OUKA
Osaka University Knowledge Archive

Title	On maximal tamely ramified pro-2-extensions over the cyclotomic Z2-extension of an imaginary quadratic field
Author(s)	Salle, Landry
Citation	Osaka Journal of Mathematics. 2010, 47(4), p. 921-942
Version Type	VoR
URL	https://doi.org/10.18910/8221
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Salle, L.
Osaka J. Math.
47 (2010), 921–942

ON MAXIMAL TAMELY RAMIFIED PRO-2-EXTENSIONS OVER THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF AN IMAGINARY QUADRATIC FIELD

LANDRY SALLE

(Received June 23, 2008, revised June 1, 2009)

Abstract

In [7], Yasushi Mizusawa gives computations which lead to a pro-2-presentation of the Galois group of the maximal unramified pro-2-extension of the cyclotomic $\mathbb{Z}_2$-extension over some imaginary quadratic fields, with low λ-invariants. We show that these methods can be applied to some maximal tamely ramified pro-2-extensions, depending on the quadratic imaginary field, and the condition of ramification.

Introduction

In [7], Mizusawa considers the following problem: given an imaginary quadratic number field k, and k_∞ its cyclotomic $\mathbb{Z}_2$-extension, can we compute a pro-2-presentation of the Galois group of the maximal unramified pro-2-extension over k_∞? Results of Ferrero ([1]) and Kida ([4]) give the maximal abelian quotient of these groups, that is, the Galois group of the maximal unramified abelian pro-2-extension of k_∞. It is computed as an Iwasawa module. Using these results, computations of some other Iwasawa modules, and group-theoretical results such as Proposition 3.2 below, Mizusawa is able to find the wanted presentation in some non-trivial (i.e. non-abelian) cases with low λ-invariant (namely $\lambda \in \{1, 2\}$). One ingredient in his computations is that Iwasawa modules over k_∞ that he considers have non-trivial torsion part. According to Ferrero and Kida's results, it can occur only if the prime 2 ramifies in the extension $k/\mathbb{Q}$.

We show in this paper that Mizusawa's method can be applied as well for the Galois group of maximal S-ramified pro-2-extension over k_∞, where S is the set of primes in k_∞ over a finite set of odd prime numbers in $\mathbb{Q}$ (hence, we consider the Galois group of a tamely ramified extension). The main result is the following:

Theorem 1. *Let p and q be two prime numbers respectively congruent to* 5 *and* 3 *modulo* 8, *and put $S = \{q\}$. Let k be the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$, and $\mathcal{G} = \mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$ the Galois group of the maximal S-ramified pro-2-extension of k_∞. Then $\mathcal{G}$ has rank* 2, *its abelianization is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}_2$-module,*

2000 Mathematics Subject Classification. Primary 11R23; Secondary 11R18.

and admits as a presentation:

$$\langle a, b \mid [a, b]a^2 \rangle,$$

where $[a, b]$ *denotes the commutator* $a^{-1}b^{-1}ab$. *The same holds if we assume* $p \equiv 3 \bmod 8$ *and* $q \equiv 5 \bmod 8$.

The first section of our paper is devoted to fixing notations and recalling useful known results. In the second section we extend results of Ferrero and Kida to find S-ramified Iwasawa module $X_S(k_\infty)$ over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field k. The description depends on the S-ramified Iwasawa module over $\mathbb{B}_\infty$, the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. We are not able to give the general description of that module, but we exhibit a few infinite families of sets S for which it is trivial or cyclic of small order. A fact to be noticed is that $X_S(k_\infty)$ can have non-trivial torsion part even if 2 does not ramify in $k/\mathbb{Q}$. Using Mizusawa's method we finally prove Theorem 1 in Section 3. Note that it is about Galois groups whose abelianizations are $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, hence with $\lambda = 1$. We do not consider cases with $\lambda = 2$. We will also quickly restrict ourselves to the case $k \neq \mathbb{Q}(i)$, since dealing with roots of unity would require special arguments.

As an application of this result, we compute Galois groups of the maximal S-ramified pro-2-extension over the layers k_n of the cyclotomic $\mathbb{Z}_2$-extension of k, the so-called S-ray 2-class field tower (Theorems 3.8 and 3.11). These results and their proofs are again inspired by Mizusawa's paper: see Proposition 4.3 in [7].

We mention that numerous computations have been done using the (free) system PARI/GP: visit `http://pari.math.u-bordeaux.fr/`.

1. Preliminaries.

1.1. Notations. Let S and D be two finite sets of odd prime numbers in $\mathbb{Q}$. We will mainly consider the imaginary quadratic field $k = \mathbb{Q}\left(\sqrt{-\prod_{p_i \in D} p_i}\right)$ and various extensions of it. For each number field K, we denote by $S(K)$ the set of places in K which are above places in S. When no confusion is possible, we will omit K.

For any place v in K, let $\mathfrak{k}_v^\times$ be the pro-2-completion of the multiplicative group of the residue class field of K at the place v (i.e., the 2-Sylow, since it is a cyclic group).

The notation $\mathcal{C}\ell(K)$, or simply $\mathcal{C}\ell$, stands for the ideal class group in the number field K, and $\mathcal{C}\ell_{\mathcal{M}}$ for the ray class group associated to the modulus $\mathcal{M}$. All the class groups that we consider are taken in the ordinary sense which means that archimedean places do not complexify in the corresponding class field extensions.

Let $\mathcal{M}$ be a modulus whose support is included in $S(K)$ for some K. In particular, if $\mathcal{M}_0 = \prod_{v \in S} \mathfrak{p}_v$, and if $\mathcal{M}$ is such that $\mathcal{M}_0 \mid \mathcal{M}$, then the 2-Sylow of the ray class groups are such that $A_{\mathcal{M}} = A_{\mathcal{M}_0}$ (see Proposition 1.2 below). In such a situation, we omit the modulus and denote by A_S that 2-Sylow. When S is empty, we omit the subscript; in particular, A is the 2-Sylow of $\mathcal{C}\ell$.

D_S denotes the subgroup of A_S generated by the places above 2; in particular $D \subset A$ (no confusion with the discriminant of the quadratic number field seems possible). Then A'_S is the quotient group A_S/D_S (it corresponds via class field theory to the maximal 2-split S-ramified abelian 2-extension).

Following [9], Section 7.3, we write $\mathbb{B}_n$ for the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, and K_n its compositum with any number field K. Taking inverse limits of various class groups according to norm maps from K_m to K_n for $m \geq n$, we obtain the so-called Iwasawa modules. For instance: $X(K_\infty) = \varprojlim A(K_n)$, $X'(K_\infty) = \varprojlim A'(K_n)$, $X_S(K_\infty) = \varprojlim A_S(K_n)$ and $X'_S(K_\infty) = \varprojlim A'_S(K_n)$, $\varprojlim D(K_n)$ and $\varprojlim D_S(K_n)$. Note that in general the Iwasawa module depends on the first layer of the $\mathbb{Z}_p$-extension we consider, and not only on K_∞. However, in our examples, they will be independent, and thus our notation will fit.

The notation E stands for the group of (global) units, $E_{\mathcal{M}}$ for the subgroup of units which are congruent to 1 modulo $\mathcal{M}$. Similarly, E' denotes the group of 2-units and $E'_{\mathcal{M}}$ the subgroup of 2-units which are congruent to 1 modulo $\mathcal{M}$. Then we define $\mathcal{E} = E \otimes_{\mathbb{Z}} \mathbb{Z}_2$ and $\mathcal{E}' = E' \otimes_{\mathbb{Z}} \mathbb{Z}_2$. Since the set S contains only finite non-2-places, we can define $\mathcal{E}_S$ as $E_{\mathcal{M}} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ for any modulus $\mathcal{M}$ built on S and divisible by $\prod_{v \in S} \mathfrak{p}_v$ (see Proposition 1.2 below). The same holds for $\mathcal{E}'_S$.

Let T be either the empty set or the set of places above 2. We use T as a superscript for unit groups and class groups: for instance $\mathcal{E}_S^T$, A_S^T denote either $\mathcal{E}_S$ and A_S, or $\mathcal{E}'_S$ and A'_S, according whether T is the empty set or the set of places above 2.

1.2. Some known results. Let us recall without proof some classical results which will be used several times. First, we state a well-known result from Iwasawa theory, which is a special case of Nakayama's lemma (see for example [2], Theorem 1).

Lemma 1.1. *Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of the number field K. Assume that all primes above p in K are totally ramified in K_∞/K. Let S be a finite set of finite primes in K, which are not above p. Take T to be either the empty set or the set of places above p in k.*

If $A_S^T(K_n) = A_S^T(K_{n+1})$ for some layer K_n, then $X_S^T(K_\infty) = A_S^T(K_n)$.

Assume moreover that there is only one prime above p in K. Then $X_S^T(K_\infty)$ is trivial if and only if $A_S^T(K)$ is trivial.

The following statement is a pro-2-completion of Theorem 4.5 in Part I of [3]. It will be used to compute S-ramified Iwasawa modules from unramified ones.

Proposition 1.2. *Let K be a number field. Let T be either the empty set or the set of places above 2. We recall that $\mathfrak{k}_v^\times$ denotes the pro-2-completion of the multi-*

plicative group of the residue class field of K at the place v. Then, there is an exact sequence:

$$1 \to \mathcal{E}^T(K)/\mathcal{E}_S^T(K) \to \prod_{v \in S(K)} \mathfrak{k}_v^\times \to \ker(A_S^T(K) \to A^T(K)) \to 1.$$

It yields the following equality:

$$\#A_S^T(K) = \#A^T(K) \frac{{}_2\phi(\mathcal{M})}{[\mathcal{E}^T(K) : \mathcal{E}_S^T(K)]},$$

where ${}_2\phi$ denotes the 2*-part of the generalized Euler function, and $\mathcal{M}$ is any modulus whose support is S and divisible by $\mathcal{M}_0 = \prod_{v \in S(K)} \mathfrak{p}_v$.*

Now we recall (a form of) the so-called genus formula which gives some information on the class group in a field L depending on the class group of a subfield K, on ramification in L/K and on norms of units (see for instance [3], Part IV, Theorems 4.2 and 4.4 for the related exact sequence, and the beginning of section 4 for a sample of references).

Proposition 1.3. *Let L/K be a cyclic extension of number fields of degree* 2*, and denote by Δ the Galois group* $\mathrm{Gal}(L/K)$*. Assume that L/K is disjoint from the S-ray* 2*-class field of K. Take T to be either the empty set or the set of places above* 2*. Then we have*:

$$\#A_S^T(L)^\Delta = \#A_S^T(K) \frac{\prod_{v \notin S \cup T} e_v \prod_{v \in T} e_v f_v}{2[\mathcal{E}_S^T(K) : \mathcal{E}_S^T(K) \cap N(\mathcal{J}_L)]},$$

where $N(\mathcal{J}_L)$ denotes the image by the norm map of the idele group of L, and where e_v and f_v denote respectively the ramification index and the inertia degree of the place v in L/K.

We will mainly use this formula in conjunction with the following well-known lemma:

Lemma 1.4. *With the notations of* Proposition 1.3*, assume moreover that $A_S^T(K)$ is trivial. Then, the quantity* $\log_2(\#A_S^T(L)^\Delta)$ *equals the number of generators of $A_S^T(L)$.*

Proof. Note that the non-trivial element σ of Δ acts by inversion on $A_S^T(L)$. Indeed, for each $\mathfrak{a}$, $\mathfrak{a}^{\sigma+1}$ can be seen as an element of $A_S^T(K)$, which is trivial by assumption. So $\mathfrak{a}^{\sigma+1}$ is in the same class as some principal ideal. The generator is still congruent to 1 modulo $S(L)$, hence $\mathfrak{a}^{\sigma+1}$ is trivial as well in $A_S^T(L)$. It implies that the Δ-invariants of the group $A_S^T(L)$ are exactly its elements of order lower than 2, and the result follows. □

Now we give a version of Hasse's theorem on units in CM-extensions (see [9], Theorem 4.12) for units and 2-units in layers of the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field:

Lemma 1.5. *Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, with $d \neq 1$ odd. Then the quotient group $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ is trivial. Moreover, if 2 does not split in $k/\mathbb{Q}$, the groups of 2-units $\mathcal{E}'(\mathbb{B}_n)$ and $\mathcal{E}'(k_n)$ are equal. If 2 splits in $k/\mathbb{Q}$, the quotient group $\mathcal{E}'(k_n)/\mathcal{E}'(\mathbb{B}_n)$ is infinite cyclic.*

If $k = \mathbb{Q}(i)$, then the quotient group $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ is cyclic of order 2^{n+1}, generated by a primitive 2^{n+2}-th root of unity, and the quotient group $\mathcal{E}'(k_n)/\mathcal{E}'(\mathbb{B}_n)$ is isomorphic to the direct product of $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ by a group of order 2.

Proof. See the proof of Theorem 5 in [1] if 2 ramifies in $k/\mathbb{Q}$ (the case where 2 is inert is essentially the same), and the proof of Theorem 6 if 2 splits.

For the case of $\mathbb{Q}(i)$ see for example Theorem 2 in [1] for the first assertion. The second one follows easily. □

The following lemma is an easy generalisation of a classical fact (see [9], Theorem 10.3 for instance) on capitulation in a CM-extension:

Lemma 1.6. *Let K be a CM-field, whose maximal real subfield we denote by K^+. Whenever S contains at least one finite place of K^+, not lying above 2, the (capitulation) kernel of the natural map $A_S(K^+) \to A_S(K)$ is trivial. If S is empty then this capitulation kernel has order 1 or 2.*

Moreover, if no place above 2 splits in K/K^+, then the same holds for $A'_S(K^+) \to A'_S(K)$.

Proof. The proof is as in the S-empty case in [9]. Let $\mathcal{M}$ be any modulus built on S divisible by at least one non-2-place of $S(K^+)$. We define $W_{\mathcal{M}}(K)$ as the set of roots of unity in K equivalent to 1 mod $\mathcal{M}$, and $W_0(K)$ as the subset of roots of unity of the form $\sigma u/u$ where u is a unit in K, and σ denotes the non-trivial element of $\mathrm{Gal}(K/K^+)$. Let us consider the map

$$\ker(\mathcal{C}\ell_{\mathcal{M}}(K^+) \to \mathcal{C}\ell_{\mathcal{M}}(K)) \to W_{\mathcal{M}}(K)/W_0(K),$$

defined as follows: given an ideal $\mathfrak{a}$ of K^+, prime to S, which capitulates in $\mathcal{C}\ell_S(K)$, the image of this ideal is $\sigma\alpha/\alpha$, where $\mathfrak{a}\mathcal{O}_K = (\alpha)$, with $\alpha \equiv 1 \bmod \mathcal{M}$. Since S is a set of places in K^+, the congruence $\sigma\alpha \equiv 1 \bmod \mathcal{M}$ holds as well. We deduce that $\sigma\alpha/\alpha \equiv 1 \bmod \mathcal{M}$. We can check that this element is indeed a root of unity, and that this map is injective, as in the S-empty case.

Then we notice that $W_0(K)$ contains $W_{\mathcal{M}}(K)^2$, and that if S contains one finite place v lying above an odd prime p, the only roots of unity which can be equivalent

to 1 modulo v are the p^n-th for $n \geq 0$, so that $W_{\mathcal{M}}(K) \subset \mu_{p^\infty}$, and the square map is an isomorphism in this group. Then the target of the previous map is trivial. Hence, for each sufficiently large modulus $\mathcal{M}$, the natural map from $\mathcal{C}\ell_{\mathcal{M}}(K^+)$ is into $\mathcal{C}\ell_{\mathcal{M}}(K)$, so the same holds for $\mathcal{C}\ell_S(K^+) \to \mathcal{C}\ell_S(K)$, and for the 2-Sylow.

The same proof holds when dealing with $A'_S(K^+) \to A'_S(K)$: the only point to be modified is that in the definition of

$$\ker(\mathcal{C}\ell_{\mathcal{M}}(K^+) \to \mathcal{C}\ell_{\mathcal{M}}(K)) \to W_{\mathcal{M}}(K)/W_0(K),$$

the ideal $\mathfrak{a}\mathcal{O}_K$ is to be written as $(\alpha)\mathfrak{p}$ where $\mathfrak{p}$ is an ideal above 2. Under the assumption that no place above 2 splits in K/K^+, the ideal $\mathfrak{p}$ is invariant under σ, and so is $\mathfrak{a}\mathcal{O}_K$, hence $\sigma\alpha/\alpha$ is a unit, and a root of unity as in [9] Theorem 10.3. The end of the proof is the same. □

2. Computation of Iwasawa modules

The main result of this section is the following:

Theorem 2.1. *Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, with d an odd integer. Let D be the set of prime numbers which divide d, and let S be a set of odd prime numbers in $\mathbb{Q}$. For any odd prime number p, let $2^{k'_p}$ be the largest 2-power dividing $p^2 - 1$. Take $T = \emptyset$ or $T = \mathrm{Pl}_2(k)$.*

Then the λ-invariant of the Iwasawa module $X_S^T(k_\infty)$ is:

$$\lambda_S^T(k_\infty) = \#(S \cup D)(\mathbb{B}_\infty) + \lambda_S^T(\mathbb{B}_\infty) - 1 - \delta,$$

where $\delta \in \{-1, 0, 1, 2\}$. More precisely, if $k = \mathbb{Q}(i)$ and $S \neq \emptyset$ then $\delta = 0$ ($\delta = -1$ if $S = \emptyset$), and if $k \neq \mathbb{Q}(i)$, and $T = \emptyset$ or 2 does not split in $k/\mathbb{Q}$, then $\delta = 0$. In the remaining case (2 splits in $k/\mathbb{Q}$ and $T = \mathrm{Pl}_2(k)$) we only show $\delta \in \{1, 2\}$ ($\delta = 1$ in the S-empty case). We recall that the number of places in $\mathbb{B}_\infty$ above an odd prime number $p \in S \cup D$ is $2^{k'_p - 3}$.

Moreover, the $\mathbb{Z}_2$-torsion part of $X_S^T(k_\infty)$ can be computed as

$$\mathrm{Tor}_{\mathbb{Z}_2} X_S^T(k_\infty) \simeq \mathrm{Tor}_{\mathbb{Z}_2} X_S^T(\mathbb{B}_\infty),$$

in the following cases: *$k \neq \mathbb{Q}(i)$ and (2 is inert in $k/\mathbb{Q}$, or 2 splits in $k/\mathbb{Q}$ with $T = \emptyset$, or 2 ramifies in $k/\mathbb{Q}$ with $T = \mathrm{Pl}_2(k)$).*

Proof. We first recall the result of Ferrero and Kida (see [1] Theorems 4, 5, 6 and [4]), about the S-empty case:

$$\lambda^T(k_\infty) = \#D(\mathbb{B}_\infty) - 1 - \delta_2,$$

with $\delta_2 = -1$ if $k = \mathbb{Q}(i)$, with $\delta_2 = 1$ if $T = \mathrm{Pl}_2(k)$, and 2 splits in $k/\mathbb{Q}$, and with $\delta_2 = 0$ in the remaining cases.

We take n sufficiently large so that places in $S(\mathbb{B}_n)$ are either split or ramified in $k_n/\mathbb{B}_n$. We apply Proposition 1.2 for the fields $\mathbb{B}_n$ and k_n, and we find the following exact commutative diagram:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \dfrac{\mathcal{E}^T(\mathbb{B}_n)}{\mathcal{E}_S^T(\mathbb{B}_n)} & \longrightarrow & \displaystyle\prod_{v\in S(\mathbb{B}_n)} \mathfrak{k}_v^\times & \longrightarrow & A_S^T(\mathbb{B}_n) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \phi_2} & & \\
1 & \longrightarrow & \dfrac{\mathcal{E}^T(k_n)}{\mathcal{E}_S^T(k_n)} & \longrightarrow & \displaystyle\prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{1+\delta_v} & \longrightarrow & \ker(A_S^T(k_n) \to A^T(k_n)) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \dfrac{\mathcal{E}^T(k_n)}{\mathcal{E}^T(\mathbb{B}_n)\mathcal{E}_S^T(k_n)} & \xrightarrow{\phi_1} & \displaystyle\prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{\delta_v} & \longrightarrow & \operatorname{coker}\phi_1 = \operatorname{coker}\phi_2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

The injectivity of ϕ_2 comes from Lemma 1.6. The injectivity of ϕ_1 follows from the snake lemma. Here are some comments on the notations. The letter T must be replaced by $'$ or by the empty set. The quantity δ_v is 0 or 1 according whether the place v ramifies or splits in $k_n/\mathbb{B}_n$. The dependence on n has been omitted from the (pro-2-completions of) residue class fields, and from ϕ_1 and ϕ_2. The vertical map in the middle is a diagonal embedding at the places v which split in $k_n/\mathbb{B}_n$. The group in first row, third column is obtained from the general formula (which involves a kernel) because of the triviality of $A(\mathbb{B}_n)$.

Taking projective limit with respect to the norm maps, we find first:

$$1 \to X_S^T(\mathbb{B}_\infty) \to \ker(X_S^T(k_\infty) \to X^T(k_\infty)) \to \varprojlim \operatorname{coker}\phi_2 \to 1.$$

Then we see that there is an isomorphism of $\mathbb{Z}_2$-modules:

$$\varprojlim \prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{\delta_v} \simeq \mathbb{Z}_2^{\#(S-D)(\mathbb{B}_\infty)}.$$

Now, we compute $\varprojlim \mathcal{E}^T(k_n)/(\mathcal{E}^T(\mathbb{B}_n)\mathcal{E}_S^T(k_n))$. It is free as a sub-$\mathbb{Z}_2$-module of a free $\mathbb{Z}_2$-module. If $k \neq \mathbb{Q}(i)$, and $T = \emptyset$ or 2 does not split in $k/\mathbb{Q}$, these groups are trivial by Lemma 1.5, hence the projective limit is trivial. If $T = \mathrm{Pl}_2(k)$ and 2 splits in $k/\mathbb{Q}$, the quotient group $\mathcal{E}'(k_n)/\mathcal{E}'(\mathbb{B}_n)$ is infinite cyclic by the same lemma, hence the quotient group $\mathcal{E}'(k_n)/(\mathcal{E}'(\mathbb{B}_n)\mathcal{E}_S'(k_n))$ is cyclic of rank at most 1, and the projective limit is either trivial or isomorphic to $\mathbb{Z}_2$.

We now focus on the case $k = \mathbb{Q}(i)$. The quantities δ_v of the diagram are all equal to 1 in this case. First, if $T = \emptyset$, according to Lemma 1.5, the group $\mathcal{E}(\mathbb{B}_n(i))/\mathcal{E}(\mathbb{B}_n)$

is cyclic generated by a primitive 2^{n+2}-th root of unity ζ_n. We claim that the groups $\mathcal{E}(\mathbb{B}_n(i))/(\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i)))$ are non-trivial for n large enough (still assuming S non-empty). Assume the contrary. Then, we can write, for each n, $\zeta_n = \epsilon\epsilon_S$, with $\epsilon \in \mathcal{E}(\mathbb{B}_n)$ and $\epsilon_S \in \mathcal{E}_S(\mathbb{B}_n(i))$. Take n such that places in S are split in $\mathbb{B}_n(i)/\mathbb{B}_n$, and choose a place v in $S(\mathbb{B}_n)$, and places v_1 and v_2 above it in $\mathbb{B}_n(i)$. Hence, in the residue class fields $\mathfrak{b}_{v_1}$ and $\mathfrak{b}_{v_2}$ of $\mathbb{B}_n(i)$ at v_1 and v_2, we obtain $\bar{\zeta}_n = \bar{\epsilon}$. But $\bar{\epsilon}$ is already in the residue class field $\mathfrak{b}_v$ of $\mathbb{B}_n$ at v. Thanks to the equalities $\mathfrak{b}_v = \mathfrak{b}_{v_1} = \mathfrak{b}_{v_2}$, it follows that $\bar{\zeta}_n$ is the same in $\mathfrak{b}_{v_1}$ and in $\mathfrak{b}_{v_2}$ which is impossible. Therefore, the claim implies that the projective limit $\varprojlim \mathcal{E}(\mathbb{B}_n(i))/(\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i)))$ is isomorphic to $\mathbb{Z}_2$ by $\mathbb{Z}_2$-freeness.

Again for $k = \mathbb{Q}(i)$, take now T to be the set of places above 2. The quotient group $\mathcal{E}'(\mathbb{B}_n(i))/\mathcal{E}'(\mathbb{B}_n)$ is the direct product of the cyclic group $\mathcal{E}(\mathbb{B}_n(i))/\mathcal{E}(\mathbb{B}_n)$ with $\mathbb{Z}/2\mathbb{Z}$ according to Lemma 1.5. Hence, the quotient group $\mathcal{E}'(\mathbb{B}_n(i))/(\mathcal{E}'(\mathbb{B}_n)\mathcal{E}'_S(\mathbb{B}_n(i)))$ has at most two generators. As above, we can prove the non-triviality of ζ_n in this quotient. Taking projective limit and using the argument of $\mathbb{Z}_2$-freeness, we conclude that the projective limit $\varprojlim \mathcal{E}'(\mathbb{B}_n(i))/(\mathcal{E}'(\mathbb{B}_n)\mathcal{E}'_S(\mathbb{B}_n(i)))$ is isomorphic to $\mathbb{Z}_2$.

Thus we find an exact sequence of $\mathbb{Z}_2$-modules:

$$1 \to \mathbb{Z}_2^{\delta_1} \to \mathbb{Z}_2^{\#(S-D)(\mathbb{B}_\infty)} \to \varprojlim \operatorname{coker} \phi_1 \to 1,$$

with $\delta_1 \in \{0, 1\}$. More precisely, if $k \neq \mathbb{Q}(i)$ and ($T = \emptyset$ or 2 does not split in $k/\mathbb{Q}$) then $\delta_1 = 0$, and if $k = \mathbb{Q}(i)$ with $S \neq \emptyset$ then $\delta_1 = 1$ (and if $S = \emptyset$, then $\delta_1 = 0$). Using this in the first exact sequence, we find:

$$\lambda_S^T(k_\infty) = \lambda^T(k_\infty) + \lambda_S^T(\mathbb{B}_\infty) + \#(S - D)(\mathbb{B}_\infty) - \delta_1.$$

The assertion about λ-invariants follows from this formula and the results of Ferrero and Kida that we have recalled.

Now we turn our attention to the torsion part. Whenever $\delta_1 = 0$ the projective limit $\varprojlim \operatorname{coker} \phi_1$ is free as a $\mathbb{Z}_2$-module. Hence the first exact sequence splits into a direct sum of $\mathbb{Z}_2$-modules:

$$\ker(X_S^T(k_\infty) \to X^T(k_\infty)) \simeq X_S^T(\mathbb{B}_\infty) \oplus \varprojlim \operatorname{coker} \phi_1.$$

Moreover by [1], Theorems 4, 6, if 2 does not ramify in $k/\mathbb{Q}$, the Iwasawa module $X^T(k_\infty)$ is $\mathbb{Z}_2$-free, whenever $T = \emptyset$ or $T = \mathrm{Pl}_2(k)$, and the same holds if 2 ramifies in $k/\mathbb{Q}$ with $T = \mathrm{Pl}_2(k)$. In those cases we find an isomorphism of $\mathbb{Z}_2$-modules:

$$X_S^T(k_\infty) \simeq X^T(k_\infty) \oplus X_S^T(\mathbb{B}_\infty) \oplus \varprojlim \operatorname{coker} \phi_1.$$

The assertion on torsion parts in the case $k \neq \mathbb{Q}(i)$ follows. □

The group $\varprojlim D_S(k_n)$ needs to be known, in particular when 2 ramifies in $k/\mathbb{Q}$. From now on, we exclude the special case $k = \mathbb{Q}(i)$, which demands some other considerations.

Proposition 2.2. *Assume that S and D are non-empty. Then $\varprojlim D_S(\mathbb{B}_n)$ is isomorphic to $\mathbb{Z}_2/2^c\mathbb{Z}_2$ for some integer c, and*:

- *If 2 is inert in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2/2^c\mathbb{Z}_2$.*
- *If 2 ramifies in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2/2^{c+1}\mathbb{Z}_2$.*
- *If 2 splits in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2/2^c\mathbb{Z}_2$.*

Proof. First note that each $D_S(\mathbb{B}_n)$ is cyclic, generated by the unique ideal above 2 in $\mathbb{B}_n$. Hence, $\varprojlim D_S(\mathbb{B}_n)$ is procyclic. Moreover, $\mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q})$ acts trivially on this subgroup of $X_S(\mathbb{B}_\infty)$, then, if $\varprojlim D_S(\mathbb{B}_n)$ were infinite, we would find a quotient of $(X_S(\mathbb{B}_\infty))_{\mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q})}$ isomorphic to $\mathbb{Z}_2$, and that would contradict the fact that $\mathbb{Q}$ has no $\mathbb{Z}_2^2$-extensions. Hence there exists some integer c such that $\varprojlim D_S(\mathbb{B}_n) \simeq \mathbb{Z}_2/2^c\mathbb{Z}_2$.

If 2 does not split in $k/\mathbb{Q}$, then $D_S(k_n)$ is cyclic for each n, generated by the unique ideal above 2 in k_n. If 2 is inert, we obtain $D_S(\mathbb{B}_n) = D_S(k_n)$ (using Lemma 1.6), while, if 2 is ramified, the ideal above 2 is not principal (see [1], Lemma 10), and, for each n, the map of Lemma 1.6 induces an exact sequence:

$$1 \to D_S(\mathbb{B}_n) \to D_S(k_n) \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Taking the projective limit, we obtain the result in these cases.

If 2 splits in $k/\mathbb{Q}$, then $D_S(k_n)$ admits $D(k_n)$ as a quotient group. Since $\varprojlim D(k_n) \simeq \mathbb{Z}_2$ (see [1], Theorem 6), it follows that $\varprojlim D_S(k_n)$ admits $\mathbb{Z}_2$ as a quotient group, hence a direct summand. Moreover, each $D_S(k_n)$ is generated by the two ideals $\mathfrak{q}_n$ and $\mathfrak{q}'_n$ above 2 in k_n. Taking n sufficiently large, so that norm from $\varprojlim D_S(\mathbb{B}_m)$ to $D_S(\mathbb{B}_n)$ is an isomorphism, those ideals are linked by $(\mathfrak{q}_n\mathfrak{q}'_n)^{2^c} = 1$ in $A_S(k_n)$, where 2^c is the order of the ideal above 2 in $A_S(\mathbb{B}_n)$. Hence, for each n, the group $D_S(k_n)$ is a quotient group of $\mathbb{Z} \oplus \mathbb{Z}/2^c\mathbb{Z}$. Taking inverse limit, we obtain that $\varprojlim D_S(k_n)$ is isomorphic to some quotient of $\mathbb{Z}_2 \oplus \mathbb{Z}/2^c\mathbb{Z}$. Taking the inverse limit in Lemma 1.6, the group $\varprojlim D_S(\mathbb{B}_n) = \mathbb{Z}/2^c\mathbb{Z}$ is a subgroup of $\varprojlim D_S(k_n)$, and Proposition 2.2 follows. □

Corollary 2.3. *Assume that S is such that $X'_S(\mathbb{B}_\infty)$ is trivial and that 2 ramifies in $k/\mathbb{Q}$, with $k \neq \mathbb{Q}(i)$. Then*:

$$X_S(k_\infty) \simeq \mathbb{Z}_2^{\lambda_S} \oplus \mathrm{Tor},$$

with:

$$\lambda_S = -1 + \sum_{p \in S \cup D(\mathbb{Q})} 2^{k'_p - 3},$$

and where the torsion part Tor *is a cyclic 2-group of order twice that of $\varprojlim D_S(\mathbb{B}_n)$* (*which is given in* Proposition 2.5).

Proof. According to the proof of Theorem 2.1, we find an isomorpshim:

$$X'_S(k_\infty) \simeq X'(k_\infty) \oplus \varprojlim \operatorname{coker} \phi_1,$$

and we see in particular that $X'_S(k_\infty)$ must be $\mathbb{Z}_2$-free. Hence the torsion part of $X_S(k_\infty)$ must be isomorphic to that of $\varprojlim D_S(k_n)$ hence to $\varprojlim D_S(k_n)$ itself according to Proposition 2.2. □

We are not able to compute $X_S(\mathbb{B}_\infty)$ in general. We will restrict ourselves to characterize the case when $X'_S(\mathbb{B}_\infty)$ is trivial in the following Proposition 2.4. Note that much more general results of this kind have been obtained using Kummer theory (see [3], V, Theorem 2.4), from which our proposition can be deduced. However, we prefer to give an elementary proof in our situation.

Proposition 2.4. *Let S denote a finite set of odd prime numbers in $\mathbb{Q}$, and the set of places above it in each $\mathbb{B}_n$. The groups $A'_S(\mathbb{B}_n)$ are trivial if and only if S satisfies one of the following conditions*:

– *S is empty.*
– *S consists of a single element p, with $p \not\equiv 1 \bmod 8$.*
– *S consists of two elements p_1, p_2 such that $p_2 \equiv 7 \bmod 8$ and $p_1 \equiv 3, 5 \bmod 8$ or $p_2 \equiv 3 \bmod 8$ and $p_1 \equiv 5 \bmod 8$.*

Proof. According to Lemma 1.1, we only have to give a characterization of the cases when the group $A'_S(\mathbb{Q})$ is trivial. We use Proposition 1.2. In this case, Euler function for the modulus $\mathcal{M}_0$ (using notations of the proposition) satisfies:

$$_2\phi(\mathcal{M}_0) = \prod_{p\in S} 2^{k_p} = 2^{\sum_{p\in S} k_p},$$

where 2^{k_p} denotes the greatest power of 2 dividing $p-1$. We then look at the quotient group $\mathcal{E}'/\mathcal{E}'_S$ which is seen as the subgroup generated by 2 and -1 in $\prod_{p\in S} \mathfrak{k}_p^\times$ (we recall that $\mathfrak{k}_p^\times$ is the pro-2-completion of the multiplicative group $\mathbb{F}_p^\times$, hence is a cyclic 2-group). In each $\mathfrak{k}_p^\times$, -1 is in the subgroup generated by 2 if and only if 2 is non-trivial. Denote its order by $o_p = 2^{a_p}$. In the product of the $\mathfrak{k}_p^\times$'s, -1 is in the subgroup generated by 2 if and only if all o_p's are equal and non-trivial. Let $\delta = 0$ if this occurs, and $\delta = 1$ if not, and take $e = 2^a$ the maximum of the o_p's (hence a is the maximum of the a_p's). Then, the order of 2 in $\mathcal{E}'/\mathcal{E}'_S$ is e, and the group $\mathcal{E}'/\mathcal{E}'_S$, generated by 2 and -1, has order $2^\delta e = 2^{\delta+a}$. Hence, we have:

$$\#A'_S(\mathbb{Q}) = 2^{\sum_{p\in S} k_p - a - \delta}.$$

It yields $\#A'_S(\mathbb{Q}) = 1$ if and only if $\sum_{p\in S} k_p = a + \delta$. For each $p \in S$, the integer $o_p = 2^{a_p}$ divides 2^{k_p}, hence $a_p \le k_p$. One easily checks that the only cases where this equality can hold are (recall that we do not consider the case $S = \emptyset$):

1. $S = \{p\}$, $k_p = a_p$ and (this is automatic in this case) $\delta = 0$.
2. $S = \{p\}$, $k_p = a_p + 1$ and $\delta = 1$.
3. $S = \{p_1, p_2\}$, $\delta = 1 = k_{p_2}$ and $k_{p_1} = a = a_{p_1}$ (making a convention on the numerotation of the two primes).

For the first case to hold, it is necessary and sufficient that 2 is not a square in $\mathbb{F}_p$, and we find that $p \equiv 3, 5 \bmod 8$ are convenient for it. To study the second case, first note that the inequality $a_p < k_p$ implies that 2 is a square in $\mathbb{F}_p$, so that $p \equiv 1, 7 \bmod 8$. If $p \equiv 7 \bmod 8$, then $k_p = 1$, $a_p = 0$ and $\delta = 1$, so that the required equality holds, whereas if $p \equiv 1 \bmod 8$, we have $k_p \geq 3$ and since either a_p or δ is trivial, the conditions cannot be fulfilled.

We end the proof by the last case. Firstly, the condition $k_{p_1} = a_{p_1}$ implies that 2 is not a square in $\mathbb{F}_{p_1}$, hence that $p_1 \equiv 3, 5 \bmod 8$. Secondly, the condition $k_{p_2} = 1$ reads as $p_2 \equiv 3, 7 \bmod 8$. As seen above, if $p_2 \equiv 7 \bmod 8$, then $a_{p_2} = 0$, hence $\delta = 1$. Thus, in all the cases with $p_1 \equiv 3, 5 \bmod 8$ and $p_2 \equiv 7 \bmod 8$ the conditions are fulfilled. We then focus on the case $p_2 \equiv 3 \bmod 8$ (for which $a_{p_2} = 1$). If $p_1 \equiv 5 \bmod 8$ then $a_{p_1} = 2 \neq a_{p_2}$ and $\delta = 1$, so that the conditions are fulfilled, whereas if $p_1 \equiv 3 \bmod 8$, then $a_{p_1} = a_{p_2} = 1$ and the conditions are not fulfilled. □

Now, we compute the whole group $A_S(\mathbb{B}_n)$, assuming that S is such that $X'_S(\mathbb{B}_\infty)$ is trivial.

Proposition 2.5. *If S consists of only one place p, and $p \equiv 3, 7 \bmod 8$ then $A_S(\mathbb{B}_n)$ is trivial for each n. If $p \equiv 5 \bmod 8$, then $A_S(\mathbb{B}_n)$ is cyclic of order 2 for each n. If S consists of two places p_1 and p_2 which are respectively congruent to 3 and 7 modulo 8 then $A_S(\mathbb{B}_n)$ is cyclic of order 2 for each n, while, if p_1 and p_2 are respectively congruent to 3 and 5 or 5 and 7 modulo 8, then it is cyclic of order 4.*

Proof. First note that since the group $A'_S(\mathbb{B}_n)$ is trivial for each n under the assumptions on S, and since there is only one place above 2 in $\mathbb{B}_n$, then the group $A_S(\mathbb{B}_n) = D_S(\mathbb{B}_n)$ is cyclic for each n. To compute its cardinality, we consider the formula from Proposition 1.2. Since S is non-empty, the unit -1 cannot be in $E_{\mathcal{M}}(\mathbb{Q})$, so $[\mathcal{E}(\mathbb{Q}) : \mathcal{E}_S(\mathbb{Q})] = 2$. The cardinality of ${}_2\phi(\mathcal{M}_0)$ is easily computed for each set S we consider, and the result of the proposition follows for $n = 0$. In particular, if $S = \{p\}$ with $p \equiv 3, 7 \bmod 8$, then $A_S(\mathbb{Q})$ is trivial, and so are the $A_S(\mathbb{B}_n)$'s for all n, according to Lemma 1.1.

For the remaining cases, we will show that $\#A_S(\mathbb{B}_1) = \#A_S(\mathbb{Q})$, in order to apply Lemma 1.1. The computations are therefore done in the first layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, namely $\mathbb{B}_1 = \mathbb{Q}(\sqrt{2})$. We apply Proposition 1.2 in that field. Assume first that $S = \{p\}$, with $p \equiv 5 \bmod 8$. We find ${}_2\phi(\mathcal{M}_0) = 8$. The group $E(\mathbb{B}_1)$ is generated by -1 and $1 - \sqrt{2}$, and the quotient group by $E_{\mathcal{M}}(\mathbb{B}_1)$ can be seen as a subgroup of the multiplicative group of the field $\mathbb{F}_{p^2}$. The greatest 2-power dividing the order of this latter group is 8. It suffices to show that $1 - \sqrt{2}$ admits a square root but

not a fourth root in this group: it follows that the greatest power of 2 dividing its order is 4, so that the quotient group $E(\mathbb{B}_1)/E_{\mathcal{M}}(\mathbb{B}_1)$ is generated by $1-\sqrt{2}$, and the 2-part of its order is 4, hence that the order of $A_S(\mathbb{B}_1)$ is 2, which concludes the proof according to Lemma 1.1. The square root of $1-\sqrt{2}$ in $\mathbb{F}_{p^2}$ is $-1/\sqrt{1+i}+(\sqrt{1+i}/2)\sqrt{2}$, where i is the primitive fourth root of unity in $\mathbb{F}_p$ such that $2i$ has odd order (ensuring that the square root of $1+i$ exists in $\mathbb{F}_p$, because $(1+i)^2=2i$). A square root $a+b\sqrt{2}$ (with $a, b \in \mathbb{F}_p$) of that element would be such that:

$$\begin{cases} a^2+2b^2 = -\dfrac{1}{\sqrt{1+i}}, \\ 2ab = \dfrac{\sqrt{1+i}}{2}. \end{cases}$$

These equations lead to:

$$b^4 + \frac{b^2}{2\sqrt{1+i}} + \frac{1+i}{32} = 0.$$

The discriminant of the underlying quadratic equation is $(1/2)((1-i)/2)^2$. Since 2 is not a square in $\mathbb{F}_p$, there is no solution to the above equation in $\mathbb{F}_p$, and we are done.

Now, assume that $S(\mathbb{Q})$ contains two primes p_1 and p_2. The following table gives the values of the quantities that appear in the formula for $A_S(\mathbb{B}_1)$, in the three cases for the congruence of p_1 and p_2 modulo 8. The proposition follows from the cardinalities of the groups in the first and in the last columns, and from Lemma 1.1. The two columns in the middle give the 2-part of the quotient group of the units by the units which are congruent to 1 modulo, respectively, the primes above p_1 and the primes above p_2. Proofs for the values in this table are to be found below:

p_1, p_2 mod 8	${}_2\phi(\mathcal{M})$	$\mathcal{E}/\mathcal{E}_{\{p_1\}}$	$\mathcal{E}/\mathcal{E}_{\{p_2\}}$	$\mathcal{E}/\mathcal{E}_S$
3, 5	64	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
3, 7	32	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
5, 7	32	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$

The values in the three first columns in the table are computed as follows: the first column is simply given by decomposition rules in $\mathbb{B}_1/\mathbb{Q}$; the cardinality of the groups in the second and third columns are consequences of the values found for $A_S(\mathbb{B}_1)$ when $S(\mathbb{Q})$ contains only one prime. Whenever the group is cyclic, it comes from the fact that it can be seen as a subgroup of the multiplicative group of some finite field (as above in the case $\#S=1$ and $p \equiv 1 \bmod 8$); in that case, it is generated by the class of $1-\sqrt{2}$. The last two entries in the third column ($p_2 \equiv 7 \bmod 8$) are deduced from the fact that the group is seen as a subgroup of $\mathbb{F}_{p_2}^{\times}\times\mathbb{F}_{p_2}^{\times}$, whose 2-part is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. In each case, the group $\mathcal{E}/\mathcal{E}_{\mathcal{M}}$ admits both $\mathcal{E}/\mathcal{E}_{p_1}$ and $\mathcal{E}/\mathcal{E}_{p_2}$ as a quotient group. It

is generated by $1-\sqrt{2}$ and -1. Now, the order of $1-\sqrt{2}$ is easily checked to be respectively 8, 8 and 4 in the three cases corresponding to the three lines in the table. Then the groups in the two last entries of the fourth column are deduced from the non-cyclicity in the third column. For the remaining entry (first line, fourth column), it only needs to be noticed that -1 cannot be in the subgroup generated by $1-\sqrt{2}$ because no odd power of $(1-\sqrt{2})^{2^k}$, for any k, can be congruent to -1 modulo both p_1 and p_2, since the groups in the second and third columns of the first line do not have the same order. □

Corollary 2.6. *The cases with S and D non-empty, and disjoint, with trivial $X'_S(\mathbb{B}_\infty)$, and $\lambda_S(k_\infty)=1$, are*:
– $D=\{p\}$ *with* $p\equiv 3 \bmod 8$ *and* $S=\{q\}$ *with* $q\equiv 3 \bmod 8$. *In this case* $X_S(k_\infty)\simeq \mathbb{Z}_2$.
– $D=\{p\}$ *with* $p\equiv 5 \bmod 8$ *and* $S=\{q\}$ *with* $q\equiv 3 \bmod 8$. *In this case* $X_S(k_\infty)\simeq \mathbb{Z}_2\oplus\mathbb{Z}/2\mathbb{Z}$.
– $D=\{p\}$ *with* $p\equiv 3 \bmod 8$ *and* $S=\{q\}$ *with* $q\equiv 5 \bmod 8$. *In this case* $X_S(k_\infty)\simeq \mathbb{Z}_2\oplus\mathbb{Z}/2\mathbb{Z}$.
– $D=\{p\}$ *with* $p\equiv 5 \bmod 8$ *and* $S=\{q\}$ *with* $q\equiv 5 \bmod 8$. *In this case* $X_S(k_\infty)\simeq \mathbb{Z}_2\oplus\mathbb{Z}/4\mathbb{Z}$.

Proof. The triviality of $X'_S(\mathbb{B}_\infty)$ implies that $X_S(\mathbb{B}_\infty)$ has trivial $\mathbb{Z}_2$-rank according to Proposition 2.5. Then the formula of Theorem 2.1 becomes, for $T=\emptyset$:

$$\lambda_S(k_\infty)=\#(S\cup D)(\mathbb{B}_\infty)-1.$$

Thus, we must find all the cases where $\#(S\cup D)(\mathbb{B}_\infty)=2$. Since we are only interested in the cases where S and D are non-empty, we see that each one must consist of a single prime number congruent to 3 or 5 modulo 8. In the case $D=\{p\}$ with $p\equiv 3 \bmod 8$, the structure of $X_S(k_\infty)$ comes from Theorem 2.1 and Proposition 2.5. In the case $D=\{p\}$ with $p\equiv 5 \bmod 8$, use Corollary 2.3 for the torsion part. □

3. Computations of Galois groups

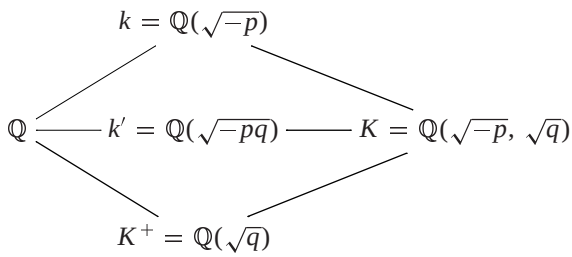
3.1. Presentation of Galois groups over k_∞. Let us recall our main theorem:

Theorem. *Let p and q be two prime numbers respectively congruent to* 5 *and* 3 *modulo* 8, *and put $S=\{q\}$. Let k be the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$, and $\mathcal{G}=\mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$ the Galois group of the maximal S-ramified pro-2-extension of k_∞. Then $\mathcal{G}$ has rank* 2 *and admits as a presentation*:

$$\langle a,\, b \mid [a,\, b]a^2\rangle.$$

The same holds if we assume $p\equiv 3 \bmod 8$ and $q\equiv 5 \bmod 8$.

The proof is almost the same in the two cases. According to Corollary 2.6, the abelianization of $\mathcal{G}$ is $\mathcal{G}^{ab} = X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. Moreover, the $\mathbb{Z}_2$-quotient of $X_S(k_\infty)$ is $X'_S(k_\infty)$. In each case, we introduce the following extensions:



For each n, the extension K_n/k_n is S-ramified and 2-split. Hence, the extension K_∞/k_∞ is the subextension of $L'_S(k_\infty)$ fixed by the subgroup $2X'_S(k_\infty)$ of $X'_S(k_\infty) \simeq \mathbb{Z}_2$. Since $L'_S(k_\infty)/k_\infty$ is procyclic, it is the maximal S-ramified 2-split pro-2-extension of k_∞. The equality $L'_S(k_\infty) = L'_S(K_\infty)$ follows, hence $X'_S(K_\infty) \simeq \mathbb{Z}_2$ as a $\mathbb{Z}_2$-module. Moreover, we have the proposition:

Proposition 3.1. *We have the equality $L'_S(K_\infty) = L'_S(k_\infty)$, and the S-ramified Iwasawa module over K_∞ satisfies $X_S(K_\infty) \simeq \mathbb{Z}_2^2$, where one direct summand is $X'_S(K_\infty)$.*

Proof. The first assertion has already been proved. Consider the exact sequences for all n:

$$1 \to D_S(K_n) \to A_S(K_n) \to A'_S(K_n) \to 1,$$

which give, by taking the projective limit:

$$1 \to \varprojlim D_S(K_n) \to X_S(K_\infty) \to X'_S(K_\infty) \to 1.$$

Since $X'_S(K_\infty)$ is free as a $\mathbb{Z}_2$-module, there is an isomorphism:

$$X_S(K_\infty) \simeq X'_S(K_\infty) \oplus \varprojlim D_S(K_n).$$

It remains to show that $\varprojlim D_S(K_n)$ is infinite and procyclic.

First we focus on the case $p \equiv 5 \bmod 8$ and $q \equiv 3 \bmod 8$. Consider the extension $k'_n/\mathbb{B}_n$. The prime 2 splits in this extension. Then, by the genus formula (Proposition 1.3), and Proposition 2.4, the group $A'_S(k'_n)$ is trivial for each n, hence $X_S(k'_\infty) = \varprojlim D_S(k'_n)$ holds. According to Propositions 2.2, 2.4 and 2.5, the groups $D_S(k'_n)$ are cyclic and their inverse limit is isomorphic to $\mathbb{Z}_2$. Then, the compositum $L_S(k'_\infty) \cdot K_\infty$ is an infinite procyclic S-ramified pro-2-extension of K_∞, and the two primes above 2 in K_∞ do not split in that extension. It is linearly disjoint from $L'_S(K_\infty)/K_\infty$.

Now, we apply Proposition 1.3 in the extension $K_n^+/\mathbb{B}_n$. The groups $A_S(\mathbb{B}_n)$ are trivial in this special case, and the only ramified place in $K_n^+/\mathbb{B}_n$ which is not in S is the place above 2. Hence, using Lemma 1.4, $A_S(K_n^+)$ is trivial. Let us write $\mathfrak{p}_{n,1}$ and $\mathfrak{p}_{n,2}$ for the places above 2 in K_n. The product $\mathfrak{p}_{n,1}\mathfrak{p}_{n,2}$ is trivial in $A_S(K_n^+)$, hence in $A_S(K_n)$ (the unique place in $S(K_n^+)$ is unramified in K_n/K_n^+, so any S-principal generator in K_n^+ is still S-principal in K_n). It follows that the subgroup $D_S(K_n)$ generated by the places above 2 is cyclic. Hence $\varprojlim D_S(K_n)$ is procyclic, and it is infinite because of the extension $L_S(k'_\infty)\,.\,K_\infty/K_\infty$.

In the case $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$, some of the arguments need to be slightly adapted. The module $X_S(k'_\infty)$ is now isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, according to Propositions 2.2, 2.4 and 2.5. In order to exhibit an infinite procyclic S-ramified 2-extension of K_∞ in which the primes above 2 do not split, one must replace $L_S(k'_\infty)\,.\,K_\infty$ by the compositum of K_∞ with the unique infinite procyclic S-ramified pro-2-extension of k'_∞. The triviality of $A_S(K_n^+)$ comes from the fact that the field K_n^+ is the maximal S-ramified 2-extension of $\mathbb{B}_n$. □

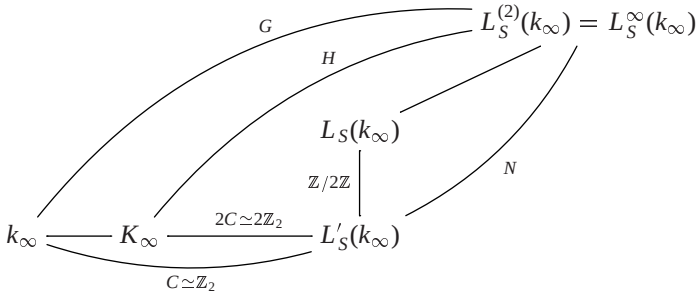
Let us now state a group theoretical proposition, whose proof can be found in [7], Section 3.2 (but the result is not explicitly stated there):

Proposition 3.2. *Let G be a metabelian pro-2-group, whose abelianization G^{ab} is isomorphic to $C \oplus \mathbb{Z}/2\mathbb{Z}$, with $C \simeq \mathbb{Z}_2$. Denote by H the subgroup of G of index 2, such that $H/G_2 \simeq 2C \oplus \mathbb{Z}/2\mathbb{Z}$. If H has rank 2, then G is metacyclic. More precisely, there is a short exact sequence*:

$$1 \to N \to G \to C \to 1,$$

where N is a procyclic subgroup of H such that $H/N \simeq 2C$.

In our setting, the field extensions associated to these groups will be as follows (here $L_S^{(2)}(k_\infty)$ denotes the maximal metabelian subextension of $L_S^\infty(k_\infty)$ over k_∞, and we will prove the equality $L_S^{(2)}(k_\infty) = L_S^\infty(k_\infty)$):



We want to apply Proposition 3.2 to $G = \mathrm{Gal}(L_S^{(2)}(k_\infty)/k_\infty)$, which is the maximal metabelian quotient of $\mathcal{G} = \mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$. We recall that there is an isomorphism $G^{ab} =$

$\mathcal{G}^{ab} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, according to Corollary 2.6. Then, take $H = \mathrm{Gal}(L_S^{(2)}(k_\infty)/K_\infty)$, its abelianization is $\mathrm{Gal}(L_S(K_\infty)/K_\infty)$ which has rank 2 according to Proposition 3.1. Hence, the assumptions of Proposition 3.2 are satisified and $L_S^{(2)}(k_\infty)$ is a procyclic pro-2-extension of $L'_S(k_\infty)$. Since $L_S(K_\infty)$ is itself an infinite procyclic extension of $L'_S(k_\infty)$ (Proposition 3.1), we deduce the equality $L_S(K_\infty) = L_S^{(2)}(k_\infty)$. Finally, since $L_S^{(2)}(k_\infty)/L_S(k_\infty)$ is procyclic, we deduce that it is the maximal S-ramified pro-2-extension of k_∞, and that $\mathcal{G} = G$.

The group $\mathcal{G}$ is a pro-2-group of rank 2 whose abelianization is $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. Let us denote by $a, b \in \mathcal{G}$ a system of representatives of generators of $X_S(k_\infty)$, such that $\bar{b} \in X_S(k_\infty)$ generates the summand $X'_S(k_\infty) \simeq \mathbb{Z}_2$, and $\bar{a}$ generates the summand $\mathbb{Z}/2\mathbb{Z}$. By restriction, the element $\bar{b}$ can be seen as a generator of the Galois group $\mathrm{Gal}(K_n/k_n)$ for each n, so it acts on the ideal $\mathfrak{p}_{n,1}$ by sending it on $\mathfrak{p}_{n,2}$ (these are the two ideals above 2 in K_n, according to the notations of Proposition 3.1). These ideals are each other inverses in $A_S(K_n)$, and generate $D_S(K_n)$, so $\bar{b}$ acts by inversion on $D_S(K_n)$. Taking the projective limit, we find that b acts by inversion on a. In the group $\mathcal{G}$ the following relation is satisfied:

$$[a, b]a^2 = 1.$$

The following lemma will enable us to prove that this is the only relation of the group $\mathcal{G}$:

Lemma 3.3. *Let $\mathcal{G}$ be a (pro-p-)group admitting as a system of generators a, b, and assume that these generators satisfy the relation $[a, b]a^2 = 1$. Then, the derived group $\mathcal{G}_2$ is included in the closed subgroup generated by a. It is in particular (pro)cyclic.*

Proof. By recursion on the minimal number of letters (among a, b, a^{-1} and b^{-1}) needed to write u, it is easily shown that each element of the form $u^{-1}au$ is in the closed subgroup generated by a. Therefore, this subgroup is normal. The derived group $\mathcal{G}_2$ is the smallest closed normal subgroup of $\mathcal{G}$ containing $[a, b]$, and that element is in the subgroup generated by a, hence the lemma follows. □

We are now in position to conclude the proof of Theorem 1. Let us denote by $\mathcal{F}$ the free pro-2-group on two generators a and b, and $\mathcal{R}$ its subgroup generated by $[a, b]a^2$. Its abelianization is easily seen to be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. There is a surjection $\mathcal{F}/\mathcal{R} \to \mathcal{G}$, and we deduce from it a commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & (\mathcal{F}/\mathcal{R})_2 & \longrightarrow & \mathcal{F}/\mathcal{R} & \longrightarrow & (\mathcal{F}/\mathcal{R})^{ab} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{G}_2 & \longrightarrow & \mathcal{G} & \longrightarrow & \mathcal{G}^{ab} & \longrightarrow & 1
\end{array}$$

The third vertical arrow is a surjection, between two groups isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, hence it is an isomorphism. It follows that the first vertical arrow is also surjective. According to Lemma 3.3, and previous results on $\mathcal{G}$, the groups $(\mathcal{F}/\mathcal{R})_2$ and $\mathcal{G}_2$ are both procyclic, hence the first vertical arrow is an isomorphism. It follows that the map $\mathcal{F}/\mathcal{R} \to \mathcal{G}$ is actually an isomorphism, which finishes the proof of Theorem 1.

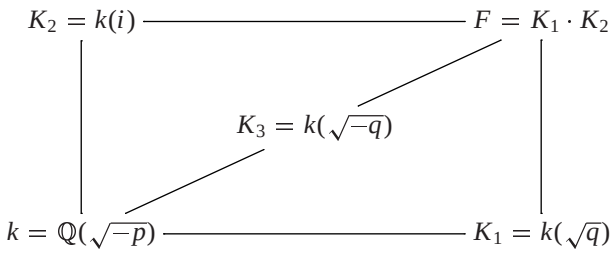
Corollary 3.4. *The cohomological dimension of* $\mathcal{G}$ *is* 2. *That of* $\mathrm{Gal}(L_S^\infty(k_\infty)/k)$ *is* 3.

Proof. These assertions are consequences of Proposition 22 in [8]. □

3.2. Presentations of Galois groups over k_n. Our aim here is to compute the Galois groups of ray class field towers above each k_n (see Theorems 3.8 and 3.11 below). The two cases $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with respectively $p \equiv 5 \bmod 8$ and $q \equiv 3 \bmod 8$, and $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$ are again only slightly different. First we prove Theorem 3.8, assuming that $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with:

$$p \equiv 5 \bmod 8, \quad q \equiv 3 \bmod 8, \quad \left(\frac{p}{q}\right) = -1.$$

We introduce the following notations:



Proposition 3.5. *Assume that the Legendre symbol* $\left(\frac{p}{q}\right)$ *is* -1. *Then the Galois group* $\mathrm{Gal}(L_S^\infty(k)/k)$ *is isomorphic to the quaternionic group* $\mathcal{Q}_8$.

Proof. First, we collect some lemmas:

Lemma 3.6. *There are isomorphisms* $A(k) \simeq \mathbb{Z}/2\mathbb{Z}$ *and* $A_S(k) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. *The Hilbert* 2*-class field of* k *is* K_2, *and its ray* 2*-class field associated to the prime* q *is* F.

Proof. We know that $A(k) \simeq D(k) \simeq \mathbb{Z}/2\mathbb{Z}$ by Lemma 10 and Theorem 5 in [1] and we obtain $D_S(k) \simeq \mathbb{Z}/2\mathbb{Z}$ by Propositions 2.2, 2.4 and 2.5. Since K_2 is an unramified 2-extension of k, it is the Hilbert 2-class field of k. Then we apply Proposition 1.2

in k: since q splits in k, the value of ${}_2\phi(\mathcal{M})$ is 4, and since $E(k)$ is generated by -1, which is not congruent to 1 modulo $\mathcal{M}$, we deduce that $\#A_S(k) = 4$. Since F is a S-ramified $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension of k, it is its q-ray 2-class field. □

Lemma 3.7. *The group $A_S(\mathbb{Q}(\sqrt{p}))$ is trivial, and the groups $A_S(K_2)$ and $A_S(K_1)$ are cyclic.*

Proof. The first assertion follows easily from the genus formula in the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, since p is the only ramified prime in this extension. Then we use the genus formula (Proposition 1.3) in $K_2/\mathbb{Q}(\sqrt{p})$:

$$\#A_S(K_2)^{\Delta} = \frac{8}{2\,.\,[\mathcal{E}_S(\mathbb{Q}(\sqrt{p})) : \mathcal{E}_S(\mathbb{Q}(\sqrt{p})) \cap N_{K_2/\mathbb{Q}(\sqrt{p})}\mathcal{J}_{K_2}]},$$

where the 8 in the numerator comes from the 3 places (the place above 2 and the two real places) which ramifiy in this extension. We use Proposition 1.2 in $\mathbb{Q}(\sqrt{p})$. The groups $A(\mathbb{Q}(\sqrt{p}))$ and $A_S(\mathbb{Q}(\sqrt{p}))$ are trivial, and q is inert in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, hence ${}_2\phi(\mathcal{M}) = 8$. We deduce that the quotient group $\mathcal{E}/\mathcal{E}_S(\mathbb{Q}(\sqrt{p}))$ is cyclic of order 8. Given $(\epsilon, -1)$ a system of generators of $\mathcal{E}$, linear algebra shows that the subgroups of $\mathcal{E}$ which give such a quotient are those generated by $-\epsilon^4$ and $(-1, \epsilon^8)$. The second possibility has to be excluded since -1 cannot lie in $\mathcal{E}_S$. Then $\mathcal{E}_S$ is generated by $-\epsilon^4$. This element cannot be a norm from K_2, since ϵ^4 is so and -1 is not. It follows that:

$$\#A_S(K_2)^{\Delta} = 2,$$

and we conclude that $A_S(K_2)$ is cyclic with Lemma 1.4.

Finally, the maximal 2-split S-ramified (abelian) 2-extension of k is a quadratic extension according to Lemma 3.6. Since K_1 has those properties, it is that extension. We deduce that $A'_S(K_1)$ is trivial. Hence $A_S(K_1) \simeq D_S(K_1)$ is cyclic, according to Proposition 3.1. □

It turns out from Lemma 3.6 that $\mathrm{Gal}(L_S^{\infty}(k)/k)$ has its abelianization isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. A table of maximal subgroups of such 2-groups is given for instance in [6] (Table 1, see there also for references). Our Lemma 3.7 together with this table ensures that the Galois group $\mathrm{Gal}(L_S^{\infty}(k)/k)$ is either abelian or isomorphic to the quaternionic group.

To conclude the proof, we will show that the ideal above p in k does not S-capitulate in K_1, using Theorem 1 in [5] (whose adaptation to the case of ray class field towers is immediate). That ideal in k is generated by $\sqrt{-p}$. Denoting by $\mathfrak{q}_1$ and $\mathfrak{q}_2$ the prime ideals above q in k, there is a rational integer r such that $\sqrt{-p} \equiv r \bmod \mathfrak{q}_1$ and $\sqrt{-p} \equiv -r \bmod \mathfrak{q}_2$. It follows that no odd power of $\sqrt{-p}$ can be congruent to 1 modulo q. The ideal generated by $\sqrt{-p}$ admits another generator, namely $-\sqrt{-p}$, and the same holds for this generator. Thus, that ideal is not trivial in $A_S(k)$.

We claim that the 2-part of $E(K_1)/E_{\mathcal{M}}(K_1)$ has order 2 as well, hence is still generated by -1. Thus the same argument holds in K_1. Let us conclude the proof of Proposition 3.5 by proving the claim: $K_1/\mathbb{Q}(\sqrt{q})$ is a CM-extension, hence, by Theorem 4.12 in [9], the index $[E(K_1) : E(\mathbb{Q}(\sqrt{q}))]$ is 1 or 2. Moreover, this index can not be 2 because the extension is ramified in the place above p, hence is not of the form $K_1 = \mathbb{Q}(\sqrt{p})(\epsilon)$ with ϵ a unit. It follows that $E(K_1) = E(\mathbb{Q}(\sqrt{q}))$, hence $\mathcal{E}(K_1)/\mathcal{E}_S(K_1) = \mathcal{E}(\mathbb{Q}(\sqrt{q}))/\mathcal{E}_S(\mathbb{Q}(\sqrt{q}))$. Applying the exact sequence of Proposition 1.2 in $\mathbb{Q}(\sqrt{q})$, we find a monomorphism from $\mathcal{E}(\mathbb{Q}(\sqrt{q}))/\mathcal{E}_S(\mathbb{Q}(\sqrt{q}))$ to $\prod_{v\in S(\mathbb{Q}(\sqrt{q}))} \mathbb{k}_v^\times$, and this group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ in our case. Hence $\mathcal{E}(K_1)/\mathcal{E}_S(K_1) \simeq \mathbb{Z}/2\mathbb{Z}$ and we are done. □

Theorem 3.8. *Under the assumptions of* Proposition 3.5, *for each* $n \geq 0$, *the group* $\mathcal{G}_n = \mathrm{Gal}(L_S^\infty(k_n)/k_n)$ *admits as a presentation*:

$$\langle a, b \mid a^2[a, b], a^{2^{n+2}}, a^{2^{n+1}} b^{-2^{n+1} w_n} \rangle,$$

where w_n *is some power of* 2. *Moreover,* $w_0 = 1$, *and, if the constant term* C_0 *of the Iwasawa polynomial of* $X'_S(k_\infty)$ *satisfies* $C_0 \equiv 2 \bmod 8$, *then* $w_n = 1$ *for all* n.

Proof. Recall that the group $\mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$ admits as a presentation $\langle a, b \mid a^2[a, b]\rangle$. Each group $\mathcal{G}_n$ can be viewed as a quotient group of the former, according to the isomorphism $\mathcal{G}_n \simeq \mathrm{Gal}(L_S^\infty(k_n) . k_\infty/k_\infty)$. Moreover, F_∞ is contained in $L_S^\infty(k) . k_\infty$ (this follows from the proof of Proposition 3.5), and it is the fixed field of the subgroup of $\mathcal{G}$ generated by a^2 and b^2. This field admits three quadratic extensions, fixed respectively by $\langle a^4, b^2\rangle$, $\langle a^2, b^4\rangle$ and $\langle a^4, a^2b^2\rangle$, and their Galois group over k_∞ are respectively dihedral, abelian and quaternionic of order 8. Thus we have the presentation:

$$\mathcal{G}_0 \simeq \langle a, b \mid a^2[a, b], a^4, a^2b^2\rangle.$$

Now, denote by $H = X_S(K_{1,\infty})$ the abelian subgroup of $\mathcal{G}$ generated by a and b^2, whose fixed field is $K_{1,\infty}$. It admits an Iwasawa module structure. There is an exact sequence:

$$1 \to \langle a\rangle \to H \to X'_S(k_\infty) \to \mathrm{Gal}(K_{1,\infty}/k_\infty) \to 1.$$

Denote by $P(T)$ the Iwasawa polynomial of the Iwasawa module $X'_S(k_\infty)$. It has degree one, hence it can be written $T + C_0$ for some C_0.

Lemma 3.9. $C_0 \equiv 2 \bmod 4$.

Proof. It is completely analogous to Lemma 4.4 in [7]. On the one hand, the Iwasawa module $X'_S(k_\infty)$ is isomorphic to $\Lambda/P(T)\Lambda$, and on the other hand its quotient by T is isomorphic to $A'_S(k)$ (by Lemma 13.15 in [9], since there is only one prime above 2 in k). The latter is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, hence there is an isomorphism

$\Lambda/(T, P(T))\Lambda \simeq \mathbb{Z}/2\mathbb{Z}$, and it proves that the constant coefficient C_0 of P is congruent to 2 modulo 4. □

There is a trivial action of some generator $\gamma \in \Gamma$ on the ideal above 2 in each layer $K_{1,n}$ of the cyclotomic extension of K_1. Taking the limit, it yields a trivial action on a, hence the subgroup $\langle a \rangle$ of H can be made isomorphic to $\Lambda/T\Lambda$, by the canonical identification between γ and $T-1$. Then, since $T \nmid P(T)$ according to Lemma 3.9, the exact sequence involving H and $X'_S(k_\infty)$ gives a pseudo-isomorphism, with trivial kernel:

$$H \sim \Lambda/TP(T)\Lambda.$$

Through this map, the element a can be identified with $P(T)$, and b^2 with T, since it generates the image of H in $X'_S(k_\infty) \simeq \Lambda/P(T)\Lambda$.

It is a classical fact of Iwasawa theory (see [9], Lemma 13.15) that the groups $\mathrm{Gal}(L_S(K_{1,\infty})/L_S(K_{1,n}) \,.\, k_\infty)$ can be computed as $\nu_n(T)Y_0$, with:

$$\nu_n(T) = \frac{(1+T)^{2^n} - 1}{T},$$
$$Y_0 = \mathrm{Gal}(L_S(K_{1,\infty})/L_S(K_{1,0}) \,.\, k_\infty) = \langle a^4, a^2b^2 \rangle.$$

The polynomial $\nu_n(T)$ admits the expansion $2^n + 2^{n-1}(2^n - 1)T + o(T)$, with $o(T)$ a polynomial such that $T^2 \mid o(T)$, for each $n \geq 1$. Then, there are relations:

$$\nu_n(T) = x_n P(T) + y_n T \bmod TP(T),$$

where $x_n = 2^{n-1}u$ and $y_n = 2^n v_n$, with $u = 2/C_0 \in \mathbb{Z}_2^\times$ (according to the previous lemma), and $v_n = 2^n - 1 - u$. Using those notations, a direct computation yields:

$$\nu_n(T)Y_0 = \langle a^{4x_nC_0}, a^{2x_nC_0}b^{-y_nC_0} \rangle = \langle a^{2^{n+2}}, a^{2^{n+1}}b^{-2^{n+1}w_n} \rangle,$$

where w_n is the greatest 2-power dividing v_n. The last assertion follows from $v_n = 2^n - 1 - u$. □

Now we turn our attention to Theorem 3.11. We take now $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with:

$$p \equiv 5 \bmod 8, \quad q \equiv 3 \bmod 8, \quad \left(\frac{p}{q}\right) = -1.$$

We recall that $K = k(\sqrt{q})$. There is no analogous to the fields K_2 and K_3 here, and the Proposition 3.5 must be replaced by:

Lemma 3.10. *Under the assumptions above. The maximal S-ramified 2-extension of k is a cyclic extension of degree 4 which contains K. The primes above 2 have inertia degree 2 in this extension.*

Proof. It follows from Theorem 2.1, and Propositions 2.2 and 2.5 that the groups $D(k)$ and $A'(k)$ are trivial. Hence, the group $A(k)$ is trivial as well. By the same propositions, the group $D_S(k)$ is cyclic of order 2.

By Proposition 1.2, the group $A_S(k)$ is then cyclic, as a quotient group of $\prod_{v\in S(k)} \mathfrak{k}_v$, provided that $S(k)$ contains only one place, and this is true in the two cases (thanks to the assumption $\left(\frac{p}{q}\right) = -1$ in the first case). The same proposition gives the cardinality of $A_S(k)$, which turns to be 4. □

The field $L_S^\infty(k) \,.\, k_\infty$ is thus a cyclic extension of degree 4 of k_∞, and it contains K_∞. The latter admits three distinct quadratic extensions, which are fixed respectively by $\langle a, b^4\rangle$, $\langle a^2, b^2\rangle$ and $\langle a^2, ab^2\rangle$. The first is 2-split over k_∞, the second one is not cyclic over that field. Hence we find:

$$Y_0 = \mathrm{Gal}(L_S(K_\infty)/L_S^\infty(k) \,.\, k_\infty) = \langle a^2, ab^2\rangle.$$

By the same computation as before, we have, for $n \geq 1$:

$$\mathrm{Gal}(L_S(K_\infty)/L_S^\infty(k_n) \,.\, k_\infty) = \nu_n(T)Y_0 = \langle a^{2x_nC_0}, a^{x_nC_0}b^{-y_nC_0}\rangle.$$

Lemma 3.9 also holds in this case, and the theorem follows.

Theorem 3.11. *Assume that $p \equiv 3 \bmod 8$ and $S = \{q\}$ with $q \equiv 5 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$. For each $n \geq 1$, the group $\mathcal{G}_n = \mathrm{Gal}(L_S^\infty(k_n)/k_n)$ admits as a presentation*:

$$\langle a, b \mid a^2[a, b], a^{2^{n+1}}, a^{2^n}b^{-2^n w_n}\rangle,$$

where w_n is some power of 2. Moreover, $w_0 = 1$, and, if the constant term of the Iwasawa polynomial of $X'_S(k_\infty)$ satisfies $C_0 \equiv 2 \bmod 8$, then $w_n = 1$ for all n.

ACKNOWLEDGEMENTS. This work is a part of my PhD thesis. I thank my supervisor Christian Maire who had to read many different versions of this paper. I had the opportunity to meet Yasushi Mizusawa in the conference Iwasawa 2006 in Limoges, and during a visit he made in Toulouse in march 2007. This work would obviously not have been done without his advices. I am very glad to thank Manabu Ozaki and Jean-Robert Belliard, particularly because they both pointed to me that a previous computation of Iwasawa modules could be widely improved, but also for useful and interesting more general discussions. Finally I thank the referee who carefully read the paper, allowed me to correct several mistakes, and suggested various improvements.

References

[1] B. Ferrero: *The cyclotomic* $\mathbf{Z}_2$*-extension of imaginary quadratic fields*, Amer. J. Math. **102** (1980), 447–459.

[2] T. Fukuda: *Remarks on* $\mathbf{Z}_p$*-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 264–266.

[3] G. Gras: Class Field Theory, Springer Monographs in Mathematics, From theory to practice; Translated from the French manuscript by Henri Cohen, Springer, Berlin, 2003.

[4] Y. Kida: *On cyclotomic* $\mathbf{Z}_2$*-extensions of imaginary quadratic fields*, Tôhoku Math. J. (2) **31** (1979), 91–96.

[5] H. Kisilevsky: *Number fields with class number congruent to* 4 mod 8 *and Hilbert's theorem* 94, J. Number Theory **8** (1976), 271–279.

[6] Y. Mizusawa: *On the maximal unramified pro-2-extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields* II, Acta Arith. **119** (2005), 93–107.

[7] Y. Mizusawa: *On the maximal unramified pro-2-extension over the cyclotomic* $\mathbb{Z}_2$*-extension of an imaginary quadratic field*, J. Théor. Nombres Bordeaux **22** (2010), 115–138.

[8] J.-P. Serre: Cohomologie Galoisienne, With a contribution by Jean-Louis Verdier, Lecture Notes in Mathematics **5**, Troisieme edition, Springer, Berlin, 1965.

[9] L.C. Washington: Introduction to Cyclotomic Fields, second edition, Graduate Texts in Mathematics **83**, Springer, New York, 1997.

Laboratoire Emile Picard
Institut de Mathématiques de Toulouse
118, route de Narbonne
31400 Toulouse
France
e-mail: salle@math.univ-toulouse.fr