ARCHIVUM MATHEMATICUM (BRNO)
Tomus 57 (2021), 13–26

ON THE 2-CLASS GROUP OF SOME NUMBER FIELDS WITH LARGE DEGREE

Mohamed Mahmoud Chems-Eddin, Abdelmalek Azizi, and Abdelkader Zekhnini

Abstract. Let d be an odd square-free integer, $m \geq 3$ any integer and $L_{m,d} := \mathbb{Q}(\zeta_{2^m}, \sqrt{d})$. In this paper, we shall determine all the fields $L_{m,d}$ having an odd class number. Furthermore, using the cyclotomic $\mathbb{Z}_2$-extensions of some number fields, we compute the rank of the 2-class group of $L_{m,d}$ whenever the prime divisors of d are congruent to 3 or 5 (mod 8).

1. Introduction

Let K be an algebraic number field. For a prime integer p, let $\mathrm{Cl}_p(K)$ denote the p-class group of K, that is the p-Sylow subgroup of its ideal class group $\mathrm{Cl}(K)$ in the wide sense. The class group $\mathrm{Cl}(K)$, its subgroup $\mathrm{Cl}_p(K)$ and their orders and structures have been investigated and studied in many papers for a long time, and there are many interesting open problems related to these topics which are the object of intense studies.

One classical and difficult problem in algebraic number theory is the determination of the rank of the p-class group of a number field K. When $p = 2$ and K is a quadratic extension of a number field k having an odd class number, the ambiguous class number formula can be used to determine this rank, involving units of k which are norms in K/k and ramified primes in K/k (cf. [6]). This fact is practically one of the most important means for structuring the 2-class group of a given number field of small degree (cf. [1, 12]). Our contribution in this article is to study the 2-rank of an infinite family of number fields, with large degree over $\mathbb{Q}$. Comparing with other papers tackling this problem, the main novelty of this article is the combination of ramification theory,

---

2020 *Mathematics Subject Classification*: primary 11R29; secondary 11R11, 11R23, 11R32.
Key words and phrases: cyclotomic $\mathbb{Z}_2$-extension, 2-rank, 2-class group.
Received November 29, 2019, revised September 2020. Editor C. Greither.
DOI: 10.5817/AM2021-1-13

ambiguous class number formula and the theory of cyclotomic $\mathbb{Z}_2$-extensions of some number fields.

Let d be an odd square-free integer, $m \geq 3$ any integer and $L_{m,d} := \mathbb{Q}(\zeta_{2^m}, \sqrt{d})$. In the present paper, we are interested in studying the parity of the class number of all the fields $L_{m,d}$. Furthermore, we compute the rank of the 2-class group of $L_{m,d}$ assuming the prime divisors of d are congruent to 3 or 5 (mod 8). Since the unit group of $\mathbb{Q}(\zeta_{2^m})$, with $m \geq 7$, is not described until today, the methods using unit groups for computing the rank of the 2-class group of a given number field are not valid for treating such problem in our case when $m \geq 7$. For this, we will call some results from Iwasawa theory to overcome the problem. In the appendix, we compute the rank of the 2-class group of $L^+_{m,d}$, the maximal real subfield of $L_{m,d}$, in terms of the number of prime divisors of d.

Finally, to sum up, let us highlight the importance of some parts of the present work. Note that the layers of the $\mathbb{Z}_2$-extensions of $\Bbbk = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ were subject of some recent studies (e.g. [8, 10]); and in this paper, we give more arithmetical properties of $L_{m,d}$ (resp. $L^+_{m,d}$), the layers of the cyclotomic $\mathbb{Z}_2$-extension of $\Bbbk$ (resp. $\mathbb{Q}(\sqrt{d})$). Furthermore, we discuss the interesting question of the parity of the class number of $L_{m,d}$, and we explicitly give the rank of its 2-class group which is strongly related to the interesting problem of the structure of the Iwasawa module (see for example Corollary 4.5 or [3]). The authors of [3] used this paper with some other techniques of Iwasawa theory to determine the structure of the 2-class group of some fields $L_{m,d}$.

Before quoting some preliminary results, let us fix the following notations which will be used throughout this paper.

Notations

- $\star$ d: An odd square-free integer,
- $\star$ m: A positive integer ≥ 3,
- $\star$ ζ_n: An n-th primitive root of unity,
- $\star$ $K_m = \mathbb{Q}(\zeta_{2^m})$,
- $\star$ $L_{m,d} = K_m(\sqrt{d})$,
- $\star$ k^+: The maximal real subfield of a number field k,
- $\star$ $\mathrm{Cl}_2(k)$: The 2-class group of a number field k,
- $\star$ k_∞: The $\mathbb{Z}_2$-extension of a number field k,
- $\star$ k_n: The nth layer of k_∞/k,
- $\star$ X_∞: $\varprojlim(\mathrm{Cl}_2(k_n))$,

- ⋆ $\mathcal{O}_k$: The ring of integers of k,
- ⋆ $h(k)$: The class number of k,
- ⋆ $h_2(k)$: The 2-class number of k,
- ⋆ N: The norm map of the extension $L_{m,d}/K_m$,
- ⋆ E_k: The unit group of k,
- ⋆ $e_{m,d}$: Defined by $(E_{K_m} : E_{K_m} \cap N(L_{m,d})) = 2^{e_{m,d}}$,
- ⋆ $\left(\frac{\alpha,d}{\mathfrak{p}}\right)$: The quadratic norm residue symbol for $L_{m,d}/K_m$,
- ⋆ ε_l: The fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{l})$,
- ⋆ $h_2(d)$: The 2-class number of the quadratic field $\mathbb{Q}(\sqrt{d})$,
- ⋆ $\mathrm{rank}_2(\mathrm{Cl}(L_{m,d}))$: The rank of the 2-class group of $L_{m,d}$.

2. Preliminary results

Let us collect some results that will be used in the sequel. Let k be an algebraic number field and k_∞ a $\mathbb{Z}_2$-extension of k, that is a Galois extension of k whose Galois group is topologically isomorphic to the 2-adic ring $\mathbb{Z}_2$. For a non-negative integer n, denote by k_n the intermediate field of k_∞/k with degree 2^n over k. Begin by the following theorem which deals with ranks and class numbers of the intermediate subextensions of k_∞/k.

Theorem 2.1 ([5])**.** *Let k_∞/k be a $\mathbb{Z}_2$-extension and n_0 an integer such that any prime of k_∞ which is ramified in k_∞/k is totally ramified in k_∞/k_{n_0}.*

1. *If there exists an integer $n \geq n_0$ such that $h_2(k_n) = h_2(k_{n+1})$, then $h_2(k_n) = h_2(k_m)$ for all $m \geq n$.*
2. *If there exists an integer $n \geq n_0$ such that* $\mathrm{rank}_2(\mathrm{Cl}(k_n)) = \mathrm{rank}_2(\mathrm{Cl}(k_{n+1}))$*, then* $\mathrm{rank}_2(\mathrm{Cl}(k_m)) = \mathrm{rank}_2(\mathrm{Cl}(k_n))$ *for all $m \geq n$.*

Theorem 2.2 ([14, Theorem 10.1])**.** *If an extension of number fields L/K contains no unramified abelian subextensions F/K, with $F \neq K$, then $h(K)$ divides $h(L)$.*

Lemma 2.3 ([14, Lemma 8.1])**.** *The cyclotomic units of K_m (resp. K_m^+)* are generated by ζ_{2^m} (resp. -1) and $\xi_{k,m} = \zeta_{2^m}^{(1-k)/2}\frac{1-\zeta_{2^m}^k}{1-\zeta_{2^m}}$, where k is an odd integer such that $1 < k < 2^{m-1}$.

The following result is a consequence of ramification theory in a Kummer extension.

Theorem 2.4 ([7])**.** *Let K/k be a quadratic extension and $\mu \in k$ prime to 2 such that $K = k(\sqrt{\mu})$. The extension K/k is unramified at finite primes if and only if μ verifies the following properties:*

1. *The principal ideal generated by μ is a square of a fractional ideal of k.*
2. *There exists $\xi \in k$ such that $\mu \equiv \xi^2 \pmod 4$.*

Lemma 2.5 ([1])**.** *Let p be a prime integer and $\mathfrak{p}_{K_3}$ a prime ideal of K_3 lying over p.*

1. *If $p \equiv 3 \mod 8$, then $\left(\frac{\zeta_8, p}{\mathfrak{p}_{K_3}}\right) = -1$ and $\left(\frac{\varepsilon_2, p}{\mathfrak{p}_{K_3}}\right) = -1$.*
2. *If $p \equiv 5 \mod 8$, then $\left(\frac{\zeta_8, p}{\mathfrak{p}_{K_3}}\right) = -1$ and $\left(\frac{\varepsilon_2, p}{\mathfrak{p}_{K_3}}\right) = 1$.*

Proposition 2.6. *Let $m \geq 3$ be an integer and d an odd square-free integer. The ring of integers of $L_{m,d}$ is given by*

$$\mathcal{O}_{L_{m,d}} = \begin{cases} \mathbb{Z}[\zeta_{2^m}, \frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \mod 4\,, \\ \mathbb{Z}[\zeta_{2^m}, \frac{1+\sqrt{-d}}{2}] & \text{if } d \equiv 3 \mod 4\,. \end{cases}$$

Furthermore, the relative discriminant of $L_{m,d}/K_m$ is $\delta_{L_{m,d}/K_m} = d\mathcal{O}_{L_{m,d}}$.

Proof. Assume that $d \equiv 1 \pmod 4$, then $\delta_{K_m} \wedge \delta_{\mathbb{Q}(\sqrt{d})} = 1$, so $\mathcal{O}_{L_{m,d}} = \mathcal{O}_{K_m}\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\zeta_{2^m}, \frac{1+\sqrt{d}}{2}] = \mathcal{O}_{K_m}[\frac{1+\sqrt{d}}{2}]$. So the relative discriminant of $L_{m,d}/K_m$ is generated by $\mathrm{disc}_{L_{m,d}/K_m}(1, \frac{1+\sqrt{d}}{2}) = (\frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2})^2 = d$. If $d \equiv 3 \pmod 4$, then $-d \equiv 1 \pmod 4$. As we have $\mathcal{O}_{L_{m,d}} = \mathcal{O}_{L_{m,-d}}$, so by the previous case we easily deduce the result. □

Proposition 2.7. *Let $m \geq 4$ be an integer and p a prime integer. Then, p decomposes into the product of two prime ideals of K_m if and only if $p \equiv 3$ or $5 \pmod 8$.*

Proof. Let p be a rational prime and $p\mathcal{O}_{K_4} = \mathfrak{p}_1 \ldots \mathfrak{p}_g$ its factorization in $\mathcal{O}_{K_4}$. Denote by f the residue degree of p in K_4, and by k the positive integer less than 16, such that $p \equiv k \pmod{16}$. Then, by the theorem of the cyclotomic reciprocity law (see [14, Theorem 2.13]), we have:

k	1	3	5	7	9	11	13	15
f	1	4	4	2	2	4	4	2
g	8	2	2	4	4	2	2	4

It follows that the rational primes that decompose into the product of two prime ideals of K_4 are exactly those which are congruent to 3 or 5 $\pmod 8$. So a prime

p decomposes into the product of two prime ideals of K_m, is congruent to 3 or 5 (mod 8). For the converse, assume that $p \equiv 3$ or $5 \pmod 8$ and $p\mathcal{O}_{K_m} = \mathfrak{p}_1\mathfrak{p}_2$, for $m \geq 4$. As $K_{m+1} = K_m(\sqrt{\zeta_{2^m}})$, then $\left(\frac{\zeta_{2^m}}{\mathfrak{p}_i}\right) = \left(\frac{\zeta_{2^{m-1}}}{\mathfrak{p}_i}\right) = -1$. So the result comes by induction. $\square$

Let us propose a new simple proof of the following well known result.

Theorem 2.8. *For all $m \geq 2$, the class number of $K_m = \mathbb{Q}(\zeta_{2^m})$ is odd and every unit of K_m is a norm of an element of K_{m+1}.*

Proof. Note first that $K_{m+1} = K_m(\sqrt{\zeta_{2^m}})$. Suppose $h(K_m)$ is odd for some $m \geq 2$. As K_{m+1}/K_m is quadratic extension, so the well known ambiguous class number formula (see [6]) implies that $\mathrm{rank}_2(K_{m+1}) = t_m - 1 - e_m$, where e_m is defined by $(E_{K_m} : E_{K_m} \cap N_{K_{m+1}/K_m}(K^*_{m+1})) = 2^{e_m}$ and t_m is the number of ramified primes in K_{m+1}/K_m. Since 2 is the only rational prime that is ramified in K_{m+1} and it is totally ramified (in K_{m+1}), hence $t_m = 1$. Thus, $\mathrm{rank}_2(K_{m+1}) = 1 - 1 - e_m = -e_m$. From which we deduce that $e_m = 0$ and $\mathrm{rank}_2(K_{m+1}) = 0$. So the result comes by induction. $\square$

3. The parity of the class number of the fields $L_{m,d}$

In this section, we investigate the parity of the class number of fields $L_{m,d}$ without relying on results of Iwasawa theory.

Theorem 3.1. *Let d be an odd square-free integer and $m \geq 3$ any integer. Then $h(L_{m,d})$ is odd if and only if d is a prime congruent to 3 or 5 (mod 8).*

Proof. Suppose that d is odd, and denote by $L^*_{m,d}$, $H_{m,d}$ the genus field and the Hilbert 2-class field of $L_{m,d}$ respectively. It is known that:

$$[L^*_{m,d} : \mathbb{Q}] = \prod_{p|\delta_{L_{m,d}}} e(p) \quad \text{and} \quad \mathrm{Cl}_2(L_{m,d}) = \mathrm{Gal}(H_{m,d}/L_{m,d}),$$

where $e(p)$ is the ramification index of p in $L_{m,d}$. So

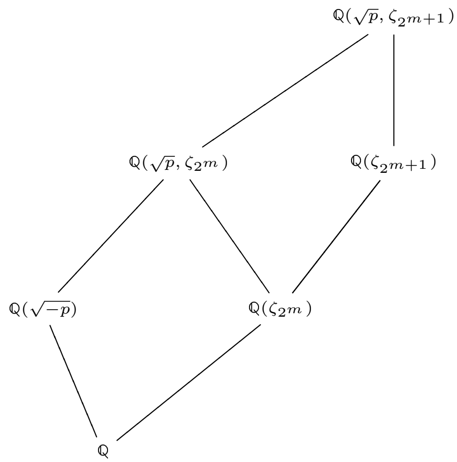
$$[L^*_{m,d} : \mathbb{Q}] = \prod_{p|2d} e(p) = [L^*_{m,d} : L_{m,d}][L_{m,d} : \mathbb{Q}] = 2^m[L^*_{m,d} : L_{m,d}].$$

Since $e(2) = 2^{m-1}$ and $e(p) = 2$ for any prime divisor p of d, we have

$$\prod_{p|d} e(p) = 2.[L^*_{m,d} : L_{m,d}].$$

Hence, if d is not a prime, then $L_{m,d} \subsetneq L^*_{m,d} \subseteq H_{m,d}$ and $h_2(L_{m,d})$ is even.

Suppose now that $d = p$ is a prime. We distinguish the following four cases:
• Assume $d = p \equiv 1 \pmod 8$. Set $p = a^2 + 16b^2 = e^2 - 32f^2$ and $\pi_1 = a + 4bi$, $\pi_2 = e + 4f\sqrt{2}$. As the ramified primes of K_m in $L_{m,d}$ are exactly the prime divisors of p in K_m, then the ideals of $L_{m,d}$ generated by π_1 and π_2 are squares of ideals of $L_{m,d}$. Note that as a and e are odd, then $a \equiv e \equiv \pm 1 \equiv i^2 \pmod 4$. It follows that the equation $\pi_j \equiv \xi^2 \pmod 4$, $j = 1$ or 2, has a solution. So $L_1 = L_{m,d}(\sqrt{\pi_1})$ and $L_2 = L_{m,d}(\sqrt{\pi_2})$ are two distinct unramified quadratic extensions of $L_{m,d}$. Thus $h(L_{m,d})$ is divisible by 4. Furthermore, $\mathrm{Cl}_2(L_{m,d})$ is not trivial and not cyclic.
• Assume now $d = p \equiv 7 \pmod 8$. We prove that $h(L_{m,p})$ is even for all $m \geq 3$ by induction on m. If $m = 3$, then $h(L_{3,p})$ is even by [1, Theorem 4.4]. Suppose that $h(L_{m,p})$ is even for some $m \geq 3$. We have $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$ is unramified at 2 and $\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}$ is totally ramified at 2, then $L_{m+1,p}/L_{m,p}$ is a quadratic extension that is ramified at primes over 2. So $h(L_{m,p})$ divides $h(L_{m+1,p})$, by Theorem 2.2. Hence, $h(L_{m+1,p})$ is even.



• Assume that $d = p \equiv 5 \pmod 8$. For $m \geq 3$, we have p decomposes into the product of two prime ideals of K_m, denote by $\mathfrak{p}_{K_m}$ one of them (such that $\mathfrak{p}_{K_{m-1}} \subset \mathfrak{p}_{K_m}$). Since $\zeta_{2^m}^2 = \zeta_{2^{m-1}}$, so the minimal polynomial of ζ_{2^m} over K_{m-1} is $X^2 - \zeta_{2^{m-1}}$ and $N_{K_m/K_{m-1}}(\zeta_{2^m}) = -\zeta_{2^{m-1}}$. Then

$$\left(\frac{\zeta_{2^m}, p}{\mathfrak{p}_{K_m}}\right) = \left(\frac{-\zeta_{2^{m-1}}, p}{\mathfrak{p}_{K_{m-1}}}\right) = \left(\frac{\zeta_{2^{m-1}}, p}{\mathfrak{p}_{K_{m-1}}}\right) = \cdots = \left(\frac{\zeta_8, p}{\mathfrak{p}_{K_3}}\right) = -1\,,$$

hence $e_{m,d} \neq 0$ and $\mathrm{rank}_2(\mathrm{Cl}(L_{m+1,p})) = 2 - 1 - e_{m+1,p} = 1 - e_{m+1,p} = 0$. Thus the 2-class group of $L_{m+1,p}$ is trivial and $h(L_{m,d})$ is odd.

• We treat the case $d = p \equiv 3 \pmod 8$, similarly to the previous one and we show that $h(L_{m,d})$ is odd. Which achieves the proof. □

Remark 3.2. Let d be a positive square-free integer, k_∞ the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$, k_n the nth layer of k_∞/k and $X_\infty = \varprojlim(\mathrm{Cl}_2(k_n))$, thus $X_\infty = 0$ if and only if $d = p$ is a prime such that $p \equiv 5$ or $3 \pmod 8$.

4. The rank of the 2-class group of the fields $L_{m,d}$

Let d be an odd composite square-free integer of prime divisors congruent to 3 or 5 $\pmod 8$ and $m \geq 3$ an integer. To state the main theorem of this section, we need the following result.

Lemma 4.1. *Let $m \geq 3$ be an integer and d an odd composite square-free integer. Let $\mathfrak{p}_{K_m}$ denote a prime ideal of K_m dividing d.*

1. *If $d = p_1, \ldots, p_r$, such that for all i, $p_i \equiv 5 \pmod 8$ is a prime, then*

$$\left(\frac{\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\right) = -1 \quad \text{and} \quad \left(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m}}\right) = 1\,.$$

2. *If $d = p_1, \ldots, p_r$, such that for all i, $p_i \equiv 3 \pmod 8$ is a prime, then*

$$\left(\frac{\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\right) = -1 \text{ and } \left(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m}}\right) = \begin{cases} -1\,, & \text{if } k \equiv \pm 3 \pmod 8 \\ 1\,, & \text{elsewhere.} \end{cases}$$

3. *If $d = p_1, \ldots, p_s, p_{s+1}, \ldots, p_r$, such that d is not prime, $p_i \equiv 5 \pmod 8$ for $1 \leq i \leq s$ and $p_j \equiv 3 \pmod 8$ for $s+1 \leq j \leq r$, then*

$$\left(\frac{\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\right) = -1 \text{ and } \left(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m}}\right) = \begin{cases} -1\,, & \text{if } \ p \equiv 3 \pmod 8 \text{ and} \\ & \qquad k \equiv \pm 3 \pmod 8 \\ 1\,, & \text{elsewhere,} \end{cases}$$

   where p is the rational prime contained in $\mathfrak{p}_{K_m}$.

Proof. Denote by $\mathfrak{p}_K$ a prime ideal of a number field K lying over p. Each case needs special computations:

1. Note that $N_{K_m/K_{m-1}}(\zeta_{2^m}) = -\zeta_{2^{m-1}}$, so

$$\left(\frac{\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\right) = \left(\frac{\zeta_{2^m}, p}{\mathfrak{p}_{K_m}}\right) = \left(\frac{\zeta_{2^{m-1}}, p}{\mathfrak{p}_{K_{m-1}}}\right) = \cdots = \left(\frac{\zeta_8, p}{\mathfrak{p}_{K_3}}\right) = -1\,, \text{ and}$$

$$\left(\frac{1-\zeta_{2^m}^k, d}{\mathfrak{p}_{K_m}}\right) = \left(\frac{N_{K_m/K_{m-1}}(1-\zeta_{2^m}^k), d}{\mathfrak{p}_{K_{m-1}}}\right) = \cdots = \left(\frac{1-\zeta_8^k, d}{\mathfrak{p}_{K_3}}\right) = \left(\frac{1-i^k, d}{\mathfrak{p}_{K_2}}\right).$$

Thus

$$\begin{aligned}
\Big(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m}}\Big) &= \Big(\frac{\zeta_{2^m}^{(1-k)/2}, d}{\mathfrak{p}_{K_m}}\Big)\Big(\frac{\frac{1-\zeta_{2^m}^k}{1-\zeta_{2^m}}, d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{(1-\zeta_{2^m}^k)(1-\zeta_{2^m}), d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{1-\zeta_{2^m}^k, d}{\mathfrak{p}_{K_m}}\Big)\Big(\frac{1-\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{1-i^k, d}{\mathfrak{p}_{K_2}}\Big)\Big(\frac{1-i, d}{\mathfrak{p}_{K_2}}\Big)\\
&= \begin{cases} -\Big(\frac{1+i,d}{\mathfrak{p}_{K_2}}\Big)\Big(\frac{1-i,d}{\mathfrak{p}_{K_2}}\Big) & \text{if } \ k\equiv 3 \pmod 4\\ \Big(\frac{1-i,d}{\mathfrak{p}_{K_2}}\Big)\Big(\frac{1-i,d}{\mathfrak{p}_{K_2}}\Big) & \text{elsewhere}\end{cases}\\
&= \begin{cases} -\Big(\frac{2,d}{\mathfrak{p}_{K_2}}\Big) = -\Big(\frac{2,p}{\mathfrak{p}_{K_2}}\Big) = -\Big(\frac{2}{p}\Big) & \text{if } \ k\equiv 3 \pmod 4\\ 1 & \text{elsewhere}\end{cases}\\
&= 1\,.
\end{aligned}$$

2. As in the previous case, we have $\Big(\frac{\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\Big) = -1$ and:

$$\begin{aligned}
\Big(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m}}\Big) &= \Big(\frac{\zeta_{2^m}^{(1-k)/2}, d}{\mathfrak{p}_{K_m}}\Big)\Big(\frac{\frac{1-\zeta_{2^m}^k}{1-\zeta_{2^m}}, d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{(1-\zeta_{2^m}^k)(1-\zeta_{2^m}), d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{1-\zeta_{2^m}^k, d}{\mathfrak{p}_{K_m}}\Big)\Big(\frac{1-\zeta_{2^m}, d}{\mathfrak{p}_{K_m}}\Big)\\
&= (-1)^{(1-k)/2}\Big(\frac{1-\zeta_8^k, d}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8, d}{\mathfrak{p}_{K_3}}\Big)\\
&= (-1)^{(3-k)/2}\Big(\frac{\zeta_8^{-1}, d}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8^k, d}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8, d}{\mathfrak{p}_{K_3}}\Big) \qquad (1)\\
&= \begin{cases} \Big(\frac{\varepsilon_2,p}{\mathfrak{p}_{K_3}}\Big), & \text{if } \ k\equiv 3 \pmod 8\\ \Big(\frac{1+\zeta_8,p}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8,p}{\mathfrak{p}_{K_3}}\Big), & \text{if } \ k\equiv 5 \pmod 8 \quad \text{(see (1))}\\ -\Big(\frac{1-\zeta_8^{-1},p}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8,p}{\mathfrak{p}_{K_3}}\Big), & \text{if } \ k\equiv 7 \pmod 8 \quad \text{(see (1))}\\ \Big(\frac{1-\zeta_8,p}{\mathfrak{p}_{K_3}}\Big)\Big(\frac{1-\zeta_8,p}{\mathfrak{p}_{K_3}}\Big), & \text{if } \ k\equiv 1 \pmod 8 \quad \text{(see (1))}\end{cases}
\end{aligned}$$

$$= \begin{cases} -1, & \text{if } k \equiv 3 \pmod 8 \quad \text{(see Lemma 2.5)} \\ \left(\frac{1-i,p}{\mathfrak{p}_{K_3}}\right), & \text{if } k \equiv 5 \pmod 8 \\ -\left(\frac{(1-\zeta_8^{-1})(1-\zeta_8),p}{\mathfrak{p}_{K_3}}\right), & \text{if } k \equiv 7 \pmod 8 \\ 1, & \text{if } k \equiv 1 \pmod 8 \end{cases}$$

$$= \begin{cases} -1, & \text{if } k \equiv 3 \pmod 8 \\ \left(\frac{1-i,p}{\mathfrak{p}_{K_2}}\right) = \left(\frac{2}{p}\right), & \text{if } k \equiv 5 \pmod 8 \\ -\left(\frac{2-\sqrt{2},p}{\mathfrak{p}_{K_3}}\right) = -\left(\frac{2-\sqrt{2},p}{\mathfrak{p}_{\mathbb{Q}(\sqrt{2})}}\right) = -\left(\frac{2}{p}\right), & \text{if } k \equiv 7 \pmod 8 \\ 1, & \text{if } k \equiv 1 \pmod 8 \end{cases}$$

$$= \begin{cases} -1, & \text{if } k \equiv \pm 3 \pmod 8, \\ 1, & \text{elsewhere.} \end{cases}$$

3. We similarly prove the third assertion.

□

Remark 4.2. Keep the above hypothesis. We have

1. ζ_{2^m} is not a norm in $L_{m,d}/K_m$.
2. $\xi_{k,m}$ is not a norm in $L_{m,d}/K_m$ if and only if d is divisible by a prime integer congruent to $3 \pmod 8$ and $k \equiv \pm 3 \pmod 8$.

Now we are able to prove the main result of this section.

Theorem 4.3. *Let $d = p_1, \ldots, p_r$ be an odd composite square-free integer such that every prime divisor p_i of d is congruent to 3 or $5 \pmod 8$ and $m \geq 3$ is an integer. Then the rank of the 2-class group of $L_{m,d}$ is $2r-2$ or $2r-3$. More precisely,* $\mathrm{rank}_2(\mathrm{Cl}(L_{m,d})) = 2r-2$ *if and only if all the prime divisors of d are in the same coset $\pmod 8$.*

Proof. The ring of integers of K_m is principal for $m \in \{3,4,5\}$ (see [11]). So $h(K_m^+) = 1$. By [14, Theorem 8.2] and Lemma 2.3, the unit group E_{K_m} of K_m is generated by ζ_{2^m} and $\xi_{k,m} = \zeta_{2^m}^{(1-k)/2}\frac{1-\zeta_{2^m}^k}{1-\zeta_{2^m}}$, where k is an odd integer such that $1 < k < 2^{m-1}$. So by the ambiguous class number formula (see [6]) and Proposition 2.6, we have $\mathrm{rank}_2(\mathrm{Cl}(L_{m,d})) = 2r-1-e_{m,d}$. Let p be a prime divisor of d and $\mathfrak{p}_{K_m}$ a prime ideal of K_m lying over p. If all the prime divisors of d are in the same coset $\pmod 8$, then by Lemma 4.1 it is easy to see that $E_{K_m}/(E_{K_m} \cap N(L_{m,d})) = \{\overline{1}, \overline{\zeta_{2^m}}\}$. Hence $e_{m,d} = 1$.

Suppose now that the prime divisors of d are not in the same coset $\pmod 8$. By Lemma 4.1, we have $\xi_{k,m}$ is a norm in $L_{m,d}/K_m$, for all $k \equiv \pm 1 \pmod 8$.

Let $k \neq k'$ be two odd positive integers such that $1 < k$, $k' < 2^{m-1}$ and k, $k' \not\equiv \pm 1 \pmod 8$. Again by Lemma 4.1, we have:

$$\left(\frac{\xi_{k,m}\xi_{k',m}, d}{\mathfrak{p}_{K_m}}\right) = 1 \text{ for all } \mathfrak{p}_{K_m} \text{ of } K_m,$$

and:

$$\left(\frac{\zeta_{2^m}\xi_{k,m}, d}{\mathfrak{p}_{\mathfrak{p}_{K_3}}}\right) = -1 \text{ if } \mathfrak{p}_{K_m} \text{ is lying over } p \equiv 5 \pmod 8.$$

So $\overline{\xi_{k,m}} = \overline{\xi_{k',m}}$ and $\overline{\xi_{k,m}} \neq \overline{\zeta_{2^m}}$ in $E_{K_m}/(E_{K_m} \cap N(L_{m,d}))$. Thus $E_{K_m}/(E_{K_m} \cap N(L_{m,d})) = \{\overline{1}, \overline{\zeta_{2^m}}, \overline{\xi_{k,m}}, \overline{\zeta_{2^m}\xi_{k,m}}\}$. Hence $e_{m,d} = 2$. So we have the theorem for $m \in \{3, 4, 5\}$. Let $\pi_1 = 2$, $\pi_2 = 2 + \sqrt{2}, \ldots, \pi_m = 2 + \sqrt{\pi_m}$. Set $\mathbb{k} = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ and $\mathbb{k}_1 = \mathbb{k}(\sqrt{\pi_1}) = L_{3,d}$, $\mathbb{k}_2 = \mathbb{k}(\sqrt{\pi_2}) = L_{2,d}, \ldots$, $\mathbb{k}_m = \mathbb{k}(\sqrt{\pi_m}) = L_{m,d}$. Thus, the cyclotomic $\mathbb{Z}_2$-extension $\mathbb{k}_\infty$ of $\mathbb{k}$ is given by $\cup_{m=0}^{\infty} \mathbb{k}_m$. As we have proved Theorem 4.3 for the three layers $\mathbb{k}_1$, $\mathbb{k}_2$ and $\mathbb{k}_3$, then Theorem 2.1 achieves the proof. □

By the previous results, it is easy to get the following interesting theorem.

Theorem 4.4. *Let d be an odd square-free integer and $m \geq 3$ an integer. Suppose that d is not a prime congruent to $7 \pmod 8$. Then $\mathrm{Cl}_2(L_{m,d})$ is cyclic non-trivial if and only if $d = pq$ with $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$.*

Proof. In fact, by [1, Theorem 5.5] we have $\mathrm{Cl}_2(L_{3,d})$ is cyclic non-trivial if and only if d has one of the following forms:

1. $d = q \equiv 7 \pmod 8$ is a prime integer.
2. $d = qp$, where $q \equiv 3 \pmod 8$ and $p \equiv 5 \pmod 8$ are prime integers.

Since $\mathrm{rank}_2(\mathrm{Cl}_2(L_{m,d})) \geq \mathrm{rank}_2(\mathrm{Cl}_2(L_{3,d}))$, then we get the result by the previous theorem. □

Corollary 4.5. *Let d be an odd square-free integer and $m \geq 3$. Suppose that d is not a prime congruent to $7 \pmod 8$. Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$, k_n the n-th layer of k_∞/k and $X_\infty = \varprojlim(\mathrm{Cl}_2(k_n))$. Thus*

1. *X_∞ is cyclic if and only if, $d = pq$ with $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$.*
2. *If $d = pq$ with $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$, then the Iwasawa λ-invariant of k equals 0 or 1.*

Remark 4.6. For any integer $r \geq 0$ there are infinitely many imaginary biquadratic number fields k such that $\mathrm{rank}(\mathrm{Cl}_2(k_n))) = r$, $\forall n \geq 1$, where k_n is the n-th layer of k_∞/k.

5. Appendix

Let $m \geq 3$ be an integer and d an odd positive square-free integer. Set $\pi_3 = 2$, $\pi_4 = 2 + \sqrt{2}, \ldots, \pi_m = 2 + \sqrt{\pi_{m-1}}$ and $K_m^+ = \mathbb{Q}(\sqrt{\pi_m})$. The maximal real subfield of $L_{m,d}$ is $L_{m,d}^+ = K_m^+(\sqrt{d})$. Note that, for several cases of positive square-free integers d, the rank of the 2-class group of $L_{m,d}^+$ is well known in terms of the decomposition of those primes in the cyclotomic tower of $\mathbb{Q}$ that ramify in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. In this appendix, we explicitly give the rank of the 2-class group of $L_{m,d}^+$ according to the number of prime divisors of d assuming that all the prime divisors of d are congruent to 3 or $5 \pmod 8$.

Lemma 5.1. *Let p be a rational prime. Then for all $m \geq 3$, p is inert in K_m^+ if and only if p is congruent to 3 or $5 \pmod 8$.*

Proof. For $m = 3$, p is inert in $K_3 = \mathbb{Q}(\sqrt{2})$ if and only if p is congruent to 3 or $5 \pmod 8$. Thus p is inert in K_m^+, implies that p is congruent to 3 or $5 \pmod 8$. We prove the converse by induction. Suppose that p is inert in K_m^+ and show that it is inert in $K_{m+1}^+ = \mathbb{Q}(\sqrt{\pi_{m+1}})$. Let $\mathfrak{p}$ denote the prime ideal of K_i^+ lying over p, for $i \leq m$. We have $\left(\frac{\pi_{m+1}}{\mathfrak{p}}\right) = \left(\frac{N_{K_m^+/K_{m-1}^+}(\pi_{m+1})}{\mathfrak{p}}\right) = \left(\frac{4-\pi_{m+1}}{\mathfrak{p}}\right) = \left(\frac{2-\sqrt{\pi_m}}{\mathfrak{p}}\right) = \cdots = \left(\frac{2}{p}\right) = -1$. It follows that p is inert in K_{m+1}^+. □

Remark 5.2. Let $d = p_1, \ldots, p_r$ be a square-free integer such that all the prime divisors p_i of d are congruent to 3 or $5 \pmod 8$ and $m \geq 3$.

- If $d \equiv 1 \pmod 4$, then we have r primes that ramify in $L_{m,d}^+/K_m^+$, which are exactly the prime divisors of d in K_m^+.
- If $d \not\equiv 1 \pmod 4$, then we have $r+1$ primes that ramify in $L_{m,d}^+/K_m^+$, which are exactly the prime of K_m^+ lying over 2 and the prime divisors of d in K_m^+.

Lemma 5.3. *Let $m \geq 3$ and d be a positive square-free integer such that all the prime divisors of d are congruent to 3 or $5 \pmod 8$ and $\mathfrak{p}_{K_m^+}$ be a prime ideal of K_m^+ dividing d. Then*

$$\left(\frac{\xi_{k,m}, d}{\mathfrak{p}_{K_m^+}}\right) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 8 \text{ and } k \equiv \pm 3 \pmod 8 \\ 1 & \text{elsewhere,} \end{cases}$$

where p is the rational prime in $\mathfrak{p}_{K_m^+}$.

Proof. By Lemmas 2.7 and 5.1, $\mathfrak{p}_{K_m^+}$ decomposes into the product of two primes of K_m. Hence, the result follows directly from Lemma 4.1. □

Theorem 5.4. *Let $m \geq 3$ and $d = p_1, \dots, p_r$ be a positive square-free integer such that every prime divisor p_i of d is congruent to 3 or 5 $\pmod 8$. Then*

$$\mathrm{rank}_2(L^+_{m,d}) = \begin{cases} r-2 & \textit{if} \quad d \equiv 1 \pmod 4 \textit{ and } d \textit{ is divisible by} \\ & \quad \textit{a prime congruent to } 3 \pmod 4, \\ r-1 & \textit{elsewhere.} \end{cases}$$

Proof. Similar to the proof of Theorem 4.3. □

Proposition 5.5. *Let $d = pq$ with $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$. Then for all $m \geq 3$, we have:*

$$h_2(L^+_{m,d}) = 2\,.$$

Proof. Let $\varepsilon_{pq} = a + b\sqrt{pq}$ with a, $b \in \mathbb{Z}$ (resp. $\varepsilon_{2pq} = x + y\sqrt{2pq}$ with x, $y \in \mathbb{Z}$) be the fundamental unit of $\mathbb{Q}(\sqrt{pq})$ (resp. $\mathbb{Q}(\sqrt{2pq})$). It is known that $N(\varepsilon_{pq}) = N(\varepsilon_{2pq}) = 1$. We have $a^2 - 1 = b^2pq$ and $x^2 - 1 = y^2 2pq$. So $a \pm 1$ and $x \pm 1$ are not squares in $\mathbb{N}$. In fact, if $x \pm 1$ is a square in $\mathbb{N}$, then

$$\begin{cases} x \pm 1 = y_1^2 \\ x \mp 1 = 2pqy_2^2\,, \end{cases}$$

for some integers y_1 and y_2 such that $y = y_1y_2$. So $1 = \left(\frac{y_1^2}{p}\right) = \left(\frac{x\pm 1}{p}\right) = \left(\frac{x\mp 1\pm 2}{p}\right) = \left(\frac{\pm 2}{p}\right) = \left(\frac{2}{p}\right) = -1$, which is absurd. Similarly $a \pm 1$ is not a square in $\mathbb{N}$. It follows by [2, Proposition 3.3] that $\{\varepsilon_2, \varepsilon_{pq}, \sqrt{\varepsilon_{pq}\varepsilon_{2pq}}\}$ is a fundamental system of units of $L^+_{3,d} = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Note that by [4, Corollary 19.7], we have $h_2(pq) = h_2(2pq) = 2$. So by Kuruda's class number formula (see [9]), we obtain

$$h_2(L^+_{3,d}) = \frac{1}{4} \cdot 2 \cdot h_2(pq)h_2(2pq)h_2(2) = 2\,.$$

Thus $h_2(d) = h_2(L^+_{3,d}) = 2$. So the result by Theorem 2.1. □

Under the hypothesis of the previous proposition we deduce that the μ-invariant and the λ-invariant vanishes for such field, as well we deduce that the ν-invariant equals 1. For more results on the Iwasawa invariants of real quadratic number fields see [13]. We close our paper by the following beautiful result:

Theorem 5.6. *Let n be an integer such that every prime p appearing in the decomposition of n with an odd exponent is congruent to 1 $\pmod{16}$ or 7 $\pmod 8$. Then the equation:*

$$n = x^2 - y^2\zeta_8\,,$$

has a solution (x, y) in $\mathbb{Q}(\zeta_8) \times \mathbb{Q}(\zeta_8)$.

Proof. We can suppose that n is a positive square-free integer of prime divisors congruent to 1 (mod 16) or 7 (mod 8). Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta_8)$. If $\mathfrak{p}$ does not divide n, then $\left(\frac{\zeta_8, n}{\mathfrak{p}}\right) = \left(\frac{n, \zeta_8}{\mathfrak{p}}\right) = 1$. If $\mathfrak{p}$ is lying over a prime divisor p of n, then we have $\left(\frac{n,\zeta_8}{\mathfrak{p}}\right) = \left(\frac{\zeta_8, n}{\mathfrak{p}}\right) = \left(\frac{\zeta_8, p}{\mathfrak{p}}\right) = 1$. So n is a norm in $K' = \mathbb{Q}(\sqrt{\zeta_8}) = \mathbb{Q}(\zeta_{16})$. Let $\alpha = x + y\zeta_{16}$ be an element of $\mathbb{Q}(\zeta_{16})$ such that $n = N_{K'/K}(\alpha) = (x + y\zeta_{16})(x - y\zeta_{16}) = x^2 - y^2\zeta_8$. Which gives the result. □

Acknowledgement. We would like to take this opportunity to sincerely thank professor Radan Kučera for his remarks that helped to complete the proof of Theorem 3.1.

We also thank the referee for his/her suggestions that held us to improve our paper.

References

[1] Azizi, A., Chems-Eddin, M.M., Zekhnini, A., *On the rank of the 2-class group of some imaginary triquadratic number fields*, Rend. Circ. Mat. Palermo, II Ser. (2019), 19 pp., `https://doi.org/10.1007/s12215-020-00589-0`.

[2] Azizi, A., Zekhnini, A., Taous, M., *On the strongly ambiguous classes of some biquadratic number fields*, Math. Bohem. **14** (2016), 363–384.

[3] Chems-Eddin, M.M., Müller, K., *2-class groups of cyclotomic towers of imaginary biquadratic fields and applications*, Accepted for publication in Int. J. Number Theory, `arXiv:2002.03602`.

[4] Connor, P.E., Hurrelbrink, J., *Class number parity*, Series in Pure Mathematics, World Scientific, 1988.

[5] Fukuda, T., *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 264–266.

[6] Gras, G., *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier (Grenoble) **23** (1973), 1–48.

[7] Hilbert, D., *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Annal. **51** (1898), 1–127.

[8] Hubbard, D., Washington, L.C., *Iwasawa Invariants of some non-cyclotomic $\mathbb{Z}$-extensions*, `arXiv:1703.06550`.

[9] Lemmermeyer, F., *Kuroda's class number formula*, Acta Arith. **66** (1994), 245–260.

[10] Li, J., Ouyang, Y., Xu, Y., Zhang, S., *l-class groups of fields in Kummer towers*, `arXiv:1905.04966`.

[11] Masley, J.M., Montgomery, H.L., *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.

[12] McCall, T.M., Parry, C.J., Ranalli, R.R., *Imaginary bicyclic biquadratic fields with cyclic 2-class group*, J. Number Theory **53** (1995), 88–99.

[13] Mouhib, A., Movahhedi, A., *Cyclicity of the unramified Iwasawa module*, Manuscripta Math. **135** (2011), 91–106.

[14] Washington, L.C., *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, second ed., 1997.

Mohamed Mahmoud Chems-Eddin,
Mohammed First University, Mathematics Department,
Sciences Faculty,
Oujda, Morocco
E-mail: 2m.chemseddin@gmail.com

Abdelmalek Azizi,
Mohammed First University, Mathematics Department,
Sciences Faculty,
Oujda, Morocco
E-mail: abdelmalekazizi@yahoo.fr

Abdelkader Zekhnini,
Mohammed First University, Mathematics Department,
Pluridisciplinary faculty,
Nador, Morocco
E-mail: zekha1@yahoo.fr