Czechoslovak Mathematical Journal

Abdelmalek Azizi; Ali Mouhib
On the Hilbert 2-class field tower of some abelian 2-extensions over the field of rational numbers

Czechoslovak Mathematical Journal, Vol. 63 (2013), No. 4, 1135–1148

Persistent URL: `http://dml.cz/dmlcz/143620`

Terms of use:

© Institute of Mathematics AS CR, 2013

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://dml.cz`

Czechoslovak Mathematical Journal, 63 (138) (2013), 1135–1148

ON THE HILBERT 2-CLASS FIELD TOWER OF SOME ABELIAN 2-EXTENSIONS OVER THE FIELD OF RATIONAL NUMBERS

Abdelmalek Azizi, Oujda, Ali Mouhib, Taza

(Received December 7, 2012)

Abstract. It is well known by results of Golod and Shafarevich that the Hilbert 2-class field tower of any real quadratic number field, in which the discriminant is not a sum of two squares and divisible by eight primes, is infinite. The aim of this article is to extend this result to any real abelian 2-extension over the field of rational numbers. So using genus theory, units of biquadratic number fields and norm residue symbol, we prove that for every real abelian 2-extension over $\mathbb{Q}$ in which eight primes ramify and one of theses primes $\equiv -1 \pmod 4$, the Hilbert 2-class field tower is infinite.

Keywords: class group; class field tower; multiquadratic number field

MSC 2010: 11R11, 11R29, 11R37

1. Introduction

Let k be a number field. We will denote the 2-ideal class group of k in the wide sense by $C_{2,k}$ and the 2-ideal class group of k in the strict sense by $C_{2,k}^{+}$. Denote by k^1 the Hilbert 2-class field of k. For n positive integer, let k^n be defined inductively as $k^0 = k$ and $k^{n+1} = (k^n)^1$. Then

$$k^0 \subset k^1 \subset k^2 \subset \ldots \subset k^n \subset \ldots$$

is called the 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.

Assume k is a real quadratic number field with discriminant d. It is well known that in the case where $\operatorname{rank}(C_{2,k}) \geqslant 6$, the Hilbert 2-class field tower of k is infinite [2]. We note that by genus theory, $\operatorname{rank}(C_{2,k}) \geqslant 6$ is equivalent to d is a sum of two squares and divisible by seven primes or d is not a sum of two squares and divisible by eight primes. In the case where $\mathrm{rank}(C_{2,k}) \leqslant 3$, there exist examples of fields k in which the Hilbert 2-class field tower is finite. In the case where $\mathrm{rank}(C_{2,k}) \in \{4,5\}$, at present no example of k with finite 2-class field tower is known.

In the case where k is any real abelian 2-extension over the field $\mathbb{Q}$ of rational numbers (i.e., abelian extension over $\mathbb{Q}$ with Galois group of order a power of 2) in which the discriminant is divisible by seven primes $\not\equiv -1 \pmod 4$, then we can see (Proposition 12.4) that the genus field of k contains some quadratic number field F in which the seven primes are ramified. Then the Hilbert 2-class field tower of F is infinite, consequently the Hilbert 2-class field tower of k is infinite, too. Therefore, in this article we will show by an elementary proof that the Hilbert 2-class field tower of any real abelian 2-extension over $\mathbb{Q}$ in which the discriminant is divisible by eight primes and one of these primes is $\equiv -1 \pmod 4$, is infinite. We mention that in [7], using some properties of the Schur multiplicator, L. V. Kuzmin proved that if $k/\mathbb{Q}$ is an abelian extension and at least eight primes ramify, then the Hilbert 2-class field tower of k is infinite.

Several works discussed the problem of 2-class field tower of real quadratic number fields k in which $\mathrm{rank}(C_{2,k}) \in \{4,5\}$:

In [8], C. Maire has shown that if $C_{2,k}$ contains a subgroup of type $(4,4,4,4)$, then the Hilbert 2-class field tower of k is infinite. F. Gerth in [1] has shown that in the case where $\mathrm{rank}(C_{2,k}) = 5$, d is not a sum of two squares (which is equivalent to the existence of a prime $\equiv -1 \pmod 4$ dividing d) and $C_{2,k}$ contains a subgroup of type $(4,4,4)$ then the Hilbert 2-class field tower of k is infinite. We mention that in [9], the second author proves that it suffices that the group $C^{+}_{2,k}$ contains a sub-group of type $(4,4,4)$ such that the Hilbert 2-class field tower of k is infinite. Usually in the case where $\mathrm{rank}(C_{2,k}) = 5$, we show that if there are at least five primes $\not\equiv -1 \pmod 4$ ramifying in k, then the Hilbert 2-class field tower of k is infinite (see Proposition 3.1).

The aim of this article is to prove the following theorem:

Theorem 1. *For every real abelian 2-extension over $\mathbb{Q}$ in which eight primes ramify and one of theses primes $\equiv -1 \pmod 4$, the Hilbert 2-class field tower is infinite.*

Remark. With the assumption of Theorem 1, the genus field $k^{(*)}$ of such abelian 2-extension over $\mathbb{Q}$ contains some real multiquadratic number field K in which eight primes ramify (see Proposition 2.4). Therefore, proving Theorem 1 is reduced to proving the following theorem:

Theorem 2. *For every real multiquadratic number field in which eight primes ramify and one of theses primes* $\equiv -1 \pmod 4$, *the Hilbert 2-class field tower is infinite.*

Proving Theorem 2 for such real multiquadratic number field k is reduced to determining a subfield M of the genus field k^* of k in which the rank of the 2-class group is larger, in order that M satisfies the Golod and Shafarevich inequality (Theorem 2.1). The field M is chosen to be quadratic, biquadratic or triquadratic number field. To prove that such a field M verifies the Golod and Shafarevich inequality, we will use Jehne's inequality (see Section 2.2), so we will determine a subfield M' of M such that M/M' is a quadratic extension with larger number of ramified primes $\mathrm{ram}(M/M')$ and with a refined upper bound of the unit index $[E_{M'}\colon E_{M'} \cap N_{M/M'}(M^*)] = 2^{e(M/M')}$, where $E_{M'}$ is the group of units of M', in order to find:

$$\mathrm{ram}(M/M') - 1 - e(M/M') \geqslant 2 + 2\sqrt{\dim(E_M/E_M^2) + 1}.$$

Consequently, when M satisfies the Golod and Shafarevich inequality, then M has infinite Hilbert 2-class field tower. Finally, since k^* contains M, and k^*/k is an abelian unramified extension, we conclude the theorem.

The proof of Theorem 2 is presented by distinguishing four cases, depending on the number of ramified primes which are not sum of two squares in the real multiquadratic number field k.

2. Preliminaries and some fundamental results

2.1. On the Golod and Shafarevich inequality. In 1964, Golod and Shafarevich established for the first time the existence of infinite Hilbert p-class field tower when p is a prime number. Their result can be phrased as follows [2]:

Theorem 2.1. *Let k be a number field, E_k the group of units of k and $C_{p,k}$ the p-class group of k. Then if*

$$\mathrm{rank}(C_{p,k}) \geqslant 2 + 2\sqrt{\dim(E_k/E_k^p) + 1},$$

then the Hilbert p-class field tower of k is infinite.

We shall refer to the above inequality as the Golod and Shafarevich inequality.

We give some remarks in the case where $p = 2$:

Remark 2.2. (1) It is clear that if k is a real quadratic number field, we have $\dim(E_k/E_k^2) = 2$. Suppose $\mathrm{rank}(C_{2,k}) \geqslant 6$, then the inequality of Golod and Shafarevich is satisfied which implies that the Hilbert 2-class field tower of k is infinite.

(2) If k is a real biquadratic (resp. triquadratic) number field, we have $\dim(E_k/E_k^2) = 4$ (resp. $\dim(E_k/E_k^2) = 8$), thus, the inequality of Golod and Shafarevich is satisfied, whenever $\mathrm{rank}(C_{2,k}) \geqslant 7$ (resp. $\mathrm{rank}(C_{2,k}) \geqslant 8$).

There exists a result which gives a lower bound for the rank of the p-class group for some number fields K. Especially, the case where K is a cyclic extension of degree p over a number field k:

2.2. On the rank of the p-class group of some number fields. Let K/k be an extension of a number field of degree a prime number p. It is well known by Jehne's results [5] that

$$\mathrm{rank}(C_{p,K}) \geqslant \mathrm{ram}(K/k) - 1 - e(K/k),$$

where $\mathrm{ram}(K/k)$ is the number of primes ramified in the extension K/k and $e(K/k)$ is the natural number defined by $p^{e(K/k)} = [E_k\colon\ E_k \cap N_{K/k}(K^*)]$.

In the case where $p = 2$ and the class number of k is odd, then by using the ambiguous class number formula, the inequality $\mathrm{rank}(C_{2,k}) \geqslant \mathrm{ram}(K/k) - 1 - e(K/k)$ becomes an equality.

2.2.1. Determination of the natural number $e(K/k)$ in some cases. It is a difficult problem to determine the value of the natural number $e(K/k)$. This is related to having information on the fundamental units of the number field k which is not every time satisfied. If the fundamental system of units of k is known, k contains all primitive roots of unity and $K = k(\sqrt[n]{\alpha})$, then we can use the results of the norm residue symbols:

A unit ε of k is a norm of an element in the extension K/k if and only if for every prime $\mathcal{P}$ of k which ramifies in K/k, the value of the norm residue symbol $((\varepsilon,\alpha)/\mathcal{P})$ is equal to 1 (for more information see [3]).

▷ The case where k is a real quadratic number field:

It is clear that in the case where k is a real quadratic number field, E_k is generated by -1 and the fundamental unit ε of k. Let K be a quadratic extension of k, then $e(K/k) \in \{0, 1, 2\}$. The value of $e(K/k)$ is related to whether $\pm\varepsilon^i$ ($i = 0$ or 1) is a norm or not in the extension K/k.

▷ The case where k is a real biquadratic number field:

It is known that in the case where k is a real biquadratic number field, we have $\dim(E_k/E_k^2) = 4$ and the fundamental system of units of k contains three units denoted $\varepsilon_1, \varepsilon_2$ and ε_3. Let K be a quadratic extension of k, then $e(K/k) \in \{1,2,3,4\}$. The value of $e(K/k)$ is related to whether the units $\pm\varepsilon_1^i\varepsilon_2^j\varepsilon_3^k$ $(i,j,k \in \{0,1\})$ are norms or not in K/k.

In the following lemma, we give some necesssary and sufficient conditions such that -1 is a norm in some quadratic extension of a real biquadratic number field. We are going to use this result in the sequel.

Lemma 2.3. *Let d_1, d_2 and d be distinct square free positive integers. Denote by $k = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and $K = k(\sqrt{d})$. Then -1 is a norm in the extension K/k if and only if for every odd prime p dividing d such that $(d_1/p) = (d_2/p) = 1$, we have $p \not\equiv -1 \pmod 4$ and if $(d_1/2) = (d_2/2) = 1$, we have $d \equiv 1 \pmod 4$ or $d \equiv 2 \pmod 8$.*

P r o o f. We know that -1 is a norm of an element in the extension K/k if and only if for every prime $\mathcal{P}$ of k ramified in K, we have $((-1,d)/\mathcal{P}) = 1$. Let $\mathcal{P}$ be an ideal prime of k ramified in K. Then $\mathcal{P}$ lies above some prime number p dividing $4d$. Denote by L the decomposition field of p in k.

Assume L is a quadratic number field. It follows by norm residue symbol properties that

$$\Big(\frac{-1,d}{\mathcal{P}}\Big) = \Big(\frac{N_{k/L}(-1),d}{\mathcal{P}}\Big) = \Big(\frac{1,d}{\mathcal{P}}\Big) = 1.$$

Assume $L = \mathbb{Q}$, then for every quadratic number field F contained in k, we see that

$$\Big(\frac{-1,d}{\mathcal{P}}\Big) = \Big(\frac{N_{k/F}(-1),d}{\mathcal{P}}\Big) = \Big(\frac{1,d}{\mathcal{P}}\Big) = 1.$$

Assume now that $L = k$, which is equivalent to $(d_1/p) = (d_2/p) = 1$. Then, in the case where p is odd, we have

$$\Big(\frac{-1,d}{\mathcal{P}}\Big) = \Big(\frac{-1,p}{p}\Big) = \Big(\frac{-1}{p}\Big).$$

It follows that

$$\Big(\frac{-1,d}{\mathcal{P}}\Big) = 1 \Longleftrightarrow p \equiv 1 \pmod 4. \tag{2.1}$$

In the case where $p = 2$, we have $((-1,d)/\mathcal{P}) = ((-1,d)/2)$ and

$$\Big(\frac{-1,d}{2}\Big) = 1 \Longleftrightarrow d \equiv 1 \pmod 4 \text{ or } d = 2d' \text{ and } d' \equiv 1 \pmod 4. \tag{2.2}$$

Consequently, using (2.1) and (2.2), we have the lemma. □

2.3. On genus field of abelian 2-extensions. Let k be an abelian 2-extension over $\mathbb{Q}$. Define $k^{(*)}$ the genus field of k, as the maximal abelian extension over $\mathbb{Q}$ which is non-ramified, at finite and infinite primes of k. We define $k_{(*)}$ the genus field in the narrow sense of k, as the maximal abelian extension over $\mathbb{Q}$ which is non-ramified, at finite primes of k. In the case where k is totally real, then $k^{(*)}$ is the maximal real subfield of $k_{(*)}$.

Let D_k be the discriminant of k. For every prime $p \mid D_k$, denote by $e(p)$ the ramification index of p in k. In the case where $p \neq 2$, let $M(p)$ be the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[M(p)\colon \mathbb{Q}] = e(p)$. Then by [4], Theorem 4, page 48, we have:

$$k_{(*)} = \prod_{p \mid D_k,\, p \neq 2} M(p)k = \prod_{p \mid D_k,\, p \neq 2} M(p)M(2),$$

where $M(2)$ is as a subfield of some $\mathbb{Q}(\zeta_{2^n})$ $(n \in \mathbb{N})$ such that $[M(2)\colon \mathbb{Q}] = e(2)$.

It is clear that in the case where $p \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{p})$ is contained in $k_{(*)}$ and in the case where $p \equiv -1 \pmod 4$, $\mathbb{Q}(\sqrt{-p})$ is contained in $k_{(*)}$. In the case where $p = 2$, $k_{(*)}$ contains at least one of the three quadratic number fields: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2}\mathrm{i})$.

We can thus see immediately the following proposition:

Proposition 2.4. *Let k be an abelian 2-extension over $\mathbb{Q}$, D_k the discriminant of k. Assume k is totally real, then $k_{(*)}$ contains some multiquadratic number field in which every prime dividing D_k is ramified.*

Assume now that k is a real multiquadratic number field. Denote by $S_1 = \{p \text{ prime ramified in } k \mid p \equiv 1 \pmod 4\}$ and by $S_2 = \{p \text{ prime ramified in } k \mid p \equiv -1 \pmod 4\}$.

By the discussion above, we have

$$[k^{(*)}\colon \mathbb{Q}] = \frac{1}{2} \prod_{p \mid D_k} e(p) \text{ or } \prod_{p \mid D_k} e(p).$$

Precisely $[k^{(*)}\colon \mathbb{Q}] = \frac{1}{2} \prod_{p \mid D_k} e(p)$ if and only if $S_2 \neq \emptyset$.

We mention that an odd prime ramified in k is of ramification index equal to 2. Moreover, if 2 is ramified in k, then the ramification index of 2 is equal to 2 or 4.

We can immediately verify that the genus field of k is of one of the following forms:

▷ Suppose that 2 is of ramification index equal to 4 in k, then

$$k^{(*)} = \prod_{\ell \mid D_k} \mathbb{Q}(\sqrt{\ell}).$$

▷ Suppose that 2 is of ramification index equal to 2 in k, then we distinguish between two cases:

(i) If for every positive integer m, $\sqrt{2m} \notin k$, then

$$k^{(*)} = \prod_{\ell \in S_1 \cup S_2} \mathbb{Q}(\sqrt{\ell}).$$

(ii) If there exists a positive integer m such that $\sqrt{2m} \in k$, then

$$k^{(*)} = \mathbb{Q}(\sqrt{2m}) \prod_{\ell \in S_1} \mathbb{Q}(\sqrt{\ell}) \prod_{\ell, \ell' \in S_2} \mathbb{Q}(\sqrt{\ell\ell'}).$$

▷ Suppose that 2 is unramified in k, then

$$k^{(*)} = \prod_{\ell \in S_1} \mathbb{Q}(\sqrt{\ell}) \prod_{\ell, \ell' \in S_2} \mathbb{Q}(\sqrt{\ell\ell'}).$$

We conclude that in all the cases, if $\mathrm{card}(S_2)$ is even, then $k^{(*)}$ contains $\mathbb{Q}\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ and if $\mathrm{card}(S_2)$ is odd, then $k^{(*)}$ contains $\mathbb{Q}\Big(\sqrt{q \prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ where q is any element in S_2.

We note that for every prime number p which is unramified in k, the residual degree of p in k is equal to 1 or 2. This follows from the fact that $k/\mathbb{Q}$ is an elementary extension and the decomposition group of p in k is cyclic of order the residual degree of p in k. Thus, we have the following lemma:

Lemma 2.5. *Let k be a biquadratic number field, d a square free positive integer and $K = k(\sqrt{d})$. Let $\ell_1, \ell_2, \ldots, \ell_n$ be distinct primes dividing d and not ramified in k. Denote by r the number of primes ℓ_i totally decomposed in k. Suppose that if 2 is ramified in k, then d is odd. We have:*

(i) *If $d \not\equiv -1 \pmod 4$, then $\mathrm{ram}(k(\sqrt{d})/k) = 2^2 r + 2(n-r)$.*

(ii) *If $d \equiv -1 \pmod 4$, then $\mathrm{ram}(k(\sqrt{d})/k) = 2^2 r + 2(n-r) + a$, where $a \in \{0, 1, 2, 4\}$ is the number of 2-adic places of k ramified in K and we have:*

$$\begin{aligned} a = 4 &\Longleftrightarrow e(2) = f(2) = 1, \\ a = 0 &\Longleftrightarrow e(2) = 4 \text{ or } e(2) = 2 \text{ and } \forall m \in \mathbb{N}^*,\ \sqrt{2m} \notin k, \\ a = 1 &\Longleftrightarrow e(2) = 2,\ f(2) = 2 \text{ and } \exists m \in \mathbb{N}^*,\ \sqrt{2m} \in k, \end{aligned}$$

where $e(2)$ and $f(2)$ are respectively the ramification index and the residual degree of 2 in k.

P r o o f. From the discussion above, a prime which is not ramified in k is totally decomposed in k or is decomposed into $1/2[k\colon \mathbb{Q}]$ primes in k. Moreover, in the case where $d \not\equiv -1 \pmod 4$, the number $\operatorname{ram}(k(\sqrt{d})/k)$ is equal to $2^2 r + 2(n-r)$. In the case where $d \equiv -1 \pmod 4$, we know that the ramification index of 2 in each multiquadratic number field is 1, 2 or 4. Precisely, the ramification index of 2 in a multiquadratic number field is equal to 4, if it contains a biquadratic number field of the form $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where d_1 is even and $d_2 \equiv -1 \pmod 4$. Consequently, we can conclude immediately (ii) of the lemma. □

On the units of some biquadratic number field: Let q_1, q_2 and q_3 be distinct prime numbers such that $q_1 \equiv q_2 \equiv q_3 \equiv -1 \pmod 4$ and $k = \mathbb{Q}(\sqrt{q_1 q_2}, \sqrt{q_1 q_3})$. In this case we refer to the results of Kuroda [6] on the fundamental system of units of biquadratic number fields. For every positive integer m, denote by ε_m the fundamental unit of the quadratic number field $\mathbb{Q}(\sqrt{m})$, then

$$\left\{\varepsilon_{q_1 q_2}, \sqrt{\varepsilon_{q_1 q_2}\varepsilon_{q_1 q_3}}, \sqrt{\varepsilon_{q_1 q_2}\varepsilon_{q_2 q_3}}\right\}$$

is a fundamental system of units of k.

We will use this system to prove the main result of this article.

On the Kronecker symbols:

Lemma 2.6. *Let m_1, m_2, m_3, m_4 be distinct positive integers and ℓ a prime number. Then one of the following two situations holds:*

(1) *There exist distinct $i, j, k \in \{1,2,3,4\}$ such that $(m_i m_j/\ell) = (m_i m_k/\ell) = 1$.*
(2) *There exist distinct $i, j \in \{1,2,3,4\}$ such that $(m_i/\ell) = (m_j/\ell) = 1$.*

P r o o f. Assume there exist distinct $i, j, k \in \{1,2,3,4\}$ such that $(m_i/\ell) = (m_j/\ell) = (m_k/\ell)$, then by quadratic reciprocity law, the first situation of the lemma holds.

If not, we find that there exist distinct $i, j, k, l \in \{1,2,3,4\}$ such that $(m_i/\ell) = (m_j/\ell) = 1$ and $(m_k/\ell) = (m_l/\ell) = -1$. It follows immediately that the second situation of the lemma is satisfied. □

Lemma 2.7. *Let $\ell_1, \ell_2, \ldots, \ell_5$ be distinct prime numbers. Then for every prime ℓ distinct from ℓ_i, $i \in \{1,2,\ldots,5\}$, there exist $i, j, k \in \{1,2,\ldots,5\}$ such that $(\ell_i \ell_j/\ell) = (\ell_i \ell_k/\ell) = 1$.*

P r o o f. It is easy to see that there exist $i, j, k \in \{1,2,\ldots,5\}$ such that $(\ell_i/\ell) = (\ell_j/\ell) = (\ell_k/\ell)$. Thus, by the quadratic reciprocity law, we obtain the result. □

3. Proof of Theorem 2

We let the notations be the same as in Section 2:

Notations:

k:	a real multiquadratic number field in which eight primes ramify
$k^{(*)}$:	the genus field of k
p_i:	prime numbers $\equiv 1 \pmod 4$
q_i:	prime numbers $\equiv -1 \pmod 4$
S_1:	$= \{p$ prime ramified in $k \mid p \equiv 1 \pmod 4\}$
S_2:	$= \{q$ prime ramified in $k \mid q \equiv -1 \pmod 4\}$
M/L:	an extension of a number field
E_M (E_L):	the unit group of M (of L, respectively)
$2^{e(M/L)}$:	$= [E_L\colon\, E_L \cap N_{M/L}(M^{(*)})]$

Remarks.

▷ It is clear that $\mathrm{card}(S_1 \cup S_2)$ is equal to seven or eight, this is related to the ramification of 2 in k.

▷ Suppose that $\mathrm{card}(S_2) \leqslant 1$, then $k^{(*)}$ contains the quadratic field $K = \mathbb{Q}\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ (see Section 2.3). Since the rank of the 2-class group of K is grater then or equels to 6, then the Hilbert 2-class field tower of K is infinite (Golod and Shafarevich), therefore as well the Hilbert 2-class field tower of $k^{(*)}$ is infinite. Consequently, using the fact that $k^{(*)}/k$ is unramified, we have the Hilbert 2-class field tower of k is infinite.

We began by obtaining some results on the tower of a real quadratic number field in which the rank of the 2-class group is grater then or equels to 5.

Proposition 3.1. *Let F be a real quadratic number field in which seven primes ramify. Suppose that there are at least five primes are not equivalent to* $-1 \pmod 4$ *ramifying in F, then the Hilbert 2-class field tower of F is infinite.*

Proof. Denote $p_1, p_2, \ldots, p_5$ the primes are not equivalent to $-1 \pmod 4$ ramified in $F = \mathbb{Q}(\sqrt{d})$ where d is a square free positive integer.

Assume $(p_i/p_j) = -1$, for all $i, j \in \{1, 2, \ldots, 5\}$ and $i \neq j$. Put $K = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_2p_3})$ and $K' = K(\sqrt{d})$. We remark that $(p_1p_2/p_k) = (p_2p_3/p_k)$, for all $k \in \{4, 5\}$. Moreover, by Lemma 2.5, we see that $\mathrm{ram}(K'/K) \geqslant 12$. In the case where $\mathrm{ram}(K'/K) > 12$, we have by Section 2.2, $\mathrm{rank}(C_{2,K'}) \geqslant \mathrm{ram}(K'/K) - e(K'/K) - 1 \geqslant 8$. We therefore can conclude by Remarks 2.2, that the Hilbert 2-class field tower of K' is infinite.

In the case where $\mathrm{ram}(K'/K) = 12$, we have every odd prime equivalent to $-1 \pmod 4$ dividing d, is not totally decomposed in K and also 2 is not totally decomposed in K. We can apply Lemma 2.3 to see that -1 is a norm in the extension M/L. Therefore, $e(K'/K) \leqslant 3$ and by Section 2.2 $\mathrm{rank}(C_{2,K'}) \geqslant \mathrm{ram}(K'/K) - e(K'/K) - 1 \geqslant 8$. Which guarantees the infiniteness of the Hilbert 2-class field tower of K'.

Now suppose that there exist $i, j \in \{1, 2, \ldots, 5\}$ such that $(p_i/p_j) = 1$, we note $(p_1/p_2) = 1$. If there exists $i \in \{3, 4, 5\}$ such that $(p_1/p_i) = 1$ or $(p_2/p_i) = 1$, we put respectively $K = \mathbb{Q}(\sqrt{p_2}, \sqrt{p_i})$ or $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_i})$ and $K' = K(\sqrt{d})$, we see then that $\mathrm{ram}(K'/K) \geqslant 12$. Proceeding in a similar way to the preceding case, we find that the Hilbert 2-class field tower of K' is infinite. In the next, suppose that for all $i \in \{3, 4, 5\}$, $(p_1/p_i) = (p_2/p_i) = -1$. We put $K = \mathbb{Q}(\sqrt{p_3p_4}, \sqrt{p_3p_5})$ and $K' = K(\sqrt{d})$. Then we see that $(p_3p_4/p_i) = (p_3p_5/p_i) = 1$ for all $i = 1, 2$, and $\mathrm{ram}(K'/K) \geqslant 12$. We obtain as well that the Hilbert 2-class field tower of K' is infinite.

Consequently, in all the cases, we constructed unramified extensions of F in which the Hilbert 2-class field tower is infinite. The proposition is thus proved. □

P r o o f of Theorem 2. The idea used to prove that k has infinite Hilbert 2-class field tower is to determine a subfield of $k^{(*)}$ in which the Hilbert 2-class field tower is infinite. This guarantees, the infiniteness of the Hilbert 2-class field tower of $k^{(*)}$ and using the fact that $k^{(*)}/k$ is unramified, we obtain the result.

We shall give a proof by distinguishing four cases, depending on the number of elements of S_2. For the case where $\mathrm{card}(S_2) \leqslant 1$, see the remarks in Section 3.

Case 1: Suppose $\mathrm{card}(S_2) = 2$

It is clear that $\mathrm{card}(S_1) \geqslant 5$. By Section 2.3, $k^{(*)}$ contains the real quadratic field $K = \mathbb{Q}\Bigl(\sqrt{\prod\limits_{\ell \in S_1 \cup S_2} \ell}\Bigr)$. Then from Proposition 3.1, the Hilbert 2-class field tower of K is infinite.

Case 2: Suppose $\mathrm{card}(S_2) = 3$

In this case, we have $\mathrm{card}(S_1) \geqslant 4$, we distinguish between the cases where 2 is ramified or not in k.

Assume 2 is unramified in k, then we have $\mathrm{card}(S_1) = 5$. It follows that $k^{(*)}$ contains the quadratic field $K = \mathbb{Q}\Bigl(\sqrt{q_1 q_2 \prod\limits_{\ell \in S_1} \ell}\Bigr)$ where q_1 and q_2 are two distinct primes in S_2 (Section 2.3). By applying Proposition 3.1, the Hilbert 2-class field tower of K is infinite.

Now, assume 2 is ramified, then by Section 2.3, three possible situations can happen:

(i) $\sqrt{2} \in k^{(*)}$, then $k^{(*)}$ contains $K = \mathbb{Q}\Big(\sqrt{2q_1q_2 \prod_{\ell \in S_1 2} \ell}\Big)$ where q_1 and q_2 are two distinct primes of S_2.

(ii) There exists $q \in S_2$ such that $\sqrt{2q} \in k^{(*)}$, then $k^{(*)}$ contains $K = \mathbb{Q}\Big(\sqrt{2 \prod_{\ell \in S_1 \cup S_2} \ell}\Big)$.

(iii) $\sqrt{2} \notin k^{(*)}$ and for all $q \in S_2$, we have $\sqrt{2q} \notin k^{(*)}$, then the quadratic field $K = \mathbb{Q}\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ is contained in $k^{(*)}$.

In the cases (i) and (ii), from Proposition 3.1, K has infinite Hilbert 2-class field tower.

In the case (iii), there are eight primes ramified in K, thus K has infinite Hilbert 2-class field tower.

Case 3: Suppose $\text{card}(S_2) = 4$

We have that the quadratic number field $K = \mathbb{Q}\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ is contained in $k^{(*)}$. In the case where 2 is unramified, we have $\text{card}(S_1 \cup S_2) = 8$, thus the Hilbert 2-class field tower of K is infinite.

Suppose that 2 is ramified in k, then we distinguish between two cases:

▷ For every positive integer m, $\sqrt{2m} \notin k$, then by Lemma 2.6, for some prime $p \in S_1$, we have:

$$\left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = 1 \quad \text{for some } q_1, q_2 \in S_2,$$

or

$$\left(\frac{q_1q_2}{p}\right) = \left(\frac{q_1q_3}{p}\right) = 1 \quad \text{for some } q_1, q_2, q_3 \in S_2.$$

Accordingly to the preceding equations, we put $K = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2})$ or $K = \mathbb{Q}(\sqrt{q_1q_2}, \sqrt{q_1q_3})$ and $K' = K\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ which is contained in $k^{(*)}$ (Section 2.3). We see by Lemma 2.5 that $\text{ram}(K'/K) \geqslant 12$. In the case where $\text{ram}(K'/K) > 12$, we have $\text{rank}(C_{2,K'}) \geqslant \text{ram}(K'/K) - e(K'/K) - 1 \geqslant 8$ (since $e(K'/K) \leqslant 4$). Thus K' satisfies the Golod and Shafarevich inequality (Remarks 2.2), therefore the Hilbert 2-class field tower of K' is infinite. Thus, the Hilbert 2-class field tower of $k^{(*)}$ is infinite too.

Now, suppose $\text{ram}(K'/K) = 12$, then p is the unique prime ramified in K' which is totally decomposed in K. Moreover by Lemma 2.3, -1 is a norm in the extension K'/K, thus $e(K'/K) \leqslant 3$. Consequently, $\text{rank}(C_{2,K'}) \geqslant \text{ram}(K'/K) - e(K'/K) - 1 \geqslant 8$ and the Hilbert 2-class field tower of K' is infinite.

▷ There exist a positive integer m such that $\sqrt{2m} \in k$. In the case where $\sqrt{2} \in k$, then the quadratic number field $\mathbb{Q}\Big(\sqrt{2 \prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ is contained in $k^{(*)}$ and has an infinite Hilbert 2-class field tower.

In the case where $\sqrt{2} \notin k$, then for each prime $q \in S_2$, $\sqrt{2q} \in k$. By Lemma 2.6, for some prime $p \in S_1$, we have:

$$\left(\frac{2q_1}{p}\right) = \left(\frac{2q_2}{p}\right) = 1 \quad \text{for some } q_1, q_2 \in S_2,$$

or

$$\left(\frac{q_1 q_2}{p}\right) = \left(\frac{q_1 q_3}{p}\right) = 1 \quad \text{for some } q_1, q_2, q_3 \in S_2.$$

Then accordingly to the preceding equations, we put $K = \mathbb{Q}(\sqrt{2q_1}, \sqrt{2q_2})$ or $K = \mathbb{Q}(\sqrt{q_1 q_2}, \sqrt{q_1 q_3})$ and $K' = K\Big(\sqrt{\prod_{\ell \in S_1 \cup S_2} \ell}\Big)$ which is contained in $k^{(*)}$ (Section 2.3). Proceeding in a similar way as in the preceding cases, we obtain that the Hilbert 2-class field tower of K' is infinite.

Case 4: Suppose $\operatorname{card}(S_2) \geqslant 5$

By Lemma 2.7, for some prime number $\ell \in S_1 \cup S_2$, there exist distinct prime numbers $q_1, q_2, q_3 \in S_2$ such that

$$\left(\frac{q_1 q_2}{\ell}\right) = \left(\frac{q_1 q_3}{\ell}\right) = 1.$$

Denote $K = \mathbb{Q}(\sqrt{q_1 q_2}, \sqrt{q_1 q_3})$ and

$$K' = K(\sqrt{d}) \text{ such that } d = \begin{cases} \prod_{\ell \in S_1 \cup S_2} \ell & \text{if } \operatorname{card}(S_2) \text{ is even,} \\ q_1 \prod_{\ell \in S_1 \cup S_2} \ell & \text{if } \operatorname{card}(S_2) \text{ is odd.} \end{cases}$$

It is clear by Section 2.3, that K' is contained $k^{(*)}$.

We have

$$\operatorname{rank}(C_{2,K'}) \geqslant \operatorname{ram}(K'/K) - e(K'/K) - 1,$$

where $0 \leqslant e(K'/K) \leqslant 4$.

With the equalities $(q_1 q_2/\ell) = (q_1 q_3/\ell) = 1$, it is easy to see by Lemma 2.5 that $\operatorname{ram}(K'/K) \geqslant 12$.

In the case where $\operatorname{ram}(K'/K) > 12$, proceeding in a similar way as in the preceding cases, we obtain that the Hilbert 2-class field tower of K' is infinite.

Suppose now that $\operatorname{ram}(K'/K) = 12$, then it suffices to prove that $e(K'/K) < 4$. By Lemma 2.3, -1 is a norm in the extension K'/K if and only if $\ell \in S_1$. Therefore, if $\ell \in S_1$, then $e(K'/K) \leqslant 3$, and proceeding in a similar way as Case 3, we see that the Hilbert 2-class field tower of K' is infinite.

In the next, we suppose that $\ell \in S_2$, then we can proceed differently to the preceding cases.

By Section 2.2, $\{\varepsilon_{q_1q_2}, (\varepsilon_{q_1q_2}\varepsilon_{q_1q_3})^{1/2}, (\varepsilon_{q_1q_2}\varepsilon_{q_2q_3})^{1/2}\}$ is a fundamental system of units of K. Then finding the inequality $e(K'/K) < 4$ is reduced to determining a unit $u \neq 1$ of the form $u = \pm\varepsilon_{q_1q_2}^i(\varepsilon_{q_1q_2}\varepsilon_{q_1q_3})^{j/2}(\varepsilon_{q_1q_2}\varepsilon_{q_2q_3})^{k/2}$, where $i, j, k \in \{0, 1\}$ such that u is a norm in the extension K'/K.

Let $\mathcal{P}$ be a prime in K ramified in the extension K'/K. It is clear that $\mathcal{P}$ lies above some prime l where l divides d. Denote by L the decomposition field of l in the extension $K/\mathbb{Q}$. *Suppose* $l \neq \ell$, then by norm residue symbol propreties, we have:

$$\Big(\frac{-1, d}{\mathcal{P}}\Big) = \Big(\frac{N_{K/L}(-1), d}{N_{K/L}(\mathcal{P})}\Big) = 1. \tag{3.1}$$

In addition, we have

$$\Big(\frac{\varepsilon_{q_1q_2}, d}{\mathcal{P}}\Big) = \Big(\frac{N_{k/L}(\varepsilon_{q_1q_2}), d}{N_{K/L}(\mathcal{P})}\Big).$$

Otherwise, it is easy to see that

$$N_{K/L}(\varepsilon_{q_1q_2}) = \begin{cases} 1 & \text{if } \ \varepsilon_{q_1q_2} \notin L, \\ \varepsilon_{q_1q_2}^2 & \text{if } \ \varepsilon_{q_1q_2} \in L. \end{cases}$$

Thus, we have

$$\Big(\frac{\varepsilon_{q_1q_2}, d}{\mathcal{P}}\Big) = 1. \tag{3.2}$$

Suppose $l = \ell$, since ℓ is totally decomposed in the extension K and $l \in S_2$, then

$$\Big(\frac{-1, d}{\mathcal{P}}\Big) = \Big(\frac{-1, \ell}{\ell}\Big) = \Big(\frac{-1}{\ell}\Big) = -1. \tag{3.3}$$

We shall prove that the value of $((\varepsilon_{q_1q_2}, d)/\mathcal{P})$ is independent of the choice of primes $\mathcal{P}$ lying above ℓ.

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two distinct primes in K lying above ℓ. By the transitivity of $\mathrm{Gal}(K/\mathbb{Q})$, there exists an isomorphisme σ of $\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathcal{P}_1) = \mathcal{P}_2$. Denote $M = \mathrm{Inv}(\sigma)$, then we have

$$\Big(\frac{\varepsilon_{q_1q_2}, d}{\mathcal{P}_1}\Big)\Big(\frac{\varepsilon_{q_1q_2}, d}{\mathcal{P}_2}\Big) = \Big(\frac{N_{K/M}(\varepsilon_{q_1q_2}), d}{N_{K'/K}(\mathcal{P}_1)}\Big) = 1. \tag{3.4}$$

The last equality proves that the value of $((\varepsilon_{q_1q_2}, d)/\mathcal{P})$ is independent of the choice of primes $\mathcal{P}$ lying above ℓ.

Consequently, using the equalities (3.1), (3.2), (3.3) and (3.4), we deduce that $\varepsilon_{q_1q_2}$ or $-\varepsilon_{q_1q_2}$ is a norm in the extension K'/K, moreover $e(K'/K) < 4$ and the Hilbert 2-class field tower of K' is infinite, finishing the proof of our theorem. □

Acknowledgement. The authors are grateful to the anonymous referee for his/her careful reading of the manuscript and helpful comments.

References

[1] *F. Gerth* III.: Some real quadratic fields with infinite Hilbert 2-class field towers. Jap. J. Math., New Ser. *31* (2005), 175–181.
[2] *E. S. Golod, I. R. Shafarevich*: On the class field tower. Izv. Akad. Nauk SSSR, Ser. Mat. *28* (1964), 261–272 (In Russian.); English translation in Transl., Ser. 2, Am. Math. Soc. *48* (1965), 91–102.
[3] *H. Hasse*: Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols. J. f. M. *162* (1930), 134–144. (In German.)
[4] *M. Ishida*: The Genus Fields of Algebraic Number Fields. Lecture Notes in Mathematics 555. Springer, Berlin, 1976.
[5] *W. Jehne*: On knots in algebraic number theory. J. Reine Angew. Math. *311–312* (1979), 215–254.
[6] *S. Kuroda*: Über den Dirichletschen Körper. J. Fac. Sci. Univ. Tokyo, Sect. I *4* (1943), 383–406. (In German.)
[7] *L. V. Kuz'min*: Homologies of profinite groups, the Schur multiplicator and class field theory. Izv. Akad. Nauk. SSSR Ser. Mat. *33* (1969), 1220–1254. (In Russian.)
[8] *C. Maire*: A refinement of the Golod-Shafarevich theorem. (Un raffinement du théorème de Golod-Šafarevič). Nagoya Math. J. *150* (1998), 1–11. (In French.)
[9] *A. Mouhib*: On the Hilbert 2-class field tower of real quadratic fields. (Sur la tour des 2-corps de classes de Hilbert des corps quadratiques réels). Ann. Sci. Math. Qué. *28* (2004), 179–187. (In French.)

Authors' addresses: Abdelmalek Azizi, Department of Mathematics, Faculty of Sciences, Mohammed I University, Oujda, Morocco, e-mail: `abdelmalekazizi@yahoo.fr`; Ali 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: `mouhibali@yahoo.fr`.