144 (2019) MATHEMATICA BOHEMICA No. 2, 177–190

REAL QUADRATIC NUMBER FIELDS WITH METACYCLIC HILBERT 2-CLASS FIELD TOWER

Said Essahel, Ahmed Dakkak, Ali Mouhib, Taza

Received September 7, 2017. Published online August 30, 2018.
Communicated by Simion Breaz

Abstract. We begin by giving a criterion for a number field K with 2-class group of rank 2 to have a metacyclic Hilbert 2-class field tower, and then we will determine all real quadratic number fields $\mathbb{Q}(\sqrt{d})$ that have a metacyclic nonabelian Hilbert 2-class field tower.

Keywords: class field tower; class group; real quadratic number field; metacyclic group

MSC 2010: 11R11, 11R29, 11R37

1. Introduction

Let K be a number field and C_K be the class group of K. The maximal unramified abelian extension of K denoted by $K^{(1)}$ is called the Hilbert class field of K. We recall that by the Artin reciprocity law we have $\mathrm{Gal}(K^{(1)}/K) \simeq C_K$. For a nonnegative integer n, let $K^{(n)}$ be defined inductively as $K^{(0)} = K$ and $K^{(n+1)} = (K^{(n)})^{(1)}$; then

$$K \subset K^{(1)} \subset K^{(2)} \subset \ldots \subset K^{(n)} \subset \ldots$$

is called the Hilbert class field tower of K. If n is the minimal integer such that $K^{(n)} = K^{(n+1)}$, then the tower is called to be finite of length n. If there is no such n, then the tower is called to be infinite. We denote $K^{(\infty)} = \bigcup_{i\in\mathbb{N}} K^{(i)}$. We recall that $K^{(\infty)}/K$ is a Galois extension and the tower of K is finite if and only if $K^{(\infty)}/K$ is of finite degree.

Let p be a prime integer number, $K_p^{(1)}$, the maximal unramified abelian p-extension of K, is called the Hilbert p-class field of K. We recall that by the class field theory we have $\mathrm{Gal}(K_p^{(1)}/K) = C_{K,p}$, the p-Sylow subgroup of C_K which is called the p-class

DOI: 10.21136/MB.2018.0102-17

group of K. For a nonnegative integer n let $K_p^{(n)}$ be defined inductively as $K_p^{(0)} = K$ and $K_p^{(n+1)} = (K_p^{(n)})_p^{(1)}$; then

$$K \subset K_p^{(1)} \subset K_p^{(2)} \subset \ldots \subset K_p^{(n)} \subset \ldots$$

is called the Hilbert p-class field tower of K. If n is the minimal integer such that $K_p^{(n)} = K_p^{(n+1)}$, then this tower is called to be finite of length n. If there is no such n, then the tower is called to be infinite. We denote $K_p^{(\infty)} = \bigcup_{i\in\mathbb{N}} K_p^{(i)}$. We recall that $K_p^{(\infty)}/K$ is a Galois extension and the tower of K is finite if and only if $K_p^{(\infty)}/K$ is of finite degree.

We recall that the 2-rank of C_K denoted by $\mathrm{rank}_2(C_K)$ is defined as the dimension of the $\mathbb{F}_2$-vector space C_K/C_K^2.

It is well known that:

- ▷ If $\mathrm{rank}_2(C_K) \geqslant 6$, then K has an infinite Hilbert 2-class field tower.
- ▷ If $\mathrm{rank}_2(C_K) = 4$ or 5, then there is no known real quadratic field with finite Hilbert 2-class field tower. In these cases, according to Martinet's conjecture, the Hilbert 2-class field tower of K is infinite (see [5]).
- ▷ If $\mathrm{rank}_2(C_K) = 2$ or 3, then there are both real quadratic number fields with a finite Hilbert 2-class field tower and real quadratic number fields with infinite Hilbert 2-class field tower (see the works of Schoof, Martinet, Mouhib ([8] and [7]), ...).
- ▷ If $\mathrm{rank}_2(C_K) = 1$, then K has a finite Hilbert 2-class field tower of length 1.

So for the case $\mathrm{rank}_2(C_K) = 2$ there is no known decision procedure to determine whether or not the Hilbert 2-class field tower of a given number field K is infinite. In this paper, we give a new family of real quadratic number fields K with $\mathrm{rank}_2(C_K) = 2$ and finite Hilbert 2-class field tower. More precisely, we will determine all real quadratic number fields K that have a metacyclic Hilbert 2-class field tower.

2. Preliminary results

2.1. The rank of a group. Let G be a group.

- ▷ If there exists a finite subset X of G such that $G = \langle X \rangle$, then we say that G has a finite rank defined as

$$\mathrm{rank}(G) = \min\{|X| \colon X \subset G \text{ and } G = \langle X \rangle\}.$$

  If no such subset exists, then G is called to be of infinite rank.
- ▷ Let $G' = [G, G]$ be the commutator subgroup of G. The quotient G/G' is called the abelianization of G and is denoted by G^{ab}. $G/p = G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p$ is a vector

space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and the integer $\mathrm{rank}_p(G) = \dim_{\mathbb{F}_p}(G/p)$ is called the p-rank of G. We note that:

⊳ if G is abelian, then $\mathrm{rank}_p(G) = \dim_{\mathbb{F}_p}(G/G^p)$;

⊳ $\mathrm{rank}_p(G) = \mathrm{rank}_p(G^{\mathrm{ab}})$.

2.2. Metacyclic group. A group G is called metacyclic if there is a normal subgroup N of G such that N and G/N are cyclic. We recall that:

(1) if G is metacyclic, then any subgroup H of G is metacyclic;

(2) if G is metacyclic and H is a normal subgroup of G, then G/H is metacyclic.

Let G be a metacyclic group and N a normal cyclic subgroup of G such that G/N is cyclic. If we denote $N = \langle a\rangle$ and $G/N = \langle bN\rangle$, then $G = \langle a, b\rangle$ and thus, G is generated by 2 elements.

Proposition 1. *Let K be a number field and p a prime integer.*

(1) *if $G = \mathrm{Gal}(K^{(\infty)}/K)$ is metacyclic, then $K^{(\infty)} = K^{(2)}$;*

(2) *if $G_p = \mathrm{Gal}(K_p^{(\infty)}/K)$ is metacyclic, then $K_p^{(\infty)} = K_p^{(2)}$.*

P r o o f. (1) We have $K \subset K^{(1)} \subset K^{(\infty)}$. By definition, $K^{(1)}$ is the largest abelian extension of K contained in $K^{(\infty)}$. We deduce that $\mathrm{Gal}(K^{(\infty)}/K^{(1)}) \cong G'$. Let N be a normal cyclic subgroup of G such that G/N is cyclic. Since G/N is abelian, $G' \subset N$ and then G' is cyclic. We deduce that $K^{(\infty)}/K^{(1)}$ is abelian unramified. So $K^{(\infty)} \subset K^{(2)}$ and then $K^{(\infty)} = K^{(2)}$.

(2) Using the same proof we prove 2. □

Proposition 2. *Let K be a number field and p a prime number. If $G_p = \mathrm{Gal}(K_p^{(\infty)}/K)$ is metacyclic nonabelian, then $\mathrm{rank}_p(C_K) = 2$.*

P r o o f. Since G_p is nonabelian, then $K_p^{(1)} \neq K_p^{(2)} = K_p^{(\infty)}$. We have $C_{K,p} \simeq G_p/[G_p, G_p]$, thus $C_{K,p}$ is metacyclic and we have $\mathrm{rank}(C_{K,p}) \leqslant 2$ and so $\mathrm{rank}(C_{K,p}) = 1$ or 2. If $\mathrm{rank}(C_{K,p}) = 1$, then according to the result of Taussky (see [9]), $K_p^{(2)} = K_p^{(1)}$, which is impossible. In conclusion, $\mathrm{rank}_p(C_K) = 2$. □

R e m a r k 1. Let K be a quadratic number field.

(1) If $G_2 = \mathrm{Gal}(K_2^{(\infty)}/K)$ is metacyclic nonabelian, then K has three quadratic extensions L_1, L_2 and L_3 contained in $K^{(1)}$.

(2) According to Proposition 2, we will be limited to determine the real quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ with $\mathrm{rank}_2(C_K) = 2$ that have a metacyclic Hilbert 2-class field tower. To select those with non abelian tower, we can use Theorem 1 or Theorem 2 in [3] depending on whether d is the sum of two squares or not, respectively.

Lemma 1. *If G is a nonmetacyclic two-generator 2-group, then the number of two-generator maximal subgroups of G is even.*

Proof. See [4]. $\square$

Theorem 1. *Let K be a number field such that $\operatorname{rank}_2(C_K) = 2$ and L_1, L_2 and L_3 be the three quadratic extensions of K contained in $K^{(1)}$. Let us denote $G = \operatorname{Gal}(K_2^{(\infty)}/K)$ and $C_i = C_{L_i,2}$ for $i = 1, 2, 3$. Then G is metacyclic if and only if $\operatorname{rank}(C_i) \leqslant 2$ for $i = 1, 2, 3$.*

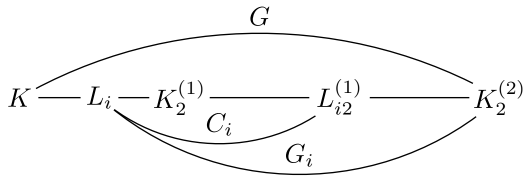
Proof. Suppose that G is metacyclic.

If G is abelian, then it is easy to see that for all i, $\operatorname{rank}(C_i) \leqslant \operatorname{rank}(G) = 2$.

Suppose that G is not abelian. For each $i \in \{1, 2, 3\}$, $K_2^{(1)}/K$ is abelian unramified, thus $K_2^{(1)}/L_i$ is also abelian unramified, hence $K_2^{(1)} \subset L_{i2}^{(1)}$. In the same way, we prove that $L_{i2}^{(1)} \subset K_2^{(2)}$ and thus

$$K \subset L_i \subset K_2^{(1)} \subset L_{i2}^{(1)} \subset K_2^{(2)}.$$

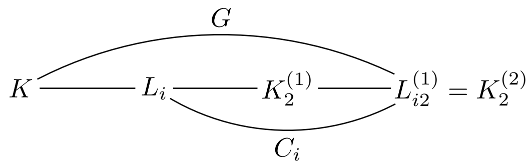
Let $G_i = \operatorname{Gal}(K_2^{(2)}/L_i)$ and $H = \operatorname{Gal}(K_2^{(2)}/L_{i2}^{(1)})$.



G_i is a subgroup of G. So G_i is metacyclic and thus $C_i \cong G_i/H$ is metacyclic, too. We deduce that $\operatorname{rank}(C_i) \leqslant 2$.

Suppose that $\operatorname{rank}(C_i) \leqslant 2$ for $i = 1, 2, 3$.

If there exists i such that $\operatorname{rank}(C_i) = 1$, then according to the result of Taussky (see [9]), $L_{i2}^{(2)} = L_{i2}^{(1)}$ and then $K_2^{(2)} = L_{i2}^{(2)} = L_{i2}^{(1)}$.



We have C_i is cyclic and $G/C_i \cong \mathbb{Z}/2\mathbb{Z}$ is cyclic, too. We deduce that G is metacyclic.

Suppose that $\operatorname{rank}(C_i) = 2$ for all $i \in \{1, 2, 3\}$. Let C be a maximal subgroup of G. We have $[G : C] = 2$, so if L is the subfield of $K_2^{(\infty)}/K$ fixed by C, then $L = L_i$ for some $i \in \{1, 2, 3\}$. Since $L_2^{(1)}$ is the maximal abelian extension of L contained in $K_2^{(\infty)}$, then $C_i \cong C/C'$ and $\operatorname{rank}(C) = \operatorname{rank}(C_i) = 2$. Using Lemma 1 and since $\operatorname{rank}(G) = \operatorname{rank}(C_K) = 2$, G is metacyclic. $\square$

3. Fields $\mathbb{Q}(\sqrt{d})$ with d sum of two squares having a nonabelian metacyclic tower

Lemma 2. *Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{\delta})$ be a biquadratic field such that $m = 2$ or m is a prime integer $\equiv 1 \pmod 4$ and δ is a square-free positive integer not divisible by any prime $\equiv 3 \pmod 4$. If r is the number of primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L and H is the 2-class group of L, then we have* $\operatorname{rank}(H) = r-1$ *or* $r-2$ *and*

(1) *if $m \equiv 1 \pmod 4$, then* $\operatorname{rank}(H) = r-1$ *if and only if*

$$\begin{cases} \text{for all } q \mid \delta \text{ such that } \left(\dfrac{q}{m}\right) = 1 \text{ we have } \left(\dfrac{m}{q}\right)_4 = \left(\dfrac{q}{m}\right)_4, \\ \left(\dfrac{2}{m}\right)_4 = (-1)^{(m-1)/8} \text{ if } m \equiv 1 \pmod 8 \text{ and } \delta = 2c; \end{cases}$$

(2) *if $m = 2$, then* $\operatorname{rank}(H) = r-1$ *if and only if for all $q|\delta$ such that $q \equiv 1 \pmod 8$ we have $\left(\frac{2}{q}\right)_4 = (-1)^{(q-1)/8}$.*

Proof. See Theorem 2 in [1]. □

Let d be a square-free integer which can be written as the sum of two squares and $K = \mathbb{Q}(\sqrt{d})$. If $\operatorname{rank}_2(C_K) = 2$, then, by the genus theory, d can be written as $d = p_1p_2p_3$, where p_i's are distinct prime integers such that for all i, $p_i \not\equiv 3 \pmod 4$.

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{p_1p_2p_3})$, where p_1, p_2 and p_3 are distinct prime integers such that $p_1, p_2 \not\equiv 3 \pmod 4$ and $p_3 \equiv 1 \pmod 4$ or $p_3 = 2$. Then the Hilbert 2-class field tower of K is metacyclic except for the case:*

$$\text{after a permutation of } p_i \text{ we have } \left(\frac{p_2}{p_1}\right) = \left(\frac{p_3}{p_1}\right) = 1 \text{ and}$$
$$\left(\frac{p_1}{p_2}\right)_4 \cdot \left(\frac{p_2}{p_1}\right)_4 = \left(\frac{p_1}{p_3}\right)_4 \cdot \left(\frac{p_3}{p_1}\right)_4 = 1.$$

Proof. Let p_1, p_2 and p_3 be three prime numbers such that $p_1 \equiv p_2 \equiv 1 \pmod 4$ and $p_3 \equiv 1 \pmod 4$ or $p_3 = 2$. The three unramified quadratic extensions of $K = \mathbb{Q}(\sqrt{p_1p_2p_3})$ are $L_1 = K(\sqrt{p_1}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2p_3})$, $L_2 = K(\sqrt{p_2}) = \mathbb{Q}(\sqrt{p_2}, \sqrt{p_1p_3})$ and $L_3 = K(\sqrt{p_3}) = \mathbb{Q}(\sqrt{p_3}, \sqrt{p_1p_2})$. We put $C_i = C_{L_i,2}$. From Theorem 1, the metacyclicity of $G = \operatorname{Gal}(K_2^{(\infty)}/K)$ depends on $\operatorname{rank}(C_i)$ for $i = 1, 2, 3$. Let us calculate them:

Assume for the moment that $p_3 \equiv 1 \pmod 4$. Let us take $m = p_1$, $\delta = p_2p_3$, $H = C_1$ and apply Lemma 2: The primes of $\mathbb{Q}(\sqrt{p_1})$ that ramify in $L_1 = K(\sqrt{p_1})$

are exactly those which are above p_2 and p_3. The number r of those primes depends on the two Legendre symbols $\left(\frac{p_2}{p_1}\right)$ and $\left(\frac{p_3}{p_1}\right)$, and we have the following table:

$\left(\frac{p_2}{p_1}\right)$	$\left(\frac{p_3}{p_1}\right)$	r	rank(C_1)	
1	1	4	3 if $\left(\frac{p_2}{p_1}\right)_4 = \left(\frac{p_1}{p_2}\right)_4$ and $\left(\frac{p_3}{p_1}\right)_4 = \left(\frac{p_1}{p_3}\right)_4$,	2 if not
1	-1	3	2 if $\left(\frac{p_2}{p_1}\right)_4 = \left(\frac{p_1}{p_2}\right)_4$,	1 if not
-1	1	3	2 if $\left(\frac{p_3}{p_1}\right)_4 = \left(\frac{p_1}{p_3}\right)_4$,	1 if not
-1	-1	2	1	

We will have similar tables for C_2 and C_3.

Now suppose that $p_3 = 2$. We recall that for every prime integer $p \equiv 1 \pmod 8$ we have

$$\left(\frac{p}{2}\right)_4 = (-1)^{(p-1)/8}.$$

So the calculation of rank(C_i) will be done in the same way as in the case $p_3 \equiv 1 \pmod 4$.

We deduce, using Theorem 1, that G is metacyclic if and only if the following condition (C) is not satisfied:

After a permutation of p_i's, we have:

$$\text{(C)} \qquad \left(\frac{p_2}{p_1}\right) = \left(\frac{p_3}{p_1}\right) = 1 \text{ and } \left(\frac{p_1}{p_2}\right)_4 \cdot \left(\frac{p_2}{p_1}\right)_4 = \left(\frac{p_1}{p_3}\right)_4 \cdot \left(\frac{p_3}{p_1}\right)_4 = 1.$$

□

4. Fields $\mathbb{Q}(\sqrt{D})$ where D is not the sum of two squares having a non abelian metacyclic tower

Let $K = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer which is not the sum of two squares and D_K the discriminant of K. If $\text{rank}_2(C_K) = 2$, then, by the genus theory, we will have one of the following cases: $D = q_1q_2q_3q_4$, $D = p_1p_2q_1q_2$, $D = q_1q_2q_3$, $D = p_1p_2q_1$, $D = 2q_1q_2q_3$, $D = 2p_1q_1q_2$ or $D = 2p_1p_2q_1$, where the p_i's are distinct prime integers $\equiv 1 \pmod 4$ and the q_i's are distinct prime integers $\equiv 3 \pmod 4$.

We will discuss all these cases using the number of negative prime discriminants dividing D_K and we will determine all the fields of the above forms that have a metacyclic tower.

4.1. Some lemmas. Let d and m be two positive square-free integers, $L = \mathbb{Q}(\sqrt{m}, \sqrt{d})$ be a biquadratic field, r the number of primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L, H the 2-ideal class group of L and

$$S = \Big\{q_1 \text{ odd prime integer: } q_1 \mid d \text{ and } \Big(\frac{m}{q_1}\Big) = 1\Big\}.$$

In the rest of this paper, we will use these notations for any unramified quadratic extension of a quadratic field $K = \mathbb{Q}(\sqrt{D})$ after writing it in the form $\mathbb{Q}(\sqrt{m}, \sqrt{d})$.

Lemma 3. *Suppose that $m = 2$ or m is a prime integer $\equiv 1 \pmod 4$. If there is a prime integer $q \equiv 3 \pmod 4$ that divides d, then $\operatorname{rank}(H) = r - 2$ or $r - 3$ and we have:*

- ▷ *If $m = 2$ or $m \equiv 5 \pmod 8$, then $\operatorname{rank}(H) = r - 2 \Leftrightarrow \big(\frac{-1}{q_1}\big) = 1$ for all $q_1 \in S$;*
- ▷ *If $m \equiv 1 \pmod 8$, then $\operatorname{rank}(H) = r - 2$ if and only if the following two conditions are satisfied:*
  - (c_1) *$\big(\frac{-1}{q_1}\big) = 1$ for all $q_1 \in S$.*
  - (c_2) *$d = 2c$ with $\big(\frac{-1}{c}\big) = 1$ or $d \equiv 1 \pmod 4$.*

Proof. See Theorem 1 in [1]. □

Lemma 4. *Let q, q' and q'' be three prime integers such that $q \equiv q' \equiv q'' \equiv -1 \pmod 4$, $m \in \{q, 2q, q'q''\}$. Let ε_m be the fundamental unit of $\mathbb{Q}(\sqrt{m})$. Then ε_m can be written as $\varepsilon_m = a_m u^2$, where $u \in \mathbb{Q}(\sqrt{m})$ and $a_m = 2$ if $m = q$ or $2q$, and $a_m = q'$ or q'' if $m = q'q''$.*

Proof. Let $m \in \{q, 2q, q'q''\}$ and $k_m = \mathbb{Q}(\sqrt{m})$, and let N be the norm map of the extension $k_m/\mathbb{Q}$. Since m is not the sum of two squares, then $N(\varepsilon_m) = 1$. By Lemma 2.3 in [6] there exists a positive square free integer b_m dividing D_m, the discriminant of k_m such that $b_m\varepsilon_m = \alpha^2$, where $\alpha \in k_m$. We note that $b_m \neq 1$ since ε_m is a fundamental unit of k_m.

If $m = q'q''$, then $D_m = m$ and $b_m = q'$, q'' or $q'q''$. If $b_m = q'q''$, then $\varepsilon_m = \big(\frac{\alpha}{\sqrt{m}}\big)^2$ which is impossible since ε_m is a fundamental unit of k_m. We conclude that $b_m = q'$ or q''. If $b_m = q'$, for example, then

$$\varepsilon_m = \frac{1}{q'}\alpha^2 = q'\Big(\frac{\alpha}{q'}\Big)^2 = q''\Big(\frac{\alpha}{\sqrt{m}}\Big)^2.$$

If $m = q$, then $b_m = 2$, q or $2q$. If $b_m = q$, then $\varepsilon_m = \big(\frac{\alpha}{\sqrt{m}}\big)^2$ which is impossible since ε_m is a fundamental unit of k_m. We conclude that $b_m = 2$ or $2q$. If $b_m = 2$, then $\varepsilon_m = 2\big(\frac{\alpha}{2}\big)^2$. If $b_m = 2q$, then $\varepsilon_m = 2\big(\frac{\alpha}{2\sqrt{m}}\big)^2$.

If $m = 2q$, then $b_m = 2$, q or $2q$. If $b_m = 2q$, then $\varepsilon_m = \left(\frac{\alpha}{\sqrt{m}}\right)^2$ which is impossible since ε_m is a fundamental unit of k_m. We conclude that $b_m = 2$ or q. If $b_m = q$, then $\varepsilon_m = 2\left(\frac{\alpha}{\sqrt{m}}\right)^2$. If $b_m = 2$, then $\varepsilon_m = 2\left(\frac{\alpha}{2}\right)^2$. □

Let q, q', q'', m, ε_m and a_m be as in the above lemma and d a positive square-free integer. Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{d})$ and H the 2-ideal class group of L.

We note that we will use these notations in the rest of this paper.

Lemma 5. *With the above assumptions and notations, if* $m = q, 2q$ *or* $m = q'q'' \equiv 5 \pmod 8$, *then* $\operatorname{rank}(H) = r - 1 - e$, *where* $e = 0, 1$ *or* 2, *and we have:*

- ▷ $e = 0$ *if and only if* $\left(\frac{-1}{q_1}\right) = \left(\frac{a_m}{q_1}\right) = 1$ *for all* $q_1 \in S$;
- ▷ $e = 2$ *if and only if exists distinct primes* $q_1, q_2, q_3 \in S$ *such that*

$$\left(\frac{-1}{q_1}\right) = \left(\frac{a_m}{q_1}\right) = -1 \quad \textit{and} \quad \left(\frac{-1}{q_3}\right) \neq \left(\frac{a_m}{q_3}\right).$$

P r o o f. See Theorem 3 in [2]. □

Lemma 6. *If* $m = q'q'' \equiv 1 \pmod 8$, *then* $\operatorname{rank}(H) = r - 1 - e$ *with* $e = 0, 1$ *or* 2, *and we have:*

- ▷ $e = 0$ *if and only if* $\left(\frac{-1}{q_1}\right) = \left(\frac{a_m}{q_1}\right) = 1$ *for all* $q_1 \in S$ *and* $d \equiv 1 \pmod 4$ *or* $d = 2c$ *with* $\left(\frac{-1}{c}\right) = \left(\frac{2}{q'}\right) = 1$;
- ▷ $e = 2$ *if and only if one of the following conditions is satisfied:*
  - (i) $d \equiv -1 \pmod 4$ *and exists* $q_1 \in S$: $\left(\frac{-1}{q_1}\right) \neq \left(\frac{a_m}{q_1}\right)$,
  - (ii) $d \equiv 1 \pmod 4$ *and exists* $q_1, q_2, q_3 \in S$ *such that*

$$\left(\frac{-1}{q_1}\right) = \left(\frac{a_m}{q_2}\right) = -1 \quad \textit{and} \quad \left(\frac{-1}{q_3}\right) \neq \left(\frac{a_m}{q_3}\right),$$

  - (iii) $d = 2c$ *with*

$$\left(\frac{2}{q'}\right) = -\left(\frac{-1}{c}\right) = 1$$

and exists $q_1 \in S$ *such that*

$$\left(\frac{-1}{q_1}\right) \neq \left(\frac{a_m}{q_1}\right) \quad \textit{or} \quad \left(\frac{2}{q'}\right) = -\left(\frac{-1}{c}\right) = -1$$

and exists $q_1 \in S$ *such that* $\left(\frac{-1}{q_1}\right) = -1$ *or* $\left(\frac{2}{q'}\right) = \left(\frac{-1}{c}\right) = 1$ *and exists distinct primes* $q_1, q_2, q_3 \in S$ *such that*

$$\left(\frac{-1}{q_1}\right) = \left(\frac{a_m}{q_2}\right) = -1 \quad \textit{and} \quad \left(\frac{-1}{q_3}\right) \neq \left(\frac{a_m}{q_3}\right).$$

P r o o f. See Theorem 4 in [2]. □

4.2. Case where D_K is divisible by at least 3 odd negative prime discriminants.

Theorem 3. *The Hilbert 2-class field tower of K is metacyclic for the cases $K=\mathbb{Q}(\sqrt{q_1q_2q_3q_4})$, $K=\mathbb{Q}(\sqrt{q_1q_2q_3})$ and $K=\mathbb{Q}(\sqrt{2q_1q_2q_3})$, where the q_i's are primes $\equiv 3 \pmod 4$.*

P r o o f. We discuss the 3 cases:

Case $K=\mathbb{Q}(\sqrt{q_1q_2q_3q_4})$: The quadratic extensions of K contained in $K^{(1)}$ are $L_1=K(\sqrt{q_1q_2})=\mathbb{Q}(\sqrt{q_1q_2},\sqrt{q_3q_4})$, $L_2=K(\sqrt{q_1q_3})=\mathbb{Q}(\sqrt{q_1q_3},\sqrt{q_2q_4})$ and $L_3=K(\sqrt{q_1q_4})=\mathbb{Q}(\sqrt{q_1q_4},\sqrt{q_2q_3})$. We put $C_i=C_{L_i,2}$.

Let us obtain an upper bound for the value of $\operatorname{rank}(C_1)$. We put $m=q_1q_2$ and $d=q_3q_4$. The primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L_1 are exactly those which are above q_3 and q_4. Their number r is $\leqslant 4$ and $r=4$ if and only if $\left(\frac{m}{q_3}\right)=\left(\frac{m}{q_4}\right)=1$. In this case $S=\{q_3,q_4\}$.

If $r\leqslant 3$, then by Lemma 5 in the case $m\equiv 5 \pmod 8$ or Lemma 6 in the case $m\equiv 1 \pmod 8$, we have $\operatorname{rank}(C_1)=1$.

If $r=4$, then the condition to have $e=0$ in Lemma 5 and Lemma 6 is not satisfied since $\left(\frac{-1}{q_3}\right)=-1$ and then $\operatorname{rank}(C_1)\leqslant 2$.

In the same way, we have $\operatorname{rank}(C_2),\operatorname{rank}(C_3)\leqslant 2$ and we conclude using Theorem 1.

Case $K=\mathbb{Q}(\sqrt{q_1q_2q_3})$: The quadratic extensions of K contained in $K^{(1)}$ are $L_1=K(\sqrt{q_1q_2})=\mathbb{Q}(\sqrt{q_3},\sqrt{q_1q_2})$, $L_2=K(\sqrt{q_2q_3})=\mathbb{Q}(\sqrt{q_1},\sqrt{q_2q_3})$ and $L_3=K(\sqrt{q_3q_1})=\mathbb{Q}(\sqrt{q_2},\sqrt{q_3q_1}))$. We put $C_i=C_{L_i,2}$. Let us compute $\operatorname{rank}(C_1)$. We put $d=q_3$ and $m=q_1q_2$. The only primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L_1 are those which are above 2 and q_3, so $r\leqslant 4$ and then $\operatorname{rank}(C_1)=r-1-e\leqslant 4-1-e=3-e$.

In the case $m\equiv 5 \pmod 8$, 2 is inert in $\mathbb{Q}(\sqrt{m})$, then $r\leqslant 3$ and $\operatorname{rank}(C_1)\leqslant 2$. If $m\equiv 1 \pmod 8$, then according to Lemma 6, $e\neq 0$ and then $\operatorname{rank}(C_1)\leqslant 2$. Similarly, we have $\operatorname{rank}(C_i)\leqslant 2$ for $i=2,3$ and the proof for this case is completed.

Case $K=\mathbb{Q}(\sqrt{2q_1q_2q_3})$: The quadratic extensions of K contained in $K^{(1)}$ are the $L_i=\mathbb{Q}(\sqrt{2q_i},\sqrt{q_jq_k})$, where $i\in\{1,2,3\}$ and $\{i,j,k\}=\{1,2,3\}$. Let us put $C_i=C_{L_i,2}$ for $i=1,2,3$. To calculate $\operatorname{rank}(C_1)$, we apply Lemma 5 with $m=2q_1$ and $d=q_2q_3$. The primes of $\mathbb{Q}(\sqrt{m})$ that ramify in $L_1=\mathbb{Q}(\sqrt{m},\sqrt{d})$ are those which are above q_2 and q_3. If $\left(\left(\frac{m}{q_2}\right),\left(\frac{m}{q_3}\right)\right)\neq(1,1)$, then their number r is $\leqslant 3$, and $\operatorname{rank}(C_1)=r-1-e\leqslant 2$. If $\left(\left(\frac{m}{q_2}\right),\left(\frac{m}{q_3}\right)\right)=(1,1)$, then $r=4$, but by Lemma 5, $e\neq 0$ and then $\operatorname{rank}(C_1)=r-1-e\leqslant 2$.

Similarly, we prove that $\operatorname{rank}(C_2)\leqslant 2$ and $\operatorname{rank}(C_3)\leqslant 2$. We conclude using Theorem 1. □

4.3. Case where D_K is divisible by exactly 1 odd negative prime discriminant.

Theorem 4. *For $K = \mathbb{Q}(\sqrt{p_1p_2q_1})$ and $K = \mathbb{Q}(\sqrt{2p_1p_2q_1})$ with $p_1 \equiv p_2 \equiv -q_1 \equiv 1 \pmod 4$, the Hilbert 2-class field tower is metacyclic except for the following two cases:*

(i) *after permutations of p_i's, we have:* $\left(\frac{2}{p_1}\right) = \left(\frac{p_2}{p_1}\right) = \left(\frac{q_1}{p_1}\right) = 1$;

(ii) $\left(\frac{q_1}{p_1}\right) = \left(\frac{q_1}{p_2}\right) = \left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = 1$.

Proof. We discuss the 2 cases:

Case $K = \mathbb{Q}(\sqrt{p_1p_2q_1})$: The quadratic extensions of K contained in $K^{(1)}$ are $L_1 = K(\sqrt{p_1}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2q_1})$, $L_2 = K(\sqrt{p_2}) = \mathbb{Q}(\sqrt{p_2}, \sqrt{p_1q_1})$ and $L_3 = K(\sqrt{p_1p_2}) = K(\sqrt{q_1}) = \mathbb{Q}(\sqrt{q_1}, \sqrt{p_1p_2})$. We put $C_i = C_{L_i,2}$.

To compute the rank of C_1, let us apply Lemma 3 with $m = p_1$ and $d = p_2q_1$. The primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L_1 are those which are above 2, p_2 and q_1. We have the following table:

$\left(\frac{2}{p_1}\right)$	$\left(\frac{p_2}{p_1}\right)$	$\left(\frac{q_1}{p_1}\right)$	r	rank(C_1)
1	1	1	6	3
1	1	-1	5	2
1	-1	1	5	2
1	-1	-1	4	1
-1	1	1	5	2
-1	1	-1	4	2
-1	-1	1	4	1
-1	-1	-1	3	1

Similarly, we calculate rank(C_2).

To calculate the rank of C_3, let us apply Lemma 5 with $m = q_1$ and $d = p_1p_2$. Note that in this case $a_m = 2$. The primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L_3 are those which are above p_1 and p_2. We have the following table:

$\left(\frac{q_1}{p_1}\right)$	$\left(\frac{q_1}{p_2}\right)$	r	rank(C_3)	
1	1	4	3 if $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = 1$,	2 if not
1	-1	3	2 if $\left(\frac{2}{p_1}\right) = 1$,	1 if not
-1	1	3	2 if $\left(\frac{2}{p_2}\right) = 1$,	1 if not
-1	-1	2	1	

We conclude using Theorem 1 and the above tables.

Case $K = \mathbb{Q}(\sqrt{2p_1p_2q_1})$: the quadratic extensions of K contained in $K^{(1)}$ are $L_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{2p_2q_1})$, $L_2 = \mathbb{Q}(\sqrt{p_2}, \sqrt{2p_1q_1})$ and $L_3 = \mathbb{Q}(\sqrt{2q_1}, \sqrt{p_1p_2})$.

To calculate rank(C_1) we take $m = p_1$ and $d = 2p_2q_1$ and apply Lemma 3. We have the following table:

$\left(\frac{2}{p_1}\right)$	$\left(\frac{p_2}{p_1}\right)$	$\left(\frac{q_1}{p_1}\right)$	r	rank(C_1)
1	1	1	6	3
1	1	-1	5	2
1	-1	1	5	2
1	-1	-1	4	1
-1	1	1	5	2
-1	1	-1	4	2
-1	-1	1	4	1
-1	-1	-1	3	1

We would have a similar table for rank(C_2).

To calculate rank(C_3) we put $m = 2q_1$ and $d = p_1p_2$ and we apply Lemma 5. We have the following table:

$\left(\frac{2q_1}{p_1}\right)$	$\left(\frac{2q_1}{p_2}\right)$	r	rank(C_3)	
1	1	4	3 if $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = 1$,	2 if not
1	-1	3	2 if $\left(\frac{2}{p_1}\right) = 1$,	1 if not
-1	1	3	2 if $\left(\frac{2}{p_2}\right) = 1$,	1 if not
-1	-1	2	1	

We conclude by using Theorem 1. □

4.4. Case where D_K is divisible by exactly 2 odd negative prime discriminants.

Theorem 5. *Let* $K = \mathbb{Q}(\sqrt{p_1p_2q_1q_2})$ *with* $p_1 \equiv p_2 \equiv 1 \pmod 4$ *and* $q_1 \equiv q_2 \equiv 3 \pmod 4$. *Then the Hilbert 2-class field tower of* K *is metacyclic except for the following two cases:*

(i) *After a permutation of* p_i*'s, we have* $\left(\frac{p_2}{p_1}\right) = \left(\frac{q_1}{p_1}\right) = \left(\frac{q_2}{p_1}\right) = 1$;

(ii) $\left(\frac{q_1}{p_1}\right) = \left(\frac{q_2}{p_1}\right) = \left(\frac{q_1}{p_2}\right) = \left(\frac{q_2}{p_2}\right) = 1$.

P r o o f. The quadratic extensions of K contained in $K^{(1)}$ are $L_1 = K(\sqrt{p_1}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2q_1q_2})$, $L_2 = K(\sqrt{p_2}) = \mathbb{Q}(\sqrt{p_2}, \sqrt{p_1q_1q_2})$ and $L_3 = K(\sqrt{p_1p_2}) = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q_1q_2})$. We put $C_i = C_{L_i,2}$.

Let us apply Lemma 3 with $m = p_1$, $d = p_2q_1q_2$ and $H = C_1$: The primes of $\mathbb{Q}(\sqrt{p_1})$ that ramify in $L_1 = K(\sqrt{p_1})$ are exactly those which are above p_2, q_1 and q_2. Their number r depends on $\left(\frac{p_1}{p_2}\right)$, $\left(\frac{p_1}{q_1}\right)$ and $\left(\frac{p_1}{q_2}\right)$. Since $d \equiv 1 \pmod 4$, the study of the cases $m \equiv 1 \pmod 8$ and $m \equiv 5 \pmod 8$ is the same and so we have the following table:

$\left(\frac{p_2}{p_1}\right)$	$\left(\frac{q_1}{p_1}\right)$	$\left(\frac{q_2}{p_1}\right)$	r	rank(C_1)
1	1	1	6	3
1	1	−1	5	2
1	−1	1	5	2
1	−1	−1	4	2
−1	1	1	5	2
−1	1	−1	4	1
−1	−1	1	4	1
−1	−1	−1	3	1

We would have a similar table for rank(C_2).

To calculate rank(C_3) we take $m = q_1q_2$, $a_m = q_1$ and $d = p_1p_2$. The primes of $\mathbb{Q}(\sqrt{m})$ that ramify in L_3 are exactly those which are above p_1 and p_2. Depending on whether $m \equiv 5 \pmod 8$ or $m \equiv 1 \pmod 8$, we apply Lemma 5 or Lemma 6, respectively. In the two cases we have the following table:

$\left(\frac{m}{p_1}\right)$	$\left(\frac{m}{p_2}\right)$	r	rank(C_3)	
1	1	4	3 if $\left(\frac{q_1}{p_1}\right) = \left(\frac{q_1}{p_2}\right) = 1$,	2 if not
1	−1	3	2 if $\left(\frac{q_1}{p_1}\right) = 1$,	1 if not
−1	−1	2	1	

We conclude using Theorem 1 and the two last tables above. □

Theorem 6. *Let $K = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ with $p_1 \equiv -q_2 \equiv -q_3 \equiv 1 \pmod 4$. The Hilbert 2-class field tower of K is metacyclic except for the following cases:*

(a) $\left(\frac{2}{p_1}\right) = \left(\frac{q_1}{p_1}\right) = \left(\frac{q_2}{p_1}\right) = 1$,
(b) $\left(\frac{2}{p_1}\right) = \left(\frac{2}{q_1}\right) = \left(\frac{2}{q_2}\right) = 1$,
(c) $\left(\frac{2}{q_1}\right) = \left(\frac{2}{q_2}\right) = \left(\frac{p_1}{q_1}\right) = \left(\frac{p_1}{q_2}\right) = 1$.

P r o o f. The quadratic extensions of K contained in $K^{(1)}$ are $L_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{2q_1q_2})$, $L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{p_1q_1q_2})$ and $L_3 = \mathbb{Q}(\sqrt{q_1q_2}, \sqrt{2p_1})$. Let us put $C_i = C_{L_i,2}$ for $i = 1, 2, 3$.

To compute $\mathrm{rank}(C_1)$ we apply Lemma 3 with $m = p_1$ and $d = 2q_1q_2$, and we have the following table:

$\left(\frac{2}{p_1}\right)$	$\left(\frac{q_1}{p_1}\right)$	$\left(\frac{q_2}{p_1}\right)$	r	$\mathrm{rank}(C_1)$
1	1	1	6	3
1	1	−1	5	2
1	−1	1	5	2
1	−1	−1	4	2
−1	1	1	5	2
−1	1	−1	4	1
−1	−1	1	4	1
−1	−1	−1	3	1

To compute $\mathrm{rank}(C_2)$ we apply Lemma 3 with $m = 2$ and $d = p_1q_1q_2$ and we have the following table:

$\left(\frac{2}{p_1}\right)$	$\left(\frac{2}{q_1}\right)$	$\left(\frac{2}{q_2}\right)$	r	$\mathrm{rank}(C_2)$
1	1	1	6	3
1	1	−1	5	2
1	−1	1	5	2
1	−1	−1	4	2
−1	1	1	5	2
−1	1	−1	4	1
−1	−1	1	4	1
−1	−1	−1	3	1

To compute $\mathrm{rank}(C_3)$ we take $m = q_1q_2$, $a_m = q_1$ and $d = 2p_1$ and apply Lemma 5 or Lemma 6 depending on whether $m \equiv 1$ or $5 \pmod 8$, respectively, and we have the following table:

$\left(\frac{2}{q_1q_2}\right)$	$\left(\frac{p_1}{q_1q_2}\right)$	r	$\mathrm{rank}(C_3)$
1	1	4	3 if $\left(\frac{p_1}{q_1}\right) = \left(\frac{2}{q_1}\right) = 1$ 2 if not
1	−1	3	$\leqslant 2$
−1	1	3	$\leqslant 2$
−1	−1	2	1

We conclude by Theorem 1. □

References

[1] *A. Azizi, A. Mouhib*: On the rank of the 2-class group of $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ where $m = 2$ or a prime $p \equiv 1 \pmod 4$. Trans. Am. Math. Soc. *353* (2001), 2741–2752. (In French.) zbl MR doi

[2] *A. Azizi, A. Mouhib*: Capitulation of the 2-ideal classes of biquadratic fields whose class field differs from the Hilbert class field. Pac. J. Math. *218* (2005), 17–36. (In French.) zbl MR doi

[3] *E. Benjamin, F. Lemmermeyer, C. Snyder*: Real quadratic fields with abelian 2-class field tower. J. Number Theory *73* (1998), 182–194. zbl MR doi

[4] *Y. Berkovich, Z. Janko*: On subgroups of finite p-group. Isr. J. Math. *171* (2009), 29–49. zbl MR doi

[5] *J. Martinet*: Tours de corps de classes et estimations de discriminants. Invent. Math. *44* (1978), 65–73. (In French.) zbl MR doi

[6] *A. Mouhib*: On the parity of the class number of multiquadratic number fields. J. Number Theory *129* (2009), 1205–1211. zbl MR doi

[7] *A. Mouhib*: On 2-class field towers of some real quadratic number fields with 2-class groups of rank 3. Ill. J. Math. *57* (2013), 1009–1018. zbl MR

[8] *A. Mouhib*: A positive proportion of some quadratic number fields with infinite Hilbert 2-class field tower. Ramanujan J. *40* (2016), 405–412. zbl MR doi

[9] *O. Taussky*: A remark on the class field tower. J. London Math. Soc. *12* (1937), 82–85. zbl MR doi

Authors' address: *Said Essahel*, *Ahmed Dakkak*, *Ali Mouhib*, Sidi Mohammed Ben Abdellah University, Sciences and Engineering Laboratory, Polydisciplinary Faculty of Taza, Taza-Gare PB 1223, Taza, Morocco, e-mail: `essahel69@yahoo.fr`, `dakkakahmed@hotmail.com`, `mouhibali@yahoo.fr`.