TOKYO J. MATH.
VOL. 31, NO. 2, 2008

On the p-class Tower of a $\mathbf{Z}_p$-extension

Ali MOUHIB and Abbas MOVAHHEDI

Université Side Mohamed Ben Ablellah and Université de Limoges

(Communicated by M. Kurihara)

Abstract. For a number field k and a prime number p, let k_∞ be a $\mathbf{Z}_p$-extension of k and $X_\infty(k)$ the Galois group over k_∞ of the maximal abelian unramified p-extension of k_∞. We first give a sufficient condition, bearing on the norm index of units in the layers of k_∞, for $X_\infty(k)$ to be finite. When the prime p is 2 and $X_\infty(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, we study the structure of the Galois group of the maximal unramified p-extension of k_∞, improving on some previous results in the case of quadratic fields.

1. Introduction

Let p be a prime number and $\mathbf{Z}_p$ the additive group of p-adic integers. Let k be an algebraic number field and k_∞ any $\mathbf{Z}_p$-extension of k. For any integer $n \geq 1$, we denote by k_n the n-th layer of k_∞/k and by A_n the p-class group of k_n. The p-class group of k will be simply denoted by A. As usual λ, μ and ν will be the Iwasawa invariants corresponding to the series of groups A_n: for n large the order of A_n is given by $p^{\lambda n+\mu p^n+\nu}$.

Let $\mathcal{L}_\infty$ be the maximal unramified p-extension of k_∞ and L_∞ the maximal abelian sub-extension of $\mathcal{L}_\infty/k_\infty$. If the number field k is totally real, the now famous conjecture of Greenberg predicts the vanishing of the two invariants λ and μ [Gr1, Gr2]. The μ-invariant vanishes precisely when the p-ranks of A_n are bounded independently of n. When k is abelian over the field of rational numbers $\mathbf{Q}$, and k_∞ is the cyclotomic $\mathbf{Z}_p$-extension of k, then we know that the corresponding μ-invariant vanishes [F-W]. For $p = 3$ and $k = \mathbf{Q}(\sqrt{39345017})$, Y. Mizusawa shows that the abelian extension L_∞/k_∞ is finite, while $\mathcal{L}_\infty/k_\infty$ is infinite [M1]. More generally, M. Ozaki showed that for any prime number p, there exist infinitely many number fields k (cyclic extensions of $\mathbf{Q}$ of degree p) such that L_∞/k_∞ is finite while $\mathcal{L}_\infty/k_\infty$ is infinite [O].

Let n_0 be the smallest integer such that all ramified primes in k_∞/k are totally ramified in k_∞/k_{n_0} and denote by U_n, for any integer n, the group of global units of k_n. In this paper, we first give a sufficient condition, bearing on the norm index $[U_{n_0} : U_{n_0} \cap N_{k_{n_0+1}/k_{n_0}}(k^*_{n_0+1})]$, for $X_\infty(k) := G(L_\infty/k_\infty)$ to be finite (Theorem 2.1, Corollary 2.6). Then, in section 3, we fix the

Received November 9, 2006; revised May 7, 2007
2000 *Mathematics Subject Classification*: 11R23, 11R11
This work was partially financed as part of project no 18607 of the CNRS/CNRST cooperation.

prime p to be 2 and study the structure of the Galois group $G(\mathcal{L}_\infty/k_\infty)$ when its abelianized $X_\infty(k)$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. There exist exactly three infinite families of non-abelian finite 2-groups which have such a property. Namely the dihedral, the semidihedral and the generalized quaternion groups (see Section 3). Let N be the smallest integer for which we simultaneously have $A(k_N) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and k_∞/k_N totally ramified at a prime of k_N. In Theorem 3.1, we prove that if $X_\infty(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and the Galois group $G(\mathcal{L}_N/k_N)$ is of quaternion type or semidihedral, then we have $G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}_N/k_N)$. Theorem 2 of [M3] turns out to be a special case of Theorem 3.1, which deals with general number fields rather than quadratic ones (see Example 3.2). Theorem 3.3 gives infinite families of quadratic fields for which the Galois group $G(\mathcal{L}_\infty/k_\infty)$ is a dihedral or generalized quaternion 2-group (see also the main Theorem of [M2] and Theorem 1 of [M3]).

The authors would like to thank Thong NGUYEN QUANG DO for his remarks on a preliminary version of this paper and also an anonymous referee for helpful comments.

2. Structure of $X_\infty(k)$ for certain number fields k

The following notations will be used throughout the paper:

p	a prime number
k	a number field
k_∞	a $\mathbf{Z}_\mathrm{p}$-extension of k
k_n	the n-th layer of k_∞/k
U_n	the group of units of k_n
A_n	the p-class group of k_n
L_n	the maximal abelian unramified p-extension of k_n
L_∞	the maximal abelian unramified p-extension of k_∞
$\mathcal{L}_n$	the maximal unramified p-extension of k_n
$\mathcal{L}_\infty$	the maximal unramified p-extension of k_∞
n_0	the smallest integer such that all ramified primes in k_∞/k are totally ramified in k_∞/k_{n_0}
s	the number of primes of k_{n_0} which are ramified in k_∞
$X_\infty(k)$	the Galois group $G(L_\infty/k_\infty)$
$N_{E/F}$	the norm map with respect to an extension E/F.

It is known that if the Iwasawa invariants λ and μ (corresponding to $X_\infty(k)$) vanish, then for n large enough, we have $A_n \overset{\sim}{\leftarrow} A_{n+1} \overset{\sim}{\leftarrow} A_{n+2} \overset{\sim}{\leftarrow} \ldots$. So, in this case, the Galois group $G(k_{n+1}/k_n)$ acts trivially on A_{n+1} and the ambiguous class formula in k_{n+1}/k_n reads as follow:

$$|A_{n+1}| = \frac{|A_n|p^s}{[k_{n+1}:k_n][U_n : U_n \cap N_{k_{n+1}/k_n}(k_{n+1}^*)]}$$
$$= \frac{|A_n|p^{s-1}}{[U_n : U_n \cap N_{k_{n+1}/k_n}(k_{n+1}^*)]}$$

Hence, for such an n, we have the following equality for the norm index of the multiplicative group of non zero elements of k_{n+1} inside the units of k_n:

$$[U_n : U_n \cap N_{k_{n+1}/k_n}(k_{n+1}^*)] = p^{s-1} .$$

The following theorem studies the converse:

THEOREM 2.1. *Let k be a number field and let k_∞ be any $\mathbf{Z}_\text{p}$-extension of k. Suppose that $A_{n_0} \neq 0$ and that the p-adic primes of k_{n_0} which are ramified in k_∞ remain inert in L_{n_0}. If, furthermore, $[U_{n_0} : U_{n_0} \cap N_{k_{n_0+1}/k_{n_0}}(k_{n_0+1}^*)] = p^{s-1}$, then $X_\infty(k) \overset{\sim}{\to} A_{n_0}$, in particular $\lambda = \mu = 0$.*

To prove the theorem we will need the following two lemmas:

LEMMA 2.2 ([Iw, §4]). *Let k be a number field. Suppose that the maximal unramified p-extension K of k is of finite degree over k. Denote by G the Galois group of K/k. Let U_k (resp. U_K) be the group of units of k (resp. K). Then*

$$U_k/N_{K/k}(U_K) \simeq M(G) ,$$

where $M(G) = H^2(G, \mathbf{Q}_\text{p}/\mathbf{Z}_\text{p})$ is the Schur multiplier of G.

Note that when F/k is an unramified cyclic p-extension, the Hasse local-global principle allows us to see that each unit of k is the norm of an element (which is not necessarily a unit) of F. If, furthermore, the p-class group of F is trivial, then the preceding lemma immediately yields the following:

COROLLARY 2.3. *If the p-class group of k is cyclic then, the maximal unramified p-extension K being the Hilbert p-class field of k, G is cyclic and $M(G) = 0$. In particular, in this case, each unit of k is the norm of a unit of K.*

LEMMA 2.4 ([F, Theorem 1]). *Let k_∞/k be a $\mathbf{Z}_\text{p}$-extension and n any integer $\geq n_0$.*

(i) *If $|A_n| = |A_{n+1}|$, then $|A_m| = |A_n|$ for all $m \geq n$. Hence $\lambda = \mu = 0$.*

(ii) *If $rank(A_{n+1}) = rank(A_n)$, then $rank(A_m) = rank(A_n)$ for all $m \geq n$. Hence $\mu = 0$.*

PROOF OF THEOREM 2.1. Introduce the field $F_{n_0+1} := L_{n_0}k_{n_0+1}$. Since k_∞/k_{n_0} is totally ramified, we have:

$$[F_{n_0+1} : k_{n_0+1}] = [L_{n_0} : k_{n_0}] .$$

The extension L_{n_0}/k_{n_0} is cyclic since, by hypothesis, the p-adic primes which are ramified in k_∞ are inert therein. Thus, by corollary 2.3, each unit of k_{n_0} is the norm of a unit of L_{n_0}. So, the map induced by the norm in the extension L_{n_0}/k_{n_0}:

$$U_{L_{n_0}}/U_{L_{n_0}} \cap N_{F_{n_0+1}/L_{n_0}}(F_{n_0+1}^*) \to U_{n_0}/U_{n_0} \cap N_{k_{n_0+1}/k_{n_0}}(k_{n_0+1}^*)$$

is surjective. Hence:

$$[U_{L_{n_0}} : U_{L_{n_0}} \cap N_{F_{n_0+1}/L_{n_0}}(F_{n_0+1}^*)] \geq [U_{n_0} : U_{n_0} \cap N_{k_{n_0+1}/k_{n_0}}(k_{n_0+1}^*)] = p^{s-1} ,$$

where we recall that s is the number of p-adic primes of k_{n_0} which are ramified in k_∞. Besides, since A_{n_0} is cyclic, the class number of L_{n_0} is prime to p. Also, by hypothesis, all the p-adic primes of k_{n_0} remain inert in L_{n_0}. Accordingly, the ambiguous class formula for the p-class groups in F_{n_0+1}/L_{n_0} reads:

$$|A(F_{n_0+1})^{G(F_{n_0+1}/L_{n_0})}| = \frac{p^{s-1}}{[U_{L_{n_0}} : U_{L_{n_0}} \cap N_{F_{n_0+1}/L_{n_0}}(F^*_{n_0+1})]}.$$

Taking into account the previous inequality, $A(F_{n_0+1})^{G(F_{n_0+1}/L_{n_0})}$ must be trivial. In other words $F_{n_0+1} = L_{n_0+1}$. Hence $A_{n_0+1} \xrightarrow{\sim} A_{n_0}$. Now we can apply Lemma 2.4: $X_\infty(k) \xrightarrow{\sim} A_{n_0}$ and so $\lambda = \mu = 0$. ∎

REMARK 2.5. Suppose that $A_{n_0} \neq 0$ and that the p-adic primes of k_{n_0} remain inert in L_{n_0} (especially A_{n_0} is cyclic). Denote by $\mathcal{P}_{n_0}$ a p-adic prime of k_{n_0} which is totally ramified in k_∞. If the number field k is totally real and if there exists an integer $n > n_0$ such that A_n is also cyclic, then under Leopoldt's conjecture, it can be proved that $X_\infty(k)$ is finite without resorting to the condition $[U_{n_0} : U_{n_0} \cap N_{k_{n_0+1}/k_{n_0}}(k^*_{n_0+1})] = p^{s-1}$ which intervenes in Theorem 2.1. Indeed, by Lemma 2.4, the group $X_\infty(k)$ is cyclic (of finite or infinite order). Moreover, one readily verifies that for all $n \geq n_0$, the class group A_n is generated by the p-adic prime of k_n lying above $\mathcal{P}_{n_0}$. This shows that the action of the Galois group $G(k_\infty/k)$ on A_n is trivial. On the other hand, if we assume Leopoldt's conjecture for k then, by [Gr1, Proposition 1], the order of $A_n^{G(k_\infty/k)}$ is bounded when n increases. This allows us to conclude that $X_\infty(k)$ is finite.

COROLLARY 2.6. *Suppose that $A_{n_0} \neq 0$ and that there is only one p-adic prime in L_{n_0}. Then $X_\infty(k)$ is a finite cyclic group isomorphic to A_{n_0}.*

PROOF. By hypotheses, we have $s = 1$, and A_{n_0} is cyclic since the p-adic prime of k_{n_0} is inert in L_{n_0}. Moreover, by the Hasse local-global principle (alternatively, by the ambiguous class formula) for the cyclic extension k_{n+1}/k_n, we see that for each $n \geq n_0$, all units of k_n are norms from elements of k_{n+1}. Thus the preceding theorem applies. ∎

We notice that when the number field k is abelian over $\mathbf{Q}$, and when the prime number p is odd, the hypotheses of the preceding corollary are not satisfied [N-L, lemma 1.5]. However for $p = 2$, as the following example shows, such a situation is perfectly possible: let p and q be two prime numbers such that $p \equiv -q \equiv 1 \pmod 4$ and $k = \mathbf{Q}(\sqrt{pq})$. The prime 2 is then totally ramified in the cyclotomic $\mathbf{Z}_2$-extension of k, so $n_0 = 0$. Suppose also that the Legendre symbol $\left(\frac{2}{p}\right) = -1$, then the 2-adic prime of k is inert in $\mathbf{Q}(\sqrt{p}, \sqrt{q})$ which is simply the Hilbert 2-class field of k [R-R]. Thus the hypotheses of the preceding corollary are satisfied and $X_\infty(k)$ is isomorphic to $A_0 = A(k) \simeq \mathbf{Z}/2\mathbf{Z}$. ∎

EXAMPLE 2.7. Let p_1 and p_2 be two prime numbers such that $p_1 \equiv p_2 \equiv 5 \pmod 8$ and $k = \mathbf{Q}(\sqrt{p_1 p_2})$. Suppose that $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, where $\varepsilon_{p_1 p_2}$ is the fundamental unit of k (*i.e.* the unit ε which generates the unit group of k modulo ± 1, with the property that $\iota(\varepsilon) > 1$ under a fixed embedding ι of k into $\mathbf{R}$). Then $\lambda(k) = 0$. Indeed according to genus theory the 2-class group of k is cyclic. The congruences $p_1 \equiv p_2 \equiv 5\,(mod\,8)$ show that 2 splits into two prime ideals $\mathcal{P}_1$ and $\mathcal{P}_2$ in k. These primes $\mathcal{P}_1$ and $\mathcal{P}_2$ remain inert in $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$, which is an unramified extension of k. Hence $\mathcal{P}_1$ et $\mathcal{P}_2$ remain inert in L. So we have $s = 2$ and A_0 cyclic. Thus all we need to apply Theorem 2.1, is to prove the following equality:

$$[U_k : U_k \cap N_{k_1/k}(k_1^*)] = 2\,,$$

where $k_1 = k(\sqrt{2})$. As $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, we can easily verify that there exist two rational integers y_1 and y_2 such that $\sqrt{\varepsilon_{p_1 p_2}} = \frac{1}{2}(y_1\sqrt{p_1} + y_2\sqrt{p_2})$(see for example [A-M, proof of Lemma 1]). Hence $p_1\varepsilon_{p_1 p_2}$ is a square in k and we can compute the following norm residue symbol in k_1/k:

$$\left(\frac{\varepsilon_{p_1 p_2},\ 2}{\mathcal{P}_1}\right) = \left(\frac{p_1,\ 2}{\mathcal{P}_1}\right) = \left(\frac{2}{p_1}\right) = -1\,.$$

Thus $\varepsilon_{p_1 p_2}$ is not a norm in k_1/k and the result holds. In fact, M. Ozaki and H. Taya [O-T] showed the vanishing of $\lambda(k)$ for prime numbers $p_1 \equiv p_2 \equiv 5\,(\mathrm{mod}\,8)$, without assuming $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$.

In what follows we are going to apply the results of this section to quadratic fields, with $p = 2$.

3. Application

Throughout this section we take the prime number to be 2. We will be interested in the number fields k for which $X_\infty(k)$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and we are going to study the (not necessarily abelian) Galois group $G(\mathcal{L}_\infty/k_\infty)$.

Any pro-2-group (not necessarily finite) whose abelianization is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is metabelian. It is known [G, Chap. 5, Theorem 4.5] that there exist exactly three infinite families of non-abelian finite 2-groups $\mathcal{G}$ of which the largest abelian factor groups are isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Namely, the generalized quaternion groups Q_m, dihedral groups D_m and the semidihedral groups S_m, of order exactly 2^m, with $m \geq 3$ for the first two families and $m \geq 4$ for the last. A representation by generators and relations of these three families are given by:

$$Q_m = \langle x, y \mid x^{2^{m-2}} = y^2 = a, a^2 = 1, y^{-1}xy = x^{-1}\rangle\,;$$

$$D_m = \langle x, y \mid x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{-1}\rangle\,;$$

$$S_m = \langle x, y \mid x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{2^{m-2}-1}\rangle\,.$$

In this section we will use the following known properties of these groups $\mathcal{G}$ (see, for instance, [Ki, Section 1]). The commutator subgroup $\mathcal{G}'$ of $\mathcal{G}$ is always cyclic: $\mathcal{G}' = \langle x^2 \rangle$. These groups $\mathcal{G}$ possess exactly three sub-groups of index 2. Namely, $\langle x \rangle$; $\langle x^2, y \rangle$ and $\langle x^2, xy \rangle$. When $\mathcal{G}$ is not the quaternion group of order 8, only one of the three maximal sub-groups of $\mathcal{G}$ is cyclic. When $m \geq 4$ the other two maximal sub-groups of $\mathcal{G}$ are not abelian and their maximal abelian factor groups are again isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Of course, when $\mathcal{G}$ is the quaternion group of order 8 its three maximal subgroups are cyclic and when $\mathcal{G}$ is the dihedral group of order 8, its three subgroups are abelian. None of the proper factor groups of $\mathcal{G}$ is of quaternion type. This will be needed in the proof of the next Theorem.

Now let k be a number field whose 2-class group is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Then, according to what we have just said, the Hilbert 2-class field tower of k terminates in at most two steps. Denote by H_1 the Hilbert 2-class field of k and by H_2 that of H_1. If $H_2 \neq H_1$, then the Galois group $G(H_2/H_1)$ is cyclic and $G(H_2/k)$ is a quaternion, dihedral or semidihedral group.

For a non-square positive integer m, denote by ε_m (resp. $h(m)$), the fundamental unit (resp. the 2-part of the class number) of the quadratic field $\mathbf{Q}(\sqrt{m})$. For any number field K and any $\mathbf{Z}_2$-extension K_∞/K, we denote by $A(K_n)$ the 2-class group of the n-th layer K_n.

We are now ready to prove the following

THEOREM 3.1. *Let k be a number field such that $X_\infty(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Let N be the smallest integer for which we simultaneously have $A(k_N) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and k_∞/k_N totally ramified at a prime of k_N. If the Galois group $G(\mathcal{L}_N/k_N)$ is of quaternion type or semidihedral, then we have*

$$G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}_N/k_N)\,.$$

In particular, $\lambda(K) = \mu(K) = 0$ for any unramified extension K of k.

PROOF. According to our hypotheses, for any integer $n \geq N$, we have $A(k_n) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Also, for $n \geq N$, the Galois group $G(\mathcal{L}_n/k_n)$ maps surjectively onto $G(\mathcal{L}_N/k_N)$.

(i) The Galois group $G(\mathcal{L}_N/k_N)$ is of quaternion type only when $G(\mathcal{L}_n/k_n) \simeq G(\mathcal{L}_N/k_N)$, since no proper factor group of $G(\mathcal{L}_n/k_n)$ is of quaternion type.

(ii) When $G(\mathcal{L}_N/k_N)$ is semidihedral, replacing k_N by a quadratic extension K_N inside L_N, the statement is reduced to the previous case. More precisely, we know that there exists a quaternion type sub-group with index 2 in $G(\mathcal{L}_N/k_N)$. Denote by K_N the sub-extension of L_N fixed by this sub-group. Since k_∞/k_N is totally ramified at a prime of k_N, this is also the case of K_∞/K_N, where $K_\infty := K_N k_\infty$. Now it is enough to apply case (i) to the $\mathbf{Z}_2$-extension K_∞/K_N in order to obtain $G(\mathcal{L}_\infty/K_\infty) \simeq G(\mathcal{L}_N/K_N)$. Consequently, $G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}_N/k_N)$. ∎

As we are going to see now, by specializing to the quadratic case, this last theorem contains Theorem 2 of [M3] which corresponds to the case A-(i) below. Let d be a square-free integer and $k := \mathbf{Q}(\sqrt{d})$. Suppose that the 2-class group A_1 of $k_1 = \mathbf{Q}(\sqrt{d}, \sqrt{2})$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. We first notice that the Galois group $G(\mathcal{L}_1/k_1)$ is never semidihedral (see [A-M, Theorems 8,9,10 and 15]). There follows a complete list of quadratic fields for which $G(\mathcal{L}_1/k_1)$ is of quaternion type [A-M, Theorems 7, 8, 9 and Proposition 10]:

(A) $k = \mathbf{Q}(\sqrt{p_1 p_2})$ where $p_1 \equiv 1,\ p_2 \equiv 5 \pmod 8$ are two distinct primes satisfying one of the two following conditions.

(i) $\left(\frac{p_1}{p_2}\right) = -1,\ \left(\frac{2}{p_1}\right)_4 = (-1)^{\frac{(p_1-1)}{8}},\ N_{\mathbf{Q}(\sqrt{2p_1})/\mathbf{Q}}(\varepsilon_{2p_1}) = -1$ and $Q_M = 2$;

(ii) $\left(\frac{p_1}{p_2}\right) = 1,\ \left(\frac{2}{p_1}\right)_4 = (-1)^{\frac{(p_1-1)}{8}} = 1,\ \left(\frac{p_2}{p_1}\right)_4 \neq \left(\frac{p_1}{p_2}\right)_4$ and $N_{\mathbf{Q}(\sqrt{2p_1})/\mathbf{Q}}(\varepsilon_{2p_1}) = 1$.

Here, for distinct primes $p \neq 2$ and q, the rational fourth-power residue symbol $\left(\frac{q}{p}\right)_4$ is 1 or -1, according to whether q is a fourth-power residue of p or not. It is defined provided the Legendre symbol $\left(\frac{q}{p}\right) = 1$. We recall that $\left(\frac{2}{p}\right)_4 \equiv 2^{(p-1)/4} \pmod p$. In A-(i) above, Q_M stands for the Hasse unit index of the group generated by the units of the three quadratic subfields in the unit group of the biquadratic field $M := \mathbf{Q}(\sqrt{2p_1}, \sqrt{p_2})$. Since $p_1 \equiv 1 \pmod 8$, we also remark that in A-(i), the condition $N_{\mathbf{Q}(\sqrt{2p_1})/\mathbf{Q}}(\varepsilon_{2p_1}) = -1$ implies that $4 \mid h(2p_1)$ (see, for instance, [C-H, Corollary 19.8]).

(B) $k = \mathbf{Q}(\sqrt{pq_1q_2})$ where $p \equiv -q_1 \equiv -q_2 \equiv 1 \pmod 4$ are three distinct primes satisfying one of the following conditions

(i) $\left(\frac{2}{p}\right) = -\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) = -\left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right) = 1,\ \left(\frac{2}{q_1}\right) = \left(\frac{q_1}{p}\right),\ \left(\frac{2}{p}\right)_4 = (-1)^{\frac{(p-1)}{8}}$ and $N_{\mathbf{Q}(\sqrt{2p})/\mathbf{Q}}(\varepsilon_{2p}) = -1$;

(ii) $\left(\frac{2}{p}\right) = -1,\ \left(\frac{2}{q_1}\right) = \left(\frac{2}{q_2}\right) = 1,\ \left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$ and $u = 2$;

(iii) $\left(\frac{2}{p}\right) = -1,\ \left(\frac{2}{q_1}\right) = \left(\frac{2}{q_2}\right) = 1,\ \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right) = -1$ and $u \in \{2q_1, 2q_2\}$;

with the additional condition "the Galois group $G(\mathcal{L}_1/k_1)$ is not abelian" in the cases B-(ii) and B-(iii). Here u is the square-free integer characterized by the fact that $\frac{1}{u} N_{\mathbf{Q}(\sqrt{2q_1q_2})/\mathbf{Q})}(1+\varepsilon_{2q_1q_2})$ is a perfect square.

Now let $k = \mathbf{Q}(\sqrt{d})$ be one of the quadratic fields introduced just above. To apply Theorem 3.1 to k, it suffices to suppose that the class number of k_2 is not divisible by 8 since then $A_1 \simeq A_2 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ so as to satisfy the hypotheses of Theorem 3.1 with $N = 1$ (Lemma 2.4). The following example, carrying out in detail the above case A-(i), corresponds to Theorem 2 of [M3].

EXAMPLE 3.2. Let $k := \mathbf{Q}(\sqrt{p_1 p_2})$, with p_1 and p_2 two distinct prime integers such that

$$p_1 \equiv 1,\ p_2 \equiv 5 \pmod 8\,, \quad \left(\frac{p_2}{p_1}\right) = -1\,, \quad \left(\frac{2}{p_1}\right)_4 = (-1)^{(p_1-1)/8}\,.$$

Then the 2-class group A_1 of k_1 is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Assuming that the class number of k_2 is not divisible by 8 (condition C_2 of [M3, Theorem 2]), we also have

$A_2 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and so $X_\infty(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. The Galois group $G(\mathcal{L}_1/k_1)$ is either abelian or dihedral or of quaternion type [A-M, Proposition 10, Theorem 8]. Moreover, if the 2-adic prime of $M = \mathbf{Q}(\sqrt{2p_1}, \sqrt{p_2})$ is not principal (condition C_1 of [M3, Theorem 2]), then $G(\mathcal{L}_1/k_1)$ turns out to be of quaternion type. Finally, by Theorem 3.1, we get

$$G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}_1/k_1)\,.$$

As in Theorem 3.1, in general $G(\mathcal{L}_\infty/k_\infty)$ is not isomorphic to $G(\mathcal{L}_N/k_N)$. We will construct such a counter example in the next theorem with $N = 0$. Let k be a real quadratic field such that $A(k) \simeq A(k_1) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Suppose k_∞/k totally ramified at 2-adic primes so that $X_\infty(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (Lemma 2.4 (i)). It is well known that for such a quadratic field k, its 2-genus field is the same as its 2-Hilbert class field. From this we immediately deduce that the same holds for $k_1 = k(\sqrt{2})$. Such a quadratic field k is of one of the two following forms [A-M, Theorem 5]:

(1) $k = \mathbf{Q}(\sqrt{q_1q_2q_3})$, with q_1, q_2 and q_3 three distinct prime numbers such that $q_1 \equiv 7 \pmod 8$, $q_2 \equiv q_3 \equiv 3 \pmod 8$ and $\left(\frac{q_1}{q_2}\right)\left(\frac{q_1}{q_3}\right) = -1$;

(2) $k = \mathbf{Q}(\sqrt{p_1p_2q})$, with p_1, p_2 and q three distinct prime numbers such that $p_1 \equiv p_2 \equiv 5 \pmod 8$, $q \equiv 3 \pmod 4$ and $\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right) = -1$.

In the first case, we have $L = \mathcal{L}$ [B-S, Theorem 1] and $L_1 = \mathcal{L}_1$ [A-M, Theorem 11]. Consequently the Galois group $G(\mathcal{L}_\infty/k_\infty)$ is abelian (Lemma 2.4). In what follows we are going to be interested in case (2) which is to be compared with the main Theorem of [M2] and Theorem 1 of [M3]:

THEOREM 3.3. *Let $k = \mathbf{Q}(\sqrt{p_1p_2q})$ where p_1, p_2 and q be three distinct prime numbers such that $p_1 \equiv p_2 \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$. Suppose that $\left(\frac{q}{p_1}\right) = -\left(\frac{q}{p_2}\right) = 1$. Then $G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}/k)$ precisely when $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$. Moreover, in this case, the Galois group $G(\mathcal{L}_\infty/k_\infty)$ is dihedral of order $4h(p_1p_2)$.*

The proof of this theorem requires a result on the units of biquadratic fields:

LEMMA 3.4. *Let p_1, p_2 and q be as in the statement of the theorem. Then a system of fundamental units of the biquadratic field $E := \mathbf{Q}(\sqrt{p_1p_2}, \sqrt{q})$ is given by*

(i) $\{\varepsilon_q, \varepsilon_{p_1p_2}, \sqrt{\varepsilon_{p_1p_2}\varepsilon_{p_1p_2q}}\}$ *when* $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$.

(ii) $\{\varepsilon_q, \varepsilon_{p_1p_2}, \varepsilon_{p_1p_2q}\}$ *when* $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = -1$.

PROOF. By [A-M, Proof of Lemma 5], there exist two rational numbers x_1 and x_2, such that

(a) If $\left(\frac{p_1}{p_2}\right) = 1$, then $\sqrt{\varepsilon_{p_1p_2q}} = x_1\sqrt{p_1} + x_2\sqrt{p_2q}$

(b) If $\left(\frac{p_1}{p_2}\right) = -1$, then $\sqrt{\varepsilon_{p_1p_2q}} = x_1\sqrt{2p_1} + x_2\sqrt{2p_2q}$.

Besides, it is easy to see that there exist two rational numbers x_3 and x_4 such that

(c) $\sqrt{\varepsilon_q} = x_3\sqrt{2} + x_4\sqrt{2q}$.

(i) When $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$, it is easy to see [A-M, Proof of Lemma 1] that there exist two rational numbers x_5 and x_6 such that

(d) $\sqrt{\varepsilon_{p_1p_2}} = x_5\sqrt{p_1} + x_6\sqrt{p_2}$.

Moreover, in this case $\left(\frac{p_1}{p_2}\right) = 1$ (see, for instance, [C-H, Proposition 19.9]) and, by (a), (c) and (d), we see that $\{\varepsilon_q, \varepsilon_{p_1p_2}, \sqrt{\varepsilon_{p_1p_2}\varepsilon_{p_1p_2q}}\}$ is a system of fundamental units of E [Ku, Satz 11].

(ii) When $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = -1$, the unit $\varepsilon_{p_1p_2}$ is not a square in E. Hence by (a), (b) and (c), we see that $\{\varepsilon_q, \varepsilon_{p_1p_2}, \varepsilon_{p_1p_2q}\}$ is a system of fundamental units of E [Ku, Satz 11]. ∎

PROOF OF THEOREM 3.3. The maximal abelian unramified 2-extension of k is given by $L = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$. Introduce the biquadratic intermediate field $E = \mathbf{Q}(\sqrt{p_1p_2}, \sqrt{q})$. In E we have $2 = \mathcal{P}^2\mathcal{P}'^2$. These two prime ideals $\mathcal{P}$ and $\mathcal{P}'$ remain inert in L and are totally ramified in E_∞, the cyclotomic $\mathbf{Z}_2$-extension of E.

Suppose first that $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = -1$. By Lemma 3.4 the set $\{\varepsilon_q, \varepsilon_{p_1p_2}, \varepsilon_{p_1p_2q}\}$ consists of a system of fundamental units of E. We want to know if each unit of E is a norm from $E_1 = E(\sqrt{2})$. So we are going to study the norm residue symbol $\left(\frac{u,\,2}{\mathcal{P}}\right)$, when u runs through the above system of fundamental units of E:
As $\mathcal{P}$ is ramified in the extension $E/\mathbf{Q}(\sqrt{p_1p_2})$, the properties of the norm residue symbol yield:

$$\left(\frac{u,\ 2}{\mathcal{P}}\right) = \left(\frac{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(u),\ 2}{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right).$$

Since $q \equiv 3 \pmod 4$, by the Hasse norm principle -1 is a norm neither in $\mathbf{Q}(\sqrt{q})/\mathbf{Q}$ nor in $\mathbf{Q}(\sqrt{p_1p_2q})/\mathbf{Q}$. Hence,

$$N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(u) = \begin{cases} \varepsilon_{p_1p_2}^2 & \text{for } u = \varepsilon_{p_1p_2}\,, \\ 1 & \text{for } u \in \{\varepsilon_q, \varepsilon_{p_1p_2q}\}\,. \end{cases}$$

So it is clear that

$$\left(\frac{u,\ 2}{\mathcal{P}}\right) = 1\,.$$

In other words, once again by the Hasse norm principle, each unit of E is a norm from E_1. Accordingly, by the ambiguous class formula, we get:

$$|\ A(E_1)\ | \geq |\ A(E_1)^{G(E_1/E)}\ | = 2\ |\ A(E)\ |\ .$$

Hence $X_\infty(E) \not\simeq A(E)$, and especially $G(\mathcal{L}_\infty/k_\infty)$ is not isomorphic to $G(\mathcal{L}/k)$.

If instead $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$, then, by Lemma 3.4, $u = \sqrt{\varepsilon_{p_1p_2}\varepsilon_{p_1p_2q}}$ is a unit in E. As in the previous case, we have:

$$\left(\frac{u,\ 2}{\mathcal{P}}\right) = \left(\frac{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(u),\ 2}{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right) = \left(\frac{\pm\varepsilon_{p_1p_2},\ 2}{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right).$$

On the other hand, the relation $\sqrt{\varepsilon_{p_1p_2}} = x_5\sqrt{p_1} + x_6\sqrt{p_2}$ of the proof of Lemma 3.4 shows that $\varepsilon_{p_1p_2}/p_1$ is a square in $\mathbf{Q}(\sqrt{p_1p_2})$. Hence

$$\left(\frac{u,\ 2}{\mathcal{P}}\right) = \left(\frac{\pm p_1,\ 2}{N_{E/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right) = \left(\frac{2}{p_1}\right) = -1$$

and the unit u is not a norm in the extension E_1/E.

Let us now prove that the 2-primary part $A(E)$ of the class group of E is cyclic in order to apply Theorem 2.1 (the 2-adic primes of E being inert in $L = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$, they remain inert in the Hilbert 2-class field of E). Denote $F := \mathbf{Q}(\sqrt{q})$. Since $A(F)$ is odd, by the genus formula the 2-rank of $A(E)$ is given by:

$$rk_2(A(E)) = t(E/F) - rk_2(U_F/U_F \cap N_{E/F}(E^*)) - 1\,,$$

where $t(E/F) = 3$ is the number of the primes which ramify in E/F, and U_F is the group of units of the quadratic field F. The relation $\sqrt{\varepsilon_q} = x_3\sqrt{2} + x_4\sqrt{2q}$ of the proof of lemma 3.4 shows that $\varepsilon_q/2$ is a square in F. The hypotheses made on p_1, p_2 and q prevent 2 (hence also ε_q) from being a norm in E/F and therefore $rk_2(A(E)) = 1$. Applying Theorem 2.1 to the field E, we obtain: $X_\infty(E) \simeq A(E) \simeq G(\mathcal{L}/E)$, which immediately yields: $G(\mathcal{L}_\infty/k_\infty) \simeq G(\mathcal{L}/k)$.

To finish the proof of Theorem 3.3, it remains to compute the order of $G(\mathcal{L}/k)$. Since $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$, we have $\left(\frac{p_1}{p_2}\right) = 1$. In this case $G(\mathcal{L}/k)$ is dihedral [B-S, table 2 page 175]. Besides, the class number formula for real biquadratic fields yields the 2-part of the class number $h(E)$ of E :

$$\frac{Q_E h(q)h(p_1p_2)h(p_1p_2q)}{4}$$

where Q_E is the Hasse unit index of the biquadratic field E (see, for instance, [S, Chapter 3, Section 12]). We have already noticed that $h(k) := h(p_1p_2q) = 4$ and $Q_E = 2$ (see Lemma 3.4). Consequently, $h(E) = 2h(p_1p_2)$ and $|G(\mathcal{L}_\infty/k_\infty)| = 2|A(E)|$ is of order $4h(p_1p_2)$. ∎

REMARKS 3.5. Let us keep the notations and hypotheses of Theorem 3.3 and Lemma 3.4. Then

(i) since $X_\infty(E) \cong A(E)$ is of order $2h(p_1p_2) = 2^{m+1}$, the smallest layer of E_∞/E in which the 2-classes of E capitulate is E_{m+1}. More generally, for all integers n the smallest layer of E_∞/E_n in which the 2-classes of E_n capitulate is E_{n+m+1}. This comes from the fact that for all integers n, the 2-adic primes of E_n remain inert in the 2-Hilbert class field of E_n.

(ii) Let K be an unramified extension of k. By Theorem 3.3, we have $\lambda(K) = \mu(K) = 0$, if $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$. This last result remains valid even independently of the value of the norm $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2})$. An outline of the proof goes as follows. Let $E = \mathbf{Q}(\sqrt{p_1p_2}, \sqrt{q})$ be the biquadratic field introduced in the proof of Theorem 3.3. It suffices to prove that $X_\infty(E)$ is a (finite or infinite) cyclic group (which already shows that $\lambda(E) \leq 1$ and $\mu(E) = 0$) and to notice that for each integer n, we have $A(E_n) = A(E_n)^{Gal(E_\infty/E)}$ (this comes from the fact that the 2-adic primes of E_n are inert in the 2-Hilbert class field of E_n). Hence the order of $A(E_n)$ is bounded when n goes to infinity [Gr1, Proposition 1]. Consequently $\lambda(E) = \mu(E) = 0$ and the same holds for each intermediate field between k and $\mathcal{L}$.

If we fix in advance distinct prime numbers $p_1 \equiv p_2 \equiv 5 \pmod 8$ such that $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$, then we know that there exist infinitely many prime numbers $q \equiv -1 \pmod 4$ such that $\left(\frac{q}{p_1}\right) = -\left(\frac{q}{p_2}\right) = 1$. Hence, there exist infinitely many quadratic fields k with dihedral Galois group $G(\mathcal{L}_\infty/k_\infty)$ of order $4h(p_1p_2)$. Numerically, one may take $p_1 = 5$ and $p_2 = 389$. In this case, $h(5 \cdot 389) = 2$. So there exist infinitely many quadratic fields k of the form $\mathbf{Q}(\sqrt{5 \cdot 389q})$ such that $G(\mathcal{L}_\infty/k_\infty)$ is dihedral of order 8.

Consider now a power 2^m of 2. Suppose there exist two distinct prime numbers $p_1 \equiv p_2 \equiv 5 \pmod 8$ such that $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$. If the class number of the quadratic field $\mathbf{Q}(\sqrt{p_1p_2})$ is divisible by 2^m (for instance, when $p_1p_2 = a^{2^{m+1}} + 4$ for an odd integer $a \geq 3$ [I]), then there are infinitely many quadratic fields $k := \mathbf{Q}(\sqrt{p_1p_2q})$ with $G(\mathcal{L}_\infty/k_\infty)$ dihedral of order divisible by 2^m (Theorem 3.3). Moreover, since the non-cyclic subgroups of a dihedral group are also dihedral, we see that there exist infinitely many number fields K (unramified extensions of k) for which $G(\mathcal{L}_\infty/K_\infty)$ is dihedral of order exactly 2^m.

References

[A-M] A. AZIZI and A. MOUHIB, Capitulation des 2-classes d'idéaux de $\mathbf{Q}(\sqrt{2}, \sqrt{d})$ où d est un entier naturel sans facteurs carrés., Acta Arith. **109** (2003), no. 1, 27–63.

[B-S] E. BENJAMIN and C. SNYDER, Real quadratic number fields with 2-class group of type (2, 2) Math. Scand. **76** (1995), no. 2, 161–178.

[C-H] CONNER, P. E. and HURRELBRINK, J., *Class number parity*, Series in Pure Mathematics, 8. World Scientific Publishing Co., Singapore, 1988.

[F-W] B. FERRERO and L. C. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

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

[G] D. GORENSTEIN, *Finite Groups*, Second edition. Chelsea Publishing Co., New York, 1980.

[Gr1] R. GREENBERG, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98** (1976), no. 1, 263–284.

[Gr2] R. GREENBERG, *Iwasawa theory—past and present.* Class field theory—its centenary and prospect (Tokyo, 1998), 335–385, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

[I] H. ICHIMURA, Note on the class numbers of certain real quadratic fields, Abh. Math. Sem. Univ. Hamburg **73** (2003), 281–288.

[Iw] K. IWASAWA, A note on the group of units of an algebraic number field, J. Math. Pures Appl. (9) **35** (1956), 189–192.

[Ki] H. KISILEVSKY, Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94, J. Number Theory **8** (1976), no. 3, 271–279.

[Ku] S. KURODA, Über den Dirichletschen Körper, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1943). 383–406.

[M1] Y. MIZUSAWA, On Greenberg's conjecture on a certain real quadratic field, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), no. 10, 163–164.

[M2] Y. MIZUSAWA, On the maximal unramified pro-2-extension of $\mathbf{Z}_2$-extension of certain real quadratic fields, J. Number Theory **105** (2004), no. 2, 203–211.

[M3] Y. MIZUSAWA, On the maximal unramified pro-2-extension of $\mathbf{Z}_2$-extension of certain real quadratic fields II, Acta Arith. **119** (2005), no. 1, 93–107.

[N-L] T. NGUYEN, QUANG DO and M. LESCOP, Iwasawa descent and co-descent for units modulo circular units, Pure Appl. Math. Q. **2** (2006), no. 2, 465–496.

[O] M. OZAKI, Iwasawa invariants of p-extensions of totally real number fields, preprint.

[O-T] M. OZAKI and H. TAYA, On the Iwasawa λ_2-invariants of certain families of real quadratic fields, Manuscripta Math. **94** (1997), no. 4, 437–444.

[R-R] L. RÉDEI and H. REICHARDT, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math. **170** (1933), 69–74.

[S] H. P. F. SWINNERTON-DYER, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts 50, Cambridge University Press, Cambridge, 2001.

Present Addresses:
ALI MOUHIB
UNIVERSITÉ SIDI MOHAMMED BEN ABDELLAH,
FACULTÉ POLYDISCIPLINAIRE DE TAZA, B.P 1223 TAZA GARE, MAROC.

ABBAS MOVAHHEDI
XLIM UMR 6172 CNRS/UNIVERSITÉ DE LIMOGES,
MATHÉMATIQUES ET INFORMATIQUE,
123, AVENUE A. THOMAS, 87060 LIMOGES, FRANCE.