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 \( Q \) (called a Cale basis) of primary irreducible elements of \( R \) such that \( x^N \) has a unique factorization into elements of \( Q \) 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 \( \text{Spec}(\overline{R}) \to \text{Spec}(R) \) 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 \( f \) 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 \( Rx + f = R \) 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 \( \text{Spec}(\overline{R}) \to \text{Spec}(R) \) 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 \( \text{Spec}(\overline{R}) \to \text{Spec}(R) \) is bijective and exhibit a Cale basis \( Q \) for such an order. The elements of
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 $Q$ 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 $Q$ 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 $V_R(I)$ the set of all prime ideals in $R$ containing $I$ and by $D_R(I)$ its complement in $\text{Spec}(R)$. If $R$ is an integral domain, $U(R)$ 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 $\text{Cop}_R(J)$ 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, $o(x)$ is its order. As usual, $\mathbb{N}^*$ is the set of nonzero natural numbers.

## 2 Almost divisibility


**Definition:** Let $R$ be a multiplicative, commutative and cancellative monoid. A subset of nonunit elements $Q$ 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 $a^n = u \prod_{q_i \in Q} q_i^{t_i}$ where $u \in U(R)$ and only finitely many of the $t_i$’s are nonzero.

118
Cale bases in algebraic orders

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

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 \( Q \). Any element of \( Q \) is a primary element and there is a bijective map

\[
\begin{cases}
Q \to \text{Max}(R) \\
q \mapsto \sqrt{Rq}
\end{cases}
\]

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

Let \( P \in \text{Max}(R) \) and \( q, q' \in Q \) 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 \( x^k = u \prod_{q_i \in Q} q_i^{t_i} \) where \( u \in \mathcal{U}(R) \). This gives \( q^{nk} = uq'^k \prod_{q_i \in Q} q_i^{t_i} \) and \( q = q' \) since \( Q \) is a Cale basis.

Let \( P \in \text{Max}(R) \) and \( x \) be a nonzero element of \( P \). There exist some \( n \in \mathbb{N}^* \) and \( t_i \in \mathbb{N} \) such that \( x^n = u \prod_{q_i \in Q} q_i^{t_i} \) where \( u \in \mathcal{U}(R) \). Then \( Rx^n = \prod_{q_i \in Q} Rq_i^{t_i} \) 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. 

\[ \square \]
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 $a^nR \cap b^nR$ 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 $Q$. 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 $a^n = u \prod_{q_i \in Q} q_i^{s_i}$, $b^n = v \prod_{q_i \in Q} q_i^{t_i}$ where $u, v \in U(R)$. For each $i$, set $m_i = \sup(s_i, t_i)$, $m'_i = \inf(s_i, t_i)$ and $c = \prod_{q_i \in Q} q_i^{m_i}$. Then $Rc \subset Ra^n \cap Rb^n$ so that $c = u^{-1}a^n a' = v^{-1}b^n b'$ with $a' = \prod_{q_i \in Q} q_i^{m_i-s_i}$ and $b' = \prod_{q_i \in Q} q_i^{m_i-t_i}$. Now, let $x, y \in R \setminus \{0\}$ be such that $xa^n = yb^n$. It follows that $xu \prod_{q_i \in Q} q_i^{s_i-m'_i} = yv \prod_{q_i \in Q} q_i^{t_i-m'_i}$ 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. Spec($\overline{R}$) $\rightarrow$ Spec($R$) is bijective.

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

(6) $\iff$ (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. \qed

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 $I(\overline{R})$ (resp. $I_1(\overline{R})$, $I_2(\overline{R})$) 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, $D_R(\mathfrak{f}) = (I_2(\overline{R}) \cap \text{Spec}(R)) \cup \{0\}$. Let $P(\overline{R})$ (resp. $P_1(\overline{R})$, $P_2(\overline{R})$) be the submonoid of all principal ideals belonging to $I(\overline{R})$ (resp. to $I_1(\overline{R})$, $I_2(\overline{R})$). Then $C(\overline{R}) = I(\overline{R})/P(\overline{R})$ (resp. $C(R) = I_1(\overline{R})/P_1(\overline{R})$) is the class group of $\overline{R}$ (resp. $R$ [9, Proposition 2]) and $C(R) \rightarrow C(\overline{R})$ is
surjective. Both of these groups are finite. Moreover, we have a monoid isomorphism $\varphi : \mathcal{I}_1(R) \to \mathcal{I}_1(\overline{R})$ defined by $\varphi(J) = J\overline{R}$ for all $J \in \mathcal{I}_1(R)$ (see [8, §3]). In particular, any ideal of $\mathcal{I}_1(R)$, as any ideal of $\mathcal{I}(\overline{R})$, is the product of maximal ideals in a unique way since $\varphi(D_R(f)) = D_{\overline{R}}(f)$. The image of an ideal $J$ of $\mathcal{I}(\overline{R})$ (resp. $\mathcal{I}_1(R)$) 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 $f$ be the conductor of an order $R$ where the integral closure is $\overline{R}$.

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

2. Let $P \in V_R(f)$ such that there exists a unique $P' \in \text{Spec}(\overline{R})$ 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) $P^\alpha$ 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 $\varphi$, we get that $Rx = P^\beta$ and $Ry = P^\gamma$ with $\alpha = \beta + \gamma$. But the definition of $\alpha$ implies that $x$ or $y$ is a unit and $q$ is an irreducible element, obviously $P$-primary.

(2) Set $\alpha = o([P'])$. There exists $p' \in P'$ such that $P'^\alpha = \overline{R}p'$.

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

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

   $V_R(f)$ 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 $P^{\alpha u} = \overline{R}p^m$, with $m < n$ and $u p^m \in R \cap P' = P$, we pick $q \in P$ such that $P^\beta = \overline{R}q$, where $\beta$ is the least $k \in \mathbb{N}^*$ such that $P^{\beta k} = \overline{R}q'$ with $q' \in R$. Then $q$ is obviously a $P$-primary element.
Let \( x, y \in R \) be such that \( q = xy \), which gives \( P^{\beta} = (\overline{Rx})(\overline{Ry}) \) so that \( \overline{Rx} = P^{\gamma} \) and \( \overline{Ry} = P^{\delta} \) with \( \beta = \gamma + \delta \). But the definition of \( \beta \) 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 \( \text{Spec}(\overline{R}) \rightarrow \text{Spec}(R) \) is bijective in Proposition 3.1, \( R \leftrightarrow \overline{R} \) 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 \( P \in D_R(\mathfrak{f}) \setminus \{0\} \), let \( \alpha = o([P]) \). Choose \( q_P \in P \) such that \( P^\alpha = Rq_P \). Set \( \mathcal{Q}_1 = \{q_P \mid P \in D_R(\mathfrak{f}) \setminus \{0\} \} \).

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

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

For each \( P_i \in V_R(\mathfrak{f}) \) such that there exists a unique \( P_i' \in \text{Spec}(\overline{R}) \) lying over \( P_i \), let \( n_i \) be the least \( n \in \mathbb{N}^* \) such that \( P_i'^n \) is a principal ideal generated by an element of \( R \). Lastly, set \( m = \text{lcm}(e(R), n_i) \) 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 \( x \in \text{Copr}_R(J) \).

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

2. In particular, \( \mathcal{Q} \) is a Cale basis for \( R \) when \( \text{Spec}(\overline{R}) \rightarrow \text{Spec}(R) \) is bijective.

**Proof:** • Since \( V_R(\mathfrak{f}) \) is a finite set, there are finitely many \( P_i \in V_R(\mathfrak{f}) \) such that there exists a unique \( P_i' \in \text{Spec}(\overline{R}) \) lying over \( P_i \).

Set \( n_i = \inf\{n \in \mathbb{N}^* \mid P_i'^n \text{ is a principal ideal generated by an element of } R\} \).

We can set \( m = \text{lcm}(e(R), n_i) \) so that \( m = e(R)e' = n_i n_i' \) and \( e(R) = \alpha_i \alpha_i' \), where \( \alpha_i = o([P_i]) \) for each \( i \) such that \( P_i \in D_R(\mathfrak{f}) \setminus \{0\} \).

Let \( x \in \text{Copr}_R(J) \). Then \( \overline{Rx} = \prod P_i'^{a_i}, \ a_i \in \mathbb{N}^*, \ P_i' \in \text{Max}(\overline{R}) \). Set \( P_i = R \cap P_i' \) and \( q_i = q_{P_i} \) for each \( i \).

Then we have \( \overline{Rx}^m = \prod_{P_i \in V_R(\mathfrak{f})} P_i'^{na_i} \prod_{P_i \in D_R(\mathfrak{f}) \setminus \{0\}} P_i'^{ma_i} \).

If \( P_i \in V_R(\mathfrak{f}) \), we get that \( P_i'^{ma_i} = P_i'^{na_i'a_i} = \overline{Rq_i^{a_i n_i'}} \), with \( q_i \in \mathcal{Q}_2 \).
If \( P_i \in D_R(f) \setminus \{0\} \), we get that \( P_i' = \overline{RP}_i \) so that \( P_i^{m_{a_i}} = P_i^{e(R)'a_i} = \overline{RP}_i^{e(R)'a_i} = \overline{Rq_i^a e^{a_i}} \), with \( q_i \in \mathbb{Q}_1 \).

This gives finally \( Rx^m = R \prod_{P_i \in V_R(f)} q_i^{n_i a_i} \prod_{P_i \in D_R(f) \setminus \{0\}} q_i^{e(R)'a_i} \), so that there exists \( u \in U(\overline{R}) \) such that \( x^m = u \prod_{q \in \mathbb{Q}} q^b_q \), \( b_q \in \mathbb{N} \). From \( v = u^{s(R)} \in R \cap U(\overline{R}) = \mathcal{U}(R) \), we deduce \( x^{ms(R)} = v \prod_{q \in \mathbb{Q}} q^{s(R)b_q} \). Set \( N = ms(R) \) and \( t_q = s(R)b_q \) for each \( q \in \mathbb{Q} \). Then \( x^N = v \prod_{q \in \mathbb{Q}} q^{t_q} \).

• Let us show that \( x^N \) has a unique factorization into elements of \( \mathbb{Q} \). Let \( v, v' \in U(R) \), \( t_q, t'_q \in \mathbb{N} \) be such that \( x^N = v \prod_{q \in \mathbb{Q}} q^{t_q} = v' \prod_{q \in \mathbb{Q}} q^{t'_q} \). This implies

\[
\prod_{q \in \mathbb{Q}} \overline{Rq}^{t_q} = \prod_{q \in \mathbb{Q}} \overline{Rq}^{t_q'} \quad \text{in} \quad \overline{R},
\]

with finitely many nonzero \( t_q \) and \( t'_q \). Taking into account the uniqueness of the primary decomposition of \( \overline{Rx}^N \) in \( \overline{R} \), we first get \( \overline{Rq}^{t_q} = \overline{Rq}^{t_q'} \), so that \( t_q = t'_q \) for each \( q \in \mathbb{Q} \), and then \( v = v' \).

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

\[\square\]

Remark: (1) If there exists a maximal ideal \( P \) in \( R \) with more than one maximal ideal in \( \overline{R} \) lying over \( P \), then \( \text{Cop}_R(J) \) 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 \( \text{Cop}_R(J) \) 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 \( \text{Cop}_R(K) \) where \( K \) is an ideal of \( R \) and such that the elements of the Cale basis of \( \text{Cop}_R(K) \) are irreducible and primary.

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

**Proof:** Let \( K \) be an ideal of \( R \) such that \( \text{Cop}_R(K) \) is an inside factorial monoid and such that the elements of the Cale basis \( \mathbb{Q}' \) of \( \text{Cop}_R(K) \) are
primary. Assume there exists a $P$-primary element $q \in \mathcal{Q}'$ with $P \in V_R(J)$. Let $P_1, \ldots, P_n \in \text{Spec}(R)$ 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 $(q^r p_1^s)\ast$ is a $P$-primary element of $R$.

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

- If $M \in D_R(f)$, 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 $M \in V_R(f)$ 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 $V_R(f)$ being finite too, there exists $s \in \mathbb{N}^*$ such that $(q^r p_1^s)/1 \in R'$ for any $M \in V_R(f) \setminus \{P\}$ 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 $M \in \text{Max}(R)$, 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 $q \in \text{Cop}_R(K)$. It follows that $q^r p_1^s \in \text{Cop}_R(K)$ and there exist $t, x \in \mathbb{N}^*$ such that $(q^r p_1^s)^t = uq^x$ (**), 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

\[
P_1^{ast}(\prod_{i=1}^n P_i^{rt_{a_i}}) = \prod_{i=1}^n P_i^{x_{a_i}},
\]

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

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

Then $V_R(J) \subset V_R(K)$ and $K \subset \sqrt{K} \subset \sqrt{J} = J$. \qed

Recall that an integral domain is weakly factorial if each nonunit is a
Cale bases in algebraic orders

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 $x \in \text{Cop}_R(\mathfrak{f})$ is a product of prime elements of $R$ in a unique way up to units.

**Proof:** We get $|\mathcal{C}(R)| = 1$. Let $x \in \text{Cop}_R(\mathfrak{f})$. Then, $Rx = \prod_{P_i \in D_R(\mathfrak{f}) \setminus \{0\}} P_i^{a_i}$, 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 $\text{Spec}(\overline{R}) \rightarrow \text{Spec}(S)$ 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

127
Let $Q$ be the Cale basis of Theorem 3.2. Any element of $Q$ belonging to $\text{Cop}_R(f)$ is irreducible in $R$ as well as in $\overline{R}$. By Proposition 3.6 of the next subsection, 2 is the $f$-primary element of $Q$, irreducible in both $R$ and $\overline{R}$. Then $Q$ 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 $f = 2\overline{R}$ is a maximal ideal in $R$. But $\overline{f} = \overline{R}(1 + i)^2$ 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 $Q$ be the Cale basis of Theorem 3.2. Any element of $Q$ belonging to $\text{Cop}_R(f)$ is irreducible in $R$ as well as in $\overline{R}$. By Proposition 3.6 of the next subsection, 2 is the $f$-primary element of $Q$, irreducible in $R$ but not in $\overline{R}$ since $2 = -i(1 + i)^2$. Then $Q$ is a Cale basis for $\overline{R}$ and its elements need not all be irreducible in $\overline{R}$.

3.2 The quadratic case

In this subsection we keep notation of Theorem 3.2 for $N$, $Q_1$ and $Q_2$. For a quadratic order, determination of elements of $Q_2$ 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 $N(x)$ 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 $f = n\mathbb{Z}[\omega]$, $n \in \mathbb{N}^*$. Then $Q_2$ 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 $P \in \text{Max}(R)$, 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 $\overline{R}p \in \text{Max}(\overline{R})$, so that $p$ is irreducible in $\overline{R}$ and in $R$.
- If $p$ is ramified, then $\overline{R}p = P'\mathbb{Z}$, where $P' \in \text{Max}(\overline{R})$.

- If $P'$ is not a principal ideal, then $p$ is irreducible in $\overline{R}$ and in $R$. 128
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 \( x, y \in \mathcal{R} \) be nonunits such that \( p = xy \). It follows that \( N(p) = p^2 = N(x)N(y) \) which gives \( N(x) = N(y) = \pm p \). But \( x \in \mathcal{R} \) can be written \( x = a + b\omega, a, b \in \mathbb{Z} \).

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

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

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

1. \( N = 2e(\mathcal{R})s(\mathcal{R}) \) if \( e(\mathcal{R}) \) is odd and if a ramified prime divides \( n \)
2. \( N = e(\mathcal{R})s(\mathcal{R}) \) if \( e(\mathcal{R}) \) 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 \( \mathcal{R} = \mathbb{Z}[3i] \). Its integral closure is the PID \( \overline{\mathcal{R}} = \mathbb{Z}[i] \) and its conductor is \( f = 3\mathbb{Z}[i] \) since 3 is inert.

As \( |\mathcal{U}(\overline{\mathcal{R}})/\mathcal{U}(\mathcal{R})| = 2 \), we get \( |\mathcal{C}(\mathcal{R})| = 2 \) by the class number formula \( |\mathcal{C}(\mathcal{R})| = |\mathcal{C}(\overline{\mathcal{R}})||\mathcal{U}(\overline{\mathcal{R}})/\mathcal{U}(\mathcal{R})|^{-1}(1 + 3) \) (see [6, Chapter 9.6]), so that \( N = 4 \). Moreover, \( 2 = -i(1+i)^2 \) is ramified in \( \overline{\mathcal{R}} \) and \( P = \mathcal{R} \cap (1+i)\overline{\mathcal{R}} = 2\mathbb{Z} + 3(1+i)\mathbb{Z} \) is a nonprincipal maximal ideal in \( \mathcal{R} \) such that \( p^2 = 2\mathcal{R} \), with 2 and 3 irreducible in \( \mathcal{R} \). We get \( 2 \in \mathcal{Q}_1 \) and \( 3 \in \mathcal{Q}_2 \). Let \( t = 3(1+i) \in \mathcal{R} \). The only maximal ideals of \( \mathcal{R} \) containing \( t \) are \( f \) 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 \( N = e(\mathcal{R})s(\mathcal{R}) \) 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 \( \mathcal{R} \).

**References**


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