ON THE GENERATORS OF
THE 2-CLASS GROUP OF THE FIELD $\mathbb{Q}(\sqrt{d}, i)$

Abdelmalek Azizi$^1$, Abdelkader Zekhnini$^2$§, Mohammed Taous$^3$

Department of Mathematics
Faculty of Science
Mohammed First University
Oujda, MOROCCO

$^3$Department of Mathematics
Faculty of Science and Technology
Moulay Ismail University
Errachidia, MOROCCO

Abstract: Let $d$ be a square free integer such that the 2-class group of the field $\mathbb{Q}(\sqrt{d}, i)$ is of type $(2, 2, 2)$. In this paper we give the generators of the 2-class group of $\mathbb{Q}(\sqrt{d}, i)$.

AMS Subject Classification: 11R37, 11R27, 11R29
Key Words: class group of type $(2,2,2)$, Hilbert class field

1. Introduction

Let $k = \mathbb{Q}(\sqrt{d}, i)$, where $d$ is a square free integer, we denote by $C_{k,2}$ the 2-class group of $k$; let $p, p_1$ and $p_2$ (resp. $q, q_1$ and $q_2$) be prime integers congruent to 1 (resp. 3) (mod 4). According to [3], $C_{k,2}$ is of type $(2, 2, 2)$ if and only if $d$ is one of the following forms:

Received: August 1, 2012

§Correspondence author
(1) $d = p_1 p_2$, where \( \left( \frac{p_1}{p_2} \right) = -1 \), \( p_1 \equiv p_2 \equiv 1 \pmod{8} \) and \( \left( \frac{2}{a+b} \right) = -1 \) with \( p_1 p_2 = a^2 + b^2 \).

(2) $d = 2p_1 p_2$, where \( p_1 \equiv p_2 \equiv 1 \pmod{4} \) and at least two elements of \( \{ \left( \frac{2}{p_1} \right), \left( \frac{2}{p_2} \right), \left( \frac{p_1}{p_2} \right) \} \) are equal to -1.

(3) $d = 2pq$, where \( p \equiv 1 \), \( q \equiv 3 \pmod{8} \) and \( \left( \frac{p}{q} \right) = -1 \).

(4) $d = pq_1 q_2$, where \( p, q_1, q_2 \) satisfy the conditions \( A \) and \( B \):

\[
A : p \equiv -q_1 \equiv -q_2 \equiv 1 \pmod{4} \) and \( \left( \frac{2}{p} \right) = \left( \frac{q_1}{q_2} \right) = - \left( \frac{q_2}{q_1} \right) = 1.
\]

\[
B : \text{One of the following three conditions is satisfied:}
\]

(I) \( \left( \frac{p}{q_1} \right) \left( \frac{p}{q_2} \right) = -1 \) and \( \left( \frac{2}{q_1} \right) = \left( \frac{2}{q_2} \right) = -1 \).

(II) \( \left( \frac{p}{q_1} \right) \left( \frac{p}{q_2} \right) = -1 \), \( \left( \frac{2}{q_1} \right) = 1 \) and \( \left( \frac{2}{q_2} \right) = -1 \).

(III) \( \left( \frac{p}{q_1} \right) = \left( \frac{p}{q_2} \right) = -1 \) and \( \left( \frac{2}{q_1} \right) \left( \frac{2}{q_2} \right) = -1 \).

(5) $d = p_1 p_2 q$, where \( p_1 \equiv p_2 \equiv 1 \pmod{4} \), \( p_1 \) or \( p_2 \equiv 5 \pmod{8} \) and at least two elements of \( \{ \left( \frac{p_1}{p_2} \right), \left( \frac{p_1}{q} \right), \left( \frac{p_2}{q} \right) \} \) are equal to -1.

In the case where \( d = p_1 p_2 q \), we adopt the following definitions:

(i) \( p_1, p_2 \) and \( q \) are called of type I if one of the following conditions holds:

a) \( \left( \frac{2}{p_1} \right) = 1 \) and \( \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{p_2} \right) = \left( \frac{p_1}{q} \right) = -1 \).

b) \( \left( \frac{2}{p_1} \right) = \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{p_2} \right) = \left( \frac{p_2}{q} \right) = -1 \) and \( \left( \frac{p_1}{q} \right) = 1 \).

c) \( \left( \frac{2}{p_1} \right) = \left( \frac{p_1}{p_2} \right) = 1 \) and \( \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{q} \right) = \left( \frac{p_2}{q} \right) = -1 \).

(ii) \( p_1, p_2 \) and \( q \) are called of type II if one of the following conditions is satisfied:

a) \( \left( \frac{2}{p_1} \right) = 1 \) and \( \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{p_2} \right) = \left( \frac{p_2}{q} \right) = -1 \).

b) \( \left( \frac{2}{p_1} \right) = \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{p_2} \right) = \left( \frac{p_1}{q} \right) = -1 \) and \( \left( \frac{p_2}{q} \right) = 1 \).

(III) \( p_1, p_2 \) and \( q \) are called of type III if one of the following conditions is satisfied:

a) \( \left( \frac{2}{p_1} \right) = \left( \frac{2}{p_2} \right) = \left( \frac{p_1}{q} \right) = \left( \frac{p_2}{q} \right) = -1 \).
result it is a deduction from theorems 1, 2, 3 and 4:

\[ C \Rightarrow \text{integer}, \]

In this paper we are interested to give the generators of \( C_{k,2} \) and our main result it is a deduction from theorems 1, 2, 3 and 4:

**Theorem (Main Result).** Let \( k = \mathbb{Q}(\sqrt{d}, i) \), where \( d \) is a square free integer, \( C_{k,2} \) the 2-class group of \( k \). Suppose \( C_{k,2} \) is of type \((2, 2, 2)\), then we have:

1. If \( d \) is of the form (1), then \( C_{k,2} = \langle [H_0^{\frac{h(d)}{2}}], [H_1], [H_2] \rangle \), where \( H_0, H_1 \) and \( H_2 \) are prime ideals in \( k \) above 2 and \( p_1 \) respectively and \( h(d) \) the class number of \( \mathbb{Q}(\sqrt{d}) \).

2. If \( d \) is of the form (2) or (3), then \( C_{k,2} = \langle [H_0], [H_1], [H_2] \rangle \), where \( H_0 \) is the prime ideal in \( k \) above 2 and \( H_1, H_2 \) are prime ideals in \( k \) above \( p_1 \) (resp. \( p \)) if \( d \) takes the form (2) (resp. (3)).

3. Assume \( d \) is of the form (4), let \( H_1, H_2 \) (resp. \( Q_1, Q_2 \)) be prime ideals in \( k \) above \( p \) (resp. \( q_1, q_2 \)), then:
   
   (i) If \( p, q_1 \) and \( q_2 \) satisfy \( B \) (I) or \( B \) (II) and \( \left( \frac{p}{q_1} \right) = -\left( \frac{p}{q_2} \right) = 1 \), then \( C_{k,2} = \langle [H_1], [H_2], [Q_2] \rangle \).
   
   (ii) Else, \( C_{k,2} = \langle [H_1], [H_2], [Q_1] \rangle \).

4. Suppose \( d \) is of the form (5), let \( H_1, H_2 \) (resp. \( H_3, H_4 \)) be prime ideals in \( k \) above \( p_1 \) (resp. \( p_2 \)), then:

   (i) If \( p_1, p_2 \) and \( q \) are of type I, then \( C_{k,2} = \langle [H_1], [H_3], [H_4] \rangle \).
   
   (ii) If \( p_1, p_2 \) and \( q \) are of type II or of type III, then \( C_{k,2} = \langle [H_1], [H_2], [H_3] \rangle \).

2. Generators of \( C_{k,2} \)

First we give some results that will be useful later.

**Proposition 1.** Let \( d \) be a square free integer, \( k = \mathbb{Q}(\sqrt{d}, i) \), \( a + ib \) an element of \( \mathbb{Z}(i) \) and \( H \) an ideal of \( k \) such that \( H^2 = (a + ib) \). Let \( \varepsilon_d = x + y\sqrt{d} \) be the fundamental unit of \( \mathbb{Q}(\sqrt{d}) \). So:

1. If \( \sqrt{a^2 + b^2} \notin \mathbb{Q}(\sqrt{d}) \), then \( H \) is not principal in \( k \).
2. If \( a^2 + b^2 = d \), then we have:
(a) If the norm of $\varepsilon_d$ is 1, then $\mathcal{H}$ is not principal in $k$.

(b) If the norm of $\varepsilon_d$ is -1, then:

(i) If $(ax \pm yd) \pm b$ or $2(-xb \pm yd) \pm a$ is a square in $\mathbb{N}$, then $\mathcal{H}$ is principal in $k$.

(ii) Else $\mathcal{H}$ is not principal in $k$.

Proof. Let $a + ib$ be an element of $\mathbb{Z}[i]$ and $\mathcal{H}$ an ideal of $k$ such that $\mathcal{H}^2 = (a + ib)$. We suppose that $\mathcal{H}$ is principal, then there exist $\alpha \in k$ and a unit $\varepsilon$ in $k$ such that: $\alpha^2 = (a + ib)\varepsilon$ (1). Let $\varepsilon_d$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$, then a fundamental system of units (UFS) of $k$ is $\{\varepsilon_d\}$ or $\{\sqrt{i}\varepsilon_d\}$; in the later case $\varepsilon_d$ is of norm 1. It comes down to cases $\varepsilon \in \{\pm 1, \pm i, \varepsilon_d, i\varepsilon_d\}$ or $\varepsilon \in \{\pm 1, \pm i, \varepsilon_d, i\varepsilon_d\}$.

(1) Suppose that $\sqrt{a^2 + b^2} \notin \mathbb{Q}(\sqrt{d})$, then we have:

(i) If $\varepsilon \in \{\pm 1, \pm i, \varepsilon_d, i\varepsilon_d\}$, then by applying the norm $N_{\mathbb{K}/\mathbb{Q}(\sqrt{d})}$ to Equation (1), we find that $\sqrt{a^2 + b^2} \notin \mathbb{Q}(\sqrt{d})$, which is not the case.

(ii) If $\varepsilon = \sqrt{i\varepsilon_d}$ or $\varepsilon = i\sqrt{i\varepsilon_d}$, then the norm $N_{\mathbb{K}/\mathbb{Q}(i)}$ applied to Equation (1), imply that $\sqrt{i} \in \mathbb{Q}(i)$, which is absurd. So $\mathcal{H}$ is not principal in $k$.

(2) Suppose that $a^2 + b^2 = d$, then we have:

(i) If $\varepsilon = 1$, so by putting $\alpha = \alpha_1 + i\alpha_2$, where $\alpha_1, \alpha_2$ are in $\mathbb{Q}(\sqrt{d})$, Equation (1) imply that

$$\begin{cases}
\alpha_1^2 - \alpha_2^2 = a, \\
2\alpha_1\alpha_2 = b;
\end{cases}
\Leftrightarrow
\begin{cases}
\alpha_1^4 - 4a\alpha_1^2 - b^2 = 0, \\
\alpha_2 = \frac{b}{2\alpha_1};
\end{cases}$$

and $\Delta' = 4d$, where $\Delta'$ is the discriminant of equation (•) for the unknown $\alpha_1^2$, thus $\alpha_1^2 = \frac{1}{2}(a \pm \sqrt{d})$, therefore equation (•) admits solution if and only if $2(a \pm \sqrt{d})$ is a square in $\mathbb{Q}(\sqrt{d})$, hence there exist $s, t$ in $\mathbb{Q}$ such that $2(a \pm \sqrt{d}) = (s + t\sqrt{d})^2 = s^2 + t^2d + 2st\sqrt{d}$, which is equivalent to:

$$\begin{cases}
s^4 - 2as^2 + d = 0, \\
t = \frac{\pm b}{s};
\end{cases}$$

and $\Delta' = a^2 - d = -b^2$, as $\Delta' < 0$, then $2(a \pm \sqrt{d})$ is not a square in $\mathbb{Q}(\sqrt{d})$. Similar proof if $\varepsilon = -1$.

(ii) Let $\varepsilon = \pm i$. So equation (1) is solvable if and only if $2(\pm b \pm \sqrt{d})$ is a square in $\mathbb{Q}(\sqrt{d})$, but this gives us a negative discriminant $\Delta = -a^2$.

(iii) Let $\varepsilon = \varepsilon_d$, then from Equation (1), there exist $\alpha_1, \alpha_2$ in $\mathbb{Q}(\sqrt{d})$ such that:
ON THE GENERATORS OF...

\[
\begin{align*}
\alpha_1^2 - \alpha_2^2 &= a_1 \varepsilon_d, \\
2\alpha_1 \alpha_2 &= b_1 \varepsilon_d; \\
\alpha_2 &= \frac{b_2 \varepsilon_d}{2\alpha_1};
\end{align*}
\]

\(\alpha_1^2 = \frac{\varepsilon_d}{2}(a \pm \sqrt{d})\), thus equation (\(*\)) admits solution if and only if \(2\varepsilon_d(a \pm \sqrt{d})\) is a square in \(\mathbb{Q}(\sqrt{d})\) i.e. if and only if there exist \(s, t\) in \(\mathbb{Q}\) such that: \(2\varepsilon_d(a \pm \sqrt{d}) = (s + t\sqrt{d})^2 = s^2 + t^2d + 2st\sqrt{d}\), as \(\varepsilon_d = x + y\sqrt{d}\), so:

\[
\begin{align*}
s^2 + t^2d &= 2xa \pm 2yd, \\
st &= ya \pm x;
\end{align*}
\]

thus \(\Delta' = 4\varepsilon_d^2d\), so \(\alpha_1 = \varepsilon_d\alpha_2\), and \(\Delta' = 4\varepsilon_d^2d\), so the discriminant of equation (\(*\)) is:

\[
\Delta' = (ax \pm yd)^2 - (ya \pm x)^2d = (a^2 - d)(x^2 - y^2d) = -b^2(x^2 - y^2d).
\]

— If the norm of \(\varepsilon_d\) is 1, then equation (\(*\)) has no solution.
— If the norm of \(\varepsilon_d\) is -1, then \(s^2 = (ax \pm yd) \pm b\). Hence equation (\(*\)) admits solution if and only if \((ax \pm yd) \pm b\) is a square in \(\mathbb{N}\).

(iv) Let \(\varepsilon = \varepsilon_d\), then by the same way we find similar results:
— If the norm of \(\varepsilon_d\) is 1, then there is no solutions.
— If the norm of \(\varepsilon_d\) is -1, then there is a solution if and only if \((ax \pm yd) \pm b\) is a square in \(\mathbb{N}\).

(v) If \(\varepsilon = \sqrt{i\varepsilon_d}\) or \(\varepsilon = i\sqrt{i\varepsilon_d}\), as in the case (1) we find that \(i\) is a square in \(\mathbb{Q}(i)\), which is absurd. \(\square\)

We proceed in the same way to prove the following result:

**Proposition 2.** Let \(d\) be a composite integer, even, square free and product at least of three prime numbers, \(k = \mathbb{Q}(\sqrt{d}, i)\), \(p\) a prime number and \(\mathcal{H}\) an ideal of \(k\) such that \(\mathcal{H}^2 = (p)\). Let \(\varepsilon_d = x + y\sqrt{d}\) be the fundamental unit of \(\mathbb{Q}(\sqrt{d})\). Then we have:

1. If the norm of \(\varepsilon_d\) is -1, so \(\mathcal{H}\) is not principal in \(k\).
2. If the norm of \(\varepsilon_d\) is 1, we have:
   1. If \(\{\varepsilon_d\}\) is UFS of \(k\), then \(\mathcal{H}\) is principal if and only if \(2p(x \pm 1)\) or \(p(x \pm 1)\) is a square in \(\mathbb{N}\).
   2. If not \(\mathcal{H}\) is not principal in \(k\).

**Remark 1.** Proposition 2 holds if \(d\) is a composite integer, odd, square free and product at least of three prime numbers and \(\mathcal{H}^2 = (p)\) or \(\mathcal{H}^2 = (pq)\), where \(p\) and \(q\) are prime numbers.
2.1. Generators of $C_{k,2}$ when $d$ is Even

If $d$ is even, then it is of the form (2) or (3); so $p_1$ (resp. $p$) splits in $\mathbb{Q}(i)$ in product of two primes which we denote by $\pi_1$ and $\pi_2$.

**Theorem 1.** Let $k = \mathbb{Q}(\sqrt{d}, i)$, where $d$ is of the form (2) or (3) and $C_{k,2}$ be the 2-class group of $k$. We denote by $\mathcal{H}_0$, $\mathcal{H}_1$ and $\mathcal{H}_2$ the prime ideals of $k$ laying above $1 + i$, $\pi_1$ and $\pi_2$ respectively, then $C_{k,2} = \langle [\mathcal{H}_0], [\mathcal{H}_1], [\mathcal{H}_2] \rangle$.

**Proof.** For both forms (2) and (3), the numbers $\pi_1$ and $\pi_2$ are ramified primes in $k/\mathbb{Q}(i)$, then there exist $\mathcal{H}_1$ and $\mathcal{H}_2$ prime ideals in $k$ such that: $\pi_j \mathcal{O}_k = (\pi_j) = \mathcal{H}_j^2$, ($j \in \{1,2\}$), where $\mathcal{O}_k$ is the ring of integers of $k$; on the other hand, 2 is totally ramified in $k$, hence there exists $\mathcal{H}_0$ an ideal prime of $k$ such that $\mathcal{H}_0^2 = (1 + i)\mathcal{O}_k$.

According to [3], if $d$ is of the form (3) (resp. (2)), then the norm of the fundamental unit of $\mathbb{Q}(\sqrt{d})$ is 1 (resp. -1) and the unit index of $k$ is 2 (resp. 1), so as $(\mathcal{H}_1 \mathcal{H}_2)^2 = (p_1)$ or $(p)$, Proposition 2 claims that $\mathcal{H}_1 \mathcal{H}_2$ is not principal in $k$; moreover if we put $p$ or $p_1 = e^2 + 4f^2$, we find that $\mathcal{H}_0^2 = (1+i)$, $\mathcal{H}_1^2 = (e+2if)$ and $\mathcal{H}_2^2 = (e-2if)$, as $\sqrt{2} \notin \mathbb{Q}(\sqrt{d})$ and $\sqrt{e^2 + (\pm 2f)^2} = \sqrt{p_1} \notin \mathbb{Q}(\sqrt{d})$, then Proposition 1 states that $\mathcal{H}_0$, $\mathcal{H}_1$ and $\mathcal{H}_2$ are of order 2 in $k$; similar with the same argument we proof that $\mathcal{H}_0 \mathcal{H}_1$, $\mathcal{H}_0 \mathcal{H}_2$ and $\mathcal{H}_0 \mathcal{H}_1 \mathcal{H}_2$ are of order 2 in $k$. This completes the proof. \qed

**Numerical Examples 1.** $d$ is of the form (2).

<table>
<thead>
<tr>
<th>$d$</th>
<th>$2,p_1,p_2$</th>
<th>$\left(\frac{2}{p_1}\right)$</th>
<th>$\left(\frac{2}{p_2}\right)$</th>
<th>$\left(\frac{p_1}{p_2}\right)$</th>
<th>$\mathcal{H}_0$</th>
<th>$\mathcal{H}_1$</th>
<th>$\mathcal{H}_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>130</td>
<td>2.13.35</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$[1,0,1]$</td>
<td>$[0,0,1]$</td>
<td>$[0,1,1]$</td>
</tr>
<tr>
<td>754</td>
<td>2.29.13</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$1$</td>
<td>$[0,1,1]$</td>
<td>$[5,0,1]$</td>
<td>$[5,0,0]$</td>
</tr>
<tr>
<td>986</td>
<td>2.17.29</td>
<td>$1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$[0,0,1]$</td>
<td>$[0,1,0]$</td>
<td>$[11,0,0]$</td>
</tr>
<tr>
<td>1066</td>
<td>2.13.41</td>
<td>$-1$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$[5,1,0]$</td>
<td>$[5,0,1]$</td>
<td>$[5,1,1]$</td>
</tr>
</tbody>
</table>

$d$ take the form (3).

<table>
<thead>
<tr>
<th>$d = 2.p.q$</th>
<th>$\left(\frac{2}{q}\right)$</th>
<th>$\mathcal{H}_0$</th>
<th>$\mathcal{H}_1$</th>
<th>$\mathcal{H}_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>246</td>
<td>$-1$</td>
<td>$[3,1,0]$</td>
<td>$[3,0,0]$</td>
<td>$[3,1,1]$</td>
</tr>
<tr>
<td>374</td>
<td>$-1$</td>
<td>$[7,0,0]$</td>
<td>$[0,1,1]$</td>
<td>$[7,1,0]$</td>
</tr>
</tbody>
</table>

2.2. Generators of $C_{k,2}$ when $d = p_1p_2$

Suppose $d$ is of the form (1), defined in the introduction. We adopt that $p_k$ denotes an ideal of a number field $k$ above a prime number $p$. We need some
lemmas.

**Lemma 1.** Let \( k = \mathbb{Q}(\sqrt{d}, i) \), where \( d = p_1p_2 = a^2 + b^2 \), \( p_1 \equiv p_2 \equiv 1 \pmod{8} \) and \( \mathcal{H}_0 \) be the prime ideal of \( k \) above \( 1+i \). If \( (\frac{2}{a+b}) = -1 \), then for all odd integer \( n \), \( \mathcal{H}_0^n \) is not principal ideal of \( k \).

**Proof.** Suppose \( \mathcal{H}_0' \) is principal in \( k \), for some odd integer \( n \), so there exists \( \alpha = \alpha_1 + \sqrt{d}\alpha_2 \in k \) such that \( \alpha_1 \) are in \( \mathbb{Q}(i) \) and \( \mathcal{H}_0' = \alpha \mathcal{O}_k \). As \( p_1 \equiv p_2 \equiv 1 \pmod{8} \), so \( 1+i \) splits in \( k/\mathbb{Q}(i) \), hence there exists a prime ideal \( \mathcal{H}_0' \) in \( k \) above \( 1+i \) such that \( \mathcal{H}_0\mathcal{H}_0' = (1+i)\mathcal{O}_k \). This allows us to write: \( (1+i)^n = \varepsilon(\alpha_1^2 - d\alpha_2^2) \), with \( \varepsilon \) is a unit of \( \mathbb{Q}(i) \). As \( \alpha_1^2 \) are squares in \( \mathbb{Q}(i) \) and \( n \) is odd, then according to [6, p. 154] and [7, p. 323] we find that:

\[
\left( \frac{1+i}{p_{\mathcal{Q}(i)}} \right) = \left( \frac{\varepsilon}{p_{\mathcal{Q}(i)}} \right) = \left( \frac{2}{p_1} \right)^4 \left( \frac{p_1}{2} \right) = \left( \frac{2}{p_2} \right)^4 \left( \frac{p_2}{2} \right) = 1.
\]

Using this result and according to [7, p. 323] we have \( (\frac{2}{a+b}) = 1 \), which contradicts our hypothesis. \( \square \)

**Lemma 2.** Let \( p_1 \) and \( p_2 \) be two prime numbers such that \( p_1 \equiv p_2 \equiv 1 \pmod{8} \), \( (\frac{p_1}{p_2}) = -1 \) and \( h(d) \) be the class number of \( \mathbb{Q}(\sqrt[p_1]{p_2}) \), then:

(i) The 2-class group of \( \mathbb{Q}(\sqrt[p_1]{p_2}) \) is generated by the class of \( p_1\mathbb{Q}(\sqrt[p_1]{p_2}) \);

(ii) The ideal \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} \) is principal.

**Proof.** (i) Since \( (\frac{p_1}{p_2}) = -1 \), then according to [4] the norm of the fundamental unit of the \( \mathbb{Q}(\sqrt[p_1]{p_2}) \) is equal to \( -1 \) and it’s 2-class number is 2, therefore the 2-class group of \( \mathbb{Q}(\sqrt[p_1]{p_2}) \) is cyclic of order 2. As \( p_1 \) is ramified in \( \mathbb{Q}(\sqrt[p_1]{p_2})/\mathbb{Q} \), so \( p_1\mathcal{O}_{\mathbb{Q}(\sqrt[p_1]{p_2})} = p_1^2 \mathcal{O}_{\mathbb{Q}(\sqrt[p_1]{p_2})} \) and \( p_1\mathcal{O}_{\mathbb{Q}(\sqrt[p_1]{p_2})} \) is a non-principal ideal, if not there exists \( \varepsilon \), unit of \( \mathbb{Q}(\sqrt[p_1]{p_2}) \), such that \( p_1\varepsilon \) is square in \( \mathbb{Q}(\sqrt[p_1]{p_2}) \), this yields that \( p_1\varepsilon \equiv p_1 \pmod{2} \), \( \varepsilon \equiv \sqrt[p_1]{p_2} \pmod{2} \), this contradicts the fact that the norm of the fundamental unity, \( \varepsilon_{p_1\mathbb{Q}(\sqrt[p_1]{p_2})} \), is \( -1 \) and \( \sqrt[p_1]{p_2} \not\in \mathbb{Q}(\sqrt[p_1]{p_2}) \). Hence the result.

(ii) We know that \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} \) is principal in \( \mathbb{Q}(\sqrt[p_1]{p_2}) \). If we suppose that \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} \) is not principal, it follows that the class of \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} \) is also a generator of the 2-class group of \( \mathbb{Q}(\sqrt[p_1]{p_2}) \). We deduce from (i) that \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} p_1\mathcal{O}_{\mathbb{Q}(\sqrt[p_1]{p_2})} \) is principal in \( \mathbb{Q}(\sqrt[p_1]{p_2}) \). As \( p_1 \) is ramified in \( \mathbb{Q}(\sqrt[p_1]{p_2})/\mathbb{Q} \) and 2 splits completely in \( \mathbb{Q}(\sqrt[p_1]{p_2})/\mathbb{Q} \), since \( p_1 \equiv p_2 \equiv 1 \pmod{8} \). This allows us to write by applying the norm that: \( 2p_1 = \alpha^2 - p_1p_2\beta^2 \), where \( \alpha^2, \beta^2 \) are in \( \mathbb{Q} \); hence \( 1 = (\frac{2p_1}{p_2}) = (\frac{2}{p_2})^4 (\frac{p_1}{p_2}) = (\frac{p_1}{p_2}) \). Which contradicts our hypotheses. Finally \( (2\mathbb{Q}(\sqrt[p_1]{p_2}))^{h(d)/2} \) is principal. \( \square \)
Theorem 2. Let $\mathbb{k} = \mathbb{Q}(\sqrt{p_1p_2}, i)$, with $p_1$, $p_2$ are prime numbers congruent to 1 (mod 8), $(\frac{2}{p_1}) = -1$ and $(\frac{2}{p_2}) = -1$, where $d = p_1p_2 = a^2 + b^2$, $C_{\mathbb{k}, 2}$ be the 2-class group de of $\mathbb{k}$. Put $p_1 = \pi_1\pi_2$, where $\pi_1$ and $\pi_2$ are in $\mathbb{Z}[i]$, let $\mathcal{H}_0$, $\mathcal{H}_1$ and $\mathcal{H}_2$ be the ideals of $\mathbb{k}$ above $1 + i$, $\pi_1$ and $\pi_2$ respectively. Then $C_{\mathbb{k}, 2} = (\langle H_{\mathcal{H}_0}^{\frac{h(d)}{2}} \rangle, [\mathcal{H}_1], [\mathcal{H}_2])$, where $h(d)$ is the class number of $\mathbb{Q}(\sqrt{p_1p_2})$.

Proof. Put $p_1 = \pi_1\pi_2$, we know that $\pi_j$ are ramified primes in $\mathbb{k}/\mathbb{Q}(i)$, so there exist prime ideals $\mathcal{H}_j$ in $\mathbb{k}$ such that $\mathcal{H}_j^2 = (\pi_j)$.

As the norm of the fundamental unit of $\mathbb{Q}(\sqrt{d})$ is -1 and $H_1^2 = (e + 2if)$, $H_2^2 = (e - 2if)$ ($\mathcal{H}_1\mathcal{H}_2)^2 = (p_1)$, where $p_1 = e^2 + 4f^2$; so Propositions 1 above and 8 in [1], state that $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_1\mathcal{H}_2$ are of order 2 in $\mathbb{k}$.

Let us proof that $\mathcal{H}_0^{\frac{h(d)}{2}}$ is of order 2 in $\mathbb{k}$. We know from [4] that $\frac{h(d)}{2}$ is an odd integer, then Lemma 1 implies that $\mathcal{H}_0^{\frac{h(d)}{2}}$ is not principal, as $\mathcal{H}_0^{\frac{h(d)}{2}} = (\mathcal{H}_0^2)^{\frac{h(d)}{2}} = (2_{\mathbb{Q}(\sqrt{d})}^{\frac{h(d)}{2}}\mathcal{O}_{\mathbb{k}}$, because $2_{\mathbb{Q}(\sqrt{d})}$ is an ramified ideal in $\mathbb{k}/\mathbb{Q}(\sqrt{d})$.

Lemma (1) leads that $\mathcal{H}_0^{\frac{h(d)}{2}}$ is principal in $\mathbb{k}$, i.e. $\mathcal{H}_0^{\frac{h(d)}{2}}$ is an ideal of order 2. $\mathcal{H}_0^{\frac{h(d)}{2}}$ $\mathcal{H}_i$ is also of order 2 in $\mathbb{k}$, in fact if for example $\mathcal{H}_0^{\frac{h(d)}{2}}\mathcal{H}_1$ is principal. So by applying the norm in $\mathbb{k}/\mathbb{Q}(\sqrt{d})$, we find that $(2_{\mathbb{Q}(\sqrt{p_1p_2})}^{\frac{h(d)}{2}}\mathcal{P}_1\mathbb{Q}(\sqrt{d})$ is an ideal principal in $\mathbb{Q}(\sqrt{d})$, afterward $\mathcal{P}_1\mathbb{Q}(\sqrt{d})$ is principal in $\mathbb{Q}(\sqrt{d})$. This contradicts Lemma 1. Let us show by absurd also that the ideal $\mathcal{H}_0^{\frac{h(d)}{2}}\mathcal{H}_1\mathcal{H}_2$ is of order 2 in $\mathbb{k}$. If not, there exists $\alpha \in \mathbb{k}$ such that $\mathcal{H}_0^{\frac{h(d)}{2}}\mathcal{H}_1\mathcal{H}_2 = (\alpha)$, as $\mathcal{H}_1\mathcal{H}_2\mathcal{H}_3\mathcal{H}_4 = (\sqrt{p_1p_2}\pi_3\pi_4) = (\sqrt{p_1p_2})$ is principal in $\mathbb{k}$, then there exists $\beta \in \mathbb{k}$ such that $\mathcal{H}_0^{\frac{h(d)}{2}}\mathcal{H}_3\mathcal{H}_4 = (\beta)$. By taking norm in $\mathbb{k}/\mathbb{Q}(i)$, we find that $(1 + i)^{\frac{h(d)}{2}}p_1 = \varepsilon(\alpha_1^2 - \alpha_2^2d)$ and $(1 + i)^{\frac{h(d)}{2}}p_2 = \varepsilon'(\beta_1^2 - \beta_2^2d)$, with $\varepsilon, \varepsilon'$ are two units in $\mathbb{Q}(i)$, $\alpha_1, \alpha_2, \beta_1$ and $\beta_2$ are elements in $\mathbb{Q}(i)$. This imply that: $\left(\frac{1 + i}{p_1\mathbb{Q}(i)}\right)\left(\frac{p_1}{p_2\mathbb{Q}(i)}\right) = 1$ and $\left(\frac{p_2}{p_1\mathbb{Q}(i)}\right) = 1$. As $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_2}\right)$, $\left(\frac{p_2}{p_1}\mathbb{Q}(i)\right) = \left(\frac{p_2}{p_1}\right)$, and $(\frac{p_1}{p_2}) = -1$, then according to [6, p. 154] we find that $\left(\frac{2}{p_1}\right)\left(\frac{p_1}{2}\right) = \left(\frac{2}{p_2}\right)\left(\frac{p_2}{2}\right) = -1$. Finally from [7, p. 323] $(\frac{2}{a+b}) = 1$, which is false. \square

Numerical Examples 2. $d$ is of the form (1).
\[ \begin{array}{|c|c|c|c|c|c|c|c|} \hline d = p_1p_2 & \left( \frac{p_1}{p_2} \right) & a & b & \left( \frac{2}{p_2} \right) & H_0 & H_1 & H_2 \\ \hline 697 = 17.41 & -1 & 11 & 24 & -1 & [3, 1, 0] & [3, 1, 1] & [0, 1, 0] \\ 3977 = 97.41 & -1 & 56 & 29 & -1 & [0, 0, 1] & [7, 0, 1] & [7, 1, 1] \\ \hline \end{array} \]

2.3. Generators of \( C_{k,2} \) when \( d = pq_1q_2 \)

**Theorem 3.** Let \( k = \mathbb{Q}(\sqrt{d}, i) \), where \( d = pq_1q_2 \) with \( p \), \( q_1 \) and \( q_2 \) are prime numbers satisfying conditions \( A \) and \( B \) defined in the introduction. Denote by \( C_{k,2} \) the 2-class group of \( k \). Put \( p_1 = \pi_1\pi_2 \), with \( \pi_1 \), \( \pi_2 \) in \( \mathbb{Z}[i] \), let \( \mathcal{H}_1 \), \( \mathcal{H}_2 \), \( \mathcal{Q}_1 \) and \( \mathcal{Q}_2 \) be the prime ideals of \( k \) above \( \pi_1 \), \( \pi_2 \), \( q_1 \) and \( q_2 \) respectively, then:

1. If \( p \), \( q_1 \) and \( q_2 \) are satisfying conditions \( B \) (I) or \( B \) (II) and \( \left( \frac{p}{q_1} \right) = -\left( \frac{p}{q_2} \right) = 1 \), then \( C_{k,2} = \langle [\mathcal{H}_1], [\mathcal{H}_2], [\mathcal{Q}_1], [\mathcal{Q}_2] \rangle \).

2. Else, \( C_{k,2} = \langle [\mathcal{H}_1], [\mathcal{H}_2], [\mathcal{Q}_1] \rangle \).

**Proof.** As \( q_1 \), \( q_2 \) are congruent to 3 (mod 4), so they are ramified in \( k/\mathbb{Q} \); let \( \mathcal{Q}_1 \) and \( \mathcal{Q}_2 \) be the ideals in \( k \) above \( q_1 \) and \( q_2 \) respectively. We know also that \( \pi_j \) are ramified in \( k/\mathbb{Q}(i) \), then there exist ideals \( \mathcal{H}_j \) in \( k \) such that: \( \langle \pi_j \rangle = \mathcal{H}_j^2 \), moreover \( \mathcal{H}_j \) is not principal in \( k \), in fact if we put \( p_1 = e^2 + 4f^2 \), then \( \mathcal{H}_j^2 = (e \pm 2if)^2 \) and as \( \sqrt{p} \not\in \mathbb{Q}(\sqrt{d}) \), therefore Proposition 1 states the result, similar for \( i, j \in \{1, 2\} \) we have \( \mathcal{H}_i\mathcal{Q}_j \) is not principal in \( k \) because \( \langle \mathcal{H}_i\mathcal{Q}_j \rangle^2 = (\pi_iq_j)^2 \) and \( \pi_iq_j = q_j(e \pm 2if) \), as \( \sqrt{eq_j}^2 + (2fq_j)^2 = q_j\sqrt{p} \not\in \mathbb{Q}(\sqrt{d}) \), hence Proposition 1 implies the result.

Let \( \varepsilon_d = x + y\sqrt{d} \) be the fundamental unit of \( \mathbb{Q}(\sqrt{d}) \); as \( d \equiv 1 \) (mod 4), then the unit index of \( k \) is 1 (corollary 3.2 in [3]), so according to [2] \( x \pm 1 \) is not a square in \( \mathbb{N} \); therefore from Remark 1, if \( \mathcal{H} \) is an ideal of \( k \) satisfy \( \mathcal{H}^2 = (l) \), where \( l \) is a prime number in \( \mathbb{N} \), then \( \mathcal{H} \) is principal if and only if \( l(x \pm 1) \) is a square in \( \mathbb{N} \).

1. For this first case the proof is of two points:

   1. Suppose \( p \), \( q_1 \) and \( q_2 \) satisfy \( B \) (I) and \( \left( \frac{p}{q_1} \right) = -\left( \frac{p}{q_2} \right) = 1 \), so as \( x^2 - 1 = y^2p_1p_2q \), the only possible case is:

   \[
   \begin{cases}
   x \pm 1 = 2q_1y_1^2, \\
   x \pm 1 = 2p_2q_2y_2^2;
   \end{cases}
   \]

   this yields that \( 2q_1(x \pm 1) \) is a square in \( \mathbb{N} \) and \( q_2(x \pm 1) \), \( 2q_2(x \pm 1) \) are not; as \( \mathcal{Q}_1^2 = (q_1) \) and \( \mathcal{Q}_2^2 = (q_2) \), therefore \( \mathcal{Q}_1 \) is principal in \( k \) and \( \mathcal{Q}_2 \) is not, the result derived.
(ii) Suppose \( p, q_1 \) and \( q_2 \) satisfy \( B \) (II) and \( \left( \frac{p}{q_1} \right) = -\left( \frac{p}{q_2} \right) = 1 \), so as \( x^2 - 1 = y^2p_1p_2q \), the only possible cases are:
\[
\begin{align*}
\{ \ & x \pm 1 = q_1y_1^2, \quad \text{or} \quad x \mp 1 = p_1p_2y_2^2; \quad \text{thus } q_1(x \pm 1) \text{ or } 2q_1(x \pm 1) \text{ is a square in } \mathbb{N} \text{ and } q_2(x \pm 1), 2q_2(x \pm 1) \text{ are not; as } Q_1^2 = (q_1) \text{ and } Q_2^2 = (q_2), \text{ so } Q_1 \text{ is principal in } \mathbb{k} \text{ and } Q_2 \text{ is not, this ends the first case of theorem.}
\end{align*}
\]

(2) In this case we have also two points to distinguish:

(i) Suppose that \( p, q_1 \) and \( q_2 \) satisfy \( B \) (I) or \( B \) (II) and \( \left( \frac{p}{q_2} \right) = -\left( \frac{p}{q_1} \right) = 1 \), we proceed as in the case (1) to prove that \( Q_2 \) is principal in \( \mathbb{k} \) and \( Q_1 \) is not; so the result.

(ii) Suppose that \( p, q_1 \) et \( q_2 \) satisfy \( B \) (III), then since \( x^2 - 1 = y^2p_1q_2 \), the only possible case is: \( \{ x \pm 1 = 2q_1q_2y_1^2, \quad x \mp 1 = 2p_1y_2^2; \quad \text{thus } \} q_1(x \pm 1) \text{ is square in } \mathbb{N} \text{ and } q_1(x \pm 1), 2q_1(x \pm 1), q_2(x \pm 1) \text{ and } 2q_2(x \pm 1) \text{ are not. This completes the proof.} \]

\[ \square \]

**Numerical Examples 3.** \( d = pq_1q_2 \) is of the form (4).

<table>
<thead>
<tr>
<th>( d = pq_1q_2 )</th>
<th>( \frac{p}{q_1} )</th>
<th>( \frac{p}{q_2} )</th>
<th>( \frac{2}{q_1} )</th>
<th>( \frac{2}{q_2} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>357 = 17.7.3</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>969 = 17.19.3</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>3553 = 17.11.19</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( d = pq_1q_2 )</th>
<th>( Q_1 )</th>
<th>( Q_2 )</th>
<th>( Q_1Q_2 )</th>
<th>( H_1 )</th>
<th>( H_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>357 = 17.7.3</td>
<td>[1, 1, 0]</td>
<td>[1, 1, 0]</td>
<td>[0, 0, 0]</td>
<td>[0, 0, 1]</td>
<td>[0, 0, 1]</td>
</tr>
<tr>
<td>969 = 17.19.3</td>
<td>[0, 0, 0]</td>
<td>[0, 1, 0]</td>
<td>[0, 1, 0]</td>
<td>[3, 1, 0]</td>
<td>[3, 0, 0]</td>
</tr>
<tr>
<td>3553 = 17.11.19</td>
<td>[0, 0, 1]</td>
<td>[0, 0, 0]</td>
<td>[0, 0, 1]</td>
<td>[3, 1, 1]</td>
<td>[3, 1, 0]</td>
</tr>
</tbody>
</table>

2.4. Generators of \( C_{k,2} \) when \( d = p_1p_2q \)

Let \( d = p_1p_2q \) satisfying the conditions of the form (5), then we have.

**Theorem 4.** Let \( k = \mathbb{Q}(\sqrt{d}, i) \), where \( d = p_1p_2q \) with \( p_1, p_2 \) and \( q \) are prime numbers such that \( p_1 \equiv p_2 \equiv -q \equiv 1 \) (mod 4), \( p_1 \equiv 5 \) or \( p_2 \equiv 5 \) (mod 8) and at least two elements of \( \{ (\frac{p_1}{p_2}), (\frac{p_1}{q}), (\frac{p_2}{q}) \} \) are equal to -1. Denote by \( C_{k,2} \) the 2-class group of \( k \). Put \( p_1 = \pi_1\pi_2, p_2 = \pi_3\pi_4, \) with \( \pi_1, \pi_2, \pi_3 \) and \( \pi_4 \)
ON THE GENERATORS OF... 783

are in \( \mathbb{Z}[i] \), let \( \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \) and \( \mathcal{H}_4 \) be the ideals in \( k \) above \( \pi_1, \pi_2, \pi_3 \) and \( \pi_4 \) respectively, then:

1. If \( p_1, p_2 \) and \( q \) are of type I, then \( C_{k,2} = \langle [\mathcal{H}_1], [\mathcal{H}_3], [\mathcal{H}_4] \rangle \).

2. If \( p_1, p_2 \) and \( q \) are of type II or of type III, then \( C_{k,2} = \langle [\mathcal{H}_1], [\mathcal{H}_2], [\mathcal{H}_3] \rangle \).

Proof. We proceed as in the previous case to prove that:

- If \( p_1, p_2 \) and \( q \) are of type I, then \( \mathcal{H}_1 \mathcal{H}_2 \) is principal in \( k \) and \( \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4 \) and \( \mathcal{H}_3 \mathcal{H}_4 \) are not.
- If \( p_1, p_2 \) and \( q \) are of type II, then \( \mathcal{H}_3 \mathcal{H}_4 \) is principal in \( k \) and \( \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4 \) and \( \mathcal{H}_1 \mathcal{H}_2 \) are not.
- If \( p_1, p_2 \) and \( q \) are of type III, then \( \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4, \mathcal{H}_1 \mathcal{H}_2 \) and \( \mathcal{H}_3 \mathcal{H}_4 \) are not principal in \( k \).

Numerical Examples 4. The last case where \( d = p_1 p_2 q \) is of the form (5).

<table>
<thead>
<tr>
<th>( p_1, p_2, q )</th>
<th>( \pi_1 )</th>
<th>( \pi_2 )</th>
<th>( \pi_3 )</th>
<th>( \pi_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.13.3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>5.13.7</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>17.5.7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13.5.11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5.17.11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( p_1, p_2, q )</th>
<th>( \mathcal{H}_1 )</th>
<th>( \mathcal{H}_2 )</th>
<th>( \mathcal{H}_1 \mathcal{H}_2 )</th>
<th>( \mathcal{H}_3 )</th>
<th>( \mathcal{H}_4 )</th>
<th>( \mathcal{H}_3 \mathcal{H}_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.13.3</td>
<td>[1, 0, 0]</td>
<td>[0, 1, 1]</td>
<td>[1, 1, 1]</td>
<td>[0, 1, 0]</td>
<td>[0, 1, 0]</td>
<td>[0, 0, 0]</td>
</tr>
<tr>
<td>5.13.7</td>
<td>[5, 1, 1]</td>
<td>[5, 0, 1]</td>
<td>[0, 1, 0]</td>
<td>[0, 1, 1]</td>
<td>[0, 0, 1]</td>
<td>[0, 1, 0]</td>
</tr>
<tr>
<td>17.5.7</td>
<td>[0, 1, 1]</td>
<td>[0, 1, 1]</td>
<td>[0, 0, 0]</td>
<td>[0, 1, 0]</td>
<td>[1, 0, 0]</td>
<td>[1, 1, 0]</td>
</tr>
<tr>
<td>13.5.11</td>
<td>[1, 0, 0]</td>
<td>[0, 1, 0]</td>
<td>[1, 1, 0]</td>
<td>[0, 1, 1]</td>
<td>[0, 1, 1]</td>
<td>[0, 0, 0]</td>
</tr>
<tr>
<td>5.17.11</td>
<td>[7, 1, 0]</td>
<td>[7, 0, 0]</td>
<td>[0, 1, 0]</td>
<td>[7, 1, 1]</td>
<td>[7, 1, 1]</td>
<td>[0, 0, 0]</td>
</tr>
</tbody>
</table>

References


A. Azizi, M. Taous, Determination des corps $\mathbb{Q}(\sqrt{d}, i)$ dont le 2-groupes de classes est de type $(2, 4)$ ou $(2, 2, 2)$, *Rend. Istit. Mat. Univ. Trieste*, 40, No. XL (2009), 93-116.


