WEAKLY FACTORIAL QUADRATIC ORDERS

Martine Picavet-L'Hermitte*

Laboratoire de Mathématiques Pures
Université Blaise Pascal-Clermont 2
63177 Aubière Cedex, France
E-mail: Martine.Picavet@math.univ-bpclermont.fr

الخلاصة :

داخل حلقة ضعيفة التعميل، كل عنصر (غير وحدة) هو حصيلة ضرب لعناصر ابتدائية. نقوم بوَصف الرُتب ضعيفة التعميل عن طريق زمرة الوحدات. لتَكن R رُتبةً مربعة ضعيفة التعميل. نبرهن أن الوحدة الجوهرية للإقفال الصحيح لِ R تحدد شكل الذرّات داخل R، مما يسمح بحساب دالاّت التعميل على R. ليكن x في R عنصراً غير وحدة وغير الصفر، نرمُز بِ $l(x)$ و $L(x)$ بالتوالي إلى inf و sup لأطوال تعاميل x كحصيلة ضرب لعناصر غير قابلة للاختزال. نعطي صيغاً مكشوفة لِ $l(x)$ و $L(x)$، نستنتج منها السلوك المقاربي لهذه الدالات وكذا مرونة الحلقة R.

ABSTRACT

In a weakly factorial domain, every nonunit element is a product of primary elements. Weakly factorial orders are characterized by means of their group of units. If R is a weakly factorial quadratic order, the fundamental unit of the integral closure of R determines the form of atoms of R, thereby allowing to compute the following factorization functions on R. We denote respectively by $l(x)$ and $L(x)$ the inf and sup of the lengths of factorizations of a nonzero nonunit $x \in R$ into a product of irreducible elements. Explicit formulas for $l(x)$ and $L(x)$ are given, from which the asymptotic behavior of these functions and the elasticity of R are deduced.

CLASSIFICATION (AMS) 13A05, 11R04, 13F15.

*Address for correspondence:
8 Rue du Forez
63670 Le Cendre
France

WEAKLY FACTORIAL QUADRATIC ORDERS

1. GENERAL RESULTS ON WEAKLY FACTORIAL ORDERS

Factorization in an algebraic order R is quite simple to study when R is a PID. For an arbitrary order R such that every atom is primary the situation is not too far from unique factorization. Then R is called a weakly factorial domain. In this paper, we characterize and study factorization in weakly factorial quadratic orders. We begin with recalling some basic definition and results.

Let R be an integral domain.

(1) R is called **atomic** if each nonzero nonunit is a finite product of irreducible elements (or **atoms**).

(2) R is called a **weakly factorial domain** if each nonunit of R is a product of primary elements (D.D. Anderson and L.A. Mahaney [3]).

(3) R is said to be a **half-factorial domain (HFD)** if R is atomic and whenever $x_1 \cdots x_m = y_1 \cdots y_n$ with $x_i, y_j \in R$ atoms, then $m = n$ (Zaks [15]).

(4) If R is an atomic domain which is not a field, Valenza defined the **elasticity** of R by

$$\rho(R) = \sup\{m/n \mid x_1 \cdots x_m = y_1 \cdots y_n \quad \text{for} \quad x_i, y_j \in R \text{ atoms}\} \text{ [13]}.$$

Moreover, $\rho(R)$ is said to be **realized by a factorization** if there are atoms $x_i, y_j \in R$ with $x_1 \cdots x_m = y_1 \cdots y_n$ and $\rho(R) = m/n$. In particular, the elasticity of an HFD is 1.

Let x be a nonzero nonunit in an atomic domain R. Define as D.F. Anderson and P. Pruis [4] did:

$$l_R(x) = \inf\{n \mid x = x_1 \cdots x_n,\ x_i \in R \text{ irreducible}\},$$

$$L_R(x) = \sup\{n \mid x = x_1 \cdots x_n,\ x_i \in R \text{ irreducible}\},$$

$$\bar{l}_R(x) = \lim_{n\to\infty} l_R(x^n)/n,\ \bar{L}_R(x) = \lim_{n\to\infty} L_R(x^n)/n.$$

In this work, we use the following notation.

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 $\mathcal{O}_K = \mathbb{Z}[\omega]$, 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 $\{1, \omega\}$.

Let χ be the (quadratic) character of K. Three types of decomposition of a prime integer p in $\mathbb{Z}[\omega]$ can occur.

- There exists a maximal ideal P in $\mathbb{Z}[\omega]$ such that $p\mathbb{Z}[\omega] = P^2$ (p is **ramified**) and $\chi(p) = 0$.
- There exist two maximal ideals P_1, P_2 in $\mathbb{Z}[\omega]$ such that $p\mathbb{Z}[\omega] = P_1 \cap P_2$ (p is **decomposed**) and $\chi(p) = 1$.
- The ideal $p\mathbb{Z}[\omega]$ is a maximal ideal in $\mathbb{Z}[\omega]$ (p is **inert**) and $\chi(p) = -1$.

For a real quadratic number field K, there is a unique unit $\varepsilon > 1$ in $\mathcal{O}_K$ such that the group of units of $\mathcal{O}_K$ is $\{\pm 1\} \times <\varepsilon>$ and ε is called the **canonical fundamental unit**.

A quadratic order in K is a subring R of $\mathcal{O}_K$, which is a free $\mathbb{Z}$-module of rank 2 with basis $\{1, n\omega\}$ where $n \in \mathbb{N}^*$. Then $\mathcal{O}_K$ is the integral closure of $R = \mathbb{Z}[n\omega]$ and $n\mathcal{O}_K$ is the conductor of R.

For a finite set S, we denote by $|S|$ the number of elements of S. For $x \in \mathbb{R}$, we set $[x] = \sup\{n \in \mathbb{Z} \mid n \leq x\}$. For an integral domain R, we denote by $\bar{R}$ its integral closure and by $\mathcal{U}(R)$ its group of units.

Section 2 is devoted to the characterization of weakly factorial quadratic orders, with emphasis on real orders, with respect to the fundamental unit. Let $R = \mathbb{Z}[n\omega]$ be a real quadratic order such that its integral closure $\bar{R}$ is a PID. Let I be the conductor of R and ε the fundamental unit of $\mathbb{Z}[\omega]$. Then R is weakly factorial if and only if $|\mathcal{U}(\bar{R})/\mathcal{U}(R)| = |\mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)| = \inf\{k \in \mathbb{N}^* \mid n \text{ divides } b_k\}$ where $\varepsilon^k = a_k + b_k\omega$, $a_k, b_k \in \mathbb{Z}$. An evaluation of this number is obtained thanks to the class number formula. In particular, we can build infinite decreasing sequences of weakly factorial orders.

In Section 3, we obtain all nonassociate atoms of a weakly factorial quadratic order. This allows us to study the length functions l and L and their asymptotic behavior.

Another interesting property of weakly factorial orders is the computation of the elasticity of such orders. This is done in Section 4. Let $R = \mathbb{Z}[n\omega]$ be a weakly factorial quadratic order with $n = \prod p_i^{e_i}$, p_i prime integers. If some p_i is decomposed, $\rho(R) = \infty$. If not, we have $\rho(R) = \sup(\{e_i + 1/2 \mid p_i \text{ ramified}\}, \{e_i \mid p_i \text{ inert}\})$.

Before studying the quadratic case, here are properties available in a general context.

First, recall a result of D.D. Anderson and L.A. Mahaney

Theorem 1.1. [3, Theorem 12] *Let R be a one-dimensional Noetherian domain. The following statements are equivalent:*

1. *R is weakly factorial.*
2. *Every atom is primary.*
3. $\mathrm{Pic}(R) = 0$.

If these conditions hold, the integral closure of R is a PID.

Moreover, the following theorem gives a characterization of weakly factorial orders.

Theorem 1.2. *Let R be an algebraic order such that its integral closure $\bar{R}$ is a PID and let I be the conductor of R. Then R is weakly factorial if and only if $|\mathcal{U}(\bar{R})/\mathcal{U}(R)| = |\mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)|$.*

Proof. By [12, Theorem 2] R is weakly factorial if and only if $\mathcal{U}(\bar{R})/\mathcal{U}(R) \to \mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)$ is an isomorphism. When proving this theorem, we showed that $\mathcal{U}(\bar{R})/\mathcal{U}(R) \to \mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)$ is always an injective group morphism. So $|\mathcal{U}(\bar{R})/\mathcal{U}(R)|$ divides $|\mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)|$, since this last number is finite, and hence the equality is equivalent to R being weakly factorial. □

The following result of F. Halter-Koch allows to work in local orders.

Theorem 1.3. [9, Corollary 1.7] *Let H be a weakly factorial monoid. Then every $a \in H \setminus H^\times$ is a product of (finitely many) mutually not related primary elements, and this representation is unique up to the order of the factors and up to associates.*

In fact, a weakly factorial domain is a weakly factorial monoid for the multiplicative structure.

Proposition 1.4. *Let R be a weakly factorial order and $x \in R$ be a nonzero nonunit element.*

1. *For each $P \in \mathrm{Max}(R)$, there is a bijection between the set of P-primary atoms of R and the set of atoms of R_P (up to units).*

2. *If* $x = \prod_{i=1}^{r}(\prod_{j=1}^{r_i} x_{i,j})$ *is a factorization into atoms in* R, *with* $x_{i,j}$ *a* P_i*-primary atom for each* j, *there exists* $u_i \in \mathcal{U}(R_{P_i})$ *such that* $x/1 = u_i \prod_{j=1}^{r_i} x_{i,j}/1$ *is a factorization into atoms in* R_{P_i} *for each* i.

3. *If* $x/1 = u_i \prod_{j=1}^{r_i} x_{i,j}/1$, $u_i \in \mathcal{U}(R_{P_i})$, *is a factorization into atoms in* R_{P_i} *for each* $P_i \in \mathrm{Max}(R)$ *such that* $x \in P_i$, *with* $x_{i,j}$ *a* P_i*-primary atom for each* j, *there exists* $u \in \mathcal{U}(R)$ *such that* $x = u \prod_{i=1}^{r}(\prod_{j=1}^{r_i} x_{i,j})$ *is a factorization into atoms in* R.

4. $l_R(x) = \sum_{P \in \mathrm{Max}(R)} l_{R_P}(x/1)$, $L_R(x) = \sum_{P \in \mathrm{Max}(R)} L_{R_P}(x/1)$.

Proof. Thanks to Theorem 1.3, there is a monoid homomorphism $\varphi : R \setminus \{0\} \to \coprod_{P \in \mathrm{Max}(R)}(R_P \setminus \{0\})/\mathcal{U}(R_P)$ defined by $\varphi(x) = (\varphi_P((x/1)_P))_{P \in \mathrm{Max}(R)}$, where $\varphi_P : R_P \setminus \{0\} \to (R_P \setminus \{0\})/\mathcal{U}(R_P)$ is the canonical map. In particular, if $z = (\varphi_P((x_P/1)_P))_{P \in \mathrm{Max}(R)}$, where $x_P = 1$ for all but finitely many $x_{P_1}, \ldots, x_{P_n}$ such that x_{P_i} is a P_i-primary element, then $z = \varphi(x_{P_1} \cdots x_{P_n})$. It follows that φ is surjective and induces an isomorphism $(R \setminus \{0\})/\mathcal{U}(R) \to \coprod_{P \in \mathrm{Max}(R)}(R_P \setminus \{0\})/\mathcal{U}(R_P)$. Then statements (1), (2), and (3) follow easily.

The proof of (4) follows from (3) since the length of a given factorization in R is the sum of the lengths of the corresponding localized factorizations. □

2. CHARACTERIZATION OF WEAKLY FACTORIAL QUADRATIC ORDERS

Let R be a quadratic order with conductor I. The orders of the two factor groups $\mathcal{U}(\bar{R})/\mathcal{U}(R)$ and $\mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)$ appearing in Theorem 1.2 can both be calculated. The class number formula for quadratic orders gives one of the orders and the study of the fundamental unit gives the second one.

Proposition 2.1. *Let* $R = \mathbb{Z}[n\omega]$ *be a quadratic order where* $n = \prod p_i^{e_i} \in \mathbb{N}^*$, p_i *prime integers and* $e_i \geq 1$.

The order of $\mathcal{U}(\bar{R}/n\bar{R})/\mathcal{U}(R/n\bar{R})$ *is* $g(n) = n \prod \left(1 - \dfrac{\chi(p_i)}{p_i}\right)$.

In particular, if n *and* m *are coprime, we have* $g(nm) = g(n)g(m)$.

Proof. Compare the class number formula $|\mathrm{Pic}(R)| = |\mathrm{Pic}(\bar{R})||\mathcal{U}(\bar{R})/\mathcal{U}(R)|^{-1} n \prod \left(1 - \dfrac{\chi(p_i)}{p_i}\right)$ (see H.M. Edwards [7, Chapter 9.6]) and the following formula $|\mathrm{Pic}(R)| = |\mathrm{Pic}(\bar{R})||\mathcal{U}(\bar{R})/\mathcal{U}(R)|^{-1}|\mathcal{U}(\bar{R}/n\bar{R})/\mathcal{U}(R/n\bar{R})|$ (see J. Neukirch [11, Theorem 12.12]). □

It remains to get the value of $|\mathcal{U}(\bar{R})/\mathcal{U}(R)|$. In the imaginary case, this is quite easy and we recover the well known imaginary quadratic orders with trivial class group (see D.A. Cox [6, Theorem 7.30]).

Corollary 2.2. *There are four non-integrally closed weakly factorial imaginary quadratic orders:* $\mathbb{Z}[2i]$, $\mathbb{Z}[2j]$, $\mathbb{Z}[3j]$, *and* $\mathbb{Z}[\sqrt{-7}]$ *where* $j = \frac{1}{2}(-1 + \sqrt{-3})$.

For a real quadratic order R, we can evaluate $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)|$ according to the fundamental unit.

Lemma 2.3. *Let* ε *be the fundamental unit of the ring of integers* $\mathcal{O}_K = \mathbb{Z}[\omega]$ *of* $K = \mathbb{Q}(\sqrt{d})$ *where* $d > 0$ *is square-free and assume that* $\mathcal{O}_K$ *is a PID. Let* $R = \mathbb{Z}[n\omega], n \in \mathbb{N}^*$. *Then* $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)|$ *is the least* $k \in \mathbb{N}^*$ *such that* $\varepsilon^k \in R$, *or equivalently, such that* n *divides* b_k, *where* $\varepsilon^k = a_k + b_k\omega$ *with* $a_k, b_k \in \mathbb{Z}$. *Such an element* ε^k *is called the* **fundamental unit** *of* R. *In particular,* R *is weakly factorial if and only if* $k = |\mathcal{U}(\mathcal{O}_K/n\mathcal{O}_K)/\mathcal{U}(R/n\mathcal{O}_K)|$.

Proof. We have $\mathcal{U}(\mathcal{O}_K) = \{\pm 1\} \times < \varepsilon >$. Moreover $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)|$ is finite and is the order of the class of ε in the factor group $\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)$, a finite cyclic group generated by the class of ε. This order is in fact the least $k \in \mathbb{N}^*$ such that $\varepsilon^k \in R$. If we set $\varepsilon^k = a_k + b_k\omega$ with $a_k, b_k \in \mathbb{Z}$, we get that $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)|$ is the least $k \in \mathbb{N}^*$ such that n divides b_k. The end of the proof follows from Theorem 1.2. □

In fact, we can restrict to integers n which are a power of a prime by the following lemma.

Lemma 2.4. *Let $\mathcal{O}_K = \mathbb{Z}[\omega]$ be the ring of integers of a real quadratic number field K. Let n and $m \in \mathbb{N}^*$ be two coprime integers and consider $R' = \mathbb{Z}[n\omega]$, $R'' = \mathbb{Z}[m\omega]$ and $R = \mathbb{Z}[nm\omega]$. Then $R = R' \cap R''$ and $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)| = \mathrm{lcm}(|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R')|, |\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R'')|)$.*

Proof. Obviously, we have $R \subset R' \cap R''$. Any $x \in R' \cap R''$ can be written $x = a + bn\omega = c + dm\omega$ with $a, b, c, d \in \mathbb{Z}$. But $\gcd(n, m) = 1$ and $\{1, \omega\}$ is a basis combine to yield n divides d so that $x \in R$. Thus $R = R' \cap R''$.

Now let ε be the fundamental unit of $\mathbb{Z}[\omega]$. Set $p = |\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)|$, $q = |\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R')|$, $r = |\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R'')|$ and $s = \mathrm{lcm}(q, r)$. Then we have $\varepsilon^s \in R' \cap R'' = R$ so that p divides s. Conversely, as $\varepsilon^p \in R = R' \cap R''$, we get that q and r divide p, and so does s. □

Proposition 2.5. *Let n and $m \in \mathbb{N}^*$ be two coprime integers. Consider $R' = \mathbb{Z}[n\omega]$ and $R'' = \mathbb{Z}[m\omega]$ two quadratic orders in the same number field K with ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$. Set $R = R' \cap R''$. Then R is weakly factorial if and only if R', R'' are weakly factorial and $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R')|, |\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R'')|$ are coprime.*

Proof. Assume first that K is a real quadratic number field. If R is weakly factorial, so are R' and R'' by [12, Corollary 2].

Conversely, assume that R' and R'' are weakly factorial. It follows that $\mathcal{O}_K$ is a PID. By Theorem 1.2, R is weakly factorial if and only if $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)| = |\mathcal{U}(\mathcal{O}_K/nm\mathcal{O}_K)/\mathcal{U}(R/nm\mathcal{O}_K)| = g(nm) = g(n)g(m)$, with notation of Proposition 2.1 since n and m are coprime. The same theorem gives $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R')| = |\mathcal{U}(\mathcal{O}_K/n\mathcal{O}_K)/\mathcal{U}(R'/n\mathcal{O}_K)| = g(n)$ and $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R'')| = |\mathcal{U}(\mathcal{O}_K/m\mathcal{O}_K)/\mathcal{U}(R''/m\mathcal{O}_K)| = g(m)$. But, thanks to Lemma 2.4, we have $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R)| = \mathrm{lcm}(g(n), g(m))$. Then R is weakly factorial if and only if $g(n)g(m) = \mathrm{lcm}(g(n), g(m))$ or equivalently, if and only if $g(n)$ and $g(m)$ are coprime. The two parts of the proposition are proved in the real case.

We can remark that this situation does not occur in the imaginary case. □

Remark. In [14, Theorem 4.1], R. Wiegand shows that a quadratic order R has torsionfree cancellation if and only if $\mathrm{Pic}(R) \to \mathrm{Pic}(\bar{R})$ is an isomorphism, which is equivalent to R being weakly factorial when $\bar{R}$ is a PID. Then, Proposition 2.5 can also be derived from [14, Remark 4.7] by replacing "torsionfree cancellation" by "weak factoriality".

Let K be a quadratic number field such that the ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$ is a PID and let $R = \mathbb{Z}[n\omega]$ be a quadratic order in K, where $n = \prod_i p_i^{e_i}$, p_i prime integers. To see whether R is weakly factorial or not, it is enough to study the orders $\mathbb{Z}[p_i^{e_i}\omega]$. A necessary condition for R to be weakly factorial is that the orders $r_i = |\mathcal{U}(\mathcal{O}_K/p_i^{e_i}\mathcal{O}_K)/\mathcal{U}(\mathbb{Z}[p_i^{e_i}\omega]/p_i^{e_i}\mathcal{O}_K)|$ are pairwise coprime. Proposition 2.1 gives these orders. If p_i is a decomposed or an inert odd prime, r_i is even, by Proposition 2.1. So, there is at most one decomposed or inert odd prime among the p_i.

We know (Hasse [13, Chapter 29.3, p. 590]) that if the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is a PID, where $d > 0$ is square-free, then d is one of the following types: (1) d is a prime integer, (2) $d = pp'$, $p \neq p'$ prime integers, $p, p' \equiv 2, 3 \pmod 4$. So, there are at most two odd prime integers p_i which are ramified in K. This gives the following corollary.

Corollary 2.6. *Let $\mathbb{Z}[n\omega]$ be a weakly factorial real quadratic order with $n = \prod_{i=1}^{r} p_i^{e_i}$, p_i prime integers. Then $r \leq 4$ with at most two p_i decomposed or inert (if there are two p_i decomposed or inert, then $2 = p_i$ is one of them and $e_i = 1$) and at most two p_i ramified (if 2 is one of them, all p_i are ramified).*

Proof. We have just proved above a part of the corollary.

Now, assume that $p_i = 2$ for some i, with 2 inert or decomposed and let $p_j = p$ be another inert or decomposed prime dividing n. As p is odd, $p \pm 1$ is even. If $e_i > 1$, then r_i and r_j are both even, so that $\mathbb{Z}[p_i^{e_i}\omega] \cap \mathbb{Z}[p_j^{e_j}\omega]$ is not weakly factorial.

If 2 is ramified and n is even, $\mathbb{Z}[n\omega]$ is not weakly factorial if some decomposed or inert prime p divides n, since p is odd. □

Set $R_n = \mathbb{Z}[p^n\omega]$ and consider the decreasing sequence $\{R_n\}_{n\in\mathbb{N}^*}$ of suborders of $\mathbb{Z}[\omega]$, where p is a prime integer. We are going to study how the weakly factorial condition behaves in the sequence.

First, we give two technical lemmata.

Lemma 2.7. *Let $K = \mathbb{Q}(\sqrt{d})$ where $d > 0$ is square-free. Consider $x = r + s\omega \in K$, $r, s \in \mathbb{Q}$. For $m \in \mathbb{N}^*$, set $x^m = r' + s'\omega$, $r', s' \in \mathbb{Q}$.*

1. *If $d \equiv 2,3 \pmod 4$, then $r' = \sum_{k=0,\text{even}}^{m} \mathrm{C}_m^k r^{m-k} s^k d^{\frac{k}{2}}$ and $s' = \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k r^{m-k} s^k d^{\frac{k-1}{2}}$.*
2. *If $d \equiv 1 \pmod 4$, then $r' = 2^{-m} \sum_{k=0,\text{even}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k}{2}} - 2^{-m} \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k-1}{2}}$ and $s' = 2^{1-m} \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k-1}{2}}$.*

Proof.

(1) If $d \equiv 2,3 \pmod 4$, we have $\omega = \sqrt{d}$ so that $x^m = (r+s\omega)^m = \sum_{k=0}^{m} \mathrm{C}_m^k r^{m-k} s^k \omega^k = \sum_{k=0}^{m} \mathrm{C}_m^k r^{m-k} s^k d^{\frac{k}{2}}$ $= \sum_{k=0,\text{even}}^{m} \mathrm{C}_m^k r^{m-k} s^k d^{\frac{k}{2}} + \left(\sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k r^{m-k} s^k d^{\frac{k-1}{2}}\right) \omega$ which gives the result.

(2) If $d \equiv 1 \pmod 4$, we get $\omega = \frac{1}{2}(1 + \sqrt{d})$ and $x = \frac{1}{2}[(2r+s) + s\sqrt{d}]$ so $x^m = \frac{1}{2}[(2r'+s') + s'\sqrt{d}] =$ $\frac{1}{2^m} \sum_{k=0}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k}{2}} = \frac{1}{2^m}[\sum_{k=0,\text{even}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k}{2}} + \sqrt{d} \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k-1}{2}}]$. Therefore it follows that $r' = \frac{1}{2^m} \sum_{k=0,\text{even}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k}{2}} - \frac{1}{2^m} \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k-1}{2}}$ and $s' = \frac{1}{2^{m-1}} \sum_{k=1,\text{odd}}^{m} \mathrm{C}_m^k (2r+s)^{m-k} s^k d^{\frac{k-1}{2}}$. □

Lemma 2.8. *Let $\mathbb{Z}[\omega]$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$ where $d > 0$ is square-free and let $\varepsilon' = a + bp\omega$, $a, b \in \mathbb{Z}$, be a unit of $\mathbb{Z}[\omega]$, with p a prime integer. For $n \in \mathbb{N}^*$, set $\varepsilon'_n = \varepsilon'^{p^{n-1}}$.*

1. *There exist $a_n, b_n \in \mathbb{Z}$ such that $\varepsilon'_n = a_n + b_n p^n \omega$.*
2. *p does not divide a_n for any $n \in \mathbb{N}^*$.*
3. *If $(p, b) = 1$, then $(p, b_n) = 1$ for any $n \in \mathbb{N}^*$, except if $p = 2$ and $d \equiv 1 \pmod 4$. In this case, b_2 is even.*

Proof. We have $\varepsilon'_n = \varepsilon'^p_{n-1}$. We prove (1) and (3) by induction on n.

(1) is satisfied for $n = 1$ since $\varepsilon'_1 = \varepsilon'$.

Assume that $\varepsilon'_{n-1} = a_{n-1} + b_{n-1} p^{n-1} \omega$, with $a_{n-1}, b_{n-1} \in \mathbb{Z}$. Now use Lemma 2.7.

If $d \equiv 2,3 \pmod 4$ the coefficient of ω in ε'_n is $\sum_{k=1,\text{odd}}^{p} \mathrm{C}_p^k a_{n-1}^{p-k} b_{n-1}^k p^{k(n-1)} d^{\frac{k-1}{2}}$. Since p divides C_p^k for $k = 1, \ldots, p-1$, then p^n divides $\mathrm{C}_p^k a_{n-1}^{p-k} b_{n-1}^k p^{k(n-1)}$ for $k = 1, \ldots, p-1$. For $k = p$, the coefficient of $d^{\frac{p-1}{2}}$ is $b_{n-1}^p p^{p(n-1)}$, divisible by p^n since $p(n-1) \geq n$.

If $d \equiv 1 \pmod 4$ the coefficient of ω in ε'^n_n is $2^{1-p}\sum_{k=1,\text{odd}}^{p} C_p^k (2a_{n-1}+b_{n-1}p^{n-1})^{p-k} b_{n-1}^k p^{k(n-1)} d^{\frac{k-1}{2}}$, divisible by p^n (same proof as in the previous case when $p \neq 2$).

If $p = 2$ this coefficient is $2^n b_{n-1}(a_{n-1} + b_{n-1}2^{n-2})$, which gives the result, since $n \geq 2$.

So (1) is proved.

(2) Since ε' and ε'^n_n are invertible, $\varepsilon'^n_n \notin p\mathbb{Z}[\omega]$, so p does not divide a_n for any $n \in \mathbb{N}^*$.

Let us prove (3) and assume that p does not divide b_{n-1}, with $n \geq 2$.

If we have $d \equiv 2,3 \pmod 4$, the same proof as in (1) gives that p^{n+1} divides $C_p^k a_{n-1}^{p-k} b_{n-1}^k p^{k(n-1)}$ for $k = 2, \ldots, p-1$ and $b_{n-1}^p p^{p(n-1)}$ when $p \neq 2$. But, for $k = 1$, we get that $p a_{n-1}^{p-1} b_{n-1} p^{n-1} = a_{n-1}^{p-1} b_{n-1} p^n$ is not divisible by p^{n+1}. The proof is straightforward for $p = 2$.

If $d \equiv 1 \pmod 4$ and $p \neq 2$, the proof is the same since p does not divide $2a_{n-1} + b_{n-1}p^{n-1}$.

In both cases, p does not divide b_n.

If $p = 2$ and $d \equiv 1 \pmod 4$, the calculation made in (1) gives that $b_n = b_{n-1}(a_{n-1} + b_{n-1}2^{n-2})$ is odd when b_{n-1} is odd, except for $n = 2$. In fact, $a + b$ is even because a and b are both odd. □

Corollary 2.9. *Let ε be the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ square-free. Set $R_n = \mathbb{Z}[p^n\omega]$, $n \in \mathbb{N}^*$, p a prime integer. Let ε_n be the fundamental unit of R_n.*

1. *Assume that R_n is weakly factorial. Then R_{n+1} is weakly factorial if and only if $\varepsilon_n \in R_n \setminus R_{n+1}$.*
2. *If R_2 is weakly factorial, so is R_n for every $n \in \mathbb{N}^*$, except when $p = 2$ and $d \equiv 1 \pmod 4$. In this case, only R_1 and R_2 are weakly factorial.*

Proof.

(1) For $n \in \mathbb{N}^*$ set $r_n = |\mathcal{U}(\mathcal{O}_K/p^n\mathcal{O}_K)/\mathcal{U}(R_n/p^n\mathcal{O}_K)|$. We have $r_n = p^{n-1}(p - \chi(p))$ by Proposition 2.1. Lemma 2.3 gives $\varepsilon_n = \varepsilon^{r_n}$ and R_{n+1} is weakly factorial if and only if the fundamental unit of R_{n+1} is $\varepsilon^{r_{n+1}}$. As $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R_{n+1})|$ divides r_{n+1}, we have $\varepsilon^{r_{n+1}} = \varepsilon_n^p \in R_{n+1}$. Moreover, $|\mathcal{U}(\mathcal{O}_K)/\mathcal{U}(R_n)| = r_n$ implies $|\mathcal{U}(R_n)/\mathcal{U}(R_{n+1})| = p$ or 1. It follows that R_{n+1} is weakly factorial if and only if $\mathcal{U}(R_n) \neq \mathcal{U}(R_{n+1})$, which is equivalent to $\varepsilon_n \in R_n \setminus R_{n+1}$.

(2) Let $\varepsilon' = \varepsilon^{r_1} = a + pb\omega$ be the fundamental unit of R_1. If R_2 is weakly factorial, we get by (1) that $\varepsilon' \notin R_2$ and $(p, b) = 1$.

Assume that $p \neq 2$ or $d \not\equiv 1 \pmod 4$. By Lemma 2.8 we get that $\varepsilon'^{p^{n-1}} \in R_n \setminus R_{n+1}$ for every $n \in \mathbb{N}^*$. An easy induction using again (1) shows that R_n is weakly factorial for every $n \in \mathbb{N}^*$.

If $p = 2$ and $d \equiv 1 \pmod 4$, Lemma 2.8 implies that b_2 is even, where $\varepsilon'^2 = a_2 + 4b_2\omega$ is the fundamental unit of R_2, so that $\varepsilon'^2 \in R_3$, which is not weakly factorial. □

Example. Actually, only four situations of decreasing sequences $\{R_n = \mathbb{Z}[p^n\omega]\}_{n\in\mathbb{N}}$ occur.

(1) Let $d = 6$. Then $\mathbb{Z}[\omega]$ is a PID and $\varepsilon = 5 + 2\omega \in \mathbb{Z}[2\omega]$, which is not weakly factorial. Now $\varepsilon \notin \mathbb{Z}[3\omega]$, which is weakly factorial, but $\varepsilon^3 = 485 + 22 \cdot 3^2\omega \in \mathbb{Z}[3^2\omega]$, which is not weakly factorial.

(2) Let $d = 5$. Then $\mathbb{Z}[\omega]$ is a PID and $\varepsilon = \omega \notin \mathbb{Z}[2\omega], \mathbb{Z}[5\omega]$, which are weakly factorial. Now, $\varepsilon^3 = 1 + 2\omega \notin \mathbb{Z}[2^2\omega]$, which is weakly factorial. By Corollary 2.9, $\mathbb{Z}[2^n\omega]$ is not weakly factorial for any $n > 2$. As $\varepsilon^5 = 3 + 5\omega \notin \mathbb{Z}[5^2\omega]$, we get that $\mathbb{Z}[5^2\omega]$ is weakly factorial and so is $\mathbb{Z}[5^n\omega]$ for any $n \in \mathbb{N}$ by Corollary 2.9.

3. LENGTH FUNCTIONS IN LOCAL WEAKLY FACTORIAL QUADRATIC ORDERS

As we have seen in Proposition 1.4, to determine atoms or lengths of factorization in a weakly factorial order R we need only to study the localizations R_P for $P \in \mathrm{Max}(R)$. In fact, it is sufficient to consider the localizations at the maximal ideals of R which contain the conductor I of R. Actually, if P does not contain I, we have an isomorphism $R_P \simeq \bar{R}_P$ and R_P is a PID. Let $R = \mathbb{Z}[n\omega]$, $n \in \mathbb{N}^*$ be a quadratic order. The prime ideals of R containing the conductor are of the form $p\mathbb{Z}[n'\omega]$, with $n = pn'$, and p a prime integer dividing n.

Observe that if no decomposed prime divides n, the spectral map $\mathrm{Spec}(\bar{R}) \to \mathrm{Spec}(R)$ is bijective (see Section 1). In this case, if p is a prime integer dividing n, there is a unique maximal ideal P in R lying over $p\mathbb{Z}$. Setting $S = \mathbb{Z} \setminus p\mathbb{Z}$, we have $R_S \simeq R_P$ and $\bar{R}_S \simeq \bar{R}_P$, which are both local domains, with $\bar{R}_P$ a DVD. If we denote by $\mathbb{Z}'$ the localization $\mathbb{Z}_S$, we are in the following situation: p is an atom in $\mathbb{Z}'$, ramified or inert in $\bar{R}_P$ as in $\bar{R}$. We can again write $\bar{R}_P = \mathbb{Z}'[\omega]$ with maximal ideal $p'\bar{R}_P$, and $R_P = \mathbb{Z}'[q\omega]$, q a power of p. Moreover, $\bar{R}_P$ and R_P are both free $\mathbb{Z}'$-modules with basis $\{1, \omega\}$ and $\{1, q\omega\}$. We call R_P a **local** order. If p is a decomposed prime there is again a unique maximal ideal P in R lying over $p\mathbb{Z}$ and isomorphisms $R_S \simeq R_P$ and $\bar{R}_S \simeq \bar{R}_P$.

Moreover, the groups of units of R_P and $\bar{R}_P$ are closely linked as can be seen by the following proposition.

Proposition 3.1. *Let $R = \mathbb{Z}[p^n\omega]$, ($p$ a prime integer) be a weakly factorial quadratic order and let $S = \mathbb{Z} \setminus p\mathbb{Z}$. Then there is an isomorphism $\mathcal{U}(\bar{R})/\mathcal{U}(R) \simeq \mathcal{U}(\bar{R}_S)/\mathcal{U}(R_S)$.*

Proof. We have obviously an injection $f : \mathcal{U}(\bar{R})/\mathcal{U}(R) \to \mathcal{U}(\bar{R}_S)/\mathcal{U}(R_S)$. Since R is weakly factorial, f is surjective. Let $x = x'/s \in \mathcal{U}(\bar{R}_S)$, $x' \in \bar{R}$, and $s \in S$. Then x' is comaximal with p^n in $\bar{R}$. There exists $u \in \mathcal{U}(\bar{R})$ such that $a = ux' \in R$ by [12, Theorem 2] which gives $x = (u^{-1}/1)(a/s)$ where $u^{-1}/1$ is the image of u^{-1} in $\mathcal{U}(\bar{R}_S)$ and $a/s \in \mathcal{U}(R_S)$. It follows also that $\mathcal{U}(\bar{R}_S)/\mathcal{U}(R_S)$ is a finite cyclic group generated by the class of the fundamental unit in the real case (in fact, we can also consider a fundamental unit in the imaginary case). □

From now on, we work with a local order of the form $R_n = \mathbb{Z}'[p^n\omega]$ where p is a prime integer, $n \in \mathbb{N}^*$. Its maximal ideal is pR_{n-1}. It follows that $R_0 = \mathbb{Z}'[\omega]$ and p^nR_0 is the conductor of R_n. We begin to characterize a family of nonassociate atoms of R_n independent of the decomposition of p in $\mathbb{Z}'[\omega]$.

Proposition 3.2. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, p a prime integer, $n \in \mathbb{N}^*, k \in \{2, \ldots, n\}$ and $u \in \mathcal{U}(\mathbb{Z}'[\omega])$. Then up^k is an atom in R_n if and only if $u \in \mathcal{U}(R_{n-k}) \setminus \mathcal{U}(R_{n-k+1})$. In this case, up^k is an associate of $\varepsilon^j p^k$ where*

- *$j = p^{n-k-1}(p - \chi(p))j'$ with $0 < j' < p^k$ and $(p, j') = 1$ if $1 < k < n$.*
- *$0 < j < p^{n-1}(p - \chi(p))$ where $p - \chi(p)$ does not divide j if $1 < k = n$.*

up is an atom in R_n for $u \in \mathcal{U}(\mathbb{Z}'[\omega])$ if and only if $u \in \mathcal{U}(R_{n-1})$. Moreover, up is associated to $\varepsilon^j p$ where

- *$j = p^{n-2}(p - \chi(p))j'$ with $0 \leq j' < p$ if $1 < n$.*
- *$0 \leq j < p - \chi(p)$ if $1 = n$.*

In addition, if p is inert, all atoms of R_n are obtained in this way.

Proof. Let $u = a + b\omega \in \mathcal{U}(\mathbb{Z}'[\omega])$, $a, b \in \mathbb{Z}'$. Then $x = up^k \in R_n$ if and only if p^{n-k} divides b if and only if $u \in \mathcal{U}(R_{n-k})$. If $u \in \mathcal{U}(R_{n-k+1})$, we get that $up^{k-1} \in R_n$ and $x = p(up^{k-1})$ is not an atom in R_n. Conversely, let $u \in \mathcal{U}(R_{n-k}) \setminus \mathcal{U}(R_{n-k+1})$ and assume that there exist $x', x'' \in R_n$ such that $x'x'' = up^k$. If neither x' nor $x'' \in \mathcal{U}(R_n)$, they belong both to pR_{n-1} so that $up^{k-2} \in R_{n-1}$ and $u \in \mathcal{U}(R_{n-k+1})$, a contradiction.

up is obviously an atom as soon as $up \in R_n$.

Assume that p is inert. Then p is an atom in R_0 and generates its maximal ideal. Any nonunit nonzero element x of R_n is of the form $x = up^k$, where $u \in \mathcal{U}(R_0)$. If $k > n$, we get that $x = (up^n)p^{k-n}$ is not an atom in R_n. Two parts of the proof are obtained.

Let $u \in \mathcal{U}(R_0)$ such that $x = up^k \in R_n$. There exists $j \in \mathbb{N}$ such that x is associated in R_n to $\varepsilon^j p^k$ since $\mathcal{U}(R_0)/\mathcal{U}(R_n)$ is a finite cyclic group generated by the class of ε. Although the value of j is not unique, we can determine a least value of j when x is an atom. In fact $\varepsilon^j p^k$ and $\varepsilon^{j'} p^k$ are associates in R_n if and only if there exists $v \in \mathcal{U}(R_n)$ such that $\varepsilon^j p^k = v\varepsilon^{j'} p^k$ if and only if $|\mathcal{U}(R_0)/\mathcal{U}(R_n)|$ divides $j - j'$. Now $|\mathcal{U}(R_0)/\mathcal{U}(R_n)| = |\mathcal{U}(R_0/p^nR_0)/\mathcal{U}(R_n/p^nR_0)| = p^{n-1}(p - \chi(p))$ (this formula holds in the local case). For the least value of j, we get the condition $0 \leq j < p^{n-1}(p - \chi(p))$. Moreover, $\varepsilon^j \in \mathcal{U}(R_{n-k}) \setminus \mathcal{U}(R_{n-k+1})$ if and only if $|\mathcal{U}(R_0)/\mathcal{U}(R_{n-k})|$ divides j and $|\mathcal{U}(R_0)/\mathcal{U}(R_{n-k+1})|$ does not divide j. So we get:

- If $1 < k < n$, then $\varepsilon^j \in \mathcal{U}(R_{n-k}) \setminus \mathcal{U}(R_{n-k+1})$ if and only if $p^{n-k-1}(p-\chi(p))$ divides j and $p^{n-k}(p-\chi(p))$ does not divide j, if and only if $j = p^{n-k-1}(p - \chi(p))j'$ with $0 < j' < p^k$ and $(p, j') = 1$.
- If $1 = k < n$, then $\varepsilon^j p$ is an atom when in R_n. Moreover, condition $\varepsilon^j \in \mathcal{U}(R_{n-1})$ where $0 \leq j < p^{n-1}(p - \chi(p))$ is equivalent to $j = p^{n-2}(p - \chi(p))j'$ with $0 \leq j' < p$.
- If $1 < k = n$, then $\varepsilon^j p^n \in R_n$ and $\varepsilon^j \notin \mathcal{U}(R_1)$ if and only if $p - \chi(p)$ does not divide j. So we get condition $0 < j < p^{n-1}(p - \chi(p))$ where $p - \chi(p)$ does not divide j.
- If $1 = k = n$, then $\varepsilon^j p$ is always an atom and we get condition $0 \leq j < p - \chi(p)$. □

When p is ramified or decomposed, we have the following additional atoms.

Proposition 3.3. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p ramified, $p \sim p'^2$ in R_0. The atoms of R_n are the up^k as in Proposition 3.2 and the up'^{2n+1} for any $u \in \mathcal{U}(R_0)$. Moreover, the up'^{2n+1} are associated to the $\varepsilon^j p'^{2n+1}$, $0 \leq j < p^n$.*

Proof. Since p is ramified, there exists an atom $p' \in R_0$ such that $p \sim p'^2$ in R_0 and $u \in \mathcal{U}(R_0)$ such that $p = up'^2$. The maximal ideal of R_n is pR_{n-1}. By Proposition 3.2, p is an atom of R_n. So there is no atom in R_n of the form $u'p'^k$ with $u' \in \mathcal{U}(R_0)$ and $k \in \mathbb{N}^*$, $k > 2n+1$ (if $k > 2n+1$, we can write $u'p'^k = (up'^2)(u^{-1}u'p'^{k-2})$ with $u^{-1}u'p'^{k-2} \in p^nR_0 \subset R_n$).

Proposition 3.2 provides a characterization of atoms of the form $u'p'^{2k}$ for some $k \in \{1, \ldots, n\}$ where $u' \in \mathcal{U}(R_0)$. We show by induction on n that the other nonassociate atoms of R_n are of the form vp'^{2n+1} for any $v \in \mathcal{U}(R_0)$ $(*)$.

- Any atom of R_1 is in pR_0. Now, vp'^3 is an atom of R_1 for any $v \in R_0$. If not, there exist $x, y \in pR_0$ such that $vp'^3 = xy$, a contradiction. So $(*)$ is shown for $n = 1$.
- Let $n \geq 1$. Assume that $(*)$ is satisfied for n. An atom of R_{n+1} is of the form $u'p'^k$ with $k \leq 2n + 3$, $u' \in \mathcal{U}(R_0)$. If k is even, we are in the situation of Proposition 3.2. If k is odd with $k \leq 2n + 1$, we can set $k = 2m + 1$ with $m \leq n$. Moreover, $u'p'^k$ lies in the maximal ideal pR_n of R_{n+1}. It follows that $v'p'^{2m-1} \in R_n$, for some $v' \in \mathcal{U}(R_0)$, a contradiction by the induction hypothesis.

First, we have $vp'^{2n+3} \in R_{n+1}$ for any $v \in \mathcal{U}(R_0)$. Now, assume that there is some $v \in \mathcal{U}(R_0)$ such that vp'^{2n+3} is not an atom in R_{n+1}. There exist $u_1, u_2 \in \mathcal{U}(R_0)$, $k' \in \mathbb{N}^*$, $k' < 2n + 3$ such that $vp'^{2n+3} = (u_1p'^{k'})(u_2p'^{2n+3-k'})$, where $u_1p'^{k'}$, $u_2p'^{2n+3-k'} \in pR_n$ so that $u_1'p'^{k'-2}, u_2'p'^{2n+1-k'} \in R_n$ for some $u_1', u_2' \in \mathcal{U}(R_0)$. One of the exponents of p' is odd and then not less than $2n + 1$, by the induction hypothesis. But $k' - 2 < 2n + 1$ and $2n + 1 - k' < 2n + 1$ lead to a contradiction. So $(*)$ holds for $n + 1$.

Because of $|\mathcal{U}(R_0)/\mathcal{U}(R_n)| = p^n$, we get the number of nonassociate atoms up'^{2n+1}. □

Proposition 3.4. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p decomposed. Set $p = p_1p_2$ where p_i is an atom of R_0 for $i = 1, 2$. The atoms of R_n are the up^k as in Proposition 3.2 and the ${up_1}^n{p_2}^{n+m}, {up_1}^{n+m}{p_2}^n$ for any $u \in \mathcal{U}(R_0)$, $m \in \mathbb{N}^*$. Moreover, these atoms are associated to the $\varepsilon^j{p_1}^n{p_2}^{n+m}$ and to the $\varepsilon^j{p_1}^{n+m}{p_2}^n$ for a given m with $0 \leq j < p^n - p^{n-1}$.*

Proof. Since p is decomposed, there exist p_1, p_2 atoms of R_0 such that $p = p_1p_2$. The maximal ideal of R_n is pR_{n-1}. So, for any $n \geq 1$, any nonzero nonunit element of R_n can be written $up_1^rp_2^s$, where $u \in \mathcal{U}(R_0)$, $r, s \in \mathbb{N}^*$.

There is no atom in R_n of the form up^k with $u \in \mathcal{U}(R_0)$, $k \in \mathbb{N}^*$, $k > n$ since we can write $up^k = (up^n)p^{k-n}$.

We show by induction on n that:

(1) no nonzero nonunit element of R_n is of the form $up_1^rp_2^s$, $u \in \mathcal{U}(R_0)$, $r \neq s$ and $\inf(r, s) < n$.

(2) ${vp_1}^n{p_2}^{n+m}, {vp_1}^{n+m}{p_2}^n$ are atoms of R_n for any $v \in \mathcal{U}(R_0)$, where $m \in \mathbb{N}^*$.

- (1) is obvious for $n = 1$ since the maximal ideal of R_1 is pR_0. If $up_1^mp_2$ is not an atom, there exist $x, y \in pR_0$ such that $up_1^mp_2 = xy$, a contradiction. So (2) is proved for $n = 1$.
- Let $n \geq 1$ and assume that (1) and (2) are satisfied for n. Consider a nonzero nonunit $x = up_1^rp_2^s \in R_{n+1}$, with $u \in \mathcal{U}(R_0)$, $r \neq s$ and $\inf(r, s) < n + 1$. Then $x \in pR_n$ implies that $up_1^{r-1}p_2^{s-1} \in R_n$ and we can assume that $0 < r < s$. As $0 \leq r - 1 < s - 1$, it follows that $up_1^{r-1}p_2^{s-1}$ is a nonzero nonunit element of R_n and then $1 \leq r - 1 < n$, a contradiction with (1). Hence (1) holds for $n + 1$.

Now assume that ${up_1}^{n+1}{p_2}^{n+1+m}$ is not an atom of R_{n+1} for some $u \in \mathcal{U}(R_0)$, $m \in \mathbb{N}^*$. For such u, there exist $u', u'' \in \mathcal{U}(R_0)$, $r_1, s_1, r_2, s_2 \in \mathbb{N}^*$ such that ${up_1}^{n+1}{p_2}^{n+1+m} = (u'p_1^{r_1}p_2^{r_2})(u''p_1^{s_1}p_2^{s_2})$ where $u'p_1^{r_1}p_2^{r_2}, u''p_1^{s_1}p_2^{s_2}$ are nonunits of R_{n+1}. It follows that $r_1 + s_1 = n + 1$ and $r_2 + s_2 = n + 1 + m$. But, since $u'p_1^{r_1}p_2^{r_2}$, $u''p_1^{s_1}p_2^{s_2} \in pR_n$, we obtain $u'p_1^{r_1-1}p_2^{r_2-1}$, $u''p_1^{s_1-1}p_2^{s_2-1} \in R_n$. Then ${up_1}^n{p_2}^{n+m} = p(u'p_1^{r_1-1}p_2^{r_2-1})(u''p_1^{s_1-1}p_2^{s_2-1})$ is a product of at least two nonunits of R_n. Indeed, $(r_2 - 1) + (s_2 - 1) = n - 1 + m \geq n > 0$. The induction hypothesis on (2) leads to a contradiction, so that we get (2) for $n + 1$. The proof is the same for ${up_1}^{n+m}{p_2}^n$.

Finally, if $n < r < s$, we can write $up_1^rp_2^s = (p_1p_2)^{r-n}(up_1^np_2^{s+n-r})$, which is not an atom for any $u \in \mathcal{U}(R_0)$.

Because of $|\mathcal{U}(R_0)/\mathcal{U}(R_n)| = p^{n-1}(p - 1)$, we get the number of nonassociate atoms ${up_1}^n{p_2}^{n+m}$. □

Once the nonassociate atoms are known, we are in a position to give an evaluation of the two length functions l and L. We have to consider the three possible decompositions of the prime integer p. First we give a lemma applicable in any case.

Lemma 3.5. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p a prime integer and $x = up^k \in R_n$, $u \in \mathcal{U}(R_0)$ such that $0 < k < 2n$. Set $s = \inf\{i \in \mathbb{N}^* \mid u \in \mathcal{U}(R_{n-i})\}$. Then $s \leq k$. Moreover:*

1. *$l(x) = 1$ if $s = k$*
2. *$l(x) = 2$ if $s < k$ and*
   - *$k < 2s$*
   - *$k = 2s$ and either $k = 2$ or $p \neq 2$*
   - *$k > 2s$ and k is even*
3. *$l(x) = 3$ if $k = 2s \neq 2$ and $p = 2$ or if $k > 2s$, $s \neq 2$ and k is odd.*
4. *$l(x) = 4$ if $p = s = 2$ and $k = 5$.*

Proof. Let $x = up^k \in R_n$ with $u \in \mathcal{U}(R_0) = \mathcal{U}(R_{n-n})$. Since $\{\mathcal{U}(R_i)\}_{i\in\mathbb{N}}$ is a decreasing sequence, consider $s = \inf\{i \in \mathbb{N}^* \mid u \in \mathcal{U}(R_{n-i})\}$. Assume $s > k \geq 1$ so that $R_{n-k} < R_{n-s}$ and $u \notin \mathcal{U}(R_{n-k})$, a contradiction.

First, note that whatever is p, only atoms of the form vp^i appear in a factorization of up^k.

(1) Case $l(x) = 1$ is given by Propositions 3.2, 3.3, and 3.4.

(2) Case $l(x) = 2$ is obtained when we can write $up^k = (u_1p^{k_1})(u_2p^{k_2})$ with $u_ip^{k_i}$ an atom for $i = 1, 2$. Assume that this condition is fulfilled and that $k_1 \leq k_2$. We have equalities $u = u_1u_2$ and $k = k_1 + k_2$ with conditions of Proposition 3.2 for $u_ip^{k_i}$ so that $R_{n-k_1} \subset R_{n-k_2}$, which implies $u \in R_{n-k_2}$.

- If $k_1 = k_2 = 1$, we have $k = 2$ and any factorization of x has length 2 as soon x is not an atom, that is, when $s = 1$. Conversely, if $k = 2$ and $s = 1$, we get $l(x) = 2$.
- Assume now that $k_2 > 1$, so that $u_2 \in R_{n-k_2} \setminus R_{n-k_2+1}$.
  - Let $s > 1$, then $u \in R_{n-s} \setminus R_{n-s+1}$ so that $R_{n-s+1} < R_{n-k_2}$ which gives $s - 1 < k_2$ or $s \leq k_2$. But we also have $u_2 = u_1^{-1}u$. Set $t = \sup(s, k_1)$. It follows that $u_2 \in R_{n-t} \setminus R_{n-k_2+1}$ so that $k_2 - 1 < t \leq k_2$ and $t = k_2$.
  * If $k_1 < s$, we obtain that $t = s = k_2$ and $k < 2s$. Conversely, if $k < 2s$, set $k_2 = s$ and $k_1 = k - s$. Take $u_1 \in R_{n-k_1} \setminus R_{n-k_1+1}$ if $k_1 > 1$ or $u_1 \in R_{n-1}$ if $k_1 = 1$. Then $u_2 = uu_1^{-1} \in R_{n-k_2} \setminus R_{n-k_2+1}$ so that $u_ip^{k_i}$ is an atom for $i = 1, 2$ and $l(x) = 2$. Case $\mathcal{U}(R_{n-k_1}) = \mathcal{U}(R_{n-k_1+1})$ cannot happen.
  * If $k_1 = s$, we obtain that $t = s = k_2 = k_1$ and $k = 2s$. Conversely, if $k = 2s$, set $k_1 = k_2 = s$. There exist $u_1, u_2 \in \mathcal{U}(R_{n-s}) \setminus \mathcal{U}(R_{n-s+1})$ such that $u = u_1u_2$ if and only if $|\mathcal{U}(R_{n-s})/\mathcal{U}(R_{n-s+1})| > 2$ and then $l(x) = 2$. This condition is satisfied if and only if $p \neq 2$.
  * If $k_1 > s$, we obtain that $t = k_2 = k_1$ and $k > 2s$ is even. Conversely, if $k > 2s$ is even, set $k_1 = k_2 = k/2 > 1$. There exist $u_1, u_2 \in \mathcal{U}(R_{n-k_1}) \setminus \mathcal{U}(R_{n-k_1+1})$ such that $u = u_1u_2$ if and only if $|\mathcal{U}(R_{n-k_1})/\mathcal{U}(R_{n-k_1+1})| > 1$, and in this case $l(x) = 2$. This condition always holds.
  - Let $s = 1 < k_2$, so that $R_{n-1} \subset R_{n-k_2+1}$. As $u_2 = uu_1^{-1} \in R_{n-k_1} \setminus R_{n-k_2+1}$, it follows that $k_2 - 1 < k_1$ and $k_1 = k_2 = k/2$ so that k is even. The converse is as in the case $k_1 > s > 1$.

(3) Consider the remaining cases for which we have $l(x) > 2$.

- $k = 2s \neq 2$ and $p = 2$. Now $x = p(up^{k-1})$ is such that $k - 1 < 2s$ so that $l(up^{k-1}) = 2$ and $l(x) = 3$.
- $k > 2s$ and k is odd. Then $k' = k - 1 \geq 2s$ is even. But $2n > k > k' \geq 2s$ gives $s < n$. We get $l(up^{k-1}) = 2$ in every case except when $k' = 2s \neq 2$ and $p = 2$. In this case, we have $x = up^{2s+1} = (up^s)(p^{s+1})$ with up^s an atom. If s is odd, let $s = 2s'+1$ and $u' \in \mathcal{U}(R_{n-s'-1}) \setminus \mathcal{U}(R_{n-s'})$ which exists since $n > s' + 1$. Then $u'p^{s'+1}$ and $u'^{-1}p^{s'+1}$ are atoms such that $x = (up^s)(u'p^{s'+1})(u'^{-1}p^{s'+1})$ which gives $l(x) = 3$. Finally, let s be even. Assume first $s \geq 4$. Since $s - 1 < s < n$ and $n > 2$, there exist $u_1 \in \mathcal{U}(R_{n-s+1}) \setminus \mathcal{U}(R_{n-s+2})$ and $u_2 \in \mathcal{U}(R_{n-2}) \setminus \mathcal{U}(R_{n-1})$ such that u_1p^{s-1} and u_2p^2 are atoms. Set $u_3 = uu_1^{-1}u_2^{-1}$, then $x = (u_3p^s)(u_1p^{s-1})(u_2p^2)$. Inequalities $2 < s - 1 < s$ give $u_3 \in \mathcal{U}(R_{n-s})$. But $u_1u_2 \in \mathcal{U}(R_{n-s+1})$ leads to $u_3 \notin \mathcal{U}(R_{n-s+1})$ so that u_3p^s is an atom and $l(x) = 3$.

(4) Let $s = 2, k = 5$ and $p = 2$, so that $u \in \mathcal{U}(R_{n-2}) \setminus \mathcal{U}(R_{n-1})$. If $l(x) = 3$, there exist $u_i \in \mathcal{U}(R_0)$, $i = 1, 2, 3$ such that $up^5 = (u_1p^{k_1})(u_2p^{k_2})(u_3p^{k_3})$ with $u_ip^{k_i}$ atoms. But $k_1 + k_2 + k_3 = 5$ gives $k_1 = k_2 = 1$ and $k_3 = 3$ or $k_1 = 1$ and $k_2 = k_3 = 2$. Since $u \in \mathcal{U}(R_{n-2}) \setminus \mathcal{U}(R_{n-1})$ and $|\mathcal{U}(R_{n-2})/\mathcal{U}(R_{n-1})| = 2$, there is no solution in both cases. But we have $x = p^3(up^2)$ which gives $l(x) = 4$. □

Theorem 3.6. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p inert and $x = up^k \in R_n$, $u \in \mathcal{U}(R_0)$. Set $s = \inf\{i \in \mathbb{N}^* \mid u \in \mathcal{U}(R_{n-i})\}$. Then*

$$l(x) = \begin{cases} 1 + [k/n] \text{ if } n \text{ does not divide } k \text{ and } k > 2n \\ k/n \text{ if } n \text{ divides } k \text{ and } k \geq 2n \\ 1, 2, 3 \text{ or } 4 \text{ under the assumptions of Lemma 3.5} \end{cases}$$

$$L(x) = k - s + 1$$

Moreover, $\bar{l}(x) = k/n$ and $\bar{L}(x) = k$.

Proof. Under the assumptions of Lemma 3.5, we get $l(x) = 1, 2, 3$, or 4.

Now, let $k \geq 2n$. The least length is obtained by a factorization by the largest atoms, that is to say, by some vp^n, $v \in \mathcal{U}(R_0) \setminus \mathcal{U}(R_1)$. Let $k = qn + r$, $0 \leq r < n$ be the Euclidean division of k by n. Then $q \geq 2$.

If $r = 0$, there exist $v_1, \ldots, v_q \in \mathcal{U}(R_0) \setminus \mathcal{U}(R_1)$ such that $u = v_1 \cdots v_q$ since $|\mathcal{U}(R_0)/\mathcal{U}(R_1)| = p + 1 \geq 3$ (consider the equation $x_1 + \cdots + x_q = a$, $a \in \mathbb{Z}/(p+1)\mathbb{Z}$, $x_1, \ldots, x_q \in \mathbb{Z}/(p+1)\mathbb{Z} \setminus \{0\}$). Then $l(x) = q = k/n$.

If $r \neq 0$, we get $l(x) > q$. Moreover, there exists $v \in \mathcal{U}(R_{n-r})$ such that vp^r is an atom. Then we use the previous method to get a factorization of $uv^{-1}p^{qn}$ and $l(x) = q + 1 = 1 + [k/n]$.

The greatest length is obtained by a factorization by the smallest atoms, that is to say, by $u'p$, $u' \in \mathcal{U}(R_{n-1})$. If $s = 1$, then up is an atom and $L(x) = k$. Let $s > 1$ so that $u \notin \mathcal{U}(R_{n-1})$ and consider a factorization $x = \prod_{i=1}^{t} u_i p^{k_i}$ where the $u_i p^{k_i}$ are atoms such that $k_1 \leq \ldots \leq k_t$. This provides the decreasing sequence $\mathcal{U}(R_{n-k_1}) \subset \ldots \subset \mathcal{U}(R_{n-k_t})$. But $u = u_1 \cdots u_t$ gives $u \in \mathcal{U}(R_{n-k_t})$ so that $s - 1 < k_t$ or $s \leq k_t$. For $k_t = s$, we get the factorization $up^k = (up^s)p^{k-s}$ into $k - s + 1$ atoms. If $k_t > s$, the exponent of p in $x(u_t p^{k_t})^{-1}$ is less than $k - s$, which gives a factorization of x with smaller length. So $L(x) = k - s + 1$ in any case.

Consider now the asymptotic behavior. Let $m \in \mathbb{N}^*$ so that $x^m = u^m p^{mk}$. For large values of m, we get $mk \geq 2n$ so $l(x^m) = [km/n] + a$, where $a = 0$ or 1 and $\bar{l}(x) = \lim_{m \to \infty} l(x^m)/m = k/n$. In the same way, we get $L(x^m) = km - s_m + 1$ where $s_m = \inf\{i \in \mathbb{N}^* \mid u^m \in \mathcal{U}(R_{n-i})\}$. But $1 \leq s_m \leq n$ so that $\bar{L}(x) = k$. □

Theorem 3.7. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p ramified and $p \sim p'^2$ in R_0, and set $m = 2n + 1$.*

Let $x = up'^k \in R_n$, $u \in \mathcal{U}(R_0)$. If k is odd, then $k \geq 2n + 1$; if k is even, set $x = u'p^{k'}$ where $k' = k/2$, $u' \in \mathcal{U}(R_0)$, $s = \inf\{i \in \mathbb{N}^* \mid u' \in \mathcal{U}(R_{n-i})\}$. If m divides k, set $a = 0$; otherwise set $a = 1$. Then

$$l(x) = \begin{cases} [k/(2n+1)] + a, \text{ if } k > 2n \\ 1, 2, 3 \text{ or } 4 \text{ under the assumptions of Lemma 3.5} \end{cases}$$

$$L(x) = \begin{cases} k/2 - s + 1 \text{ if } k \text{ is even} \\ (k+1)/2 - n \text{ if } k \text{ is odd} \end{cases}$$

Moreover, $\bar{l}(x) = k/(2n+1)$ and $\bar{L}(x) = k/2$.

Proof. By Proposition 3.3, the atoms of R_n are of the form up^k as in Proposition 3.2 and the up'^{2n+1} for any $u \in \mathcal{U}(R_0)$. Let $x = up'^k \in R_n$, $u \in \mathcal{U}(R_0)$. If $k \leq 2n$, we get that k is even and assumptions of Lemma 3.5 hold, so $l(x) = 1, 2, 3$ or 4.

Assume $k \geq 2n+1 = m$. Set $k = qm + r$, $0 \leq r < m$. The largest atoms are the vp'^{2n+1} for any $v \in \mathcal{U}(R_0)$. If $r = 0$, we can write $x = up'^{qm}$ so that $l(x) = q$. If $r \neq 0$, we get $m+1 \leq m+r < 2m$ and $q \geq 1$. There exist $u'', u_1, u_2 \in \mathcal{U}(R_0)$, $k_1, k_2 \in \mathbb{N}^*$ such that $u_i p'^{k_i}$ are atoms with $up'^k = u''p'^{(q-1)m}(u_1 p'^{k_1})(u_2 p'^{k_2})$ (we have to consider two cases according to the evenness of $m+r$). So $l(x) = q+1$.

The smallest atoms are of the form vp, $v \in \mathcal{U}(R_{n-1})$. If k is even, set $k = 2k'$ so that $x = u'p^{k'}$ with $u' \in \mathcal{U}(R_0)$ and $s = \inf\{i \in \mathbb{N}^* \mid u' \in \mathcal{U}(R_{n-i})\}$. Proof of Theorem 3.6 is again valid and shows that $L(x) = k' - s + 1 = k/2 - s + 1$. If k is odd, p'^{2n+1} appears at last one time in the factorization of x. But, we can write $x = (u''p'^{2n+1})p^{\frac{k-(2n+1)}{2}}$, $u'' \in \mathcal{U}(R_0)$, which gives $L(x) = 1 + (k-(2n+1))/2 = (k+1)/2 - n$.

Consider now the asymptotic behavior. Let $m \in \mathbb{N}^*$ so that $x^m = u^m p'^{mk}$. For large values of m, we get $mk > 4n$ so $l(x^m) = [km/(2n+1)] + a$, where $a = 0$ or 1 and $\bar{l}(x) = k/(2n+1)$. In the same way, we get $L(x^m) = km/2 + b$ where $b = 1 - s$ or $1/2 - n$ so that $\bar{L}(x) = k/2$. □

Theorem 3.8. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p decomposed and $p = p_1p_2$ where p_i are two atoms of R_0 for $i = 1,2$. Let $x = up_1^{k_1}p_2^{k_2} \in R_n$, $u \in \mathcal{U}(R_0)$. Then $k_1, k_2 \neq 0$ and $k_1 = k_2$ if $\inf(k_1,k_2) < n$. Set $s = \inf\{i \in \mathbb{N}^* \mid u \in \mathcal{U}(R_{n-i})\}$. Then*

$$l(x) = \begin{cases} 1,2,3 \text{ or } 4 \text{ under assumptions of Lemma 3.5} \\ 1 \text{ if } \inf(k_1,k_2) = n \text{ with } k_1 \neq k_2 \\ 3 \text{ if } \inf(k_1,k_2) = 2n,\ k_1 = k_2,\ p = 2,\ n > 4 \text{ or } n = 3, s \neq 1 \text{ or } n = 4, s \neq 3 \text{ or } p = 3,\ n = s > 1 \\ \text{or } |k_1 - k_2| = 1,\ p = 2 \\ 4 \text{ if } k_1 = k_2 = 2n,\ p = 2,\ n = 2 \text{ or } n = 3, s = 1 \text{ or } n = 4, s = 3 \\ 2 \text{ in the other cases} \end{cases}$$

$$L(x) = \begin{cases} \inf(k_1,k_2) + 1 - s \text{ if } k_1 = k_2 \\ \inf(k_1,k_2) + 1 - n \text{ if } k_1 \neq k_2 \end{cases}$$

Moreover, $\bar{L}(x) = \inf(k_1,k_2)$ and $\bar{l}(x) = 0$.

Proof. By Proposition 3.4, the atoms of R_n are the vp^k as in Proposition 3.2 and the $vp_1{}^n p_2{}^{n+m}, vp_1{}^{n+m}p_2{}^n$ for any $v \in \mathcal{U}(R_0)$, $m \in \mathbb{N}^*$. Let $x = up_1{}^{k_1}p_2{}^{k_2} \in R_n$, $u \in \mathcal{U}(R_0)$. Then $k_1, k_2 \neq 0$ and $k_1 = k_2$ if $\inf(k_1,k_2) < n$. In this case, $x = up^k$ with $k < n$ and results are those of Lemma 3.5 for $l(x)$ and Proposition 3.6 for $L(x)$.

- Assume $n \leq \inf(k_1,k_2) < 2n$. If $k_1 = k_2$, only atoms of the form $vp^{k'}$ factorize x and we use again Lemma 3.5. Let $k_1 \neq k_2$ and assume $k_1 < k_2$. As the largest atoms are of the form $vp_1{}^n p_2{}^{n+m}$, $vp_1{}^{n+m}p_2{}^n$ for any $v \in \mathcal{U}(R_0)$ and $m \in \mathbb{N}^*$, we can write $x = (u''p^{k_1-n})(uu''^{-1}p_1^n p_2^{k_2+n-k_1})$, where $u''p^{k_1-n}$ is an atom, if $k_1 > n$, so that $l(x) = 2$ and $l(x) = 1$ if $k_1 = n$.

- Assume $2n = \inf(k_1,k_2) = k_1$.

  * If $k_1 = k_2$, we get $x = up^{2n}$. Proof of Theorem 3.6 works if $|\mathcal{U}(R_0)/\mathcal{U}(R_1)| = p - 1 \geq 3$, that is if $p \neq 2,3$ or if $n = 1$. In this case, $l(x) = 2$.

- Let $p = 2$, so that $\mathcal{U}(R_0) = \mathcal{U}(R_1)$. The largest atoms of R_n are of the form vp^{n-1}, $v \in \mathcal{U}(R_0)$, so that $l(x) > 2$. In fact, we can write $up^{2n} = \prod_{i=1}^{3} u_i p^{k'_i}$, $u_i \in \mathcal{U}(R_0)$, with $u_i p^{k'_i}$ an atom, so that $l(x) = 3$ in any case (write $2n = (n-1) + (n-1) + 2 = (n-1) + (n-2) + 3$), except when $n = 2$ or $n = 3, s = 1$ or $n = 4, s = 3$, and in this case, $l(x) = 4$.

- Let $p = 3$, so that $|\mathcal{U}(R_0)/\mathcal{U}(R_1)| = 2$. The largest atoms of R_n are of the form vp^n, $v \in \mathcal{U}(R_0) \setminus \mathcal{U}(R_1)$.

  If $s < n$, we write $up^{2n} = (u_1 p^n)(u_1^{-1} u p^n)$, $u_1 \in \mathcal{U}(R_0) \setminus \mathcal{U}(R_1)$ which gives $l(x) = 2$.

  If $s = n > 1$, we cannot write $up^{2n} = (u_1 p^n)(u_2 p^n)$, with $u_1, u_2 \in \mathcal{U}(R_0) \setminus \mathcal{U}(R_1)$ but $up^{2n} = p(up^{2n-1})$, with $2n - 1 < 2s$ gives $l(x) = 3$ by Lemma 3.5. If $s = n = 1$, we get $l(x) = 2$.

  * If $k_1 < k_2$, we get $l(x) = 2$ except if $k_2 = k_1 + 1$ and $p = 2$. In this case, $l(x) = 3$.

- Let $\inf(k_1, k_2) > 2n$. We can write $x = (up_1^n {p_2}^{k_2 - n})({p_1}^{k_1 - n} p_2^n)$ so that $l(x) = 2$.

  The smallest atoms of R_n are of the form $u'p$ with $u' \in \mathcal{U}(R_{n-1})$. If $k_1 = k_2$, we can argue as in Theorem 3.6 and $L(x) = k_1 - s + 1$. Assume $k_1 \neq k_2$, for instance, $k_1 < k_2$, so that $n \leq k_1 < k_2$. We can then write $x = (up_1^n {p_2}^{k_2 + n - k_1}) p^{k_1 - n}$ and $L(x) = 1 + k_1 - n$.

  Consider now the asymptotic behavior. Let $m \in \mathbb{N}^*$ so that $x^m = u^m {p_1}^{mk_1} {p_2}^{mk_2}$. It is obvious that $\bar{l}(x) = 0$ and $\bar{L}(x) = \inf(k_1, k_2)$. □

These results allow a concrete application of the following result of D.D. Anderson, D.F Anderson, S.T. Chapman, and W.W. Smith [2, Theorem 12] to the monoid of nonzero elements of a local order.

Theorem 3.9. *Let H be an atomic monoid and $x \in H$ a nonunit such that $\{y \in H \mid y$ divides x^n for some integer $n \geq 1\}$ has only a finite number of nonassociate irreducible elements. Then $\bar{L}_H(x)$ and $\bar{l}_H(x)$ are each positive rational numbers. Moreover, there are integers $m, n \geq 1$ such that $\bar{l}_H(x) = l_H(x^{km})/km$ and $\bar{L}_H(x) = L_H(x^{kn})/kn$ for all integers $k \geq 1$.*

In our situation, we know exactly the values of m and n.

Theorem 3.10. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, $n \in \mathbb{N}^*$, p inert or ramified and $x \in R_n$ a nonzero nonunit. There are $m, m' \in \mathbb{N}^*$ such that $\bar{l}(x) = l(x^{rm})/rm$ and $\bar{L}(x) = L(x^{rm'})/rm'$ for all $r \in \mathbb{N}^*$. For instance, $m = 2n$, $m' = p^{n-1}(p+1)$ if p is inert and $m = 2n + 1$, $m' = p^n$ if p is ramified.*

Proof. Let p be inert and $x = up^k \in R_n$, $u \in \mathcal{U}(R_0)$. By Proposition 3.6, we have $\bar{l}(x) = k/n$ and $\bar{L}(x) = k$. Set $m = 2n$ and $m' = p^{n-1}(p+1)$ and take any $r \in \mathbb{N}^*$. Then $x^{rm} = u^{rm} p^{2rkn}$ and $l(x^{rm})/rm = 2rkn/2rn^2 = \bar{l}(x)$. In the same way, $x^{rm'} = u^{rp^{n-1}(p+1)} p^{rkp^{n-1}(p+1)} \sim p^{rkp^{n-1}(p+1)}$ in R_n since $|\mathcal{U}(R_0)/\mathcal{U}(R_n)| = p^{n-1}(p+1)$, so that $s_{x^{rm'}} = 1$. Then $L(x^{rm'})/rm' = rkp^{n-1}(p+1)/rp^{n-1}(p+1) = \bar{L}(x)$.

Let $p \sim p'^2$ in R_0 ramified and $x = up'^k \in R_n$, $u \in \mathcal{U}(R_0)$. By Proposition 3.7, we have $\bar{l}(x) = k/(2n+1)$ and $\bar{L}(x) = k/2$. Set $m = 2n + 1$, $m' = 2p^n$ and take any $r \in \mathbb{N}^*$. Then $x^{rm} = u^{rm} p'^{rk(2n+1)}$ and $l(x^{rm})/rm = rk/r(2n+1) = \bar{l}(x)$. In the same way, $x^{rm'} = u^{2rp^n} p'^{2rkp^n} \sim p'^{2rkp^n}$ in R_n since $|\mathcal{U}(R_0)/\mathcal{U}(R_n)| = p^n$, so that $s_{x^{rm'}} = 1$. Then $L(x^{rm'})/rm' = rkp^n/2rp^n = \bar{L}(x)$. □

Remark. This theorem does not hold for p decomposed since $\bar{l}(x) = 0$ for any nonzero nonunit $x \in R_n$. In fact, $\{y \in R_n \mid y$ divides x^k for some $k \in \mathbb{N}^*\}$ has an infinite number of nonassociate atoms. For instance, if $x = p^n = {p_1}^n {p_2}^n$, we get that ${p_1}^n {p_2}^{n+mn}$ is an atom which divides x^{m+2} for each $m \in \mathbb{N}^*$.

4. ELASTICITY OF A WEAKLY FACTORIAL QUADRATIC ORDER

Since the two length functions $l(x)$ and $L(x)$ are known for every nonzero nonunit element x of a weakly factorial quadratic order R, it is quite easy to calculate the elasticity of R. Indeed, $\rho(R) = \sup\{\rho(x) \mid x \in R \setminus \mathcal{U}(R),\ x \neq 0\}$ where we set $\rho(x) = L(x)/l(x)$ (note that $\rho(x) = 1$ if x is an atom). It is enough to work with a local order R with finitely many atoms in $\bar{R}$. The following theorem gives a relation between elasticities of an order and its localizations.

Theorem 4.1. *Let $R = \mathbb{Z}[n\omega]$, $n \in \mathbb{N}^*$ be a weakly factorial quadratic order.*

Then $\rho(R) = \sup\{\rho(R_P) \mid P \in \mathrm{Max}(R),\ n \in P\}$.

Proof. We apply the result of D.D. Anderson and D.F. Anderson [1, Corollary 2.15] to one-dimensional domains which gives $\rho(R) = \sup\{\rho(R_P) \mid P \in \mathrm{Max}(R)\}$. Moreover, the conductor of R is $n\bar{R}$. For $P \in \mathrm{Max}(R)$ such that $n \notin P$, we get that $R_P = (\bar{R})_P$, with $(\bar{R})_P$ a PID, so $\rho(R_P) = 1$. □

So, we have to reduce to the local case and consider the three possible decompositions of a prime p.

Proposition 4.2. *Let $R = \mathbb{Z}'[p^n\omega]$ be a local order, p a decomposed prime and $n \in \mathbb{N}^*$. Then $\rho(R) = \infty$.*

Proof. $l(x) \leq 4$ for any nonzero nonunit $x \in R$ but $L(x)$ can take any value $k \in \mathbb{N}^*$ (Proposition 3.8). □

Proposition 4.3. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, p an inert prime and $n \in \mathbb{N}^*$. Then $\rho(R_n) = n$.*

Proof. Let $x = up^k \in R_n$, $u \in \mathcal{U}(R_0)$ and use Proposition 3.6 and Lemma 3.5. Set $s = \inf\{i \in \mathbb{N}^* \mid u \in \mathcal{U}(R_{n-i})\}$. Assume that x is not an atom. If $k \leq 2n$, then $l(x) \geq 2$ and $L(x) \leq 2n$ gives $\rho(x) \leq n$. If $k > 2n$ we get also $\rho(x) \leq n$ and $\rho(p^{3n}) = n$ so that $\rho(R_n) = n$. □

Proposition 4.4. *Let $R_n = \mathbb{Z}'[p^n\omega]$ be a local order, p a ramified prime and $n \in \mathbb{N}^*$. Then $\rho(R_n) = n + \frac{1}{2}$.*

Proof. Let $x = up'^k \in R_n$, $u \in \mathcal{U}(R_0)$, where $p \sim p'^2$ in R_0 and use Proposition 3.7 and Lemma 3.5. Assume that x is not an atom. If $k \leq 2n$, then $l(x) \geq 2$ and $L(x) \leq n$ gives $\rho(x) \leq n/2$. Let $k \geq 2n+1$. Thus $L(x) \leq k/2$ and $l(x) \geq k/(2n+1)$ gives $\rho(x) \leq n + 1/2$. Now, consider $x = p'^{2k(2n+1)}$ so that $\rho(x) = n + 1/2$ and $\rho(R_n) = n + 1/2$. □

Gathering these different cases and globalizing, we obtain the following.

Theorem 4.5. *Let $R = \mathbb{Z}[n\omega]$ be a weakly factorial quadratic order with $n = \prod p_i^{e_i}$, p_i prime integers, $e_i \geq 1$. If one of the p_i is decomposed, $\rho(R) = \infty$. If not, we have $\rho(R) = \sup(\{e_i + \frac{1}{2} \mid p_i$ ramified$\}$,$\{e_i \mid p_i$ inert$\})$.*

We recall here the following result of F. Halter-Koch.

Theorem 4.6. [8, Corollary 4] *Let R be an order in an algebraic number field and $\bar{R}$ its integral closure.*

1. *If for some prime ideal P of R there is more than one prime ideal of $\bar{R}$ lying over P, then $\rho(R) = \infty$.*
2. *If for every prime ideal P of R there is exactly one prime ideal of $\bar{R}$ lying over P, then $\rho(R)$ is realized by a factorization and $\rho(R)$ is rational.*

Remarks

(1) Let $R = \mathbb{Z}[n\omega]$ be a weakly factorial quadratic order such that a decomposed prime p divides n and let P be the maximal ideal of R containing p. There are two prime ideals in $\bar{R}$ lying over P so $\rho(R) = \infty$.

(2) We can remark that in the local case and for any prime, $\rho(R) = \bar{L}(x)/\bar{l}(x)$, for any nonzero nonunit $x \in R$.

In [5, Theorem 1.4] S.T. Chapman and J.C. Rosales obtained the following result. A Krull monoid M with $\mathcal{C}(M)$ a torsion group is half-factorial if and only if $\bar{l}(x) = \bar{L}(x) = 1$ for every irreducible $x \in M$. This result can be extended to the case of weakly factorial quadratic orders.

Theorem 4.7. *Let R be a weakly factorial quadratic order. Then R is half-factorial if and only if $\bar{l}(x) = \bar{L}(x)$ for every atom $x \in R$.*

Proof. One implication is obvious. Assume that $\bar{l}(x) = \bar{L}(x)$ for any atom $x \in R$. We can limit to the local case by [12, Proposition 14] and Proposition 1.4 since any atom is primary. Remark 2 gives $\rho(R) = 1$ and R is half-factorial. We could also use [5, Proposition 1.2] of S.T. Chapman and J.C. Rosales, which omits the Krull assumption but requires $\bar{l}(x) = \bar{L}(x)$ for any nonunit x. □

ACKNOWLEDGEMENT

The author wishes to thank one of the referees for showing her the link between torsionfree cancellation and weak factoriality for quadratic orders and both referees for their suggestions.

REFERENCES

[1] D.D. Anderson and D.F. Anderson, "Elasticity of Factorizations in Integral Domains", *J. Pure Appl. Algebra*, **80** (1992), pp. 217–235.

[2] D.D. Anderson, D.F. Anderson, S.T. Chapman, and W.W. Smith, "Rational Elasticity of Factorizations in Krull Domains", *Proc. Amer. Math. Soc.*, **117** (1993), pp. 37–43.

[3] D.D. Anderson and L.A. Mahaney, "On Primary Factorizations", *J. Pure Appl. Algebra*, **54** (1988), pp. 141–154.

[4] D.F. Anderson and P. Pruis, "Length Functions on Integral Domains", *Proc. Amer. Math. Soc.*, **113** (1991), pp. 933–937.

[5] S.T. Chapman and J.C. Rosales, "On the Asymptotic Values of Length Functions in Krull and Finitely Generated Commutative Monoids", preprint.

[6] D.A. Cox, *Primes of the Form $x^2 + ny^2$*. New York: Wiley, 1989.

[7] H.M. Edwards, *Fermat's Last Theorem*. Berlin: Springer GTM, 1977.

[8] F. Halter-Koch, "Elasticity of Factorizations in Atomic Monoids and Integral Domains", *J. Théorie des Nombres de Bordeaux*, **7** (1995), pp. 367–385.

[9] F. Halter-Koch, "Divisor Theories with Primary Elements and Weakly Krull Domains", *Boll. U. M. I.*, **9-B** (1995), pp. 417–441.

[10] H. Hasse, *Number Theory*. Berlin: Springer, 1980.

[11] J. Neukirch, *Algebraische Zahlentheorie*. Berlin: Springer, 1992.

[12] M. Picavet-L'Hermitte, Factorization in Some Orders with a PID as Integral Closure", in *Algebraic Number Theory and Diophantine Analysis*. Berlin and New York: de Gruyter, 2000, pp. 365–390.

[13] R.J. Valenza, "Elasticity of Factorization in Number Fields", *J. Number Theory*, **36** (1990), pp. 212–218.

[14] R. Wiegand, "Cancellation over Commutative Rings of Dimension One and Two", *J. Algebra*, **88** (1984), pp. 438–459.

[15] A. Zaks, "Half-Factorial Domains", *Bull. Amer. Math. Soc.*, **82** (1976), pp. 721–723.

Paper Received 4 October 2000; Accepted 22 April 2001.