Mohamed Mahmoud Chems-Eddin; Abdelmalek Azizi; Abdelkader Zekhnini; Idriss Jerrari

On the Hilbert 2-class field tower of some imaginary biquadratic number fields

Czechoslovak Mathematical Journal, Vol. 71 (2021), No. 1, 269–281

Persistent URL: http://dml.cz/dmlcz/148739

Czechoslovak Mathematical Journal, 71 (146) (2021), 269–281

ON THE HILBERT 2-CLASS FIELD TOWER OF SOME IMAGINARY BIQUADRATIC NUMBER FIELDS

Mohamed Mahmoud Chems-Eddin, Abdelmalek Azizi, Oujda,
Abdelkader Zekhnini, Nador, Idriss Jerrari, Oujda

Received July 27, 2019. Published online October 27, 2020.

Abstract. Let $\Bbbk=\mathbb{Q}(\sqrt{2},\sqrt{d})$ be an imaginary bicyclic biquadratic number field, where d is an odd negative square-free integer and $\Bbbk_2^{(2)}$ its second Hilbert 2-class field. Denote by $G=\mathrm{Gal}(\Bbbk_2^{(2)}/\Bbbk)$ the Galois group of $\Bbbk_2^{(2)}/\Bbbk$. The purpose of this note is to investigate the Hilbert 2-class field tower of $\Bbbk$ and then deduce the structure of G.

Keywords: 2-class group; imaginary biquadratic number field; capitulation; Hilbert 2-class field

MSC 2020: 11R11, 11R27, 11R29, 11R37

1. Introduction

Let k be an algebraic number field. For a prime number p, let $\mathrm{Cl}_p(k)$ be the p-Sylow subgroup of the ideal class group $\mathrm{Cl}(k)$ of k. Let $k_p^{(1)}$ be the Hilbert p-class field of k, that is the maximal unramified (including the infinite primes) abelian field extension of k whose degree over k is a p-power. Put $k_p^{(0)}=k$ and let $k_p^{(i)}$ denote the Hilbert p-class field of $k_p^{(i-1)}$ for any integer $i\geqslant 1$. Then the sequence of fields

$$k=k_p^{(0)}\subset k_p^{(1)}\subset k_p^{(2)}\subset\ldots\subset k_p^{(i)}\ldots$$

is called the *p-class field tower* of k. If $k_p^{(i)}\neq k_p^{(i-1)}$ for all $i\geqslant 1$ the tower is said to be infinite, otherwise the tower is said to be finite, and the minimal integer i satisfying the condition $k_p^{(i)}=k_p^{(i-1)}$ is called the *length of the tower*.

One of the most important and difficult problems in algebraic number theory is to decide whether a p-class field tower of a number field is finite or not. Furthermore,

DOI: 10.21136/CMJ.2020.0333-19

the study of structure of the Galois group of the tower is an open problem. However, for $p = 2$ and $\mathrm{Cl}_p(k)$ being isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Hilbert 2-class field tower of k terminates in at most two steps and the structure of the Galois group $G = \mathrm{Gal}(k_2^{(2)}/k)$ is closely related to the capitulation problem in the unramified quadratic extensions of k, see [15]. Our contribution in this paper is to investigate the Hilbert 2-class field tower of some families of imaginary bicyclic biquadratic number fields $\Bbbk = \mathbb{Q}(\sqrt{2}, \sqrt{d})$, where d is an odd negative square free integer, and to determine the structure of G involving the capitulation problem.

Note that we are looking forward to make a detailed study of some imaginary triquadratic number fields of the form $\mathbb{Q}(\zeta_8, \sqrt{d})$ for which the 2-class group is related to the one of $\Bbbk$ in many cases (see for example [4], Theorem 5.17). Note also that there are many works interested in such question for the fields $\mathbb{Q}(\sqrt{-2}, \sqrt{-d})$, $\mathbb{Q}(\sqrt{2}, \sqrt{-d})$ and $\mathbb{Q}(\sqrt{-1}, \sqrt{d})$, d always being an odd negative square free integer (see for example [3], [5], [7]), which are all subfields of $\mathbb{Q}(\zeta_8, \sqrt{d})$.

2. Notations and preliminary results

Let k be a number field. Along this paper, we adopt the following notations:

- ▷ d: a negative odd square free integer,
- ▷ $\Bbbk = \mathbb{Q}(\sqrt{2}, \sqrt{d})$,
- ▷ k^*: the absolute genus field of k,
- ▷ $\mathcal{O}_k$: the ring of integers of k,
- ▷ $k_2^{(1)}$: the Hilbert 2-class field of k,
- ▷ $k_2^{(2)}$: the Hilbert 2-class field of $k_2^{(1)}$,
- ▷ G: the Galois group of $\Bbbk_2^{(2)}/\Bbbk$,
- ▷ $[\mathfrak{a}]$: the class of an ideal $\mathfrak{a}$ in $\mathcal{O}_k$,
- ▷ $\mathrm{Cl}(k)$: the class group of k,
- ▷ $\mathrm{Cl}_2(k)$: the 2-class group of k,
- ▷ $h_2(k)$: the 2-class number of k,
- ▷ $h_2(m)$: the 2-class number of a quadratic field $\mathbb{Q}(\sqrt{m})$,
- ▷ $N_{k'/k}$: the norm map of some extension k'/k,
- ▷ N: the absolute norm of a quadratic extension over $\mathbb{Q}$,
- ▷ E_k: the unit group of $\mathcal{O}_k$,
- ▷ ε_m: the fundamental unit of $\mathbb{Q}(\sqrt{m})$, if $m > 1$ is a square-free integer,
- ▷ $(a/p)_4$: the biquadratic residue symbol,
- ▷ k^+: the maximal real subfield of k, if k is a CM-field,
- ▷ W_k: the group of roots of unity contained in k,

▷ $Q_k = (E_k : W_k E_{k^+})$ is Hasse's unit index, if k is a CM-field,

▷ $q(k) = \left(E_k : \prod_i E_{k_i}\right)$ is the unit index of k, if k is multiquadratic, and k_i are the quadratic subfields of k.

Let us start by determining fields $\mathbb{k} = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ satisfying the condition that $\mathrm{Cl}_2(\mathbb{k})$ is of type $(2,2)$ (i.e., isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). We will also deduce the group of units of $\mathbb{k}$. From [18], Proposition 4 we get the following results.

Proposition 2.1. *Let d be an odd negative square free integer. Then the rank of $\mathrm{Cl}_2(\mathbb{k})$ equals 2 if and only if d takes one of the following forms:*
(1) *$d = -p$ for a prime $p \equiv 1 \pmod 8$,*
(2) *$d = -pq \equiv 3 \pmod 4$ for primes p and q such that $(2/p) = (2/q) = -1$,*
(3) *$d = -pq \equiv 1 \pmod 4$ for primes p and q such that $(2/p) \neq (2/q)$,*
(4) *$d = -p_1p_2q$ for primes $p_1 \equiv p_2 \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$,*
(5) *$d = -q_1q_2q_3$ for primes $q_1 \equiv q_2 \equiv q_3 \equiv 3 \pmod 8$.*

The third assertion of the above proposition implies the following theorem which gives conditions to have $\mathrm{Cl}_2(\mathbb{k})$ of type $(2,2)$.

Theorem 2.2. *Let d be an odd negative square free integer. Then $\mathrm{Cl}_2(\mathbb{k})$ is of type $(2,2)$ if and only if d takes one of the following forms:*
(1) *$d = -pq$ for primes $p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$ satisfying $(p/q) = -1$,*
(2) *$d = -pq$ for primes $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$ satisfying $(p/q) = -1$.*

Proof. Let d be an odd negative square free integer such that $d \neq -1$. By the class number formula (see [20]), we have:

$$h_2(\mathbb{k}) = \frac{1}{2}q(\mathbb{k})h_2(2)h_2(2d)h_2(d) = \frac{1}{2}q(\mathbb{k})h_2(2d)h_2(d).$$

We have that $-d\varepsilon_2$ is not a square in $\mathbb{Q}(\sqrt{2})$. In fact, if $-d\varepsilon_2 = \alpha^2$ for some α in $\mathbb{Q}(\sqrt{2})$ then $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(-d\varepsilon_2) = -d^2 = N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha)^2$. So, by [1], Proposition 3, $\{\varepsilon_2\}$ is a fundamental system of units of $\mathbb{k}$. It follows that $q(\mathbb{k}) = 1$ and

$$h_2(\mathbb{k}) = \frac{1}{2}h_2(2d)h_2(d). \tag{1}$$

We discuss each case of d appearing in the previous proposition. Recall that for any prime p' we have $(2/p') = -1$ if and only if $p' \equiv 3 \pmod 8$ or $p' \equiv 5 \pmod 8$.

▷ Suppose that d takes the first form of Proposition 2.1. We have that $h_2(-2p)$ and $h_2(-p)$ are divisible by 4 (see [13]), so by the formula (1), $h_2(\mathbb{k})$ is divisible by 8. Hence this case is eliminated.

- ▷ The second item of Proposition 2.1 is equivalent to the statement: $d = -pq$ with $p \equiv q \equiv 3 \pmod 8$ or $p \equiv q \equiv 5 \pmod 8$. If $p \equiv q \equiv 3 \pmod 8$, then by [14], pages 354 and 356, $h_2(-pq)$ and $h_2(-2pq)$ are divisible by 4 and 8, respectively. If $p \equiv q \equiv 5 \pmod 8$, then by [14], pages 348–350, $h_2(-pq)$ and $h_2(-2pq)$ are divisible by 8 and 4, respectively. It follows by the formula (1) that $h_2(\Bbbk)$ is divisible by 16. Hence this case is eliminated.
- ▷ The third item of Proposition 2.1 is equivalent to the statement: $d = -pq$ with [$p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$] or [$p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$].

  Suppose that, $d = -pq$ with $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$. If $(p/q) = -1$, then by [14], pages 353 and [8], Corollary 19.6, we have $h_2(-2pq) = 4$ and $h_2(-pq) = 2$, so by the formula (1), $h_2(\Bbbk) = 4$. If $(p/q) = 1$, then again by [14], page 353 and [8], Corollary 19.6, $h_2(-2pq)$ and $h_2(-pq)$ are divisible by 8 and 4, respectively. Thus, by formula (1), $h_2(\Bbbk)$ is divisible by 16. Similarly, we show that if $d = -pq$ with $p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$, then $\mathrm{Cl}_2(\Bbbk) \simeq (2, 2)$ if and only if $(p/q) = -1$.
- ▷ The fourth item of Proposition 2.1 is equivalent to the statement: $d = -p_1p_2q$ with $p_1 \equiv p_2 \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$. Thus $h_2(\Bbbk) = \frac{1}{2}h_2(-2p_1p_2q)h_2(-p_1p_2q)$. So by the genus theory of quadratic number fields (see e.g. [14], page 315) $h_2(\Bbbk)$ is divisible by 16.
- ▷ Again by the genus theory of quadratic number fields we eliminate the fifth item of Proposition 2.1 and show that $h_2(\Bbbk)$ is divisible by 16. This completes the proof.

□

By the previous proof we deduce the following corollary.

Corollary 2.3. *Let $d \neq -1$ be an odd negative square free integer and $\Bbbk = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Then $E_\Bbbk = \langle -1, \varepsilon_2 \rangle$ if $d < -3$ and $E_\Bbbk = \langle \zeta_6, \varepsilon_2 \rangle$ if $d = -3$. Thus $q(\Bbbk) = Q_\Bbbk = 1$.*

By [12], one deduces easily the following result.

Proposition 2.4. *Let d be an odd negative square free integer. If $p_1, \ldots, p_r$ are the prime divisors of d, then the genus field of $\Bbbk = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ is*

$$\Bbbk^* = \Bbbk\left(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*}\right)$$

with $p_i^* = (-1)^{(p_i-1)/2}p_i$. In particular, if d takes one of the forms of Theorem 2.2, we infer that $\Bbbk^* = \Bbbk(\sqrt{p}, \sqrt{-q}) = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$.

3. Main results

Let us begin by recalling some points that are necessary for what follows. Let Q_m, D_m, and S_m denote the quaternion, dihedral and semidihedral groups of order 2^m, respectively, where $m \geqslant 3$ and $m \geqslant 4$ for S_m. In addition, let A denote the Klein four-group. Each of these groups is generated by two elements x and y, and admits a representation by generators and relations as follows:

$$\begin{aligned}
A &= \{x, y\colon\ x^2 = y^2 = 1,\ y^{-1}xy = x\},\\
Q_m &= \{x, y\colon\ x^{2^{m-2}} = y^2 = a,\ a^2 = 1,\ y^{-1}xy = x^{-1}\},\\
D_m &= \{x, y\colon\ x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{-1}\},\\
S_m &= \{x, y\colon\ x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{2^{m-2}-1}\}.
\end{aligned}$$

We recall some well known properties of 2-groups G such that G/G' is of type $(2,2)$, where G' denotes the commutator subgroup of G (see for more details [15], pages 272–273 and [9], Chapter 5).

Let k be an algebraic number field and $\mathrm{Cl}_2(k)$ the 2-Sylow subgroup of its ideal class group $\mathrm{Cl}(k)$. Let $k_2^{(1)}$ (or $k_2^{(2)}$) be the first (or second) Hilbert 2-class field of k, respectively. Put $G = \mathrm{Gal}(k_2^{(2)}/k)$, then if G' denotes the commutator subgroup of G, we have by the class field theory $G' \simeq \mathrm{Gal}(k_2^{(2)}/k_2^{(1)})$ and $G/G' \simeq \mathrm{Gal}(k_2^{(1)}/k) \simeq \mathrm{Cl}_2(k)$. Assume in all what follows that $\mathrm{Cl}_2(k)$ is of type $(2,2)$, then it is known that G is isomorphic to A, Q_m, D_m or S_m.

Let x and y be as above. Note that the commutator subgroup G' of G is always cyclic and $G' = \langle x^2\rangle$. The group G possesses exactly three subgroups of index 2 which are

$$H_1 = \langle x\rangle, \quad H_2 = \langle x^2, y\rangle, \quad H_3 = \langle x^2, xy\rangle.$$

Furthermore, if G is isomorphic to A (or Q_3), then the subgroups H_i are cyclic of order 2 (or 4), respectively. If G is isomorphic to Q_m with $m > 3$, D_m or S_m, then H_1 is cyclic and H_i/H_i' is of type $(2,2)$ for $i \in \{2,3\}$, where H_i' is the commutator subgroup of H_i.

Let F_i be the subfield of $k_2^{(2)}$ fixed by H_i, where $i \in \{1,2,3\}$. It is clear that F_1 has a cyclic 2-class group and $k_2^{(2)}$ is exactly the Hilbert 2-class field of F_1 (see the proof of Corollary 3.8 below). If $k_2^{(2)} \neq k_2^{(1)}$, $\langle x^4\rangle$ is the unique subgroup of G' of index 2. Let L (L is defined only if $k_2^{(2)} \neq k_2^{(1)}$) be the subfield of $k_2^{(2)}$ fixed by $\langle x^4\rangle$. Then F_1, F_2 and F_3 are the three quadratic subextensions of $k_2^{(1)}/k$ and L is the unique subfield of $k_2^{(2)}$ such that L/k is a nonabelian Galois extension of degree 8. We first recall the definition of Taussky's conditions A and B, see [19].

Definition 3.1. Let k' be a cyclic unramified extension of a number field k and let j denote the basic homomorphism: $j_{k'/k}\colon \mathrm{Cl}(k) \to \mathrm{Cl}(k')$, induced by the extension of ideals from k to k'. Then:

(1) k'/k satisfies condition A if and only if $|\ker(j_{k'/k}) \cap N_{k'/k}(\mathrm{Cl}(k'))| > 1$.

(2) k'/k satisfies condition B if and only if $|\ker(j_{k'/k}) \cap N_{k'/k}(\mathrm{Cl}(k'))| = 1$.

Set $j_{F_i/k} = j_i$, $i = 1, 2, 3$. Then we have:

Theorem 3.2 ([15], Theorem 2)**.**

(1) *If $k_2^{(1)} = k_2^{(2)}$, then F_i satisfy condition A, $|\ker(j_i)| = 4$ for $i = 1, 2, 3$ and G is abelian of type $(2, 2)$.*

(2) *If $\mathrm{Gal}(L/k) \simeq Q_3$, then F_i satisfy condition A and $|\ker(j_i)| = 2$ for $i = 1, 2, 3$ and $G \simeq Q_3$.*

(3) *If $\mathrm{Gal}(L/k) \simeq D_3$, then F_2, F_3 satisfy condition B and $|\ker j_2| = |\ker j_3| = 2$. Furthermore, if F_1 satisfies condition B, then $|\ker j_1| = 2$ and $G \simeq S_m$; if F_1 satisfies condition A and $|\ker j_1| = 2$ then $G \simeq Q_m$. If F_1 satisfies condition A and $|\ker j_1| = 4$ then $G \simeq D_m$.*

These results are summarized in the following table.

$\lvert\ker j_1\rvert(A/B)$	$\lvert\ker j_2\rvert(A/B)$	$\lvert\ker j_3\rvert(A/B)$	G
4	4	4	$(2, 2)$
$2A$	$2A$	$2A$	Q_3
4	$2B$	$2B$	D_m, $m \geqslant 3$
$2A$	$2B$	$2B$	Q_m, $m > 3$
$2B$	$2B$	$2B$	S_m, $m > 3$

By Theorem 3.2 and group theoretic properties quoted in the beginning of this section, one can easily deduce the following remark.

Remark 3.3. The 2-class groups of the three unramified quadratic extensions of k are cyclic if and only if $k^{(1)} = k^{(2)}$ or $k^{(1)} \neq k^{(2)}$ and $G \simeq Q_3$. In the other cases the 2-class group of only one unramified quadratic extension is cyclic and the other are of type $(2, 2)$.

3.1. First case. In this subsection, we suppose that d takes the second form of Theorem 2.2, i.e.,

$$d = -pq \quad \text{with} \quad p \equiv 1 \pmod 8, \quad q \equiv 3 \pmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1.$$

Let $\Bbbk^*$ be the genus field of $\Bbbk$ and k_1, k_2 two other unramified quadratic extensions of $\Bbbk$.

Lemma 3.4. *Let $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $\Bbbk^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$. Then we have:*

(1) *$\{\varepsilon_p, \varepsilon_2, \sqrt{\varepsilon_{2p}}\}$ is a fundamental system of units of $\Bbbk^*$ if and only if the norm of ε_{2p} is 1.*

(2) *$\{\varepsilon_{2p}, \varepsilon_2, \sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}\}$ is a fundamental system of units of $\Bbbk*$ if and only if the norm of ε_{2p} is -1.*

Proof. Note that the norms of ε_2 and ε_p equal -1. If the norm of ε_{2p} equals 1, then by [7], Théorème 3, $\{\varepsilon_p, \varepsilon_2, \sqrt{\varepsilon_{2p}}\}$ is a fundamental system of units of $\mathbb{Q}(\sqrt{2}, \sqrt{p})$. It follows by [2], Proposition 20, that $\{\varepsilon_p, \varepsilon_2, \sqrt{\varepsilon_{2p}}\}$ is a fundamental system of units of $\Bbbk^*$. Similarly, if the norm of ε_{2p} equals -1, then $\{\sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}, \varepsilon_2, \varepsilon_{2p}\}$ is a fundamental system of units of $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ and by [2], Proposition 22, $\{\sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}, \varepsilon_2, \varepsilon_{2p}\}$ is a fundamental system of units of $\Bbbk^*$. □

Lemma 3.5. *Let $d = -pq$ with $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$. We have: $N_{\Bbbk^*/\Bbbk}(\sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}) = \pm\varepsilon_2$ if $N(\varepsilon_{2p}) = -1$ and $N_{\Bbbk^*/\Bbbk}(\sqrt{\varepsilon_{2p}}) = \pm 1$ if $N(\varepsilon_{2p}) = 1$.*

Proof. We have $N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\varepsilon_p) = -1$. If $N(\varepsilon_{2p}) = -1$, then:

$$\begin{aligned} N_{\Bbbk^*/\Bbbk}(\varepsilon_p\varepsilon_2\varepsilon_{2p}) &= N_{\Bbbk^*/\Bbbk}(\varepsilon_p)N_{\Bbbk^*/\Bbbk}(\varepsilon_2)N_{\Bbbk^*/\Bbbk}(\varepsilon_{2p}) \\ &= \varepsilon_2^2 N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\varepsilon_p)N_{\mathbb{Q}(\sqrt{2p})/\mathbb{Q}}(\varepsilon_{2p}) = \varepsilon_2^2. \end{aligned}$$

Thus $N_{\Bbbk^*/\Bbbk}(\sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}) = \pm\varepsilon_2$. Similarly, if $N(\varepsilon_{2p}) = 1$ then $N_{\Bbbk^*/\Bbbk}(\sqrt{\varepsilon_{2p}}) = \pm 1$. □

Proposition 3.6. *Let $d = -pq$ be such that $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $(p/q) = -1$. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two prime ideals of $\Bbbk = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ lying over p. Then $\mathrm{Cl}_2(\Bbbk)$ is generated by $[\mathcal{P}_1]$ and $[\mathcal{P}_2]$. Furthermore:*

(1) *If the norm of ε_{2p} is -1, then only $[1]$ and $[\mathcal{P}_1\mathcal{P}_2]$ capitulate in $\Bbbk^*$.*

(2) *If the norm of ε_{2p} is 1, then all the classes of $\mathrm{Cl}_2(\Bbbk)$ capitulate in $\Bbbk^*$.*

Proof. Let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}(\sqrt{-pq})$ lying over p. We claim that $\mathfrak{p}$ is not principal, as otherwise, with some $\alpha = x + y\sqrt{-pq} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-pq})}$, we would get $\mathfrak{p} = (\alpha) = (x + y\sqrt{-pq})$, so $N(\mathfrak{p}) = (x^2 + y^2pq)$, yielding that $\pm p = x^2 + y^2pq$. Thus p divides x, hence $\pm 1 = a^2p + y^2q$, where $x = pa$. We deduce that $(q/p) = (p/q) = 1$, which contradicts the fact that $(p/q) = -1$.

On the other hand, as $N_{\Bbbk/\mathbb{Q}(\sqrt{-pq})}(\mathcal{P}_i) = \mathfrak{p}$, so the class $[\mathcal{P}_i]$ is not trivial. To make sure that $\mathcal{P}_1$ and $\mathcal{P}_2$ are not in the same coset, it suffices to prove that $\mathcal{P}_1\mathcal{P}_2$ is not principal. Suppose that $\mathcal{P}_1\mathcal{P}_2$ is principal, i.e., there exists $\beta \in \Bbbk$ such that $\mathcal{P}_1\mathcal{P}_2 = \beta\mathcal{O}_{\Bbbk}$. So $p\mathcal{O}_{\Bbbk} = \mathcal{P}_1^2\mathcal{P}_2^2 = \beta^2\mathcal{O}_{\Bbbk}$. Thus, after modifying the chosen β by the square of unit we get $p\varepsilon_2^e = \pm\beta^2$ for some $e \in \{0, 1\}$. Set $\beta = \beta_1 + \beta_2\sqrt{2}$, $\beta_1, \beta_2 \in \mathbb{Q}(\sqrt{-pq})$. So $p\varepsilon_2^e = \pm(\beta_1^2 + 2\beta_2^2 + 2\beta_1\beta_2\sqrt{2}) = \pm\beta_1^2 \pm 2\beta_2^2 \pm 2\beta_1\beta_2\sqrt{2}$.

If $e = 0$, then $p = \pm\beta_1^2 \pm 2\beta_2^2 \pm 2\beta_1\beta_2\sqrt{2}$ and $\beta_1 = 0$ or $\beta_2 = 0$. It follows that $p = \pm\beta_1^2$ or $p = \pm 2\beta_2^2$, which is impossible. If $e = 1$, then $p(1 + \sqrt{2}) = p + p\sqrt{2} = \pm\beta_1^2 \pm 2\beta_2^2 \pm 2\beta_1\beta_2\sqrt{2}$, so $\pm p = 2\beta_1\beta_2 = \beta_1^2 + 2\beta_2^2$, this implies that $(\beta_1 - \beta_2)^2 = -\beta_2^2$. Thus $\sqrt{-1} = (\beta_1 - \beta_2)/\beta_2 \in \mathbb{Q}(\sqrt{-pq})$, which is impossible, too. Hence $\mathcal{P}_1\mathcal{P}_2$ is not principal. So $[\mathcal{P}_1]$ and $[\mathcal{P}_2]$ generate $\mathrm{Cl}_2(\Bbbk)$.

Since $\sqrt{p} \in \Bbbk^*$ and $p = \sqrt{p}^2$, then $\mathcal{P}_1\mathcal{P}_2$ capitulates in $\Bbbk^*$. As the number of classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate in $\Bbbk^*$ is exactly $[\Bbbk^* : \Bbbk][E_{\Bbbk} : N_{\Bbbk^*/\Bbbk}(E_{\Bbbk^*})] = 2[E_{\Bbbk} : N_{\Bbbk^*/\Bbbk}(E_{\Bbbk^*})]$ (see [11]), then there are two cases to distinguish:

▷ If the norm of ε_{2p} is -1, then by Corollary 2.3 and Lemmas 3.4, 3.5 there are exactly 2 classes that capitulate in $\Bbbk^*$. So the first item follows.

▷ If the norm of ε_{2p} is 1, then by Corollary 2.3 and Lemmas 3.4, 3.5 there are 4 classes of $\mathrm{Cl}_2(\Bbbk)$ that capitulate in $\Bbbk^*$. So the second item follows.

□

In the following proposition, we characterize the structure of a 2-class of $\Bbbk^*$. For this recall, by the ambiguous class number formula (see e.g. [10]), that if F/k is a quadratic extension of number fields such that k has an odd class number, then the rank of the 2-class group F is given by $t - 1 - e$, where e is defined as

$$[E_k : E_k \cap N_{F/k}(F^*)] = 2^e$$

and t is the number of prime ideals of k ramified in F.

Proposition 3.7. *Let $d = -pq$ be such that $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $(p/q) = -1$. Set $\Bbbk^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$. Then the 2-class group of $\Bbbk^*$ is cyclic and $h_2(\Bbbk^*) = h_2(2p)$. Moreover:*

(1) *$h_2(\Bbbk^*) = 2$ if and only if $(2/p)_4 = -(-1)^{(p-1)/8}$. In this case, $N(\varepsilon_{2p}) = 1$.*

(2) *If $(2/p)_4 = (-1)^{(p-1)/8} = -1$, then $h_2(\Bbbk^*) = 4$ and $N(\varepsilon_{2p}) = -1$.*

(3) *If $(2/p)_4 = (-1)^{(p-1)/8} = 1$, then $h_2(\Bbbk^*)$ is divisible by 4 (and $h_2(\Bbbk^*)$ is divisible by 8 whenever $N(\varepsilon_{2p}) = -1$).*

Proof. We have $q(\Bbbk^*) = 2$ by Lemma 3.4, $h_2(-2pq) = 4$ by [14], page 353, $h_2(p) = h_2(-q) = h_2(2) = 1$ by [8], Corollary 18.4 and $h_2(-2q) = h_2(-pq) = 2$ by [8], Corollary 19.6. Thus, by the class number formula (see [20]), we get

$$\begin{aligned} h_2(\Bbbk^*) &= \frac{1}{2^5} q(\Bbbk^*) h_2(p) h_2(2p) h_2(-q) h_2(-2q) h_2(-pq) h_2(-2pq) h_2(2) \\ &= \frac{1}{2^5} \cdot 2 \cdot 1 \cdot h_2(2p) \cdot 1 \cdot 2 \cdot 2 \cdot 4 \cdot 1 = h_2(2p). \end{aligned} \tag{2}$$

Set $k' = \mathbb{Q}(\sqrt{2}, \sqrt{-q})$. As $p\mathcal{O}_{k'} = \mathcal{P}\mathcal{P}'$ in k', then it is easy to see that these two prime ideals are the only ramified primes of $\Bbbk^*/k'$. We have $h_2(k') = 1$, thus by

Kuroda's class number formula (see [17]), Corollary 2.3 and the above settings, we get

$$h_2(k') = \frac{1}{2}q(k')h_2(2)h_2(-2q)h_2(-q) = 1.$$

It follows that the rank of the 2-class group of $\mathbb{k}^*$ is $2-1-e = 1-e$, where e is defined as above for $F = \mathbb{k}^*$ and $k = k'$. Since $h_2(2p)$ is even by [8], Corollary 18.4, then by the equality (2), we have that $e = 0$ and $\mathrm{Cl}_2(\mathbb{k}^*)$ is cyclic. Hence, [16], Theorem 2 completes the proof. □

Corollary 3.8. *Let $d = -pq$ be such that $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $(p/q) = -1$. Then $|G| = 2 \cdot h_2(2p)$.*

P r o o f. Since $\mathbb{k}_2^{(1)}/\mathbb{k}^*$ is an unramified extension, then

$$\mathbb{k} \subset \mathbb{k}^* \subset \mathbb{k}_2^{(1)} \subset \mathbb{k}^{*(1)}_2 \subset \mathbb{k}_2^{(2)} \subset \mathbb{k}^{*(2)}_2.$$

By Proposition 3.7, $\mathrm{Cl}_2(\mathbb{k}^*)$ is cyclic. So the 2-class field tower of $\mathbb{k}^*$ terminates at its Hilbert 2-class field $\mathbb{k}^{*(1)}_2$, i.e., $\mathbb{k}^{*(1)}_2 = \mathbb{k}^{*(2)}_2$, thus $\mathbb{k}^*$ and $\mathbb{k}_2^{(1)}$ have the same Hilbert 2-class field which is $\mathbb{k}_2^{(2)}$. It follows that $|G| = 2 \cdot h_2(\mathbb{k}^*) = 2 \cdot h_2(2p)$. □

Now we are able to state our first main theorem.

Theorem 3.9. *Let $d = -pq$ be such that $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $(p/q) = -1$. Set $\mathbb{k}^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$.*

(1) *If $(2/p)_4 \neq (-1)^{(p-1)/8}$, then all the classes of $\mathrm{Cl}_2(\mathbb{k})$ capitulate in the three unramified quadratic extensions $\mathbb{k}^*$, k_1 and k_2 of $\mathbb{k}$, and G is abelian.*

(2) *If $(2/p)_4 = (-1)^{(p-1)/8} = -1$, then $N(\varepsilon_{2p}) = -1$ and in each field $\mathbb{k}^*$, k_1 and k_2, there are exactly 2 classes of $\mathrm{Cl}_2(\mathbb{k})$, which capitulate, and thus G is the quaternion group of order 8.*

(3) *If $(2/p)_4 = (-1)^{(p-1)/8} = 1$ and $N(\varepsilon_{2p}) = 1$, then $h_2(2p) = 2^m$ with $m \geqslant 2$ and all the classes of $\mathrm{Cl}_2(\mathbb{k})$ capitulate in $\mathbb{k}^*$, and only 2 classes capitulate in each k_1 and k_2, and G is dihedral of order 2^{m+1}.*

(4) *If $(2/p)_4 = (-1)^{(p-1)/8} = 1$ and $N(\varepsilon_{2p}) = -1$, then $h_2(2p) = 2^m$ with $m > 2$ and in each field $\mathbb{k}^*$, k_1 and k_2, there are exactly 2 classes of $\mathrm{Cl}_2(\mathbb{k})$ which capitulate and G is the quaternion group of order 2^{m+1}.*

P r o o f. (1) As $(2/p)_4 \neq (-1)^{(p-1)/8}$, then by Proposition 3.7, $h_2(\mathbb{k}^*) = 2$. Thus by Corollary 3.8, $|G| = 4$. It follows that $\mathbb{k}^{(1)} = \mathbb{k}^{(2)}$. Hence, G is abelian and the four classes of $\mathrm{Cl}_2(\mathbb{k})$ capitulate in $\mathbb{k}^*$, k_1 and k_2.

(2) As the norm of ε_{2p} equals -1, then by Proposition 3.6, $\mathcal{P}_1\mathcal{P}_2$ capitulates in $\mathbb{k}^*$. Since $\mathcal{P}_1$ and $\mathcal{P}_2$ are inert in $\mathbb{k}^*$, then by the Artin reciprocity law $\mathbb{k}^*/\mathbb{k}$ satisfies

condition A. It follows by Proposition 3.7, Corollary 3.8 and Theorem 3.2 that G is a quaternion of order 8 and there are exactly 2 classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate in the three unramified quadratic extensions of $\Bbbk$.

(3) Since the norm of ε_{2p} equals 1, then, by Proposition 3.6, all the classes capitulate in $\Bbbk^*$. Hence by Proposition 3.7, Corollary 3.8 and Theorem 3.2, G is dihedral of order 2^{m+1} and there are exactly 2 classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate in the other unramified quadratic extensions of $\Bbbk$.

(4) The proof of the fourth item is similar to the second one. □

Remark 3.10. Let $d = -pq$ be such that $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $(p/q) = -1$. By Remark 3.3, if p satisfies one of the conditions mentioned in the first and second items of the previous theorem, then $\mathrm{Cl}_2(\Bbbk^*) \simeq \mathbb{Z}/h_2(2p)\mathbb{Z}$, $\mathrm{Cl}_2(k_1)$ and $\mathrm{Cl}_2(k_2)$ are cyclic, otherwise $\mathrm{Cl}_2(\Bbbk^*) \simeq \mathbb{Z}/h_2(2p)\mathbb{Z}$ and $\mathrm{Cl}_2(k_1) \simeq \mathrm{Cl}_2(k_2) \simeq (2,2)$.

3.2. Second case.

3.2. Second case. In this subsection, we suppose that d takes the first form of Theorem 2.2, i.e.,

$$d = -pq \quad \text{with} \quad p \equiv 5 \pmod 8, \quad q \equiv 7 \pmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1.$$

Denote always by $\Bbbk^*$ the genus field of $\Bbbk$ and by k_1, k_2 two other unramified quadratic extensions of $\Bbbk$.

Lemma 3.11. *Let $d = -pq$ with $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$ and $\Bbbk^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$. Then, $\{\varepsilon_2, \varepsilon_{2p}, \sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}\}$ is a fundamental system of units of $\Bbbk^*$ and $N_{\Bbbk^*/\Bbbk}(\sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}) = \pm\varepsilon_2$.*

P r o o f. It is known that the norms of ε_2, ε_p, ε_{2p} equal -1. On the other hand, since $\{\varepsilon_2, \varepsilon_{2p}, \sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}\}$ is a fundamental system of units of $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ (see [6], Théorème 6), thus, by [2], Proposition 22, $\{\varepsilon_2, \varepsilon_{2p}, \sqrt{\varepsilon_p\varepsilon_2\varepsilon_{2p}}\}$ is a fundamental system of units of $\Bbbk^*$. □

Proposition 3.12. *Let $d = -pq$ with $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$ and $(p/q) = -1$, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two prime ideals of $\Bbbk$ lying over q. Then $\mathrm{Cl}_2(\Bbbk)$ is generated by $[\mathcal{Q}_1]$ and $[\mathcal{Q}_2]$. Furthermore, the classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate in $\Bbbk^*$ are $[1]$ and $[\mathcal{Q}_1\mathcal{Q}_2]$.*

P r o o f. By considering $\mathfrak{q}$, the prime ideal of $\mathbb{Q}(\sqrt{-pq})$ lying over q, we proceed as in Proposition 3.6 to prove that $[\mathcal{Q}_1]$ and $[\mathcal{Q}_2]$ generate $\mathrm{Cl}_2(\Bbbk)$. The number of classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate in $\Bbbk^*$ is exactly $[\Bbbk^* : \Bbbk][E_\Bbbk : N_{\Bbbk^*/\Bbbk}(E_{\Bbbk^*})] =$

$2[E_{\Bbbk} : N_{\Bbbk^*/\Bbbk}(E_{\Bbbk^*})]$ (see [11]). As $\sqrt{-q} \in \Bbbk^*$ and $-q = \sqrt{-q}^2$, then $\mathcal{Q}_1\mathcal{Q}_2$ capitulates in $\Bbbk^*$. By Corollary 2.3 and Lemma 3.11, we have $[\Bbbk^* : \Bbbk][E_{\Bbbk} : N_{\Bbbk^*/\Bbbk}(E_{\Bbbk^*})] = 2$. So the statemment holds. □

The following proposition gives the structure of the 2-class group of $\Bbbk^*$.

Proposition 3.13. *Let $d = -pq$ with $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$ and $(p/q) = -1$. Let $\Bbbk^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$, then the 2-class group of $\Bbbk^*$ is cyclic and $h_2(\Bbbk^*) = h_2(-2q)$. Furthermore, $\mathrm{Cl}_2(\Bbbk^*) = \mathbb{Z}/4\mathbb{Z}$ if and only if $q \equiv 7 \pmod{16}$.*

Proof. We have $q(\Bbbk^*) = 2$, $h_2(2p) = 2$, $h_2(-pq) = 2$, $h_2(p) = h_2(-q) = h_2(2) = 1$ and $h_2(-2pq) = 4$ by Lemma 3.11, [8], Corollaries 19.8, 19.6, 18.4 and [14], page 353, respectively. Then, the class number formula (see [20]) gives

$$\begin{aligned} h_2(\Bbbk^*) &= \frac{1}{2^5} q(\Bbbk^*) h_2(p) h_2(2p) h_2(-q) h_2(-2q) h_2(-pq) h_2(-2pq) h_2(2) \\ &= \frac{1}{2^5} \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot h_2(-2q) \cdot 2 \cdot 4 \cdot 1 = h_2(-2q). \end{aligned}$$

As q decomposes into the product of two prime ideals of $k' = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ and $h_2(k') = 1$ (see [8], Proposition 21.5), then by the ambiguous class number formula (see [10]), the rank of the 2-class group of $\Bbbk^*$ is $2 - 1 - e = 1 - e$. Since $h_2(-2q)$ is even (see [8], Corollary 18.4) then $e = 0$. Thus, $\mathrm{Cl}_2(\Bbbk^*)$ is cyclic. We have that $h_2(-2q)$ is divisible by 4 (see [8], Corollary 19.6) and $h_2(-2q)$ is divisible by 8 if and only if $q \equiv -1 \pmod{16}$ (see [13], Théorème 4), so the result follows. □

In a way similar to Corollary 3.8 and Theorem 3.9, we prove our second main result.

Theorem 3.14. *Let $d = -pq$ be such that $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$ and $(p/q) = -1$. Let $\Bbbk^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q})$, k_1 and k_2 be the three quadratic unramified extensions of $\Bbbk$. Set $h_2(-2q) = 2^m$, $m \geqslant 2$, then in each field $\Bbbk^*$, k_1 and k_2, there are exactly two ideal classes of $\mathrm{Cl}_2(\Bbbk)$ which capitulate. Thus G is the quaternion group of order 2^{m+1}.*

By Proposition 3.13, Theorem 3.14 and Remark 3.3, we easily deduce the following remark.

Remark 3.15. Let $d = -pq$ be such that $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$ and $(p/q) = -1$. If $q \equiv 7 \pmod{16}$, then $\mathrm{Cl}_2(\Bbbk^*) \simeq \mathbb{Z}/4\mathbb{Z}$, $\mathrm{Cl}_2(k_1)$, and $\mathrm{Cl}_2(k_2)$ are cyclic, otherwise $\mathrm{Cl}_2(\Bbbk^*) \simeq \mathbb{Z}/h_2(-2q)\mathbb{Z}$ and $\mathrm{Cl}_2(k_1) \simeq \mathrm{Cl}_2(k_2) \simeq (2, 2)$.

Acknowledgment. We would like to thank the unknown referee for his/her several helpful suggestions and for calling our attention to the missing details.

[1] *A. Azizi*: Unités de certains corps de nombres imaginaires et abéliens sur $\mathbb{Q}$. Ann. Sci. Math. Qué. *23* (1999), 15–21. (In French.) zbl MR

[2] *A. Azizi*: Sur les unités de certains corps de nombres de degré 8 sur $\mathbb{Q}$. Ann. Sci. Math. Qué. *29* (2005), 111–129. (In French.) zbl MR

[3] *A. Azizi, I. Benhamza*: Sur la capitulation des 2-classes d'idéaux de $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$. Ann. Sci. Math. Qué. *29* (2005), 1–20. (In French.) zbl MR

[4] *A. Azizi, M. M. Chems-Eddin, A. Zekhnini*: On the rank of the 2-class group of some imaginary triquadratic number fields. Available at `https://arxiv.org/abs/1905.01225` (2019), 21 pages.

[5] *A. Azizi, A. Mouhib*: Capitulation des 2-classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{d})$ où d est un entier naturel sans facteurs carrés. Acta Arith. *109* (2003), 27–63. (In French.) zbl MR doi

[6] *A. Azizi, M. Talbi*: Capitulation des 2-classes d'idéaux de certains corps biquadratiques cycliques. Acta Arith. *127* (2007), 231–248. (In French.) zbl MR doi

[7] *A. Azizi, M. Taous*: Capitulation des 2-classes d'idéaux de $k = \mathbb{Q}(\sqrt{2p}, i)$. Acta Arith. *131* (2008), 103–123. (In French.) zbl MR doi

[8] *P. E. Conner, J. Hurrelbrink*: Class Number Parity. Series in Pure Mathematics 8. World Scientific, Singapore, 1988. zbl MR doi

[9] *D. Gorenstein*: Finite Groups. Harper's Series in Modern Mathematics. Harper and Row, New York, 1968. zbl MR

[10] *G. Gras*: Sur les ℓ-classes d'idéaux dans les extensions cycliques rélatives de degré premier ℓ. I. Ann. Inst. Fourier *23* (1973), 1–48. (In French.) zbl MR doi

[11] *F.-P. Heider, B. Schmithals*: Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen. J. Reine Angew. Math. *336* (1982), 1–25. (In German.) zbl MR doi

[12] *M. Ishida*: The Genus Fields of Algebraic Number Fields. Lecture Notes in Mathematics 555. Springer, Berlin, 1976. zbl MR doi

[13] *P. Kaplan*: Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique. J. Math. Soc. Japan *25* (1973), 596–608. (In French.) zbl MR doi

[14] *P. Kaplan*: Sur le 2-groupe des classes d'idéaux des corps quadratiques. J. Reine. Angew. Math. *283-284* (1976), 313–363. (In French.) zbl MR doi

[15] *H. Kisilevsky*: Number fields with class number congruent to 4 (mod 8) and Hilbert's Theorem 94. J. Number Theory *8* (1976), 271–279. zbl MR doi

[16] *R. Kučera*: On the parity of the class number of a biquadratic field. J. Number Theory *52* (1995), 43–52. zbl MR doi

[17] *F. Lemmermeyer*: Kuroda's class number formula. Acta Arith. *66* (1994), 245–260. zbl MR doi

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

[19] *O. Taussky*: A remark concerning Hilbert's Theorem 94. J. Reine Angew. Math. *239–240* (1969), 435–438. zbl MR doi

[20] *H. Wada*: On the class number and the unit group of certain algebraic number fields. J. Fac. Sci., Univ. Tokyo, Sect. I *13* (1966), 201–209. zbl MR

Authors' addresses: Mohamed Mahmoud Chems-Eddin, Abdelmalek Azizi, Mohammed First University, Mathematics Department, Sciences Faculty, Mohammed V Avenue, P. O. Box 524, Oujda 60000, Morocco, e-mail: 2m.chemseddin@gmail.com, abdelmalekazizi@yahoo.fr; Abdelkader Zekhnini (corresponding author), Mohammed First University, Mathematics Department, Pluridisciplinary Faculty, B.P. 300, Selouane, Nador 62700, Morocco, e-mail: zekha1@yahoo.fr; Idriss Jerrari, Mohammed First University, Mathematics Department, Sciences Faculty, Mohammed V Avenue, P. O. Box 524, Oujda 60000, Morocco, e-mail: idriss_math@hotmail.fr.