p \nmid h(k^+(\mu_p))$ and $p \nmid (\mathcal{O}_k^\times : \mathcal{O}_{k^+}^\times)$*

If S' is any set of primes of k of norm $\equiv 1 \mod p$ and $S = S' \cup \{\mathfrak{p}\}$, then (k, S, p) satisfies $(*)$, and $\text{Б}_{S\cap S_p}(k) = \text{Б}_{\{\mathfrak{p}\}}(k) = 0$.

Proof. By our assumptions, $[k_\mathfrak{p} : \mathbb{Q}_p] = [k : \mathbb{Q}]/2 = r$. Since $\text{Б}_S(K) \subset \text{Б}_{\{\mathfrak{p}\}}(K)$ it remains to show that $\text{Б}_{\{\mathfrak{p}\}}(K) = 0$. By virtue of the exact sequences (1) and (2), this is equivalent to the injectivity of the map

$$\mathcal{O}_k^\times/p \to U_{k_\mathfrak{p}}/U_{k_\mathfrak{p}}^p.$$

Let us assume (i). Suppose $x \in \mathcal{O}_k^\times/p$ is a non-trivial element of the kernel of this map. Then x is contained in the kernel of

$$\mathcal{O}_k^\times/p \to U_{k_\mathfrak{p}}/U_{k_\mathfrak{p}}^p \times U_{k_{\bar{\mathfrak{p}}}}/U_{k_{\bar{\mathfrak{p}}}}^p.$$

as well. Therefore $k(\sqrt[p]{x})/k$ is a non-trivial unramified extension. By Kummer theory, the abelian extension $k(\mu_p, \sqrt[p]{x})/k(\mu_p)$ is unramified of degree p, contradicting (i). Now we assume that (ii) is fulfilled. Since $p \nmid (\mathcal{O}_k^\times : \mathcal{O}_{k^+}^\times)$ and p splits in k/k^+ we have a commutative diagram

$$\begin{tikzcd}
\mathcal{O}_k^\times/p \arrow[r] & U_{k_\mathfrak{p}}/U_{k_\mathfrak{p}}^p \\
\mathcal{O}_{k^+}^\times/p \arrow[r] \arrow[u] & U_{k_p^+}/U_{k_p^+}^p \arrow[u]
\end{tikzcd}$$

in which the vertical maps are isomorphisms. Thus it suffices to show the injectivity of the map $\mathcal{O}_{k^+}^\times/p \to U_{k_p^+}/U_{k_p^+}^p$. This is proved in the same way as in case (i). □

Example 2.5. *Let $k = \mathbb{Q}(\sqrt{3}, \sqrt{-7})$ and $p = 5$. Computations with the computer algebra system MAGMA(*[MAG]*) show that the assumptions of Prop.2.4 are fulfilled.*

3. The case of imaginary quadratic number fields

Let p be an odd prime number and k an imaginary quadratic number field whose class number is not divisible by p, and which is different from $\mathbb{Q}(\sqrt{-3})$ if $p = 3$. Assume furthermore that p splits in k, $p\mathcal{O}_k = \mathfrak{p}\bar{\mathfrak{p}}$. Let $S' =$

$\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ be a set of primes of k whose norm is congruent to 1 mod p. Put $S = S' \cup \{\mathfrak{p}\}$.

Proposition 3.1. *The triple (k, S, p) has property $(*)$, and* $Б_{S\cap S_p}(k) = 0$.

Proof. It suffices to show that $Б_{S\cap S_p}(k) = 0$. We have

$$V_\varnothing(k) \cong \mathcal{O}_k^\times/p = 0.$$

The result follows since $V_{S\cap S_p}(k) \subset V_\varnothing(k)$. □

In the above situation, the set of automorphisms $\{\tau_{\mathfrak{q}_1,1}, \ldots, \tau_{\mathfrak{q}_n,1}, \tau_{\mathfrak{p},1}\}$ constructed in §2 is a minimal system of generators of $G_S(k)(p)$. Let I_k denote the idèle group of k, and for a subset T of S let U_T be the subgroup of I_k consisting of those idèles whose components for $\mathfrak{q} \in T$ are 1 and for $\mathfrak{q} \notin T$ are units. We remark that for each subset T of S we have isomorphisms

$$H_1(G_T(p), \mathbb{Z}/p\mathbb{Z}) \cong I_k/(U_T I_k^p k^\times) \cong U_\varnothing/U_T U_\varnothing^p \cong \prod_{\mathfrak{q}\in T} U_\mathfrak{q}/U_\mathfrak{q}^p \cong (\mathbb{Z}/p\mathbb{Z})^{\#T},$$

see [K],§11.3. For the following considerations we set $\mathfrak{q}_{n+1} = \mathfrak{p}$. We make the same definition as in [V].

Definition 3.2. *For two primes $\mathfrak{q}_i$, $\mathfrak{q}_j \in S$, the* linking number $\ell_{ij} \in \mathbb{Z}/p\mathbb{Z}$ *of $\mathfrak{q}_i$ and $\mathfrak{q}_j$ is defined by the formula*

$$\sigma_{\mathfrak{q}_i} \equiv \tau_{\mathfrak{q}_j}^{\ell_{ij}} \mod G_{\{\mathfrak{q}_j\}}(p)^p$$

where, by abuse of notation, $\sigma_{\mathfrak{q}_i}$ and $\tau_{\mathfrak{q}_j}$, respectively, denote the images of $\sigma_{\mathfrak{q}_i} \in G_S(k)(p)$ and $\tau_{\mathfrak{q}_j} \in G_S(k)(p)$, respectively, in $G_{\{\mathfrak{q}_j\}}(p)$.

In other words, ℓ_{ij} is the image of the Frobenius automorphism $\sigma_{\mathfrak{q}_i} \in G_S(k)(p)$ in $H_1(G_{\{\mathfrak{q}_j\}}(p), \mathbb{Z}/p\mathbb{Z})$ which we identify with $\mathbb{Z}/p\mathbb{Z}$ by means of its generator $\tau_{\mathfrak{q}_j}$. Note that $\ell_{ii} = 0$ for all $i = 1, \ldots, n$. The linking number ℓ_{ij} is independent of the choice of the uniformizer $\pi_{\mathfrak{q}_i}$ of $k_{\mathfrak{q}_i}$ (this follows from the above isomorphism for the case $T = \{\mathfrak{q}_j\}$), but it depends on the choice of $\alpha_{\mathfrak{q}_j}$. If $\alpha_{\mathfrak{q}_j}$ would be replaced by $\alpha_{\mathfrak{q}_j}^s$, where s is prime to p, then ℓ_{ij} would be multiplied by s. The defining equation of the linking number ℓ_{ij} is equivalent to

$$\hat{\pi}_{\mathfrak{q}_i} \equiv \hat{\alpha}_{\mathfrak{q}_j}^{\ell_{ij}} \mod U_{\{\mathfrak{q}_j\}} I_k^p k^\times.$$

Proposition 3.3. *Under the above assumptions, we have*

$$h^1(G_S(k)(p)) = n + 1$$

and

$$h^2(G_S(k)(p)) \le n.$$

The group $G_S(k)(p)$ has a presentation $G_S(k)(p) = F/R$ where F is the free pro-p-group on generators $x_1, \ldots, x_{n+1}$, and R is generated as a normal subgroup of F by relations $r_1, \ldots, r_n$ which are given modulo F_3 by

$$r_i \equiv x_i^{\mathrm{N}(\mathfrak{q}_i)-1} \prod_{\substack{j=1\\ j\ne i}}^{n+1} [x_i, x_j]^{\ell_{ij}} \mod F_3,\ i = 1, \ldots, n.$$

Proof. This is immediate from the construction of the presentation carried out in the proof of 2.2. □

Theorem 2.3 now implies

Theorem 3.4. *Let p be an odd prime number, k an imaginary quadratic number field whose class number is not divisible by p, and which is different from $\mathbb{Q}(\sqrt{-3})$ if $p = 3$. Assume furthermore that p splits in k, $p\mathcal{O}_k = \mathfrak{p}\bar{\mathfrak{p}}$. Let $S' = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ be a set of primes of k whose norm is congruent to 1 mod p. Put $\mathfrak{q}_{n+1} = \mathfrak{p}$ and $S = S' \cup \{\mathfrak{q}_{n+1}\}$. Assume that one of the following conditions is fulfilled:*

(i) $\ell_{i,n+1} \neq 0$ *for* $1 \leq i \leq n$.

(ii) $\ell_{n,n+1} \neq 0$ *and* $\ell_{i,n} \neq 0$ *for* $i < n$.

Then $G_S(k)(p)$ is a mild pro-p-group of deficiency one. In particular, $G_S(k)(p)$ is of cohomological dimension 2.

Corollary 3.5. *Let p be an odd prime number, k an imaginary quadratic number field whose class number is not divisible by p, and which is different from $\mathbb{Q}(\sqrt{-3})$ if $p = 3$. Assume furthermore that p splits in k, $p\mathcal{O}_k = \mathfrak{p}\bar{\mathfrak{p}}$. Let $q_1, \dots, q_n$ be prime numbers which are inert $k/\mathbb{Q}$ with $q_i \equiv 1 \mod p$, $q_i \not\equiv 1 \mod p^2$ for $i = 1, \dots, n$. Put $S = \{(q_1), \dots, (q_n), \mathfrak{p}\}$. Then $G_S(k)(p)$ is a mild pro-p-group.*

Proof. We set $\mathfrak{q}_i = (q_i)$ for $1 \leq i \leq n$, $\mathfrak{q}_{n+1} = \mathfrak{p}$. We will verify condition (i) of 3.4, i.e. we will show that $\ell_{i,n+1} \neq 0$ for $1 \leq i \leq n$. For $1 \leq i \leq n$, $\pi_{\mathfrak{q}_i} = q_i$ is a uniformizer of $k_{\mathfrak{q}_i}$, and an element of $U_\mathfrak{q}$ for all primes $\mathfrak{q} \neq \mathfrak{q}_i$ of k. Hence, the idèle $\hat{\pi}_{\mathfrak{q}_i}$, when considered modulo $U_{\{\mathfrak{q}_{n+1}\}} I_k^p k^\times$, is equivalent to the idèle whose $\mathfrak{q}$-component is equal to 1 for $\mathfrak{q} \neq \mathfrak{q}_{n+1}$ and equal to q_i^{-1} for $\mathfrak{q} = \mathfrak{q}_{n+1}$. Since we are only interested in the non-vanishing of $\ell_{i,n+1}$ we may assume without loss of generality that $\alpha_{n+1} = 1 + p$. In particular, $\ell_{i,n+1}$ is given by

$$q_i \equiv (1+p)^{-\ell_{i,n+1}} \mod U_\mathfrak{p}^p.$$

By our assumptions, $\ell_{i,n+1} \neq 0$ □

Example 3.6. *Let $k = \mathbb{Q}(\sqrt{-5})$, $p = 3$, $S = \{(13), (31), (3, 1 + \sqrt{-5})\}$. Then $G_S(k)(p)$ is a mild pro-p-group.*

References

[K] Koch, H.: *Galoissche Theorie der p-Erweiterungen.* Deutscher Verlag der Wiss., 1970 (English translation Berlin 2002)

[L] Labute, J.: *Mild Pro-p-Groups and Galois Groups of p-Extensions of* $\mathbb{Q}$. J. Reine Angew. Math. 596 (2006), 155-182

[M] Maire, C.: *Sur la dimension cohomologique des pro-p-extensions de corps de nombres.* J. Theor. Nombres Bordx. 17, No. 2 (2005), 575-606

[MAG] Bosma, W., Cannon, J.J., Playoust, C.: *The Magma Algebra System I: The User Language.* J. Symbolic Comput. 24 (1997), 235-265.

[NSW] Neukirch, J., Schmidt, A., Wingberg, K.: *Cohomology of number fields.* Springer 2000

[S1] Schmidt, A.: *Circular sets of prime numbers and p-extensions of the rationals.* J. Reine Angew. Math. 596 (2006), 115-130

[S2] Schmidt, A.: *Rings of integers of type* $K(\pi, 1)$. Preprints der Forschergruppe Algebraische Zykel und L-Funktionen Regensburg/Leipzig Nr. 7, 2007

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

[W] Wingberg, K.: *Galois groups of number fields generated by torsion points of elliptic curves.* Nagoya Math. J. 104 (1986), 43-53

Denis Vogel
NWF I - Mathematik, Universität Regensburg
93040 Regensburg
Deutschland
email: denis.vogel@mathematik.uni-regensburg.de