The lattice of primary ideals of orders in quadratic number fields

Paolo Zanardo (University of Padova)

Conference on Rings and Polynomials, Graz 2016

Joint work with Giulio Peruginelli.

Let $d \in \mathbb{Z}$ be square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $D = \mathbb{Z}[\omega]$, where either $\omega = \sqrt{d}$ or $\omega = (1 + \sqrt{d})/2$, when $d \equiv 2, 3$ or $d \equiv 1 \bmod 4$, respectively.
A proper quadratic order is an integral domain O with integral closure $D \neq O$. It has the form $O = \mathbb{Z}[f\omega]$, for some $f > 0$. The *conductor* of O in D is

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

We get $\mathfrak{F}^2 = f\mathfrak{F}$, hence $\mathfrak{F}^k = f^{k-1}\mathfrak{F}$ for each $k > 0$. We focus on the case where the conductor is a prime ideal of O, which holds if and only if f is a prime number.
A proper order does not enjoy unique factorization into prime ideals. Being a one-dimensional Noetherian domain, each ideal of O is uniquely a product of primary ideals.
Each primary ideal coprime to the conductor $\mathfrak{F}$ is equal to a power of its radical.

Butts and Pall, Acta Arith. 1968 and 1972, 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. They mainly focused on invertible ideals.

We describe the lattice of $\mathfrak{F}$-primary ideals of a quadratic order O.
We provide generating sets, that show the relations of containment of these ideals.
We get three completely different lattices of $\mathfrak{F}$-primary ideals, according to whether fD is a prime ideal in D (inert case), or a product of two distinct prime ideals of D (split case), or the square of a prime ideal of D (ramified case). These lattices have a crucial property in common, a *structure by layers*.
The structure is determined by its first layer, the set of $\mathfrak{F}$-primary ideals not contained in $\mathfrak{F}^2$. The remainder of the lattice is formed by the n-th layers ($n > 1$), i.e. the ideals $Q \subseteq \mathfrak{F}^n$ and $Q \nsubseteq \mathfrak{F}^{n+1}$, that reproduce the same pattern of the first layer.
Recall that, when $N \neq \mathfrak{F}$ is a prime ideal of O, the lattice of N-primary ideals is just the chain of the powers of N.

Definition. A $\mathfrak{F}$-primary ideal Q is called $\mathfrak{F}$-*basic* if $Q \not\subseteq \mathfrak{F}^2 = f\mathfrak{F}$.

LEMMA 1

Let Q' be any $\mathfrak{F}$-primary ideal. If $\mathfrak{F}^n$ is the highest power of $\mathfrak{F}$ containing Q', then $Q' = f^{n-1}Q$, where Q is a $\mathfrak{F}$-basic ideal.

By Lemma 1, the lattice $\mathcal{L}$ of all the $\mathfrak{F}$-primary ideals is determined by the lattice $\mathcal{L}_1$ of $\mathfrak{F}$-basic ideals.
$\mathcal{L}_1$ will be the first layer of $\mathcal{L}$; the other layers are the $\mathcal{L}_n$ $(n > 0)$, of the $\mathfrak{F}$-primary ideals $Q \subseteq \mathfrak{F}^n$, $Q \not\subseteq \mathfrak{F}^{n+1}$. 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 $\mathcal{L}$ is structured by layers.
So it suffices to investigate $\mathcal{L}_1$.

Let Q be $\mathfrak{F}$-basic. Then $Q = (f^k, f\alpha)$, where f^k is the smallest positive integer contained in Q, and $\alpha \in D$.
We firstly characterize the $\mathfrak{F}$-basic ideals of O that are also D-modules.

THEOREM 2

Let $Q = (f^k, f\alpha)$ be a $\mathfrak{F}$-basic ideal different from fO, where f^k is the smallest positive integer 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.

Theorem 3

Let $Q = (f^k, f\alpha)$ be a $\mathfrak{F}$-basic ideal different from fO, where f^k is the smallest positive integer contained in Q.

(I) $\mathfrak{F}^k$ is the least power of $\mathfrak{F}$ contained in Q

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

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

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

The lattice of $\mathfrak{F}$-basic ideals.

We analyze separately the lattice $\mathcal{L}_1$ of $\mathfrak{F}$-basic ideals, in the three cases f inert, split or ramified in D.

Inert case.

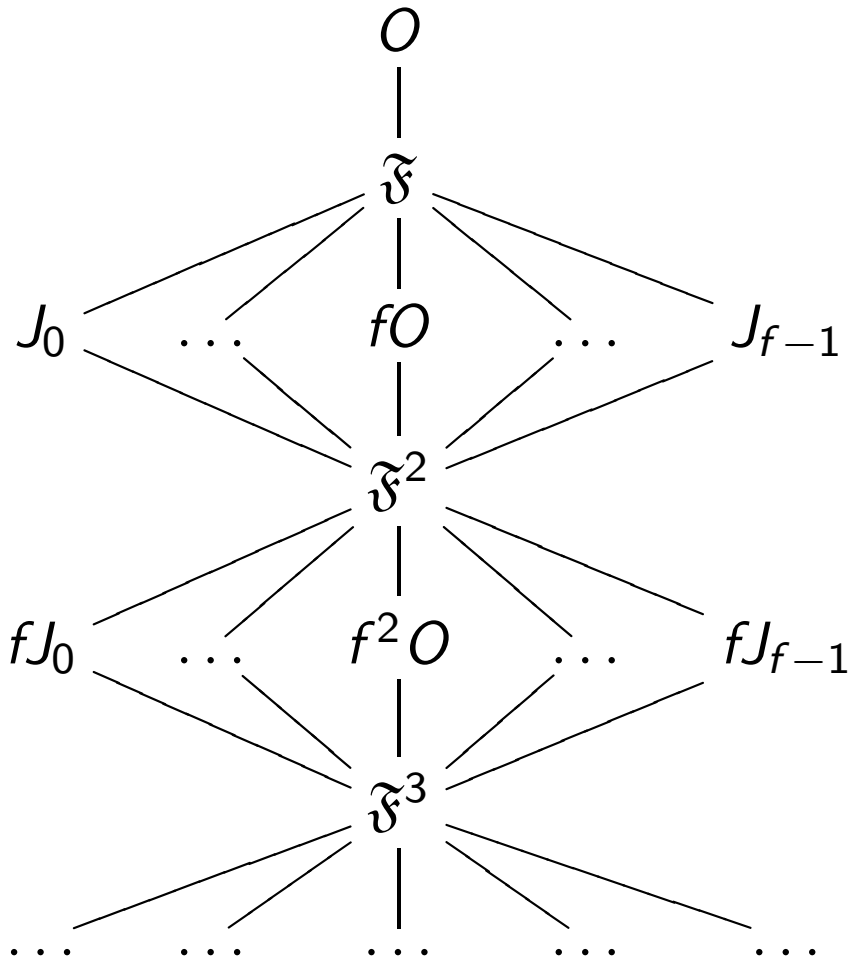
Here $O = \mathbb{Z}[f\omega]$ and $fD = \mathfrak{F}$ is a prime ideal of D.

Theorem 4

Let fD be a prime ideal of D. Then every $\mathfrak{F}$-basic ideal contains $\mathfrak{F}^2$, and coincides with one of the following pairwise distinct ideals

$$fO = (f, f^2\omega),\ J_a = (f^2, f(a+\omega)), \quad 0 \leq a < f.$$

The lattice of $\mathfrak{F}$-primary ideals in the inert case is $\mathfrak{F}$-*chained* in the sense of Salce, Houston J. Math. 2005.



Split case.

Here $\mathfrak{F} = fD$ splits in D, i.e., $fD = P\bar{P}$, where $P \neq \bar{P}$ are prime ideals of D.
Let m be the order of P in the class group of D, i.e., $P^m = \beta D$ is principal, m minimum.

Proposition

For $n \geq 0$, let $t_n = f\beta^n \in O$. The principal ideals $t_n O$ are $\mathfrak{F}$-basic, pairwise incomparable, and do not contain $\mathfrak{F}^2$ if $n > 0$;
$t_0 O = fO \supset \mathfrak{F}^2$.

So in the split case there are infinitely many basic ideals.

An element $t \in O$ is called *basic* if tO is $\mathfrak{F}$-basic.

THEOREM 5

Let $t \in O$ be basic. Then $t \in \{t_n w, \bar{t}_n w : w \in D^*\}$. Moreover
(a) $t_h w O \neq \bar{t}_k w' O$ for any $h, k > 0$, $w, w' \in D^*$;
(b) $t_h w O = t_k w' O$ if and only if $h = k$ and $w/w' \in O$.

We define a chain of ideals whose importance is shown by the next theorem.

For $k \geq 1$, define $Q_k = (f^k, t_k)$.

Then $\mathfrak{F} = Q_1$. We have $Q_1 \supset Q_2 \supset \cdots \supset Q_k \supset \ldots$

Theorem 6

Let Q be a $\mathfrak{F}$-basic ideal. Then there exists $k \geq 1$ such that either $fQ_k \subset Q \subseteq Q_k$, or $f\bar{Q}_k \subset Q \subseteq \bar{Q}_k$.

Non-principal $\mathfrak{F}$-basic ideals of O that contain a basic element.

THEOREM 7

Let Q be $\mathfrak{F}$-basic and not principal. If Q contains a basic element, then either $Q = Q_k = (f^k, t_k)$ or $Q = \bar{Q}_k$ for some $k \geq 1$.

$\mathfrak{F}$-basic ideals of O that do not contain basic elements.

THEOREM 8

Let Q be $\mathfrak{F}$-basic, such that $fQ_k \subset Q \subseteq Q_k = (f^k, t_k)$, $k \geq 1$. If Q does not contain any basic element, then

(I) $Q \neq Q_k$;

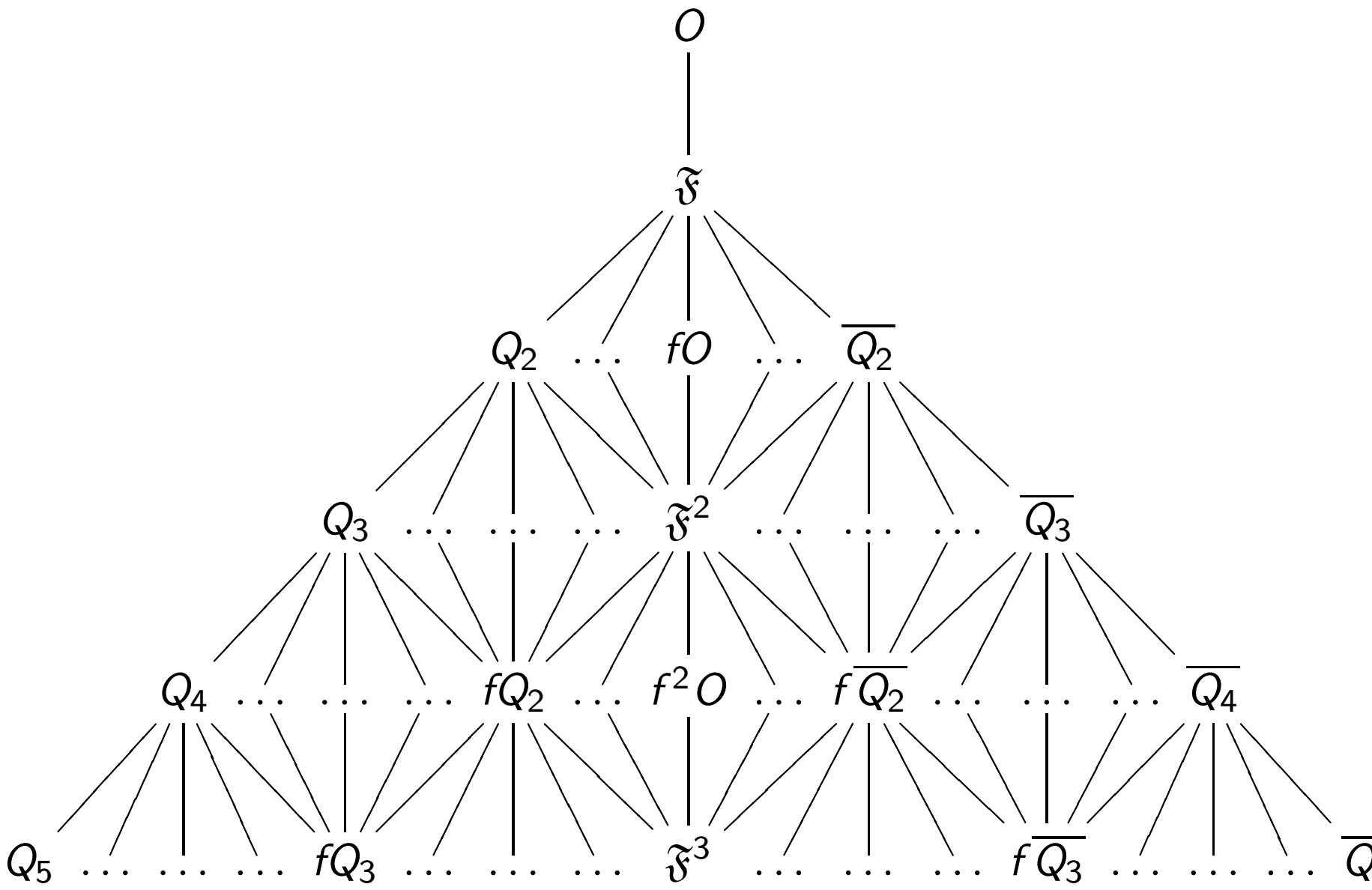
(II) $Q = (f^{k+1}, af^k + t_k)$ for some $1 \leq a \leq f-1$;

(III) Q does not properly contain any $\mathfrak{F}$-basic ideal.

(IV) Q is an invertible ideal of O.

Analogous results hold if $f\bar{Q}_k \subset Q \subseteq \bar{Q}_k$.

Lattice of $\mathfrak{F}$-primary ideals in the split case.



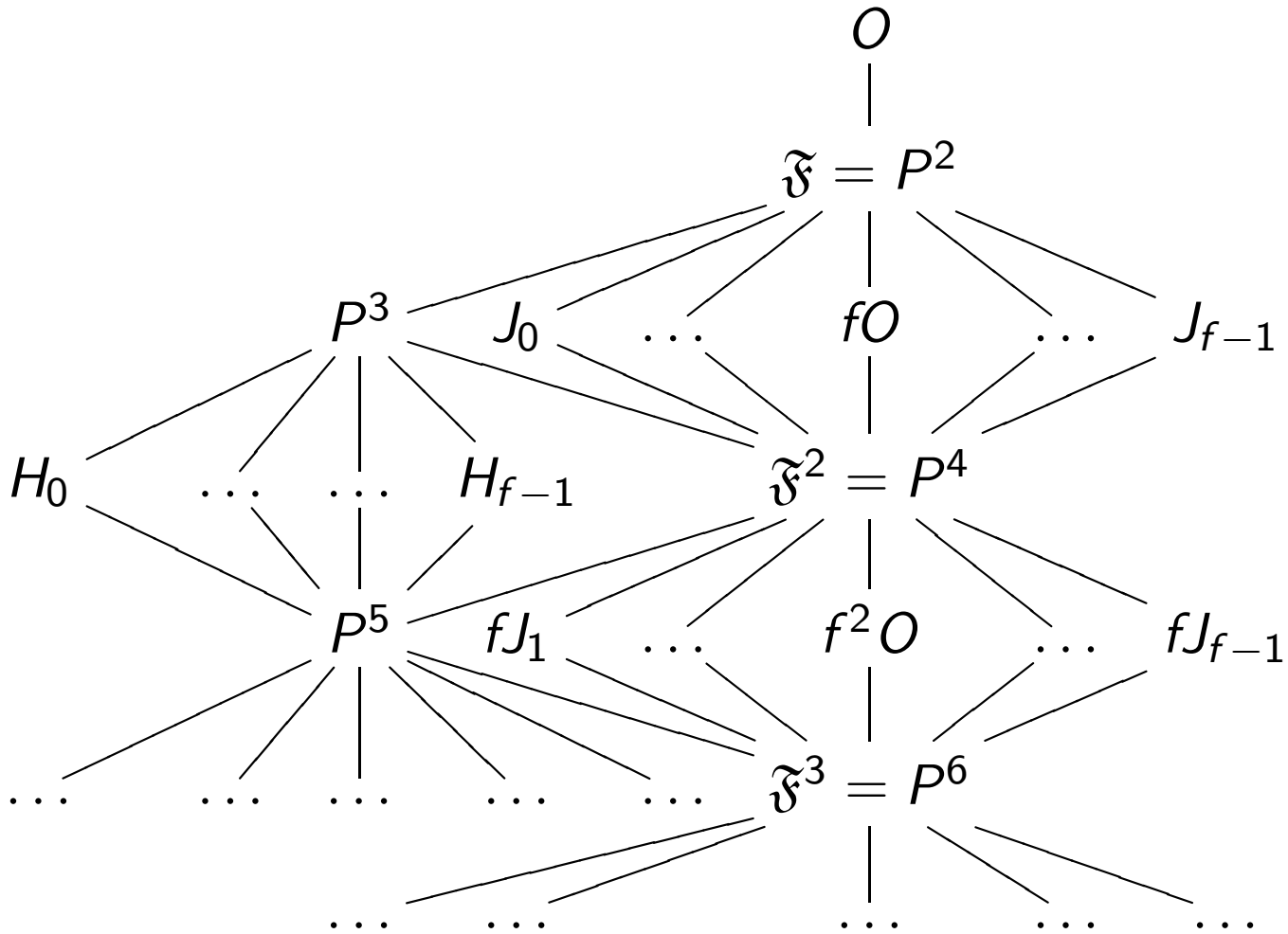
Ramified case.

Recall that f is ramified if and only if either $f \mid d$, when $d \equiv 1 \bmod 4$, or $f \mid 4d$, when $d \equiv 2, 3 \bmod 4$.
Say $\mathfrak{F} = P^2$, P prime ideal of D. Then $P = fD + \sqrt{d}D$, except for $f = 2$ and $d \equiv 3 \bmod 4$, when $P = 2D + (1 + \sqrt{d})D$.

Theorem 9

Let $\mathfrak{F} = P^2$, P prime ideal of D. If $Q \neq \mathfrak{F}$ is $\mathfrak{F}$-basic, then
(i) either $P^4 \subset Q \subset P^2$ or $P^5 \subset Q \subseteq P^3$.
(ii) If $P^4 \subset Q \subset P^2$, then either $Q = J_a = (f^2, fa + f\sqrt{d})$, $0 \leq a < f$, or $Q = fO$.
(iii) if $P^5 \subset Q \subset P^3$, then $Q = H_a = (f^3, af^2 + f\sqrt{d})$, $0 \leq a < f$, except for $f = 2$ and $d \equiv 3 \bmod 4$. In this latter case, either $Q = (8, 2(1 + \sqrt{d}))$, or $Q = (8, 4 + 2(1 + \sqrt{d}))$.

Lattice of $\mathfrak{F}$-primary ideals in the ramified case.



We determine the principal *intermediate* ideals tO, i.e., such that $\mathfrak{F}^2 \subset tO \subset \mathfrak{F}$.

THEOREM

As above, let $O = \mathbb{Z}[f\omega] \subset D = \mathbb{Z}[\omega] \subset \mathbb{Q}[\sqrt{d}]$.

(I) Let $d < 0$. Then the only principal intermediate ideal is fO, except for $d = -1$, where the principal intermediate ideals are fO and fiO, and $d = -3$, where the principal intermediate ideals are fO and $f\omega O$, $f\omega^2 O$, $\omega = (1 + \sqrt{-3})/2$.

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