The lattice of primary ideals of orders in quadratic number fields

G. Peruginelli and P. Zanardo

March 23, 2015

Abstract

Let \( O \) be an order in a quadratic number field \( K \) with ring of integers \( D \), such that the conductor \( \mathfrak{f} = fD \) is a prime ideal of \( O \). We give a complete description of the \( \mathfrak{f} \)-primary ideals of \( O \). They form a lattice with a particular structure by layers; the first layer, which is the core of the lattice, consists of those \( \mathfrak{f} \)-primary ideals not contained in \( \mathfrak{f}^2 \). We get three different cases, according to whether the prime number \( f \) is split, inert or ramified in \( D \).

Keywords: Orders, Conductor, Primary ideal, Lattice of ideals.

MSC Classification codes: 11R11, 11R04.

Introduction

One of the equivalent definition of a Dedekind domain is that every ideal is equal to a product of prime ideals; the fact that this factorization into prime ideals is unique is a consequence of the definition (see for example [9, §6, p. 270]). We are interested here in quadratic orders, that is, integral domains \( O \) whose integral closure is the ring of integers \( D \) of a quadratic number field \( K = \mathbb{Q}[^2d], \) \( d \) a square-free integer. We say that an order is proper if it is not integrally closed, that is, \( O \subsetneq D \). Since a Dedekind domain is integrally closed ([9, Theorem 13, p. 275]), a proper order does not enjoy the aforementioned property of unique factorization into prime ideals.
However, since an order is a one-dimensional Noetherian domain, each ideal of \( O \) can be written uniquely as a product of primary ideals (see for example \[9, Theorem 9, Chapt. IV, § 5, p. 213\]). An order \( O \) is determined by its conductor \( \mathfrak{F} \), defined as the largest ideal of \( D \) contained in \( O \); equivalently, \( \mathfrak{F} = \{ x \in O : xD \subseteq O \} \). Since \( D \) is a finitely generated \( O \)-module, \( \mathfrak{F} \) is always non-zero and it is a proper ideal of \( O \) if and only if the order is proper. Each ideal coprime to the conductor has a unique factorization into prime ideals of \( O \) \[6, Lemma 2.26, p. 389\]. These ideals are said to be regular. In particular, each regular primary ideal is equal to a power of its radical. Actually, this condition characterizes the regular primary ideals (see \[5, Lemma 2.3\]). More interesting is the situation for primary ideals that are non-regular. Here we consider the case where the conductor \( \mathfrak{F} \) of a quadratic order \( O \) is a prime ideal of \( O \), so that \( \mathfrak{F} = fD \), for some prime number \( f \in \mathbb{Z} \).

Among many others, we recall that Butts and Pall, in \[1\] and \[2\], have investigated ideals in quadratic orders. They addressed the problem of determining the number of factorizations of an ideal as a product of two ideals with given norms, without the assumption that the ideal is regular. The main results they gave are focused on invertible ideals. From a different point of view, Zanardo and Zannier \[8\] studied the class semigroup of quadratic orders, showing that it has a Clifford semigroup structure.

The purpose of the present paper is to give a detailed description of the structure of the lattice of \( \mathfrak{F} \)-primary ideals of a quadratic order \( O \). We also provide generating sets for each \( \mathfrak{F} \)-primary ideal, in a somehow canonical way. By means of such generators, we immediately see the relations of containment between these ideals; in particular, we find at once the minimal power of \( \mathfrak{F} \) contained in a \( \mathfrak{F} \)-primary ideal.

We get three completely different lattices of \( \mathfrak{F} \)-primary ideals, according to whether \( fD \) is a prime ideal in \( D \) (inert case), or it is the product of two distinct prime ideals of \( D \) (split case), or it is equal to the square of a prime ideal of \( D \) (ramified case). However, these lattices have a crucial property in common, namely, a structure by layers. This means that the structure of the lattice is determined by its first layer, namely the set of \( \mathfrak{F} \)-primary ideals not contained in \( \mathfrak{F}^2 \), which we call basic \( \mathfrak{F} \)-primary ideals. The remaining part of the lattice is formed by the \( n \)-th layers \((n > 1)\) of the ideals contained in \( \mathfrak{F}^n \) and not contained in \( \mathfrak{F}^{n+1} \), and all these layers reproduce the same pattern of the first layer.

Quadratic orders in number fields is a natural and important class of integral domains whose lattice of primary ideals is a disjoint union of lattices structured by layers. From the previous discussion it follows that when \( N \neq \mathfrak{F} \) is a prime ideal of \( O \), the lattice of \( N \)-primary ideals is just a chain.
In Sections 1 and 2 we give the definition of $\mathfrak{F}$-basic ideals, which are $\mathfrak{F}$-primary ideals not contained in $\mathfrak{F}^2$, and prove their main properties. The $\mathfrak{F}$-basic ideals constitute the first layer of the lattice of $\mathfrak{F}$-primary ideals, hence it suffices to describe them to determine the whole structure. We firstly characterize the $\mathfrak{F}$-basic ideals which are also $\mathfrak{D}$-modules (that is, ideals of $\mathfrak{D}$). This is a crucial step to get a complete description of the first layer, since every $\mathfrak{F}$-basic ideal lies between a suitable $\mathfrak{F}$-basic $\mathfrak{D}$-module $Q$ and $fQ$. Moreover, for each $\mathfrak{F}$-basic ideal (either $\mathfrak{D}$-module or not), we define a special set of generators that make the mutual relations of containment evident. We also identify the $\mathfrak{F}$-basic ideals that are principal. We show that there are exactly $f + 1$ pairwise distinct intermediate ideals properly lying between $\mathfrak{F}$ and $\mathfrak{F}^2$. Moreover, the quotient group of the units of $\mathfrak{D}/\mathfrak{F}$ modulo the units of $\mathfrak{O}/\mathfrak{F}$ acts freely on the set of intermediate ideals which are not $\mathfrak{D}$-modules (Proposition 2.10).

In Section 3 we examine separately the three cases mentioned above, namely, $f$ inert, split or ramified in $\mathfrak{D}$.

When $f$ is inert, $\mathfrak{F}$ itself is the only $\mathfrak{F}$-basic ideal that is a $\mathfrak{D}$-module. As a consequence of this fact all the basic ideals lie between $\mathfrak{F}$ and $\mathfrak{F}^2$, and, in particular, their number is finite, equal to $f + 2$. Note that, under the present circumstances, the local ring $\mathfrak{O}_{\mathfrak{F}}$ is $\mathfrak{F}$-chained, in the sense of Salce’s paper [7].

The split case is the most interesting one. In fact, we have infinitely many $\mathfrak{F}$-basic ideals, each of them lying between a special $\mathfrak{F}$-basic ideal $Q_k$ ($k > 0$) that is also a $\mathfrak{D}$-module, and $fQ_k$. The $Q_k$’s are generated by $f^k$ and a naturally defined element $t_k \in \mathfrak{F}$ which generates a basic $\mathfrak{F}$-primary ideal. There are exactly $f - 1$ ideals properly between $Q_k$ and $fQ_k$ that are not $\mathfrak{D}$-modules, and they are described in terms of the generators of $Q_k$.

Finally, in the case $f$ is ramified, we again get finitely many $\mathfrak{F}$-basic ideals, but not all of them are between $\mathfrak{F}$ and $\mathfrak{F}^2$. Indeed, if $\mathfrak{F} = fD = P^2$, where $P$ is a prime ideal of $\mathfrak{D}$, the $\mathfrak{F}$-basic ideals all lie either between $\mathfrak{F} = P^2$ and $\mathfrak{F}^2 = P^4$, or between $P^3$ and $P^5$. Under the present circumstances, in order to obtain the generators of the $\mathfrak{F}$-basic ideals, we must take care of the exceptional case when $f = 2$ and $d \equiv 3$ modulo 4.

1 General definitions and results

In what follows, we will freely use the standard results on rings of integers in number fields, as can be found, for instance, in [9, Chapter V] and [6, §6.2]. As usual, for both elements $z \in \mathfrak{D}$ and ideals $I$, the symbols $\bar{z}$, $\bar{I}$ and $N(z)$, $N(I)$ denote the conjugates and the norms, respectively; $D^*$, $\mathfrak{O}^*$ denote the multiplicative groups of
the units of $D$ and $O$. If $I$ is an ideal of $O$, $ID$ denotes the extended ideal in $D$, i.e., the ideal of $D$ generated by $I$. Moreover, in order to simplify the notation, the symbol $A \subset B$ will denote proper containment.

We fix some standing notation. Let $d$ be a square-free integer. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is equal to $D = \mathbb{Z}[\omega]$, where either $\omega = \sqrt{d}$, when $d \equiv 2, 3$ modulo 4, or $\omega = (1 + \sqrt{d})/2$, when $d \equiv 1$ modulo 4. In the latter case, we get $\omega^2 = \omega - (1 + d)/4$.

Let us fix $f > 0$ and consider the order $O = \mathbb{Z}[f\omega] = \mathbb{Z} + f\omega\mathbb{Z}$ with integral closure $D$. By definition, the conductor of $O$ in $D$ is the ideal $F = \{x \in O : xD \subseteq O\} = fD = f\mathbb{Z} + f\omega\mathbb{Z} = fO + f\omega O$.

Recall that $F$ is the largest ideal of $D$ contained in $O$. In particular, $F$ is not a principal ideal of $O$. A direct check shows that $F^2 = fF$, hence $F^k = f^{k-1}F$ for each $k > 0$. It is also useful to note that $N(F^k) = |O/F^k| = |\mathbb{Z}/f^k\mathbb{Z} + \mathbb{Z}f\omega/\mathbb{Z}f^k\omega| = f^{2k-1}$.

Since $O/F \cong \mathbb{Z}/f\mathbb{Z}$, we immediately see that $F$ is a prime ideal of $O$ if and only if $f$ is a prime number. We are interested in studying the $F$-primary ideals of $O$, hence, in what follows, $F$ will be a prime ideal in $O$; equivalently, $f$ will always denote an assigned prime number.

**Lemma 1.1.** In the above notation, take any $\alpha \in F \setminus fO$. Then $F = (f, \alpha)$.

**Proof.** It suffices to show that $f\omega \in (f, \alpha)$. Say $\alpha = fa + f\omega b$, where $a, b \in \mathbb{Z}$ and $f$ does not divide $b$, since $\alpha \notin fO$. Take $c, k \in \mathbb{Z}$ such that $cb = 1 + fk$. We get

$$c\alpha = f\omega + f(ca + f\omega k),$$

whence $f\omega \in (f, \alpha)$, as required. \qed

We give a definition which is crucial for our discussion.

**Definition 1.2.** We say that a $F$-primary ideal $Q$ is $F$-basic if $Q \not\subset F^2 = fF$.

By definition, $F$ is a $F$-basic ideal. Moreover, if $Q$ is a $F$-primary ideal containing $f$, then either $Q = fO$ or $Q = F$, since $|F/fO| = f$ is a prime number; in particular, these ideals are $F$-basic.

**Lemma 1.3.** Let $Q$ be a $F$-primary ideal.

(i) $Q$ is $F$-basic if and only if either $Q \not\subset fO$ or $Q \supseteq fO$. 

4
(ii) If $\mathfrak{F}^k$ is the highest power of $\mathfrak{F}$ containing $Q$, then $Q = f^{k-1}Q'$, where $Q'$ is a $\mathfrak{F}$-basic ideal.

(iii) If $Q/f^m$ is $\mathfrak{F}$-basic for some $m > 0$, then $m$ is unique and coincides with $k - 1$.

Proof. (i) If either $Q \not\subset fO$ or $Q \supset fO$, then $Q$ is not contained in $\mathfrak{F}^2$, since $\mathfrak{F}^2 = f\mathfrak{F} \subset fO$, so in this case $Q$ is $\mathfrak{F}$-basic. Conversely, assume that $Q$ is a $\mathfrak{F}$-basic ideal. If $Q \supset fO$ we are done, so suppose $f \not\in Q$. Let us show that $Q \not\subset fO$. Assume, for a contradiction, that $Q \subset fO$. It follows that $Q' = Q/f$ is a proper ideal of $O$. Then $Q'$ is a product of primary ideals of $O$, but, since $Q = fQ'$ is $\mathfrak{F}$-primary, $Q'$ is $\mathfrak{F}$-primary, as well. In particular, $Q' \subset \mathfrak{F}$, so $Q = fQ' \subset f\mathfrak{F} = \mathfrak{F}^2$, i.e., $Q$ is not $\mathfrak{F}$-basic, a contradiction.

(ii) Since $\mathfrak{F}^k = f^{k-1}\mathfrak{F} \supset Q$, we get $Q/f^{k-1} = Q' \subset \mathfrak{F}$. So, as well as $Q$, $Q'$ is $\mathfrak{F}$-primary. Moreover, $Q' \not\subset \mathfrak{F}^2$, otherwise $f^{k-1}\mathfrak{F}^2 = \mathfrak{F}^{k+1} \supset f^{k-1}Q' = Q$, against the maximality of $k$. We conclude that $Q'$ is $\mathfrak{F}$-basic.

(iii) From $Q/f^m \subset \mathfrak{F}$ we get $Q \subset f^m\mathfrak{F} = \mathfrak{F}^{m+1}$, whence $m + 1 \leq k$, by the definition of $k$. Moreover, from $Q/f^m \subset \mathfrak{F}^2 = f\mathfrak{F}$ we get $Q \subset f^{m+1}\mathfrak{F} = \mathfrak{F}^{m+2}$, hence $m + 2 > k$.

Let us note that a $\mathfrak{F}$-basic ideal is a primitive ideal of $O$, that is, an ideal that cannot be written as $mJ$, where $m \in \mathbb{N}$, $m \geq 2$ and $J \subset O$ is an ideal (the definition of primitive ideal is quite standard, see for example [2]).

Given a $\mathfrak{F}$-primary ideal $Q$, the $\mathfrak{F}$-basic ideal $Q'$ contained in $Q$, as defined in (ii) above, is called the basic component of $Q$. Roughly speaking, the basic component of a $\mathfrak{F}$-primary ideal $Q$ is obtained by extracting from $Q$ the highest power of $f$. It is uniquely determined by (ii) and (iii). It follows that the lattice $\mathcal{L}$ of all the $\mathfrak{F}$-primary ideals will be determined as soon as we know the lattice $\mathcal{L}_1$ of the $\mathfrak{F}$-basic ideals. In fact, $\mathcal{L}_1$ will be the first layer of $\mathcal{L}$, and the other layers of the lattice will be the $\mathcal{L}_n$ ($n > 0$), consisting of those $\mathfrak{F}$-primary ideals contained in $\mathfrak{F}^n$ but not in $\mathfrak{F}^{n+1}$. By Lemma 1.3, the elements of $\mathcal{L}_n$ are obtained by those of $\mathcal{L}_1$, just multiplying by $f^{n-1}$. Therefore, the $\mathcal{L}_n$ are reproductions of $\mathcal{L}_1$, and the whole lattice $\mathcal{L}$ is structured by layers.

The preceding remarks show that if suffices to focus our attention on $\mathcal{L}_1$. Hence, in what follows, we will investigate the $\mathfrak{F}$-basic ideals of $O$ and their mutual relations of containment.

The next notion is related to the basic ideals that are principal.

Definition 1.4. Let $t \in O$. We say that $t$ is $\mathfrak{F}$-primary if $tO$ is an $\mathfrak{F}$-primary ideal. We say that $t$ is $\mathfrak{F}$-basic (or simply basic) if $tO$ is a $\mathfrak{F}$-basic ideal.
Obviously, \( f \) is a basic element of \( O \). An element \( t \) in \( O \) which is \( \mathfrak{f} \)-primary lies in \( \mathfrak{f} = f\mathbb{Z} + f\omega\mathbb{Z} \) and therefore has the form \( t = fx + f\omega y \), for some \( x, y \in \mathbb{Z} \). The next proposition characterizes primary ideals and primary elements in terms of their norms. The proof is straightforward, using the properties of the norm.

**Proposition 1.5.** An ideal \( Q \) of \( O \) is \( \mathfrak{f} \)-primary if and only if its norm is a power of \( f \). In particular, if \( t = fx + f\omega y \in \mathfrak{f} \) is \( \mathfrak{f} \)-primary, then \( \text{g.c.d.}(x, y) = f^a \), for some \( a \geq 0 \). Moreover, \( t \) is \( \mathfrak{f} \)-basic if and only if \( x, y \) are coprime.

Given a \( \mathfrak{f} \)-primary element \( t \) as above, \( t \) is in \( fO \) if and only if \( f \) divides \( y \), since \( t = f(x + \omega y) \) and \( x + \omega y \in O \) if and only if \( f \mid y \). So, by Lemma 1.3, \( t \) is \( \mathfrak{f} \)-basic if \( y \not\in f\mathbb{Z} \) (note also that in this case \( x, y \) are coprime, since \( f \) is the only common prime factor of \( x \) and \( y \)). If \( t \) is a basic element and \( t \in fO \), then \( tO = fO \), that is, \( t \) and \( f \) are associated in \( O \).

However, it is possible that \( t \not\in fO \), but \( \mathfrak{f}^2 \subset tO \subset \mathfrak{f} \). We will see in the next section that this happens precisely when \( t \) and \( f \) are associated in \( D \) but not in \( O \) (Lemma 2.7).

**Proposition 1.6.** Let \( t \in O \) be \( \mathfrak{f} \)-basic. Then \( t \) is an irreducible element of \( O \) which is not prime.

**Proof.** Let us assume, for a contradiction, that \( t = rs \), where \( r, s \in O \), and neither \( r \) nor \( s \) is a unit in \( O \). Since the norm is a multiplicative function on \( O \), \( r, s \) are \( \mathfrak{f} \)-primary elements. In particular, \( r, s \in \mathfrak{f} \). But then \( t = rs \in \mathfrak{f}^2 \), contradiction.

Moreover, \( tO \) is not a prime ideal, since it is strictly contained in the conductor \( \mathfrak{f} \) (the only prime ideal containing \( t \)), which is not principal.

### 2 Intermediate \( \mathfrak{f} \)-primary ideals

Let \( Q \) be a \( \mathfrak{f} \)-primary ideal not contained in \( fO \); then, clearly, \( Q \) is \( \mathfrak{f} \)-basic. Using, for instance, the Claim in [8], page 358, it is readily seen that there exists \( r \in Q \) such that \( Q = (f^k, r) = f^k\mathbb{Z} \oplus r\mathbb{Z} \), where \( f^k \) is the minimum integer contained in \( Q \), and \( r = f\gamma \), for some \( \gamma \in D \). Moreover, \( \gamma \not\in O \), since, by assumption \( Q \not\subseteq fO \). The minimality of \( k \) implies that \( f^k \mid N(s) \), for every \( s \in Q \), since \( \text{g.c.d.}(f^k, N(s)) \) lies in \( Q \). We also have \( N(Q) = f^k \); in fact, \( \mathfrak{f} = (f, r) \), by Lemma 1.3, hence \( \mathfrak{f}/Q = f^{k-1} \), and therefore \( |O/\mathfrak{f}| = f \) yields \( |O/Q| = f^k \). Finally, \( Q/fQ \cong \mathbb{Z}/f\mathbb{Z} \oplus \mathbb{Z}/f\mathbb{Z} \) (as Abelian groups), since \( fQ = f^{k+1}\mathbb{Z} \oplus fr\mathbb{Z} \).

The following easy lemma will be useful to determine whether or not an ideal of \( O \) is a \( D \)-module.
Lemma 2.1. Let $I$ be an ideal of $O$. If $zI \subseteq I$ for some $z \in D \setminus O$, then $I = ID$.

Proof. To get $I = ID$, it suffices to show that $\omega I \subseteq I$. Say $z = a + \omega b$, where $b \notin f\mathbb{Z}$, since $z \notin O$. Let $\lambda b + \mu f = 1$, for suitable $\lambda, \mu \in \mathbb{Z}$. We get

$$\lambda z = \lambda a + \omega - \mu f \omega,$$

hence, for every $s \in I$, we get

$$\omega s = z \lambda s - \lambda as + \mu f \omega s \in I.$$

We conclude that $\omega I \subseteq I$. \hfill \Box

The next result characterizes the $\mathfrak{F}$-basic ideals of $O$ that are also $D$-modules. These kind of ideals will be crucial in the description of the lattice of $\mathfrak{F}$-basic ideals. The equivalence $(ii) \iff (iii)$ of Theorem 2.2 also follows from [1, p. 34]. We give a direct proof for the sake of completeness.

Theorem 2.2. Let $Q = (f^k, f\alpha)$ be a $\mathfrak{F}$-basic ideal different from $fO$, where $f^k$ is the minimal power of $f$ contained in $Q$. The following are equivalent

(i) $Q$ is a $D$-module.

(ii) $f^{k+1}$ divides $N(f\alpha)$.

(iii) $Q$ is not an invertible ideal.

Proof. (i) $\iff$ (ii). Say $\alpha = a + b\omega$, with $a, b \in \mathbb{Z}$; then $b \notin f\mathbb{Z}$, since $Q \notin fO$. Let us assume that $f^{k+1} | N(f\alpha)$. It is clear that $Q = QD$ if and only if $\omega Q \subseteq Q$. By Lemma 1.1 we have $(f, f\alpha) = \mathfrak{F}$, hence we get

$$\omega f^k = f^{k-1}(f\omega) \in f^{k-1}\mathfrak{F} = f^{k-1}(f, f\alpha) \subseteq Q,$$

without any assumption on $N(f\omega)$.

Let us verify that $\omega f\alpha \in Q$. We have

$$\omega f\alpha = xf^k + yf\alpha, \quad x, y \in O$$

if and only if $f\alpha(\omega - y) = xf^k$. Let $\alpha \bar{\alpha} = f^h m$, where $m \notin f\mathbb{Z}$, and observe that $h \geq k - 1$, since $f^{k+1} | N(f\alpha)$. Let $x = x_0 f\alpha \bar{\alpha}/f^k \in \mathbb{Z}$, for a suitable $x_0$ to be chosen below. Then the above equality is equivalent to

$$\omega - y = x_0 \bar{\alpha} = x_0 a + x_0 b \bar{\omega}.$$
or
\[ y = -x_0a - x_0b\bar{\omega} + \omega. \]
Since either \( \bar{\omega} = -\omega \), or \( \bar{\omega} = 1 - \omega \), if we choose \( x_0 \in \mathbb{Z} \) such that \( 1 + x_0b \in f\mathbb{Z} \) we get \( y \in O \), in both cases. So \( \omega f\alpha \in Q \), as required.

Conversely, assume that \( f^{k+1} \) does not divide \( N(f\alpha) \), hence \( N(f\alpha) = f^km \), where \( m \notin f\mathbb{Z} \). Assume for a contradiction that \( \omega f\alpha \in Q \). Then the preceding relation \( f\alpha(\omega - y) = xf^k (x, y \in O) \) is equivalent to \( mf\alpha(\omega - y) = xf\alpha f\bar{\alpha} \). We get \( m(\omega - y) = xf\bar{\alpha} \), whence \( m\omega \in O \), a contradiction.

(i), (ii) \(\Leftrightarrow\) (iii). If \( Q \) is an invertible ideal of \( O \), then \( QQ' = sO \), for some ideal \( Q' \) and \( 0 \neq s \in O \). Since \( sO \neq sD \) for every principal ideal \( sO \) of \( O \), it follows that \( QD \neq Q \).

Conversely, assume that \( N(f\alpha) = f^km \), where \( m \notin f\mathbb{Z} \). We get
\[
(f^k, f\alpha)[f^k, f\bar{\alpha}] = f^k(f^k, f\alpha, f\bar{\alpha}, m) = f^kO,
\]

hence \( Q \) is an invertible ideal of \( O \).

If \( I \) is an ideal of \( O \) and \( ID \) is the extended ideal in \( D \), \([ID : I]\) denotes the index of \( I \) in \( ID \) as Abelian groups. Note that \( I = JD \), for some ideal \( J \) of \( O \), if and only if \( I \) is also a \( D \)-module.

**Lemma 2.3.** Let \( I \subset O \) be an ideal. If \( I \subset ID \), then \([ID : I] = f\).

**Proof.** We firstly show that \( f\alpha \in I \) for every \( \alpha \in ID \). In fact, by definition of extended ideal, \( \alpha = \sum a_i\beta_i \), for suitable \( a_i \in I \) and \( \beta_i \in D \). Then \( f\alpha = \sum a_i f\beta_i \) is an element of \( I \), since each \( f\beta_i \) is in \( O \). In particular, we have \( fID \subset I \subset ID \), where the inclusions are strict, since \( I \) is not a \( D \)-module. Since \( f \) is a prime number and the index of \( fID \) in \( ID \) is \( f^2 \), it follows that the index of \( I \) in \( ID \) is \( f \).

Note that the above proof works for any order of index \( f \) in the ring of integers of any number field, not necessarily quadratic.

**Lemma 2.4.** Let \( I \subset Q \) be \( \mathfrak{p} \)-primary ideals, where \( Q \neq QD \). Then \( I \subset fQD \).

**Proof.** We have \([Q : I] = f^m \), for some \( m \geq 1 \). In particular, \( f^mQ \subset I \) and so \([I : f^mQ] = f^m \), since \([J : f^mJ] = f^{2m} \) for every nonzero ideal \( J \) of \( O \).

We firstly assume that \( I = ID \). Then \( f^mQD \subset I \) and \([f^mQD : f^mQ] = f \) (by Lemma 2.3) yield \([I : f^mQD] = [I : f^mQ]/[f^mQD : f^mQ] = f^{m-1} \). It follows that \( f^{m-1}I \subset f^mQD \), whence \( I \subset fQD \).
Now we assume that $I \subset ID$, so $f = [ID : I]$ by Lemma 2.3. If $ID \subset Q$, then by the first part of the proof it follows that $ID \subset fQD$, hence $I \subset fQD$, as well. If $ID \not\subset Q$, then $ID \cap Q \neq ID$. We get $[ID : f^mQ] = [ID : I][I : f^mQ] = f^{m+1}$, so $[ID : f^mQD] = [ID : f^mQ]/[f^mQ : f^mQD] = f^m$. It follows that $[ID \cap Q : f^mQD] = f^m$, where $m' < m$ since $ID \cap Q \subset ID$. Then we get $f^{m'}I \subset f^m(ID \cap Q) \subset f^mQD$, so $I \subset f^{m-m'}QD \subseteq fQD$, as required. \hfill \Box

Let $A = \{0, 1, \ldots, f - 1\}$. An easy computation shows that the $f + 1$ subgroups of $Z/fZ \oplus Z/fZ$ generated by the elements $(1, a) + fZ \oplus fZ$, $a \in A$, and $(0, 1) + fZ \oplus fZ$ are distinct and cover all the proper nonzero subgroups of $Z/fZ \oplus Z/fZ$.

**Theorem 2.5.** Let $Q = (f^k, f\alpha)$ be a $\mathcal{F}$-basic ideal different from $fO$, where $f^k$ is the minimal power of $f$ contained in $Q$.

(i) $\mathcal{F}^k$ is the minimum power of $\mathcal{F}$ contained in $Q$.

(ii) If $Q$ is a D-module, then there are exactly $f + 1$ ideals of $O$ lying properly between $Q$ and $fQ$, namely the pairwise distinct ideals

\[ J = (f^k, f^2\alpha); \quad J_a = (f^{k+1}, af^k + f\alpha), \quad a = 0, 1, \ldots, f - 1. \]

(iii) If $Q \neq QD$, then there is a unique ideal of $O$ lying properly between $Q$ and $fQ$, namely $J = (f^k, f^2\alpha) = fQD$.

**Proof.** (i) Recall that $\alpha \notin O$, since $Q \not\subseteq fO$, so that $\mathcal{F} = (f, f\alpha)$. Then $Q \supseteq (f^k, f^k\alpha) = f^{k-1}\mathcal{F} = \mathcal{F}^k$, where the equality holds only if $k = 1$. Of course, $k$ is minimum, since $f^{k-1} \in \mathcal{F}^{k-1} \setminus Q$.

(ii) Say $\alpha = a_1 + \omega a_2$, where $a_2 \notin fZ$, since $\alpha \notin O$. Since $Q/fQ \cong Z/fZ \oplus Z/fZ$ (as Abelian groups) and $Z/fZ \oplus Z/fZ$ has exactly $f + 1$ proper non-zero subgroups, it suffices to show that the ideals $J, J_a$ ($a = 0, \ldots, f - 1$) are pairwise distinct and lie properly between $Q$ and $fQ$.

It is clear that the ideals $J, J_a, 0 \leq a \leq f - 1$ lie between $Q$ and $fQ = (f^{k+1}, f^2\alpha)$. We firstly verify that these ideals are pairwise distinct.

Let us suppose that $J_a = J_b$. Then we get the equality

\[ f(af^{k-1} + \alpha) = (x_0 + x_1f\omega)f^{k+1} + (y_0 + y_1f\omega)(f(bf^{k-1} + \alpha)). \]

for suitable $x_0, x_1, y_0, y_1 \in Z$. It follows that

\[ af^{k-1} + \alpha - x_0f^k - y_0(bf^{k-1} + \alpha) \in \omega Q \subseteq Q, \]
where $\omega Q \subseteq Q$ since $Q$ is a $D$-module. The above relation yields $(1 - y_0)\alpha \in O$, so $1 - y_0 \in f\mathbb{Z}$, since $a_1 \notin f\mathbb{Z}$. Then we get $af^{k-1} - y_0bf^{k-1} \in Q$, hence $a - y_0b \in f\mathbb{Z}$, by the minimality of $k$. We conclude that

$$1 \equiv y_0, \ a \equiv y_0b \mod f,$$

so $a \equiv b$ modulo $f$, and therefore $a = b$, since these integers both lie in $\{0, 1, \ldots, f - 1\}$. We remark that we have actually proved that $J_a \not\subseteq J_b$ whenever $a \neq b$.

Since $J_a \not\subseteq fO$, for every $a \leq f - 1$, we get $J_a \neq J \subseteq fO$, and $J_a \supset fQ$. Moreover $Q \supset J$, since $Q \not\subseteq fO$, and $J \supset fQ$, since $f^{k-1} \notin Q$ yields $f^k \in J \setminus fQ$.

It remains to show that $J_a \neq Q$ for $a = 0, 1, \ldots, f - 1$. Assume, for a contradiction, that $J_a = Q$ for some $b \leq f - 1$. Then we get $J_a \subseteq Q = J_b$ for every $a \neq b$, which is impossible, as remarked above.

(iii) Under the present circumstances, we get $Q \supset fQD \supset fQ$, since $Q$ is not a $D$-module. Take any primary ideal, say $I$, properly lying between $Q$ and $fQ$. Then Lemma 2.4 shows that $I \subseteq fQD$, hence we actually get the equality $I = fQD$, since, in any case, $Q \supset J \supset fQ$.

The preceding theorem allows us to determine the ideals lying between $\mathfrak{F}$ and $\mathfrak{F}^2$. Indeed, the following corollary derives immediately from (ii) of Theorem 2.5, since $\mathfrak{F}$ is a $D$-module and $\mathfrak{F}^2 = f\mathfrak{F}$.

**Corollary 2.6.** There are exactly $f + 1$ ideals of $O$ that lie properly between $\mathfrak{F}$ and $\mathfrak{F}^2$, namely the pairwise distinct ideals $J = (f, f^2\omega) = fO$, $J_a = (f^2, f(a + \omega))$, $a = 0, 1, \ldots, f - 1$.

Next, we determine the intermediate ideals that are principal, or, equivalently, the basic elements $t \in O$ such that $\mathfrak{F}^2 \subseteq tO \subset \mathfrak{F}$.

**Lemma 2.7.** A principal ideal $tO$ lies properly between $\mathfrak{F}$ and $\mathfrak{F}^2$ if and only if $t = fw$, for a suitable unit $w$ of $D$. Moreover $fwO = fw'O$ if and only if $w/w' \in O$.

**Proof.** Assume that $\mathfrak{F} \supset tO \supset \mathfrak{F}^2$. The extended ideals satisfy $\mathfrak{F} \supset tD \supset \mathfrak{F}^2$, where the second containment is strict, since $tD \supset tO \supset \mathfrak{F}^2$. Since $|\mathfrak{F}/\mathfrak{F}^2| = f^2$, we get $tD = \mathfrak{F} = fD$, which is possible only if $t = fw$ for some unit $w$ of $D$. Conversely, for every unit $w$ of $D$, from $\mathfrak{F} \supset fO \supset \mathfrak{F}^2$ we get $w\mathfrak{F} = \mathfrak{F} \supset fwO \supset w\mathfrak{F}^2 = \mathfrak{F}^2$.

The last statement is immediate.
In particular, Lemma 2.7 implies that the number of principal $\mathfrak{F}$-primary ideals between $\mathfrak{F}$ and $\mathfrak{F}^2$ is equal to $|D^*/O^*|.

Since $\mathfrak{F} = fD$, it is well-known that there are three possibilities for the factorization into prime ideals of $\mathfrak{F}$ in $D$, namely:

i) $fD$ is a prime ideal of $D$ (inert case).

ii) $fD = \bar{P}P$, $P \subset D$ a prime ideal (split case) $fD = P^2$.

iii) $P \subset D$ a prime ideal (ramified case).

**Proposition 2.8.** Let $\tau = |D^*/O^*|$. According to the factorization of the conductor ideal $\mathfrak{F}$ in $D$, we have

i) $\tau | f + 1$ (inert case).

ii) $\tau | f - 1$ (split case)

iii) $\tau | f$ (ramified case).

**Proof.** As we have said at the beginning of Section 1, since $f$ is prime, $\mathfrak{F}$ is a prime ideal in $O$ and $O/\mathfrak{F} \cong \mathbb{F}_f$, the finite field with $f$ elements. In particular, the group of units of $O/\mathfrak{F}$ has cardinality $f - 1$. Since $\mathfrak{F}$ is also an ideal of $D$, we have three possibilities:

$$D/\mathfrak{F} \cong \begin{cases} 
\mathbb{F}_f^2, & \text{inert case} \\
\mathbb{F}_f \times \mathbb{F}_f, & \text{split case} \\
D/P^2, & \text{ramified case}
\end{cases}$$

In the ramified case, $D/P^2$ is a local ring with maximal ideal $P/P^2$. In each of the three cases, the group of units of $D/\mathfrak{F}$ has cardinality equal to $f^2 - 1$, $f^2 - f$ and $(f - 1)^2$, respectively.

The canonical ring homomorphism $\pi : D \to D/\mathfrak{F}$ induces a group homomorphism $\pi^* : D^* \to (D/\mathfrak{F})^*$ (which is not necessarily surjective). We have the following group homomorphism:

$$\frac{D^*}{O^*} \to \frac{(D/\mathfrak{F})^*}{(O/\mathfrak{F})^*}$$

$$u + O^* \mapsto \pi^*(u) + (O/\mathfrak{F})^*$$

We claim that the latter group homomorphism is injective. In fact, if $\pi^*(u) \in (O/\mathfrak{F})^*$, then $\pi(u) \in O/\mathfrak{F}$, so we get $u \in O^*$, since $\pi^{-1}(O/\mathfrak{F}) = O$. It follows that $\tau = |D^*/O^*|$ divides the cardinality of $(D/\mathfrak{F})^*/(O/\mathfrak{F})^*$, which in the three cases is equal to: i) $f + 1$ (inert), ii) $f - 1$ (split), iii) $f$ (ramified).
Remark 2.9. We note that the same conclusion of Proposition 2.8 can be obtained by means of a well-known formula that gives the class number of \( O \) in terms of the class number of \( D \) (see [3, p. 146-148]). By Corollary 2.6 there are \( f + 1 \) ideals properly between \( \mathfrak{F} \) and \( \mathfrak{F}^2 \). In each of the three cases mentioned above, the number of these intermediate ideals of \( O \) that are also \( D \)-modules is:

i) inert case: there is no intermediate \( D \)-module, since there are no \( D \)-modules between \( \mathfrak{F} = \mathfrak{P} \) and \( \mathfrak{F}^2 = \mathfrak{P}^2 \).

ii) split case: \( 2 \); the only \( D \)-modules between \( \mathfrak{F} = \mathfrak{P} \) and \( \mathfrak{F}^2 = \mathfrak{P}^2 \) are \( \mathfrak{P}^2 \) and \( \mathfrak{P} \).

iii) ramified case: \( 1 \); the only \( D \)-module between \( \mathfrak{F} = \mathfrak{P}^2 \) and \( \mathfrak{F}^2 = \mathfrak{P}^4 \) is \( \mathfrak{P}^3 \).

Hence, \( \tau = |D^*/O^*| \) divides the number of ideals properly between \( \mathfrak{F} \) and \( \mathfrak{F}^2 \) that are not \( D \)-modules (\( f + 1, f - 1 \) and \( f \), resp.), and this last number is equal to the cardinality of \( (D/\mathfrak{F})^*/(O/\mathfrak{F})^* \).

This last fact is an evidence of the following general result. We recall that an action of a group \( G \) on a set \( S \) is free if the stabilizer of each element \( s \in S \) is trivial, that is, \( \text{Stab}(s) = \{ g \in G \mid gs = s \} = \{1\} \).

**Proposition 2.10.** The multiplicative group \( (D/\mathfrak{F})^*/(O/\mathfrak{F})^* \) acts freely on the set of the ideals \( I \) of \( O \) that lie properly between \( \mathfrak{F} \) and \( \mathfrak{F}^2 \) and are not \( D \)-modules.

**Proof.** Let \( \mathcal{I} \) be the set of ideals of \( O \) lying properly between \( \mathfrak{F} \) and \( \mathfrak{F}^2 \). The set \( \mathcal{I} \) is in one-to-one correspondence with the set \( [\mathcal{I}] \) of proper non-zero ideals of \( O/\mathfrak{F}^2 \), by the canonical map \( I \mapsto I + \mathfrak{F}^2 = [I] \). Recall that \( \mathfrak{F}/\mathfrak{F}^2 \) is in a natural way a \( (D/F) \)-module, and so also a \( (O/F) \)-module.

For any assigned \( [z] \in (D/\mathfrak{F})^* \) and \( [I] \in [\mathcal{I}] \), we set \( [z] \cdot [I] = [zI] \). Since \( [I] \) is a \( O/\mathfrak{F} \)-module contained in \( \mathfrak{F}/\mathfrak{F}^2 \), it is straightforward to see that \( [zI] \) is also a \( O/\mathfrak{F} \)-module, contained in \( [z] \cdot \mathfrak{F}/\mathfrak{F}^2 = \mathfrak{F}/\mathfrak{F}^2 \), where the last equality holds since \( [z] \) is a unit in \( D/\mathfrak{F} \). We have thus defined an action of \( (D/\mathfrak{F})^* \) on \( [\mathcal{I}] \). In particular, every element \( [I] \) of \( [\mathcal{I}] \) is fixed by the elements of the subgroup \( (O/\mathfrak{F})^* \subset (D/\mathfrak{F})^* \), i.e., \( [z] \cdot [I] = [I] \), for every \( [z] \in (O/\mathfrak{F})^* \). Hence we have an induced natural action of the group \( G = (D/\mathfrak{F})^*/(O/\mathfrak{F})^* \) on \( [\mathcal{I}] \). We can partition \( \mathcal{I} \) into the union of the subset \( \mathcal{I}_D \) of the ideals that are also \( D \)-modules and the complementary subset \( \mathcal{I}_O \). The set \( \mathcal{I} \) is therefore partitioned by the natural map into the union of the set \( [\mathcal{I}]_{D/\mathfrak{F}} \) of \( O/\mathfrak{F} \)-modules which are also \( D/\mathfrak{F} \)-modules and the subset \( [\mathcal{I}]_{O/\mathfrak{F}} \) of \( O/\mathfrak{F} \)-modules.
which are not $D/\mathfrak{f}$-modules. By Lemma 2.11 for any assigned $I \in \mathcal{I}_O$ and $z \in D \setminus O$, we get $zI \not\subset I$. Hence, the sets $[\mathcal{I}]_{D/\mathfrak{f}}$ and $[\mathcal{I}]_{O/\mathfrak{f}}$ are characterized as follows:

$$[\mathcal{I}]_{D/\mathfrak{f}} = \{ \mathcal{I} \in [\mathcal{I}] \mid \forall g \in G, g \cdot [I] = [I] \}$$

$$[\mathcal{I}]_{O/\mathfrak{f}} = \{ \mathcal{I} \in [\mathcal{I}] \mid \forall g \in G, g \neq 1, g \cdot [I] \neq [I] \}.$$

Then $[\mathcal{I}]_{D/\mathfrak{f}}$ is precisely the subset of $[\mathcal{I}]$ of the fixed elements under the action of $G$ and $[\mathcal{I}]_{O/\mathfrak{f}}$ is the subset of elements whose stabilizer under the action of $G$ is trivial. We conclude that $G$ acts freely on the subset $[\mathcal{I}]_{O/\mathfrak{f}}$.

By the above proposition, the cardinality of $G$ divides the cardinality of $[\mathcal{I}]_{O/\mathfrak{f}}$. However, in the present case where the conductor is $fD$, $f \in \mathbb{Z}$ a prime number, we know by the above discussion that the two cardinalities coincide in all the three possible cases, inert, split and ramified.

In the final result of this section we characterize the intermediate ideals that are principal.

**Theorem 2.11.** Let $d$ be a square-free integer and let $O = \mathbb{Z}[f\omega]$ be an order in $D = \mathbb{Z}[\omega]$, the ring of integers of the number field $\mathbb{Q}[\sqrt{d}]$.

(i) Let $d < 0$. Then the only principal $\mathfrak{f}$-basic intermediate ideal is $fO$, except for $d = -1, \omega = i$ is a unit of $D$, hence, by Lemma 2.7, $fO = (f^2, f\omega)$ is a principal ideal different from $fO$. If $d = -3$, $f\omega = (1 + \sqrt{-3})/2$, $f\omega^2O, f\omegaO$, $f\omegaO = (1 + \sqrt{-3})/2$, we get $f\omegaO = (f^2, f\omega)$.

(ii) For $d > 0$, let $u \in D^*$ be the fundamental unit, and let $\tau = |D^*/O^*|$. Then the distinct principal $\mathfrak{f}$-basic intermediate ideals are exactly the $fu^jO$, $j = 0, \ldots, \tau - 1$. Let $u^j = x_j + \omega y_j \in D^* \setminus O^*$ ($x_j, y_j \in \mathbb{Z}$). Then $fu^jO = (f^2, f(a + \omega))$, where $a \equiv x_jy_j^{-1}$ modulo $f$.

**Proof.** (i) Take $d < 0$, different from $-1, -3$. Then the only units of $D$ are $\pm 1$, hence Lemma 2.7 shows that $fO$ is the unique $\mathfrak{f}$-basic intermediate principal ideal. If $d = -1$, then $\omega = i$ is a unit of $D$, hence, by Lemma 2.7, $fO = (f^2, f\omega)$ is a principal ideal different from $fO$. If $d = -3$, then $\omega = (1 + \sqrt{-3})/2$ is a unit of $D$, hence $f\omegaO$ and $f\omega^2O = f(\omega - 1)O$ are distinct principal $\mathfrak{f}$-basic intermediate ideals, different from $fO$. It is straightforward to verify that $f\omegaO = (f^2, f\omega)$ and $f\omega^2O = (f^2, f(1 + \omega))$.

(ii) Lemma 2.7 shows that every principal $\mathfrak{f}$-basic intermediate ideal has the form $fu^nO$, for some $n \geq 0$. Moreover, if $n = q\tau + j$, with $0 \leq j < \tau$, we clearly get
The principal ideals \( fu^jO \), \( j = 0, \ldots, \tau - 1 \), are \( \mathfrak{F} \)-basic intermediate, and are pairwise distinct, since \( u^i \not\in O \) whenever \( i \neq j \) and \( 0 \leq i, j < \tau \). Recall that \( y_j \not\in f\mathbb{Z} \), since \( u^j \not\in O \) for \( j = 1, \ldots, \tau - 1 \). By Corollary 2.6 \( fu^iO = (f^2, f(a + \omega)) \), for some \( 0 \leq a < f \), and this equality of ideals holds exactly if \( f(a + \omega) \in fu^jO \). Equivalently, we get the following equality in \( D \)

\[
 a + \omega = (x_j + \omega y_j)(b + f\omega c) \quad \exists \, b, c \in \mathbb{Z}
\]

Reducing modulo \( fD \), we get the congruences

\[
 a \equiv x_j b \mod f \quad 1 \equiv y_j b \mod f
\]

whence \( a \equiv x_j y_j^{-1} \), modulo \( f \).

An easy computation allows us to find the mutual conjugates of the \( \mathfrak{F} \)-basic intermediate ideals.

**Proposition 2.12.** In the above notation, the conjugate ideal of \( (f^2, f(a + \omega)) \), \( 0 \leq a < f - 1 \), is either \( (f^2, f(f-a+\omega)) \), when \( d \equiv 2, 3 \mod 4 \), or \( (f^2, f(f-a-1+\omega)) \), when \( d \equiv 1 \mod 4 \).

### 3 The lattice of basic ideals.

In the present section we analyze separately the lattice \( \mathcal{L}_1 \) of \( \mathfrak{F} \)-basic ideals, in each of the three cases that may appear, namely \( f \) inert, split or ramified in \( D \).

#### 3.1 Inert case.

The next theorem gives a complete description of the lattice of the \( \mathfrak{F} \)-basic ideals of \( O = \mathbb{Z}[f\omega] \), in the case when \( f \) is a prime element of \( D = \mathbb{Z}[\omega] \). Recall that infinitely many prime numbers remain prime elements in \( D \); actually the well-known Tchebotarev Density Theorem (see [3, §8]) says that the density of such primes is \( 1/2 \).

**Theorem 3.1.** Suppose \( \mathfrak{F} = fD \) is a prime ideal of \( D \). Then every basic \( \mathfrak{F} \)-primary ideal of \( O \) contains \( \mathfrak{F}^2 \), and lies in the following set of pairwise distinct ideals

\[
 \mathcal{J} = \{(f, f^2\omega), (f^2, f(a + \omega)) : 0 \leq a < f \}.
\]
Proof. Let $Q$ be a basic ideal. The extended ideal $QD$ is equal to $\mathfrak{f}$, since $Q$ is $\mathfrak{f}$-primary ($\mathfrak{f}$ is the only prime ideal of $O$ that contains $Q$, hence the only prime ideal of $D$ that contains $Q$) and $Q$ is not contained in $\mathfrak{f}^2$ by definition. It follows by Lemma 2.3 that $fQD = f\mathfrak{f} = \mathfrak{f}^2 \subset Q$.

Finally, $Q$ lies in the set $\mathcal{J}$ by Corollary 2.6.

The principal basic $\mathfrak{f}$-primary ideals are described in Theorem 2.11. Their number is exactly equal to the number of distinct non-associated basic elements of $O$, which is equal to $|D^*/O^*|$, see Lemma 2.7. Moreover, their norm is equal to $f^2$, since the ideal they generate lies in between $\mathfrak{f}$ and $\mathfrak{f}^2$.

The following diagram represents the lattice of $\mathfrak{f}$-primary ideals in the inert case. Note that, in the diagram, only the powers of $\mathfrak{f}$ are $D$-modules. For this reason, by Theorem 2.2, all the proper intermediate ideals are invertible.

![Diagram of $\mathfrak{f}$-primary ideals]

3.2 Split case.

Throughout this section, we assume that $\mathfrak{f} = fD$ splits as an ideal of $D$, say $fD = PP$, where $P \neq \bar{P}$ are prime ideals of $D$ of norm $f$, both of which lie above $\mathfrak{f}$, considered as an ideal of $O$. Note that $P$ is principal if and only if $f$ is not irreducible in $D$ (recall that $f$ is always irreducible in $O$, by Proposition 1.6). However, some power of $P$ is a principal ideal of $D$, since the class group of $D$ is finite. For the remainder of this section, we will denote by $m$ the order of $P$ in the class group of $D$ (i.e., the minimum power $m$ of $P$ such that $P^m$ is principal), and by $\beta$ a fixed generator of $P^m$. 
Similarly to the inert case, there exist infinitely many prime numbers that split in $D$.

**Lemma 3.2.** In the above notation, $\beta^n \notin O$ for every $n > 0$.

*Proof.* Assume, for a contradiction, that $\beta^n \in O$. Then $\beta^n \in O \cap P = \mathfrak{F}$. It follows that $\beta^n D = P^{mn} \subseteq \mathfrak{F} = P \bar{P} \subset \bar{P}$, whence $P \subseteq \bar{P}$, impossible. \hfill \Box

The next proposition gives a way to construct $\mathfrak{F}$-basic principal ideals, not containing $\mathfrak{F}^2$.

**Proposition 3.3.** The elements $t_n = f \beta^n$, for $n \in \mathbb{N}$, are $\mathfrak{F}$-basic, and the principal ideals $t_n O$, for $n > 0$, are pairwise incomparable and do not contain $\mathfrak{F}^2$.

*Proof.* Recall that $N(\beta) = f^m$. Then $N(t_n) = f^2 N(\beta^n) = f^{mn+2}$, so the principal ideal $t_n O$ is $\mathfrak{F}$-primary, for every $n > 0$, in view of Proposition 1.5. Now note that $t_n \notin \mathfrak{F}^2 = f \mathfrak{F}$, for every $n \geq 0$, since $t_n/f = \beta^n \notin \mathfrak{F} \subset O$. We conclude that $t_n$ is $\mathfrak{F}$-basic for every $n \geq 0$. Pick now two distinct non-negative integers $n, m$, with $n = m + h, h > 0$. Then $t_n O$ and $t_m O$ are not comparable, since $t_n/t_m = \beta^h \notin O$ and $t_m/t_n = \beta^{-h} \notin O$. It follows that the ideals $t_n O (n \geq 0)$ are pairwise incomparable. Finally, since $t_n$ has norm strictly greater than $f^2$, for $n > 0$, $\mathfrak{F}^2$ is not contained in $t_n O$. \hfill \Box

In the notation of Proposition 3.3, we define $t_0 = f = f \beta^0$. Differently from the $t_n$ with $n > 0$, $t_0 O \supset \mathfrak{F}^2$. The Proposition also shows that in the split case, unlike the inert case, there are basic elements of arbitrary large norm, so, they are infinitely many.

The following theorem describes all the $\mathfrak{F}$-basic elements of $O$ which are associated to the elements $t_n = f \beta^n$, as introduced in Proposition 3.3. Note that the only elements of norm $f^2$ are $f w = t_0 w$, where $w$ is a unit of $D$ (see Lemma 2.7).

**Theorem 3.4.** Let $t$ be a basic element of $O$ of norm $f^{s+2}$, $s \geq 0$. Then $s = mn$, for some $n \in \mathbb{N}$, and $t \in \{ t_n w, t_n w : w \in D^* \}$. Moreover, $t_h w O \neq t_k w' O$ for any positive integers $h, k$ and $w, w' \in D^*$, and $t_h w O = t_k w' O$ if and only if $h = k$ and $w/w' \in O$.

*Proof.* Since $t$ is $\mathfrak{F}$-basic, $P, \bar{P}$ are the only prime ideals of $D$ above $tD$. Then we get

$$tD = P^k \bar{P}^h, \quad h, k > 0.$$ 

Moreover, since $t \notin \mathfrak{F}^2 = P^2 \bar{P}^2$, the integers $h, k$ are not both $> 1$. Let us assume that $h = 1$, whence $tD = f P^{k-1}$. Then $P^{k-1}$ is principal, hence $k - 1 = mn$, for
some positive integer \( n \). It follows that \( N(t) = f^{s+2} = f^2N(P^{mn}) = f^{mn+2} \), hence we get the desired equality \( s = mn \).

Now, we have \( tD = fP^{mn} = f\beta^nD = t_nD \), which is possible only if \( t = t_nw \), for some \( w \in D^* \).

In the case \( k = 1 \) we will symmetrically get \( t = \bar{t}_nw \) for some \( w \in D^* \).

Finally, if \( t_hwO = \bar{t}_kw'O \), then \( h = k \) otherwise \( t_h, t_k \) have different norms and we get that some power of \( \beta \) is in \( O \), which is impossible by Lemma 3.2. Moreover, \( t_hwO = t_kw'O \) implies \( h = k \) as before, hence we also get \( w/w' \in O \). \( \square \)

Our next step is to classify the non-principal basic \( \mathfrak{F} \)-primary ideals.

We recall that a Special PIR (Special Principal Ideal Ring) \( R \) is a principal ideal ring with a unique prime ideal \( M \), such that \( M \) is nilpotent (see [9, p. 245]). So, in the case when \( M = pR \), for some \( p \in R \), we get \( p^n = 0 \) for some \( n > 1 \).

**Lemma 3.5.** The quotient ring \( O/t_nO \) is a Special PIR for every \( n \geq 0 \). In particular, \( O/t_nO \) is a chained ring.

**Proof.** The claim is immediate when \( t_n = t_0 = f \), since \( \mathfrak{F}/fO \) is the unique nonzero proper ideal of \( O/fO \), it is generated by \( f\omega + fO \), and \((\mathfrak{F}/fO)^2 = 0\), since \( \mathfrak{F}^2 \subset fO \). Thus we may assume that \( n \geq 1 \).

Note that, if \( I \) is an ideal of \( O \) containing \( t_n \), then \( I \) is basic \( \mathfrak{F} \)-primary, since any prime ideal containing \( I \) must contain the \( \mathfrak{F} \)-basic element \( t_n \). The ideal \( I \) is basic since \( t_n \notin \mathfrak{F}^2 \). In particular, \( O/t_nO \) has a unique maximal ideal, equal to \( \mathfrak{F}/t_nO \). Since \( \mathfrak{F} = (f, t_n) \) by Lemma 1.1, it follows that \( \mathfrak{F}/t_nO \) is a principal ideal of \( O/t_nO \), generated by \( f + t_nO \). From this fact, it is not difficult to see that every nonzero ideal of \( O/t_nO \) is principal, generated by some \( f^i + t_nO \), for some \( 1 \leq i \leq mn + 1 \) (see [4, Proposition 4], for example). Indeed, \( f^k \in t_nO \) if and only if \( h \geq mn + 2 \), since \( N(t_n) = f^{mn+2} \). \( \square \)

The next corollary follows at once from the previous lemma and gives all the basic \( \mathfrak{F} \)-primary ideals that contain some \( \mathfrak{F} \)-basic element.

**Corollary 3.6.** The ideals (necessarily \( \mathfrak{F} \)-primary) that contain \( t_nO \) are the \((f^i, t_n)\), for \( i = 1, \ldots, mn + 2 \). Moreover, the norm of \((f^i, t_n)\) is \( f^i \).

**Proof.** The first claim follows from Lemma 3.5. The second claim follows from Theorem 2.2, since \( f^i \) is the least power of \( f \) contained in \((f^i, t_n)\). \( \square \)

**Proposition 3.7.** Let \( i \in \mathbb{N} \) and \( t \in O \) be a basic \( \mathfrak{F} \)-primary element of norm \( f^m \), \( m > i \). The ideal \( I = (f^i, t) \) of \( O \) is a \( D \)-module, equal either to \( I = P^i \bar{P} \) or \( I = P \bar{P}^i \). In particular, we get \((f^i, t_n) = (f^i, t_n)\), for every \( n \geq i \).
Proof. Since \( f^{i+1} \mid N(t) \), we get \( I = ID \), by Theorem 2.2. Without loss of generality, we suppose that \( tD = P^{m-1} \). Since \( D \) is a Dedekind domain, \( f^iD + tD \) is the greatest common divisor of \( f^iD \) and \( tD \), so it is equal to \( P^i \), since \( f^iD = (PP)^i \). Hence, \( I = ID = P^i \). The last claim follows immediately, since \( f^i \) divides \( N(t_n) = nm + 2 \) for every \( n \geq i \).

For every \( k \geq 1 \), we define \( Q_k = (f^k, t_k) = P^k \). in this notation, \( Q_1 = \mathfrak{F} \).

**Lemma 3.8.** Let \( Q \) be a \( \mathfrak{F} \)-basic ideal. Then there exists \( k \geq 1 \) such that \( fQ_k \subset Q \subset Q_k \).

**Proof.** Since \( Q \) is basic, exactly by the same proof of Theorem 3.4 given in the case of principal basic ideals, we have \( QD = P^k \) for some \( k \geq 1 \) (or its conjugate), so \( Q \subset Q_k \). By Lemma 2.3, either \( Q = Q_k \) or \( [Q_k : Q] = f \). In both cases, we get \( fQ_k \subset Q \subset Q_k \) and \( Q = Q_k \).

The next theorem gives a description of the ideals of \( O \) that contain a basic element.

**Theorem 3.9.** (i) The ideals \( Q_k = (f^k, t_k) \) are pairwise distinct, as \( k \) ranges in \( \mathbb{N} \);

(ii) an ideal \( Q \) of \( O \) contains \( Q_k \) if and only if \( Q \in \{ Q_i : i = 0, \ldots, k \} \);

(iii) if \( Q \) contains a basic element and it is not principal, then either \( Q = Q_k \) or \( Q = Q_k \) for some \( k \in \mathbb{N} \).

**Proof.** (i) By Proposition 3.7, we get \( Q_k = P^k \) (not the conjugate, since \( \beta^k \in P \)). Hence the \( Q_k \) are pairwise distinct, as \( k \) ranges.

(ii) For \( 0 \leq i \leq k \), by Proposition 3.7 we get

\[
Q_i = (f^i, t_i) = (f^i, t_k) \supseteq (f^k, t_k) = Q_k.
\]

Conversely, if \( I \supseteq Q_k \), then \( I \) contains \( t_k \), hence, by Corollary 3.6 we get \( I = (f^j, t_k) \), for some \( j \in \{1, \ldots, k + 1 \} \), so \( I = (f^j, t_k) = (f^j, t_j) = Q_j \).

(iii) This follows from (ii) and its proof, possibly replacing the \( Q_i \) with their conjugates.

In order to complete the description of the lattice of \( \mathfrak{F} \)-basic ideals, it remains to find the basic ideals of \( O \) that do not contain a \( \mathfrak{F} \)-basic element.

**Theorem 3.10.** Let \( Q \) be a basic \( \mathfrak{F} \)-primary ideal not containing any basic element. Then
(i) $Q$ lies properly between $Q_k$ and $fQ_k$, for some $k > 0$;

(ii) $Q = (f^{k+1}, af^k + t_k)$ for some $1 \leq a \leq f - 1$;

(iii) $Q$ does not contain any other basic $\mathfrak{F}$-primary ideal;

(iv) $Q$ is an invertible ideal of $O$.

Proof. (i) The ideal $Q$, being $\mathfrak{F}$-basic, must lie between some $Q_k$ and $fQ_k$ by Lemma 3.8, and it is different from $Q_k$, since it does not contain basic elements.

(ii) This follows from Theorem 2.2, since, necessarily, $Q$ is different from $(f^k, ft_k) = fQ_{k-1}$, which is not a $\mathfrak{F}$-basic primary ideal, and from $(f^{k+1}, t_k)$, which contains the $\mathfrak{F}$-basic element $t_k$.

(iii) Say $Q'$ is a basic ideal contained in $Q = (f^{k+1}, af^k + t_k)$. Then $Q'$ cannot contain a $\mathfrak{F}$-basic element, hence, by (ii) we get $Q' = (f^{h+1}, bf^h + t_h)$, for some $h > 0$, $b \in \{1, \ldots, f-1\}$. Let us assume, for a contradiction, that $Q \neq Q'$, so $Q \supset Q'$. It follows that $h > k$. Then we readily see that $Q' \subset Q$ if and only if $t_h \in Q$, impossible, since $t_h$ is $\mathfrak{F}$-basic.

(iv) Let $f\gamma = af^k + t_k = f(af^{k-1} + \beta^k)$. By Theorem 2.2, it suffices to show that $f^{k+2}$ does not divide $N(f\gamma)$. We get

$$N(\gamma) = a^2 f^{2k-2} + af^{k-1}(\beta^k + \bar{\beta}^k) + f^{mk}.$$ 

Since $f$ does not divide the trace of $\beta^k$ (otherwise $\beta^k \in fD = \mathfrak{F}$, impossible), we readily see that $N(\gamma) = f^{k-1}b$, where $b \notin f\mathbb{Z}$. It follows that $N(f\gamma) \notin f^{k+2}\mathbb{Z}$.

Note that, by Theorem 2.2, an ideal $Q$ satisfying the hypothesis of the previous Theorem, is not a $D$-module. The converse of Theorem 2.2 iv) is false: consider any principal $\mathfrak{F}$-primary ideal generated by a basic element. Therefore, the basic ideals that are invertible are either principal, necessarily generated by a $\mathfrak{F}$-basic element, or they do not contain any $\mathfrak{F}$-basic element.

Remark 3.11. Let $k \in \mathbb{N}$. By Theorem 3.4, there exist principal intermediate ideals between $Q_k$ and $fQ_k$ if and only if $Q_k$ is principal as an ideal of $D$, generated by a $\mathfrak{F}$-basic element of $O$. In fact, if $fQ_k \subset tO \subset Q_k$ then we have $tD = Q_k$. Conversely, if $Q_k \subseteq \mathfrak{F} = fD$ is principal, then $Q_k$ is generated by an element of the form $f\beta$, for some $\beta \in D \setminus O$. Hence, $f\beta O$ is an intermediate ideal between $fQ_k$ and $Q_k$. Moreover, as we saw in the proof of Theorem 3.4, the last condition holds if and only if $m$ divides $k - 1$. For such $k$’s, there are $\tau$ intermediate principal ideals between $Q_k$ and $fQ_k$ (essentially by the same phenomenon of Lemma 2.7).
In the case where \( k = ms + 1, \ s \in \mathbb{N}, \) we know by Proposition 3.7 that \( Q_k = (f^k, t_s), \) and \( Q_k \supset t_sO \supset fQ_k. \) We identify which of the ideals \( J_a \) (see Theorem 2.5 and Theorem 3.10) coincides with \( t_sO. \) By Proposition 3.7, \( \beta^n = b_n + c_n\omega, \) where \( c_n \notin f\mathbb{Z}, \) since \( \beta^n \notin O \) for every \( n > 0 \) (Lemma 3.2). We show that

\[ t_sO = (f^{k+1}, f^ka + t_k), \quad \text{where} \quad ac_s \equiv c_{k-s} \mod f. \]

Since the intermediate ideals between \( Q_k \) and \( fQ_k \) are pairwise incomparable (Theorem 2.5), it suffices to show that \( t_sO \supseteq (f^{k+1}, f^ka + t_k). \) Since \( N(\beta^s) = f^{ms} = f^{k-1} \) we immediately get \( f^{k+1} \in f\beta^sO, \) as well as the equality

\[ f^ka + f\beta^k = f\beta^s(\beta^{k-s} + a\overline{\beta}^s). \]

Hence it suffices to show that \( z = \beta^{k-s} + a\overline{\beta}^s = b_{k-s} + c_{k-s}\omega + a(b_s + c_s\overline{\omega}) \in O. \) Since either \( \overline{\omega} = -\omega, \) or \( \overline{\omega} = 1 - \omega, \) in both cases \( z \) lies in \( O \) if and only if \( c_{k-s} - ac_s \in f\mathbb{Z}. \) The desired conclusion follows.

The diagram below represents the lattice of \( \mathfrak{F} \)-primary ideals in the split case.
3.3 Ramified case.

Here we assume that \( f \) is ramified. Recall that this condition holds if and only if either \( f \mid d \), when \( d \equiv 1 \) modulo 4, or \( f \mid 4d \), when \( d \equiv 2, 3 \) modulo 4.

**Theorem 3.12.** Suppose \( \mathfrak{F} = P^2 \), for some prime ideal \( P \) of \( D \).

(i) If \( d \equiv 1, 2 \) modulo 4, then \( P = fD + \sqrt{d}D \). If \( d \equiv 3 \) modulo 4, and \( f \neq 2 \), then \( P = fD + \sqrt{d}D \). Finally, if \( f = 2 \) and \( d \equiv 3 \) modulo 4, then \( P = 2D + (1 + \sqrt{d})D \).

(ii) Let \( Q \subseteq \mathfrak{F} \) be a basic \( \mathfrak{F} \)-primary ideal. Then either

\[
P^4 = \mathfrak{F}^2 \subset Q \subseteq \mathfrak{F} = P^2
\]

or

\[
P^5 \subset Q \subseteq P^3.
\]

(iii) If \( \mathfrak{F} \supset Q \supset \mathfrak{F}^2 \), then either \( Q = J_a = (f^2, f(a + \sqrt{d})) \), for some \( a = 0, 1, \ldots, f - 1 \), or \( Q = J = (f, f^2\sqrt{d}) = fO \).

(iv) if \( P^3 \supset Q \supset P^5 = fP^3 \), then \( Q = H_a = (f^3, af^2 + f\sqrt{d}) \), for some \( a = 0, 1, \ldots, f - 1 \), or \( Q = (f^2, f^2\sqrt{d}) = f\mathfrak{F} = P^4 \), except when \( f = 2 \) and \( d \equiv 3 \) modulo 4; in this latter case, we either get \( Q = (8, 2(1 + \sqrt{d})) \) or \( Q = (8, 4 + 2(1 + \sqrt{d})) = P^4 \).

**Proof.** (i) In any case, we have \( \mathfrak{F} = (f, f\sqrt{d}) \). Assume that \( f \mid d \); we get \( fd = f\lambda \), with \( \lambda \notin f\mathbb{Z} \), since \( d \) is square-free. Then the ideal of \( D \) \( (f, \sqrt{d}) \) satisfies \( (f, \sqrt{d})^2 = (f^2, d)D = fD + \sqrt{d}D \), hence it coincides with \( P \). This argument covers all the possible cases, except when \( f = 2 \) and \( d \equiv 3 \) modulo 4. Under this latter circumstance, we take the ideal \( (2, 1 + \sqrt{d}) \), whose square is \( (4, 1 + d + 2\sqrt{d}) = (4, 2\sqrt{d}) = 2D = \mathfrak{F} \), where the preceding equalities hold since \( d + 1 \in 4\mathbb{Z} \), and \( d \in (2, \sqrt{d}) \) is odd. It follows that \( P = (2, 1 + \sqrt{d}) \) as required.

(ii) Since \( D \) is a Dedekind domain and \( Q \) is a basic \( \mathfrak{F} \)-primary ideal, \( QD \) is equal either to \( P^2 \) or to \( P^3 \). In both cases, by Lemma 2.3, \( fQD \subset Q \subseteq QD \), which is the statement.

(iii) and (iv) follow from Corollary 2.6 and Theorem 2.5, since, by (i), either \( P^3 = P\mathfrak{F} = PfD = fP = (f^2, f\sqrt{d}) \) or \( P^3 = 2P = (4, 2(1 + \sqrt{d})) \), in the exceptional case. In this latter case, we immediately get the equality \( (4, 4(1 + \sqrt{d})) = 2\mathfrak{F} = \mathfrak{F}^2 = P^4 \). \( \square \)
Besides the basic elements \( t \in \mathfrak{f} \) such that \( \mathfrak{f}^2 \subset tO \subset \mathfrak{f} \), which are associated to \( f \) by a unit of \( D \) (see Lemma 2.7), in the ramified case we may have other basic elements such that \( P^5 \subset tO \subset P^3 \), according to whether \( P \) is a principal ideal of \( D \) or not, as the next result shows.

**Proposition 3.13.** There exists a basic element \( t \in O \) such that \( P^5 \subset tO \subset P^3 \) if and only if \( P \) is a principal ideal of \( D \). If this condition holds, say \( P = \beta D \), for some \( \beta \in D \), then every basic element is associated to \( f\beta \) by a unit of \( D \).

**Proof.** Let us assume that \( P = \beta D \), for some \( \beta \in D \). Under the present circumstances we get \( N(\beta) = f \) and \( f = u\beta^2 \), for some unit \( u \in D \). Clearly, \( \beta \notin O \), otherwise \( \beta \in P \cap O = \mathfrak{f} = P^2 \), which is impossible. Hence, \( t = f\beta \) is a basic element, according to Lemma 1.3 and Proposition 1.5, since its norm is \( f^3 \) and \( t \notin fO \). Since \( tD = \beta^3D = P^3 \), we get \( \beta^5D = P^5 \subset tO \subset P^3 \).

Conversely, let \( t \in O \) be a basic element such that \( P^5 \subset tO \subset P^3 \). Using Lemma 2.3 we get \( tD = P^3 = fP \), so \( P = \frac{1}{f}D \) is a principal ideal of \( D \).

The last claim follows arguing as in Lemma 2.7.

Summarizing, the set of basic elements in the ramified case is:

i) \( \{fu : u \in D^*\} \), if \( P \) is not a principal ideal of \( D \). These elements have norm \( f^2 \) and their number is \( \tau = |D^*/O^*| \) (Lemma 2.7).

ii) \( \{fu, f\beta v : u, v \in D^*\} \), if \( P \) is a principal ideal of \( D \) generated by an element \( \beta \). We have \( N(fu) = f^2 \), \( N(f\beta v) = f^3 \), and the total number of these elements is \( 2\tau \) (Lemma 2.7 and Corollary 3.13).

The diagram below represents the lattice of \( \mathfrak{f} \)-primary ideals in the ramified case. By Theorem 2.2 and the above description of the basic ideals, all the basic ideals, with the exception of \( \mathfrak{f} \) and \( P^3 \), are invertible.
References

[1] H. S. Butts, G. Pall, Modules and binary quadratic forms. Acta Arith. 15 (1968) 23–44.

[2] H. S. Butts, G. Pall, Ideals not prime to the conductor in quadratic orders. Acta Arith. 21 (1972), 261–270.

[3] D. A. Cox, Primes of the form $x^2 + ny^2$, Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[4] T. W. Hungerford, On the structure of Principal Ideal Rings, Pacific J. Math., 25 (1968) 543–547.

[5] G. Peruginelli, L. Salce, P. Zanardo, Idempotent pairs and PRINC domains, submitted.

[6] M. Post, H. Zassenhaus, Algorithmic Algebraic Number Theory. Encyclopedia of Mathematics and its Applications, 30. Cambridge University Press, Cambridge, 1989.

[7] L. Salce, On the minimal injective cogenerator over almost perfect domains. Houston J. Math. 31 (2005), no. 3, 693-705.
[8] P. Zanardo, U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Camb. Phil. Soc. 115 (1994) 379-391.

[9] O. Zariski, P. Samuel, *Commutative Algebra, vol. I*, Springer-Verlag, New York-Heidelberg-Berlin, 1975.