ANNALES MATHÉMATIQUES

BLAISE PASCAL

Martine Picavet-L'Hermitte

Cale Bases in Algebraic Orders

Volume 10, n°1 (2003), p. 117-131.

<http://ambp.cedram.org/item?id=AMBP_2003__10_1_117_0>

ANNALES MATHEMATIQUES BLAISE PASCAL **10**, 117-131 (2003)

Cale Bases in Algebraic Orders

Martine Picavet-L'Hermitte

Abstract

Let R be a non-maximal order in a finite algebraic number field with integral closure $\overline{R}$. Although R is not a unique factorization domain, we obtain a positive integer N and a family $\mathcal{Q}$ (called a Cale basis) of primary irreducible elements of R such that x^N has a unique factorization into elements of $\mathcal{Q}$ for each $x \in R$ coprime with the conductor of R. Moreover, this property holds for each nonzero $x \in R$ when the natural map $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ is bijective. This last condition is actually equivalent to several properties linked to almost divisibility properties like inside factorial domains, almost Bézout domains, almost GCD domains.

1 Introduction

Let K be a number field and $\mathcal{O}_K$ its ring of integers. A subring of $\mathcal{O}_K$ with quotient field K is called an **algebraic order** in K. Let R be a non-integrally closed order with integral closure $\overline{R}$. Since R cannot be a unique factorization domain, an element of R need not have a unique factorization into irreducibles. Let R be a quadratic order such that $\mathfrak{f}$ is the conductor of $R \hookrightarrow \overline{R}$. A. Faisant got a unique factorization into a family of irreducibles for any x^e where $x \in R$ is such that $Rx + \mathfrak{f} = R$ and e is the exponent of the class group of R [7, Théorème 2]. We are going to generalize his result to an arbitrary order and to a larger class of elements, using the notion of Cale basis defined by S.T. Chapman, F. Halter-Koch and U. Krause in [4]. In Section 2, we show that there exists a Cale basis for an order R if and only if the spectral map $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ is bijective. This condition is also equivalent to $R \hookrightarrow \overline{R}$ is a root extension, or R is an API-domain (resp. AD-domain, AB-domain, AP-domain, AGCD-domain, AUFD). These integral domains were studied by D. D. Anderson and M. Zafrullah in [3] and [11]. In Section 3, we consider orders R such that $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ is bijective and exhibit a Cale basis $\mathcal{Q}$ for such an order. The elements of

$\mathcal{Q}$ are primary and irreducible and we determine a number N, linked to some integers associated to R, such that x^N has a unique factorization into elements of $\mathcal{Q}$ for each nonzero $x \in R$. When R is an arbitrary order, we restrict this property to a smaller class of nonzero elements of R. We do not know whether the integer N is the minimum number such that x^N has a unique factorization into elements of $\mathcal{Q}$ for each nonzero $x \in R$, but we get an affirmative answer for $\mathbb{Z}[3i]$.

A generalization of these results can be gotten by considering a residually finite one-dimensional Noetherian integral domain R with torsion class group or finite class group and such that its integral closure is a finitely generated R-module.

Throughout the paper, we use the following notation:

For a commutative ring R and an ideal I in R, we denote by $\mathrm{V}_R(I)$ the set of all prime ideals in R containing I and by $\mathrm{D}_R(I)$ its complement in $\mathrm{Spec}(R)$. If R is an integral domain, $\mathcal{U}(R)$ is the set of all units of R and $\overline{R}$ is the integral closure of R. The conductor of $R \hookrightarrow \overline{R}$ is called the *conductor* of R. For $a, b \in R \setminus \{0\}$, we write $a|b$ if $b = ac$ for some $c \in R$. Let J be an ideal of R and x an element of R: we say that x is *coprime* to J if $Rx + J = R$ and we denote by $\mathrm{Cop}_R(J)$ the monoid of elements of R coprime to J. The cardinal number of a finite set S is denoted by $|S|$. When an element x of a group has a finite order, $\mathrm{o}(x)$ is its order. As usual, $\mathbb{N}^*$ is the set of nonzero natural numbers.

2 Almost divisibility

A Cale basis generalizes for an integral domain the set of irreducible elements of a unique factorization domain. In fact, S.T. Chapman, F. Halter-Koch and U. Krause first introduced this notion in [4] for monoids and later on extended it to integral domains.

Definition: Let R be a multiplicative, commutative and cancellative monoid. A subset of nonunit elements $\mathcal{Q}$ of R is a *Cale basis* if R has the following two properties:

1. For every nonunit $a \in R$, there exist some $n \in \mathbb{N}^*$ and $t_i \in \mathbb{N}$ such that $a^n = u \prod_{q_i \in \mathcal{Q}} q_i^{t_i}$ where $u \in \mathcal{U}(R)$ and only finitely many of the t_i's are nonzero.

2. If $u \prod_{q_i \in \mathcal{Q}} q_i^{t_i} = v \prod_{q_i \in \mathcal{Q}} q_i^{s_i}$ where $u, v \in \mathcal{U}(R)$ and $s_i, t_i \in \mathbb{N}$ with $s_i = t_i = 0$ for almost all $q_i \in \mathcal{Q}$, then $u = v$ and $t_i = s_i$ for all $q_i \in \mathcal{Q}$.

3. A monoid is called *inside factorial* if it possesses a Cale basis.

4. An integral domain R is called *inside factorial* if its multiplicative monoid $R \setminus \{0\}$ is inside factorial.

Remark: In [4], the authors give the definition of an inside factorial monoid by means of divisor homomorphisms, but their result [4, Proposition 4] allows us to use this simpler definition.

Proposition 2.1: *Let R be a one-dimensional Noetherian inside factorial domain with Cale basis $\mathcal{Q}$. Any element of $\mathcal{Q}$ is a primary element and there is a bijective map*

$$\begin{cases} \mathcal{Q} \to \mathrm{Max}(R) \\ q \mapsto \sqrt{Rq} \end{cases}$$

Proof: Let $q \in \mathcal{Q}$ and show that Rq is a primary ideal. Let $x, y \in R \setminus \{0\}$ be such that $q|(xy)^k = x^k y^k$ for some $k \in \mathbb{N}^*$. By [4, Lemma 2 (f)], there exists some $n \in \mathbb{N}^*$ such that $q|x^{kn}$ or $q|y^{kn}$. This implies that $\sqrt{Rq}$ is a maximal ideal in R and Rq is a primary ideal.

Let $P \in \mathrm{Max}(R)$ and $q, q' \in \mathcal{Q}$ be two P-primary elements. R being Noetherian, there exists some $n \in \mathbb{N}^*$ such that $Rq^n \subset P^n \subset Rq'$, so that $q'|q^n$. Set $q^n = q'x$, $x \in R$. Since R is inside factorial, there exist some $k \in \mathbb{N}^*$ and $t_i \in \mathbb{N}$ such that $x^k = u \prod_{q_i \in \mathcal{Q}} q_i^{t_i}$ where $u \in \mathcal{U}(R)$. This gives $q^{nk} = uq'^k \prod_{q_i \in \mathcal{Q}} q_i^{t_i}$ and $q = q'$ since $\mathcal{Q}$ is a Cale basis.

Let $P \in \mathrm{Max}(R)$ and x be a nonzero element of P. There exist some $n \in \mathbb{N}^*$ and $t_i \in \mathbb{N}$ such that $x^n = u \prod_{q_i \in \mathcal{Q}} q_i^{t_i}$ where $u \in \mathcal{U}(R)$. Then $Rx^n = \prod_{q_i \in \mathcal{Q}} Rq_i^{t_i}$ with $Rq_i^{t_i}$ a P_i-primary ideal and $t_i \neq 0$ for each P_i containing x. Moreover we have $P_i \neq P_j$ for $i \neq j$. Since P contains x, one of the P_i such that $t_i \neq 0$ is P so that q_i is P-primary. So we get the bijection. □

Remark: We recover here the structure of Cale bases gotten in [4, Theorem 2] with the additional new property that every element of the Cale basis is a primary element.

For a one-dimensional Noetherian domain with torsion class group, the notion of inside factorial domain is equivalent to a lot of special integral domains with different divisibility properties we are going to recall now (see [11], [3] and [1]).

Definition: Let R be an integral domain with integral closure $\overline{R}$. We say that

1. $R \hookrightarrow \overline{R}$ is a *root extension* if for each $x \in \overline{R}$, there exists an $n \in \mathbb{N}^*$ with $x^n \in R$ [3].

2. R is an *almost principal ideal domain* (API-domain) if for any nonempty subset $\{a_i\} \subseteq R \setminus \{0\}$, there exists an $n \in \mathbb{N}^*$ with $(\{a_i^n\})$ principal [3, Definition 4.2].

3. R is an *AD-domain* if for any nonempty subset $\{a_i\} \subseteq R \setminus \{0\}$, there exists an $n \in \mathbb{N}^*$ with $(\{a_i^n\})$ invertible [3, Definition 4.2].

4. R is an *almost Bézout domain* (AB-domain) if for $a, b \in R \setminus \{0\}$, there exists an $n \in \mathbb{N}^*$ such that (a^n, b^n) is principal [3, Definition 4.1].

5. R is an *almost Prüfer domain* (AP-domain) if for $a, b \in R \setminus \{0\}$, there exists an $n \in \mathbb{N}^*$ such that (a^n, b^n) is invertible [3, Definition 4.1].

6. R is an *almost GCD-domain* (AGCD-domain) if for $a, b \in R \setminus \{0\}$, there exists an $n \in \mathbb{N}^*$ such that $a^n R \cap b^n R$ is principal [11].

7. A nonzero nonunit $p \in R$ is a *prime block* if for all $a, b \in R$ with $aR \cap pR \neq apR$ and $bR \cap pR \neq bpR$, there exist an $n \in \mathbb{N}^*$ and $d \in R$ such that $(a^n, b^n) \subset dR$ with $(a^n/d)R \cap pR = (a^n/d)pR$ or $(b^n/d)R \cap pR = (b^n/d)pR$. Then R is an *almost unique factorization domain* (AUFD) if every nonzero nonunit of R is expressible as a product of finitely many prime blocks [11, Definition 1.10].

8. R is an *almost weakly factorial domain* if some power of each nonzero nonunit element of R is a product of primary elements [1].

We first give a result for one-dimensional Noetherian integral domains.

Proposition 2.2: *Let R be a one-dimensional Noetherian inside factorial domain with Cale basis $\mathcal{Q}$. Then R is an AGCD and an almost weakly factorial domain.*

Proof: R is obviously an almost weakly factorial domain (see also [1, Theorem 3.9]). Let $a, b \in R \setminus \{0\}$. There exist some $n \in \mathbb{N}^*$ and $s_i, t_i \in \mathbb{N}$ such that $a^n = u \prod_{q_i \in \mathcal{Q}} q_i^{s_i}$, $b^n = v \prod_{q_i \in \mathcal{Q}} q_i^{t_i}$ where $u, v \in \mathcal{U}(R)$. For each i, set $m_i = \sup(s_i, t_i)$, $m'_i = \inf(s_i, t_i)$ and $c = \prod_{q_i \in \mathcal{Q}} q_i^{m_i}$. Then $Rc \subset Ra^n \cap Rb^n$ so that $c = u^{-1}a^n a' = v^{-1}b^n b'$ with $a' = \prod_{q_i \in \mathcal{Q}} q_i^{m_i - s_i}$ and $b' = \prod_{q_i \in \mathcal{Q}} q_i^{m_i - t_i}$. Now, let $x, y \in R \setminus \{0\}$ be such that $xa^n = yb^n$. It follows that $xu \prod_{q_i \in \mathcal{Q}} q_i^{s_i - m'_i} = yv \prod_{q_i \in \mathcal{Q}} q_i^{t_i - m'_i}$ where q_i appears in the product in at most one side and $uxb' = vya'$. Assume $m'_i = s_i \neq t_i$. Since $Rq_i^{t_i - m'_i}$ is a P_i-primary ideal and $q_j \notin P_i$ for each $j \neq i$ by Proposition 2.1, we get that $q_i^{m_i - s_i} = q_i^{t_i - m'_i}$ divides x. Repeating the process for each i such that $t_i > m'_i$, we get that $a' \mid x$ and $xa^n \in Rc$. Then $Rc = Ra^n \cap Rb^n$ and R is an AGCD. □

More precisely, for one-dimensional Noetherian integral domains with torsion class group, we have the following.

Theorem 2.3: *Let R be a one-dimensional Noetherian integral domain with torsion class group and with integral closure $\overline{R}$. The following conditions are equivalent.*

1. *$R \hookrightarrow \overline{R}$ is a root extension.*
2. *R is an API-domain.*
3. *R is an AD-domain.*
4. *R is an AB-domain.*
5. *R is an AP-domain.*
6. *R is an AGCD-domain.*

7. *R is an AUFD.*

8. *R is an inside factorial domain.*

Moreover, if $\overline{R}$ is a finitely generated R-module and R is residually finite, these conditions are equivalent to

9. $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ *is bijective.*

Proof: (1) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) by [3, Corollary 4.8] since $\overline{R}$ is a Prüfer domain.

(1) $\Leftrightarrow$ (8) by [4, Corollary 6].

(6) $\Leftrightarrow$ (7) by [11, Proposition 2.1 and Theorem 2.12].

At last, implications (4) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (5) and (4) $\Rightarrow$ (6) are obvious since R is Noetherian.

(6) $\Rightarrow$ (1) follows from [3, Theorem 3.1] and (1) $\Rightarrow$ (9) is true in any case by [3, Theorem 2.1].

Moreover, if $\overline{R}$ is a finitely generated R-module and R is residually finite, we get (9) $\Rightarrow$ (1). Indeed, it is enough to mimic the proof of [9, Proposition 3] since $R \hookrightarrow \overline{R}$ is factored in finitely many root extensions. $\square$

Remark: In [5, page 178] and [3, page 297], the authors asked about non-integrally closed AGCD domains of finite t-character or of characteristic 0. The previous theorem gives examples of such domains.

3 Structure of Cale bases of algebraic orders

In this section, we consider algebraic orders where Theorem 2.3 reveals as being useful. A generalization to residually finite one-dimensional Noetherian integral domains R with finite class group and with integral closure $\overline{R}$ such that $\overline{R}$ is a finitely generated R-module can be easily made. We use the following notation.

Let R be an order with integral closure $\overline{R}$ and conductor $\mathfrak{f}$. Set $\mathcal{I}(\overline{R})$ (resp. $\mathcal{I}_{\mathfrak{f}}(\overline{R})$, $\mathcal{I}_{\mathfrak{f}}(R)$) the monoid of all nonzero ideals of $\overline{R}$ (resp. the monoid of all nonzero ideals of $\overline{R}$ comaximal to $\mathfrak{f}$, the monoid of all nonzero ideals of R comaximal to $\mathfrak{f}$). In particular, $\mathrm{D}_R(\mathfrak{f}) = (\mathcal{I}_{\mathfrak{f}}(R) \cap \mathrm{Spec}(R)) \cup \{0\}$. Let $\mathcal{P}(\overline{R})$ (resp. $\mathcal{P}_{\mathfrak{f}}(R)$) be the submonoid of all principal ideals belonging to $\mathcal{I}(\overline{R})$ (resp. to $\mathcal{I}_{\mathfrak{f}}(R)$). Then $\mathcal{C}(\overline{R}) = \mathcal{I}(\overline{R})/\mathcal{P}(\overline{R})$ (resp. $\mathcal{C}(R) = \mathcal{I}_{\mathfrak{f}}(R)/\mathcal{P}_{\mathfrak{f}}(R)$) is the class group of $\overline{R}$ (resp. R [9, Proposition 2]) and $\mathcal{C}(R) \to \mathcal{C}(\overline{R})$ is surjective. Both of these groups are finite. Moreover, we have a monoid isomorphism $\varphi : \mathcal{I}_{\mathfrak{f}}(R) \to \mathcal{I}_{\mathfrak{f}}(\overline{R})$ defined by $\varphi(J) = J\overline{R}$ for all $J \in \mathcal{I}_{\mathfrak{f}}(R)$ (see [8, §3]). In particular, any ideal of $\mathcal{I}_{\mathfrak{f}}(R)$, as any ideal of $\mathcal{I}(\overline{R})$, is the product of maximal ideals in a unique way since $\varphi(\mathrm{D}_R(\mathfrak{f})) = \mathrm{D}_{\overline{R}}(\mathfrak{f})$. The image of an ideal J of $\mathcal{I}(\overline{R})$ (resp. $\mathcal{I}_{\mathfrak{f}}(R)$) in $\mathcal{C}(\overline{R})$ (resp. $\mathcal{C}(R)$) is denoted by $[J]$. The exponent of $\mathcal{C}(R)$ is denoted by $e(R)$ and $s(R)$ is the order of the factor group $\mathcal{U}(\overline{R})/\mathcal{U}(R)$.

3.1 Building a Cale basis

Proposition 3.1: *Let $\mathfrak{f}$ be the conductor of an order R where the integral closure is $\overline{R}$.*

1. *Let $P \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}$ and $\alpha = \mathrm{o}([P])$. There exists an irreducible P-primary element $q \in P$ such that $P^\alpha = Rq$.*

2. *Let $P \in \mathrm{V}_R(\mathfrak{f})$ such that there exists a unique $P' \in \mathrm{Spec}(\overline{R})$ lying over P. There exists a P-primary element $q \in P$ such that $P'^n = \overline{R}q$ for some $n \in \mathbb{N}^*$ and such that $P'^{n'} = \overline{R}q'$ with $q' \in R$ implies $n \leq n'$. Such an element q is irreducible in R.*

Proof:
(1) P^α is a principal ideal. Let $q \in R$ be such that $P^\alpha = Rq$ and suppose there exist $x, y \in R$ such that $q = xy$ so that $P^\alpha = (Rx)(Ry)$. Using the monoid isomorphism φ, we get that $Rx = P^\beta$ and $Ry = P^\gamma$ with $\alpha = \beta + \gamma$. But the definition of α implies that x or y is a unit and q is an irreducible element, obviously P-primary.
(2) Set $\alpha = \mathrm{o}([P'])$. There exists $p' \in P'$ such that $P'^\alpha = \overline{R}p'$.

Let $Q \in \mathrm{D}_R(\mathfrak{f})$. Then $R_Q \to \overline{R}_Q$ is an isomorphism, so that $p'/1 \in R_Q$.

Let $P \neq Q \in \mathrm{V}_R(\mathfrak{f})$. Then $p'/1 \in \mathcal{U}(\overline{R}_Q)$. As $|\mathcal{U}(\overline{R}_Q)/\mathcal{U}(R_Q)|$ is finite, there exists $n_Q \in \mathbb{N}^*$ such that $(p'/1)^{n_Q} \in R_Q$.

Lastly, $R_P \hookrightarrow \overline{R}_P$ is a root extension in view of Theorem 2.3 (9). It follows that there exists $n_P \in \mathbb{N}^*$ such that $(p'/1)^{n_P} \in R_P$.

$\mathrm{V}_R(\mathfrak{f})$ being finite, there exists a least $n \in \mathbb{N}^*$ such that $p'^n \in R \cap P' = P$. In case there exists $u \in \mathcal{U}(\overline{R})$ such that $P'^{m\alpha} = \overline{R}p'^m$, with $m < n$ and $up'^m \in R \cap P' = P$, we pick $q \in P$ such that $P'^\beta = \overline{R}q$, where β is the least $k \in \mathbb{N}^*$ such that $P'^k = \overline{R}q'$ with $q' \in R$. Then q is obviously a P-primary element.

Let $x, y \in R$ be such that $q = xy$, which gives $P'^{\beta} = (\overline{R}x)(\overline{R}y)$ so that $\overline{R}x = P'^{\gamma}$ and $\overline{R}y = P'^{\delta}$ with $\beta = \gamma + \delta$. But the definition of β implies that x or y is in $\mathcal{U}(\overline{R}) \cap R = \mathcal{U}(R)$ and q is an irreducible element in R. $\square$

Remark: If we assume that $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ is bijective in Proposition 3.1, $R \hookrightarrow \overline{R}$ is a root extension in view of Theorem 2.3 (1). Then, there exists a least $n \in \mathbb{N}^*$ such that $p'^n \in R \cap P' = P$.

Theorem 3.2: *Let R be an order with conductor $\mathfrak{f}$ and integral closure $\overline{R}$.*

For each $P \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}$, let $\alpha = \mathrm{o}([P])$. Choose $q_P \in P$ such that $P^{\alpha} = Rq_P$. Set $\mathcal{Q}_1 = \{q_P \mid P \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}\}$.

For each $P \in \mathrm{V}_R(\mathfrak{f})$ such that there exists a unique $P' \in \mathrm{Spec}(\overline{R})$ lying over P, choose $q_P \in P$ such that q_P generates a least power of P'. Set $\mathcal{Q}_2 = \{q_P \mid P \in \mathrm{V}_R(\mathfrak{f})$, there exists a unique $P' \in \mathrm{Spec}(\overline{R})$ lying over $P\}$.

To end, set $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$ and let J be the intersection of all $P \in \mathrm{V}_R(\mathfrak{f})$ such that there exists more than one ideal in $\mathrm{Spec}(\overline{R})$ lying over P.

For each $P_i \in \mathrm{V}_R(\mathfrak{f})$ such that there exists a unique $P'_i \in \mathrm{Spec}(\overline{R})$ lying over P_i let n_i be the least $n \in \mathbb{N}^*$ such that P'^n_i is a principal ideal generated by an element of R. Lastly, set $m = \mathrm{lcm}(e(R), n_i)$ and $N = ms(R)$. Then

1. *Up to units of R, x^N is a product of elements of $\mathcal{Q}$ in a unique way, for each $x \in \mathrm{Cop}_R(J)$.*

   In particular, $\mathrm{Cop}_R(J)$ is an inside factorial monoid with Cale basis $\mathcal{Q}$.

2. *In particular, $\mathcal{Q}$ is a Cale basis for R when $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(R)$ is bijective.*

Proof: • Since $\mathrm{V}_R(\mathfrak{f})$ is a finite set, there are finitely many $P_i \in \mathrm{V}_R(\mathfrak{f})$ such that there exists a unique $P'_i \in \mathrm{Spec}(\overline{R})$ lying over P_i.
Set $n_i = \inf\{n \in \mathbb{N}^* \mid P'^n_i$ is a principal ideal generated by an element of $R\}$.
We can set $m = \mathrm{lcm}(e(R), n_i)$ so that $m = e(R)e' = n_i n'_i$ and $e(R) = \alpha_i \alpha'_i$, where $\alpha_i = \mathrm{o}([P_i])$ for each i such that $P_i \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}$.

Let $x \in \mathrm{Cop}_R(J)$. Then $\overline{R}x = \prod P'^{a_i}_i$, $a_i \in \mathbb{N}^*$, $P'_i \in \mathrm{Max}(\overline{R})$. Set $P_i = R \cap P'_i$ and $q_i = q_{P_i}$ for each i.
Then we have $\overline{R}x^m = \displaystyle\prod_{P_i \in \mathrm{V}_R(\mathfrak{f})} P'^{ma_i}_i \prod_{P_i \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}} P'^{ma_i}_i$.

If $P_i \in \mathrm{V}_R(\mathfrak{f})$, we get that $P'^{ma_i}_i = P'^{n_i n'_i a_i}_i = \overline{R}q_i^{a_i n'_i}$, with $q_i \in \mathcal{Q}_2$.

If $P_i \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}$, we get that $P'_i = \overline{R}P_i$ so that $P_i'^{ma_i} = P_i'^{e(R)e'a_i} = \overline{R}P_i^{e(R)e'a_i} = \overline{R}q_i^{a_ie'\alpha'_i}$, with $q_i \in \mathcal{Q}_1$.
This gives finally $\overline{R}x^m = \overline{R} \prod_{P_i \in \mathrm{V}_R(\mathfrak{f})} q_i^{n'_ia_i} \prod_{P_i \in \mathrm{D}_R(\mathfrak{f})\setminus\{0\}} q_i^{e'\alpha'_ia_i}$, so that there exists $u \in \mathcal{U}(\overline{R})$ such that $x^m = u \prod_{q\in\mathcal{Q}} q^{b_q}$, $b_q \in \mathbb{N}$. From $v = u^{s(R)} \in R \cap \mathcal{U}(\overline{R}) = \mathcal{U}(R)$, we deduce $x^{ms(R)} = v \prod_{q\in\mathcal{Q}} q^{s(R)b_q}$. Set $N = ms(R)$ and $t_q = s(R)b_q$ for each $q \in \mathcal{Q}$. Then $x^N = v \prod_{q\in\mathcal{Q}} q^{t_q}$.

• Let us show that x^N has a unique factorization into elements of $\mathcal{Q}$. Let $v, v' \in \mathcal{U}(R),\ t_q, t'_q \in \mathbb{N}$ be such that $x^N = v \prod_{q\in\mathcal{Q}} q^{t_q} = v' \prod_{q\in\mathcal{Q}} q^{t'_q}$. This implies $\prod_{q\in\mathcal{Q}} \overline{R}q^{t_q} = \prod_{q\in\mathcal{Q}} \overline{R}q^{t'_q}$ in $\overline{R}$, with finitely many nonzero t_q and t'_q. Taking into account the uniqueness of the primary decomposition of $\overline{R}x^N$ in $\overline{R}$, we first get $\overline{R}q^{t_q} = \overline{R}q^{t'_q}$, so that $t_q = t'_q$ for each $q \in \mathcal{Q}$, and then $v = v'$.

It follows that $\mathcal{Q}$ is a Cale basis for $\mathrm{Cop}_R(J)$, which is an inside factorial monoid. Part (2) is then a special case of the general case. □

Remark: (1) If there exists a maximal ideal P in R with more than one maximal ideal in $\overline{R}$ lying over P, then $\mathrm{Cop}_R(J)$ is not the largest inside factorial monoid contained in R where the elements of the Cale basis are primary.

Indeed, let q be a P-primary element. The monoid generated by $\mathrm{Cop}_R(J)$ and q is still inside factorial.

(2) Nevertheless, under the previous assumption, we can ask if there exists in R a largest inside factorial monoid of the form $\mathrm{Cop}_R(K)$ where K is an ideal of R and such that the elements of the Cale basis of $\mathrm{Cop}_R(K)$ are irreducible and primary.

Proposition 3.3: *Under notation of Theorem* 3.2*, J is the greatest ideal K of R such that* $\mathrm{Cop}_R(K)$ *is an inside factorial monoid and such that the elements of the Cale basis of* $\mathrm{Cop}_R(K)$ *are primary. Moreover, we get* $\mathrm{Cop}_R(K) \subset \mathrm{Cop}_R(J)$ *for any such an ideal K.*

Proof: Let K be an ideal of R such that $\mathrm{Cop}_R(K)$ is an inside factorial monoid and such that the elements of the Cale basis $\mathcal{Q}'$ of $\mathrm{Cop}_R(K)$ are primary. Assume there exists a P-primary element $q \in \mathcal{Q}'$ with $P \in \mathrm{V}_R(J)$. Let $P_1, \dots, P_n \in \mathrm{Spec}(\overline{R})$ be lying over P with $n > 1$, so that $\mathfrak{f} \subset P$. Let $p_1 \in \overline{R}$ be a P_1-primary element. We first show that there exist some r and $s \in \mathbb{N}^*$ such that $q^r p_1^s$ is a P-primary element of R.

For a maximal ideal $M \in \mathrm{Max}(R)$, we denote by X' the localization of an R-module X at M.

• If $M \in \mathrm{D}_R(\mathfrak{f})$, we get an isomorphism $R' \simeq \overline{R}'$.
Then $p_1/1 \in R'$ and $(q^{r'} p_1^{s'})/1 \in R'$ for any $r', s' \in \mathbb{N}^*$. Moreover, we have $(q^{r'} p_1^{s'})/1 \in \mathcal{U}(R')$.

• If $M \in \mathrm{V}_R(\mathfrak{f})$ and $M \neq P$, then $p_1/1 \in \mathcal{U}(\overline{R}')$ and there exists $s_M \in \mathbb{N}^*$ such that $(p_1^{s_M})/1 \in \mathcal{U}(R')$ since $\mathcal{U}(\overline{R}')/\mathcal{U}(R')$ has a finite order. Because of $\mathrm{V}_R(\mathfrak{f})$ being finite too, there exists $s \in \mathbb{N}^*$ such that $(q^{r'} p_1^s)/1 \in R'$ for any $M \in \mathrm{V}_R(\mathfrak{f}) \setminus \{P\}$ and for any $r' \in \mathbb{N}^*$. Moreover, $(q^{r'} p_1^s)/1 \in \mathcal{U}(R')$.

• If $M = P$, we get that $\mathfrak{f}'$ is a P'-primary ideal and the conductor of R'. There exists $r \in \mathbb{N}^*$ such that $P'^r \subset \mathfrak{f}'$, so that $q^r/1 \in \mathfrak{f}'$. This implies $(q^r p_1^s)/1 \in P' \subset R'$.

To conclude, there exist $r, s \in \mathbb{N}^*$ such that $(q^r p_1^s)/1 \in R_M$ for any $M \in \mathrm{Max}(R)$, which gives $q^r p_1^s \in R$ and is a P-primary element in R by the previous discussion. But $P + K = R$ since $q \in \mathrm{Cop}_R(K)$. It follows that $q^r p_1^s \in \mathrm{Cop}_R(K)$ and there exist $t, x \in \mathbb{N}^*$ such that $(q^r p_1^s)^t = u q^x$ $(*)$, with $u \in \mathcal{U}(R)$. As q is a P-primary element, we get in $\overline{R}$ the two factorizations $\overline{R}q = \prod_{i=1}^{n} P_i^{a_i}$ and $\overline{R}p_1 = P_1^a$, with $a_i, a \in \mathbb{N}^*$. From $(*)$, we get $P_1^{ast}(\prod_{i=1}^{n} P_i^{rta_i}) = \prod_{i=1}^{n} P_i^{xa_i}$, which gives :

- if $i = 1$, then $rta_1 + ast = a_1 x$ (1)
- if $i \neq 1$, then $rta_i = a_i x$ (i)

so that $x = rt$ by (i) and then $ast = 0$ by (1), a contradiction.

Hence, any P-primary element $q \in \mathcal{Q}'$ is such that $P \in \mathrm{D}_R(J)$.

For any $x \in \mathrm{Cop}_R(K)$, let $k \in \mathbb{N}^*$ be such that $x^k = u \prod_{q \in \mathcal{Q}'} q^{b_q}$, so that any maximal ideal $P \in \mathrm{V}_R(x)$ is in $\mathrm{D}_R(J)$. This implies that $x \in \mathrm{Cop}_R(J)$.

We have just shown that $\mathrm{Cop}_R(K) \subset \mathrm{Cop}_R(J)$. To end, any $P \in \mathrm{D}_R(K)$ contains some $q \in \mathrm{Cop}_R(K) \subset \mathrm{Cop}_R(J)$ so that $P \in \mathrm{D}_R(J)$.

Then $\mathrm{V}_R(J) \subset \mathrm{V}_R(K)$ and $K \subset \sqrt{K} \subset \sqrt{J} = J$. □

Recall that an integral domain is weakly factorial if each nonunit is a product of primary elements (D. D. Anderson and L. A. Mahaney [2]). In particular, the class group of a one-dimensional weakly factorial Noetherian domain is trivial [2, Theorem 12]. The following corollary generalizes the quadratic case worked out by A. Faisant [7, Corollaire].

Corollary 3.4: *Let R be a weakly factorial order with conductor $\mathfrak{f}$. Then each $x \in \mathrm{Cop}_R(\mathfrak{f})$ is a product of prime elements of R in a unique way up to units.*

PROOF: We get $|\mathcal{C}(R)| = 1$. Let $x \in \mathrm{Cop}_R(\mathfrak{f})$. Then, $Rx = \prod_{P_i \in \mathrm{D}_R(\mathfrak{f}) \setminus \{0\}} P_i^{a_i}$, where each P_i is a principal ideal generated by a prime element $p_i \in \mathcal{Q}_1$ (notation of Theorem 3.2). It follows that $x = u \prod_{p_i \in \mathcal{Q}_1} p_i^{a_i},\ u \in \mathcal{U}(R)$. □

Corollary 3.5:

1. *Let R be an inside factorial order with integral closure $\overline{R}$. Let $\mathcal{Q}$ be the Cale basis defined in Theorem 3.2. Any overring S of R contained in $\overline{R}$ is inside factorial and $\mathcal{Q}$ is still a Cale basis for S.*

2. *Let R_1 and R_2 be two inside factorial orders with the same integral closure. Then $R = R_1 \cap R_2$ is inside factorial. Moreover, there exists a common Cale basis for R_1 and R_2.*

PROOF: (1) Since $R \hookrightarrow \overline{R}$ is a root extension, so is $S \hookrightarrow \overline{R}$ and S is inside factorial by Theorem 2.3. Moreover, the spectral map $\mathrm{Spec}(\overline{R}) \to \mathrm{Spec}(S)$ is bijective. Then, the construction of $\mathcal{Q}$ in the proof of Theorem 3.2 shows that $\mathcal{Q}$ is also a Cale basis for S.

We may also use [4, Proposition 5].

(2) Set $R = R_1 \cap R_2$. Then R is an order with the same integral closure $\overline{R}$ as R_1 and R_2. Since $R_1 \hookrightarrow \overline{R}$ and $R_2 \hookrightarrow \overline{R}$ are root extensions, so is $R \hookrightarrow \overline{R}$ and R is inside factorial by Theorem 2.3. Part (1) gives that any Cale basis for R is also a Cale basis for R_1 and R_2.

□

Remark: The elements of the Cale basis $\mathcal{Q}$ gotten in Theorem 3.2 are irreducible in R. The following examples show how they behave in the integral closure $\overline{R}$.

(1) Consider the quadratic order $R = \mathbb{Z}[\sqrt{-3}]$ with conductor $\mathfrak{f} = 2\overline{R}$, a maximal ideal in R and $\overline{R}$. Then R is weakly factorial and inside factorial

[10, Corollary 2.2]. Let $\mathcal{Q}$ be the Cale basis of Theorem 3.2. Any element of $\mathcal{Q}$ belonging to $\mathrm{Cop}_R(\mathfrak{f})$ is irreducible in R as well as in $\overline{R}$. By Proposition 3.6 of the next subsection, 2 is the $\mathfrak{f}$-primary element of $\mathcal{Q}$ irreducible in both R and $\overline{R}$. Then $\mathcal{Q}$ is a Cale basis for $\overline{R}$ and its elements are also irreducible in $\overline{R}$.
(2) Consider the quadratic order $R = \mathbb{Z}[2i]$. Its conductor $\mathfrak{f} = 2\overline{R}$ is a maximal ideal in R. But $\mathfrak{f} = \overline{R}(1+i)^2$ where $\overline{R}(1+i)$ is a maximal ideal in $\overline{R}$. Then R is weakly factorial and inside factorial [10, Corollary 2.2]. Let $\mathcal{Q}$ be the Cale basis of Theorem 3.2. Any element of $\mathcal{Q}$ belonging to $\mathrm{Cop}_R(\mathfrak{f})$ is irreducible in R as well as in $\overline{R}$. By Proposition 3.6 of the next subsection, 2 is the $\mathfrak{f}$-primary element of $\mathcal{Q}$, irreducible in R but not in $\overline{R}$ since $2 = -i(1+i)^2$. Then $\mathcal{Q}$ is a Cale basis for $\overline{R}$ and its elements need not be all irreducible in $\overline{R}$.

3.2 The quadratic case

In this subsection we keep notation of Theorem 3.2 for N, $\mathcal{Q}_1$ and $\mathcal{Q}_2$. For a quadratic order, determination of elements of $\mathcal{Q}_2$ and the number N is simple. The characterization of quadratic inside factorial orders is given in [4, Example 3].

Let d be a square-free integer and consider the quadratic number field $K = \mathbb{Q}(\sqrt{d})$. It is well-known that the ring of integers of K is $\mathbb{Z}[\omega]$, where $\omega = \frac{1}{2}(1+\sqrt{d})$ if $d \equiv 1 \pmod 4$ and $\omega = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$. Moreover, $\mathbb{Z}[\omega]$ is a free $\mathbb{Z}$-module with basis $\{1, \omega\}$. A quadratic order in K is a subring R of $\mathbb{Z}[\omega]$ which is a free $\mathbb{Z}$-module of rank 2 with basis $\{1, n\omega\}$ where $n \in \mathbb{N}^*$. Then $\mathbb{Z}[\omega]$ is the integral closure $\overline{R}$ of $R = \mathbb{Z}[n\omega]$ and $n\mathbb{Z}[\omega]$ is the conductor of R. We denote by $\mathrm{N}(x)$ the norm of an element $x \in \mathbb{Z}[\omega]$.

Proposition 3.6: *Let $R = \mathbb{Z}[n\omega]$ be a quadratic order with conductor $\mathfrak{f} = n\mathbb{Z}[\omega]$, $n \in \mathbb{N}^*$. Then $\mathcal{Q}_2$ is the set of ramified and inert primes dividing n.*

In particular, $\mathbb{Z}[n\omega] \hookrightarrow \mathbb{Z}[\omega]$ is a root extension if and only if no decomposed prime divides n.

Proof: Let $P \in \mathrm{Max}(R)$, with $p\mathbb{Z} = \mathbb{Z} \cap P$. There is only one maximal ideal lying over P in $\overline{R}$ if p is ramified or inert. By [12, Proposition 12], we have $P = p\mathbb{Z} + n\omega\mathbb{Z}$ when $p|n$.
- If p is inert, then $\overline{R}p \in \mathrm{Max}(\overline{R})$, so that p is irreducible in $\overline{R}$ and in R.
- If p is ramified, then $\overline{R}p = P'^2$, where $P' \in \mathrm{Max}(\overline{R})$.
  - If P' is not a principal ideal, then p is irreducible in $\overline{R}$ and in R.

- Let $P' = \overline{R}p'$, $p' \in \overline{R}$. Then $p = up'^2$ with $u \in \mathcal{U}(\overline{R})$. Indeed, p is still irreducible in R. Deny and let $x, y \in R$ be nonunits such that $p = xy$. It follows that $\mathrm{N}(p) = p^2 = \mathrm{N}(x)\mathrm{N}(y)$ which gives $\mathrm{N}(x) = \mathrm{N}(y) = \pm p$. But $x \in R$ can be written $x = a + bn\omega$, $a, b \in \mathbb{Z}$.

If $d \equiv 2, 3 \pmod 4$, we get $\mathrm{N}(x) = a^2 - n^2b^2d$, with $p|n$ and $p|\mathrm{N}(x)$. Then $p|a$, $p^2|a^2$, $p^2|n^2$ so that $p^2|\mathrm{N}(x)$, a contradiction.

If $d \equiv 1 \pmod 4$, we get $d = 1 + 4k$, $k \in \mathbb{Z}$. It follows that $\mathrm{N}(x) = a^2 + abn - n^2b^2k$. The same argument leads to a contradiction. $\square$

Corollary 3.7: *Let $R = \mathbb{Z}[n\omega]$ be a quadratic order, $n \in \mathbb{N}^*$, with conductor $\mathfrak{f} = n\mathbb{Z}[\omega]$. The integer N is*

1. *$N = 2e(R)s(R)$ if $e(R)$ is odd and if a ramified prime divides n*

2. *$N = e(R)s(R)$ if $e(R)$ is even or if no ramified prime divides n.*

Remark: We can ask whether the integer N gotten in Theorem 3.2 or in Corollary 3.7 is the least integer n such that x^n is a product of elements of $\mathcal{Q}$ in a unique way, for any nonzero nonunit x of an inside factorial order. We can answer in the quadratic case by an example.

Example: Consider $R = \mathbb{Z}[3i]$. Its integral closure is the PID $\overline{R} = \mathbb{Z}[i]$ and its conductor is $\mathfrak{f} = 3\overline{R} \in \mathrm{Max}(R)$ since 3 is inert.

As $|\mathcal{U}(\overline{R})/\mathcal{U}(R)| = 2$, we get $|\mathcal{C}(R)| = 2$ by the class number formula $|\mathcal{C}(R)| = |\mathcal{C}(\overline{R})||\mathcal{U}(\overline{R})/\mathcal{U}(R)|^{-1}(1+3)$ (see [6, Chapter 9.6]), so that $N = 4$. Moreover, $2 = -i(1+i)^2$ is ramified in $\overline{R}$ and $P = R \cap (1+i)\overline{R} = 2\mathbb{Z} + 3(1+i)\mathbb{Z}$ is a nonprincipal maximal ideal in R such that $P^2 = 2R$, with 2 and 3 irreducible in R. We get $2 \in \mathcal{Q}_1$ and $3 \in \mathcal{Q}_2$. Let $t = 3(1+i) \in R$. The only maximal ideals of R containing t are $\mathfrak{f}$ and P. Now $t^2 = 3^2(2i)$, $t^3 = 3^3 \cdot 2(-1+i)$ and $t^4 = -3^4 \cdot 2^2$. Then t^4 is the least power which has, up to units of R, a unique factorization into elements of $\mathcal{Q}$. It follows that $N = e(R)s(R)$ is the least integer n such that x^n is a product of elements of $\mathcal{Q}$ in a unique way, for any nonzero nonunit x of R.

References

[1] D. D. Anderson, K. R. Knopp, and R. L. Lewin. Almost Bézout domains II. *J. Algebra*, 167:547–556, 1994.

[2] D. D. Anderson and L. A. Mahaney. On primary factorizations. *J. Pure Appl. Algebra*, 54:141–154, 1988.

[3] D. D. Anderson and M. Zafrullah. Almost Bézout domains. *J. Algebra*, 142:285–309, 1991.

[4] S.T. Chapman, F. Halter-Koch, and U. Krause. Inside factorial monoids and integral domains. *J. Algebra*, 252:350–375, 2002.

[5] T. Dumitrescu, Y. Lequain, J. L. Mott, and M. Zafrullah. Almost GCD domains of finite t-character. *J. Algebra*, 245:161–181, 2001.

[6] H. M. Edwards. *Fermat's last Theorem*. Springer GTM, Berlin, 1977.

[7] A. Faisant. Interprétation factorielle du nombre de classes dans les ordres des corps quadratiques. *Ann. Math. Blaise Pascal*, 7 (2):13–18, 2000.

[8] A. Geroldinger, F. Halter-Koch, and J. Kaczorowski. Non-unique factorizations in orders of global fields. *J. Reine Angew. Math.*, 459:89–118, 1995.

[9] M. Picavet-L'Hermitte. Factorization in some orders with a PID as integral closure. In F. Halter-Koch and R. Tichy, editors, *Algebraic Number Theory and Diophantine Analysis*, pages 365–390. de Gruyter, Berlin-NewYork, 2000.

[10] M. Picavet-L'Hermitte. Weakly factorial quadratic orders. *Arab. J. Sci. and Engineering*, 26:171–186, 2001.

[11] M. Zafrullah. A general theory of almost factoriality. *Manuscripta Math.*, 51:29–62, 1985.

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

Cale bases in algebraic orders

Martine Picavet-L'Hermitte
Université Blaise Pascal
Laboratoire de Mathématiques
Pures
Les Cézeaux
63177 AUBIERE CEDEX
FRANCE
Martine.Picavet@math.univ-bpclermont.fr