

A positive proportion of some quadratic number fields with infinite Hilbert 2-class field tower

A. Mouhib¹

Received: 14 December 2014 / Accepted: 8 June 2015 © Springer Science+Business Media New York 2015

Abstract We show that a positive proportion of real and imaginary quadratic number fields with 2-class rank equal to 2 have 4-rank equal to 1 or 2 and infinite Hilbert 2-class field tower.

Keywords Class group · Class field tower · Quadratic number fields

Mathematics Subject Classification 11R29 · 11R32 · 11R37

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, i.e., 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 nonnegative 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.

Published online: 08 September 2015

Université Mohammed Ben Abdellah, Fes LSI, Sciences and Engineering Laboratory, Polydisciplinary Faculty of Taza, B.P 1223 Taza-Gare, Morocco



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

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

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

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

Assume that k is an imaginary quadratic number field. It is known that the Hilbert 2-class field tower of k is infinite if $r_2(k) \ge 5$ [1,5]. Also it is known that if $r_4(k) \ge 3$, then k has infinite Hilbert 2-class field tower [6,7]. In the case where $r_2(k) = 2$ or 3, the Hilbert 2-class field tower of k may be finite [9,13]. In the case where $r_2(k) = 4$, it has been conjectured that k has infinite Hilbert 2-class field tower [13]. This conjecture has been proved in the case where the discriminant of k is divisible by at most one prime k mod 4 [14]. Note that for each k (0, 1, 2, 3), there are infinitely many fields k such that

$$r_2(k) = 3$$
, $r_4(k) = i$

and infinite Hilbert 2-class field tower [2,3]. On other hand, it is known by group theory that if $r_2(k) = 2$ and $r_4(k) = 0$, then k has finite Hilbert 2-class field tower of length at most 2 [9]. Moreover, B. Schmithals showed that the quadratic number field $k = \mathbf{Q}(\sqrt{-25355})$ with $r_2(k) = 2$ has infinite Hilbert 2-class field tower [17] and it is shown that there exist infinitely many imaginary quadratic number fields k such that

$$r_2(k) = 2$$
, $r_4(k) = 1$

and infinite Hilbert 2-class field tower [14]. However, the case $r_2(k) = 2$ and $r_4(k) = 2$ is not treated any where.

Assume that k is a real quadratic number field. It is well known that if $r_2(k) \ge 6$, then the Hilbert 2-class field tower of k is infinite [5]. If $r_4(k) \ge 4$, then k has infinite Hilbert 2-class field tower [12]. Also a positive proportion of the fields k with $r_2(k) = 5$ for $0 \le r_4(k) \le 5$, $r_2(k) = 4$, for $0 \le r_4(k) \le 4$ and $r_4 = 3$ for $0 \le r_4(k) \le 3$ have infinite Hilbert 2-class field tower [2,4]. Moreover, there are infinitely many real quadratic number fields k such that

$$r_2(k) = 3, r_4(k) = 1$$

and finite Hilbert 2-class field tower [15]. However, it is not known that there is a positive proportion of real quadratic number fields k such that $r_2(k) = 2$ and $r_4(k) \in \{1, 2\}$ with infinite Hilbert 2-class field tower.

The aim of this article is to study the cases which are not treated in the literature, and then we prove the following theorem.



Theorem 1.1 For each $i \in \{1, 2\}$, there exist infinitely many imaginary (resp. real) quadratic number fields k such that $r_2(k) = 2$, $r_4(k) = i$ and infinite Hilbert 2-class field tower.

2 Preliminary results

2.1 Genus theory

Let p be a prime number and K/k be a Galois extension of number fields with degree p and Galois group G. Denote by E_k the unit group of k and 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 define the p-rank of C_K , denoted $r_p(K)$ as the dimension of the elementary abelian p-group C_K/C_K^p viewed as a vector space over \mathbb{F}_p . We note that B(K/k) is a vector space over \mathbb{F}_p , let $d_p(B(K/k))$ be its dimension.

By classical results of genus theory [8], we have

$$r_p(K) \ge ram(K/k) - dim_{\mathbb{F}_p}(B(K/k)) - 1;$$

where 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 p=2 and the class number of k is odd, the preceding inequality becomes an equality. Indeed, one can verify that the kernel of the homomorphism

$$f: C_K \longrightarrow C_K^2$$

$$C \longmapsto C^2$$

is exactly the invariant group $(C_K)^G$. Hence, we have

$$r_2(K) = dim_{\mathbb{F}_2}(C_K/C_K^2) = dim_{\mathbb{F}_2}((C_K)^G) = ram(K/k) - dim_{\mathbb{F}_2}(B(K/k)) - 1.$$

We note that

$$dim_{\mathbb{F}_2}(B(K/k)) \le \begin{cases} [k:\mathbf{Q}] & \text{if } k \text{ totally real,} \\ \frac{1}{2}[k:\mathbf{Q}] & \text{if not,} \end{cases}$$

2.2 4-Rank of the class group of quadratic number fields

Let *k* be a quadratic number field of discriminant *d*. We shall need the following results of Scholz, Rédei and Reichardt on the 2-class group of real quadratic number fields (see [16,18] and for more informations, see [11]).

A factorization of the discriminant d into relatively prime discriminants d_1 and d_2 : $d = d_1 \cdot d_2$ is called a C_4 -factorization if

(1)
$$d$$
 is not a sum of two squares and $\left(\frac{d_1}{p_2}\right) = \left(\frac{d_2}{p_1}\right) = 1$ for all primes $p_i|d_i$, or



(2)
$$d$$
 is a sum of two squares, $\left(\frac{d_1}{p_2}\right) = \left(\frac{d_2}{p_1}\right) = 1$ for all primes $p_i | d_i$ and $\left(\frac{d_1}{d_2}\right)_4 = \left(\frac{d_2}{d_1}\right)_4$.

Suppose we have a C_4 -factorization of d, and then there exists a cyclic extension over k of order 4 which is unramified outside ∞ . We have the following proposition:

Proposition 2.1 The 4-rank $r_4(k)$ of k equals the number of independent C_4 -factorizations of d.

2.3 Golod and Shafarevich inequality and Cebotarev density

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 [1], we know that the Hilbert 2-class field tower of k is infinite if

$$r_2(k) \ge 2 + 2\sqrt{r_2(E_k) + 1},$$
 (*)

where $r_2(E_k)$ is exactly the number of infinite primes of k.

We mention the following form of the Cebotarev density [10].

Proposition 2.2 Let K/k be a Galois extension with group G. Let $\sigma \in G$. Let [K:k] = N, and let c be the number of elements in the conjugacy class of σ in G. Then those primes P of k which are unramified in K and for which there exists $\mathcal{B}|P$ such that the Frobenius automorphism of \mathcal{B} in the extension K/k verifies

$$(\mathcal{B}, K/k) = \sigma$$

have a density, and this density is equal to $\frac{c}{N}$.

3 Proof of Theorem 1.1

To give the proof of Theorem 1.1, we distinguish between two cases:

Imaginary case: the case where $r_2(k)=2$ and $r_4(k)=1$ has been studied in [14]. Next, we construct infinitely many imaginary quadratic number fields k such that $r_2(k)=2$ and $r_4(k)=2$. Let p and p' be distinct prime numbers such that $p\equiv p'\equiv 1\pmod 4$ and $F=\mathbf{Q}(\sqrt{pp'})$. Denote by F^1 the Hilbert 2-class field of F and $h=[F^1:F]$. Suppose that h is divisible by 8. Introduce the number field $L=F^1(i)$, the compositum of F^1 and the imaginary quadratic number field $\mathbf{Q}(i)$. It is clear that L/\mathbf{Q} is a Galois extension of degree divisible by 4h. Let σ be the generator of the Galois group $Gal(L/F^1)$ of the extension L/F^1 , so σ fixes F^1 and transforms i to -i. Let S be the set of primes ℓ of \mathbf{Q} which are unramified in L and for which there exists $\mathcal{B}|\ell$ such that $(\mathcal{B},L/\mathbf{Q})=\sigma$. Hence by Proposition 2.2, S has a density equal to $\frac{c}{4h}$, where c is the number of elements in the conjugacy class of σ in $Gal(L/\mathbf{Q})$. Moreover, let \mathcal{B} be a prime ideal of L over a prime ℓ of S such that $(\mathcal{B},L/\mathbf{Q})=\sigma$, then for each prime \mathcal{L} of F^1 under \mathcal{B} , we have

$$(\mathcal{L}, F^1/\mathbf{Q}) = (\mathcal{B}, L/\mathbf{Q}) | F^1 = 1 \text{ (restriction of } \sigma \text{ to } F^1)$$



since σ acts trivially on F^1 . Hence all primes of S are totally decomposed in F^1 and inert in the extension M/F^1 . It is clear that for each prime ℓ of S, we have $\ell \equiv 3 \pmod{4}$, since ℓ is inert in $\mathbf{Q}(i)$. Also ℓ is decomposed in F, then $\binom{pp'}{\ell} = 1$ and we must have

$$\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p'}\right) = 1,$$

otherwise, we find $\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p'}\right) = -1$ and then the prime ideals of F above ℓ will be inert in $F(\sqrt{p})$ which is unramified over F, this is contrary to the fact that all primes of S are totally decomposed in F^1 . So, let $k = \mathbf{Q}(\sqrt{-pp'\ell})$, where $\ell \equiv 3 \pmod 4$ and $\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p'}\right) = 1$. It is clear by Genus theory that, $r_2(k) = 2$. Moreover, since h is divisible by 4, then by Proposition 2.1, $r_4(F) = 1$, and thus, $\left(\frac{p}{p'}\right) = 1$. It follows that we have two independant C_4 -factorizations of the discriminant of k; hence by Proposition 2.1, the 4-rank of the class group of k is equal to 2. It remains to prove that the Hilbert 2-class field tower of k is infinite. We have the extension $F^1(\sqrt{-\ell})/F^1$ is ramified at the archimedean and the ℓ -adic primes of F^1 . The number of infinite primes of F^1 is equal to $[F^1: \mathbf{Q}] = 2h$, and also since ℓ is totally decomposed in F^1 , the number of ℓ -adic primes of F^1 is equal to 2h, so $ram(F^1(\sqrt{-\ell})/F^1) = 4h$. On other hand, we have $dim(B(F^1(\sqrt{-\ell})/F^1)) \leq [F^1: \mathbf{Q}] = 2h$ and $r_2(E_{F^1(\sqrt{-\ell})}) = [F^1: \mathbf{Q}] = 2h$. Hence, since h is divisible by 8, one can readily verify that

$$ram(F^{1}(\sqrt{-\ell})/F^{1}) - dim_{\mathbb{F}_{2}}(B(F^{1}(\sqrt{-\ell})/F^{1}))) - 1 \ge 2 + 2\sqrt{r_{2}(E_{F^{1}(\sqrt{-\ell})}) + 1}.$$

By Sect. 2.1, we have

$$r_2(F^1(\sqrt{-\ell})) \ge ram(F^1(\sqrt{-\ell})/F^1) - dim_{\mathbb{F}_2}(B(F^1(\sqrt{-\ell})/F^1))) - 1,$$

so $F^1(\sqrt{-\ell})$ satisfies the inequality (*) of Sect. 2.3, and consequently $F^1(\sqrt{-\ell})$ has infinite Hilbert 2-class field tower. Therefore, since $F^1(\sqrt{-\ell})/k$ is an unramified 2-extension, k has infinite Hilbert 2-class field tower.

Real case: First we prove the Theorem for real quadratic number fields k with 2-rank equal to 2 and 4-rank equal to 2. Let $F = \mathbf{Q}(\sqrt{pp'})$ be the real quadratic number field introduced in the imaginary case and suppose that $h = [F^1 : F]$ is divisible by 8. In [19], the author proves that there exists an infinite set S of primes ℓ of \mathbf{Q} which are totally decomposed in $F^1(\sqrt{E_{F^1}})$, where E_{F^1} is the group of units of F^1 and the Hilbert 2-class field tower of the field $k = \mathbf{Q}(\sqrt{pp'\ell})$ is infinite. It remains to prove that the infinite family of real quadratic number fields k verifies

$$r_2(k) = r_4(k) = 2.$$

Since each prime $\ell \in S$ is totally decomposed in $F^1(\sqrt{E_{F^1}})/\mathbb{Q}$, in particular is decomposed in $\mathbb{Q}(i)$, $\ell \equiv 1 \pmod{4}$. Therefore, all primes of S are $\equiv 1 \pmod{4}$, and



by genus theory, we have $r_2(k) = 2$. Next we are going to prove that $r_4(k) = 2$, which is reduced by Proposition 2.1 to prove that we have 2 independant C_4 -factorizations of the discriminant $d = \ell pp'$ of k. Since h is divisible by 4 then by Proposition 2.1, the discriminant pp' of the biquadratic number field F has a C_4 factorization, and this means that

$$\left(\frac{p'}{p}\right) = 1 \text{ and } \left(\frac{p}{p'}\right)_4 = \left(\frac{p'}{p}\right)_4.$$
 (1)

On other hand, since $L = \mathbf{Q}(\sqrt{p}, \sqrt{p'})$ is an abelian unramified extension over F, each prime $\ell \in S$ is totally decomposed in L; therefore, we must have

$$\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p'}\right) = 1. \tag{2}$$

The real quadratic number fields $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{p'})$ are contained in F^1 . Denote ε_p (resp. $\varepsilon_{p'}$) the fundamental unit of $\mathbf{Q}(\sqrt{p})$ (resp. $\mathbf{Q}(\sqrt{p'})$). Since ℓ is totally decomposed in $F^1(\sqrt{E_{F^1}})$, in particular is decomposed in $\mathbf{Q}(\sqrt{p})(\sqrt{\varepsilon_p})$ and in $\mathbf{Q}(\sqrt{p'})(\sqrt{\varepsilon_{p'}})$, for each prime ideal \mathcal{L} (resp. \mathcal{L}') of $\mathbf{Q}(\sqrt{p})$ (resp. $\mathbf{Q}(\sqrt{p'})$) above $\ell \in S$, \mathcal{L} (resp. \mathcal{L}') is totally decomposed in $\mathbf{Q}(\sqrt{p})(\sqrt{\varepsilon_p})$ (resp. $\mathbf{Q}(\sqrt{p'})(\sqrt{\varepsilon_{p'}})$). Hence, the value of the norm residue symbol,

$$\left(\frac{\varepsilon_p,\ \ell}{\mathcal{L}}\right) = \left(\mathcal{L}, \mathbf{Q}(\sqrt{p})(\sqrt{\varepsilon_p})/\mathbf{Q}(\sqrt{p})\right) = 1,$$

where the symbol in the middle is the Artin map applied to the prime ideal \mathcal{L} in the extension $\mathbf{Q}(\sqrt{p})(\sqrt{\varepsilon_p})/\mathbf{Q}(\sqrt{p})$. The same occurs for

$$\left(\frac{\varepsilon_{p'}, \ \ell}{\mathcal{L}'}\right) = \left(\mathcal{L}', \mathbf{Q}(\sqrt{p'})(\sqrt{\varepsilon_{p'}})/\mathbf{Q}(\sqrt{p'})\right) = 1.$$

Therefore, we obtain that all units of $\mathbf{Q}(\sqrt{p})$ (resp. $\mathbf{Q}(\sqrt{p'})$) are norms in $M = \mathbf{Q}(\sqrt{p}, \sqrt{\ell})$ (resp. $M' = \mathbf{Q}(\sqrt{p'}, \sqrt{\ell})$). Then, we have

$$dim_{\mathbb{F}_2}(B(M/\mathbf{Q}(\sqrt{p}))) = dim_{\mathbb{F}_2}(B(M'/\mathbf{Q}(\sqrt{p'}))) = 0.$$

On other hand, $ram(M/\mathbf{Q}(\sqrt{p})) = ram(M'/\mathbf{Q}(\sqrt{p'})) = 2$ and since the class number of $\mathbf{Q}(\sqrt{p})$ (resp. $\mathbf{Q}(\sqrt{p'})$) is odd, it follows from the discussion of Sect. 2.1 that

$$r_2(M) = r_2(M') = 1.$$

Consequently, the 2-class number of $\mathbf{Q}(\sqrt{p\ell})$ (resp. $\mathbf{Q}(\sqrt{p'\ell})$) is divisible by 4; thus, the 4-rank of the class group of $\mathbf{Q}(\sqrt{p\ell})$ (resp. $\mathbf{Q}(\sqrt{p'\ell})$) is equal to 1. Hence, using Proposition 2.1, we have the following equalities:



$$\left(\frac{p}{\ell}\right)_4 = \left(\frac{\ell}{p}\right)_4 \text{ and } \left(\frac{p'}{\ell}\right)_4 = \left(\frac{\ell}{p'}\right)_4.$$
 (3)

Combining (1), (2) and (3), the discriminant $pp'\ell$ of k has 2 independant C_4 -factorizations:

$$p \cdot \ell \ell'$$
 and $p' \cdot \ell \ell'$,

finishing the proof in the case where $r_2(k) = r_4(k) = 2$.

Now, we give infinitely many real quadratic number fields k such that $r_2(k) = 2$, $r_4(k) = 4$ with infinite Hilbert 2-class field tower.

Let $F = \mathbf{Q}(\sqrt{pp'})$ be the quadratic number field introduced above and suppose that h is divisible by 32, so we must have

$$\left(\frac{p}{p'}\right) = 1. \tag{4}$$

As in the imaginary case, there exist infinitely many prime numbers $\ell \equiv 3 \pmod 4$ such that ℓ is totally decomposed in the Hilbert 2-class field F^1 of F, and then we have

$$\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p'}\right) = 1. \tag{5}$$

Also, by the distribution of prime numbers in an arithmetic progression, there exist infinitely many prime numbers $\ell' \equiv 3 \pmod{4}$ such that

$$\left(\frac{\ell'}{p}\right) = -\left(\frac{\ell'}{p'}\right) = 1. \tag{6}$$

Let $k = \mathbf{Q}(\sqrt{\ell\ell'pp'})$; it is clear by Genus theory that $r_2(k) = 2$. From the equalities (4), (5) and (6), we deduce that we have exactly one C_4 -factorization of the discriminant $\ell\ell'pp'$ of k:

$$p \cdot p' \ell \ell'$$

Therefore, we have $r_4(k)=1$. On other hand, ℓ is totally decomposed in F^1 , and then the number of ℓ -adic primes of F^1 is equal to 2h, where $h=[F^1:F]$. Moreover, by equalities (6), ℓ' is inert in F; thus, the ℓ' -adic prime of F is principal. So by the reciprocity law applied in the extension F^1/F , the ℓ -adic prime of F is totally decomposed in F^1 , and then the number of ℓ' -adic primes of F^1 is equal to h. Hence the number of ramified primes in the extension $F^1(\sqrt{\ell \ell'})/F^1$ is equal to

$$ram(F^{1}(\sqrt{\ell\ell'})/F^{1}) = 2h + h = 3h.$$



On other hand, we have $dim_{\mathbb{F}_2}(B(F^1(\sqrt{\ell\ell'})/F^1)) \leq [F^1: \mathbf{Q}] = 2h$ and $r_2(E_{F^1(\sqrt{\ell\ell'}})) = 4h$. Hence, since $h \geq 32$, one can readily verify that

$$ram\big(F^1\big(\sqrt{\ell\ell'}\big)/F^1\big) - dim_{\mathbb{F}_2}\big(B\big(F^1\big(\sqrt{\ell\ell'}\big)/F^1\big)\big)\big) - 1 \geq 2 + 2\sqrt{r_2(E_{F^1(\sqrt{\ell\ell'}}) + 1}.$$

By Sect. 2.1, we have

$$r_2\big(F^1\big(\sqrt{\ell\ell'}\big)\big) \geq ram\big(F^1\big(\sqrt{\ell\ell'}\big)/F^1\big) - dim_{\mathbb{F}_2}\big(B\big(F^1\big(\sqrt{\ell\ell'}\big)/F^1\big)\big)\big) - 1,$$

so $F^1(\sqrt{\ell\ell'})$ satisfies the inequality (*) of Sect. 2.3, and consequently $F^1(\sqrt{\ell\ell'})$ has infinite Hilbert 2-class field tower. Therefore, since $F^1(\sqrt{\ell\ell'})/k$ is an unramified 2-extension, k has infinite Hilbert 2-class field tower. Hence, the proof of the theorem is now complete.

References

- 1. Cassels, J., Fröhlich, A.: Algebraic Number Theory. Academic Press, London (1986)
- 2. Gerth, F.: Quadratic fields with infinite Hilbert 2-class field towers. Acta Arith. 106(2), 151-158 (2003)
- 3. Gerth, F.: A density result for some imaginary quadratic fields with infinite Hilbert 2-class field tower. Arch. Math. (Basel) 82(1), 23–27 (2004)
- Gerth, F.: Densities for some real quadratic fields with infinite Hilbert 2-class field towers. J. Number Theory 118, 90–97 (2006)
- Golod, E.S., Shafarevich, I.R.: On the class field tower. Izv. Akad. auk SSSR Ser. Math. 28, 261–272 (1964) (in Russian); English translation in AMS Transl. 48
- 6. Hajir, F.: On a theorem of Koch. Pac. J. Math. 176(1), 15–18 (1996)
- 7. Hajir, F.: Correction to 'On a theorem of Koch'. Pac. J. Math. 196(2), 507–508 (2000)
- 8. Jehne, W.: On knots in algebraic number theory. J. Reine Angew. Math. 311(312), 215–254 (1979)
- Kisilevsky, H.: Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94. J. Number Theory 8, 271–279 (1976)
- 10. Lang, S.: Algebraic Number Theory. Addison-Wesley, Reading (1970)
- 11. Lemmermeyer, F.: Higher Descent on Pell Conics. I. From Legendre to Selmer, arXiv: math/0311309v1
- 12. Maire, C.: Un raffinement du théorème de Golod-Safarevic. Nagoya Math. J. 150, 1-11 (1998)
- 13. Martinet, J.: Tours de corps de classes et estimations de discriminants. Invent. Math. 44, 65-73 (1978)
- Mouhib, A.: Infinite Hilbert 2-class field tower of quadratic number fields. Acta Arith. 145, 267–272 (2010)
- Mouhib, A.: On 2-class field towers of some real quadratic number fields with 2-class groups of rank
 Ill. J. Math. 57, 1009–1018 (2013)
- Rédei, L., Reichardt, H.: Die anzahl der durch 4 teilbaren invarienten der klasen-gruppe eines beliebigen quadratischen Zahlkorpers. J. Reine Angew. Math. 170, 69–74 (1933)
- Schmithals, B.: Konstruktion imaginärquadratischer Körper mit undendlichem Klassenkörperturm. Arch. Math. 34, 307–312 (1980)
- 18. Scholz, A.: Über die Lösbarkeit der Gleichung $t^2 Du^2 = -4$. Math. Z. 39, 95–111 (1934)
- 19. Schoof, R.: Infinite class field towers of quadratic fields. J. Reine Angew. Math. 372, 209–220 (1986)

