Arithmetical Koch Groups

by Kay Wingberg at Heidelberg

Version: November 23, 2007

Let k be a number field, p a prime number and S a finite set of primes of k. The Galois group $G(k_S(p)|k)$ of the maximal p-extension of k which is unramified outside S is an important object in order to study the arithmetic of k. If all primes dividing p are in S, then a lot is known about the structure of $G(k_S(p)|k)$, in particular, it is of cohomological dimension less or equal to 2 (if $p = 2$ one has to require that k is totally imaginary).

If S is disjoint to the set S_p of primes above p, the group $G(k_S(p)|k)$ is very mysterious. By a famous theorem of Golod and Šafarevič, it is in general infinite, but on the other hand it is a so-called *fab* pro-p-group, i.e. the maximal abelian quotient of every open subgroup of $G(k_S(p)|k)$ is finite. Furthermore, nothing was known on the cohomological dimension of $G(k_S(p)|k)$ so far.

Recently, J. Labute [2] showed that pro-p-groups who have a presentation in terms of generators and relations of a certain type, so-called mild pro-p-groups, are of cohomological dimension equal to 2. A special case are pro-p-groups of *Koch type*, with certain further conditions on the relations (the linking diagram of the considered group has to be a non-singular circuit, see the definitions in the next section).

If $k = \mathbb{Q}$, then the group $G(\mathbb{Q}_S(p)|\mathbb{Q})$, $S \cap S_p = \varnothing$, is of Koch type, see H. Koch [1]. Labute used these results on the relation structure of $G(\mathbb{Q}_S(p)|\mathbb{Q})$ and ended up with a criterion on the set S for the group $G(\mathbb{Q}_S(p)|\mathbb{Q})$ to be of cohomological dimension 2. A. Schmidt [5] extended the result of Labute by arithmetic methods and weakened Labute's condition on S.

There is another case when the Galois group $G(k_S(p)|k)$, $S \cap S_p = \varnothing$, is of Koch type: k has to be an imaginary quadratic number field not containing the p-th roots of unity and its class number is not divisible by p. Therefore, if the linking diagram of $G(k_S(p)|k)$ is a non-singular circuit, then this group is of cohomological dimension equal to 2, see the paper of D. Vogel [6]. It seems that there are no other algebraic number fields k and sets S as the cases mentioned above such that the Galois group $G(k_S(p)|k)$ is of Koch type.

In this paper we will consider the maximal p-extension $k_S^T(p)$ of the number field k with restricted ramification at a finite set S containing S_p, which, in addition, is completely decomposed at the finite set T. The groups $G(k_S^T(p)|k)$ are a rich source of pro-p-groups of Koch type. Under certain conditions on T and S (and conditions on k) we will show that $G(k_S^T(p)|k)$ is a pro-p Schur group (i.e. has as many generators as relations), is of Koch type, its maximal abelian quotient is finite, and the cohomological dimension is equal to 2. Moreover, if p is odd and k is totally real, and assuming that the Leopoldt conjecture holds for totally real number fields, then $G(k_S^T(p)|k)$ is a fab pro-p-group.

The author wants to thank J. Gärtner and A. Schmidt for helpful conversations concerning this paper.

1 Pro-p-groups of Koch type

Let p be a prime number and let G be a pro-p-group. We denote the cohomology groups $H^i(G, \mathbb{Z}/p\mathbb{Z})$ by $H^i(G)$, and put $h^i(G) = \dim_{\mathbb{F}_p} H^i(G)$ and

$$\chi_2(G) = \sum_{i=0}^{2} (-1)^i \, h^i(G).$$

Let G_n be the n-th term in the lower p-central series defined recursively by $G_1 = G$ and $G_{n+1} = (G_n)^p[G_n, G]$. We recall some definitions.

Definition 1.1 *A pro-p-group G is called* **Schur group** *if $h^1(G) = h^2(G)$.*

Definition 1.2 *A pro-p-group G is called* **fab** *if U^{ab} is finite for all open subgroups U of G.*

For the notion of a pro-p duality group we refer to [4] III §4.

Proposition 1.3 *Let G be a fab pro-p-group of cohomological dimension equal to 2. Then G is a duality group. Furthermore, the strict cohomological dimension of G is equal to 3.*

Proof: In order to prove the first part of the proposition it suffices to show that the terms

$$D_i(G, \mathbb{Z}/p\mathbb{Z}) = \varinjlim_U H^i(U)^\vee$$

are trivial for $i = 0, 1$; here U runs through the open subgroups of G, and the transition maps are the duals of the corestriction maps, see [4] (3.4.6). For $i = 0$ this is clear, since G is infinite. For $i = 1$ we have

$$D_1(G, \mathbb{Z}/p\mathbb{Z}) = \varinjlim_U U^{ab}/p.$$

Since U^{ab} is finite for all open subgroups U of G, it follows from the group theoretical form of the principal ideal theorem, see [3] VI. (7.6), that

$$D_1(G, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Suppose that $scd_p G = 2$, i.e. $H^2(U, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ for all open subgroups U of G. From the exact sequence $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \to 0$, we obtain the exact sequence

$$0 \to ({}_pU^{ab})^\vee \to H^2(U) \to {}_pH^2(U, \mathbb{Q}_p/\mathbb{Z}_p) \to 0.$$

Since G is fab, we obtain

$$h^1(U) = \dim_{\mathbb{F}_p}(U^{ab}/p) = \dim_{\mathbb{F}_p}({}_pU^{ab}) = h^2(U),$$

i.e. $\chi_2(U) = 1$. Since $cd_p G = 2$, we have $\chi_2(U) = (G:U)\chi_2(G)$. This contradiction finishes the proof of the proposition. $\square$

Let G be a finitely represented pro-p-group and let $1 \to R \to F \to G \to 1$ be a minimal presentation, where F is the free pro-p-group on the generators $x_1, \ldots, x_d$ and $R = (w_1, \ldots, w_r)$ is the normal subgroup of F generated by the elements w_i, $i = 1, \ldots, r$.

Definition 1.4 *The minimal presentation $< x_1, \ldots, x_d | w_1, \ldots, w_r >$ of the pro-p-group G is said to be of* **Koch type** *if $r \le d$ and the relations w_i satisfy a congruence of the form*

$$w_i \equiv x_i^{p\,a_i} \prod_{i \ne j} [x_i, x_j]^{a_{ij}} \mod F_3$$

with $a_i, a_{ij} \in \mathbb{Z}$. The group G is of Koch type if it has a presentation of Koch type.

Examples: 1. Let p be an odd prime and S a finite set of prime numbers not containing p. Let $G = G(\mathbb{Q}_S(p)|\mathbb{Q})$ be the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside S. We can assume that $S = \{q_1, \cdots, q_d\}$ with $q_i \equiv 1 \bmod p$. Work of Koch [1] shows that $G = < x_1, \ldots, x_d | w_1, \ldots, w_d >$ where

$$w_i \equiv x_i^{q_i - 1} \prod_{i \ne j} [x_i, x_j]^{b_{ij}} \mod F_3,$$

and $q_i \equiv g_j^{b_{ij}} \bmod q_j$, where g_j is a primitive root for the prime q_j.Observe that $r = d$.

2. 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

$p = 3$. Let S be a set of primes of k whose norm is congruent to 1 mod p. If $G = G(k_S(p)|k)$ is the Galois group of the maximal p-extension of k unramified outside S, then G has a presentation of Koch type with $r = d$, see [1] or [6].

Let G be a pro-p-group of Koch type. Following Labute, we associate to $G =< x_1, \dots, x_d | w_1, \dots, w_r >$ and $S = \{x_1, \dots, x_d\}$ a directed graph, denoted by $\Gamma_S(p)$, with vertices the elements of S and a directed edge $x_i x_j$ from x_i to x_j if

$$l(x_i, x_j) := a_{ij} \mod p \neq 0.$$

The graph $\Gamma_S(p)$, together with the $l(x_i, x_j) \in \mathbb{Z}/p\mathbb{Z}$, $i, j \leq d$, is called the **linking diagram** of (G, S).

Definition 1.5 *Let $G =< x_1, \dots, x_d | w_1, \dots, w_r >$ be a pro-p-group of Koch type and let $\Gamma_S(p)$ be the associated linking diagram of (G, S). The set S is called* **strictly circular** *with respect to p (and $\Gamma_S(p)$ a* **non-singular circuit***) if there exists an ordering $S = \{v_1, \dots, v_d\}$ of the elements in S such that the following conditions are fulfilled:*

(1) *The vertices $v_1, \dots, v_d$ of $\Gamma_S(p)$ form a circuit $v_1 v_2 \dots v_d v_1$.*

(2) *If i, j are both odd, then $v_i v_j$ is not an edge of $\Gamma_S(p)$.*

(3) *If $l_{ij} = l(v_i, v_j)$, then $l_{12} l_{23} \cdots l_{d-1,d} l_{d1} - l_{1d} l_{21} l_{32} \cdots l_{d,d-1} \neq 0$.*

We remark that condition (2) implies that d is even and $d \geq 4$ and that condition (3) is satisfied if there exists an edge $v_i v_j$ of the circuit $v_1 v_2 \cdots v_d v_1$ such that $v_j v_i$ is not an edge $\Gamma_S(p)$.

Theorem 1.6 (Labute [2], Thm. 1.6.) *Let G be a pro-p-group of Koch type on the minimal set of generators S. If S is strictly circular with respect to p, then* $\operatorname{cd} G = 2$.

2 Galois extensions of number fields which are completely decomposed at given primes

We will use the following notation. Let S, T be sets of primes of k. Then

$k_S(p)$ is the maximal p-extension of k which is unramified outside S,

$k_S^T(p)$ is the maximal p-extension of k which is unramified outside S and completely decomposed at T.

Furthermore, $k(p)$ denotes the maximal p-extension of k. For a prime $\mathfrak{p}$ of k, let $k_\mathfrak{p}$ be the completion of k with respect to $\mathfrak{p}$, $U_\mathfrak{p}$ the group of units and $\mu(k_\mathfrak{p})$ the group of roots of unity in $k_\mathfrak{p}$. We denote the decomposition group and inertia group of $G(k(p)|k)$ with respect to $\mathfrak{p}$ by $G_\mathfrak{p}(k) = G_\mathfrak{p}(k(p)|k)$ and $T_\mathfrak{p}(k) = T_\mathfrak{p}(k(p)|k)$, respectively.

Considering the extension $k_S(p)|k$, the following primes cannot ramify in a p-extension, and are therefore redundant in S:

1. Complex primes.
2. Real primes if $p \neq 2$.
3. Primes $\mathfrak{p} \nmid p$ with $N(\mathfrak{p}) \not\equiv 1 \bmod p$.

Removing all these redundant places from S, we obtain a subset $S_{\min} \subseteq S$ which has the property that $G(k_S(p)|k) = G(k_{S_{\min}}(p)|k)$. Let

$$\tilde{S} = S \backslash (S_p \cup S_\infty)$$

the subset of finite primes of S not above p, and let

$$n_S = \sum_{\mathfrak{p} \in S_p \cap S} n_\mathfrak{p}, \quad \delta_S = \sum_{\mathfrak{p} \in S_p \cap S} \delta_\mathfrak{p} - \delta,$$

where $n_\mathfrak{p} = [k_\mathfrak{p} : \mathbb{Q}_p]$,

$$\delta = \begin{cases} 1, & \mu_p \subseteq k, \\ 0, & \mu_p \nsubseteq k, \end{cases} \qquad \text{and} \qquad \delta_\mathfrak{p} = \begin{cases} 1, & \mu_p \subseteq k_\mathfrak{p}, \\ 0, & \mu_p \nsubseteq k_\mathfrak{p}. \end{cases}$$

Furthermore, $\theta = \theta(S)$ is equal to 1 if $\mu_p \subseteq k$ and $S_{\min} = \varnothing$, and zero in all other cases. Finally, $Б_S(k)$ denotes the dual of the Kummer group

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

Proposition 2.1 *Let p be a prime number and assume that the number field k is totally imaginary if $p = 2$. Let T and $S = S_{\min}$ be finite sets of primes of k such that $T \cap S = \varnothing$. Then*

$$\begin{aligned} \chi_2(G(k_S^T(p)|k)) &\leq \theta + r_1 + r_2 - n_S + \#T, \\ h^1(G(k_S^T(p)|k)) &\geq 1 + \#\tilde{S} + \delta_S + n_S + \dim_{\mathbb{F}_p} Б_S - r_1 - r_2 - \#T. \end{aligned}$$

Proof: Since $T \cap S = \varnothing$, we have a surjection

$$\bigoplus_{\mathfrak{p} \in T} G_\mathfrak{p}(k)/T_\mathfrak{p}(k) \twoheadrightarrow \left(G(k_S(p)|k_S^T(p))^{ab}\right)_{G(k_S^T(p)|k)}$$

(here M_G denotes the G-coinvariants of a G-module M). Thus we obtain

$$\dim_{\mathbb{F}_p} H^1(G(k_S(p)|k_S^T(p)))^{G(k_S^T(p)|k)} \leq \#T.$$

Using [4] (8.7.11), the exact 5-term sequence

$$0 \longrightarrow H^1(G(k_S^T(p)|k)) \longrightarrow H^1(G(k_S(p)|k)) \longrightarrow H^1(G(k_S(p)|k_S^T(p)))^{G(k_S^T(p)|k)}$$
$$\longrightarrow H^2(G(k_S^T(p)|k)) \longrightarrow H^2(G(k_S(p)|k))$$

gives us the inequalities

$$\begin{aligned} & h^2(G(k_S^T(p)|k)) - h^1(G(k_S^T(p)|k)) \\ \leq\ & h^2(G(k_S(p)|k)) - h^1(G(k_S(p)|k)) + \dim_{\mathbb{F}_p} H^1(G(k_S(p)|k_S^T(p)))^{G(k_S^T(p)|k)} \\ \leq\ & \theta - 1 + r_1 + r_2 - n_S + \#T \end{aligned}$$

and

$$h^1(G(k_S^T(p)|k)) \geq h^1(G(k_S(p)|k)) - \#T = 1 + \#\tilde{S} + \delta_S + n_S + \dim_{\mathbb{F}_p} Б_S - r_1 - r_2 - \#T.$$

□

Corollary 2.2 *With the assumptions of proposition* (2.1) *let*

$$c(S,T) = \max\{0, \theta + r_1 + r_2 - n_S + \#T\}.$$

Assume that

$$\#\tilde{S} \geq \left(1 + \sqrt{c(S,T)}\,\right)^2 - (\delta_S + \dim_{\mathbb{F}_p} Б_S + \theta).$$

Then the group $G(k_S^T(p)|k)$ is infinite.

Proof: Let $G = G(k_S^T(p)|k)$ and suppose that this group is finite. Then, by the Golod Safarevič inequality, see [4] (3.9.7),

$$h^2(G) > \frac{h^1(G)^2}{4}.$$

From proposition (2.1) it follows that

$$c(S,T) - 1 \geq \theta - 1 + r_1 + r_2 - n_S + \#T \geq h^2(G) - h^1(G) > h^1(G)^2/4 - h^1(G),$$

hence

$$\#\tilde{S} + (\delta_S + \dim_{\mathbb{F}_p} Б_S + \theta) - c(S,T) + 1 \leq h^1(G) < 2 + 2\sqrt{c(S,T)},$$

which contradicts the assumption on $\#\tilde{S}$. $\square$

Let $K_1,\dots,K_\rho$ be independent $\mathbb{Z}_p$-extensions of k such that $\tilde{k}=\bigcup_{i=1}^{\rho}K_i$ is the compositum of all $\mathbb{Z}_p$-extensions of k. Recall that $\tilde{k}\subseteq k_S(p)$, if $S_p\subseteq S$. We say that a finite set T of primes of k has the property $(*)$ if the following holds:

Property $(*)$**:** The cardinality of T is equal to ρ, and if $T=\{\mathfrak{p}_1,\dots,\mathfrak{p}_\rho\}$, then

$$\mathfrak{p}_i \text{ does not decompose in } K_i|k, \text{ i.e. } G_{\mathfrak{p}_i}(K_i|k)=G(K_i|k), \quad i=1,\dots,\rho.$$

If S is a finite set of primes of k such that $S\cap T=\varnothing$, then it follows that the homomorphism

$$\mathop{\ast}_{\mathfrak{p}\in T} G_{\mathfrak{p}}(k(p)|k)/T_{\mathfrak{p}}(k(p)|k)\longrightarrow G(k_S(p)|k)\longrightarrow G(\tilde{k}\cap k_S(p)|k)$$

is surjective, and, in particular, $G(k_S^T(p)|k)^{ab}$ is finite.

Proposition 2.3 *Let p be a prime number and assume that the number field k is totally imaginary if $p=2$. Let T and $S_p\subseteq S=S_{\min}$ be finite sets of primes of k such that $T\cap S=\varnothing$.*

(i) *If $\#T=r_2+1$, then*

$$\chi_2(G(k_S^T(p)|k))\le 1.$$

(ii) *Assume that the Leopoldt conjecture holds for k and p, and that T has the property $(*)$. Then*

$$h^1(G(k_S^T(p)|k))=h^2(G(k_S^T(p)|k))$$

and

$$G(k_S^T(p)|k)^{ab}\cong \operatorname{Tor} G(k_S(p)|k)^{ab}.$$

In particular, $G(k_S^T(p)|k)^{ab}$ is finite. If $\#S\backslash S_p\ge 4$, then $G(k_S^T(p)|k)$ is infinite.

(iii) *Assume in addition to the assumptions of* (ii) *that*

$$\dim_{\mathbb{F}_p} Б_S=0 \text{ and } \sum_{\mathfrak{p}\in S_p}\delta_{\mathfrak{p}}=\delta.$$

Then

$$h^1(G(k_S^T(p)|k))=h^2(G(k_S^T(p)|k))=\#S\backslash S_p.$$

Proof: Let $G = G(k_S^T(p)|k)$. By proposition (2.1), we have

$$\chi_2(G) \leq 0 + r_1 + r_2 - [k:\mathbb{Q}] + \#T = 1$$

proving (i).

From the exact sequence $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \to 0$, we obtain the exact sequence

$$0 \to ({}_pG^{ab})^\vee \to H^2(G) \to {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \to 0.$$

By assumption, the Leopoldt conjecture holds, i.e. $\rho = \mathrm{rank}_{\mathbb{Z}_p} G(\tilde{k}|k) = r_2 + 1$. Therefore, as T has the property $(*)$, G^{ab} is finite. It follows that

$$h^1(G) = \dim_{\mathbb{F}_p} {}_pG^{ab} \leq h^2(G).$$

Since $h^1(G) \geq h^2(G)$ by (i), we get equality. The commutative and exact diagram

$$\begin{array}{ccccccc} & & \mathrm{Tor}\, G(k_S(p)|k)^{ab} & & & & \\ & & \downarrow & \searrow & & & \\ \bigoplus_{\mathfrak{p}\in T} G_{\mathfrak{p}}(k(p)|k)/T_{\mathfrak{p}}(k(p)|k) & \longrightarrow & G(k_S(p)|k)^{ab} & \longrightarrow & G(k_S^T(p)|k)^{ab} & \longrightarrow & 0 \\ & \searrow^{\cong} & \downarrow & & & & \\ & & G(\tilde{k}|k) & & & & \end{array}$$

shows $\mathrm{Tor}\, G(k_S(p)|k)^{ab} \xrightarrow{\sim} G(k_S^T(p)|k)^{ab}$. Furthermore, it follows from $c(S,T) = 1$ and corollary (2.2), that $G(k_S^T(p)|k)$ is infinite, if $\#S\backslash S_p \geq 4$. This proves (ii).

From proposition (2.1) it follows that $h^1(G) \geq \#\tilde{S}$, and using [4] (8.7.11), we have $h^2(G) \leq \#\tilde{S}$. This proves (iii). $\square$

Theorem 2.4 *Let p be a prime number and assume that the number field k is totally imaginary if $p = 2$. Let T and $S_p \subseteq S = S_{\min}$ be finite sets of primes of k such that $T \cap S = \varnothing$. Assume that*

(a) *T has the property $(*)$.*

(b) *$\dim_{\mathbb{F}_p} \text{Б}_{S_p} = 0$ and $\sum_{\mathfrak{p}\in S_p} \delta_{\mathfrak{p}} = \delta$.*

Then the following holds:

(i) *The canonical homomorphism*

$$\mathop{\ast}_{\mathfrak{p}\in S\backslash S_p} T_{\mathfrak{p}}(k(p)|k) \twoheadrightarrow G(k_S^T(p)|k)$$

is surjective.

(ii) *There is an isomorphism*

$$\bigoplus_{\mathfrak{p}\in S\backslash S_p} \mu(k_\mathfrak{p})(p) \xrightarrow{\sim} G(k_S^T(p)|k)^{ab}.$$

(iii) *The map*

$$H^2(G(k_S^T(p)|k)) \hookrightarrow \bigoplus_{\mathfrak{p}\in S\backslash S_p} H^2(G_\mathfrak{p})$$

is injective.

(iv) *The pro-p-group $G(k_S^T(p)|k)$ is of Koch type and*

$$h^1(G(k_S^T(p)|k)) = h^2(G(k_S^T(p)|k)) = \#S\backslash S_p.$$

(v) *$G(k_S^T(p)|k)^{ab}$ is finite. If $\#S\backslash S_p \geq 4$, then $G(k_S^T(p)|k)$ is infinite.*

Proof: Since $\dim_{\mathbb{F}_p} \text{Б}_{S_p} = 0$ and $\sum_{\mathfrak{p}\in S_p} \delta_\mathfrak{p} = \delta$, the pro-$p$-group $G(k_{S_p}(p)|k)$ is free, see [4] (8.7.10). Therefore Leopoldt's conjecture holds for k and p. Furthermore $\text{Б}_S = 0$ as Б_{S_p} surjects onto Б_S. From proposition (2.3) it follows that the assertion on the dimensions in (iv) and assertion (v) are true.

The cokernel of the canonical homomorphism

$$\mathop{\ast}_{\mathfrak{p}\in S\backslash S_p} T_\mathfrak{p}(k(p)|k) \longrightarrow G(k_S^T(p)|k)$$

is the Galois group $G(k_{S_p}^T(p)|k)$. Since $G(k_{S_p}(p)|k)$ is a free pro-p-group of rank r_2+1, we have $G(k_{S_p}(p)|k)^{ab} \cong \mathbb{Z}_p^{r_2+1}$. Using the assumption $(*)$ for T, we get

$$G(k_{S_p}^T(p)|k)^{ab} = 0,$$

hence $G(k_{S_p}^T(p)|k) = 1$, i.e. we proved (i).

Since the Leopoldt's conjecture holds for k and p, we have

$$(\operatorname{Tor} G(k_S(p)|k)^{ab})^\vee \cong H^2(G(k_S(p)|k), \mathbb{Z}/p^r\mathbb{Z})$$

for $r \in \mathbb{N}$ big enough. The exact sequence

$$H^2(G(k_S(p)|k), \mathbb{Z}/p^r\mathbb{Z}) \to \bigoplus_{\mathfrak{p}\in S} H^2(G_\mathfrak{p}(k), \mathbb{Z}/p^r\mathbb{Z}) \to H^0(G(k_S(p)|k), \mu_{p^r})^\vee \to 0$$

implies that we obtain a surjection

$$H^2(G(k_S(p)|k), \mathbb{Z}/p^r\mathbb{Z}) \twoheadrightarrow \bigoplus_{\mathfrak{p}\in S\backslash S_p} H^2(G_\mathfrak{p}(k), \mathbb{Z}/p^r\mathbb{Z}) \cong \bigoplus_{\mathfrak{p}\in S\backslash S_p} \mu(k_\mathfrak{p})(p)^\vee.$$

Using proposition (2.3)(ii), it follows that we obtain an injection

$$\bigoplus_{\mathfrak{p}\in S\setminus S_p} \mu(k_{\mathfrak{p}})(p) \hookrightarrow G(k_S^T(p)|k)^{ab}.$$

On the other hand, by (i) the map

$$\bigoplus_{\mathfrak{p}\in S\setminus S_p} \mu(k_{\mathfrak{p}})(p) \cong \bigoplus_{\mathfrak{p}\in S\setminus S_p} T_{\mathfrak{p}}(k)/[T_{\mathfrak{p}}(k), G_{\mathfrak{p}}(k)] \twoheadrightarrow G(k_S^T(p)|k)^{ab}$$

is surjective. This proves (ii).

In order to prove (iii), we consider the exact sequence

$$1 \longrightarrow \mathcal{K} \longrightarrow \mathop{\ast}_{\mathfrak{p}\in S\setminus S_p} G_{\mathfrak{p}}(k) \longrightarrow G(k_S^T(p)|k) \longrightarrow 1,$$

where $\mathcal{K}$ is the kernel of the natural map $\ast_{\mathfrak{p}\in S\setminus S_p} G_{\mathfrak{p}}(k) \to G(k_S^T(p)|k)$ which is surjective by (i). For an abelian group A we obtain (using (i) again) the commutative and exact diagram

$$\begin{array}{ccccccc}
 & & & & \bigoplus_{\mathfrak{p}\in S\setminus S_p} H^1_{nr}(G_{\mathfrak{p}}(k), A) & & \\
 & & & & \downarrow & \searrow & \\
0 \longrightarrow & H^1(G(k_S^T(p)|k), A) & \longrightarrow & & \bigoplus_{\mathfrak{p}\in S\setminus S_p} H^1(G_{\mathfrak{p}}(k), A) & \xrightarrow{res} & H^1(\mathcal{K}, A)^{G(k_S^T(p)|k)} \\
 & \| & & & \downarrow & & \\
 & H^1(G(k_S^T(p)|k), A) & \hookrightarrow & & \bigoplus_{\mathfrak{p}\in S\setminus S_p} H^1(T_{\mathfrak{p}}(k), A)^{G_{\mathfrak{p}}(k)}. & &
\end{array}$$

If $A = \mathbb{Q}_p/\mathbb{Z}_p$, then lower map is an isomorphism by (ii). Furthermore, since the Leopoldt's conjecture holds, we have $H^2(G(k_S^T(p)|k), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, and so the map *res* is surjective. If follows that

$$\bigoplus_{\mathfrak{p}\in S\setminus S_p} H^1_{nr}(G_{\mathfrak{p}}(k), \mathbb{Q}_p/\mathbb{Z}_p) \cong H^1(\mathcal{K}, \mathbb{Q}_p/\mathbb{Z}_p)^{G(k_S^T(p)|k)},$$

hence

$$\bigoplus_{\mathfrak{p}\in S\setminus S_p} H^1_{nr}(G_{\mathfrak{p}}(k), \mathbb{Z}/p\mathbb{Z}) \cong H^1(\mathcal{K}, \mathbb{Z}/p\mathbb{Z})^{G(k_S^T(p)|k)}.$$

Considering the diagram above with $A = \mathbb{Z}/p\mathbb{Z}$, we obtain the desired injection $H^2(G(k_S^T(p)|k)) \hookrightarrow \bigoplus_{\mathfrak{p}\in S\setminus S_p} H^2(G_{\mathfrak{p}}(k))$.

Let $\tilde{S} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_d\}$ and let τ_i be a generator of the cyclic group $T_{\mathfrak{q}_i}(k)$, $i = 1, \ldots, d$. Then by (i) and (iv) the set $\{\tau_1, \ldots, \tau_d\}$ is a minimal set of generators of the group $G(k_S^T(p)|k)$. Let F be the free pro-p-group on the generators $x_1, \ldots, x_d$, and let

$$1 \longrightarrow R \longrightarrow F \stackrel{\pi}{\longrightarrow} G(k_S^T(p)|k) \longrightarrow 1$$

be a minimal presentation of the group $G(k_S^T(p)|k)$, where π maps x_i to τ_i, $i = 1, \ldots, d$. From (iv) and [4] (7.5.2) it follows that a set of defining relations is given by

$$w_i = x_i^{N(\mathfrak{q}_i)-1}[x_i, y_i], \quad i = 1, \ldots, d,$$

where $y_i \in F$ denotes a pre-image of the Frobenius automorphism σ_i with respect to $\mathfrak{q}_i$, see [1],§11.4. Let

$$y_i \equiv \prod_{i\neq j} x_j^{l_{ij}} \mod F_2$$

with $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$. Then we obtain

$$w_i = x_i^{N(q_i)-1}[x_i, y_i] \equiv x_i^{N(q_i)-1}[x_i, \prod_{i\neq j} x_j^{l_{ij}}] \equiv x_i^{N(q_i)-1} \prod_{i\neq j} [x_i, x_j]^{l_{ij}} \mod F_3.$$

Thus $G(k_S^T(p)|k)$ is a pro-p-group of Koch type. □

From theorem (2.4) and Labute's theorem (1.6) we obtain

Theorem 2.5 *Let p be a prime number and assume that the number field k is totally imaginary if $p = 2$. Let T and $S_p \subseteq S = S_{\min}$ be finite sets of primes of k such that $T \cap S = \varnothing$. Assume that*

(a) *T has the property $(*)$,*

(b) $\dim_{\mathbb{F}_p} \text{Б}_{S_p} = 0$ *and* $\sum_{\mathfrak{p}\in S_p} \delta_{\mathfrak{p}} = \delta$,

(c) $\Gamma_{S\setminus S_p}(p)$ *is a non-singular circuit.*

Then $G(k_S^T(p)|k)$ is a pro-p Schur group, $G(k_S^T(p)|k)^{ab}$ is finite and

$$\mathrm{cd}_p\, G(k_S^T(p)|k) = 2.$$

Corollary 2.6 *With the notation and assumptions of theorem (2.5) assume in addition, that p is odd and k is totally real. Assume further that the Leopoldt conjecture holds for totally real number fields.*

Then $G(k_S^T(p)|k)$ is a fab pro-p-group, and a duality group of dimension 2 and strict cohomological dimension equal to 3.

Proof: If $K|k$ is a finite Galois extension inside $k_S^T(p)$, then K is also totally real as $p \neq 2$. Since the Leopoldt conjecture holds for K and p, there is only one $\mathbb{Z}_p$-extension of K, the cyclotomic one. The prolongations of the only prime $\mathfrak{q} \in T(k)$ are inert in this extension. Therefore $G(k_S^T(p)|K)^{ab}$ is finite. The second assertion follows from (1.3). □

It seems that among the conditions of (2.6) the assumption that k is totally real in order to show that $G(k_S^T(p)|k)$ is fab is not necessary but we can not prove it. The next results show that theorem (2.5) is not empty. The idea of the proof is inspired by [2] prop. 6.1.

Proposition 2.7 *Let k be a number field and let p be a prime number such that $\mu_p \nsubseteq k$. Let T and $S = S_{\min}$ be finite disjoint sets of primes of k with $S_p \subseteq S$. Assume that conditions* (a) *and* (b) *of* (2.5) *hold, and let*

$$\mathop{\ast}_{\mathfrak{p}\in\tilde{S}} T_{\mathfrak{p}}(k(p)|k) \twoheadrightarrow G(k_S^T(p)|k)$$

be a minimal presentation of the pro-p-group $G(k_S^T(p)|k)$ of Koch type, where $\tilde{S} = S \backslash S_p = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. Let $q_i = \mathfrak{q}_i \cap \mathbb{Q}$, $i = 1, \ldots, m$, be the underlying prime numbers, and assume that for all i

(i) $q_i \equiv 1 \bmod p$ *and* $q_i \neq q_j$ *if* $i \neq j$,

(ii) *the prime number q_i is unramified in $k|\mathbb{Q}$,*

(iii) *the image of $\mathfrak{q}_i$ in the p-primary part $Cl_k(p)$ of the ideal class group of k is trivial.*

Then a prime $\mathfrak{q}_{m+1}$ can be found satisfying (i)-(iii) *such that the additional edges of the linking diagram $\Gamma_{\tilde{S}\cup\{\mathfrak{q}\}}(p)$ of $(G(k_{S\cup\{\mathfrak{q}\}}^T(p)|k), \tilde{S} \cup \{\mathfrak{q}\})$ are arbitrarily prescribed.*

Remark: Often we identify the sets $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ and $\{\tau_{\mathfrak{q}_1}, \ldots, \tau_{\mathfrak{q}_m}\}$ of primes of k and generators of $G(k_S^T(p)|k)$, respectively, and denote them by the same letter.

Proof: First we observe that, if $\mathfrak{q} \notin T \cup S$ is a prime of k with $N_{k|\mathbb{Q}}\,\mathfrak{q} \equiv 1 \bmod p$, then by theorem (2.4) the group $G(k_{S\cup\{\mathfrak{q}\}}^T(p)|k)$ is also of Koch type and

$$\mathop{\ast}_{\mathfrak{p}\in\tilde{S}\cup\{\mathfrak{q}\}} T_{\mathfrak{p}}(k(p)|k) \twoheadrightarrow G(k_{S\cup\{\mathfrak{q}\}}^T(p)|k)$$

is a minimal presentation of $G(k_{S\cup\{\mathfrak{q}\}}^T(p)|k)$.

If $\bar{k}$ is the maximal abelian p-extension of $k(\mu_p)$ and $\mathfrak{q}$ a non-archimedean prime of $k(\mu_p)$ not lying above p, then

$$G_{\mathfrak{q}}(\bar{k}|k(\mu_p)) = <\sigma_{\mathfrak{q}}, \tau_{\mathfrak{q}}> \subseteq G(\bar{k}|k(\mu_p)),$$

where $< \tau_{\mathfrak{q}} >$ is the inertia subgroup of the decomposition group $G_{\mathfrak{q}}(\bar{k}|k(\mu_p))$ of $G(\bar{k}|k(\mu_p))$ with respect to $\mathfrak{q}$, and $\sigma_{\mathfrak{q}}$ is a Frobenius lift.

By (i) and (ii) there is a unique extension E_i of $k(\mu_p)$ contained in $k(\mu_{pq_i})$ of degree p, i.e. $G(E_i|k(\mu_p)) \cong \mathbb{Z}/p\mathbb{Z}$. By (iii), there exists a natural number h_i prime to p such that $\mathfrak{q}_i^{h_i} = (\pi_{\mathfrak{q}_i})$ is a principal ideal of k. Let

$$F_i = k(\mu_p, \sqrt[p]{\pi_{\mathfrak{q}_i}})$$

with Galois group $G(F_i|k(\mu_p)) \cong \mathbb{Z}/p\mathbb{Z}$, and let H_k be the p-elementary Hilbert field of k, i.e. the maximal p-elementary abelian unramified extension of k, with Galois group $G(H_k(\mu_p)|k(\mu_p)) \cong \mathbb{Z}/p\mathbb{Z}^{\epsilon}$ for some $\epsilon \geq 0$. The fields

$$E_1, \ldots, E_m, F_1, \ldots, F_m, H_k(\mu_p)$$

are linearly disjoint over $k(\mu_p)$, and let K be the composite of these fields. The field K is Galois over k and the subgroup $H = G(K|k(\mu_p))$ of $G(K|k)$ is the direct product of the Galois groups of these fields over $k(\mu_p)$.

If $\sigma_{\mathfrak{Q}} \in G(K|k)$ is the Frobenius automorphism at the unramified prime $\mathfrak{Q}$ of K and $\mathfrak{Q}$ lies above the prime $\mathfrak{q}$ of k, then $\sigma_{\mathfrak{Q}} \in G(K|k(\mu_p))$ if and only if $N_{k|\mathbb{Q}}\,\mathfrak{q} \equiv 1 \bmod p$. Furthermore, the restriction of $\sigma_{\mathfrak{Q}}$ to $H_k(\mu_p)$ is the identity if and only if the image of $\mathfrak{q}$ in $Cl_k(p)$ is trivial.

Assume a prime $\mathfrak{q}_{m+1}$ of k is given such that the underlying prime number q_{m+1} is unramified in K, $q_{m+1} \equiv 1 \bmod p$ (and so $N_{k|\mathbb{Q}}\,\mathfrak{q}_{m+1} \equiv 1 \bmod p$), $q_{m+1} \neq q_j$ for $j = 1, \ldots, m$, and the image of $\mathfrak{q}_{m+1}$ in $Cl_k(p)$ is trivial. Then we choose a prolongation of $\mathfrak{q}_{m+1}$ to $k(\mu_p)$, which we also denote by $\mathfrak{q}_{m+1}$. Let $\mathfrak{Q}|\mathfrak{q}_{m+1}$ be a prime of K; we denote $\sigma_{\mathfrak{Q}}$ by $\sigma_{\mathfrak{q}_{m+1}} = \sigma_{\mathfrak{q}_{m+1}}|_K$ as H is abelian. Let $h \in \mathbb{N}$ be prime to p such that $(\mathfrak{q}_{m+1})^h = (\pi_{\mathfrak{q}_{m+1}})$ is a principal ideal of k. Since

$$G(E_i|k(\mu_p)) = < \tau_{\mathfrak{q}_i} G(\bar{k}|E_i) > \cong \mathbb{Z}/p\mathbb{Z},$$

we get

$$\sigma_{\mathfrak{q}_{m+1}}|_{E_i} \equiv (\tau_{\mathfrak{q}_i}|_{E_i})^{l_{m+1,i}} \mod G(\bar{k}|E_i),$$

where $l_{m+1,i} \in \mathbb{Z}/p\mathbb{Z}$. Therefore the restriction of $\sigma_{\mathfrak{q}_{m+1}}$ to E_i is the identity if and only if the restriction of $(\sigma_{\mathfrak{q}_{m+1}})^h$ to E_i is the identity (recall that h is prime to p), and this is the case if and only if $\pi_{\mathfrak{q}_{m+1}}$ is a p-th power mod $\mathfrak{q}_i$. If $F_i = k(\mu_p, \sqrt[p]{\pi_{\mathfrak{q}_i}})$, then

$$\sigma_{\mathfrak{q}_{m+1}}|_{F_i}(\sqrt[p]{\pi_{\mathfrak{q}_i}}) = \sigma_{\mathfrak{q}_{m+1}}|_{(F_i)_{\mathfrak{q}_{m+1}}}(\sqrt[p]{\pi_{\mathfrak{q}_i}}) = \left(\frac{\pi_{\mathfrak{q}_i}}{\mathfrak{q}_{m+1}}\right) \sqrt[p]{\pi_{\mathfrak{q}_i}}\,,$$

where $\left(\frac{\pi_{\mathfrak{q}_i}}{\mathfrak{q}_{m+1}}\right) \in \mu_p \subseteq (F_i)_{\mathfrak{q}_{m+1}}$ is the Hilbert symbol, see [3] §8. We have

$$\left(\frac{\pi_{\mathfrak{q}_i}}{\mathfrak{q}_{m+1}}\right) = 1 \text{ if and only if } \pi_{\mathfrak{q}_i} \equiv \alpha^p \mod \mathfrak{q}_{m+1}$$

for some $\alpha \in k(\mu_p)$, i.e. the restriction of $\sigma_{\mathfrak{q}_{m+1}}$ to F_i is the identity if and only if $\pi_{\mathfrak{q}_i}$ is a p-th power mod $\mathfrak{q}_{m+1}$. Let $G = G(k^T_{S\cup\{\mathfrak{q}_{m+1}\}}(p)|k)$, then

$$\sigma_{\mathfrak{q}_{m+1}} \equiv \prod_{1\le j\le m} (\tau_{\mathfrak{q}_j})^{l_{m+1,j}} \mod G_2$$

and

$$\sigma_{\mathfrak{q}_i} \equiv \prod_{\substack{1\le j\le m+1\\ j\ne i}} (\tau_{\mathfrak{q}_j})^{l_{ij}} \mod G_2$$

with $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$. By the considerations above, $l_{m+1,j} = 0$ if and only if $\pi_{\mathfrak{q}_{m+1}}$ is a p-th power modulo $\mathfrak{q}_j$ and this is the case if and only if the restriction of $\sigma_{\mathfrak{q}_{m+1}}$ to E_j is the identity, and $l_{i,m+1} = 0$ if and only if $\pi_{\mathfrak{q}_i}$ is a p-th power modulo $\mathfrak{q}_{m+1}$ and this is the case if and only if the restriction of $\sigma_{\mathfrak{q}_{m+1}}$ to F_i is the identity.

By the Čebotarev density theorem, for every $g \in H$ there exist infinitely many primes $\mathfrak{q}$ of k of degree equal to 1 such that $\sigma_{\mathfrak{q}} = g$. Thus we may assume that $\mathfrak{q} = \mathfrak{q}_{m+1}$ is not in T, that the underlying prime number q_{m+1} is different to q_i, $i = 1,\dots,m$, and that q_{m+1} is unramified in $K|\mathbb{Q}$. Since $\sigma_{\mathfrak{q}_{m+1}} \in H$, it follows that $q_{m+1} = N_{k|\mathbb{Q}}\,\mathfrak{q}_{m+1} \equiv 1 \bmod p$. Thus $\mathfrak{q}_{m+1}$ satisfies (i) and (ii). Furthermore, choosing the element $g \in H$ suitable, we can extend the directed graph $\Gamma_{\tilde{S}}(p)$ by a single prime $\mathfrak{q}_{m+1} \notin T \cup S$ satisfying (i), (ii) and, in addition, (iii) with prescribed edges joining the primes of $\tilde{S}$ to $\mathfrak{q}_{m+1}$ and $\mathfrak{q}_{m+1}$ to the primes of $\tilde{S}$. □

Corollary 2.8 *With the notation and assumptions of* (2.7) *let* $\#\tilde{S} \ge 2$. *Then* $\tilde{S}$ *can be extended to a set* $\tilde{S}'$ *with* $\#\tilde{S}' = 2\#\tilde{S}$ *such that the linking diagram* $\Gamma_{\tilde{S}'}(p)$ *of* $(G(k^T_{\tilde{S}'\cup S_p}(p)|k), \tilde{S}')$ *is a non-singular circuit.*

Proof: Let $\tilde{S} = \{\mathfrak{q}_1,\dots,\mathfrak{q}_m\}$. We extend $\tilde{S}$ by a single prime $\mathfrak{r}_1$ so that $\mathfrak{q}_1\mathfrak{r}_1$, $\mathfrak{r}_1\mathfrak{q}_2$ are edges with $\mathfrak{r}_1\mathfrak{q}_1$ not an edge. Now extend the new graph $\Gamma_{\tilde{S}\cup\{\mathfrak{r}_1\}}(p)$ by another prime $\mathfrak{r}_2$ so that $\mathfrak{q}_2\mathfrak{r}_2$ and $\mathfrak{r}_2\mathfrak{q}_2$ are the only new edges. Continuing in this way, we see that we can extend $\Gamma_{\tilde{S}}(p)$ to a non-singular circuit $\Gamma_{\tilde{S}'}(p)$ having $2m$ vertices. If $1 \le i \le m$, let $v_{2i-1} = \mathfrak{r}_i$ and $v_{2i} = \mathfrak{q}_i$. Then $v_1 \cdots v_{2m} v_1$ is the required non-singular circuit. □

Example: Let $k = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where p is an odd regular prime number and ζ_p a primitive p-root of unity. Then k has property (b) of theorem (2.5). Let $T = \{\mathfrak{p}_0\}$ where $\mathfrak{p}_0$ is a prime of k which is inert in first step of the cyclotomic $\mathbb{Z}_p$-extension of k. Then T has the property $(*)$. Let $\tilde{S} = \{\mathfrak{q}_1,\dots,\mathfrak{q}_m\}$, $m \ge 2$, be a set of primes of k lying over pairwise different prime numbers $q_1,\dots,q_m$ such that $q_i \equiv 1 \bmod p$, and $\mathfrak{p}_0 \notin \tilde{S}$. By (2.8), we can extend $\tilde{S}$ to a set $\tilde{S}'$ such that the linking diagram $\Gamma_{\tilde{S}'}(p)$ of $(G(k^T_{\tilde{S}'\cup S_p}(p)|k), \tilde{S}')$ is a non-singular circuit.

References

[1] Koch, H. *Galoissche Theorie der p-Erweiterungen.* Deutscher Verlag der Wissenschaften (1970), English translation: Springer 2002

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

[3] Neukirch, J. *Algebraische Zahlentheorie.* Springer 1992, English translation: Algebraic Number Theory. Springer 1999

[4] Neukirch, J., Schmidt, A., Wingberg, K. *Cohomology of Number Fields.* Springer 2000

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

[6] Vogel, D. *Circular sets of primes of imaginary quadratic number fields.* Preprints der Forschergruppe *Algebraische Zykel und L-Funktionen* Regensburg/Leipzig Nr. 5, 2006.
`http://www.mathematik.uni-regensburg.de/FGAlgZyk`

Mathematisches Institut
der Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
Germany

e-mail: wingberg@mathi.uni-heidelberg.de