ACTA ARITHMETICA
145.3 (2010)

Infinite Hilbert 2-class field tower of quadratic number fields

by

A. Mouhib (Taza)

1. Introduction. Let k be a number field. We will denote the ideal class group of k in the wide sense by C_k. Let k^1 be the Hilbert 2-class field of k (i.e., the maximal abelian unramified 2-extension of k), and for $n \geq 2$, let k^n be the Hilbert 2-class field of k^{n-1}. Then

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

is the Hilbert 2-class field tower of k. We say that the tower is *finite* if $k^n = k^{n+1}$ for some n, and *infinite* otherwise.

We define the 2-*rank* of C_k as the dimension of the elementary abelian 2-group C_k/C_k^2 viewed as a vector space over $\mathbb{F}_2$:

$$\mathrm{rank}_2(C_k) = \dim_{\mathbb{F}_2}(C_k/C_k^2),$$

where $\mathbb{F}_2$ is the finite field with two elements. We define the 4-*rank* of C_k by

$$\mathrm{rank}_4(C_k) = \mathrm{rank}_2(C_k^2) = \dim_{\mathbb{F}_2}(C_k^2/C_k^4).$$

Assume k is an imaginary quadratic number field. It is well known that if $\mathrm{rank}_2(C_k) \geq 5$, then the Hilbert 2-class field tower of k is infinite [5]. In the case where $\mathrm{rank}_2(C_k) = 2$ or 3, the Hilbert 2-class field tower of k may be finite ([9], [10]), and if $\mathrm{rank}_2(C_k) = 1$ then the Hilbert 2-class field tower of k is finite of length 1. It has been conjectured that if $\mathrm{rank}_2(C_k) = 4$, then k has infinite Hilbert 2-class field tower [10]. We mention that Hajir proved that if C_k contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then k has infinite Hilbert 2-class field tower ([6], [7]).

Now suppose that $\mathrm{rank}_2(C_k) = 4$ and the discriminant of k is divisible by exactly one negative prime discriminant. In [2], under some conditions on the 4-rank of C_k and the Kronecker symbols of the primes dividing the discriminant of k, the author proves that k has infinite Hilbert 2-class field tower. Y. Sueyoshi proves the same result under some conditions on the Rédei matrix [14].

2010 *Mathematics Subject Classification*: 11R29, 11R32, 11R37.
Key words and phrases: class group, class field tower, multiquadratic number fields.

DOI: 10.4064/aa145-3-4

In Section 3 of this article, we investigate Martinet's question and the above conjecture by generalizing the preceding results. We prove the following theorem:

THEOREM. *Let k be an imaginary quadratic number field whose discriminant is divisible by at most one negative prime discriminant and* $\mathrm{rank}_2(C_k) = 4$*. Then the Hilbert 2-class field tower of k is infinite.*

Also, in Section 3, we show that a positive proportion of imaginary quadratic number fields with the class group of 2-rank equal to 2 and 4-rank equal to 1 have infinite Hilbert 2-class field towers.

2. Known results

2.1. Golod and Shafarevich inequality. Let k be a number field, C_k be the class group of k and E_k be the group of units of k. Then, from [3, p. 233], we know that the Hilbert 2-class field tower of k is infinite if

$$(*) \qquad \mathrm{rank}_2(C_k) \geq 2 + 2\sqrt{\mathrm{rank}_2(E_k) + 1},$$

where $\mathrm{rank}_2(E_k)$ is exactly the number of infinite primes of k.

REMARKS. If k is an imaginary quadratic number field, then $\mathrm{rank}_2(E_k) = 1$. Suppose $\mathrm{rank}_2(C_k) \geq 5$. Then the inequality $(*)$ is satisfied and k has infinite Hilbert 2-class field tower.

If k is an imaginary biquadratic number field, then $\mathrm{rank}_2(E_k) = 2$. Suppose $\mathrm{rank}_2(C_k) \geq 6$. Then the inequality $(*)$ is satisfied and k has infinite Hilbert 2-class field tower.

If k is an imaginary triquadratic number field, then $\mathrm{rank}_2(E_k) = 4$, and the inequality $(*)$ is satisfied whenever $\mathrm{rank}_2(C_k) \geq 7$.

2.2. Genus theory. Let K be a quadratic extension of a number field k. By classical results of genus theory [8], we have

$$\mathrm{rank}_2(C_K) \geq \mathrm{ram}(K/k) - \dim_{\mathbb{F}_2}(E_k/E_k \cap N_{K/k}(K^*)) - 1,$$

where $\mathrm{ram}(K/k)$ is the number of primes that ramify in the extension K/k, and $N_{K/k}$ is the norm map in the extension K/k. In the case where the class number of k is odd, the preceding inequality becomes an equality (see for instance [1]).

We note that

$$\dim_{\mathbb{F}_2}(E_k/E_k \cap N_{K/k}(K^*)) \leq \begin{cases} [k:\mathbb{Q}] & \text{if } k \text{ totally real,} \\ \frac{1}{2}[k:\mathbb{Q}] & \text{if not.} \end{cases}$$

Now let k be a quadratic number field of discriminant d, and t be the number of primes that ramify in k. By genus theory, we have

$$\mathrm{rank}_2(C_k) = \begin{cases} t-2 & \text{if } d \text{ is positive and not a sum of two squares,} \\ t-1 & \text{otherwise.} \end{cases}$$

3. Main results

3.1. Proof of the Theorem. We let the notations be as in Section 2. In this section we investigate Martinet's conjecture, we give a proof of the Theorem and we show that a positive proportion of some imaginary quadratic number fields have infinite Hilbert 2-class field tower. We begin with the following two lemmas.

LEMMA 3.1. *Let p_1, p_2, p_3 and p_4 be distinct prime numbers* $\not\equiv -1 \pmod 4$ *and* $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$. *Then* $\mathrm{rank}_2(C_K) \geq 2$.

Proof. See [11, Theorem 5.3]. ∎

LEMMA 3.2. *Let p be a prime number and L/K be a Galois extension of algebraic number fields whose Galois group G is an elementary p-group. Then for each place $\mathcal{P}$ of K unramified in L, the number of $\mathcal{P}$-places of L is equal to $[L : K]$ or $(1/p)[L : K]$.*

Proof. We know that if $\mathcal{P}$ is unramified in the extension L/K, then the decomposition group of $\mathcal{P}$ is a cyclic subgroup of G. Since G is an elementary p-group, the decomposition group of $\mathcal{P}$ is of order 1 or p, proving the lemma. ∎

Proof of the Theorem. By hypotheses, we have $\mathrm{rank}_2(C_k) = 4$ and the discriminant d of k is divisible by at most one prime $\equiv -1 \pmod 4$. So, denote by p_1, p_2, p_3, p_4 and p distinct prime numbers dividing d such that $p_i \not\equiv -1 \pmod 4$, $1 \leq i \leq 4$ and $p = 2$ or $p \equiv -1 \pmod 4$. We put $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$ and let M be the decomposition field of p in K. From Lemma 3.2, $M = K$ or K/M is a quadratic extension. Let F be the composite field of M and k which is a totally complex quadratic extension of the totally real field M.

Suppose that $M = K$. Then the extension F/M is ramified at all archimedean places and p-adic places of M, so $\mathrm{ram}(F/M) = 2[M : \mathbb{Q}] = 32$. We have $\dim_{\mathbb{F}_2}(E_M/E_M \cap N_{F/M}(F^*)) \leq [M : \mathbb{Q}]$ and $\mathrm{rank}_2(E_F) = [M : \mathbb{Q}] = 16$. Hence one can readily verify that

$$\mathrm{ram}(F/M) - \dim_{\mathbb{F}_2}(E_M/E_M \cap N_{F/M}(F^*)) - 1 \geq 2 + 2\sqrt{\mathrm{rank}_2(E_F) + 1}.$$

By Section 2.2, we have

$$\mathrm{rank}_2(C_F) \geq \mathrm{ram}(F/M) - \dim_{\mathbb{F}_2}(E_M/E_M \cap N_{F/M}(F^*)) - 1,$$

so the extension F/M satisfies the inequality $(*)$ of Section 2.1, and consequently F has infinite Hilbert 2-class field tower. Therefore, since F/k is unramified, k has infinite Hilbert 2-class field tower.

Suppose that K/M is a quadratic extension. In the case where K/M is ramified, there exists a unique $i \in \{1, 2, 3, 4\}$ such that the p_i-adic places of M are ramified in K. So the extension F/M is ramified at all archimedian places, p-adic places and p_i-adic places of M. Moreover, we have $\mathrm{ram}(F/M) = 3[M:\mathbb{Q}] = 24$ or $\mathrm{ram}(F/M) = 2[M:\mathbb{Q}] + \frac{1}{2}[M:\mathbb{Q}] = 20$ respectively if p_i is totally decomposed in M or not. Therefore, as in the preceding case, we show that the Hilbert 2-class tower of k is infinite. It remains to study the case where K/M is an unramified quadratic extension.

Suppose that K/M is unramified. By Lemma 3.1 we have $\mathrm{rank}_2(C_K) \geq 2$, so the 2-part of the class group of M can never be trivial or cyclic. This implies that $\mathrm{rank}_2(C_M) \geq 2$. Let $\tilde{M}$ be the maximal elementary unramified extension of M. One can verify that $\tilde{M}$ is normal over $\mathbb{Q}$. Denote by F the composite field of $\tilde{M}$ and k which is a totally complex quadratic extension of the totally real field $\tilde{M}$. The extension $F/\tilde{M}$ is ramified at all archimedian places and p-adic places of $\tilde{M}$. By Lemma 3.2, each p-adic place of M is totally decomposed or decomposed into $\frac{1}{2}[\tilde{M}:M]$ places in $\tilde{M}$, so $\mathrm{ram}(F/\tilde{M}) \geq [\tilde{M}:\mathbb{Q}] + \frac{1}{2}[\tilde{M}:\mathbb{Q}]$. On the other hand since $\mathrm{rank}_2(E_F) = [\tilde{M}:\mathbb{Q}]$ and $[\tilde{M}:\mathbb{Q}] \geq 32$, one can obtain

$$\mathrm{ram}(F/\tilde{M}) - \dim_{\mathbb{F}_2}(E_{\tilde{M}}/E_{\tilde{M}} \cap N_{F/\tilde{M}}(F^*)) - 1 \geq 2 + 2\sqrt{\mathrm{rank}_2(E_F) + 1},$$

hence the extension F satisfies the inequality $(*)$, and consequently F has infinite Hilbert 2-class field tower. The fact that F/k is unramified implies that k has infinite Hilbert 2-class field tower. ∎

3.2. The positive proportion of imaginary quadratic number fields k with 2-rank of C_k equal to 2. It is well known that every number field whose 2-part of its class group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has finite Hilbert 2-class field tower that terminates in at most two steps [9].

In [10], J. Martinet asked the following question: is there any imaginary quadratic number field with 2-class group of rank 2 and infinite Hilbert 2-class field tower?

Schmithals showed that the quadratic number field $k = \mathbb{Q}(\sqrt{-25355})$ with $\mathrm{rank}_2(C_k) = 2$ has infinite Hilbert 2-class field tower [13].

In the following proposition we show that a positive proportion of imaginary quadratic number fields with 2-rank of its class group equal to 2 and its 4-rank equal to 1 have infinite Hilbert 2-class field towers.

PROPOSITION 3.3. *Let p_1 and p_2 be distinct prime numbers such that the class number of $\mathbb{Q}(\sqrt{p_1p_2})$ is divisible by 16. Then for each prime number $p \equiv -1 \pmod 4$ such that $\left(\frac{p_1p_2}{p}\right) = -1$, the Hilbert 2-class field tower of $\mathbb{Q}(\sqrt{-p_1p_2p})$ is infinite.*

Proof. From genus theory, the 2-class group of $k = \mathbb{Q}(\sqrt{p_1p_2})$ is cyclique. Since by hypotheses, the class number of k is divisible by 4, we have $\left(\frac{p_1}{p_2}\right) = 1$ [12]. Moreover, $\left(\frac{p_1p_2}{p}\right) = -1$ and thus the Rédei matrix of

$\mathbb{Q}(\sqrt{-p_1p_2p})$ has rank 1, which implies that the 4-rank of the class group of $\mathbb{Q}(\sqrt{-p_1p_2p})$ is equal to 1 [4]. Now let k^1 be the Hilbert 2-class field of k and F be the composite field of k^1 and $\mathbb{Q}(\sqrt{-p})$ which is a totally complex quadratic extension of the totally real field k^1. It is clear that $F/\mathbb{Q}(\sqrt{-p_1p_2p})$ is unramified. Then proving the theorem is reduced to proving that F has infinite Hilbert 2-class field tower.

The prime number p is inert in the extension $k/\mathbb{Q}$, since $\left(\frac{p_1p_2}{p}\right) = -1$. Thus the p-adic place of k is principal. So by the reciprocity law applied in the extension k^1/k, the p-adic place of k is totally decomposed in k^1. Note that the number of p-adic places that ramify in F/k^1 is equal to $[k^1 : k]$. Thus $\mathrm{ram}(F/k^1) = 3[k^1 : k]$. From Section 2.2, we have

$$\mathrm{rank}_2(C_F) \geq \mathrm{ram}(F/k^1) - \dim_{\mathbb{F}_2}(E_{k^1}/E_{k^1} \cap N_{F/k^1}(F^*)) - 1$$

and since $\dim_{\mathbb{F}_2}(E_{k^1}/E_{k^1} \cap N_{F/k^1}(F^*)) \leq 2[k^1 : k]$, it follows that $\mathrm{rank}_2(C_F) \geq [k^1 : k] - 1 \geq 15$. On the other hand, since $\mathrm{rank}_2(E_F) = 2[k^1 : k]$ and one can verify that $[k^1 : k] - 1 \geq 2 + 2\sqrt{2[k^1 : k] + 1}$, by the inequality $(*)$ of Section 2.1 we deduce that the Hilbert 2-class field tower of F is infinite. Hence $\mathbb{Q}(\sqrt{-p_1p_2p})$ has infinite Hilbert 2-class field tower. ∎

By the distribution of prime numbers in an arithmetic progression, there exist infinitely many primes p satisfying the conditions of the preceding proposition. Thus the proposition shows that a positive proportion of the imaginary quadratic number fields with 2-rank of the class group equal to 2 and 4-rank equal to 1 have infinite Hilbert 2-class field towers.

From the following proposition we construct imaginary quadratic number fields k such that $\mathrm{rank}_2(C_k) = \mathrm{rank}_4(C_k) = 2$ and k has infinite Hilbert 2-class field tower.

Proposition 3.4. *Let d be a positive integer such that $d \not\equiv 1 \pmod 4$ and $k = \mathbb{Q}(\sqrt{d})$. Suppose that 8 divides the order of C_k. Then for every prime number $p \equiv -1 \pmod 4$ such that the equation $x^2 - dy^2 = p$ has a solution in $\mathbb{Z} \times \mathbb{Z}$, the imaginary quadratic number field $\mathbb{Q}(\sqrt{-pd})$ has infinite Hilbert 2-class field tower.*

Proof. The equation $x^2 - dy^2 = p$ having a solution in $\mathbb{Z} \times \mathbb{Z}$ implies that p is decomposed into two distinct primes $\mathcal{P}_1$ and $\mathcal{P}_2$ in k. We have $po_k = \mathcal{P}_1\mathcal{P}_2 = (a - b\sqrt{d})(a + b\sqrt{d})o_k$ where a and b are two positive integers and o_k the ring of integers of k. Then the places $\mathcal{P}_1$ and $\mathcal{P}_2$ are principal. Therefore, $\mathcal{P}_1$ and $\mathcal{P}_2$ are totally decomposed in the Hilbert 2-class field k^1 of k, so p is totally decomposed in k^1. The extension $k^1(\sqrt{-p})/k^1$ is ramified at the archimedian and the p-adic places of k^1, hence it is easy to see that $k^1(\sqrt{-p})$ satisfies the equality $(*)$, so the Hilbert 2-class field tower of $k^1(\sqrt{-p})$ is infinite. The fact that $k^1(\sqrt{-p})/\mathbb{Q}(\sqrt{-pd})$ is unramified proves the example. ∎

Let $d = 226$ and $p = 367$. The class number of $k = \mathbb{Q}(\sqrt{d})$ is equal to 8. Since $49^2 - 3^2 d = p$, from the preceding proposition $\mathbb{Q}(\sqrt{-pd})$ has infinite Hilbert 2-class field tower.

Let $d = 226$ and $p = 503$. The class number of $k = \mathbb{Q}(\sqrt{d})$ is equal to 8. Since $27^2 - d = p$, from the preceding proposition $\mathbb{Q}(\sqrt{-pd})$ has infinite Hilbert 2-class field tower.

References

[1] A. Azizi et A. Mouhib, *Sur le rang du 2-groupe de classes de* $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ *où* $m = 2$ *ou un premier* $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc. 353 (2001), 2741–2752.

[2] E. Benjamin, *On imaginary quadratic number fields with 2-class group of rank 4 and infinite 2-class field tower,* Pacific J. Math. 201 (2001), 257–266.

[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1986.

[4] F. Gerth, *The 4-class ranks of quadratic fields*, Invent. Math. 77 (1984), 489–515.

[5] E. S. Golod and I. R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261–272 (in Russian); English transl.: Amer. Math. Soc. Transl. 48 (1965), 91–102.

[6] F. Hajir, *On a theorem of Koch*, Pacific J. Math. 176 (1996), 15–18.

[7] —, *Correction to "On a theorem of Koch"*, ibid. 196 (2000), 507–508.

[8] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. 311/312 (1979), 215–254.

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

[10] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Invent. Math. 44 (1978), 65–73.

[11] A. Mouhib et A. Movahhedi, *Sur le 2-groupe de classes des corps multiquadratiques réels*, J. Théor. Nombres Bordeaux 17 (2005), 619–641.

[12] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.

[13] B. Schmithals, *Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm*, Arch. Math. (Basel) 34 (1980), 307–312.

[14] Y. Sueyoshi, *Infinite 2-class field towers of some imaginary quadratic number fields*, Acta Arith. 113 (2004), 251–257.

A. Mouhib
Laboratoire Informatique, Mathématique, Automatique et Optoélectronique
Faculté polydisciplinaire
Université Mohamed Ben Abdellah
B/P 1223, Taza-Gare, Maroc
E-mail: mouhibali@yahoo.fr.

Received on 5.10.2009
and in revised form on 21.4.2010 (6166)