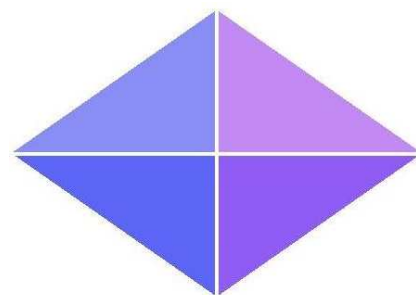


DFG-Forschergruppe
Regensburg/Leipzig
Algebraische Zyklen und
L-Funktionen



Circular sets of primes of imaginary
quadratic number fields

Denis Vogel

Preprint Nr. 05/2006

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 $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ be a set of primes of K whose

Date: July 18, 2007.

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 $\mathfrak{q} \in T$ are 1 and for $\mathfrak{q} \notin T$ are units. For $\mathfrak{q} \in S$ we denote by $K_{\mathfrak{q}}$ the completion of K at $\mathfrak{q}$ and by $U_{\mathfrak{q}}$ the unit group of $K_{\mathfrak{q}}$. Furthermore, let $\pi_{\mathfrak{q}}$ be a uniformizer of $K_{\mathfrak{q}}$ and let $\alpha_{\mathfrak{q}}$ be a generator of the cyclic group $U_{\mathfrak{q}}/U_{\mathfrak{q}}^p$. Let Ω be an extension of $\mathfrak{q}$ to $K_S(p)$. We let $\sigma_{\mathfrak{q}}$ be an element of $G_S(p)$ with the following properties:

- (1) $\sigma_{\mathfrak{q}}$ is a lift of the Frobenius automorphism of Ω ;
- (2) 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.

Let $\tau_{\mathfrak{q}}$ denote an element of $G_S(p)$ such that

- (1) $\tau_{\mathfrak{q}}$ is an element of the inertia group T_{Ω} of Ω in $K_S(p)/K$;
- (2) the restriction of $\tau_{\mathfrak{q}}$ to $\tilde{K}/K$ equals $(\hat{\alpha}_{\mathfrak{q}}, \tilde{K}/K)$, where $\hat{\alpha}_{\mathfrak{q}}$ denotes the idèle whose $\mathfrak{q}$ -component equals $\alpha_{\mathfrak{q}}$ and all other components are equal to 1.

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

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

Let V_T denote the Kummer group

$$V_T = \{a \in K^{\times} \mid a \in K_{\mathfrak{q}}^{\times p} \text{ for } \mathfrak{q} \in T \text{ and } a \in U_{\mathfrak{q}} K_{\mathfrak{q}}^{\times p} \text{ for } \mathfrak{q} \notin T\}$$

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

$$0 \rightarrow \mathcal{O}_K^{\times}/p \rightarrow V_{\emptyset}(K) \rightarrow {}_p\text{Cl}(K) \rightarrow 0.$$

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

$$I_K/(U_T I_K^p K^{\times}) \cong U_{\emptyset}/U_T U_{\emptyset}^p = \prod_{\mathfrak{q} \in T} U_{\mathfrak{q}}/U_{\mathfrak{q}}^p = (\mathbb{Z}/p\mathbb{Z})^{\#T}$$

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

Definition 2.1. 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

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

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

In other words, ℓ_{ij} is the image of the Frobenius automorphism $\sigma_{\mathfrak{q}_i} \in G_S(p)$ 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 $i = 1, \dots, n$. 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

$$\hat{\pi}_{\mathfrak{q}_i} \equiv \hat{\alpha}_{\mathfrak{q}_j}^{\ell_{ij}} \pmod{U_{\{\mathfrak{q}_j\}} I_K^p K^\times}$$

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

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

In the number theoretical context described above, the linking number ℓ_{ij} is given by the image of the Frobenius automorphism σ_i under the map

$$\begin{aligned} \pi_1^{et}(X - S) &\twoheadrightarrow \pi_1^{et}(X - \{\mathfrak{q}_j\}) \twoheadrightarrow H_1(X - \{\mathfrak{q}_j\}, \mathbb{Z}/p\mathbb{Z}) = H_1(G_{\{\mathfrak{q}_j\}}(p), \mathbb{Z}/p\mathbb{Z}) \\ &\cong \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

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

We denote by $\Gamma_S(p)$ the directed graph with vertices the primes of S and a directed edge $\mathfrak{q}_i \mathfrak{q}_j$ from $\mathfrak{q}_i$ to $\mathfrak{q}_j$ if $\ell_{ij} \neq 0$. The graph $\Gamma_S(p)$, together with the ℓ_{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 $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ of the primes in S such that the following conditions are fulfilled:

- (1) The vertices $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ of $\Gamma_S(p)$ form a circuit $\mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_n \mathfrak{q}_1$.
- (2) If i, j are both odd, then $\mathfrak{q}_i \mathfrak{q}_j$ is not an edge of $\Gamma_S(p)$.
- (3) $\ell_{12} \ell_{23} \dots \ell_{n-1, n} \ell_{n1} \neq \ell_{1n} \ell_{21} \dots \ell_{n, n-1}$.

We remark that condition (1) implies that n is even and ≥ 4 . Note that condition (3) does not depend on the choice of the $\alpha_{\mathfrak{q}_j}$. It is satisfied if there exists an edge $\mathfrak{q}_i \mathfrak{q}_j$ of the circuit $\mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_n \mathfrak{q}_1$ such that $\mathfrak{q}_j \mathfrak{q}_i$ 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 $x_1, \dots, x_n$, and R is minimally generated as a normal subgroup of F by relations $r_1, \dots, r_n$ which are given modulo $F_{(3)}$ by

$$r_i \equiv x_i^{N(\mathfrak{q}_i)-1} \prod_{\substack{j=1 \\ j \neq i}}^n [x_i, x_j]^{\ell_{ij}} \pmod{F_{(3)}}, \quad i = 1, \dots, n.$$

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 $\tau_{q_1}, \dots, \tau_{q_n}$. 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_∞ of K inside $K_S(p)$. By [NSW], Thm. 10.3.20(ii), a $\mathbb{Z}_p$ -extension of K is ramified at 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

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

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

$$y_i \equiv \prod_{\substack{j=1 \\ j \neq i}}^n x_j^{\ell_{ij}} \pmod{F_{(2)}}.$$

Hence we obtain

$$r_i \equiv x_i^{N(q_i)-1} [x_i, y_i] \equiv x_i^{N(q_i)-1} [x_i, \prod_{\substack{j=1 \\ j \neq i}}^n x_j^{\ell_{ij}}] \equiv x_i^{N(q_i)-1} \prod_{\substack{j=1 \\ j \neq i}}^n [x_i, x_j]^{\ell_{ij}} \pmod{F_{(3)}},$$

which finishes the proof. $\square$

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 $S = \{q_1, \dots, q_n\}$ 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 $S = \{q_1, \dots, q_n\}$, 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 for all primes $q \neq q_i$ of K . Hence, the idèle $\hat{\pi}_{q_i}$, when considered modulo $U_{\{q_j\}}^p I_K^p K^\times$, is equivalent to the idèle whose q -component is equal to 1 for $q \neq q_j S$ and equal to q_i^{-1} for $q = q_j$. This means that, after a choice of a generator α_{q_j} of $U_{q_j}/U_{q_j}^p$, ℓ_{ij} is given by

$$q_i = \alpha_{q_j}^{-\ell_{ij}} \pmod{U_{q_j}^p}.$$

Equivalently, we can choose a primitive root ϵ_j of $\kappa_{\mathfrak{q}_j}^\times$, where $\kappa_{\mathfrak{q}_j}$ denotes the residue field of $\mathfrak{q}_j$. Then ℓ_{ij} is the image in $\mathbb{Z}/p\mathbb{Z}$ of any integer c satisfying

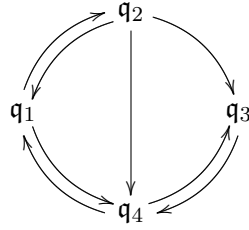
$$q_i = \epsilon_j^{-c} \pmod{\mathfrak{q}_j}.$$

In particular, $\ell_{ij} = 0$ if and only if q_i is a p -th power modulo $\mathfrak{q}_j$. This is equivalent to q_i being a p -th power modulo q_j : if $q_i \equiv x^p \pmod{\mathfrak{q}_j}$ for some $x \in \mathcal{O}_K$, then $q_i^2 \equiv N_{K/\mathbb{Q}}(x)^p \pmod{q_j}$, and the claim follows. This implies in the case under consideration, that $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ is strictly circular with respect to p if and only if $S_{\mathbb{Q}} = \{q_1, \dots, q_n\}$ 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

$$\mathfrak{q}_1 = (61), \quad \mathfrak{q}_2 = (19), \quad \mathfrak{q}_3 = (163), \quad \mathfrak{q}_4 = (7)$$

and $S = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$. 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 $\pi_{\mathfrak{q}_i}$ have been chosen in $K^\times$, and $\pi_{\mathfrak{q}_i}$ has been a unit in $U_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{q}_i\}$. 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 $\mathfrak{q}_j$ as the uniformizer $\pi_{\mathfrak{q}_j}$ and ℓ_{ij} can be obtained from the same equations as above with q_j replaced by $\pi_{\mathfrak{q}_j}$.

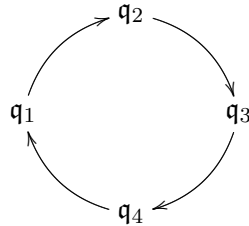
Example 3.2. Let $K = \mathbb{Q}(i)$, $p = 3$. We put

$$\mathfrak{q}_1 = (2 + 15i), \quad \mathfrak{q}_2 = (4 + 15i), \quad \mathfrak{q}_3 = \bar{\mathfrak{q}}_1, \quad \mathfrak{q}_4 = \bar{\mathfrak{q}}_2$$

and $S = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$. Then we have $q_1 = q_3 = 229$, $q_2 = q_4 = 241$, and we set

$$\pi_{\mathfrak{q}_1} = 2 + 15i, \quad \pi_{\mathfrak{q}_2} = 4 + 15i, \quad \pi_{\mathfrak{q}_3} = \bar{\pi}_{\mathfrak{q}_1}, \quad \pi_{\mathfrak{q}_4} = \bar{\pi}_{\mathfrak{q}_2}$$

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 $\{\mathfrak{q}_1, \mathfrak{q}_2, \bar{\mathfrak{q}}_1, \bar{\mathfrak{q}}_2\}$ 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:

$$q_1 \mathcal{O}_K = \mathfrak{q}_1 \mathfrak{q}_3, \quad q_2 \mathcal{O}_K = \mathfrak{q}_2 \mathfrak{q}_4.$$

This definition of the primes $\mathfrak{q}_i$ 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:

$$\ell_{12} + \ell_{32} = 0, \quad \ell_{14} + \ell_{34} = 0, \quad \ell_{21} + \ell_{41} = 0, \quad \ell_{23} + \ell_{43} = 0.$$

If ρ_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 $\rho_1, \dots, \rho_4$ is not strongly free (cf. the definition of strong freeness in [La]), which implies, in particular, that the set $\{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$ 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 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 $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ 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*

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

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

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

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

$$H^i(G, \mathbb{Z}/p\mathbb{Z}) \cong H_{\text{ét}}^i(X, \mathbb{Z}/p\mathbb{Z}), \quad i = 0, 1$$

and a short exact sequence

$$0 \rightarrow H^2(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\phi} H_{et}^2(X, \mathbb{Z}/p\mathbb{Z}) \rightarrow H_{et}^2(\tilde{X}, \mathbb{Z}/p\mathbb{Z})^G \rightarrow 0.$$

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

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

and

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

the latter group sitting in an exact sequence

$$0 \rightarrow \mathcal{O}_K^\times/p \rightarrow \text{Ext}_{\bar{X}}^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m) \rightarrow {}_p\text{Cl}(K) \rightarrow 0.$$

Our assumptions on K implies

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

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

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

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

$$H_{\{\mathfrak{q}\}}^3(\text{Spec } \mathcal{O}_{\mathfrak{q}}^h, \mathbb{Z}/p\mathbb{Z}) \cong \text{Hom}_{\text{Spec } \mathcal{O}_{\mathfrak{q}}^h}(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m)^\vee.$$

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

$$H_{et}^2(\tilde{X}, \mathbb{Z}/p\mathbb{Z})^G = 0.$$

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 1 mod p . Assume that $\text{cd } G(K_S(p)/K) = 2$. Let $\mathfrak{l} \notin S$ 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*

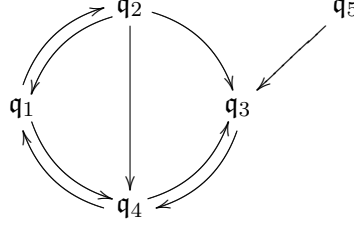
$$\text{cd } G(K_{S \cup \{\mathfrak{l}\}}(p)/K) = 2.$$

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 $\mathfrak{q} \in S \setminus T$ there exists an edge from $\mathfrak{q}$ 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 $\mathfrak{q} \in S$ such that the linking number of $\mathfrak{q}$ and a certain prime $\mathfrak{l}$ of T is nontrivial, then $\mathfrak{q}$ does not split completely in $K_T(p)/K$. To see this, we fix an extension $\mathfrak{Q}$ of $\mathfrak{q}$ to $L = K_{\{\mathfrak{l}\}}(p)^{ab}$. Since the linking number of $\mathfrak{q}$ and $\mathfrak{l}$ is nontrivial, the Frobenius of $\mathfrak{Q}$ in L/K generates the whole Galois group $G(L/K) \cong \mathbb{Z}/p\mathbb{Z}$. Hence $\mathfrak{q}$ 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 $\mathfrak{q}_5 = l\mathcal{O}_K$, and $S = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4, \mathfrak{q}_5\}$ where $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4$ are given as in Example 3.1, the linking diagram looks as follows:



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

Example 4.5. Let $K = \mathbb{Q}(\sqrt{-359})$, $p = 3$ and $S = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$, where $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4$ are given as in Example 3.1. Wet set $\mathfrak{l} = (37, 14 + \sqrt{-359})$. Note that $\mathfrak{l} \nmid 37$, and 37 is completely decomposed in $K/\mathbb{Q}$. The unique subfield L of degree 3 over K of the extension $K(\mu_7)/K$ is a subfield of $K_S(p)/K$, and the prime $\mathfrak{l}$ of K is inert in L . Therefore, we obtain by Thm. 4.2 that $\text{cd } G(K_{S \cup \{\mathfrak{l}\}}(p)/K) = 2$.

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 $\text{cd } G(K_S(p)/K) \leq 2$. Then $\text{scd } G(K_S(p)/K) = 3$ and $G(K_S(p)/K)$ is a pro- p duality group.

REFERENCES

- [Ko] Koch, H.: *Galoissche Theorie der p -Erweiterungen*. Deutscher Verlag der Wiss., 1970 (English translation Berlin 2002)
- [La] Labute, J.: *Mild Pro- p -Groups and Galois Groups of p -Extensions of $\mathbb{Q}$* (to appear in J. Reine Angew. Math.)
- [NSW] Neukirch, J., Schmidt, A., Wingberg, K.: *Cohomology of number fields*. Springer 2000
- [Mi] Milne, J.: *Arithmetic duality theorems*. Academic Press 1986
- [S] Schmidt, A.: *Circular sets of prime numbers and p -extensions of the rationals*. (to appear in J. Reine Angew. Math.)

Denis Vogel

NWF I - Mathematik, Universität Regensburg

93040 Regensburg

Deutschland

email: denis.vogel@mathematik.uni-regensburg.de