CIRCULAR SETS OF PRIMES OF IMAGINARY QUADRATIC NUMBER FIELDS

DENIS VOGEL

Abstract. Let $p$ be an odd prime number and let $K$ be an imaginary quadratic number field whose class number is not divisible by $p$. For a set $S$ of primes of $K$ whose norm is congruent to 1 modulo $p$, we introduce the notion of strict circularity. We show that if $S$ is strictly circular, then the group $G(K_S(p)/K)$ is of cohomological dimension 2 and give some explicit examples.

1. Introduction

Let $K$ be a number field, $p$ a prime number and $S$ a finite set of primes of $K$ not containing any primes dividing $p$. Only little has been known on the structure of the Galois group $G(K_S(p)/K)$ of the maximal $p$-extension of $K$ unramified outside $S$, in particular there has been no result on the cohomological dimension of $G(K_S(p)/K)$. Recently, Labute [La] 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. If $K = \mathbb{Q}$, Labute used results of Koch 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. Schmidt [S] extended the result of Labute by arithmetic methods and weakened Labute’s condition on $S$.

The objective of this paper is to study the case where $K$ is an imaginary quadratic number field whose class number is not divisible by $p$. In the first section we introduce the notions of the linking number of two primes and of strict circularity of a set of primes of $K$, all of this in complete analogy with the case $K = \mathbb{Q}$. Using Labute’s results we obtain the criterion that if $S$ is strictly circular then $G(K_S(p)/K)$ is a mild pro-$p$-group and hence of cohomological dimension 2. In the following section we give some explicit examples of strictly circular sets of primes, and in section 4 we study how a strictly circular set $T$ can be enlarged to set $S$ of primes of $K$, such that $G(K_S(p)/K)$ has cohomological dimension 2 as well.

I would like to thank A. Schmidt for the suggestion to study this problem and for many remarks and comments he made.

2. Linking numbers and strictly circular sets

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 $S = \{q_1, \ldots, q_n\}$ be a set of primes of $K$ whose

Date: May 12, 2006.
norm is congruent to 1 mod $p$. For a subset $T$ of $S$, we denote the maximal $p$-extension of $K$ unramified outside $T$ by $K_T(p)$, and we put $G_T(p) = G(K_T(p)/K)$.

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 $q \in T$ are 1 and for $q \notin T$ are units. For $q \in S$ we denote by $K_q$ the completion of $K$ at $q$ and by $U_q$ the unit group of $K_q$. Furthermore, let $\pi_q$ be a uniformizer of $K_q$ and let $\alpha_q$ be a generator of the cyclic group $U_q/\mathbb{Z}_q$. Let $\Omega$ be an extension of $q$ to $K_S(p)$. We let $\sigma_q$ be an element of $G_S(p)$ with the following properties:

1. $\sigma_q$ is a lift of the Frobenius automorphism of $\Omega$;
2. the restriction of $\sigma_q$ to the maximal abelian subextension $\tilde{K}/K$ of $K_S(p)/K$ is equal to $(\tilde{\pi}_q, \tilde{K}/K)$, where $\tilde{\pi}_q$ denotes the idèle whose $q$-component equals $\pi_q$ and all other components are 1.

Let $\tau_q$ denote an element of $G_S(p)$ such that

1. $\tau_q$ is an element of the inertia group $I_\Omega$ of $K_S(p)/K$;
2. the restriction of $\tau_q$ to $\tilde{K}/K$ equals $(\tilde{\alpha}_q, \tilde{K}/K)$, where $\tilde{\alpha}_q$ denotes the idèle whose $q$-component equals $\alpha_q$ and all other components are equal to 1.

For any subset $T$ of $S$, class field theory provides an isomorphism

$$I_K/(U_T p_K K^\times) \cong G_T(p)/G_T(p)[G_T(p), G_T(p)] = H_1(G_T(p), \mathbb{Z}/p\mathbb{Z}).$$

Let $V_T$ denote the Kummer group

$$V_T = \{ a \in K^\times \mid a \in K_q^{\times m} \text{ for } q \in T \text{ and } a \in U_q K_q^{\times m} \text{ for } q \notin T \}$$

We remark that due to [NSW], 8.7.2, we have an exact sequence

$$0 \to \mathcal{O}_K^\times /p \to V_\varnothing(K) \to p\text{Cl}(K) \to 0.$$ 

By our assumptions, this yields that $V_\varnothing(K) = 0$, and since $V_T(K) \subset V_\varnothing(K)$ we have $V_T(K) = 0$. This implies that the dual of the Kummer group $\text{Br}_T(K) = (V_T(K))^\vee$ is trivial. The group on the left hand side of the above isomorphism is therefore given by

$$I_K/(U_T p_K K^\times) \cong U_\varnothing /U_T U_\varnothing^p = \prod_{q \in T} U_q/\mathbb{Z}_q^p = (\mathbb{Z}/p\mathbb{Z})^{\#T}$$

(see [Ko], §11.3). In particular, the automorphism $\tau_q$ restricts to a generator of the cyclic group $H_1(G_{\{q\}}(p), \mathbb{Z}/p\mathbb{Z})$. We use this fact for the definition of the linking numbers.

**Definition 2.1.** For two primes $q_i, q_j \in S$, the linking number $\ell_{ij} \in \mathbb{Z}/p\mathbb{Z}$ of $q_i$ and $q_j$ is defined by the formula

$$\sigma_{q_i} \equiv \tau_{q_j}^{\ell_{ij}} \mod G_{\{q_j\}}(p)^p$$

where, by abuse of notation, $\sigma_{q_i}$ and $\tau_{q_j}$, respectively, denote the images of $\sigma_{q_i} \in G_S(p)$ and $\tau_{q_j} \in G_S(p)$, respectively, in $G_{\{q_j\}}(p)$.

In other words, $\ell_{ij}$ is the image of the Frobenius automorphism $\sigma_{q_i}$ in $H_1(G_{\{q_i\}}(p), \mathbb{Z}/p\mathbb{Z})$ which we identify with $\mathbb{Z}/p\mathbb{Z}$ by means of its generator $\tau_{q_i}$. Note that $\ell_{ii} = 0$ for all $i = 1, \ldots, n$. The linking number $\ell_{ij}$ is independent of the choice of the uniformizer $\pi_{q_i}$ of $K_{q_i}$ (this follows
CIRCULAR SETS OF PRIMES OF IMAGINARY QUADRATIC NUMBER FIELDS 3

from the above isomorphism for the case $T = \{q_j\}$, but it depends on the choice of $\alpha_{q_i}$. If $\alpha_{q_i}$ would be replaced by $\alpha_{q_i}^s$, where $s$ is prime to $p$, then $\ell_{ij}$ would be multiplied by $s$. The defining equation of the linking number $\ell_{ij}$ is equivalent to

$$\hat{n}_{q_i} \equiv \alpha_{q_i}^{\ell_{ij}} \mod U_{\{q_j\}}^P K^\times,$$

which makes it possible to calculate the linking numbers in some examples, see section 3.

Let us pause here for a moment to explain the analogy to link theory. Assume we are given two disjoint knots $I$ and $J$ in $S^3$. Then the linking number $\text{lk}(I, J)$ is defined as follows. The knot $I$ is a loop in $S^3 - J$, hence it represents an element of $\pi_1(S^3 - J)$. After a choice of a generator of the infinite cyclic group $H_1(S^3 - J)$, $\text{lk}(I, J)$ is defined as the image of $I$ under the map

$$\pi_1(S^3 - J) \to \pi_1^{ab}(S^3 - J) \cong H_1(S^3 - J) \cong \mathbb{Z}.$$

In the number theoretical context described above, the linking number $\ell_{ij}$ is given by the image of the Frobenius automorphism $\sigma_i$ under the map

$$\pi_1^c(X - S) \to \pi_1^c(X - \{q_j\}) \to H_1(X - \{q_j\}, \mathbb{Z}/p\mathbb{Z}) = H_1(G_{\{q_i\}}(p), \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z},$$

where $X = \text{Spec}(\mathcal{O}_K)$ and we have chosen a generator of the cyclic group $H_1(X - \{q_j\}, \mathbb{Z}/p\mathbb{Z})$.

We denote by $\Gamma_S(p)$ the directed graph with vertices the primes of $S$ and a directed edge $q_i q_j$ from $q_i$ to $q_j$ if $\ell_{ij} \neq 0$. The graph $\Gamma_S(p)$, together with the $\ell_{ij}$ is called the linking diagram of $S$.

**Definition 2.2.** A finite set of primes of $K$ whose norm is congruent to 1 modulo $p$ is called strictly circular with respect to $p$ (and $\Gamma_S(p)$ a non-singular circuit) if there exists an ordering $S = \{q_1, \ldots, q_n\}$ of the primes in $S$ such that the following conditions are fulfilled:

1. The vertices $q_1, \ldots, q_n$ of $\Gamma_S(p)$ form a circuit $q_1 q_2 \ldots q_n q_1$.
2. If $i, j$ are both odd, then $q_i q_j$ is not an edge of $\Gamma_S(p)$.
3. $\ell_{12} \ell_{23} \ldots \ell_{n-1,n} \ell_{n1} \neq \ell_{1n} \ell_{21} \ldots \ell_{n,n-1}.$

We remark that condition (1) implies that $n$ is even and $\geq 4$. Note that condition (3) does not depend on the choice of the $\alpha_{q_i}$. It is satisfied if there exists an edge $q_i q_j$ of the circuit $q_1 q_2 \ldots q_n q_1$ such that $q_i q_j$ is not an edge of $\Gamma_S(p)$.

We will now show that $G$ has representation of Koch type.

**Proposition 2.3** (Koch). The group $G_S(p)$ has a presentation of Koch type, i.e. we have a minimal presentation $G_S(p) = F/R$ where $F$ is the free pro-$p$-group on generators $x_1, \ldots, x_n$, and $R$ is minimally generated as a normal subgroup of $F$ by relations $r_1, \ldots, r_n$ which are given modulo $F_{(3)}$ by

$$r_i \equiv x_i^{N(q_i)-1} \prod_{j=1}^n [x_i, x_j]^{\ell_{ij}} \mod F_{(3)}, \; i = 1, \ldots, n.$$

Here $F_{(3)}$ denotes the third step of the descending $p$-central series of $F$. 
Proof. We have already seen above that $G_S(p)$ has a minimal generating system consisting of the $n$ elements $r_{q_1}, \ldots, r_{q_n}$. The abelianization $G_S(p)^{ab}$ of $G_S(p)$ is a finitely generated abelian pro-$p$-group. If $G_S(p)^{ab}$ were infinite, it would have a quotient isomorphic to $\mathbb{Z}_p$, which corresponds to a $\mathbb{Z}_p$-extension $K_\infty$ of $K$ inside $K_S(p)$. By [NSW], Thm. 10.3.20(ii), a $\mathbb{Z}_p$-extension of $K$ is ramified at least one prime dividing $p$. This contradicts $K_\infty \subset K_S(p)$, hence $G_S(p)^{ab}$ is finite. In particular, $G_S(p)$ has at least as many relations as generators. From [NSW], 8.7.11 we obtain the inequality

$$\dim_{\mathbb{Z}/p\mathbb{Z}} H^1(G_S(p), \mathbb{Z}/p\mathbb{Z}) \geq \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}),$$

which implies that a minimal system of generators of $R$ as a normal subgroup of $F$ consists of $n$ elements. Such a system is given by the set of relations

$$r_i = x_i^{N(q_i)} [x_i, y_i], \quad i = 1, \ldots, n,$$

where $y_i \in F$ denotes a preimage of $\sigma_{q_i}$, see [Ko], §11.4. The definition of the $+\text{linking numbers}$ yields

$$y_i \equiv \prod_{j=1 \atop j \neq i}^n x_j^{\ell_{ij}} \mod F(2).$$

Hence we obtain

$$r_i \equiv x_i^{N(q_i)} [x_i, y_i] \equiv x_i^{N(q_i)} [x_i, \prod_{j=1 \atop j \neq i}^n x_j^{\ell_{ij}}] \equiv x_i^{N(q_i)} \prod_{j=1 \atop j \neq i}^n [x_i, x_j^{\ell_{ij}}] \mod F(3),$$

which finishes the proof. 

Since $G_S(p)$ is of Koch a type, a result of Labute, ([La], Thm. 1.6.), applies, which states that $G_S(p)$ is a mild pro-$p$-group if $S$ is strictly circular with respect to $p$. Then, in particular, $G_S(p)$ has cohomological dimension 2. We summarize our considerations in the following

**Theorem 2.4.** Let $p$ be an odd prime number and let $K$ be 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 $S = \{q_1, \ldots, q_n\}$ be a set of primes of $K$ whose norm is congruent to 1 mod $p$. Is $S$ is strictly circular with respect to $p$, then $G(K_S(p)/K)$ is a mild pro-$p$-group and hence of cohomological dimension 2.

3. Some examples

We use the same notation as in section 1. We let $S = \{q_1, \ldots, q_n\}$, and denote by $q_i$ the prime of $\mathbb{Z}$ lying below $q_i$.

We firstly consider the case where each $q_i$ is inert in $K/\mathbb{Q}$. Then $\pi_{q_i} = q_i$ is a uniformizer of $K_{q_i}$, and an element of $U_{q_i}$ for all primes $q \neq q_i$ of $K$. Hence, the idèle $\hat{q}_i$, when considered modulo $U_{q_i}U_{K}^{p}K^{\times}$, is equivalent to the idèle whose $q$-component is equal to 1 for $q \not\in S$ and $q = q_i$, and equal to $q_i^{-1}$ for $q \in S \setminus \{q_i\}$. This means that, after a choice of a generator $\alpha_{q_i}$ of $U_{q_i}/U_{q_i}^{p}$, $\ell_{ij}$ is given by

$$q_i = \alpha_{q_i}^{-\ell_{ij}} \mod U_{q_i}^{p}.$$
Equivalently, we can choose a primitive root \( \epsilon_j \) of \( \kappa_{q_j}^\times \), where \( \kappa_{q_j} \) denotes the residue field of \( q_j \). Then \( \ell_{ij} \) is the image in \( \mathbb{Z}/p\mathbb{Z} \) of any integer \( c \) satisfying
\[
q_i = \epsilon_j^{-c} \mod q_j.
\]
In particular, \( \ell_{ij} = 0 \) if and only if \( q_i \) is a \( p \)-th power modulo \( q_j \). This is equivalent to \( q_i \) being a \( p \)-th power modulo \( q_j \): if \( q_i \equiv x^p \mod q_j \) for some \( x \in \mathcal{O}_K \), then \( q_i^2 \equiv N_{K/Q}(x)^p \mod q_j \), and the claim follows. This implies in the case under consideration, that \( S = \{q_1, \ldots, q_n\} \) is strictly circular with respect to \( p \) if and only if \( S_Q = \{q_1, \ldots, q_n\} \) is strictly circular (over \( \mathbb{Q} \)) with respect to \( p \).

**Example 3.1.** (cf. the example after Thm 2.1 in [S]) Let \( K = \mathbb{Q}(\sqrt{-359}) \), \( p = 3 \). The class number of \( K \) equals 19. The prime numbers 7, 19, 61, 163 are inert in \( K/\mathbb{Q} \). We set
\[
q_1 = (61), \quad q_2 = (19), \quad q_3 = (163), \quad q_4 = (7)
\]
and \( S = \{q_1, q_2, q_3, q_4\} \). The linking diagram has the following shape:

Hence, \( S \) is a circular set of primes and \( \text{cd} \, G(K_S(3)/K) = 2 \).

In the calculations above we have made use of two things: the uniformizers \( \pi_{q_i} \) have been chosen in \( K^\times \), and \( \pi_{q_i} \) has been a unit in \( U_{q_i} \) for all \( q_i \in S \setminus \{q_1\} \).

Another case in which this is easily achieved is the case when the ideal class group of \( K \) is trivial. Then we can take a generator of \( q_j \) as the uniformizer \( \pi_{q_j} \) and \( \ell_{ij} \) can be obtained from the same equations as above with \( q_j \) replaced by \( \pi_{q_j} \).

**Example 3.2.** Let \( K = \mathbb{Q}(i) \), \( p = 3 \). We put
\[
q_1 = (2 + 15i), \quad q_2 = (4 + 15i), \quad q_3 = \overline{q}_1, \quad q_4 = \overline{q}_2
\]
and \( S = \{q_1, q_2, q_3, q_4\} \). Then we have \( q_1 = q_3 = 229, q_2 = q_4 = 241 \), and we set
\[
\pi_{q_1} = 2 + 15i, \quad \pi_{q_2} = 4 + 15i, \quad \pi_{q_3} = \overline{\pi}_{q_1}, \quad \pi_{q_4} = \overline{\pi}_{q_2}
\]
The linking diagram has the following shape:

Hence \( \text{cd} \, G(K_S(3)/K) = 2 \). Note that, by [Ko], Ex. 11.15, \( G(\mathbb{Q}_{\{q_1,q_2\}}(3)/\mathbb{Q}) \) is finite.
The last example raises the following question. There are no examples known of prime numbers $q_1$, $q_2$ congruent to 1 modulo $p$ where one can show that the cohomological dimension of $G(\mathbb{Q}(q_1,q_2))(p)/\mathbb{Q}$ equals 2. Is it possible to obtain such an example by considering strictly circular sets of primes \{q_1,q_2,\bar{q}_1,\bar{q}_2\} of an imaginary quadratic number field $K$ of class number one, in combination with some kind of descent argument? Unfortunately, the answer to this question is negative as the following considerations show.

Let $q_1$, $q_2$ be prime numbers congruent to 1 modulo $p$, and assume there exists an imaginary quadratic number field of class number one in which $q_1$, $q_2$ are completely decomposed:

$q_1\mathcal{O}_K = q_1q_3, \quad q_2\mathcal{O}_K = q_2q_4$.

This definition of the primes $q_i$ implies (for an appropriate choice of the primitive roots) the following equations for the linking numbers:

$\ell_{12} = \ell_{34}, \quad \ell_{23} = \ell_{41}, \quad \ell_{13} = \ell_{31}, \quad \ell_{24} = \ell_{42}$.

Since we want to avoid that the group $G(\mathbb{Q}(q_1,q_2))(p)/\mathbb{Q}$ is finite, we have to make sure that the conditions of [Ko], Ex. 11.15 are not fulfilled, and therefore we have in addition to assume that $q_1$ is a $p$-th power modulo $q_2$ and that $q_2$ is a $p$-th power modulo $q_1$. It is easily seen that this puts the following restraints on the linking numbers:

$\ell_{12} + \ell_{32} = 0, \quad \ell_{14} + \ell_{34} = 0, \quad \ell_{23} + \ell_{41} = 0, \quad \ell_{23} + \ell_{43} = 0$.

If $\rho_i$ denotes the initial form of the image of $r_i$ in the graded Lie algebra associated to the descending $p$-central series of $F$, the above conditions yield the equation

$\ell_{23}\rho_1 - \ell_{12}\rho_2 + \ell_{23}\rho_3 - \ell_{12}\rho_4 = 0$.

This means that the sequence $\rho_1,\ldots,\rho_4$ is not strongly free (cf. the definition of strong freeness in [La]), which implies, in particular, that the set \{q_1,q_2,q_3,q_4\} is not strictly circular, and this holds true as well if we make a different choice of the primitive roots.

4. Enlarging the set of primes

**Proposition 4.1.** Let $p$ be an odd prime number and 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 $S = \{q_1,\ldots,q_n\}$ be a set of primes of $K$ whose norm is congruent to 1 mod $p$. If $\text{cd} G(K_S(p)/K) \leq 2$, then the scheme $X = \text{Spec}(\mathcal{O}_K) - S$ is a $K(\pi,1)$ for the étale topology, i.e. for any discrete $p$-primary $G(K_S(p)/K)$-module $M$, considered as a locally constant étale sheaf on $X$, the natural homomorphism

$H^i(G(K_S(p)/K), M) \rightarrow H^i_{\text{ét}}(X, M)$

is an isomorphism for all $i$.

**Proof.** We put $G = G(K_S(p)/K)$. In the same way as in the proof of [S], Prop. 3.2., the Hochschild-Serre spectral sequence

$E_2^{pq} = H^p(G, H^q_{\text{ét}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z})) \Rightarrow H^{p+q}_{\text{ét}}(X, \mathbb{Z}/p\mathbb{Z})$,

where $\tilde{X}$ denotes the universal $p$-covering of $X$, implies isomorphisms

$H^i(G, \mathbb{Z}/p\mathbb{Z}) \cong H^i_{\text{ét}}(X, \mathbb{Z}/p\mathbb{Z}), \quad i = 0, 1$. 
and a short exact sequence

$$0 \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\phi} H^2_{et}(X, \mathbb{Z}/p\mathbb{Z}) \to H^2_{et}(\bar{X}, \mathbb{Z}/p\mathbb{Z})^G \to 0.$$  

We set $\bar{X} = \text{Spec} \mathcal{O}_K$. By the flat duality theorem of Artin-Mazur, ([Mi], III, Thm. 3.1), we have

$$H^3_{et}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) = \text{Hom}_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m) = 0$$

and

$$H^2_{et}(X, \mathbb{Z}/p\mathbb{Z})^\vee = \text{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m),$$

the latter group sitting in an exact sequence

$$0 \to \mathcal{O}^h_{K}/p \to \text{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m) \to p \text{Cl}(K) \to 0.$$  

Our assumptions on $K$ implies

$$H^2_{et}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) = 0.$$  

The excision sequence for the pair $(\bar{X}, X)$ yields an isomorphism

$$H^2_{et}(X, \mathbb{Z}/p\mathbb{Z}) = \bigoplus_{q \in S} H^3_{et}(\text{Spec} \mathcal{O}^h_q, \mathbb{Z}/p\mathbb{Z}),$$

where $\mathcal{O}^h_q$ denotes the henselization of the local ring of $\bar{X}$ at $q$. The local duality theorem ([Mi], II, Thm. 1.8) gives

$$H^3_{et}(\text{Spec} \mathcal{O}^h_q, \mathbb{Z}/p\mathbb{Z}) \cong \text{Hom}_{\text{Spec} \mathcal{O}^h_q}(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m)^\vee.$$  

As we have assumed that for all $q \in S$, the norm of $q$ is congruent to 1 modulo $p$, we obtain $\dim_{\mathbb{Z}/p\mathbb{Z}} H^2_{et}(X, \mathbb{Z}/p\mathbb{Z}) = n$. Hence, by the proof of Lemma 2.3, $\phi$ is an isomorphism, and therefore

$$H^2_{et}(\bar{X}, \mathbb{Z}/p\mathbb{Z})^G = 0.$$  

The proof is then concluded as in [S], Prop. 3.2. $\square$

**Theorem 4.2.** Let $p$ be an odd prime number and let $K$ be 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 $p$. Assume that $\text{cd} G(K_S(p)/K) = 2$. Let $l \notin S$ be a prime whose norm is congruent to 1 modulo $p$, and which does not split completely in the extension $K_S(p)/K$. Then

$$\text{cd} G(K_{S \cup \{l\}}(p)/K) = 2.$$  

**Proof.** The proof is the same as the proof of [S], Thm. 2.3, we just have to replace Prop. 3.2. of (loc.cit.) by Prop. 4.1. above. $\square$

**Corollary 4.3.** Assume that $S$ contains a strictly circular subset $T$ such for each $q \in S \setminus T$ there exists an edge from $q$ to a prime of $T$. Then $\text{cd}(G(K_S(p)/K)) = 2$.

**Proof.** We only need to remark that if we are given a prime $q \in S$ such that the linking number of $q$ and a certain prime $l$ of $T$ is nontrivial, then $q$ does not split completely in $K_T(p)/K$. To see this, we fix an extension $\mathcal{Q}$ of $q$ to $L = K_{\{l\}}(p)^{ab}$. Since the linking number of $q$ and $l$ is nontrivial, the Frobenius of $\mathcal{Q}$ in $L/K$ generates the whole Galois group $G(L/K) \cong \mathbb{Z}/p\mathbb{Z}$. Hence $q$ does not split completely in $L/K$, which proves the claim. $\square$
Example 4.4. Let $K = \mathbb{Q}(\sqrt{-359})$, $p = 3$. The prime number $l = 113$ is inert in $K/\mathbb{Q}$, and if we put $q_5 = l \mathcal{O}_K$, and $S = \{q_1, q_2, q_3, q_4\}$ where $q_1, q_2, q_3, q_4$ are given as in Example 3.1, the linking diagram looks as follows:

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{linking_diagram.png}
\end{figure}

Hence, by Cor. 4.3 we have $cd G(K_S(p)/K) = 2$ (although $S$ is not strictly circular with respect to $p$).

Example 4.5. Let $K = \mathbb{Q}(\sqrt{-359})$, $p = 3$ and $S = \{q_1, q_2, q_3, q_4\}$, where $q_1, q_2, q_3, q_4$ are given as in Example 3.1. Let $l = (37, 14 + \sqrt{-359})$. Note that $l|37$, and 37 is completely decomposed in $K/\mathbb{Q}$. The unique subfield $L$ of degree 3 over $K$ of the extension $K(\mu_7)/K$, and the prime $l$ of $K$ is inert in $L$. Therefore, we obtain by Thm. 4.2 that $cd G(K_S,p)/K) = 2$.

Another result from [S] which carries over to our situation with identical proof is given by the following theorem.

**Theorem 4.6.** Let $p$ be an odd prime number and let $K$ be 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 $p$. Assume that $G(K_S(p)/K) \neq 1$ and $cd G(K_S(p)/K) \leq 2$. Then $scd G(K_S(p)/K) = 3$ and $G(K_S(p)/K)$ is a pro-$p$ duality group.

**References**


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