International Journal of Algebra, Vol. 6, 2012, no. 15, 729 - 745

A Relation between Ideals, Diophantine Equations and Factorization in Quadratic Fields $\mathbb{F}$ with $h_{\mathbb{F}} = 2$

Alejandro Aguilar-Zavoznik[1] **and Mario Pineda-Ruelas**[2]

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

Abstract

We solve the diophantine equations $d_1\, a_1^2 - d_2\, a_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right)$ to decide if an ideal in the ring of integers in a quadratic field $\mathbb{F}$ with $h_{\mathbb{F}} = 2$ is principal or non-principal. As a consequence of this, we distinguish prime and irreducible elements.

Mathematics Subject Classification: 11R11, 11R29, 11D09.

Keywords: Class number, diophantine equations, irreducible and prime element, Hilbert class field.

1 Introduction

Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, $\mathcal{O}_{\mathbb{F}}$ the ring of integers of $\mathbb{F}$, $Cl_{\mathbb{F}}$ its class group, $h_{\mathbb{F}}$ its class number, $\delta_{\mathbb{F}}$ the absolute discriminant of $\mathbb{F}$, $\delta_{\mathbb{K}/\mathbb{F}}$ the relative discriminant of $\mathbb{K}/\mathbb{F}$, $\overline{\mathfrak{I}_{\mathbb{F}}}$ denotes the class of the ideal $\mathfrak{I}_{\mathbb{F}}$ in $Cl_{\mathbb{F}}$ and $\mathbb{H}_{\mathbb{F}}$ is the Hilbert class field of $\mathbb{F}$. For $a \in \mathbb{Z}$, $b \in \mathbb{N}$, we will write $\left[\frac{a}{b}\right] = 1$ if and only if $x^2 \equiv a \pmod{b}$ is solvable with $x \in \mathbb{Z}$ and $\left[\frac{a}{b}\right] = -1$ if the congruence has no solutions. In [1], the authors proved:

Theorem 1.1. *Let $\mathbb{F}$ be a quadratic number field such that $Cl_{\mathbb{F}}$ has exponent 2 and $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ is an ideal such that* g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right), \delta_{\mathbb{F}}\right) = 1$. *Then $\mathfrak{I}_{\mathbb{F}}$ is a non-principal ideal if and only if* $\left[\dfrac{\pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right)}{d}\right] = -1$. □

In this paper we are going to relate this equivalence with diophantine equations of the form

$$d_1\, a_1^2 - d_2\, a_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right) \tag{1}$$

for $d = d_1\, d_2$, $d_1, d_2 \in \mathbb{Z}$. To accomplish this, we are going to find explicitly the Hilbert class field of a quadratic field such that $Cl_{\mathbb{F}}$ has exponent 2. The solubility of equation (1) has been studied using continued fractions, for example, in [4], [6], [7] and [8]. As an application, we will give a criterion to decide whether an element in $\mathcal{O}_{\mathbb{F}}$ is prime, irreducible or compound for certain class of quadratic number fields.

2 Extensions of ideals

Let us consider an extension of number fields $\mathbb{K}/\mathbb{F}$ and $\mathcal{O}_{\mathbb{K}}, \mathcal{O}_{\mathbb{F}}$ their rings of integers respectively. We will denote $\langle \alpha_1, \ldots, \alpha_t \rangle_{\mathbb{K}}$ the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by $\alpha_1, \ldots, \alpha_t \in \mathcal{O}_{\mathbb{K}}$, $\langle A_1, \ldots, A_t \rangle_{\mathbb{F}}$ the ideal of $\mathcal{O}_{\mathbb{F}}$ generated by $A_1, \ldots, A_t \in \mathcal{O}_{\mathbb{F}}$, $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ the absolute norm of $\alpha \in \mathbb{K}$, $N_{\mathbb{F}/\mathbb{Q}}(A)$ the absolute norm of $A \in \mathbb{F}$ and $N_{\mathbb{K}/\mathbb{F}}(\alpha)$ the relative norm of $\alpha \in \mathbb{K}$ in $\mathbb{K}/\mathbb{F}$. If $\mathfrak{I}_{\mathbb{F}}$ is an ideal of $\mathcal{O}_{\mathbb{F}}$, then $\langle \mathfrak{I}_{\mathbb{F}} \rangle_{\mathbb{K}}$ is the extension of $\mathfrak{I}_{\mathbb{F}}$ in $\mathcal{O}_{\mathbb{K}}$, this is, the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by the elements of $\mathfrak{I}_{\mathbb{F}}$. If $\mathfrak{I}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}}$, the contraction of $\mathfrak{I}_{\mathbb{K}}$ to $\mathcal{O}_{\mathbb{F}}$ is the ideal $\mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}}$. It is easy to show that:

Proposition 2.1. *Let $\mathbb{F} \subseteq \mathbb{K}$ be two number fields, $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{K}}$ their ring of integers and $\mathfrak{I}_{\mathbb{F}} = \langle A_1, A_2 \rangle_{\mathbb{F}}$ an ideal of $\mathcal{O}_{\mathbb{F}}$ with $A_1, A_2 \in \mathcal{O}_{\mathbb{F}}$. Then $\langle \mathfrak{I}_{\mathbb{F}} \rangle_{\mathbb{K}} = \langle A_1, A_2 \rangle_{\mathbb{K}}$.* □

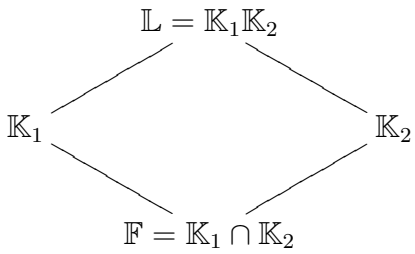
Corollary 2.2. *Let $\mathbb{F} \subseteq \mathbb{K}$ be two number fields, $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{K}}$ their rings of integers and $\mathfrak{I}_{\mathbb{K}}$ an ideal of $\mathcal{O}_{\mathbb{K}}$ with $\mathfrak{I}_{\mathbb{K}} = \langle A_1, A_2 \rangle_{\mathbb{K}}$, where $A_1, A_2 \in \mathcal{O}_{\mathbb{F}}$. Then $\mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}} = \langle A_1, A_2 \rangle_{\mathbb{F}}$.* □

If we extend an ideal of $\mathcal{O}_{\mathbb{F}}$ to $\mathcal{O}_{\mathbb{K}}$ and then restrict it back to $\mathcal{O}_{\mathbb{F}}$, the ideal remains the same. The inverse process can change the ideal. For example, consider $\mathbb{F} = \mathbb{Q}$ and $\mathbb{K} = \mathbb{Q}(\sqrt{10})$ and the ideal $\mathfrak{I}_{\mathbb{K}} = \left\langle 2, \sqrt{10} \right\rangle_{\mathbb{K}}$. The contraction $\mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}} = \langle 2 \rangle_{\mathbb{F}}$ and $\langle \mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}} \rangle_{\mathbb{K}} = \langle 2 \rangle_{\mathbb{K}} \neq \left\langle 2, \sqrt{10} \right\rangle_{\mathbb{K}}$.

The next result helps us to calculate the ramification index of an ideal in the composition of two fields.

Proposition 2.3. *Let $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ be number fields as in the next diagram,*

where every extension is Galois:



and $\mathfrak{p}_\mathbb{F}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_\mathbb{L}$ *prime ideals in the rings of integers of* $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ *respectively, such that* $\mathfrak{p}_\mathbb{F} = \mathfrak{p}_\mathbb{L} \cap \mathcal{O}_\mathbb{F} = \mathfrak{p}_1 \cap \mathcal{O}_\mathbb{F} = \mathfrak{p}_2 \cap \mathcal{O}_\mathbb{F}$, $\mathfrak{p}_1 = \mathfrak{p}_\mathbb{L} \cap \mathbb{K}_1$ *and* $\mathfrak{p}_2 = \mathfrak{p}_\mathbb{L} \cap \mathbb{K}_2$. *Let* $\mathfrak{q}_1, \mathfrak{q}_2 \in \{\mathfrak{p}_\mathbb{F}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_\mathbb{L}\}$ *such that* $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$. *If* $e(\mathfrak{q}_1/\mathfrak{q}_2)$ *denote the ramification index of* $\mathfrak{q}_1$ *over* $\mathfrak{q}_2$, *then* $e(\mathfrak{p}_\mathbb{L}/\mathfrak{p}_\mathbb{F}) = e(\mathfrak{p}_{\mathbb{K}_1}/\mathfrak{p}_\mathbb{F})e(\mathfrak{p}_{\mathbb{K}_2}/\mathfrak{p}_\mathbb{F})$.

Proof. See [9], pp. 263, **E**. □

3 The Hilbert class field of a family of quadratic fields

In this section we will describe the Hilbert class field of a quadratic field such that $Cl_\mathbb{F}$ has exponent 2. In [2] Proposition 1.2, H. Cohen and X. Roblot affirm that if $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d > 0$ and $h_\mathbb{F} = 2$, then there exist a divisor d_2 of $\delta_\mathbb{F}$ with $1 < d_2 < \delta_\mathbb{F}$ and $d_2 \equiv 0, 1 \pmod 4$, such that $\mathbb{H}_\mathbb{F} = \mathbb{F}(\sqrt{d_2})$. The problem is to find d_2. They affirm that, using theory of genera or Kummer theory, d_2 can be found in a finite number of steps. We will give a proof of this fact in which we find explicitly d_2. We will finish the section generalizing this result when the exponent of $Cl_\mathbb{F}$ is 2, including the imaginary case.

As an immediate consequence of Gauss Theorem on the 2-rank of $Cl_\mathbb{F}$ (see [1], Theorem 3, or [5] Theorem 3.70) we have:

Proposition 3.1. *Let* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *with* $h_\mathbb{F} = 2$. *For some distinct* $p, q, r > 0$ *odd rational prime numbers,* d *has one of the next forms:*

1. $d = 2\,p$ *with* $p \equiv 1 \pmod 4$.
2. $d = p\,q$ *with* $p \equiv q \equiv 1 \pmod 4$.
3. $d = p\,q$ *with* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$.
4. $d = 2\,p\,q$ *with* $p \equiv q \equiv 3 \pmod 4$.
5. $d = 2\,p\,q$ *with* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$.
6. $d = p\,q\,r$ *with* $p \equiv 1 \pmod 4$, $q \equiv r \equiv 3 \pmod 4$.

7. $d = -p$ *with* $p \equiv 1 \pmod 4$.
8. $d = -2\,p$.
9. $d = -p\,q$ *with* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$. □

In each one of the cases that we described in the previous proposition, there is exactly one way of factoring $d = d_1\,d_2$ such that $d_1, d_2 \neq 1$, $d_2 \equiv 1 \pmod 4$ and where at least one of the factors is positive:

1. $d_1 = 2$, $d_2 = p$.
2. $d_1 = p$, $d_2 = q$.
3. $d_1 = q$, $d_2 = p$.
4. $d_1 = 2$, $d_2 = p\,q$.
5. $d_1 = 2\,q$, $d_2 = p$.
6. $d_1 = p$, $d_2 = q\,r$.
7. $d_1 = -1$, $d_2 = p$.
8. $d_1 = -2, d_2 = p$ if $p \equiv 1 \pmod 4$ and $d_1 = 2, d_2 = -p$ if $p \equiv 3 \pmod 4$.
9. $d_1 = -q$, $d_2 = p$.

Theorem 3.2. *Let* $d = d_1\,d_2$, $d_2 \equiv 1 \pmod 4$, $d_1, d_2 \neq 1$ *and* $d_1 > 0$ *or* $d_2 > 0$. *If* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *with* $h_{\mathbb{F}} = 2$, *then* $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

Proof. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Note that $\left\{1, \dfrac{1+\sqrt{d_2}}{2}\right\}$ and $\{1, \sqrt{d_1}\}$ are bases of $\mathbb{K}/\mathbb{F}$ using only algebraic integers. If $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{K}}$ is a base of $\mathbb{K}$ as an $\mathbb{F}$-vector space, we will denote $\Delta(\mathcal{B})$ the discriminant of $\mathcal{B}$. We know that $\Delta(\{1, \sqrt{d_1}\}) = 4d_1$ and $\Delta\left(\left\{1, \dfrac{1+\sqrt{d_2}}{2}\right\}\right) = d_2$, furthermore

$$\text{g.c.d.}\,(4d_1, d_2) = \text{g.c.d.}\,(d_1, d_2) = 1.$$

Then, $\delta_{\mathbb{K}/\mathbb{F}} = \mathcal{O}_{\mathbb{F}}$ and $\mathbb{K}/\mathbb{F}$ is an unramified extension, including the infinite primes. Therefore $\mathbb{H}_{\mathbb{F}} = \mathbb{K}$. □

Theorem 3.3. *Let* $d = p_0 \cdots p_g$ *be a square-free rational integer,* $p_i > 0$ *prime for all* i *and* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *such that* $Cl_{\mathbb{F}}$ *has exponent* 2*:*

1. *If* $p_i \equiv 1, 2 \pmod 4$ *for all* i, *then* $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_g})$.

2. *If* $p_0 = 2$, $p_1 \equiv 3 \pmod 4$ *and* $p_i \equiv 1 \pmod 4$ *for* $i \geq 2$, *then*

$$\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{2\,p_1}, \sqrt{p_2}, \ldots, \sqrt{p_g}).$$

3. *If* $d \equiv 1, 2 \pmod 4$ *and for some* $0 \leq t < g$ *we have that* $p_0, \ldots, p_{t-1} \equiv 1, 2 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$, *then the Hilbert class field of* $\mathbb{F}$ *is*

$$\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_{t-1}}, \sqrt{p_g p_t}, \sqrt{p_g p_{t+1}}, \ldots, \sqrt{p_g p_{g-1}}).$$

Let us observe that there must be at least two prime numbers $p_{g-1}, p_g \equiv 3 \pmod 4$ *and the case* $t = 0$ *means* $p_i \equiv 3 \pmod 4$ *for* $i = 0, \ldots, g$.

4. *If* $d \equiv 3 \pmod 4$, *then* $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_g})$.

Proof. We will only prove the first assertion. For $i = 1, \ldots, g$ consider $\mathbb{L}_i = \mathbb{F}(\sqrt{p_i})$. Using the ideas of the proof of Theorem 3.2, it is easy to show that $\mathbb{L}_i/\mathbb{F}$ is an unramified extension. Since $\mathbb{L}_i/\mathbb{F}$ are unramified and $\mathbb{L}_i \cap \mathbb{L}_j = \mathbb{F}$ for $i \neq j$, then $\mathbb{L}_1 \cdots \mathbb{L}_g/\mathbb{F}$ is unramified as a consequence of Proposition 2.3. Finally, using Gauss Theorem on the 2-rank of a quadratic field, $[\mathbb{L}_1 \cdots \mathbb{L}_g : \mathbb{F}] = 2^{g-1} = o(Cl_{\mathbb{F}})$. Therefore, $\mathbb{H}_{\mathbb{F}} = \mathbb{L}_1 \cdots \mathbb{L}_g$. The proof of the other assertions are similar to these one. □

We have the imaginary version of the previous theorem. The proof is done as in the real case.

Theorem 3.4. *Let* $d = -p_0 \cdots p_g$ *be a square-free integer with* p_i *positive rational prime numbers and* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *such that the exponent of* $Cl_{\mathbb{F}}$ *is* 2*:*

1. *If* $d \equiv 1 \pmod 4$, *where* $p_0, \ldots, p_{t-1} \equiv 1 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$ *for some* $0 \leq t \leq g + 1$, *then*

$$\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_{t-1}}, \sqrt{-p_t}, \ldots, \sqrt{-p_g}).$$

The case $t = g+1$ *means that there is no prime number* $p \equiv 3 \pmod 4$.

2. *If* $d \equiv 2 \pmod 4$, *where* $p_0 = 2$, $p_1, \ldots, p_{t-1} \equiv 1 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$ *for some* $1 \leq t \leq g + 1$, *then*

$$\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{\pm 2}, \sqrt{p_1}, \ldots, \sqrt{p_{t-1}}, \sqrt{-p_t}, \ldots, \sqrt{-p_g}),$$

where the sign of 2 *is* $+$ *if* $d/2 \equiv 1 \pmod 4$ *and* $-$ *if* $d/2 \equiv 3 \pmod 4$.

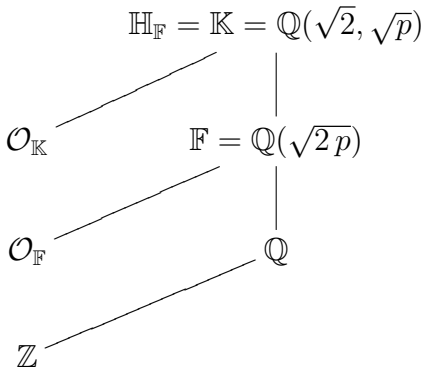
3. *If* $d \equiv 3 \pmod 4$, *then* $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{-1}, \sqrt{p_0}, \ldots, \sqrt{p_g})$. □

4 Principal ideals and diophantine equations

In this section, we are going to find a method to classify principal ideals in some quadratic fields. The criteria found in [1] is more general than the one we are going to find, but now we will have the advantage of relating this problem with the solutions of the diophantine equation of the form $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2\, N_{\mathbb{F}/\mathbb{Q}}\,(I)$, where the variables are b_1 and b_2. In this work, when we say the diophantine equation $f(b_1, b_2) = \pm c$ is solvable, we mean that it has one solution, $b_1, b_2 \in \mathbb{Z}$ for at least one of the signs. Sometimes the equation has solutions for both signs, other times, only one sign works.

Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $h_{\mathbb{F}} = 2$. As seen in the previous section, there exist $d_1, d_2 \in \mathbb{Z}$ with $d_2 \equiv 1 \pmod 4$ such that $d = d_1\, d_2$ and at least one is positive. Since every prime that divides d_1 or d_2 is ramified in $\mathbb{F}$, then there exist ideals $\mathfrak{d}_1, \mathfrak{d}_2$ such that $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_1) = |d_1|$ and $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_1) = |d_2|$. Clearly, $\mathfrak{d}_1, \mathfrak{d}_2$ are unique. Since $\mathfrak{d}_1\mathfrak{d}_2 = \left\langle \sqrt{d} \right\rangle_{\mathbb{F}}$, then both ideals are principal or both are non-principal. From the previous equality we see that $\overline{\mathfrak{d}_2} = \overline{\mathfrak{d}_1}^{-1}$ and since $\mathfrak{d}_1^2 = \langle d_1 \rangle_{\mathbb{F}}$, then $\overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_1}^{-1}$, hence $\overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_2}$.

First, we will study the case $d = 2\,p$, $0 < p \equiv 5 \pmod 8$ a rational prime. Here we have a simple criterion to identify principal and non-principal ideals. Let $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$, $\mathbb{H}_{\mathbb{F}} = \mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ the Hilbert class field of $\mathbb{F}$ and $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{K}}$ the respective rings of integers. Clearly, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \sqrt{2\,p}\,\mathbb{Z}$.



Since $2 \mid \delta_{\mathbb{F}}$, then $\langle 2 \rangle_{\mathbb{F}}$ ramifies and if $\mathfrak{p}_2 = \left\langle 2, \sqrt{2\,p} \right\rangle_{\mathbb{F}}$, then $\langle 2 \rangle_{\mathbb{F}} = \mathfrak{p}_2^2$. We have $p \equiv 5 \pmod 8$ hence $\left(\dfrac{2}{p}\right) = \left[\dfrac{2}{p}\right] = \left[\dfrac{2}{2\,p}\right] = -1$ (see [1], Lemma 4), then $\mathfrak{p}_2$ is a non-principal ideal and, since $\mathfrak{p}_2^2$ is principal, we have $h_{\mathbb{F}}$ is even. Now we will study the case $h_{\mathbb{F}} = 2$.

Lemma 4.1. *Let* $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ *with* $0 < p \equiv 5 \pmod 8$, $h_{\mathbb{F}} = 2$, $\mathfrak{p}_2 = \left\langle 2, \sqrt{2\,p} \right\rangle_{\mathbb{F}}$ *and* $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{p})$. *Then:*

1. $\langle \mathfrak{p}_2 \rangle_{\mathbb{K}} = \left\langle \sqrt{2} \right\rangle_{\mathbb{K}}$.

2. *If $\mathfrak{J}_{\mathbb{F}}$ is a non-principal ideal of $\mathcal{O}_{\mathbb{F}}$, then there exists $B = b_1\sqrt{2}+b_2\sqrt{p} \in \mathcal{O}_{\mathbb{K}}$ such that $b_1, b_2 \in \mathbb{Z}$ and $\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}} = \langle B \rangle_{\mathbb{K}}$.*

Proof. Clearly, $\langle \mathfrak{p}_2 \rangle_{\mathbb{K}} = \left\langle 2, \sqrt{2\,p} \right\rangle_{\mathbb{K}}$. In $\mathcal{O}_{\mathbb{K}}$, $\sqrt{2} \mid 2$ and $\sqrt{2} \mid \sqrt{2\,p}$, hence $\left\langle \sqrt{2} \right\rangle_{\mathbb{K}} \mid \langle \mathfrak{p}_2 \rangle_{\mathbb{K}}$. On one hand, since $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}(\alpha)\right)$, we have

$$N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{2}\right) = N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}\left(\sqrt{2}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}(-2) = 4, \tag{2}$$

and on the other hand

$$N_{\mathbb{K}/\mathbb{Q}}\left(\langle \mathfrak{p}_2 \rangle_{\mathbb{K}}\right) = N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}\left(\langle \mathfrak{p}_2 \rangle_{\mathbb{K}}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}\left({\mathfrak{p}_2}^2\right) = N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{p}_2\right)^2 = 4 \tag{3}$$

(see [9], pp 235, **C** and **D**) Now, 1 follows from (2) and (3).

Since $h_{\mathbb{F}} = 2$, then $\overline{\mathfrak{p}_2} = \overline{\mathfrak{J}_{\mathbb{F}}}$ and $\mathfrak{p}_2\mathfrak{J}_{\mathbb{F}}$ is principal. Let $\mathfrak{p}_2\mathfrak{J}_{\mathbb{F}} = \langle A \rangle_{\mathbb{F}}$. If we consider this equality in $\mathbb{K}$ we have

$$\langle A \rangle_{\mathbb{K}} = \langle \mathfrak{p}_2 \rangle_{\mathbb{K}} \langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}} = \left\langle \sqrt{2} \right\rangle_{\mathbb{K}} \langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}}\,.$$

The field $\mathbb{K}$ is the Hilbert class field of $\mathbb{F}$, then $\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}}$ must be a principal ideal, say $\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}} = \langle \beta \rangle_{\mathbb{K}}$. Because of this

$$\left\langle \sqrt{2} \right\rangle_{\mathbb{K}} \langle \beta \rangle_{\mathbb{K}} = \left\langle \sqrt{2}\,\beta \right\rangle_{\mathbb{K}} = \langle A \rangle_{\mathbb{K}}\,,$$

which shows that $\sqrt{2}\,\beta\,\mu = A$ for some unit $\mu \in \mathcal{O}_{\mathbb{K}}$ and $A = a_1 + a_2\sqrt{2\,p}$. Since $\langle \beta \rangle_{\mathbb{K}} = \langle \mu\,\beta \rangle_{\mathbb{K}}$ we can suppose

$$\sqrt{2}\,\beta = A = a_1 + a_2\sqrt{2\,p}.$$

From the previous equality we have $\sqrt{2} \mid A$ and, since $\sqrt{2} \mid a_2\sqrt{2\,p}$, then $\sqrt{2} \mid a_1$, where $a_1 \in \mathbb{Z}$ and a_1 must be even. Therefore

$$\sqrt{2}\,\beta = 2\frac{a_1}{2} + a_2\,\sqrt{p}\,\sqrt{2} = \sqrt{2}\left(\frac{a_1}{2}\sqrt{2} + a_2\sqrt{p}\right),$$

with $\dfrac{a_1}{2}, a_2 \in \mathbb{Z}$. Hence, for each non-principal ideal $\mathfrak{J}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ there exists an element of the form $b_1\sqrt{2} + b_2\sqrt{p} \in \mathcal{O}_{\mathbb{K}}$ where $b_1, b_2 \in \mathbb{Z}$ such that $\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}} = \left\langle b_1\sqrt{2} + b_2\sqrt{p} \right\rangle_{\mathbb{K}}$. This proves 2. □

Observe that if $\mathfrak{J}_{\mathbb{F}}$ is an ideal of $\mathcal{O}_{\mathbb{F}}$ such that $\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}} = \langle \beta \rangle_{\mathbb{K}}$ for some $\beta = b_1\sqrt{2} + b_2\sqrt{p}$, then

$$N_{\mathbb{K}/\mathbb{Q}}(\beta) = (b_1\sqrt{2} + b_2\sqrt{p})(b_1\sqrt{2} - b_2\sqrt{p})(-b_1\sqrt{2} + b_2\sqrt{p})(-b_1\sqrt{2} - b_2\sqrt{p}),$$

this is $N_{\mathbb{K}/\mathbb{Q}}(\beta) = (2\,b_1^2 - p\,b_2^2)^2$. Furthermore, $N_{\mathbb{K}/\mathbb{Q}}\left(\langle \mathfrak{J}_{\mathbb{F}} \rangle_{\mathbb{K}}\right) = \left(N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{J}_{\mathbb{F}}\right)\right)^2$ and $|2\,b_1^2 - p\,b_2^2| = N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{J}_{\mathbb{F}}\right)$. From this, if $\mathfrak{J}_{\mathbb{F}}$ is a non-principal ideal, then, $2\,b_1^2 - p\,b_2^2 = \pm N_{\mathbb{F}}(\mathfrak{J}_{\mathbb{F}})$ has an integer solution on the variables b_1, b_2 for at least one sign. Also, on any real quadratic field $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, if $\mathfrak{J}_{\mathbb{F}}$ is a principal ideal of $\mathcal{O}_{\mathbb{F}}$, then one of the equations $b_1^2 - d\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{J}_{\mathbb{F}}\right)$ must have an integer solution.

Proposition 4.2. *Let $d \equiv 5 \pmod 8$ be a rational integer, $c \in \mathbb{N}$ odd and b_1, b_2, b_3, b_4 variables. Consider the equations:*

1. $b_1^2 - 2\,d\,b_2^2 = \pm c$.
2. $2\,b_3^2 - d\,b_4^2 = \pm c$.

It is not possible that 1 *and* 2 *are solvable at the same time.*

Proof. Since $d \equiv 5 \pmod 8$, $-2\,d \equiv 6 \pmod 8$. The squares modulo 8 are $0, 1, 4$, multiplying this values times 6 we get $0, 6, 0$ modulo 8. With this in mind, the possible odd values of $b_1^2 - 2\,d\,b_2^2 \equiv b_1^2 + 6\,b_2^2 \pmod 8$ are ± 1. With a similar procedure, the only odd values that $2\,b_3^2 - d\,b_4^2 \equiv 2\,b_3^2 + 3\,b_4^2 \pmod 8$ can take modulo 8 are ± 3. Therefore, the proposition holds. □

From the previous proof we can conclude that:

Theorem 4.3. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ be a real quadratic field with $h_{\mathbb{F}} = 2$, $p \equiv 5 \pmod 8$ a rational prime and $\mathcal{O}_{\mathbb{F}}$ the ring of integers of $\mathbb{F}$. If $\mathfrak{I}_{\mathbb{F}}$ is an ideal of $\mathcal{O}_{\mathbb{F}}$ with $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ odd, then:*

1. *$\mathfrak{I}_{\mathbb{F}}$ is principal if and only if at least one of the equations $b_1^2 - 2\,p\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ have a solution with $b_1, b_2 \in \mathbb{Z}$.*
2. *$\mathfrak{I}_{\mathbb{F}}$ is a non-principal ideal if and only if there exists a solution of $2\,b_1^2 - p\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ with $b_1, b_2, \in \mathbb{Z}$.*
3. *$\mathfrak{I}_{\mathbb{F}}$ is a principal ideal if and only if $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}) \equiv \pm 1 \pmod 8$.* □

If an ideal $\mathfrak{I}_{\mathbb{F}}$ has even norm, we can factor it as $\mathfrak{I}_{\mathbb{F}} = \mathfrak{p}_2^k \mathfrak{I}_{\mathbb{F}}{}'$, where $\mathfrak{I}_{\mathbb{F}}{}'$ has odd norm and $\mathfrak{p}_2$ is the only ideal of $\mathcal{O}_{\mathbb{F}}$ with $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_2) = 2$. If k is even, the ideal is principal if and only if $\mathfrak{I}_{\mathbb{F}}{}'$ is principal. If k is odd, then $\mathfrak{I}_{\mathbb{F}}$ is principal if and only if $\mathfrak{I}_{\mathbb{F}}{}'$ is a non-principal ideal.

Theorem 4.4. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ be a real quadratic field with $h_{\mathbb{F}} = 2$, $p \equiv 5 \pmod 8$, $\mathcal{O}_{\mathbb{F}}$ its ring of integers and $\mathfrak{I}_{\mathbb{F}}$ an ideal of $\mathcal{O}_{\mathbb{F}}$ with $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ even. If $\mathfrak{I}_{\mathbb{F}} = \mathfrak{p}_2^k \mathfrak{I}_{\mathbb{F}}{}'$ as before, then $\mathfrak{I}_{\mathbb{F}}$ is principal if and only if one of the following assertions is true:*

1. *k is odd and $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}{}') \equiv \pm 1 \pmod 8$.*
2. *k is even and $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}{}') \equiv \pm 3 \pmod 8$.* □

We have proved that, when $d = 2\,p > 0$ with $p \equiv 5 \pmod 8$ and $h_{\mathbb{F}} = 2$, if $\mathfrak{I}_{\mathbb{F}}$ is a principal ideal of $\mathcal{O}_{\mathbb{F}}$ with odd norm, then $\langle \mathfrak{I}_{\mathbb{F}} \rangle_{\mathbb{K}}$ has a generator of the form $a_1 + a_2\sqrt{d}$, and if the ideal is non-principal, it has a generator $a_1\sqrt{d_1} + a_2\sqrt{d_2}$. We will say that an element of the form $a_1 + a_2\sqrt{d}$ is a type 1

element and the type 2 elements will be those with the form $a_1\sqrt{d_1}+a_2\sqrt{d_2}$. It will be important to observe what happens if we multiply this kind of elements. Let $d = d_1\, d_2$:

$$(a_1 + a_2\sqrt{d})(a_3\sqrt{d_1} + a_4\sqrt{d_2}) = (a_1\, a_3 + a_2\, a_4\, d_2)\sqrt{d_1} + (a_1\, a_4 + a_2\, a_3\, d_1)\sqrt{d_2},$$

$$(a_1\sqrt{d_1} + a_2\sqrt{d_2})(a_3\sqrt{d_1} + a_4\sqrt{d_2}) = (a_1\, a_3\, d_1 + a_2\, a_4\, d_2) + (a_1\, a_4 + a_2\, a_3)\sqrt{d},$$

this products are in agreement with the fact that a principal ideal times a non-principal ideal is a non-principal ideal, while the product of two non-principal ideals gives a principal ideal. Also, observe that $\mathfrak{d}_1^2 = \langle d_1\rangle_{\mathbb{F}}$ and $\left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}^2 = \langle d_1\rangle_{\mathbb{K}}$, which implies $\langle\mathfrak{d}_1\rangle_{\mathbb{K}}^2 = \left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}^2$, and using the unique factorization on ideals, $\langle\mathfrak{d}_1\rangle_{\mathbb{K}} = \left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}$. In the same way, $\langle\mathfrak{d}_2\rangle_{\mathbb{K}} = \left\langle\sqrt{d_2}\right\rangle_{\mathbb{K}}$. In some cases it is possible that $a_1, a_2 \notin \mathbb{Z}$, but $a_1 + a_2\sqrt{d}$ or $a_1\sqrt{d_1} + a_2\sqrt{d_2}$ are algebraic integers, for example, if $d \equiv 1 \pmod 4$, then $\dfrac{1+\sqrt{d}}{2}$ is an algebraic integer.

Next, we will see that with certain hypothesis we can generalize the previous results and we will see what happens in the other cases.

Proposition 4.5. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d = d_1\, d_2$ square free, $d_1, d_2 \in \mathbb{Z}$ and $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. If $\mathfrak{I}_{\mathbb{F}}, \mathfrak{J}_{\mathbb{F}}$ are ideals of $\mathcal{O}_{\mathbb{F}}$ such that $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ and $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ with $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ type 2 elements, then $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$ in $Cl_{\mathbb{F}}$.*

Proof. Let $\mathfrak{d}_1, \mathfrak{d}_2$ be the only ideals of $\mathcal{O}_{\mathbb{F}}$ with norms $|d_1|, |d_2|$ respectively. Let us multiply $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ and $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ by $\sqrt{d_1}$. Since α, β and $\sqrt{d_1}$ are type 2 elements, then $\alpha\sqrt{d_1}$ and $\beta\sqrt{d_2}$ are type 1 elements, this is $\langle\mathfrak{I}_{\mathbb{F}}\mathfrak{d}_1\rangle_{\mathbb{K}}$ and $\langle\mathfrak{J}_{\mathbb{F}}\mathfrak{d}_1\rangle_{\mathbb{K}}$ have type 1 generators, which shows that $\mathfrak{I}_{\mathbb{F}}\mathfrak{d}_1$ and $\mathfrak{J}_{\mathbb{F}}\mathfrak{d}_1$ are principal ideals in $\mathcal{O}_{\mathbb{F}}$, so, they are related. Because of this, there exist $A, B \in \mathcal{O}_{\mathbb{F}} - \{0\}$ such that $A\,\mathfrak{I}_{\mathbb{F}}\,\mathfrak{d}_1 = B\,\mathfrak{J}_{\mathbb{F}}\,\mathfrak{d}_1$. Using the cancellation law, $A\,\mathfrak{I}_{\mathbb{F}} = B\,\mathfrak{J}_{\mathbb{F}}$ and $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$. □

Proposition 4.6. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d = d_1\, d_2$ a square-free rational integer, $d_1, d_2 \in \mathbb{Z}$ and $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. If $\mathfrak{I}_{\mathbb{F}}, \mathfrak{J}_{\mathbb{F}}$ are ideals in $\mathcal{O}_{\mathbb{F}}$ such that $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$ in $Cl_{\mathbb{F}}$ and $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ with $\alpha \in \mathcal{O}_{\mathbb{K}}$ a type 2 element, then there exist a type 2 element $\beta \in \mathcal{O}_{\mathbb{K}}$ such that $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$.*

Proof. Since $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$, then there exist $A, B \in \mathcal{O}_{\mathbb{F}} - \{0\}$ such that $A\mathfrak{I}_{\mathbb{F}} = B\mathfrak{J}_{\mathbb{F}}$. Hence, $\langle A\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle A\,\alpha\rangle_{\mathbb{K}} = \langle B\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$. From the previous equality, $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$ must be a principal ideal, say $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ for some $\beta \in \mathcal{O}_{\mathbb{K}}$. Therefore, there exists a unit $\mu \in \mathcal{O}_{\mathbb{K}}$ such that $A\,\alpha = B\,\beta\,\mu$. We may assume that $\beta = \beta\mu$ and $A\,\alpha = B\,\beta$. Operating,

$$\beta = \frac{A}{B}\alpha,$$

where $\frac{A}{B} \in \mathbb{K}$ is a type 1 element and α is a type 2 element. Even though one of the elements is not necessarily an algebraic integer, the product is still a type 2 algebraic integer and β is the element we are looking for. □

Since $\langle \mathfrak{d}_1 \rangle_{\mathbb{K}} = \langle \sqrt{d_1} \rangle_{\mathbb{K}}$, then there always exists a class of $Cl_{\mathbb{F}}$ with an ideal such that, when we extend it to $\mathcal{O}_{\mathbb{K}}$ it has a type 2 generator. Using the previous results, for each factorization $d = d_1\, d_2$ we have a class related with the type 2 elements that emerge with this numbers. Nevertheless, this classes are not necessarily unequal, it is possible that one class of ideals correspond to the type 2 elements of two distinct factorizations of d, as it can be seen on the Corollary 4.8. The next result shows that this criterion is stronger, not only it helps us to identify ideals of $\mathcal{O}_{\mathbb{F}}$ related with $\mathfrak{d}_1$ and $\mathfrak{d}_2$, it also works to classify the ideals of $\mathcal{O}_{\mathbb{K}}$ such that when we restrict them to $\mathcal{O}_{\mathbb{F}}$ they are related with this pair of ideals.

Proposition 4.7. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d = d_1\, d_2$ a square-free integer, $d_1, d_2 \in \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and $\mathfrak{d}_1, \mathfrak{d}_2$ the only ideals of $\mathcal{O}_{\mathbb{F}}$ with norms $|d_1|, |d_2|$ respectively. If $\mathfrak{I}_{\mathbb{K}} = \langle \alpha \rangle_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}}$ with $\alpha = a_1\sqrt{d_1} + a_2\sqrt{d_2}$, $a_1, a_2 \in \mathbb{Q}$, then $\mathfrak{I}_{\mathbb{F}} = \mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}}$ is an ideal such that $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_2}$.*

Proof. Let $\beta_1 = \alpha\sqrt{d_1}, \beta_2 = \alpha\sqrt{d_2} \in \mathcal{O}_{\mathbb{F}}$. Let us consider the ideal $\mathfrak{J}_{\mathbb{K}} = \langle \beta_1, \beta_2 \rangle_{\mathbb{K}}$. We know that $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) \mid \text{g.c.d.}\left(N_{\mathbb{K}/\mathbb{Q}}(\beta_1), N_{\mathbb{K}/\mathbb{Q}}(\beta_2)\right)$. Since d_1 and d_2 are relatively primes and using the definition of β_1 and β_2, then $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{d_1}\right)$ and $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{d_2}\right)$ are relatively primes too. This implies that

$$\text{g.c.d.}\left(N_{\mathbb{K}/\mathbb{Q}}(\beta_1), N_{\mathbb{K}/\mathbb{Q}}(\beta_2)\right) = |N_{\mathbb{K}/\mathbb{Q}}(\alpha)|$$

and, in consequence, $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) \mid N_{\mathbb{K}/\mathbb{Q}}(\alpha)$. Since $\alpha \mid \mathfrak{J}_{\mathbb{K}}$, then $\mathfrak{I}_{\mathbb{K}} = \mathfrak{J}_{\mathbb{K}}$, this is $\langle \alpha \rangle_{\mathbb{K}} = \langle \beta_1, \beta_2 \rangle_{\mathbb{K}}$. We know that $\beta_1, \beta_2 \in \mathcal{O}_{\mathbb{F}}$, so, using Corollary 2.2, we obtain $\mathfrak{I}_{\mathbb{F}} = \mathfrak{I}_{\mathbb{K}} \cap \mathcal{O}_{\mathbb{F}} = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}}$, an ideal that, when we extend it to $\mathcal{O}_{\mathbb{K}}$ it is $\mathfrak{I}_{\mathbb{K}} = \langle \alpha \rangle_{\mathbb{K}}$, so, for Proposition 4.5, $\mathfrak{I}_{\mathbb{F}}$ is related with $\mathfrak{d}_1$ and $\mathfrak{d}_2$. □

The next corollaries generalize what we found for the case $d = 2\,p$. Observe that if $d \equiv 1 \pmod 4$, then an integral basis of $\mathcal{O}_{\mathbb{F}}$ is $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ and since any type 2 algebraic integer multiplied by $\sqrt{d_1}$ or $\sqrt{d_2}$ must be in $\mathcal{O}_{\mathbb{F}}$, then in this case we can have elements of the form $\frac{a_1\sqrt{d_1} + a_2\sqrt{d_2}}{2}$ with $a_1, a_2 \in \mathbb{Z}$ odd. Because of this, we need to include a $s^2 = 4$ in the right side of the diophantine equations that we will use next.

Corollary 4.8. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d = d_1\, d_2$ square-free, $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathfrak{d}_1, \mathfrak{d}_2$ the only ideals of $\mathcal{O}_{\mathbb{F}}$ with $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = |d_1|$, $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_2) = |d_2|$ and $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ an ideal. If $\mathfrak{d}_1, \mathfrak{d}_2$ are principal ideals, then $\mathfrak{I}_{\mathbb{F}}$ is a principal*

ideal if and only if there exists a solution of $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2\, N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$ *with* $b_1, b_2 \in \mathbb{Z}$ *where* $s = 1$ *if* $d \equiv 2, 3 \pmod 4$ *or* $s = 2$ *if* $d \equiv 1 \pmod 4$. □

Corollary 4.9. *Let* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *with* $d = d_1\, d_2$ *square-free,* $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathfrak{d}_1, \mathfrak{d}_2$ *the only ideals of* $\mathcal{O}_{\mathbb{F}}$ *with* $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_1) = |d_1|$ *and* $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_2) = |d_2|$, $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ *an ideal and* $s = 1$ *if* $d \equiv 2, 3 \pmod 4$ *or* $s = 2$ *if* $d \equiv 1 \pmod 4$. *If* $\mathfrak{d}_1, \mathfrak{d}_2$ *are non-principal ideals, then:*

1. $\mathfrak{I}_{\mathbb{F}}$ *is principal if and only if at least one of the equations* $b_1^2 - d\, b_2^2 = \pm s^2 N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$ *has a solution with* $b_1, b_2 \in \mathbb{Z}$.

2. $\mathfrak{I}_{\mathbb{F}}$ *is a non-principal ideal if and only if there exists a solution of* $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2 N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$ *with* $b_1, b_2, \in \mathbb{Z}$. □

Example 4.10. *Let* $d = 2 \cdot 3 \cdot 5 \cdot 7$ *and* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. *In the next table we can see the different factorizations of* d *with* d_1, d_2 *positive integers.*

d_1	d_2
1	210
2	105
3	70
5	42
6	35
7	30
10	21
14	15

Let $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7$ *be the only ideals of* $\mathcal{O}_{\mathbb{F}}$ *with norm* $2, 3, 5, 7$ *respectively. Since* d *has four prime factors and some of this are congruent with* 3 *modulo* 4, *then the* 2*-rank of* $Cl_{\mathbb{F}}$ *is* 2, *in fact* $Cl_{\mathbb{F}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *where* $\mathfrak{p}_2\mathfrak{p}_7$ *and* $\mathfrak{p}_3\mathfrak{p}_5$ *are principal ideals,* $\mathfrak{p}_2, \mathfrak{p}_7, \mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ *are in the same class,* $\mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ *are in a second class of non-principal ideals and* $\mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_5, \mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_3\mathfrak{p}_7$ *are in the last class. In this case, an ideal* $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ *is principal if and only if*

$$b_1^2 - 210\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}}) \quad \textit{and} \quad 14 b_1^2 - 15\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$$

are solvable; $\mathfrak{I}_{\mathbb{F}} \in \overline{\mathfrak{p}_2}$ *if and only if*

$$2\, b_1^2 - 105\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}}) \quad \textit{and} \quad 7 b_1^2 - 30\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$$

are solvable; $\mathfrak{I}_{\mathbb{F}} \in \overline{\mathfrak{p}_3}$ *if and only if*

$$3\, b_1^2 - 70\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}}) \quad \textit{and} \quad 5 b_1^2 - 42\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I}_{\mathbb{F}})$$

are solvable; $\mathfrak{I}_{\mathbb{F}} \in \overline{\mathfrak{p}_2\mathfrak{p}_3}$ *if and only if*

$$6\,b_1^2 - 35\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right) \quad \textit{and} \quad 10\,b_1^2 - 21\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right)$$

are solvable.

In the case $d = 2\,p > 0$ with $p \equiv 5 \pmod 8$ we already saw that $\mathfrak{d}_1, \mathfrak{d}_2$ are non-principal ideals. We will finish this section showing that if $p \equiv 1 \pmod 8$ the mentioned ideals are principal. The next example will be helpful as a guide for the proof.

Example 4.11. *Let* $d = d_1\,d_2$ *with* $d_1 = 2$ *and* $d_2 = 17$, $\mathfrak{d}_1, \mathfrak{d}_2$ *the only ideals of* $\mathcal{O}_{\mathbb{F}}$ *such that* $N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{d}_1\right) = d_1$ *and* $N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{d}_2\right) = d_2$. *In this case* $\mathfrak{d}_1, \mathfrak{d}_2$ *are principal ideals. In fact, the prime* 3 *splits in* $\mathbb{F}$ *since* $34 \equiv 1 \pmod 3$ *and*

$$\left(\frac{\delta_{\mathbb{F}}}{3}\right) = \left(\frac{4 \cdot 34}{3}\right) = \left(\frac{34}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Also,

$$\langle 3\rangle_{\mathbb{F}} = \left\langle 3, 1 + \sqrt{34}\right\rangle_{\mathbb{F}} \left\langle 3, 1 - \sqrt{34}\right\rangle_{\mathbb{F}}.$$

None of this ideals are principal, since otherwise, there is $\alpha = a_1 + a_2\sqrt{34}$ *with* $N_{\mathbb{F}/\mathbb{Q}}\left(\alpha\right) = \pm 3$. *We will prove that* α *can not exist. Since* $a_1^2 - 34\,a_2^2$ *is odd, then* a_1 *must be odd, hence* $a_1^2 \equiv 1 \pmod 8$. *If* a_2 *is even, then* $34\,a_2^2 \equiv 0 \pmod 8$ *and if* a_2 *is odd, then* $34\,a_2^2 \equiv 2 \pmod 8$. *Therefore* $a_1^2 - 34\,a_2^2 \equiv \pm 1 \pmod 8$. *This proves that there are no elements with norm* ± 3 *modulo* 8, *hence,* $\left\langle 3, 1 + \sqrt{34}\right\rangle_{\mathbb{F}}$ *and* $\left\langle 3, 1 - \sqrt{34}\right\rangle_{\mathbb{F}}$ *are non-principal ideals.*

It is clear that $17\,b_1^2 - 2\,b_2^2 = \pm 3$ *has no integer solution, watching it as a congruence modulo* 8. *Therefore, none of the four equations* $a_1^2 - 34\,a_2^2 = \pm 3$ *and* $17\,b_1^2 - 2\,b_2^2 = \pm 3$ *has an integer solution. Using the contrapositive of* Corollary 4.9, *the ideals* $\mathfrak{d}_1$ *and* $\mathfrak{d}_2$ *must be non-principals.*

The previous example can be generalized when $d = 2\,p$, $p \equiv 1 \pmod 8$.

Proposition 4.12. *Let* $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ *with* $p > 0$ *a rational prime and* $p \equiv 1 \pmod 8$. *Then, there exists a non-principal ideal* $\mathfrak{I}_{\mathbb{F}}$ *of* $\mathcal{O}_{\mathbb{F}}$ *such that the equation* $p\,b_1^2 - 2\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{F}}\right)$ *has no integer solution.*

Proof. In general, if $p \equiv 1 \pmod 8$, then $p\,b_1^2 - 2\,b_2^2 \equiv \pm 1 \pmod 8$, so, it is enough to find a non-principal ideal with norm $\pm 3 \pmod 8$.

Let $a \in \mathbb{Z}$ be such that $\left(\frac{a}{p}\right) = -1$. Since g.c.d. $(p, 8) = 1$, there exist $b \in \mathbb{Z}$ such that $b \equiv a \pmod p$ and $b \equiv 3 \pmod 8$. Using Dirichlet's Theorem on primes in arithmetic progression, there exist an infinity of rational prime

numbers $\equiv b \pmod{8\,p}$. Let q be one of this prime numbers. Since $q \equiv 3 \pmod 8$ and $q \equiv a \pmod p$ we have

$$\left(\frac{2}{q}\right) = -1, \quad \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1, \quad \left[\frac{q}{2\,p}\right] = -1, \quad \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1.$$

From this, there is an ideal $\mathfrak{q}$ with $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{q}) = q$ such that $\mathfrak{q}$ is a non-principal ideal. Now, we observe that $p\,b_1^2 - 2\,b_2^2 \equiv \pm 3 \pmod 8$ has no integer solution since $q \equiv 3 \pmod 8$. □

Corollary 4.13. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ with $p > 0$ a rational prime, $p \equiv 1 \pmod 8$, $h_{\mathbb{F}} = 2$ and $\mathfrak{d}_1, \mathfrak{d}_2$ the only ideals of $\mathcal{O}_{\mathbb{F}}$ such that $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = 2$ and $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_2) = p$. Then, $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are principal ideals.*

Proof. Using Proposition 4.12, there is a non-principal ideal $\mathfrak{I}_{\mathbb{F}}$ that does not satisfy the equation $p\,b_1^2 - 2\,b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$. Because of the Proposition 4.6, none of the non-principal ideals solve the equation, so the class that solves the equation is the one with the principal ideals. The assertion follows using the contrapositive of Corollary 4.9. □

In the imaginary case, the next result asserts that $\mathfrak{d}_1, \mathfrak{d}_2$ are non-principal ideals unless $|d_1| = 1$ or $|d_2| = 1$.

Proposition 4.14. *Let $d = d_1\,d_2 < 0$ be a square-free rational integers with $|d_1| \neq 1 \neq |d_2|$, $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ and $\mathfrak{d}_1, \mathfrak{d}_2$ the only ideals of $\mathcal{O}_{\mathbb{F}}$ with norms $|d_1|, |d_2|$ respectively. The ideals $\mathfrak{d}_1, \mathfrak{d}_2$ are non-principal.*

Proof. Let $A = a_1 + a_2\sqrt{d}$ with $N_{\mathbb{F}/\mathbb{Q}}(A) = a_1^2 - d\,a_2^2 = a_1^2 + |d|\,a_2^2$ square-free. Using this condition, $a_2 \neq 0$, so $N_{\mathbb{F}/\mathbb{Q}}(A) \geq |d|$. Since d_1, d_2 are square-free integers and $|d_1| < |d|$, $|d_2| < |d|$, then there is no element with norm $|d_1|$ or $|d_2|$, so $\mathfrak{d}_1, \mathfrak{d}_2$ are non-principal ideals. □

Corollary 4.15. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ with $d = d_1\,d_2 < 0$, $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $|d_1| \neq 1 \neq |d_2|$, $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ an ideal and $s = 1$ if $d \equiv 2, 3 \pmod 4$, $s = 2$ if $d \equiv 1 \pmod 4$. Then:*

1. *$\mathfrak{I}_{\mathbb{F}}$ is principal if and only if the equation $b_1^2 - d\,b_2^2 = s^2 N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ has a solution with $b_1, b_2 \in \mathbb{Z}$.*

2. *$\mathfrak{I}_{\mathbb{F}}$ is a non-principal ideal if and only if $d_1\,b_1^2 - d_2\,b_2^2 = \pm s^2 N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ is solvable with $b_1, b_2 \in \mathbb{Z}$.* □

In [10], H. Stark classified the imaginary quadratic fields with $h_{\mathbb{F}} = 2$:

Theorem 4.16. *If $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field, then $h_{\mathbb{F}} = 2$ if and only if $d = -5$, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427.* □

We can apply the Corollary 4.15 to these 18 numbers except for $d = -5$, -13, -37, that are the ones without the condition $|d_1| \neq 1 \neq |d_2|$. In these cases we use Theorem 1.1 to classify principal ideals.

5 Classification of prime and irreducible elements in quadratic fields with $h_{\mathbb{F}} = 2$

Now we are going to study an application of Theorem 1.1 or of the affirmation 3 of Theorem 4.3. We will use this to classify prime, irreducible and compound elements of the ring of integers of a quadratic field with $h_{\mathbb{F}} = 2$. The next proposition will be helpful to achieve this. It's proof is simple, so we leave it to the readers.

Proposition 5.1. *Let $\mathbb{F}$ be a number field, $\mathcal{O}_{\mathbb{F}}$ the ring of integers of $\mathbb{F}$ and $P \in \mathcal{O}_{\mathbb{F}} - \{0\}$. Then:*

1. *P is a prime element if and only if $\langle P \rangle$ is a prime ideal.*
2. *P is an irreducible element if and only if the ideal $\langle P \rangle$ is maximal in the set of of proper principal ideals of $\mathcal{O}_{\mathbb{F}}$.* □

If $h_{\mathbb{F}} = 2$, then the product of two non-principal ideals gives a principal ideal. From Proposition 5.1 it follows that P is irreducible but not prime if and only if $\langle P \rangle = \mathfrak{pq}$ where $\mathfrak{p}, \mathfrak{q}$ are non-principal prime ideals.

Let $\mathfrak{I}_{\mathbb{F}}$ be an ideal such that g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}), \delta_{\mathbb{F}}\right) > 1$. If we want to know if $\mathfrak{I}_{\mathbb{F}}$ is principal, we factor $\mathfrak{I}_{\mathbb{F}} = \mathfrak{I}_1\mathfrak{I}_2$ in such a way that g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_1), \delta_{\mathbb{F}}\right) = 1$ and each prime ideal that divides $\mathfrak{I}_2$ is a ramified ideal. Then $\mathfrak{I}_{\mathbb{F}}$ is principal if and only if $\overline{\mathfrak{I}_1} = \overline{\mathfrak{I}_2}^{-1}$. If $h_{\mathbb{F}} = 2$, then $\mathfrak{I}_{\mathbb{F}}$ is principal if and only if $\mathfrak{I}_1, \mathfrak{I}_2$ are both principal or both non-principal ideals.

Theorem 5.2. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with d a square-free rational integer, $h_{\mathbb{F}} = 2$ and $P \in \mathcal{O}_{\mathbb{F}}$ such that* g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}(P), \delta_{\mathbb{F}}\right) = 1$. *Then P is prime if and only if one of the following assertions holds:*

1. *$|N_{\mathbb{F}/\mathbb{Q}}(P)| = q$ is a rational prime such that $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = 1$ and $\left[\dfrac{q}{d}\right] = 1$ or $\left[\dfrac{-q}{d}\right] = 1$.*
2. *$N_{\mathbb{F}/\mathbb{Q}}(P) = q^2$ where q is a rational prime number such that $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = -1$.*

Proof. It is enough to prove that $|N_{\mathbb{F}/\mathbb{Q}}(P)| = q$ is prime if and only if 1 holds. Remember that $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})$ is prime if and only if $\mathfrak{I}_{\mathbb{F}}$ is a ramified or split prime ideal. By hypothesis, g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}(P), \delta_{\mathbb{F}}\right) = 1$, so $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = 1$. Using Theorem 1.1, it follows that $\mathfrak{I}_{\mathbb{F}}$ is a principal ideal if and only if $\left[\dfrac{q}{d}\right] = 1$ or $\left[\dfrac{-q}{d}\right] = 1$, in particular, if $\mathfrak{I}_{\mathbb{F}} = \langle P \rangle$ then 1 holds. The assertion 2 happens when q is an inert prime. □

Theorem 5.3. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with d a square-free rational integer, $h_{\mathbb{F}} = 2$ and $P \in \mathcal{O}_{\mathbb{F}}$ such that* g.c.d. $\left(N_{\mathbb{F}/\mathbb{Q}}(P), \delta_{\mathbb{F}}\right) = 1$. *Then P is irreducible if and only if one of the next assertions holds:*

1. *P is a prime element.*
2. *$|N_{\mathbb{F}/\mathbb{Q}}(P)| = pq$, where p, q are rational prime elements with $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$ and $\left[\frac{\pm p}{d}\right] = \left[\frac{\pm q}{d}\right] = -1$, for at least one of the signs, where $\pm p$ and $\pm q$ can have the same sign or not.*

Proof. If P is a non-prime irreducible element, then $\langle P \rangle = \mathfrak{pq}$, where $\mathfrak{p}, \mathfrak{q}$ are non-principal prime ideals. The norm of each of these ideals must be prime numbers, since otherwise $\mathfrak{p}$ and $\mathfrak{q}$ must be both principal ideals. Let $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}) = p$, $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{q}) = q$. Hence $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$. The condition $\left[\frac{\pm p}{d}\right] = \left[\frac{\pm q}{d}\right] = -1$ proves that the ideals are non-principal. □

The case when $\mathbb{F}$ is an imaginary quadratic field is similar, the only difference is that instead of $\pm$, we only need $+$, since there are only positive norms.

Example 5.4. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. In this example, $Cl_{\mathbb{F}} = \{\overline{1}, \overline{\langle 2, \sqrt{10}\rangle}\}$, so $h_{\mathbb{F}} = 2$. The ramified primes are 2 and 5 and $\langle 2, \sqrt{10}\rangle$ and $\langle 5, \sqrt{10}\rangle$ are non-principal ideals. A Prime p splits if $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = 1$, this is, if $p \equiv 1,\ 3,\ 9,\ 13,\ 27,\ 31,\ 37,\ 39 \pmod{40}$. On the other hand, using* Theorem 4.3, $\left[\frac{\pm a}{10}\right] = 1$ *if and only if $a \equiv \pm 1 \pmod 8$. If $p \equiv 7,\ 11,\ 17,\ 19,\ 21,\ 23,\ 29,\ 33 \pmod{40}$, then p is inert. Hence, we have:*

1. *$P \in \mathcal{O}_{\mathbb{F}}$ is a prime element if and only if one of the next assertions holds:*
   a) *$|N_{\mathbb{F}/\mathbb{Q}}(P)| = p$ for a rational prime $p \equiv \pm 1 \pmod 8$.*
   b) *$|N_{\mathbb{F}/\mathbb{Q}}(P)| = p^2$, with $p \equiv 7,\ 11,\ 17,\ 19,\ 21,\ 23,\ 29,\ 33 \pmod{40}$.*
2. *$P \in \mathcal{O}_{\mathbb{F}}$ is irreducible but not a prime element if $|N_{\mathbb{F}/\mathbb{Q}}(P)| = pq$ with p, q prime numbers such that $p \equiv 2,\ 3,\ 5 \pmod 8$ and $q \equiv 2,\ 3,\ 5 \pmod 8$.*

Example 5.5. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{34})$. Since $Cl_{\mathbb{F}} = \{\overline{\mathcal{O}_{\mathbb{F}}}, \overline{\mathfrak{p}_3}\}$, where $\mathfrak{p}_3 = \left\langle 3, 1 + \sqrt{34}\right\rangle$, then $h_{\mathbb{F}} = 2$. Using* Theorem 3.2, *$d_1 = 2$, $d_2 = 17 \equiv 1 \pmod 8$, hence $\mathfrak{d}_1 = \left\langle 6 + \sqrt{34}\right\rangle$ is a principal ideal. This means that we can not give the solution modulo 8 as we did in the previous example, so we must express the result modulo $34 \cdot 4 = 136$, using* Theorem 1.1.

1. *$P \in \mathcal{O}_{\mathbb{F}}$ is a prime element if and only if one of the next assertions is true:*

   a) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p$ *for some rational prime* $p \equiv 1,\ 2,\ 9,\ 15,\ 17,\ 25,\ 33,\ 47,\ 49,\ 55,\ 81,\ 87,\ 89,\ 103,\ 111,\ 121,\ 127,\ 135 \pmod{136}$.

   b) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p^2$*, for some rational prime* $p \equiv 7,\ 13,\ 19,\ 21,\ 23,\ 31,\ 35,\ 39,\ 41,\ 43,\ 53,\ 57,\ 59,\ 63,\ 65,\ 67,\ 69,\ 71,\ 73,\ 77,\ 79,\ 83,\ 93,\ 95,\ 97,\ 101,\ 105,\ 113,\ 115,\ 117,\ 123,\ 129 \pmod{136}$.

2. *$P \in \mathcal{O}_{\mathbb{F}}$ is irreducible but not prime if* $|N_{\mathbb{F}/\mathbb{Q}}(P)| = pq$ *with* $p \equiv 3,\ 5,\ 11,\ 27,\ 29,\ 37,\ 45,\ 61,\ 75,\ 91,\ 99,\ 107,\ 109,\ 125,\ 131,\ 133 \pmod{136}$, $q \equiv 3,\ 5,\ 11,\ 27,\ 29,\ 37,\ 45,\ 61,\ 75,\ 91,\ 99,\ 107,\ 109,\ 125,\ 131,\ 133 \pmod{136}$ *and* p, q *rational primes.*

Example 5.6. *Let us consider* $\mathbb{F} = \mathbb{Q}(\sqrt{-5})$*, where* $\delta_{\mathbb{F}} = -20$*,* $h_{\mathbb{F}} = 2$ *and* $Cl_{\mathbb{F}} = \{\overline{\mathcal{O}_{\mathbb{F}}}, \overline{\langle 2, 1+\sqrt{-5}\rangle_{\mathbb{F}}}\}$*. Using Theorem 1.1, we know that an ideal* $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ *with* $\gcd(N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}), \delta_{\mathbb{F}}) = 1$ *is principal if and only if* $\left[\dfrac{N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})}{5}\right] = 1$*. It is easy to see that* $\langle 2, 1+\sqrt{-5}\rangle$ *is a non-principal ideal since* $b_1^2 + 5\,b_2^2 = 2$ *has no solution with* $b_1, b_2 \in \mathbb{Z}$ *and the only ideal with norm* 5 *is* $\langle\sqrt{-5}\rangle_{\mathbb{F}}$*. So:*

1. *$P \in \mathcal{O}_{\mathbb{F}}$ is a prime element if and only if one of the next assertions is true:*

   a) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p$ *for some prime* $p \equiv 0,\ 1,\ 4 \pmod{5}$*. This happens when* $p \equiv 1,\ 5,\ 9 \pmod{20}$.

   b) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p^2$*, with* $p \equiv 11,\ 13,\ 17,\ 19 \pmod{20}$ *a rational prime number.*

2. *$P \in \mathcal{O}_{\mathbb{F}}$ is irreducible but not prime if* $|N_{\mathbb{F}/\mathbb{Q}}(P)| = pq$ *with* $p \equiv 2,\ 3,\ 7 \pmod{20}$ *and* $q \equiv 2,\ 3,\ 7 \pmod{20}$.

References

[1] Aguilar-Zavoznik A., Pineda-Ruelas M., 2-class group of quadratic fields, *JP J. Algebra Number Theory Appl.*, **22**, no. 2 (2011), 155-174.

[2] Cohen H., Roblot X. F., Computing the Hilbert class field of real quadratic fields, *Math. Comp.*, **69**, no. 231 (1999), 1229-1244.

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

[4] Halter-Koch F., Diophantine equations of Pellian type, *J. Number Theory*, **131**, no. 9 (2011), 1597-1615.

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

[6] Mollin R., The Diophantine equation $ax^2 - by^2 = c$ and simple continued fractions, *Int. Math. J.*, **2**, no. 1 (2002), 1-6.

[7] Mollin R., The Diophantine equation $AX^2 - BY^2 = C$ solved via continued fractions, *Acta Math. Univ. Comenian. (N.S.)*, **71**, no. 2 (2002), 121-138.

[8] Mollin R., A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$, *JP J. Algebra Number Theory Appl.*, **4**, no. 1 (2004), 159-207.

[9] Ribenboim P., *Clasical theory of algebraic numbers*, Springer-Velag, UTX, New York, 2001.

[10] Stark H., On complex quadratic fields with class-number two (Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday), *Math. Comp.*, **29** (1975), 289-302.

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

Received: March, 2012