JP Journal of Algebra, Number Theory and Applications
Volume 22, Number 2, 2011, Pages 155-174
Published Online: July 12, 2011
This paper is available online at http://pphmj.com/journals/jpanta.htm

2-CLASS GROUP OF QUADRATIC FIELDS

ALEJANDRO AGUILAR-ZAVOZNIK and MARIO PINEDA-RUELAS

Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa
Av San Rafael Atlixco No. 186, Col.Vicentina
C.P.09340 Del. Iztapalapa, D.F., México
e-mail: aaz@xanum.uam.mx
mpr@xanum.uam.mx

Abstract

We find explicitly the 2-class group of a quadratic field. We use this result to give a criterion to decide whether an ideal is principal if the exponent of $Cl_{\mathbb{F}}$ is 2.

1. Introduction

Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ be a quadratic field, $\mathcal{O}_{\mathbb{F}}$ the ring of integers of $\mathbb{F}$, $Cl_{\mathbb{F}}$ the class group of $\mathbb{F}$, Cl_2 the 2-Sylow subgroup of $Cl_{\mathbb{F}}$ and $\delta_{\mathbb{F}}$ the discriminant of $\mathbb{F}$. It is well known that the rank of Cl_2 depends on the number and type of the prime factors of *d*. However, obtaining Cl_2 is not an easy task. In [1], [2], [4] and [6], the theory of quadratic forms is used to give an algorithm that computes Cl_2. Given a class $\bar{I} \in Cl_2$, they give different methods to obtain, if possible, another class $\bar{J}$ such that $\bar{J}^2 = \bar{I}$. It is easy to find representatives of all the ambiguous ideal classes (i.e., classes of order 2) and we can use any of the previous methods to construct Cl_2. In this paper, we will give another procedure to compute Cl_2, but instead of starting from the ambiguous classes, we will give elements $\alpha \in \mathcal{O}_{\mathbb{F}}$ such that $\langle\overline{\alpha}\rangle$

2010 Mathematics Subject Classification: 11R11, 11R29, 11Y40.

Keywords and phrases: quadratic field, 2-class group.

Received January 27, 2011

is maximal in the set of cyclic subgroups of Cl_2. If the exponent of $Cl_{\mathbb{F}}$ is 2, then we give a criterion to decide if an ideal of $\mathcal{O}_{\mathbb{F}}$ is principal or non-principal. With the aid of the computer programs KASH3 [3] and Sage [7], we solve some explicit examples.

2. Some Results on Finite Abelian Groups

We use C_n to denote the cyclic group of order n and for $a \in \mathbb{Z}$, we will write $\overline{a}$ to denote the class of a in C_n, where we assume that $C_n = \mathbb{Z}/n\mathbb{Z}$. Let $G = \langle g_1, \ldots, g_r \rangle$ be a finite abelian group. We are interested in finding $h_1, \ldots, h_k \in G$ that satisfy

$$G = \langle h_1, \ldots, h_k \rangle \cong \langle h_1 \rangle \oplus \cdots \oplus \langle h_k \rangle.$$

Let $\mathcal{C}_G = \{\langle a \rangle : a \in G\}$. Then

Proposition 1. *Let* $G = G_1 \oplus \cdots \oplus G_k$ *be a finite abelian* p*-group where each* G_j *is a cyclic* p*-group. If* $(\overline{a_1}, \ldots, \overline{a_k}) \in G$, *then* $\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle$ *is a maximal element in* $\mathcal{C}_G$ *if and only if* $\gcd(a_i, p) = 1$ *for some* i.

Proof. Suppose that $\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle$ is maximal in $\mathcal{C}_G$ and $\gcd(a_i, p) = p$ for all i. If $b_i = a_i / p$, then we have

$$\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle = \langle (\overline{pb_1}, \ldots, \overline{pb_k}) \rangle = \langle p(\overline{b_1}, \ldots, \overline{b_k}) \rangle.$$

Since

$$o(\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle) = \frac{o(\langle (\overline{b_1}, \ldots, \overline{b_k}) \rangle)}{p},$$

then

$$\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle \subsetneq \langle (\overline{b_1}, \ldots, \overline{b_k}) \rangle,$$

so that $\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle$ is not a maximal element in $\mathcal{C}_G$.

Conversely, we may assume without loss of generality that $\gcd(a_1, p) = 1$. Let $\langle (\overline{c_1}, \ldots, \overline{c_k}) \rangle \in \mathcal{C}_G$ be such that $\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle \subseteq \langle (\overline{c_1}, \ldots, \overline{c_k}) \rangle$. Let $n \in \mathbb{Z}$ be such that $\langle (\overline{a_1}, \ldots, \overline{a_k}) \rangle = \langle n(\overline{c_1}, \ldots, \overline{c_k}) \rangle$. We consider the projection $\phi : G \to G_1$. Since

$\gcd(a_1, p) = 1$, $\phi(\langle(\overline{a_1}, \ldots, \overline{a_k})\rangle) = G_1$. From the equality

$$o((\overline{a_1}, \ldots, \overline{a_k})) = \frac{o((\overline{c_1}, \ldots, \overline{c_k}))}{\gcd(n, o((\overline{c_1}, \ldots, \overline{c_k})))},$$

it follows that if $\gcd(n, o((\overline{c_1}, \ldots, \overline{c_k}))) > 1$, then $p \mid n$ and $\phi(\langle n(\overline{c_1}, \ldots, \overline{c_k})\rangle) \neq G_1$, which is impossible. Therefore, $\gcd(n, o((\overline{c_1}, \ldots, \overline{c_k}))) = 1$ and from this it follows that $\langle(\overline{a_1}, \ldots, \overline{a_k})\rangle$ is a maximal element in $\mathcal{C}_G$. □

Next result is similar to the Fundamental Theorem of the Finite Abelian Groups.

Proposition 2. *Let G be a finite abelian p-group, H a subgroup of G, $g \in G$ such that $G = \langle H, g\rangle$, $g \notin H$ and $o(g) \leq o(\langle h\rangle)$ for all $\langle h\rangle$ maximal in $\mathcal{C}_H$. Then there is $g' \in G$ such that $G = \langle H, g'\rangle \cong H \oplus \langle g'\rangle$.*

Proof. Let $\mu = sp^m$ be the smallest positive integer such that $\mu g \in H$ and $\gcd(s, p) = 1$. Since $\langle g\rangle = \langle sg\rangle$, we may assume that $\mu = p^m$. Now consider $h \in H$ with $\langle h\rangle$ maximal in $\mathcal{C}_H$, $p^m g \in \langle h\rangle$ and let $\nu = tp^n$ be the least positive integer such that $\gcd(t, p) = 1$ and $p^m g = \nu h$. As before, we can replace h with th and assume that $\nu = p^n$. It is clear that if $o(g) = p^{m+r}$, then $o(h) = p^{n+r}$. If e is the identity of G, then

$$e = p^{m+r} g = p^m p^r g = p^r(p^m g) = (p^r - 1)(p^m g) + (p^m g)$$

$$= (p^r - 1)(p^n h) + (p^m g) = p^m((p^r - 1)p^{n-m} h + g).$$

Let $g' = (p^r - 1)p^{n-m} h + g$. It is clear that $g' \neq e$ and $o(g') \leq p^m$. Suppose that $o(g') = p^j$ and $1 \leq j < m$. Then

$$e = p^j g' = p^j((p^r - 1)p^{n-m} h + g) = p^j((p^r - 1)p^{n-m} h) + p^j g \in \langle h\rangle.$$

Therefore, $p^j g \in \langle h\rangle$ which is impossible. Thus $j = m$.

Since $g' = (p^r - 1)p^{n-m} h + g$, we obtain $G = \langle H, g'\rangle$. The assertion $\langle H, g'\rangle \cong H \oplus \langle g'\rangle$ is a consequence of $H \cap \langle g'\rangle = \langle e\rangle$. □

Next, we will describe an algorithm that will help us modify the set of generators of a finite abelian group G so that the new set of generators decompose G as a direct sum.

Algorithm. Let $G = \langle g_1, \ldots, g_r \rangle$ be a finite abelian group and assume that $o(g_i)$ are known for $i = 1, \ldots, r$. First, we study the case when G is a p-group. In the process that we are describing, whenever we change some generator (if required), we will reindex the new elements so that

$$o(g_1) \geq o(g_2) \geq \cdots \geq o(g_r).$$

Let $G' = \langle g_1, g_2 \rangle, H' = \langle g_1 \rangle$ and $g = g_2$ as in Proposition 2. If $g_2 \in H'$, then $G = \langle g_1, g_3, \ldots, g_r \rangle$. So we can assume that $g_2 \notin H'$. By using Proposition 2, there is $g_2' \in G'$ such that

$$G' = \langle H', g_2' \rangle \cong H' \oplus \langle g_2' \rangle \quad \text{and} \quad \langle g_1, g_2, \ldots, g_r \rangle = \langle g_1, g_2', \ldots, g_r \rangle.$$

It is possible that $o(g_2') < o(g_3)$. If this was the case, then we reindex and repeat the process until $g_2' = g_2$. Therefore, $G' \cong \langle g_1 \rangle \oplus \langle g_2 \rangle$. For the next step, we let $G' = \langle g_1, g_2, g_3 \rangle$, $H' = \langle g_1, g_2 \rangle \cong \langle g_1 \rangle \oplus \langle g_2 \rangle$ and $g = g_3$ as in Proposition 2. We may assume that $g_3 \notin H'$. Since $o(g_1) \geq o(g_2) \geq o(g_3)$, the order of any maximal cyclic subgroup of H' is greater or equal to $o(g_3)$ and therefore satisfies the hypothesis of Proposition 2. Let $g_3' \in G'$ such that $G' = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \langle g_3' \rangle$. If $o(g_3') < o(g_4)$, then repeat the process until we obtain $g_3' = g_3$ and $G' = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \langle g_3 \rangle$. Continuing with this, we can construct explicitly a basis $\{g_1, \ldots, g_t\}$ of G such that $G \cong \langle g_1 \rangle \oplus \cdots \oplus \langle g_t \rangle$. In general, if G is a finite abelian group, then we apply the Algorithm to each p-Sylow subgroup of G.

We will refer to the procedure that we have described previously as the Algorithm.

Example 1. Let $G = C_{16} \oplus C_8 \oplus C_8 \oplus C_4$ and $H = \langle g_1, g_2, g_3, g_4, g_5 \rangle$, where $g_1 = (\overline{1}, \overline{1}, \overline{1}, \overline{1})$, $g_2 = (\overline{3}, \overline{1}, \overline{1}, \overline{1})$, $g_3 = (\overline{7}, \overline{3}, \overline{0}, \overline{2})$, $g_4 = (\overline{3}, \overline{0}, \overline{1}, \overline{1})$, $g_5 = (\overline{12}, \overline{6}, \overline{3}, \overline{1}) \in G$. Using the Algorithm, we will find the representation of H as a direct sum of cyclic subgroups of H. Note that

$$o(g_1) = o(g_2) = o(g_3) = o(g_4) = 16, \quad o(g_5) = 8,$$

so, according to the Algorithm, they are arranged already in a proper way. We apply Proposition 2 to $G' = \langle g_1, g_2 \rangle$, $H' = \langle g_1 \rangle$ and $g = g_2$. The minimal positive integers m and n such that $\mu g_1 = \nu g_2$ are $\mu = 12$ and $\nu = 4$. Since $12 = 3 \cdot 4$, we replace g_1 with $3g_1$, and call g_1 again the new element. With this notation, we have $g_1 = (\overline{3}, \overline{3}, \overline{3}, \overline{3})$. If $h = g_1$, then we have $4g \in \langle h \rangle$ and the minimal positive integers μ and ν such that $\mu g = \nu h$ are $\mu = \nu = 2^2$. Note that $2^{2+2} g = 2^{2+2} h = e$. Therefore, the values we need to construct g' as in Proposition 2, are $r = m = n = 2$ and

$$g' = (2^2 - 1)(2^{2-2})h + g = 3h + g = 3(\overline{3}, \overline{3}, \overline{3}, \overline{3}) + (\overline{3}, \overline{1}, \overline{1}, \overline{1}) = (\overline{12}, \overline{2}, \overline{2}, \overline{2}).$$

Since $o(g') = 4$, we replace g_2 with g' and arrange the generators so that $o(g_1) \geq \cdots \geq o(g_5)$. We have

$$g_1 = (\overline{1}, \overline{1}, \overline{1}, \overline{1}),$$

$$g_2 = (\overline{7}, \overline{3}, \overline{0}, \overline{2}),$$

$$g_3 = (\overline{3}, \overline{0}, \overline{1}, \overline{1}),$$

$$g_4 = (\overline{12}, \overline{6}, \overline{3}, \overline{1}),$$

$$g_5 = (\overline{12}, \overline{2}, \overline{2}, \overline{2}).$$

We repeat the process with $g = g_2$, $h = g_1$, $8g = 8h$, $16g = 16h = e$, $m = n = 3$, $r = 1$ and

$$g' = (2^1 - 1)(2^0)h + g = (\overline{1}, \overline{1}, \overline{1}, \overline{1}) + (\overline{7}, \overline{3}, \overline{0}, \overline{2}) = (\overline{8}, \overline{4}, \overline{1}, \overline{3}).$$

We replace g_2 with g' and reorder. Thus, we obtain a new list of generators of H:

$$g_1 = (\overline{1}, \overline{1}, \overline{1}, \overline{1}),$$

$$g_2 = (\overline{3}, \overline{0}, \overline{1}, \overline{1}),$$

$$g_3 = (\overline{12}, \overline{6}, \overline{3}, \overline{1}),$$

$$g_4 = (\overline{8}, \overline{4}, \overline{1}, \overline{3}),$$

$$g_5 = (\overline{12}, \overline{2}, \overline{2}, \overline{2}).$$

We repeat the procedure with the new $g = g_2$, $H' = \langle g_1 \rangle$, $h = g_1$, $8g = 8h$, $16g = 16h = e$, $m = n = 3$, $r = 1$. Therefore,

$$g' = (2^1 - 1)(2^0)h + g = (\bar{1}, \bar{1}, \bar{1}, \bar{1}) + (\bar{3}, \bar{0}, \bar{1}, \bar{1}) = (\bar{4}, \bar{1}, \bar{2}, \bar{2}).$$

Thus, we obtained a new list of generators of H:

$$g_1 = (\bar{1}, \bar{1}, \bar{1}, \bar{1}),$$

$$g_2 = (\bar{4}, \bar{1}, \bar{2}, \bar{2}),$$

$$g_3 = (\overline{12}, \bar{6}, \bar{3}, \bar{1}),$$

$$g_4 = (\bar{8}, \bar{4}, \bar{1}, \bar{3}),$$

$$g_5 = (\overline{12}, \bar{2}, \bar{2}, \bar{2}).$$

We note that, if we apply the process again, then there will be no change since $16g_1 = 8g_2 = e$ and $r = 0$. Continuing with $g = g_3$, $H' = \langle g_1, g_2 \rangle$ and $h = g_1$, we observe that $8g = 16h = e$ and $r = 0$. Therefore, there is no need to change g_3.

In the next step, we apply the Algorithm with $g = g_4$, $H' = \langle g_1, g_2, g_3 \rangle$. In this case, we have $g_4 = 12g_1 + 6g_2 + 3g_3 \in H'$. Therefore,

$$g_1 = (\bar{1}, \bar{1}, \bar{1}, \bar{1}), \quad g_2 = (\bar{4}, \bar{1}, \bar{2}, \bar{2}), \quad g_3 = (\overline{12}, \bar{6}, \bar{3}, \bar{1}), \quad g_4 = (\overline{12}, \bar{2}, \bar{2}, \bar{2}).$$

As in the previous step, $g = g_4 \in H' = \langle g_1, g_2, g_3 \rangle$. Therefore, the generators that we are looking for are g_1, g_2, g_3 and

$$H = \langle (\bar{1}, \bar{1}, \bar{1}, \bar{1}), (\bar{4}, \bar{1}, \bar{2}, \bar{2}), (\overline{12}, \bar{6}, \bar{3}, \bar{1}) \cong C_{16} \oplus C_8 \oplus C_8,$$

where $o(g_1) = 16$, $o(g_2) = o(g_3) = 8$.

3. 2-class Groups of Real Quadratic Fields

As an application of the Algorithm, we are going to construct generators of the 2-Sylow subgroup of the ideal class group of a real quadratic field. Next theorem is well known ([5, Theorem 3.70]).

Theorem 3 (Gauss's Theorem on the 2-rank of $Cl_{\mathbb{F}}$)**.** *Let* $\mathbb{F}$ *be a quadratic field and t the number of distinct factors of* $\delta_{\mathbb{F}}$. *If there is some prime* $p \equiv 3 \pmod 4$ *such that* $p \mid \delta_{\mathbb{F}}$ *and* $d > 0$, *then the rank of* Cl_2 *is* $t - 2$. *In any other case, the rank is* $t - 1$.

Let $a, b \in \mathbb{Z}$, $b > 1$. We will use the following notation:

$$\left[\frac{a}{b}\right] = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod b \text{ solvable}, \\ -1, & \text{if } x^2 \equiv a \pmod b \text{ is not solvable}. \end{cases}$$

If b is a prime number and $\gcd(a, b) = 1$, then $\left[\frac{a}{b}\right]$ is just Legendre's symbol $\left(\frac{a}{b}\right)$. As consequence of the Chinese Remainder Theorem, we have:

Lemma 4. *Let* $a, b = b_1 \cdots b_t > 1$ *be integers such that* $\gcd(b_i, b_j) = 1$ *for* $i \neq j$. *Then* $\left[\frac{a}{b}\right] = 1$ *if and only if* $\left[\frac{a}{b_i}\right] = 1$ *for* $i = 1, \ldots, t$.

Lemma 5. *Let* $b_1, \ldots, b_t \in \{-1, 1\}$, $a, n, p_1, \ldots, p_t \in \mathbb{Z}^+$, $a < 2^n$ *odd and where* p_i *is an odd prime number for* $i = 1, \ldots, t$. *Then there is a rational prime q such that*

$$q \equiv a \pmod{2^n}, \quad \left(\frac{q}{p_1}\right) = b_1, \ldots, \left(\frac{q}{p_t}\right) = b_t.$$

Proof. Let $c_1, \ldots, c_t \in \mathbb{Z}$ such that $\left(\frac{c_i}{p_i}\right) = b_i$. Using the Chinese Remainder Theorem, there is $c \in \mathbb{Z}$ satisfying

$$\begin{gathered} c \equiv a \pmod{2^n} \\ c \equiv c_1 \pmod{p_1} \\ \vdots \\ c \equiv c_t \pmod{p_t}. \end{gathered}$$

Since $p_i \nmid c_i$, $\gcd(c, 2^n p_1 \cdots p_t) = 1$ and by Dirichlet's Theorem, there are infinite primes $q \equiv c \pmod{2^n p_1 \cdots p_t}$. $\square$

Lemma 6. *Let* $d = p_0 p_1 \cdots p_g$ *be a square free positive integer,* $p_i \equiv 1 \pmod 4$ *for* $0 \leq i \leq g$. *Then there are primes* $q_1, \ldots, q_g$ *such that*

$$\left(\frac{d}{q_i}\right) = 1 \quad \textit{and} \quad \left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$$

Proof. It follows from Lemma 5, Quadratic Reciprocity Law and Lemma 4. □

From the first assertion of Lemma 5, we note that the primes $q_1, \ldots, q_g$ can be chosen in such a way that $q_i \equiv 1 \pmod 4$. The choosing of such kind of primes will be relevant in the next results.

Lemma 7. *Let* $d = 2p_1 \cdots p_g$ *be a square free positive integer with* $p_i \equiv 1 \pmod 4$ *for* $1 \leq i \leq g$. *There are* $q_1, \ldots, q_g$ *primes that satisfy*

$$\left(\frac{4d}{q_i}\right) = 1 \quad \textit{and} \quad \left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$$

Proof. By Lemma 5 and the Quadratic Reciprocity Law, we choose $q_1 \equiv 5 \pmod 8$ such that

$$\left(\frac{p_1}{q_1}\right) = -1 \quad \text{and} \quad \left(\frac{p_j}{q_1}\right) = 1, \quad 2 \leq j \leq g.$$

Therefore,

$$\left(\frac{d}{q_1}\right) = \left(\frac{2}{q_1}\right)\left(\frac{p_1}{q_1}\right)\left(\frac{p_2}{q_1}\right)\cdots\left(\frac{p_g}{q_1}\right) = (-1)(-1)(1)\cdots(1) = 1.$$

Finally, $\left(\frac{4d}{q_1}\right) = \left(\frac{d}{q_1}\right)$. As in the proof of the previous lemma, it follows that

$$\left[\frac{q_1}{d}\right] = \left[\frac{-q_1}{d}\right] = -1.$$

The primes $q_2, \ldots, q_g$ are obtained as in Lemma 6 with the additional condition $q_i \equiv 1 \pmod 8$. □

Lemma 8. *Let* $d = p_0 p_1 \cdots p_g \equiv 1 \pmod 4$ *with* $g \geq 1$ *be a positive square free integer such that for some* $t \in \{-1, 0, 1, \ldots, g-2\}$,

$$p_0, \ldots, p_t \equiv 1 \pmod 4, \quad p_{t+1}, \ldots, p_g \equiv 3 \pmod 4.$$

Then there exist primes $q_1, \ldots, q_{g-1}$ *such that* $\left(\frac{d}{q_i}\right) = 1$ *and* $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$

Proof. The first primes $q_1, \ldots, q_t$ are obtained as in Lemma 6 such that $q_i \equiv 1 \pmod 4$. For $t + 1 \le i \le g - 1$, we choose the primes q_i such that

$$\left(\frac{p_{i-1}}{q_i}\right) = \left(\frac{p_i}{q_i}\right) = -1, \quad \left(\frac{p_j}{q_i}\right) = 1, \quad j \ne i - 1, i.$$

Hence $\left(\frac{d}{q_i}\right) = -1$, $\left[\frac{q_i}{d}\right] = -1$. Finally, since $\left(\frac{q_i}{p_g}\right) = 1$, we obtain $\left(\frac{-q_i}{p_g}\right) = -1$ and $\left[\frac{-q_i}{p_g}\right] = \left[\frac{-q_i}{d}\right] = -1.$ □

Lemma 9. *Let* $d = p_0 p_1 \cdots p_g \equiv 3 \pmod 4$ *be a positive square free integer such that for some* $t \in \{-1, 0, 1, \ldots, g - 1\}$,

$$p_0, \ldots, p_t \equiv 1 \pmod 4, \quad p_{t+1}, \ldots, p_g \equiv 3 \pmod 4.$$

Then there exist primes $q_1, \ldots, q_g$ *such that* $\left(\frac{4d}{q_i}\right) = 1$ *and* $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$

Proof. The primes $q_1, \ldots, q_t$ are obtained as in Lemma 6. Since $d \equiv 3 \pmod 4$, we have an odd number of primes $\equiv 3 \pmod 4$. First, suppose that p_g is the only prime such that $p_g \equiv 3 \pmod 4$. In this case, we choose a prime $q_g \equiv 1 \pmod 4$ satisfying

$$\left(\frac{p_{g-1}}{q_g}\right) = \left(\frac{q_g}{p_{g-1}}\right) = \left(\frac{q_g}{p_g}\right) = -1.$$

Therefore, $\left[\frac{-q_g}{d}\right] = -1$. Finally, if more than one prime is $\equiv 3 \pmod 4$, then instead of using p_g as in Lemma 8, we use any of the primes $p_j \equiv 3 \pmod 4$ such that $\left(\frac{q_i}{p_j}\right) = 1$. The proof follows as in the previous lemmas. □

Lemma 10. *Let* $d = 2p_1 \cdots p_g$ *be square free with* $p_1, \ldots, p_t \equiv 1 \pmod 4$ *and* $p_{t+1}, \ldots, p_g \equiv 3 \pmod 4$ *for* $0 \le t \le g - 1$. *Then there are primes* $q_1, \ldots, q_{g-1}$ *such that* $\left(\frac{4d}{q_i}\right) = 1$ *and* $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1$.

Proof. If $t > 0$, then $q_1, \ldots, q_t$ are obtained as in Lemma 7 and the primes $q_{t+1}, \ldots, q_{g-1}$ are obtained as in Lemma 8. If $t = 0$, then $p_i \equiv 3 \pmod 4$ for $i = 1, \ldots, g$ and $g \ge 2$. In this case, we choose $q_1 \equiv 5 \pmod 8$ in such a way that

$$\left(\frac{p_1}{q_1}\right) = -1, \quad \left(\frac{p_i}{q_1}\right) = 1, \quad i > 1.$$

From this and $\left(\frac{2}{q_1}\right) = -1$, it follows that

$$\left(\frac{4d}{q_1}\right) = 1, \qquad \left[\frac{q_1}{d}\right] = \left[\frac{-q_1}{d}\right] = -1.$$

The primes $q_2, \ldots, q_{g-1}$ are obtained as in Lemma 8. □

From now on, we write $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, $d > 0$ square free. Let $\mathcal{P} = \{q_1, \ldots, q_t\}$ obtained in Lemmas 6, 7, 8, 9 or 10. We observe that there are infinitely many $a_i \in \mathbb{N}$ such that $a_i^2 \equiv d \pmod{q_i}$. We fix one of them and define the ideals $\mathfrak{q}_i = \langle q_i, a_i + \sqrt{d}\rangle$. It is clear that $\mathfrak{q}_i$ is a prime ideal, $N(\mathfrak{q}_i) = q_i$ and $\langle q_i \rangle = \mathfrak{q}_i \mathfrak{q}_i'$, where $\mathfrak{q}_i' = \langle q_i, a_i - \sqrt{d}\rangle$. Given $\mathcal{P}$ as above, we define $\mathcal{I}_{\mathcal{P}} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$. We will write $\operatorname{ord}_I(J)$ to indicate that $I^{\operatorname{ord}_I(J)} \mid J$ and $I^{\operatorname{ord}_I(J)+1} \nmid J$.

Observe that $N(a_1 + a_2\sqrt{d}) = a_1^2 - da_2^2$, so if $I = \langle a_1 + a_2\sqrt{d}\rangle$, then $N(I) \equiv a_1^2 \pmod d$ or $-N(I) \equiv a_1^2 \pmod d$. Therefore, if $\left[\frac{\pm N(I)}{d}\right] = -1$, then I is a non-principal ideal.

Theorem 11. *Let* $d = p_0 p_1 \cdots p_g$ *be a positive square free integer and* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. *If* $I = \prod_{\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}} \mathfrak{q}^{\operatorname{ord}_{\mathfrak{q}}(I)}$ *and* $\operatorname{ord}_{\mathfrak{q}}(I)$ *is odd for some* $\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}$, *then*

(1) $\left[\frac{\pm N(I)}{d}\right] = -1$ *and therefore I is non-principal.*

(2) *If* $\bar{I} \in Cl_{\mathbb{F}}$ *is the class of I, then* $o(\bar{I})$ *is even.*

(3) *Let* $J = \prod_{\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}} \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}}(J)}$ *such that for some* $\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}$, $\mathrm{ord}_{\mathfrak{q}}(J)$ *is odd and* $\mathrm{ord}_{\mathfrak{q}}(I) \not\equiv \mathrm{ord}_{\mathfrak{q}}(J) \pmod 2$. *Then* $\bar{I} \neq \bar{J}$.

Proof. For the first assertion, we need that $\left[\frac{N(I)}{p_1'}\right] = \left[\frac{-N(I)}{p_2'}\right] = -1$ for certain prime divisors p_1', p_2' of d. Let $j = \max\{i : \mathrm{ord}_{\mathfrak{q}_i}(I) \text{ is odd}\}$. We observe that $j > 0$ and p_j is odd. We know that $\left(\frac{q_j}{p_j}\right) = \left(\frac{q_j^{\mathrm{ord}_{\mathfrak{q}_j}(I)}}{p_j}\right) = -1$, we have that for any $\mathfrak{q}_i \in \mathcal{I}_{\mathcal{P}}$, either $i < j$ or $\mathrm{ord}_{\mathfrak{q}_i}(I)$ is even. Then by construction, $\left(\frac{q_i^{\mathrm{ord}_{\mathfrak{q}_j}(I)}}{p_j}\right) = 1$ if $q_i \mid N(I)$, $q_i \neq q_j$. Therefore, $\left(\frac{N(I)}{p_j}\right) = \left[\frac{N(I)}{d}\right] = -1$. If some prime divisor p of d, $p \equiv 1 \pmod 4$, satisfies $\left(\frac{N(I)}{p}\right) = -1$, then $\left(\frac{-N(I)}{p}\right) = \left[\frac{-N(I)}{d}\right] = -1$. Now consider the case $\left(\frac{N(I)}{p}\right) = 1$, $p \equiv 1 \pmod 4$, $p \mid d$. If $d \equiv 1, 2 \pmod 4$, then it follows from Lemmas 8, 10 that $\left(\frac{N(I)}{p_g}\right) = 1$. Therefore,

$$\left(\frac{-N(I)}{p_g}\right) = \left[\frac{-N(I)}{p_g}\right] = \left[\frac{-N(I)}{d}\right] = -1.$$

Consider the case $d \equiv 3 \pmod 4$, $\left(\frac{N(I)}{p}\right) = 1$, $p \equiv 1 \pmod 4$. At the beginning of the proof, we saw that there is an odd prime $p_j \mid d$ such that $\left(\frac{N(I)}{p_j}\right) = -1$. If $k = \min\{i : \mathrm{ord}_{\mathfrak{q}_i}(I) \text{ is odd}\}$, then it follows that $\left(\frac{N(I)}{p_{k-1}}\right) = -1$. Since $d \equiv 3 \pmod 4$, d must have an odd number of prime divisors of the form $4x + 3$ and since p_j, $p_{k-1} \equiv 3 \pmod 4$, there are at least three of such prime numbers. Let $q_i \in \mathcal{P}$ be such that $\mathrm{ord}_{\mathfrak{q}_i}(I)$ is odd. Each of these has associated two prime divisors

$p_{i-1},\ \ p_i$ of d such that $\left(\frac{q_i}{p_{i-1}}\right) = \left(\frac{q_i}{p_i}\right) = -1$. Hence, there is an even number of pairs (p_l, q_m) that satisfy $\left(\frac{q_m}{p_l}\right) = -1$. Therefore, among the symbols $\left(\frac{N(I)}{p_0}\right), \ldots, \left(\frac{N(I)}{p_g}\right)$, an even number of them take the value -1 for some primes $p_i \equiv 3 \pmod 4$. It follows that there is some prime $p \equiv 3 \pmod 4$ such that $\left(\frac{N(I)}{p}\right) = 1$. As in the case $d \equiv 1, 2 \pmod 4$, we obtain $\left(\frac{-N(I)}{p}\right) = \left[\frac{-N(I)}{d}\right] = -1$. We note that $o(\bar{I})$ is even since I^a is non-principal for $a \in \mathbb{N}$ odd.

Finally, the class $\bar{I}^{-1}$ has a representative $I' = \prod_{\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}} \mathfrak{q}^{o(\bar{\mathfrak{q}}) - \mathrm{ord}_{\mathfrak{q}}(I)}$, where $\mathrm{ord}_{\mathfrak{q}}(I') \equiv \mathrm{ord}_{\mathfrak{q}}(I) \pmod 2$. Thus $\mathrm{ord}_{\mathfrak{q}}(JI')$ is odd and JI' is non-principal. Therefore, $\bar{J} \neq \bar{I}'^{-1}$ and so $\bar{I} \neq \bar{J}$. □

Lemma 12. *Let* $\mathbb{F}$ *be as always, I, J ideals of* $\mathcal{O}_{\mathbb{F}}$ *such that* $\left[\frac{\pm N(I)}{d}\right] = -1$, $o(\bar{I})$ *even and such that for any ramified prime* p, $p \nmid N(I)$ *and* $p \nmid N(J)$. *If* $J \in \bar{I}$, *then* $\left[\frac{\pm N(J)}{d}\right] = -1$.

Proof. Let $J \in \bar{I}$ such that $\left[\frac{N(J)}{d}\right] = 1$ or $\left[\frac{-N(J)}{d}\right] = 1$. Since $\bar{I}$ has even order, we have $\left[\frac{N(I^{o(\bar{I})})}{d}\right] = 1$. From the multiplicity of Legendre's symbol and Lemma 4, we obtain $\left[\frac{\pm N(I^{o(\bar{I})-1})}{d}\right] = -1$. Since $\left[\frac{N(J)}{d}\right] = 1$ or $\left[\frac{-N(J)}{d}\right] = 1$, in both cases, we have

$$\left[\frac{N(I^{o(\bar{I})-1}J)}{d}\right] = \left[\frac{-N(I^{o(\bar{I})-1}J)}{d}\right] = -1.$$

From $\overline{I^{o(\bar{I})-1}} = \bar{I}^{-1} = \bar{J}^{-1}$, it follows that $I^{o(\bar{I})-1}J$ is a principal ideal, which is impossible. Therefore, $\left[\frac{\pm N(J)}{d}\right] = -1$. □

If $\mathfrak{q}_i \in \mathcal{I}_{\mathcal{P}}$, then $o(\overline{\mathfrak{q}_i}) = 2^{k_i} t_i$ for some $k_i, t_i \in \mathbb{N}$ and t_i odd. For $\mathfrak{q}_i \in \mathcal{I}_{\mathcal{P}}$, we define $J_i = \mathfrak{q}_i^{t_i}$. Let $\mathcal{J}_{\mathcal{P}} = \{J_1, ..., J_{|\mathcal{P}|}\}$. Observe that since $\mathfrak{q}_i \neq \mathfrak{q}_j$ for $i \neq j$, $J_i \neq J_j$.

Lemma 13. *Let* $\mathbb{F}$ *be a real quadratic field and* J_i *as above. Then*:

(1) $\left[\frac{\pm N(J_i)}{d}\right] = -1$ *for* $1 \leq i \leq |\mathcal{P}|$.

(2) *If* $J_i \in \mathcal{J}_{\mathcal{P}}$, *then* $\overline{J_i} \notin \langle \overline{J_1}, ..., \overline{J_{i-1}}, \overline{J_{i+1}}, ..., \overline{J_{|\mathcal{P}|}} \rangle$.

(3) *We can modify the elements of* $\mathcal{J}_{\mathcal{P}}$ *in such a way that*

$$\langle \overline{J_1}, ..., \overline{J_{|\mathcal{P}|}} \rangle \cong \langle \overline{J_1} \rangle \times \cdots \times \langle \overline{J_{|\mathcal{P}|}} \rangle.$$

Proof. Before we start the proof, we observe that all the ideals we will be using are such that their norms and d are relative primes, so we can use Lemma 12. (1) follows from Lemma 4 since t_i is odd. For (2), let us suppose that $\overline{J_i} \in \langle \overline{J_1}, ..., \overline{J_{i-1}}, \overline{J_{i+1}}, ..., \overline{J_{|\mathcal{P}|}} \rangle$. Let $I = \prod_{J_l \in \mathcal{J}_{\mathcal{P}}} J_l^{e_l}$ with $e_i = 0$ and e_j non-negative integers. Clearly, $\bar{I} \in \langle \overline{J_1}, ..., \overline{J_{i-1}}, \overline{J_{i+1}}, ..., \overline{J_{|\mathcal{P}|}} \rangle$. If $I \in \overline{J_i}$, since $\left[\frac{\pm N(J_i)}{d}\right] = -1$, then $\left[\frac{\pm N(I)}{d}\right] = -1$. From this, some e_l is odd. Since $e_i = 0$, by Theorem 11(3), we have $J_i = \mathfrak{q}_i^{t_i} \notin \bar{I}$. As consequence of (2) we have that the rank of $\langle \overline{J_1}, ..., \overline{J_{|\mathcal{P}|}} \rangle$ is $|\mathcal{P}|$. To prove (3), we use the Algorithm. □

Theorem 14. *If* $\mathbb{F}$ *is a real quadratic field, then* $Cl_2 = \langle \overline{J_1}, ..., \overline{J_{|\mathcal{P}|}} \rangle$.

Proof. By Lemma 13 and Theorem 3, we know that $G_{\mathcal{J}} = \langle \overline{J_1}, ..., \overline{J_{|\mathcal{P}|}} \rangle$ is a 2-group with rank equal to the rank of Cl_2. Suppose there exists an ideal $I \subseteq \mathcal{O}_{\mathbb{F}}$ such that $o(\bar{I}) = 2^k$ with $k \in \mathbb{N}$ and $\gcd(N(I), \delta_{\mathbb{F}}) = 1$. Since the 2-rank of $Cl_{\mathbb{F}}$ is equal to the 2-rank of $G_{\mathcal{J}}$, there exist $t, e_1, ..., e_{|\mathcal{P}|} \in \mathbb{N}$ such that

$$\overline{I^t} = \overline{\prod_{J_i \in \mathcal{J}_{\mathcal{P}}} J_i^{e_i}},$$

with $\overline{I^t} \neq \overline{\mathcal{O}_{\mathbb{F}}}$. We chose the smallest t satisfying this condition. Note that t is even, otherwise $\bar{I} \in G_{\mathcal{J}}$. Thus $\left[\frac{N(I^t)}{d}\right] = 1$. On the other hand, at least one e_i is odd, since otherwise t would not be minimum. From Theorem 11, we have that $\left[\frac{N(I^t)}{d}\right] = -1$. This shows that any ideal $I \subseteq \mathcal{O}_{\mathbb{F}}$ with $\gcd(N(I), \delta_{\mathbb{F}}) = 1$ satisfies $\bar{I} \in G_{\mathcal{J}}$. Let p be a ramified prime and $\mathfrak{p}$ a prime ideal such that $N(\mathfrak{p}) = p$. We know that the rank of Cl_2 is the same as $G_{\mathcal{J}}$, so $\langle G_{\mathcal{J}}, \overline{\mathfrak{p}} \rangle$ must have the same rank as $G_{\mathcal{J}}$. This implies $\overline{\mathfrak{p}} \in G_{\mathcal{J}}$ or there is a maximal $H \in C_{G_{\mathcal{J}}}$ such that $H \subseteq \langle \overline{\mathfrak{p}} \rangle$. If the latter happens, $1 < o(H) \leq o(\overline{\mathfrak{p}}) \leq 2$, so $H = \langle \overline{\mathfrak{p}} \rangle$, $\overline{\mathfrak{p}} \in G_{\mathcal{J}}$ and therefore $G_{\mathcal{J}} = \langle G_{\mathcal{J}}, \overline{\mathfrak{p}} \rangle$. We apply this argument to all ramified primes to obtain $Cl_2 = G_{\mathcal{J}}$. $\square$

Lemma 15. *Let* $\mathbb{F}$ *be a real quadratic field. Every class in* $Cl_{\mathbb{F}}$ *has a representative I such that* $\gcd(N(I), \delta_{\mathbb{F}}) = 1$.

Proof. Let $\bar{J} \in Cl_{\mathbb{F}}$ such that $J = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1 \cdots \mathfrak{q}_r$, where $\mathfrak{p}_i$ is a ramified prime ideal for $1 \leq i \leq k$ and $\mathfrak{q}_i$ is an unramified prime ideal for $1 \leq i \leq r$. It will suffice to prove that every $\overline{\mathfrak{p}_i}$ has a representative that satisfies the affirmation.

First, we will prove the assertion for $d \equiv 1, 2 \pmod 4$. In this case, a prime p is ramified if and only if $p \mid d$, and the ideal of norm p_i is

$$\mathfrak{p}_i = \langle p_i, \sqrt{d} \rangle = \langle p_i, p_i + \sqrt{d} \rangle.$$

So we have

$$\langle p_i - \sqrt{d} \rangle \mathfrak{p}_i = \langle p_i(p_i - \sqrt{d}), p_i^2 - d \rangle = \langle p_i \rangle \langle p_i - \sqrt{d}, p_i - d/p_i \rangle,$$

so $\mathfrak{p}_i$ is in the same class than $\mathfrak{p}_i' = \langle p_i - \sqrt{d}, p_i - d/p_i \rangle$. Note that $\mathfrak{p}_i'$ is not necessarily a prime ideal. Observe that $\gcd(p, p_i - d/p_i) = 1$ for every prime p such that $p \mid d$, then $p \nmid p_i - d/p_i$ and $p \nmid N(p_i - d/p_i)$. The fact that $\mathfrak{p}_i' \mid \langle p_i - d/p_i \rangle$ implies $p \nmid N(\mathfrak{p}_i')$. Therefore, $\gcd(d, N(\mathfrak{p}_i')) = 1$. If we change every $\mathfrak{p}_i$ for $\mathfrak{p}_i'$, then we get a new ideal I related to J without ramified prime factors.

Now suppose $d \equiv 3 \pmod 4$. We proceed similarly as in the previous case, and we obtain an ideal $I \in \bar{J}$ such that $\gcd(N(I), d) = 1$. In this case, 2 is a ramified prime but $2 \nmid d$, so it is possible that $\mathfrak{p} = \langle 2, 1 + \sqrt{d}\rangle \mid I$. In this case, we have

$$\mathfrak{p}\langle 1 - \sqrt{d}\rangle = \langle 2(1 - \sqrt{d}), 1 - d\rangle = \langle 2\rangle\langle 1 - \sqrt{d} + (1 - d)/2\rangle,$$

where $\mathfrak{p}' = \langle 1 - \sqrt{d}, (1 - d)/2\rangle \sim \mathfrak{p}$ and $\frac{1-d}{2} \in \mathbb{Z}$ is odd. In particular, $2 \nmid N(\mathfrak{p}')$. Since $\gcd(1 - d, d) = 1$, we have $\gcd(N(\mathfrak{p}'), d) = 1$, hence $\gcd(N(\mathfrak{p}'), \delta_{\mathbb{F}}) = 1$. Replacing $\mathfrak{p}$ for $\mathfrak{p}'$, we obtain the ideal we wanted. □

Proposition 16. *Let* $\mathbb{F}$ *be a real quadratic field such that* $|Cl_{\mathbb{F}}| = 2^k$ *for some* $k \in \mathbb{N}$ *and* $\bar{I} \in Cl_{\mathbb{F}}$ *with* $\gcd(N(I), \delta_{\mathbb{F}}) = 1$. *Then* $\langle \bar{I}\rangle$ *is maximal in* $\mathcal{C}_{Cl_{\mathbb{F}}}$ *if and only if* $\left[\frac{\pm N(I)}{d}\right] = -1$.

Proof. We know that $Cl_{\mathbb{F}} = G_{\mathcal{J}} \cong \langle \overline{J_1}\rangle \times \cdots \times \langle \overline{J_{|\mathcal{P}|}}\rangle$. If $\langle \bar{I}\rangle$ is maximal in $\mathcal{C}_{Cl_{\mathbb{F}}}$, then I is related with some ideal

$$J = \prod_{J_i \in \mathcal{J}_{\mathcal{P}}} J_i^{\operatorname{ord}_{J_i} J}$$

with $\operatorname{ord}_{J_i} J$ odd. Theorem 11 implies that $\left[\frac{\pm N(I)}{d}\right] = -1$. Conversely, suppose $\langle \bar{I}\rangle$ is not maximal. Then $\langle \bar{I}\rangle \subsetneq \langle \bar{J}\rangle$ for a class $\bar{J}$. We can choose J in such a way that $\gcd(N(J), \delta_{\mathbb{F}}) = 1$. Therefore, $\bar{I} = \bar{J}^t$ for some $t \in \mathbb{N}$. As a consequence of the fact that $\bar{I} \neq \bar{J}$, we have that t is even. So, $\left[\frac{N(I)}{d}\right] = \left[\frac{N(J^t)}{d}\right] = 1$. □

Example 2. Let $\mathbb{F} = \mathbb{Q}(\sqrt{322})$. Since $322 = 2 \cdot 7 \cdot 23$, from Theorem 3 we have that the rank of Cl_2 is 1. We apply Lemma 10 with $t = 0$, $g = 2$. We will find a non-principal ideal $\mathfrak{q}_1$ such that it generates Cl_2. For this, we need a prime q_1 such that

$$\left(\frac{4 \cdot 322}{q_1}\right) = 1 \quad \text{and} \quad \left[\frac{\pm q_1}{322}\right] = -1.$$

Following the proof of Lemma 10, it is enough that q_1 satisfies

$$q_1 \equiv 5 \pmod 8, \quad \left(\frac{q_1}{7}\right) = \left(\frac{7}{q_1}\right) = -1, \quad \left(\frac{q_1}{23}\right) = \left(\frac{23}{q_1}\right) = 1. \tag{1}$$

From Lemma 5, we have that 325 satisfies (1), but it is not a prime. From Dirichlet's Theorem, we obtain that $q_1 = 325 + 1283 = 1613$ is prime and

$$\langle 1613 \rangle = \langle 1613, 100 + \sqrt{322} \rangle \langle 1613, 100 - \sqrt{322} \rangle.$$

Hence $\overline{\mathfrak{q}_1} = \overline{\langle 1613, 100 + \sqrt{322} \rangle}$ generates Cl_2 and $o(\overline{\mathfrak{q}_1}) = 4$.

Example 3. Let $d = 272490 = 2 \cdot 5 \cdot 293 \cdot 3 \cdot 31$ and $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. To find suitable generators of Cl_2, we use Lemma 10 with $g = 4$, $t = 2$. We observe that the rank of Cl_2 is 3. According to Lemma 7, we need a prime number q_1 such that

$$q_1 \equiv 5 \pmod 8, \quad \left(\frac{q_1}{5}\right) = -1, \quad \left(\frac{q_1}{293}\right) = \left(\frac{q_1}{3}\right) = \left(\frac{q_1}{31}\right) = 1.$$

Therefore, it is sufficient that q_1 satisfies

$$\begin{aligned} q_1 &\equiv 5 \pmod 8, \\ q_1 &\equiv 3 \pmod 5, \\ q_1 &\equiv 1 \pmod{27249}. \end{aligned} \tag{2}$$

The prime number $q_1 = 762973$ solves (2) and

$$\mathfrak{q}_1 = \langle 762973, 349636 + \sqrt{272490} \rangle$$

is a prime ideal such that $N(\mathfrak{q}_1) = q_1$ and $o(\overline{\mathfrak{q}_1}) = 8$. Similarly, we find $q_2 = 1895713$ and the prime ideal $\mathfrak{q}_2 = \langle 1895713, 507828 + \sqrt{272490} \rangle$ satisfies $N(\mathfrak{q}_2) = q_2$, $o(\overline{\mathfrak{q}_2}) = 8$. The prime $q_3 = 5674241$ and the prime ideal $\mathfrak{q}_3 = \langle 5674241, 1813618 + \sqrt{272490} \rangle$ satisfies $N(\mathfrak{q}_3) = q_3$, $o(\overline{\mathfrak{q}_3}) = 8$. Therefore, $Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_3} \rangle$.

The minimal relations between $\overline{\mathfrak{q}_1}$, $\overline{\mathfrak{q}_2}$, $\overline{\mathfrak{q}_3}$ that appear in Proposition 2 are

$$\overline{\mathfrak{q}_1}^4 = \overline{\mathfrak{q}_2}^4, \quad \overline{\mathfrak{q}_1}^2 = \overline{\mathfrak{q}_3}^2, \quad \overline{\mathfrak{q}_1}^8 = \overline{\mathfrak{q}_2}^8 = \overline{\mathfrak{q}_3}^8 = \overline{\mathcal{O}_{\mathbb{F}}}.$$

We replace $\overline{\mathfrak{q}_2}$ with $\overline{\mathfrak{q}_1}^{(2^1-1)(2^0)}\overline{\mathfrak{q}_2} = \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}$ and $\overline{\mathfrak{q}_3}$ with $\overline{\mathfrak{q}_1}^{(2^2-1)(2^0)}\overline{\mathfrak{q}_3} = \overline{\mathfrak{q}_1}^3\overline{\mathfrak{q}_3}$. Now we have $Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_1}^3\overline{\mathfrak{q}_3}\rangle$, with $o(\overline{\mathfrak{q}_1}) = 8$, $o(\overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}) = 4$ and $o(\overline{\mathfrak{q}_1}^3\overline{\mathfrak{q}_3}) = 2$. Continuing with the Algorithm, we check that this set of generators of Cl_2 cannot be simplified any further. Therefore,

$$Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_1\mathfrak{q}_2}, \overline{\mathfrak{q}_1}^3\overline{\mathfrak{q}_3}\rangle \cong \langle \overline{\mathfrak{q}_1}\rangle \times \langle \overline{\mathfrak{q}_1\mathfrak{q}_2}\rangle \times \langle \overline{\mathfrak{q}_1}^3\overline{\mathfrak{q}_3}\rangle \cong C_8 \times C_4 \times C_2.$$

4. Other Cases

Similar results can be found when we have an imaginary quadratic field $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$, where d is a rational positive squarefree integer. In this case, the norm of an element in $\mathbb{F}$ is always positive, hence, we will use $\left[\frac{N(I)}{d}\right]$ instead of $\left[\frac{\pm N(I)}{d}\right]$ and to construct $\mathcal{P}$, $\mathcal{I}_{\mathcal{P}}$, $\mathcal{J}_{\mathcal{P}}$ we will need to find prime numbers as follows:

1. If $d = p_0 \cdots p_g$ as in Lemma 6, then we can find $g+1$ prime numbers $q_0, \ldots, q_g$ such that $\left(\frac{p_i}{q_i}\right) = -1$, $\left(\frac{p_j}{q_i}\right) = 1$ for $i \neq j$ and $q_i \equiv 3 \pmod 4$. In this case, $\left(\frac{-1}{d}\right) = -1$ and $\left(\frac{q_i}{p_i}\right) = -1$.
2. If $d = 2p_1 \cdots p_g$ as in Lemma 7 or $d = p_0 p_1 \cdots p_g \equiv 3 \pmod 4$ as in Lemma 9, then we can find g prime numbers such that $\left(\frac{\delta_{\mathbb{F}}}{q_i}\right) = 1$ and $\left[\frac{q_i}{d}\right] = -1$. In fact, we can use the same q_i's we found in the real case.
3. If $d = p_0 p_1 \cdots p_g \equiv 1 \pmod 4$ as in Lemma 8, then $-d \equiv 3 \pmod 4$ and $\delta_{\mathbb{F}} = -4d$. In this case, we can find $g+1$ prime numbers $q_0, \ldots, q_g$ such that $\left(\frac{p_i}{q_i}\right) = -1$, $\left(\frac{p_j}{q_i}\right) = 1$, for $i \neq j$ and $q_i \equiv 3 \pmod 4$. Since $g \geq 1$, we always have a prime p_j such that $\left(\frac{p_j}{q_i}\right) = 1$ and $\left(\frac{q_i}{p_j}\right) = -1$, hence $\left[\frac{q_i}{d}\right] = -1$.

4. If $d = 2p_1 \cdots p_g \equiv 1 \pmod 4$ as in Lemma 10, then there are g primes

$$q_1, \ldots, q_g \text{ such that } \left(\frac{p_i}{q_i}\right) = -1, \left(\frac{p_j}{q_i}\right) = 1 \text{ for } i \neq j \text{ and } q_i \equiv 5 \pmod 8.$$

With these prime numbers, we define $\mathcal{P}$, $\mathcal{I}_{\mathcal{P}}$ and $\mathcal{J}_{\mathcal{P}}$ as in the real case. Lemmas 12, 13 and 15, Proposition 16 and Theorems 11 and 14 can be generalized removing the minus sign in $\left[\frac{\pm N(I)}{d}\right]$.

A particular case of what we have studied is when the exponent of $Cl_{\mathbb{F}}$ is 2. The next results follow from Theorem 14:

Corollary 17. *Let* $\mathbb{F}$ *be a quadratic field such that* $Cl_{\mathbb{F}}$ *has exponent* 2. *Then* $Cl_{\mathbb{F}} = \langle \mathcal{J}_{\mathcal{P}} \rangle$ *and each class contains an ideal of the form* $\prod_{J \in A} J$ *for some* $A \subseteq \mathcal{J}_{\mathcal{P}}$, *where we define* $\prod_{J \in \varnothing} J = \mathcal{O}_{\mathbb{F}}$.

Theorem 18. *Let* $\mathbb{F}$ *be a real quadratic field such that* $Cl_{\mathbb{F}}$ *has exponent* 2 *and* $I \subseteq \mathcal{O}_{\mathbb{F}}$ *be an ideal such that* $\gcd(N(I), \delta_{\mathbb{F}}) = 1$. *Then I is non-principal if and only if* $\left[\frac{\pm N(I)}{d}\right] = -1$.

Proof. Every class is represented by an ideal $I_A = \prod_{J \in A} J$ for some $\varnothing \neq A \subseteq \mathcal{J}_{\mathcal{P}}$. By Theorem 11(1), we have $\left[\frac{\pm N(I_A)}{d}\right] = -1$. If some ideal I satisfies $\left[\frac{\pm N(I)}{d}\right] = -1$, then by Lemma 12, any ideal J contained in $\bar{I}$ such that $\gcd(N(J), \delta_{\mathbb{F}}) = 1$ satisfies $\left[\frac{\pm N(J)}{d}\right] = -1$. Therefore, any non-principal ideal satisfies $\left[\frac{\pm N(I)}{d}\right] = -1$. The converse is true in any real quadratic field. □

The condition $\gcd(N(I), \delta_{\mathbb{F}}) = 1$ is necessary, otherwise if $\gcd(N(I), \delta_{\mathbb{F}}) > 1$, then there might exist non-principal ideals I such that $\left[\frac{N(I)}{d}\right] = 1$ or $\left[\frac{-N(I)}{d}\right] = 1$.

For example, if $\mathbb{F} = \mathbb{Q}(\sqrt{10})$, then $\left[\frac{\pm 5}{10}\right] = 1$ but $\langle 5, \sqrt{10}\rangle$ is non-principal. A similar result can be stated for the imaginary case.

Example 4. We are going to find the 2-class group of the imaginary quadratic field $\mathbb{F} = \mathbb{Q}(\sqrt{-665})$. Since $-665 = -(5)(7)(19) \equiv 3 \pmod 4$, $\delta_{\mathbb{F}} = -2660$, $p_0 = 5$, $p_1 = 7$ and $p_2 = 19$. The next table shows the first prime numbers $q \equiv 3 \pmod 4$ such that $\left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$. Here we can see that $q_0 = 3$, $q_1 = 71$ and $q_2 = 131$ satisfy the conditions that we required previously. In this case, $\mathfrak{p}_1 = \langle 3, 4 + \sqrt{-665}\rangle$, $\mathfrak{p}_2 = \langle 71, 20 + \sqrt{-665}\rangle$ and $\mathfrak{p}_3 = \langle 131, 11 + \sqrt{-665}\rangle$, $o(\mathfrak{p}_1) = o(\mathfrak{p}_2) = o(\mathfrak{p}_3) = 6$, $\mathcal{I}_{\mathcal{P}} = \{\mathfrak{p}_1^3, \mathfrak{p}_2^3, \mathfrak{p}_3^3\}$. If we apply the Algorithm, then we will find that $\mathcal{I}_{\mathcal{P}} = \mathcal{J}_{\mathcal{P}}$ and

$$Cl_2 \cong C_2 \times C_2 \times C_2.$$

q	$\left(\frac{\delta_F}{q}\right)$	$\left(\frac{5}{q}\right)$	$\left(\frac{7}{q}\right)$	$\left(\frac{19}{q}\right)$	$\left[\frac{q}{665}\right]$
3	**1**	**–1**	**1**	**1**	**–1**
23	1	–1	–1	–1	–1
43	1	–1	–1	–1	–1
71	**1**	**1**	**–1**	**1**	**–1**
79	1	1	–1	1	–1
103	1	–1	1	1	–1
131	**1**	**1**	**1**	**–1**	**–1**
139	1	1	1	–1	–1
151	1	1	–1	1	–1

Example 5. If $\mathbb{F} = \mathbb{Q}(\sqrt{-21})$, then $Cl_{\mathbb{F}} \cong C_2 \times C_2$; hence, an ideal is principal if and only if $\left[\frac{N(I)}{21}\right] = 1$. For example, $\langle 5, 2 + \sqrt{-21}\rangle$ is a non-principal ideal since $N(I) = 5$ and $\left[\frac{5}{21}\right] = -1$. The ideal $\langle 37, 41 + \sqrt{-21}\rangle$ is principal since $N(I) = 37$ and $4^2 \equiv 37 \pmod{21}$.

References

[1] J. M. Basilla and H. Wada, On efficient computation of the 2-parts of ideal class groups of quadratic fields, Proc. Japan Acad. Ser. A Math. Sci. 80(10) (2004), 191-193.

[2] W. Bosma and P. Stevenhagen, On the computation of quadratic 2-class groups, J. de Théorie des Nombres de Bordeaux 8(2) (1996), 283-313.

[3] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, KANT V4, J. Symbolic Comp. 24 (1997), 267-283.

[4] H. Hasse, An algorithm for determining the structure of the 2-Sylow subgroups of the divisor class group of a quadratic number field, Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973), Academic Press, 1975, pp. 341-352.

[5] R. Mollin, Algebraic Number Theory, CRC Press, 1999.

[6] D. Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, Math. Comp. 25 (1971), 837-853.

[7] W. A. Stein et al., Sage Mathematics Software (Version 4.6.1), The Sage Development Team, 2010, http://www.sagemath.org.