International Journal of Number Theory
Vol. 12, No. 7 (2016) 2025–2040
© The Author(s)
DOI: 10.1142/S1793042117500737

World Scientific
www.worldscientific.com

The lattice of primary ideals of orders in quadratic number fields

Giulio Peruginelli
Via Pietro Coccoluto Ferrigni 68
57125 Livorno, Italy
g.peruginelli@tiscali.it

Paolo Zanardo
Department of Mathematics, University of Padova
Via Trieste 63, 35121 Padova, Italy
pzanardo@math.unipd.it

Received 13 November 2015
Accepted 29 June 2016
Published 19 August 2016

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, where $f \in \mathbb{Z}$ is a prime. 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.

Mathematics Subject Classification 2010: 11R11, 11R04

1. Introduction

A Dedekind domain is defined as an integral domain in which every ideal can be factored into a product of prime ideals [8, §6, Chap. IV, p. 270]; moreover, this factorization is necessarily unique [8, Corollary, p. 273]. 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 $K = \mathbb{Q}[\sqrt{d}]$, d a square-free integer. We say that an order is proper if it is not integrally closed, that is, $O \subsetneq D$ (recall that D is a Dedekind domain). Since a Dedekind domain is necessarily integrally closed, if O is a proper order then there exist ideals of O which cannot be factored into a product of 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 ([8, Theorem 9, §5, Chap. IV, 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, called *regular*, has a unique factorization into prime ideals of O [3]. In particular, each regular primary ideal is equal to a power of its radical. Actually, this condition characterizes the regular primary ideals (see [6, Lemma 2.3]). More interesting is the situation for primary ideals that are non-regular. In this paper, we focus on the most natural case when the conductor $\mathfrak{F}$ is a prime ideal of O, so that $\mathfrak{F} = fD$, for some prime number $f \in \mathbb{Z}$. In this case, it makes sense to talk about $\mathfrak{F}$-primary ideals (i.e. primary ideals whose radical is equal to $\mathfrak{F}$). In particular, we will relate the structure of the lattice of $\mathfrak{F}$-primary ideals to the splitting type of f in D. We reserve further investigations for the general case to a future work.

Our purpose is to give a detailed description of the structure of the lattice of $\mathfrak{F}$-primary ideals of a quadratic order O. 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 nth layers of the ideals contained in $\mathfrak{F}^n$ and not contained in $\mathfrak{F}^{n+1}$, for each $n > 1$, and all these layers reproduce the same pattern of the first layer.

In Secs. 2 and 3, we characterize the $\mathfrak{F}$-basic ideals. We firstly characterize the $\mathfrak{F}$-basic ideals which are also D-modules (that is, ideals of 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 D-module Q and fQ. 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 $\mathfrak{F}^2$.

In Sec. 4, we examine separately the three cases mentioned above, namely, f inert, split or ramified in D, that gives rise to different structures of the corresponding lattices of $\mathfrak{F}$-primary ideals.

In the general case of a proper quadratic order O whose conductor $\mathfrak{F}$ is not necessarily a prime ideal, we know that $\mathfrak{F}$ can be written uniquely as a product of primary ideals $\mathfrak{G}_1, \ldots, \mathfrak{G}_s$ whose radicals are distinct maximal ideals $\mathfrak{F}_1, \ldots, \mathfrak{F}_s$ of O. In Remark 4.11 at the end of the paper we make some initial comments on this case that we intend to thoroughly investigate in a coming paper.

2. General Definitions and Results

In what follows, we will freely use the standard results on rings of integers in quadratic number fields. For example, see [5; 8, Chap. V]. As usual, for elements

$z \in D$ and ideals I, the symbols $\bar{z}$, $\bar{I}$ and $N(z)$, $N(I)$ denote the conjugates and the norms, respectively; D^*, 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 "$\subset$" will denote proper containment and as usual "$I \not\subset J$" will denote that I is not contained in J.

We fix some notation. Let d be a square-free integer. The ring of integers of $K = \mathbb{Q}(\sqrt{d})$ 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 now f be a positive integer and $O = \mathbb{Z}[f\omega]$ be the unique quadratic order in K such that $[D : O] = f$. For $\alpha, \beta \in O$, we set $(\alpha, \beta) = \alpha O + \beta O$; in general, (α, β) strictly contains the $\mathbb{Z}$-module $\alpha\mathbb{Z} + \beta\mathbb{Z}$. By definition, the conductor of O in D is the ideal

$$\mathfrak{F} = \{x \in O : xD \subseteq O\} = fD = f\mathbb{Z} + f\omega\mathbb{Z} = fO + f\omega O.$$

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

$$N(\mathfrak{F}^k) = |O/\mathfrak{F}^k| = |\mathbb{Z}/f^k\mathbb{Z} \oplus f\omega\mathbb{Z}/f^k\omega\mathbb{Z}| = f^{2k-1}.$$

Since $O/\mathfrak{F} \cong \mathbb{Z}/f\mathbb{Z}$, we immediately see that $\mathfrak{F}$ is a prime ideal of O if and only if f is a prime number. As we have already said in Sec. 1, throughout the paper we will assume that $\mathfrak{F}$ is a prime ideal; equivalently, f will always denote an assigned prime number. In particular, under the present circumstances, in order to study non-regular ideals, it will make sense to talk about $\mathfrak{F}$-primary ideals. Note that there is no ideal of O lying properly between fO and $\mathfrak{F}$, since $[\mathfrak{F} : fO] = f$.

It is well known that every primitive ideal Q of O (i.e. $Q \not\subset nO$, for each $n \geq 2$) can be written as

$$Q = q\mathbb{Z} + (a + f\omega)\mathbb{Z} = (q, a + f\omega),$$

where $q, a \in \mathbb{Z}$, such that $q\mathbb{Z} = Q \cap \mathbb{Z}$ and q divides $N(a+f\omega)$ (see for example [2, 7]). The ideal Q is O-invertible if and only if $(Q : Q) = \{x \in \mathbb{Q}(\sqrt{d}) : xQ \subseteq Q\} = O$ [3, Proposition 7.4]. Otherwise, Q is not O-invertible and $(Q : Q) = D$ (i.e. Q is a D-module). Note that Q is O-invertible if and only if $Q\bar{Q} = N(Q)O$; otherwise, $Q\bar{Q} = N(Q)fD$.

Lemma 2.1. *In the above notation, let $\alpha \in \mathfrak{F} \backslash fO$. Then $\mathfrak{F} = (f, \alpha)$.*

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. □

Let Q be an ideal of O. Using the properties of the norm, it is clear that Q is $\mathfrak{F}$-primary if and only if its norm $N(Q)$ is a positive power of f. Moreover, if Q is a primitive $\mathfrak{F}$-primary ideal of norm f^k, then

$$Q = f^k\mathbb{Z} + f\alpha\mathbb{Z} = f^kO + f\alpha O, \tag{2.1}$$

for some $\alpha \in D\backslash O$.

We give a definition which is crucial for our discussion.

Definition 2.2. Let $Q \subset O$ be a $\mathfrak{F}$-primary ideal and let $t \in O$. We say that Q is $\mathfrak{F}$-*basic* if $Q \not\subset \mathfrak{F}^2 = f\mathfrak{F}$. 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 $\mathfrak{F}$-primary basic ideal.

By definition, $\mathfrak{F}$ and fO are $\mathfrak{F}$-basic ideals; indeed, they are the only $\mathfrak{F}$-primary ideals containing f, since there are no intermediate ideals between fO and $\mathfrak{F}$. 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 following equivalences for a $\mathfrak{F}$-primary ideal Q are straightforward:

$$Q \text{ is } \mathfrak{F}\text{-basic} \Leftrightarrow Q \text{ is primitive} \Leftrightarrow Q \not\subset fO. \tag{2.2}$$

Given an $\mathfrak{F}$-primary ideal Q, the next lemma shows how to associate to Q an $\mathfrak{F}$-basic primary ideal in a canonical way.

Lemma 2.3. *Let Q be a $\mathfrak{F}$-primary ideal and let $k = \max\{n \in \mathbb{N} \mid \mathfrak{F}^n \supseteq Q\}$. Then we have*:

(i) *$Q = f^{k-1}Q'$, where Q' is a $\mathfrak{F}$-basic ideal.*
(ii) *If Q/f^m is $\mathfrak{F}$-basic for some $m > 0$, then m coincides with $k-1$.*

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

(ii) From $Q/f^m \subseteq \mathfrak{F}$ we get $Q \subseteq f^m\mathfrak{F} = \mathfrak{F}^{m+1}$, whence $m+1 \leq k$, by the definition of k. Moreover, from $Q/f^m \not\subset \mathfrak{F}^2 = f\mathfrak{F}$ we get $Q \not\subset f^{m+1}\mathfrak{F} = \mathfrak{F}^{m+2}$, hence $m+2 > k$. □

Given a $\mathfrak{F}$-primary ideal Q, the uniquely determined $\mathfrak{F}$-basic ideal Q' containing Q, as defined in (i) of Lemma 2.3, is called the *basic component* of Q. It follows that the lattice $\mathcal{L}$ of all the $\mathfrak{F}$-primary ideals is determined by 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 2.3, the elements of $\mathcal{L}_n$ are obtained by those of $\mathcal{L}_1$, just multiplying by f^{n-1}. Without loss of generality, we focus our attention on $\mathcal{L}_1$. Hence, in what follows, we will investigate the $\mathfrak{F}$-basic ideals of O.

The next proposition characterizes primary elements in terms of their norms.

Proposition 2.4. *Let* $t = fx + f\omega y \in \mathfrak{F}$ *be* $\mathfrak{F}$*-primary,* $x, y \in \mathbb{Z}$*. Then* 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. If the latter conditions hold, then* t *is an irreducible element of* O *which is not prime.*

Proof. The proof of the first two claims of the statement is straightforward, using the properties of the norm. For the last claim, 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. □

Let $t \in O$ be an $\mathfrak{F}$-primary element, $t = fx + f\omega y$, $x, y \in \mathbb{Z}$. Note that 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 (2.2), if $y \notin f\mathbb{Z}$ then t is $\mathfrak{F}$-basic. 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, for a basic element t, it is possible that $t \notin fO$, 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 3.4).

3. Intermediate $\mathfrak{F}$-Primary Ideals

Throughout this section, given a basic $\mathfrak{F}$-primary ideal $Q \subset O$ different from fO, by (2.1) and (2.2) we may suppose that $Q = (f^k, f\alpha)$, where $f^k = N(Q)$ and $\alpha \in D \setminus O$.

The following easy lemma determines whether an ideal of O is a D-module or not. 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.

Lemma 3.1. *Let* I *be an ideal of* O*.*

(i) *If* $zI \subseteq I$ *for some* $z \in D \setminus O$*, then* $I = ID$*.*
(ii) *If* $I \subset ID$*, then* $[ID : I] = f$*.*

Proof. (i) By the preliminaries of Sec. 2, $(I : I)$ is equal to O if and only if I is not a D-module. Hence, $(I : I) = D$, which proves the claim.

(ii) Let $\alpha = \sum_i a_i\beta_i \in ID$, for some $a_i \in I$ and $\beta_i \in D$. Then $f\alpha = \sum_i a_i f\beta_i$ is an element of I, since each $f\beta_i$ is in O. In particular, $fID \subset I \subset ID$, 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. □

The next proposition characterizes the $\mathfrak{F}$-basic ideals of O that are also D-modules. This kind of ideals will be crucial in the description of the lattice of

$\mathfrak{F}$-basic ideals. This result also follows from [1, p. 34]. We give a direct proof for the sake of completeness.

Proposition 3.2. *Let $Q = (f^k, f\alpha)$ be a $\mathfrak{F}$-basic ideal different from fO. Then Q is a D-module if and only if f^{k-1} divides $N(\alpha)$.*

Proof. Recall that Q is a D-module if and only if Q is not O-invertible (see Sec. 2). We have $Q\bar{Q} = (f^{2k}, f^{k+1}\alpha, f^{k+1}\bar{\alpha}, f^2 N(\alpha))$. If Q is a D-module, then $Q\bar{Q} = f^{k+1}D$ and therefore $f^{k-1} \mid N(\alpha)$. If $f^{k-1} \mid N(\alpha)$ then $Q\bar{Q} \subset f^{k+1}O$, hence $Q\bar{Q} \neq f^kO$, so Q is not O-invertible. □

We describe now the primary ideals lying in between a given $\mathfrak{F}$-primary ideal Q and fQ, according to whether Q is a D-module or not.

Theorem 3.3. *Let $Q = (f^k, f\alpha)$ be a $\mathfrak{F}$-basic ideal different from fO.*

(i) *$\mathfrak{F}^k$ is the minimum power of $\mathfrak{F}$ 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 $Q \not\subset fO$, so that $\mathfrak{F} = (f, f\alpha)$ (Lemma 2.1). Then $Q \supseteq (f^k, f^k\alpha) = f^{k-1}\mathfrak{F} = \mathfrak{F}^k$, where the equality holds if and only if $k = 1$. Since $f^{k-1} \in \mathfrak{F}^{k-1} \backslash Q$, k is the minimal integer such that $\mathfrak{F}^k \subseteq Q$.

(ii) Let $\alpha = a_1 + \omega a_2$, where $a_2 \notin f\mathbb{Z}$, since $\alpha \notin O$. Since $Q/fQ \cong \mathbb{Z}/f\mathbb{Z} \oplus \mathbb{Z}/f\mathbb{Z}$ (as abelian groups) and $\mathbb{Z}/f\mathbb{Z} \oplus \mathbb{Z}/f\mathbb{Z}$ 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

$$f(af^{k-1} + \alpha) = (x_0 + x_1 f\omega)f^{k+1} + (y_0 + y_1 f\omega)(f(bf^{k-1} + \alpha)),$$

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

$$af^{k-1} + \alpha - x_0 f^k - y_0(bf^{k-1} + \alpha) \in \omega Q \subseteq Q,$$

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 $af^{k-1} - y_0 bf^{k-1} \in Q$, hence $a - y_0 b \in f\mathbb{Z}$, by the minimality of k. We conclude that

$$1 \equiv y_0, \quad a \equiv y_0 b \mod f,$$

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

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

It remains to show that $J_a \neq Q$, for $a = 0, \dots, f-1$. Assume, for a contradiction, that $J_b = Q$ 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. Let J be an $\mathfrak{F}$-primary ideal properly lying between Q and fQ. Since Q is not a D-module, Q is an invertible O-ideal (see Sec. 2). Therefore, $I = JQ^{-1}$ is an $\mathfrak{F}$-primary ideal of O, so we get $J = QI \subseteq Q\mathfrak{F} = fQD$. Hence, we actually get the equality $J = fQD$, since $[Q : fQ] = f^2$. In particular, $J = (f^k, f^2\alpha)$. □

In particular, the preceding theorem allows us to determine the ideals lying between $\mathfrak{F}$ and $\mathfrak{F}^2$, since $\mathfrak{F}$ is a D-module and $\mathfrak{F}^2 = f\mathfrak{F}$.

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

Lemma 3.4. *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 $\mathfrak{F} \supseteq tD \supset \mathfrak{F}^2$, 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 3.4 implies that the number of principal $\mathfrak{F}$-primary ideals between $\mathfrak{F}$ and $\mathfrak{F}^2$ is equal to $|D^*/O^*|$. This last quantity depends on how the prime f splits in D.

Proposition 3.5. *Let $\tau = |D^*/O^*|$. Then we have*:

(i) *if f is inert in D, then $\tau \mid f + 1$.*
(ii) *if f is split in D, then $\tau \mid f - 1$.*
(iii) *if f is ramified in D, then $\tau \mid f$.*

Proof. Since f is prime, $O/\mathfrak{F} \cong \mathbb{F}_f$, the finite field with f elements. In particular, the group of units of $O/\mathfrak{F}$ has cardinality $f - 1$. The residue ring $D/\mathfrak{F}$ is isomorphic either to $\mathbb{F}_{f^2}$ (inert case), $\mathbb{F}_f \times \mathbb{F}_f$ (split case) or to a finite local ring with principal maximal ideal (ramified case). In each of the three cases, the group of units of $D/\mathfrak{F}$ has cardinality equal to $f^2 - 1$, $(f - 1)^2$ and $f^2 - f$, respectively.

The canonical ring homomorphism $\pi : D \twoheadrightarrow D/\mathfrak{F}$ induces a group homomorphism $\pi^* : D^* \to (D/\mathfrak{F})^*$ (which is not necessarily surjective). We have an induced group homomorphism: $D^*/O^* \to (D/\mathfrak{F})^*/(O/\mathfrak{F})^*$, $u + O^* \mapsto \pi^*(u) + (O/\mathfrak{F})^*$. 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 3.6. We note that the same conclusion of Proposition 3.5 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, pp. 146–148]). By Theorem 3.3, there are $f+1$ ideals properly lying 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 D-modules is:

(i) inert case: there is no intermediate D-module, since there are no D-modules between $\mathfrak{F} = P$ and $\mathfrak{F}^2 = P^2$.
(ii) split case: 2; the only D-modules between $\mathfrak{F} = P\overline{P}$ and $\mathfrak{F}^2 = P^2\overline{P}^2$ are $P^2\overline{P}$ and $P\overline{P}^2$.
(iii) ramified case: 1; the only D-module between $\mathfrak{F} = P^2$ and $\mathfrak{F}^2 = P^4$ is 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, respectively), 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, $\mathrm{Stab}(s) = \{g \in G \mid gs = s\} = \{1\}$.

Proposition 3.7. *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 $(D/\mathfrak{F})$-module, and so also a $(O/\mathfrak{F})$-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 3.1, for any assigned $I \in \mathcal{I}_O$ and $z \in D \backslash O$, we get $zI \not\subset I$. Hence, the sets $[\mathcal{I}]_{D/\mathfrak{F}}$ and $[\mathcal{I}]_{O/\mathfrak{F}}$ are characterized as follows:

$$[\mathcal{I}]_{D/\mathfrak{F}} = \{\bar{I} \in [\mathcal{I}] \,|\, \forall\, g \in G, g \cdot [I] = [I]\},$$
$$[\mathcal{I}]_{O/\mathfrak{F}} = \{\bar{I} \in [\mathcal{I}] \,|\, \forall\, g \in G, g \neq 1, g \cdot [I] \neq [I]\}.$$

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.

4. The Lattice of Basic Ideals

In this section, we analyze separately the lattice of $\mathfrak{F}$-basic ideals, in each of the three cases that may appear, namely: f inert, split or ramified in D, respectively.

4.1. *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 $D = \mathbb{Z}[\omega]$.

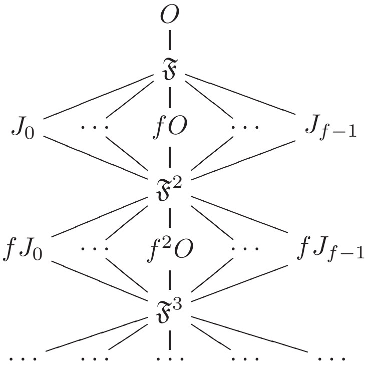
Theorem 4.1. *Suppose $\mathfrak{F} = fD$ is a prime ideal of D. Then every basic $\mathfrak{F}$-primary ideal of O contains $\mathfrak{F}^2$, and lies in the following set of pairwise distinct ideals*

$$\mathcal{J} = \{(f, f^2\omega), (f^2, f(a+\omega)) : 0 \leq a < f\}.$$

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 3.1 that $fQD = f\mathfrak{F} = \mathfrak{F}^2 \subset Q$. By Theorem 3.3, Q lies in the set $\mathcal{J}$. □

The number of principal basic $\mathfrak{F}$-primary ideals is exactly equal to the number of distinct non-associated basic elements of O, which is equal to $|D^*/O^*|$, by Lemma 3.4. 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. We recall that only the powers of $\mathfrak{F}$ are D-modules (see Remark 3.6). For this reason, all the proper intermediate ideals are O-invertible (see Sec. 2).



4.2. *Split case*

Throughout this section, we assume that $\mathfrak{F} = fD$ splits as an ideal of D, say $fD = P\bar{P}$, 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 2.4). 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 $\beta \in D$ a fixed generator of P^m.

Lemma 4.2. *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. □

The following theorem describes all the $\mathfrak{F}$-basic elements of O: it turns out that they are associated to the elements $t_n = f\beta^n$, for some $n \in \mathbb{N}$. In particular, in the split case, unlike the inert case, there are basic elements of arbitrary large norm, so, they are infinitely many.

Theorem 4.3. *For each $n \in \mathbb{N}$, let $t_n = f\beta^n$. An element $t \in O$ is basic if and only of t is associated in D either to t_n or its conjugate, for some $n \in \mathbb{N}$. Moreover, the principal ideals $t_nwO, \bar{t_n}w'O$, for $n > 0$ and $w, w' \in D^*$, $w/w' \notin O$, are pairwise incomparable and do not contain $\mathfrak{F}^2$.*

Proof. Since $N(t_n) = f^2N(\beta^n) = f^{mn+2}$, every element t_n is $\mathfrak{F}$-primary. Moreover, note that $t_n \notin \mathfrak{F}^2 = f\mathfrak{F}$, since $t_n/f = \beta^n \notin \mathfrak{F}$, so that t_n is $\mathfrak{F}$-basic, for every $n \geq 0$. Pick now two distinct non-negative integers n, m, with $n = m + h$, $h > 0$. Since $t_n/t_m = \beta^h \notin O$ and $t_m/t_n = \beta^{-h} \notin O$, it follows that the ideals t_nO, for $n \geq 0$, 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_nO.

Conversely, let t be a basic element of O of norm f^{s+2}, $s \geq 0$. 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 $tD = fP^{k-1}$. Then P^{k-1} is principal, hence $k - 1 = mn$, for some positive integer n. It follows that $N(t) = f^{s+2} = f^2 N(P^{mn}) = f^{mn+2}$, so, $s = mn$. Now, we have $tD = fP^{mn} = f\beta^n D = t_n D$, which is possible only if $t = t_n w$, for some $w \in D^*$. In the case $k = 1$ we symmetrically get $t = \bar{t}_n w$ for some $w \in D^*$.

Finally, if $t_h w O = \bar{t}_k w' O$, then $h = k$ otherwise t_h, t_k have different norms and we get that some power of β is in O, which is impossible by Lemma 4.2. Moreover, $t_h w O = t_k w' O$ implies $h = k$ as before, hence we also get $w/w' \in O$. □

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

We recall that a Special Principal Ideal Ring (or special PIR, for short) R is a principal ideal ring with a unique prime ideal M, such that M is nilpotent (see [8, p. 245]). So, in the case when $M = pR$, for some $p \in R$, we get $p^n = 0$ for some $n > 1$. Note that a Special PIR is a chained ring, i.e. the ideals are linearly ordered.

The next lemma gives all the basic $\mathfrak{F}$-primary ideals that contain some $\mathfrak{F}$-basic element.

Lemma 4.4. *The quotient ring O/t_nO is a Special PIR for every $n \geq 0$. In particular, the ideals (necessarily $\mathfrak{F}$-primary) that contain t_nO are equal to (f^i, t_n), for $i = 1, \ldots, mn + 2$, and their norm of (f^i, t_n) is f^i.*

Proof. The claim is immediate when $t_n = t_0 = f$, since $\mathfrak{F}/fO$ is the unique non-zero proper ideal of O/fO, it is generated by $f\omega + fO$, and $(\mathfrak{F}/fO)^2 = 0$, since $\mathfrak{F}^2 \subset fO$. 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. In particular, O/t_nO has a unique maximal ideal, equal to $\mathfrak{F}/t_nO$. Since $\mathfrak{F} = (f, t_n)$ by Lemma 2.1, 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 non-zero 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, $f^h \in t_nO$ if and only if $h \geq mn + 2$, since $N(t_n) = f^{mn+2}$.

Since f^i is the least power of f contained in the basic ideal (f^i, t_n) (which therefore is primitive by (2.2)), the last claim follows by the preliminaries in Sec. 2. □

Proposition 4.5. *Let $t \in O$ be a basic $\mathfrak{F}$-primary element of norm f^m, and let $i \in \mathbb{N}$ be such that $i < m$. Then the ideal $I = (f^i, t)$ of O is a D-module and is equal either to $P^i\bar{P}$ or $P\bar{P}^i$. In particular, we get $(f^i, t_i) = (f^i, t_n)$, for every $n \geq i$.*

Proof. Since $f^{i+1} \mid N(t)$, we get $I = ID$, by Proposition 3.2. Without loss of generality, we suppose that $tD = P^{m-1}\bar{P}$ (see the proof of Theorem 4.3). Since D is a

Dedekind domain, $f^iD + tD$ is the greatest common divisor of f^iD and tD, so it is equal to $P^i\bar{P}$, since $f^iD = (P\bar{P})^i$. Hence, $I = ID = P^i\bar{P}$. The last claim follows immediately, since f^i divides $N(t_n) = f^{nm+2}$ for every $n \geq i$. □

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

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

Theorem 4.6. (i) *Let Q be a $\mathfrak{F}$-basic ideal. Then there exists $k \geq 1$ such that $fQ_k \subset Q \subseteq Q_k$.*

(ii) *The ideals $Q_k = (f^k, t_k)$, for $k \in \mathbb{N}$, are pairwise distinct.*

(iii) *An ideal I of O contains Q_k if and only if $I \in \{Q_i : i = 0, \ldots, k\}$.*

(iv) *If Q contains a basic element and it is not principal, then either $Q = Q_k$ or $Q = \bar{Q}_k$ for some $k \in \mathbb{N}$.*

Proof. (i) Since Q is basic, as in the proof of Theorem 4.3, we have $QD = P^k\bar{P} = Q_k$, for some $k \geq 1$ (or its conjugate), so $Q \subseteq Q_k$. By Lemma 3.1, either $Q = Q_k$ or $[Q_k : Q] = f$. In each case, we get $fQ_k \subset Q \subseteq Q_k$.

(ii) By Proposition 4.5, we get $Q_k = P^k\bar{P}$ (and not the conjugate, since $\beta^k \in P\backslash\bar{P}$). Hence the Q_k's are pairwise distinct, as k ranges in $\mathbb{N}$.

(iii) For $0 \leq i \leq k$, by Proposition 4.5 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 Lemma 4.4, we get $I = (f^j, t_k)$, for some $j \in \{1, \ldots, k+1\}$, so $I = (f^j, t_k) = (f^j, t_j) = Q_j$.

(iv) This follows from (ii) and its proof, possibly replacing 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 4.7. *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 Theorem 4.6(i), and it is different from Q_k, since it does not contain basic elements.

(ii) This follows from Theorem 3.3, 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.

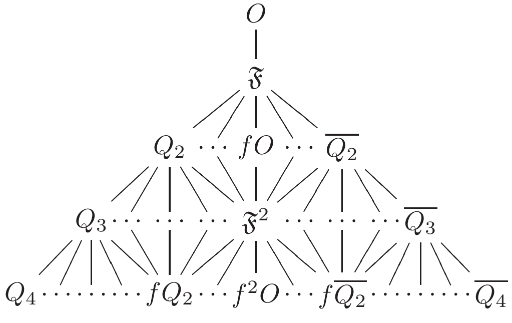
(iii) Let Q' be a basic ideal contained in $Q = (f^{k+1}, af^k + t_k)$. Then Q' cannot contain a $\mathfrak{F}$-basic element, hence, by (ii) we get $Q' = (f^{h+1}, bf^h + t_h)$, for some $h > 0$, $b \in \{1, \dots, f-1\}$. Let us assume, for a contradiction, that $Q \neq Q'$, so $Q \supset Q'$. It follows 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 Proposition 3.2, it suffices to show that f^k does not divide $N(\gamma)$. 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 β^k (otherwise $\beta^k \in fD = \mathfrak{F}$, impossible), we see that $N(\gamma) = f^{k-1}b$, where $b \notin f\mathbb{Z}$. □

Note that an ideal Q satisfying the hypothesis of the previous theorem is not a D-module. The converse of Theorem 4.7(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 4.8. Let $k \in \mathbb{N}$. By Theorem 4.3, 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 $\beta \in D \backslash O$. Hence, $f\beta O$ is an intermediate ideal between fQ_k and Q_k. Moreover, as we saw in the proof of Theorem 4.3, the last condition holds if and only if m divides $k-1$. For such k's, there are $\tau = [D^* : O^*]$ intermediate principal ideals between Q_k and fQ_k (essentially by the same phenomenon of Lemma 3.4).

The diagram below represents the lattice of $\mathfrak{F}$-primary ideals in the split case.



4.3. *Ramified case*

We assume now that f is ramified in D, so $\mathfrak{F} = P^2$, for some prime ideal P of D.

Theorem 4.9. (i) *If* $d \equiv 1, 2 \pmod 4$ *or* $d \equiv 3 \pmod 4$ *and* $f \neq 2$, *then we have* $P = fD + \sqrt{d}D$. *If* $d \equiv 3 \pmod 4$ *and* $f = 2$, *then* $P = 2D + (1 + \sqrt{d})D$.

(ii) *Let* $Q \subseteq \mathfrak{F}$ *be a basic* $\mathfrak{F}$*-primary ideal. Then either* $P^4 \subset Q \subseteq P^2$ *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* $d \equiv 3 \pmod 4$; *in this latter case, we either get* $Q = (8, 2(1+\sqrt{d}))$ *or* $Q = (8, 4 + 2(1+\sqrt{d}))$, *or* $Q = (4, 4(1+\sqrt{d})) = P^4$.

Proof. (i) In any case, we have $\mathfrak{F} = (f, f\sqrt{d})$. Assume that $f \mid d$; we get $d = f\lambda$, with $\lambda \notin f\mathbb{Z}$, since d is square-free. Then the ideal $(f, \sqrt{d})$ of D satisfies $(f, \sqrt{d})^2 = (f^2, d)D = fD = \mathfrak{F}$, 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 3.1, $fQD \subset Q \subseteq QD$, which is the statement.

(iii) and (iv) follow from Theorem 3.3, 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 $(4, 4(1+\sqrt{d})) = 2\mathfrak{F} = \mathfrak{F}^2 = P^4$. □

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 3.4), 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.

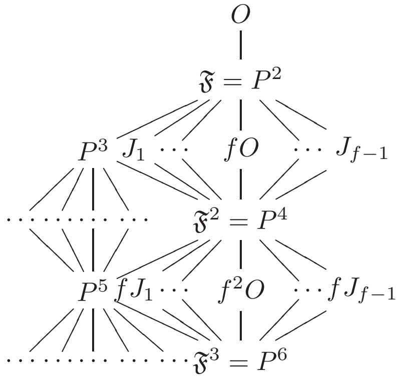
Proposition 4.10. *There exists a basic element* $t \in O$ *such that* $P^5 \subset tO \subset P^3$ *if and only if* P *is a principal ideal of* D. *If this condition holds, say* $P = \beta D$, *for some* $\beta \in D$, *then every basic element is associated to* $f\beta$ *by a unit of* D.

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 Proposition 2.4, since its norm is f^3 and $t \notin fO$. Since $tD = \beta^3 D = P^3$, we get $\beta^5 D = P^5 \subset tO \subset P^3$.

Conversely, let $t \in O$ be a basic element such that $P^5 \subset tO \subset P^3$. Using Lemma 3.1, we get $tD = P^3 = fP$, so $P = \frac{t}{f}D$ is a principal ideal of D.

The last claim follows arguing as in Lemma 3.4. □

The diagram below represents the lattice of $\mathfrak{F}$-primary ideals in the ramified case. By Proposition 3.2 and the above description of the basic ideals, all the basic ideals, with the exception of $\mathfrak{F}$ and P^3, are invertible.



In our final remark we make some considerations for the case where f is not prime.

Remark 4.11. We retain the preceding notation, but here we assume that f is not a prime number, say $f = \prod_{i=1}^{n} f_i^{s_i}$, where the $f_i \in \mathbb{Z}$ are pairwise distinct prime numbers and $s_i \geq 0$. Under the present circumstances, it is straightforward to verify that the conductor $\mathfrak{F} = (f, f\omega)$ is the product $\mathfrak{F} = \prod_{i=1}^{n} \mathfrak{G}_i$, where $\mathfrak{G}_i = (f_i^{s_i}, f\omega)$, for $i = 1, \ldots, n$. The $\mathfrak{G}_i$ are primary ideals of O, namely, $\sqrt{\mathfrak{G}_i} = \mathfrak{F}_i = (f_i, f\omega)$, where the $\mathfrak{F}_i$'s are the prime ideals of O that contain $\mathfrak{F}$. Then the lattice of the primary ideals of $O = \mathbb{Z}[f\omega]$ is given by the disjoint union of the lattices of the $\mathfrak{F}_i$-primary ideals, together with the chains of the powers of the prime ideals N of O that are coprime with $\mathfrak{F}$. So we may confine ourselves to a prime ideal $\mathfrak{F}_i$, for a fixed $i \in \{1, \ldots, n\}$. It can be easily verified that $\mathfrak{F}_i^2 = f_i\mathfrak{F}_i$, so also the lattice of the $\mathfrak{F}_i$-primary ideals has a structure by layers. The main definitions and several results, proved above for the case of $\mathfrak{F}$ prime, can be adapted to $\mathfrak{F}_i$-primary ideals. We intend to examine thoroughly this general case in a future paper. The main difference with the case of $\mathfrak{F}$ prime is that the $\mathfrak{F}_i$ are not D-modules, and, in fact, no $\mathfrak{F}_i$-primary ideal is a D-module if f is not a power of a single prime.

As an instance, we give a generalization of the formula we obtained in the case of prime conductor to the general case. We use the notation $O_f = \mathbb{Z}[f\omega]$. Then for each $i = 1, \ldots, n$ we have

$$\mathfrak{F}_i = f_iO_f + f\omega O_f = f_iO_{f/f_i} = (O_f : O_{f/f_i})$$

that is, $\mathfrak{F}_i$ is the conductor of the order $O_{f/f_i} = \mathbb{Z}[\frac{f}{f_i}\omega]$ into the order $\mathbb{Z}[f\omega]$.

Acknowledgments

This research has been supported by "Progetti di Eccellenza 2011/12" of Fondazione CARIPARO and by the grant "Assegni Senior" of the University of Padova.

References

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

[2] ———, 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* (John Wiley & Sons, New York, 1989).

[4] T. W. Hungerford, On the structure of principal ideal rings, *Pacific J. Math.* **25** (1968) 543–547.

[5] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, Carus Mathematical Monographs, Vol. 10 (Mathematical Association of America, New York, 1950).

[6] G. Peruginelli, L. Salce and P. Zanardo, Idempotent pairs and PRINC domains, in *Multiplicative Ideal Theory and Factorization Theory — Commutative and Non-Commutative Perspectives* (Springer, New York, 2016), pp. 309–322.

[7] P. Zanardo and U. Zannier, The class semigroup of orders in number fields, *Math. Proc. Cambridge Philos. Soc.* **115** (1994) 379–391.

[8] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1 (Springer, New York, 1975).