Illinois Journal of Mathematics
Volume 57, Number 4, Winter 2013, Pages 1009–1018
S 0019-2082

ON 2-CLASS FIELD TOWERS OF SOME REAL QUADRATIC NUMBER FIELDS WITH 2-CLASS GROUPS OF RANK 3

A. MOUHIB

ABSTRACT. We construct an infinite family of real quadratic number fields with class group of 2-rank $= 3$, 4-rank $= 1$ and finite Hilbert 2-class field tower.

1. Introduction

Let k be a number field, and let C_k be the class group of k. Let k^1 be the Hilbert 2-class field of k, that is, the maximal unramified (including the infinite primes) abelian field extension of k whose degree over k is a power of 2. Let k^n for n a non-negative integer, be defined inductively as $k^0 = k$ and $k^{n+1} = (k^n)^1$; then

$$k \subset k^1 \subset k^2 \subset \cdots \subset k^n \subset \cdots$$

is called the Hilbert 2-class field tower of k. If n is the minimal integer such that $k^n = k^{n+1}$, then n is called the length of the tower. If no such n exists, then the tower is said to be of infinite length.

We define the 2-rank of C_k, denoted $r_2(k)$ as the dimension of the elementary Abelian 2-group C_k/C_k^2 viewed as a vector space over $\mathbb{F}_2$:

$$r_2(k) = \dim_{\mathbb{F}_2}\left(C_k/C_k^2\right),$$

where $\mathbb{F}_2$ is the finite field with two elements. We define the 4-rank of C_k, denoted $r_4(k)$ by:

$$r_4(k) = \dim_{\mathbb{F}_2}\left(C_k^2/C_k^4\right).$$

Assume k is a real quadratic number field. It is well known that if $r_2(k) \geq 6$, then the Hilbert 2-class field tower of k is infinite [5], but it is not known how far from best possible this bound is. In the case where $r_2(k) = 2$ or 3, there are examples of fields k with finite Hilbert 2-class field tower. We mention that in the case where C_k contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times$

Received February 12, 2013; received in final form February 2, 2014.
2010 *Mathematics Subject Classification.* 11R29, 11R32, 11R37.

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then k has infinite Hilbert 2-class field tower ([6], [7]). Also a positive proportion of the fields k with $r_2(k)=5$ and $r_4(k)=i$ (with $i=0,1,2,$ or 3) have infinite Hilbert 2-class field towers, and a positive proportion of the fields k with $r_2(k)=4$ and $r_4(k)=i$ (with $i=0,1,2,$ or 3) have infinite Hilbert 2-class field towers [4].

The aim of this article is to construct an infinite family of real quadratic number fields k such that $r_2(k)=3$, $r_4(k)=1$ and finite Hilbert 2-class field tower. We mention that there are infinitely many imaginary quadratic number fields k such that $r_2(k)=3$, $r_4(k)=0$ and finite Hilbert 2-class field tower [9].

2. Preliminary results

Let p be a prime number and K/k be a Galois extension of number fields with degree p. We define the genus field of the extension K/k denoted $G(K/k)$ as the maximal Abelian p-extension of k, which is unramified over K at all finite and infinite primes. Denote by E_k the unit group of k and $\mathrm{ram}(K/k)$ the number of primes ramified in K/k. Denote by $B(K/k)$ the elementary Abelian p-group $E_k/E_k \cap N_{K/k}(K^*)$. We note that $B(K/k)$ is a vector space over $\mathbb{F}_p$, let $d_p(B(K/k))$ be its dimension.

In the case where $p=2$ and the class number of k is odd, then by the ambiguous class number formula we have (see, e.g., [1]):

$$(*) \qquad r_2(K) = \mathrm{ram}(K/k) - d_2\big(B(K/k)\big) - 1.$$

The value of $r_2(K)$ is related to determining whenever the units of k are norms or not in K.

Now, let k be a quadratic number field of discriminant d. A factorization of the discriminant d into relatively prime discriminants d_1 and $d_2 : d = d_1 d_2$ is called a C_4-factorization if $(\frac{d_1}{p_2}) = (\frac{d_2}{p_1}) = 1$ for all primes $p_i | d_i$. We shall need the following result of Rédei and Reichardt on the 2-class group of real quadratic number fields (see [13], [14] and for more information and results see [10]).

Proposition 2.1. *Let k be a quadratic number field with discriminant d. The* 4-rank *$r_4(k)$ of k equals the number of independent C_4-factorizations of d.*

In the following proposition, we give the rank of the class group of some number fields.

Proposition 2.2. *Let p be a prime number and K/k be a ramified Galois extension of number fields with degree p. Let k^1 be the Hilbert p-class field of k. Suppose that the p-class group of k is cyclic and each ramified prime in the extension Kk^1/k^1 is inert in the extension k^1/k. Then we have an isomorphism induced by the norm map*:

$$B\big(Kk^1/k^1\big) \longrightarrow B(K/k)$$

and we have

$$d_p\big(B\big(Kk^1/k^1\big)\big) = d_p\big(B(K/k)\big).$$

In particular case, if $p = 2$, *then we have*:

$$r_2\big(Kk^1\big) = \mathrm{ram}(K/k) - d_2\big(B(K/k)\big) - 1.$$

Proof. Let the map induced by the norm in the extension k^1/k:

$$\phi : B\big(Kk^1/k^1\big) \longrightarrow B(K/k).$$

Since, the p-class group of k is cyclic, then each unit of k is a norm of a unit in k^1 (see [11]). Therefore the map ϕ is surjective, hence

$$\big|B\big(Kk^1/k^1\big)\big| \geq \big|B(K/k)\big|. \tag{1}$$

Accordingly, the ambiguous class number formula for the p-class groups in the extension K/k reads:

$$\big|A(K)^{\mathrm{Gal}(K/k)}\big| = \big[G(K/k) : K\big] = \frac{|A(k)|p^s}{p|B(K/k)|},$$

where s is the number of primes ramified in the extension K/k. Also, since the p-class group of k is cyclic, then the p-class number of k^1 is trivial. Consequently, the ambiguous class number formula for the p-class groups in the extension Kk^1/k^1 reads:

$$\big|A\big(Kk^1\big)^{\mathrm{Gal}(Kk^1/k^1)}\big| = \big[G\big(Kk^1/k^1\big) : Kk^1\big] = \frac{p^s}{p|B(Kk^1/k^1)|}.$$

On other hand, since Kk^1/k is Abelian and Kk^1/K is unramified, then the genus field $G(K/k)$ of K/k contains Kk^1. Also, since $G(K/k)/k^1$ is Abelian and $G(K/k)/Kk^1$ is unramified, then $G(K/k)$ is contained in the genus field $G(Kk^1/k^1)$ of Kk^1/k^1. Hence, one readily verifies that:

$$\begin{aligned}\big[G(K/k) : K\big] = \big[Kk^1 : K\big]\big[G(K/k) : Kk^1\big] &= \big|A(k)\big|\big[G(K/k) : Kk^1\big] \\ &\leq \big|A(k)\big|\big[G\big(Kk^1/k^1\big) : Kk^1\big].\end{aligned}$$

So we obtain,

$$\big|B\big(Kk^1/k^1\big)\big| \leq \big|B(K/k)\big|. \tag{2}$$

Consequently, from (1) and (2), we have

$$\big|B\big(Kk^1/k^1\big)\big| = \big|B(K/k)\big|,$$

then ϕ is an isomorphism. Since $B(K/k)$ and $B(Kk^1/k^1)$ are elementary p-groups, so

$$d_p\big(B\big(Kk^1/k^1\big)\big) = d_p\big(B(K/k)\big).$$

In the case where $p = 2$, the class number of k^1 is odd and by the formula ($*$) of Section 2, we obtain

$$r_2\big(Kk^1\big) = \mathrm{ram}(K/k) - d_2\big(B(K/k)\big) - 1. \qquad \square$$

In the following, we will study some family of real quadratic number fields in which the 2-class group is of rank equal to 3 and finite Hilbert 2-class field tower.

Let p_1, p_2, p_3 and q be distinct prime numbers and $k = \mathbf{Q}(\sqrt{qp_1p_2p_3})$ be a quadratic number field such that the following conditions are satisfied:

(1) $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$,
(2) $(\frac{q}{p_1}) = (\frac{q}{p_2}) = (\frac{p_3}{p_1}) = (\frac{p_3}{p_2}) = (\frac{2}{p_3}) = -(\frac{q}{p_3}) = -1$,
(3) $(\frac{2}{p_1}) = (\frac{2}{p_2})$ and $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$, where $\varepsilon_{p_1p_2}$ is the fundamental unit of $\mathbf{Q}(\sqrt{p_1p_2})$.

It's clear by genus theory that the rank of the 2-class group of k is equal to 3.

LEMMA 2.3. *Let k be the real quadratic number field defined above verifying the conditions (1), (2) and (5). Then the 2-class group of k is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}, n \geq 2$.*

Proof. By the hypotheses above, we find that:

$$\left(\frac{p_1p_2}{p_3}\right) = \left(\frac{p_1p_2}{q}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) = \left(\frac{p_3q}{p_1}\right) = \left(\frac{p_3q}{p_2}\right) = 1,$$

then one can verify that there is only one C_4-factorization of the discriminant $d = 4qp_1p_2p_3$ of k into relatively prime discriminants $d_1 = p_1p_2$ and $d_2 = 4qp_3 : d = d_1.d_2$. Then by Proposition 2.1, there exists only one cyclic extension over k of degree 4 which is unramified at all finite and infinite primes. Consequently, we obtain the result. □

LEMMA 2.4. *Let q, p_1 and p_2 be distinct prime numbers such that $p_1 \equiv p_2 \equiv -q \equiv 1 \pmod 4$ and $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$. Then the 2-class group of the biquadratic number field $L = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2})$ is cyclic non-trivial.*

Proof. By genus theory, the genus field of L is exactly the triquadratic number field $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_2})$, then the 2-class group of L is non-trivial. It remains to prove that the 2-class group of L is cyclic. Also by genus theory the 2-class group of $\mathbf{Q}(\sqrt{q})$ is trivial. Moreover, since $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, then the number of ramified primes in the extension $L/\mathbf{Q}(\sqrt{q})$ is equal to 2: $\mathrm{ram}(L/\mathbf{Q}(\sqrt{q})) = 2$. Consequently by the formula (∗) and the fact that the 2-class group of L is non-trivial, we find:

$$r_2(L) = \mathrm{ram}\big(L/\mathbf{Q}(\sqrt{q})\big) - d_2\big(B\big(L/\mathbf{Q}(\sqrt{q})\big)\big) - 1 = 1. \qquad \square$$

LEMMA 2.5. *Let q, p_1, p_2 and p_3 be distinct prime numbers such that $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$ and $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$. Denote by L^1 the Hilbert 2-class field of $L = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2})$, then the class number of $L^1(\sqrt{p_3})$ is even.*

Proof. By Lemma 2.4, the extension L^1/L is an unramified cyclic extension, so the extension $L^1(\sqrt{p_3})/L(\sqrt{p_3})$ is also an unramified cyclic extension. On other hand, by [12, Theorem 3.3], the 2-rank of the class group of the multiquadratic number field $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ is greater than or equal to two. Hence, since $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})/L(\sqrt{p_3})$ is an unramified quadratic extension, then the 2-rank of the class group of $L(\sqrt{p_3})$ is greater than or equal to two. Consequently, the fact that the cyclic extension $L^1(\sqrt{p_3})/L(\sqrt{p_3})$ is unramified shows that the class number of $L^1(\sqrt{p_3})$ is even. □

3. The tower of 2-Hilbert class field of k is finite of length at most three

In this section, we give an infinite family of real quadratic number fields with 2-class group isomorphic with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}, n \geq 2$ and with finite Hilbert 2-class field of length at most three. The objective is to prove the following theorem:

THEOREM 3.1. *Let p_1, p_2, p_3 and q be distinct prime numbers such that $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$, $(\frac{q}{p_1}) = (\frac{q}{p_2}) = (\frac{p_3}{p_1}) = (\frac{p_3}{p_2}) = (\frac{2}{p_3}) = -(\frac{q}{p_3}) = -1$, $(\frac{2}{p_1}) = (\frac{2}{p_2})$ and $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$. Then the Hilbert 2-class field tower of $k = \mathbf{Q}(\sqrt{q p_1 p_2 p_3})$ is finite of length at most three.*

Before proving our main theorem, we establish the following lemma on units. We denote, for every integer m, ε_m the fundamental unit of $\mathbf{Q}(\sqrt{m})$.

LEMMA 3.2. *Let q, p_1 and p_2 be distinct prime numbers such that $p_1 \equiv p_2 \equiv -q \equiv 1 \pmod 4$, $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$ and $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$. Then the biquadratic number field $L = \mathbf{Q}(\sqrt{q}, \sqrt{p_1 p_2})$ contains one of the following units $\sqrt{\varepsilon_q \varepsilon_{q p_1 p_2}}$, $\sqrt{\varepsilon_{p_1 p_2} \varepsilon_{q p_1 p_2}}$ or $\sqrt{\varepsilon_q \varepsilon_{p_1 p_2} \varepsilon_{q p_1 p_2}}$.*

Proof. For every positive integer m such that $N_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\varepsilon_m) = 1$, we have by Hilbert's theorem 90, $\varepsilon_m = \frac{\alpha}{\alpha^\sigma}$ where σ is the non-trivial automorphism of $\mathbf{Q}(\sqrt{m})$ and α is an element of $\mathbf{Q}(\sqrt{m})$. Moreover, since σ acts trivially on $\mathbf{Q}$, then we can choose α such that it becomes an integer in $\mathbf{Q}(\sqrt{m})$ not divisible by any rational integer. Let $\mathcal{P}$ be a prime ideal of $\mathbf{Q}(\sqrt{m})$ dividing the ideal (α) generated by α. It is clear that $\mathcal{P}^\sigma$ divides (α), so under the hypothesis α is not divisible by any rational number, the prime ideal $\mathcal{P}$ must lies above than a prime number l ramified in $\mathbf{Q}(\sqrt{m})$. Then, $\alpha\alpha^\sigma = N_{K/\mathbf{Q}}(\alpha)$ divides the discriminant of $\mathbf{Q}(\sqrt{m})$ and since $\varepsilon_m \alpha\alpha^\sigma = \alpha^2$, then there exists an integer $m' := \alpha^{1+\sigma}$ dividing the discriminant of $\mathbf{Q}(\sqrt{m})$ such that m' is a norm in the extension $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ and $m'\varepsilon_m$ is a square in $\mathbf{Q}(\sqrt{m})$.

On other hand, the discriminant of $\mathbf{Q}(\sqrt{p_1 p_2})$ is equal to $p_1 p_2$, then there exists an integer $m' | p_1 p_2$ such that $\sqrt{m' \varepsilon_{p_1 p_2}} \in \mathbf{Q}(\sqrt{p_1 p_2})$. Since $\varepsilon_{p_1 p_2}$ is the fundamental unit of $\mathbf{Q}(\sqrt{p_1 p_2})$, then m' must be contained in $\{p_1, p_2\}$. Either way, we can conclude that:

$$\sqrt{p_1 \varepsilon_{p_1 p_2}} \in \mathbf{Q}(\sqrt{p_1 p_2}). \tag{3}$$

The discriminant of $\mathbf{Q}(\sqrt{q})$ is equal to $4q$, then there exists an integer $m'|2q$ such that $\sqrt{m'\varepsilon_q} \in \mathbf{Q}(\sqrt{q})$. Since ε_q is the fundamental unit of $\mathbf{Q}(\sqrt{q})$, then m' must be contained in $\{2, 2q\}$. Either way, we can conclude that:

$$\sqrt{2\varepsilon_q} \in \mathbf{Q}(\sqrt{q}). \tag{4}$$

Also, since the discriminant of $\mathbf{Q}(\sqrt{qp_1p_2})$ is equal to $4qp_1p_2$, then there exists an integer $m'|2qp_1p_2$ such that $\sqrt{m'\varepsilon_{qp_1p_2}} \in \mathbf{Q}(\sqrt{qp_1p_2})$ and m' is a norm in the extension $\mathbf{Q}(\sqrt{qp_1p_2})/\mathbf{Q}$. Since $\varepsilon_{qp_1p_2}$ is the fundamental unit of $\mathbf{Q}(\sqrt{qp_1p_2})$, then $m' \notin \{1, qp_1p_2\}$. On other hand, since $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, then q is not a norm in the extension $\mathbf{Q}(\sqrt{qp_1p_2})/\mathbf{Q}$, so $m' \notin \{q, p_1p_2\}$ and we have:

(5) $\sqrt{m'\varepsilon_{qp_1p_2}} \in \mathbf{Q}(\sqrt{qp_1p_2})$ such that $m'|2qp_1p_2$ and $m' \notin \{1, q, p_1p_2, qp_1p_2\}$.

Consequently, using (3), (4) and (5), we obtain that one of the units $\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}$, $\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$ or $\sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$ is contained in L. □

Proof of Theorem 3.1. By Lemma 2.4, the 2-class group of the biquadratic field $L = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2})$ is cyclic non-trivial. Denote by L^1 the Hilbert 2-class field of L, then the class number of L^1 is odd. By formula $(*)$ of Section 2, we have

$$r_2\big(L^1(\sqrt{p_3})\big) = \mathrm{ram}\big(L^1(\sqrt{p_3})/L^1\big) - d_2\big(B\big(L^1(\sqrt{p_3})/L^1\big)\big) - 1.$$

It is clear that the p_3-adic places of L^1 are the unique ramified places in $L^1(\sqrt{p_3})/L^1$. Since $(\frac{q}{p_3}) = -(\frac{p_1}{p_3}) = -(\frac{p_2}{p_3}) = 1$, then p_3 is totally decomposed in L and the p_3-adic places of L are inert in the triquadratic extension $L(\sqrt{p_1})$. Moreover, the cyclicity of the 2-class group of L implies that the p_3-adic places of L are inert in L^1. Since $\mathrm{ram}(L(\sqrt{p_3})/L) = 4$, then by Proposition 2.2, we conclude $r_2(L^1(\sqrt{p_3})) = 3 - d_2(B(L(\sqrt{p_3})/L))$. Next, we prove that $d_2(B(L(\sqrt{p_3})/L)) = 2$.

We have ε_q and $\varepsilon_{p_1p_2}$ are units of L. Since $\sqrt{p_1\varepsilon_{p_1p_2}} \in \mathbf{Q}(\sqrt{p_1p_2})$ (see (3) in the proof of Lemma 3.2) and $\sqrt{2\varepsilon_q} \in \mathbf{Q}(\sqrt{q})$ (see (4) in the proof of Lemma 3.2), we have for each p_3-adic place $\mathcal{P}$ of L:

$$\left(\frac{\varepsilon_q, p_3}{\mathcal{P}}\right) = \left(\frac{2, p_3}{\mathcal{P}}\right) = \left(\frac{2}{p_3}\right) = -1 \tag{6}$$

and

$$\left(\frac{\varepsilon_{p_1p_2}, p_3}{\mathcal{P}}\right) = \left(\frac{p_1, p_3}{\mathcal{P}}\right) = \left(\frac{p_1}{p_3}\right) = -1. \tag{7}$$

Then ε_q and $\varepsilon_{p_1p_2}$ are not norms in the extension $L(\sqrt{p_3})/L$, but the product $\varepsilon_q\varepsilon_{p_1p_2}$ is a norm in $L(\sqrt{p_3})/L$. Therefore, $d_2(B(L(\sqrt{p_3})/L)) \geq 1$. We are going in the next to determine a new unit u in L such that u and $u\varepsilon_l$, $l \in \{q, p_1p_2\}$ are not norms in the extension $L(\sqrt{p_3})/L$.

From Lemma 3.2, one of the units $\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}$, $\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$ or $\sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$ is contained in L.

In the case where u is a unit of L such that u is one of the units $\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}$ or $\sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$, let σ be the non-trivial $\mathbf{Q}(\sqrt{q})$-isomorphism of L. Then for each p_3-adic place $\mathcal{P}$ of L, we have:

$$\left(\frac{u, p_3}{\mathcal{P}}\right)\left(\frac{u, p_3}{\sigma(\mathcal{P})}\right) = \left(\frac{N_{L/\mathbf{Q}(\sqrt{q})}(u), p_3}{N_{L/\mathbf{Q}(\sqrt{q})}(\mathcal{P})}\right) = \left(\frac{\pm\varepsilon_q, p_3}{N_{L/\mathbf{Q}(\sqrt{q})}(\mathcal{P})}\right).$$

Using equality (6), we obtain:

$$\left(\frac{\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}, p_3}{\mathcal{P}}\right)\left(\frac{\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}, p_3}{\sigma(\mathcal{P})}\right) = \left(\frac{2}{p_3}\right) = -1 \tag{8}$$

and

$$\left(\frac{\sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\mathcal{P}}\right)\left(\frac{\sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\sigma(\mathcal{P})}\right) = \left(\frac{2}{p_3}\right) = -1. \tag{9}$$

In the case where $u = \sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}$, let τ be the non-trivial $\mathbf{Q}(\sqrt{p_1p_2})$-isomorphism of L. Then for each p_3-adic place $\mathcal{P}$ of L, we have:

$$\begin{aligned}\left(\frac{\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\mathcal{P}}\right)\left(\frac{\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\tau(\mathcal{P})}\right) &= \left(\frac{N_{L/\mathbf{Q}(\sqrt{p_1p_2})}(\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}), p_3}{N_{L/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right)\\ &= \left(\frac{\pm\varepsilon_{p_1p_2}, p_3}{N_{L/\mathbf{Q}(\sqrt{p_1p_2})}(\mathcal{P})}\right).\end{aligned}$$

Using equality (7), we obtain:

$$\left(\frac{\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\mathcal{P}}\right)\left(\frac{\sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, p_3}{\tau(\mathcal{P})}\right) = \left(\frac{p_1}{p_3}\right) = -1. \tag{10}$$

Consequently, for $u \in \{\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}, \sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, \sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}\}$ and $l \in \{q, p_1p_2\}$, u and $u\varepsilon_l$ are not norms in the extension $L(\sqrt{p_3})/L$. Then, we have

$$d_2\big(B\big(L(\sqrt{p_3})/L\big)\big) \geq 2.$$

By Lemma 2.5, the class number of $L^1(\sqrt{p_3})$ is even, then

$$r_2\big(L^1(\sqrt{p_3})\big) = 3 - d_2\big(B\big(L(\sqrt{p_3})/L\big)\big) = 1.$$

Hence the Hilbert 2-class field tower of $L^1(\sqrt{p_3})$ is of length 1. Consequently, the Hilbert 2-class field tower of k is finite. □

Next, we give the length of the Hilbert 2-class field tower of k. Denote by $\mathcal{L}(k)$ the maximal unramified 2-extension of k. We need the following lemma.

LEMMA 3.3. *Let p_1, p_3 and q be distinct prime numbers such that $p_1 \equiv p_3 \equiv -q \equiv 1 \pmod 4$ and $(\frac{q}{p_3}) = -(\frac{p_1}{p_3}) = -(\frac{q}{p_1}) = -(\frac{2}{p_3}) = 1$. Then the class number of the triquadratic number field $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})$ is odd.*

Proof. Since $(\frac{q}{p_3}) = -(\frac{p_1}{p_3}) = -(\frac{q}{p_1}) = -(\frac{2}{p_3}) = 1$, then one can verify that there is no C_4-factorization of the discriminant of the quadratic number field $\mathbf{Q}(\sqrt{qp_1p_3})$ into relatively prime discriminants, so by Proposition 2.1, the 2-class group of $\mathbf{Q}(\sqrt{qp_1p_3})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see also [3]). Consequently, since $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})/\mathbf{Q}(\sqrt{qp_1p_3})$ is an unramified Abelian extension, then $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})$ is the Hilbert 2-class field of $\mathbf{Q}(\sqrt{qp_1p_3})$. Hence, by [2], $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})$ is exactly the maximal unramified 2-extension of $\mathbf{Q}(\sqrt{qp_1p_3})$, finally the class number of $\mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})$ is odd. □

We have the following theorem.

THEOREM 3.4. *We keep the hypotheses of Theorem 3.1, then the Hilbert 2-class field tower of k is of length two.*

Proof. Note that since the 2-class group of k is of rank 3, then $\mathcal{L}(k)/k$ can never be Abelian (see [2, Corollary 2]). Denote $F = \mathbf{Q}(\sqrt{q}, \sqrt{p_3})$, $F_1 = \mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_3})$, $F_2 = \mathbf{Q}(\sqrt{q}, \sqrt{p_2}, \sqrt{p_3})$, $F_3 = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2}, \sqrt{p_3})$ and let $k^* = \mathbf{Q}(\sqrt{q}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ the genus field of k. It is clear that F_1, F_2 and F_3 are the sub-extensions of the biquadratic extension k^*/F. Let σ and τ respectively the generator of the Galois group $\mathrm{Gal}(k^*/F_1)$ and $\mathrm{Gal}(k^*/F_2)$, so $\mathrm{Gal}(k^*/F_3)$ is generated by $\sigma\tau$. By Lemma 3.3, F_1 and F_2 have odd class number, so σ and τ act on each class C of the 2-class group of k^* as C^{-1}, therefore $\sigma\tau$ acts trivially on the 2-class group of k^*. Hence, since k^*/F_3 is an unramified quadratic extension, then the fields F_3 and k^* have the some Hilbert 2-class field. On other hand, from the proof of Theorem 3.1, the 2-class groups of $L = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2})$ and $L^1(\sqrt{p_3})$ are cyclic. This yields, that $\mathrm{Gal}(\mathcal{L}(k)/F_3)$ is metacyclic, so by Burnside's basic theorem, the 2-class group of F_3 is of rank 2. Consequently, by [2, Proposition 7], $\mathcal{L}(k)$ is exactly the Hilbert 2-class field of F_3 and k^*. □

REMARK 3.5. For each number field M, let $h(M)$ (resp. E_M) denote the 2-part of the class number of M (resp. the unit group of M).

We keep the notations and hypotheses of Theorem 3.1. We have $|\,\mathrm{Gal}(\mathcal{L}(k)/k)| = 2^2 h(F_3)$, where $h(F_3)$ is the 2-part of the class number of $F_3 = \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2}, \sqrt{p_3})$. By Kuroda's class number formula of a mutiquadratic number field [8], we have:

$$h(F_3) = \frac{Q_{F_3} \prod_{i=1}^{i=7} h(k_i)}{2^9},$$

where Q_{F_3} is the unit index: $Q_{F_3} = [E_{F_3} : \prod_{i=1}^{i=7} E_{k_i}]$ and $k_i, i \in \{1, 2, \ldots, 7\}$ are the distinct quadratic number fields contained in F_3.

By genus theory, we have $h(\mathbf{Q}(\sqrt{p_3})) = h(\mathbf{Q}(\sqrt{q})) = 1$ and $h(\mathbf{Q}(\sqrt{p_1p_2}))$ is even. From Lemma 2.3, we have $h(\mathbf{Q}(\sqrt{qp_1p_2p_3})) = 2^{n+2}$, where $n \geq 2$. Also, by genus theory and Proposition 2.1, one can verify that:

$$h\big(\mathbf{Q}(\sqrt{qp_3})\big) = 2, \qquad h\big(\mathbf{Q}(\sqrt{p_1p_2p_3})\big) = 4 \quad \text{and} \quad h\big(\mathbf{Q}(\sqrt{p_1p_2q})\big) = 4.$$

This yields that

$$\left|\mathrm{Gal}\big(\mathcal{L}(k)/k\big)\right| = 2^2 h(F_3) = 2^n Q_{F_3} h(p_1p_2). \tag{11}$$

The computation of the unit index Q_{F_3} is not easy. In the following, we give a refined lower bound of Q_{F_3}. By Lemma 3.2, there exist a unit $u \in \mathbf{Q}(\sqrt{q}, \sqrt{p_1p_2})$, such that u is one of the following units:

$$u \in \{\sqrt{\varepsilon_q\varepsilon_{qp_1p_2}}, \sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}, \sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2}}\}. \tag{12}$$

Also, from the proof of Lemma 3.2, if $N_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\varepsilon_m) = 1$, then there exist a positive integer m' dividing the discriminant of $\mathbf{Q}(\sqrt{m})$ such that m' is a norm in the extension $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ and $m'\varepsilon_m$ is a square in $\mathbf{Q}(\sqrt{m})$. Then using the some thechniques in the proof of Lemma 3.2, we prove that there exist a unit $v = \sqrt{\varepsilon_{qp_3}}$ such that:

$$\sqrt{q}v \in \mathbf{Q}(\sqrt{qp_3}), \tag{13}$$

and using (3) and (4) in the proof of Lemma 3.2, we find a unit $w \in F_3$ such that w is one of the following units:

$$u \in \{\sqrt{\varepsilon_{qp_1p_2p_3}}, \sqrt{\varepsilon_q\varepsilon_{qp_1p_2p_3}}, \sqrt{\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2p_3}}, \sqrt{\varepsilon_q\varepsilon_{p_1p_2}\varepsilon_{qp_1p_2p_3}}\}. \tag{14}$$

Hence, by (12), (13) and (14), we have three independent units u, v, w of F_3 such that for $i_0, j_0, k_0 \in \{0, 1\}$:

$$u^{i_0}v^{j_0}w^{k_0} \notin \prod_{i=1}^{i=7} E_{k_i}.$$

Then, we have 2^3 divides Q_{F_3} and from (11), we conclude $2^{n+3}h(p_1p_2)$ divides $|\,\mathrm{Gal}(\mathcal{L}(k)/k)|$. The order of the group $|\,\mathrm{Gal}(\mathcal{L}(k)/k)|$ increases, whenever the 2-part of the class number of $\mathbf{Q}(\sqrt{p_1p_2})$ increases.

Example. Let $p_1 = 13$, $p_2 = 29$ and $p_3 = 37$. We have $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = 1$ and

$$\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = \left(\frac{2}{p_3}\right) = \left(\frac{p_3}{p_1}\right) = \left(\frac{p_3}{p_2}\right) = -1.$$

It remains to determine an infinite family of prime numbers q such that $q \equiv -1 \pmod 4$ and

$$\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right) = -\left(\frac{q}{p_3}\right) = -1.$$

We have

$$\left(\frac{11}{p_1}\right) = \left(\frac{11}{p_2}\right) = -\left(\frac{11}{p_3}\right) = -1.$$

We know that there are infinitely many prime numbers in an arithmetic progession:

$$q \equiv 11 \pmod{4 \cdot 13 \cdot 29 \cdot 37}.$$

Consequently, we construct an infinite family of real quadratic number fields k verifying the conditions of Theorem 3.1 with 2-class group isomorphic with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ $(n \geq 2)$ and finite Hilbert 2-class field tower.

We remark that the value of the integer n may increase:

For $q = 11$, the 2-class group of k is isomorphic with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}$.

For $q = 47$, one can verify that $(\frac{q}{13}) = (\frac{q}{29}) = -(\frac{q}{37}) = -1$ and the 2-class group of k is isomorphic with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^4\mathbb{Z}$.

References

[1] A. Azizi and A. Mouhib, *Sur le rang du 2-groupe de classes de* $\mathbf{Q}(\sqrt{m}, \sqrt{d})$ *où* $m = 2$ *ou un premier* $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2741–2752. MR 1828471

[2] E. Benjamin and F. Lemmermeyer, *Real quadratic fields with abelian* 2*-class field tower*, J. Number Theory **73** (1998), 182–194. MR 1658015

[3] E. Benjamin and C. Snyder, *Real quadratic number fields with* 2*-class groupe of type* (2, 2), Math. Scand. **76** (1995), 161–178. MR 1354574

[4] F. Gerth, *Quadratic fields with infinite Hilbert 2-class field towers*, Acta Arith. **106** (2003), 151–158. MR 1958981

[5] E. S. Golod and I. R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Math. **28** (1964), 261–272 (in Russian). English translation in *AMS Transl.* **48** (1965), 91–102. MR 0161852

[6] F. Hajir, *On a theorem of Koch*, Pacific J. Math. **176** (1996), no. 1, 15–18. MR 1433980

[7] F. Hajir, *Correction to "On a theorem of Koch*," Pacific J. Math. **196** (2000), no. 2, 507–508. MR 1800589

[8] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I **4** (1943), 383–406. MR 0021031

[9] F. Lemmermeyer, *On* 2*-class field towers of some imaginary quadratic number fields*, Abh. Math. Semin. Univ. Hambg. **67** (1997), 205–214. MR 1481537

[10] F. Lemmermeyer, *Higher descent on Pell conics. I. From Legendre to Selmer*, available at `arXiv:math/0311309v1`.

[11] A. Mouhib, *On the parity of the class number of real multiquadratic number fields*, J. Number. Theory **129** (2009), 1205–1211. MR 2521470

[12] A. Mouhib, *Sur la borne inférieure du rang du 2-groupe de classes des corps multiquadratiques réels*, Canad. Math. Bull. **54** (2011), 330–337. MR 2884250

[13] L. Rédei, *Die Anzahl der durch 4 teilbaren Invarienten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **49** (1932), 338–363.

[14] L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarienten der klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74.

A. Mouhib, LIMAO, Department of Mathematics, Physics and Computer Science, Polydisciplinary Faculty of Taza, Sidi Mohamed Ben Abdellah University, B/P 1223, Taza-Gare, Morocco

E-mail address: `mouhibali@yahoo.fr`