Some Diophantine equations associated to seminormal Cohen-Kaplansky domains

Abdallah Badra, Martine Picavet-L'Hermitte

SOME DIOPHANTINE EQUATIONS ASSOCIATED TO SEMINORMAL COHEN-KAPLANSKY DOMAINS

ABDALLAH BADRA AND MARTINE PICAVET-L'HERMITTE

ABSTRACT. A Cohen-Kaplansky domain (CK domain) R is an integral domain where every nonzero nonunit element of R is a finite product of irreducible elements and such that R has only finitely many nonassociate irreducible elements. In this paper, we investigate seminormal CK domains and obtain the form of their irreducible elements. The solutions of a system of diophantine equations allow us to give a formula for the number of distinct factorizations of a nonzero nonunit element of R, with an asymptotic formula for this number.

1. INTRODUCTION

Let R be an *atomic* integral domain, that is, each nonzero nonunit element of R can be written as a finite product of irreducible elements (or *atoms*). The simplest situation is when R has only a finite number of (nonassociate) atoms. Such a domain R was called a *Cohen-Kaplansky domain (CK domain)* by D.D. Anderson and J.L. Mott in [2] who obtained many conditions equivalent to R being a CK domain, after I.S. Cohen and I. Kaplansky [4] inaugurated the study of CK domains. In Section 2 we recall and give basic results on CK domains.

An atomic domain R is called a *half-factorial* domain (*HFD*) if each factorization of a nonzero nonunit element of R into a product of atoms has the same length (Zaks [15]). A ring R is called *seminormal* if whenever $x, y \in R$ satisfy $x^3 = y^2$, there is $a \in R$ with $x = a^2,\ y = a^3$ [14]. Section 3 is devoted to the study of seminormal CK domains. In particular, we show that a seminormal CK domain is half-factorial and obtain some equivalent conditions for a CK domain to be seminormal. As factorization properties of CK domains and seminormality are preserved by localization, we consider a local seminormal CK domain R. Let $\bar{R}$ be its integral closure. Then $\bar{R}$ is a DVR with maximal ideal $\bar{R}p$, which is also the maximal ideal of R. Moreover the atoms of R are of the form vp, where v is a unit of $\bar{R}$. If $\mathcal{U}(\bar{R})$ (resp. $\mathcal{U}(R)$) is the group of units of $\bar{R}$ (resp. R), the factor group $\mathcal{U}(\bar{R})/\mathcal{U}(R)$ is a finite cyclic group. Let $\bar{u}$ be a generator of $\mathcal{U}(\bar{R})/\mathcal{U}(R)$ and n the order of $\bar{u}$. If $x = vp^k$ is a nonzero nonunit element of R with $\bar{v} = \bar{u}^r,\ r \in \{0, \dots, n-1\}$, in $\mathcal{U}(\bar{R})/\mathcal{U}(R)$, the distinct factorizations of x in R into atoms are

---

2000 *Mathematics Subject Classification.* Primary 11D04, 1315; Secondary 13A05, 20M14.

Key words and phrases. CK domain, half-factorial, seminormal, t-closed, diophantine equations.

deduced from the system of diophantine equations in $(a_1, \dots, a_n) \in \mathbb{N}^n$:

$$(S) \quad \begin{cases} \displaystyle\sum_{i=1}^{n} a_i = k \\ \displaystyle\sum_{i=1}^{n} \overline{ia_i} = \bar{r} \text{ in } \mathbb{Z}/n\mathbb{Z} \end{cases}$$

The calculation of the number of solutions of this system is the object of Section 4. If we denote by $\eta(x)$ the number of non-associated irreducible factorizations of x into atoms, we get that $\eta(x)$ is the number of solutions of the system (S).

Section 5 ends this paper with the asymptotic behaviour of the function η where we use the following result by F. Halter-Koch :

Theorem 1.1. [6, Theorem 1]. *Let H be an atomic monoid such that each nonunit x has finitely many non-associated factorizations into irreducibles. Suppose that there are only finitely many irreducible elements of H which divide some power of x. There exists two constants $A \in \mathbb{Q}$ and $d \in \mathbb{N}$, $A > 0$ such that $\eta(x^n) = An^d + O(n^{d-1})$.*

An explicit value for A and d is obtained for a local seminormal CK domain.

For a ring R, we denote by $\mathrm{Max}(R)$ the set of maximal ideals of R and by $\mathcal{U}(R)$ its group of units. Let $x, y \in R$. We say that x and y are *associates* ($x \sim y$) if there exists $u \in \mathcal{U}(R)$ such that $x = uy$. For an integral domain R, we denote by $\bar{R}$ its integral closure. The conductor $[R : \bar{R}]$ of an integral domain R in its integral closure is called 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 $[x] = \sup\{n \in \mathbb{Z} \mid n \leq x\}$.

2. Basic results on CK domains

We first recall some of useful results concerning CK domains.

Theorem 2.1. [2, Theorem 4.3] *For an integral domain R, the following statements are equivalent.*

1. *R is a CK domain.*
2. *$\bar{R}$ is a semilocal PID with $\bar{R}/[R : \bar{R}]$ finite and $|\mathrm{Max}(R)| = |\mathrm{Max}(\bar{R})|$.*
3. *R is a one-dimensional semilocal domain with R/M finite for each nonprincipal maximal ideal M of R, $\bar{R}$ is a finitely generated R-module (equivalently, $[R : \bar{R}] \neq 0$), and $|\mathrm{Max}(R)| = |\mathrm{Max}(\bar{R})|$.*

This theorem implies the following properties.

Proposition 2.2. [2, Theorem 4.3, Theorem 3.1, Theorem 2.1 and Corollary 2.5] *Let R be a CK domain. Then*

1. *R is Noetherian and for each $x \in \bar{R}$, there exists an $n \in \mathbb{N}^*$ with $x^n \in R$.*
2. *$\mathcal{U}(\bar{R})/\mathcal{U}(R)$ is a finite group.*
3. *R_M is a CK domain for each maximal ideal M of R. In particular, $\bar{R}_M$ is a DVR.*
4. *Let T be an overring of R. Then T is also a CK domain.*
5. *The atoms of R are primary.*

D.D. Anderson and J.L. Mott [2] say that a pair of rings $R \subset S$ is a *root extension* if for each $s \in S$, there exists an $n = n(s) \in \mathbb{N}^*$ with $s^n \in R$. For such an extension we have $|\operatorname{Max}(R)| = |\operatorname{Max}(S)|$. Hence $R \subset \bar{R}$ is a root extension when R is a CK domain.

Proposition 2.3. *Let R_1 and R_2 be two CK domains with the same integral closure R'. Then $R = R_1 \cap R_2$ is a CK domain with integral closure R'.*

Proof. Set $R = R_1 \cap R_2$. Define $I_1 = [R_1 : R']$, $I_2 = [R_2 : R']$ and $I = [R : R']$. Then $I_1 \cap I_2$ is a common ideal of R' and R contained in I so that $I \neq 0$. Let $a, b \in R'$ with $b \neq 0$ and i a nonzero element of I. Then ia and ib are in R and hence $a/b = ia/ib$ shows that R has the same quotient field as R'. Moreover, $R \subset R'$ is a root extension. Then R' is obviously the integral closure of R and is a semilocal PID. Since R'/I_1 and R'/I_2 are finite, this gives that $R'/(I_1 \cap I_2)$ is also finite because isomorphic to a subring of $R'/I_1 \times R'/I_2$, so that R'/I is finite.

Moreover, we have $|\operatorname{Max}(R)| = |\operatorname{Max}(R')|$ because $R \subset R'$ is a root extension. Applying Theorem 2.1, (2), we get that R is a CK domain with integral closure R'. □

Corollary 2.4. *Let D be a DVR with maximal ideal M such that D/M is finite. Let I be a nonzero ideal of D. The set of underrings of D with integral closure D and with conductor I has a least element and all these underrings are CK domains.*

Proof. Set $\mathcal{E} = \{R \text{ underring of } D \mid \bar{R} = D,\ [R : D] = I\}$. Since D/M is finite, so is D/I. Indeed, if $M = Dp$ for some atom $p \in D$, then $I = Dp^n$, for some integer n and an obvious induction shows that $|D/I| = |D/M|^n$. Consider $R \in \mathcal{E}$. Then the finiteness of D/I implies the finiteness of R/I. So D is a finitely generated R-module because D/I is a finitely generated R/I-module. It follows that $|\operatorname{Max}(R)| = 1$ and R is a CK domain by Theorem 2.1, (2).

Since D/I is finite, there are finitely many subrings of D/I, and so finitely many $R \in \mathcal{E}$. Let R and $S \in \mathcal{E}$ and set $T = R \cap S$. By Proposition 2.3, T is a CK domain with conductor $J \supset I$. But $T \subset R$ implies $J \subset I$, so that $J = I$ and $T \in \mathcal{E}$. Therefore the intersection of all elements of $\mathcal{E}$ is a CK domain with conductor I and integral closure D and is the least element of $\mathcal{E}$. □

3. Characterization of seminormal CK domains

Let R be an integral domain with quotient field K. We say that R is *t-closed* if whenever $x \in K$ and $x^2 - rx, x^3 - rx^2 \in R$ for some $r \in R$, then $x \in R$ [9]. A t-closed integral domain is seminormal. Recall that an integral domain R is said to be a *pseudo-valuation domain* (PVD) if there exists a valuation overring V of R such that $\operatorname{Spec}(R) = \operatorname{Spec}(V)$ [8] and an integral domain R is said to be a *locally pseudo-valuation domain* (locally PVD) if each of its localizations at a prime ideal is a PVD [5].

Proposition 3.1. *Let R be a one-dimensional Noetherian integral domain such that its integral closure $\bar{R}$ is a finitely generated R-module. The following conditions are equivalent :*

1. *R is seminormal and the canonical map $\operatorname{Spec}(\bar{R}) \to \operatorname{Spec}(R)$ is bijective.*
2. *R is t-closed.*
3. *R is a locally PVD.*
4. *The conductor I of R is a radical ideal in $\bar{R}$ and $|\operatorname{Max}(R)| = |\operatorname{Max}(\bar{R})|$.*

In particular, a CK domain R is seminormal if and only if R is t-closed.

Proof. (1) $\Leftrightarrow$ (2) is [9, Proposition 3.7].
(2) $\Leftrightarrow$ (3) is [10, Corollary 3.4].
(2) $\Leftrightarrow$ (4) comes from [9, Corollary 3.8 and Proposition 2.8]. Indeed, for any $P \in \mathrm{Max}(R)$, the conductor of R_P is I_P. □

We obtain as a corollary a first characterization of local seminormal (or t-closed) CK domains.

Corollary 3.2. *Let R be a local CK domain with integral closure $\bar{R} \neq R$. Let $\bar{R}p$ be the maximal ideal of $\bar{R}$. Then R is seminormal if and only if $\mathcal{U}(\bar{R})p \subset R$.*

Proof. Assume that R is seminormal. By Proposition 3.1 (4), $\bar{R}p$ is the conductor of R, so that $\mathcal{U}(\bar{R})p \subset \bar{R}p \subset R$.
Conversely, if $\mathcal{U}(\bar{R})p \subset R$, we get that $\mathcal{U}(\bar{R})p^n \subset R$ for any integer n and $\bar{R}p \subset R$ gives that $\bar{R}p$ is the conductor of R so that R is seminormal. □

In the nonlocal case, this condition is not fulfilled :

Corollary 3.3. *Let R be a CK domain with integral closure $\bar{R} \neq R$.*
Let $\bar{R}p_i$, $i = 1, \dots, n$, be the maximal ideals of $\bar{R}$.
Then $\mathcal{U}(\bar{R})p_i \subset R$ for any $i = 1, \dots, n$, implies that R is seminormal and $n = 1$.

Proof. The case $n = 1$ is the previous Corollary. Assume $n > 1$. Any nonunit of $\bar{R}$ is in R. Moreover, $\bar{R}p_1$ and $\bar{R}p_2$ are comaximal ideals of $\bar{R}$. For any $u \in \mathcal{U}(\bar{R})$, there exists $v, w \in \bar{R}$ such that $u = vp_1 + wp_2 \in R$. Then $\bar{R} = R$, a contradiction. □

Corollary 2.4 has a new formulation in the seminormal case.

Corollary 3.4. *Let D be a DVR with maximal ideal M such that D/M is finite. The set of seminormal underrings of D with integral closure D is linearly ordered.*

Proof. Let R be a seminormal proper underring of D. Since its conductor is a radical ideal of D, it has to be M, a maximal ideal in R so that R/M is a subfield of the finite field D/M. But the set of subfields of D/M is linearly ordered.
Let R_1, R_2 be two seminormal proper underrings of D with integral closure D. Their conductor is M and we have, for instance, $R_1/M \subset R_2/M$, which gives $R_1 \subset R_2$. □

Here is a fundamental link between seminormal CK domains and factorization.

Proposition 3.5. *A seminormal CK domain is half-factorial.*

Proof. Let R be a seminormal CK domain and $P \in \mathrm{Max}(R)$. Then R_P is a PVD by Proposition 3.1 and a CK domain by Proposition 2.2 (3). So R_P is a HFD for any $P \in \mathrm{Max}(R)$ [2, Theorem 6.2]. The same holds for R [2, Theorem 6.1]. □

The following theorem gives the additional condition necessary for a CK half-factorial domain to be seminormal.

Theorem 3.6. *Let R be a CK domain with integral closure $\bar{R}$.*
Let $\bar{R}p_i$, $i = 1, \dots, n$, be the maximal ideals of $\bar{R}$. Then R is seminormal if and only if R is a HFD and $\mathcal{U}(\bar{R})p_1 \cdots p_n \subset R$. Moreover, if these conditions are satisfied, we can choose $p_i \in R$ for each $i = 1, \dots, n$.

Proof. We can assume $R \neq \bar{R}$ (the case $R = \bar{R}$ is trivial).

Let R be a seminormal CK domain. Then R is a HFD by the previous Proposition and the conductor I of R is a product of some of the $\bar{R}p_i$. It follows that $\mathcal{U}(\bar{R})p_1 \cdots p_n \subset R$.

Conversely, assume that R is a HFD and $\mathcal{U}(\bar{R})p_1 \cdots p_n \subset R$ and let I be the conductor of R. For each $i = 1, \dots, n$, set $P_i = R \cap \bar{R}p_i$, $R_i = R_{P_i}$ and $\overline{R_i} = \overline{R_{P_i}} = \bar{R}_{P_i}$.

First, we show that we may assume $p_i \in R$ for each $i = 1, \dots, n$.

- If P_i is comaximal with I, then $R_i = \overline{R_i}$ and $p_i/1$ is an atom in R_i [2, Theorem 2.1 (2)]. Then there exists a P_i-primary atom $p \in R$ and $s \in R \setminus P_i$ such that $sp_i = p$, which implies $s \in \mathcal{U}(\bar{R})$, so that $\bar{R}p_i = \bar{R}p$.

- Let P_i be non comaximal with I and let x be a P_i-primary atom in R. There exist $u \in \mathcal{U}(\bar{R})$ and an integer k such that $x = up_i^k$ since $x \notin P_j$ for any $j \neq i$. But R_i is a HFD, which implies that $x/1 \simeq p_i/1$ in $\overline{R_i}$ [2, Theorem 6.3] and so $k = 1$. Then $x \simeq p_i$ in $\bar{R}$.

The assumption can be rewritten $\mathcal{U}(\bar{R})p_1 \cdots p_n \subset R$ with $p_i \in R$ for each $i = 1, \dots, n$. This gives finally $\bar{R}p_1 \cdots p_n \subset I \subset R$ and I is a radical ideal in $\bar{R}$. Moreover, R being a CK domain, we get $|\operatorname{Max}(R)| = |\operatorname{Max}(\bar{R})|$ and thus R is seminormal by Proposition 3.1 (4). □

In the local case, we obtain another characterization for a CK half-factorial domain to be seminormal.

Proposition 3.7. *Let R be a local CK domain with integral closure $\bar{R}$. Then R is seminormal if and only if R is a HFD and has $|\mathcal{U}(\bar{R})/\mathcal{U}(R)|$ nonassociate atoms.*

Proof. We can assume $R \neq \bar{R}$ (the case $R = \bar{R}$ is trivial).

Let R be seminormal. Then R is a HFD by the previous Theorem. Let $\bar{R}p$ be the maximal ideal of $\bar{R}$ and let $a_1, \dots, a_n$ be the nonassociate atoms of R. They are of the form $a_i = u_i p$, $u_i \in \mathcal{U}(\bar{R})$ by [2, Theorem 6.3 (3)]. But since R is seminormal, its conductor is $\bar{R}p$. It follows that $up \in R$ for any $u \in \mathcal{U}(\bar{R})$. Let up, vp be two atoms of R, where $u, v \in \mathcal{U}(\bar{R})$. Then up and vp are associates in R if and only if there exists $w \in \mathcal{U}(R)$ such that $up = wvp$, which is equivalent to $\bar{u} = \bar{v}$ in $\mathcal{U}(\bar{R})/\mathcal{U}(R)$. Hence two atoms up, vp of R, with $u, v \in \mathcal{U}(\bar{R})$, are nonassociates in R if and only if $\bar{u} \neq \bar{v}$ in $\mathcal{U}(\bar{R})/\mathcal{U}(R)$. Then R has $|\mathcal{U}(\bar{R})/\mathcal{U}(R)|$ nonassociate atoms (see also [2, Corollary 5.6]).

Conversely, let R be a HFD with $n = |\mathcal{U}(\bar{R})/\mathcal{U}(R)|$ nonassociate atoms. They are of the form $a_i = u_i p$, $u_i \in \mathcal{U}(\bar{R})$, $i = 1, \dots, n$ and $\{\bar{u}_1, \dots, \bar{u}_n\} = \mathcal{U}(\bar{R})/\mathcal{U}(R)$. It follows that $up \in R$ for any $u \in \mathcal{U}(\bar{R})$. In particular, $p \in R$ so that $p^n \in R$ for any integer $n > 0$ and we get that $\bar{R}p \subset R$. Then $\bar{R}p$ is the conductor of R and R is seminormal. □

A seminormal CK domain has a property which is not too far from unique factorization. In [3], S.T. Chapman, F. Halter-Koch and U. Krause defined an integral domain R to be *inside factorial* with *Cale basis* $\mathcal{Q}$, if, for every nonzero nonunit $x \in R$, there exists some $n \in \mathbb{N}^*$ such that x^n has a unique factorization, up to units, into elements of $\mathcal{Q}$.

Proposition 3.8. *Let R be a seminormal CK domain with integral closure $\bar{R}$. Then R is inside factorial with Cale basis $\{p_1, \dots, p_n\}$, where the $\bar{R}p_i$ are the maximal ideals of $\bar{R}$ with $p_i \in R$ for $i = 1, \dots, n$.*

Proof. We have seen in Theorem 3.6 that we can choose p_i in R, where the $\bar{R}p_i$ are the maximal ideals of $\bar{R}$.
The atoms of R are of the form $u_{ij}p_i$, with $u_{ij} \in \mathcal{U}(\bar{R}),\ i = 1, \dots , n$ [2, Theorem 2.1 (2)]. Let $r = |\mathcal{U}(\bar{R})/\mathcal{U}(R)|$. Then $u^r \in R$ for any $u \in \mathcal{U}(\bar{R})$. Let x be a nonzero nonunit of R. As an element of $\bar{R}$, it can be written $x = u \prod p_i^{\alpha_i},\ u \in \mathcal{U}(\bar{R})$. Then $x^r = u^r \prod p_i^{r\alpha_i}$ with $u^r \in \mathcal{U}(R)$ and this factorization into the p_i is obviously unique. □

Remark 3.9. Under assumptions of the previous Proposition, let e be the exponent of the factor group $\mathcal{U}(\bar{R})/\mathcal{U}(R)$. Then e is the least integer r such that x^r has a unique factorization, up to units, into elements of $\{p_1, \dots , p_n\}$, for every nonzero nonunit $x \in R$. Indeed, e is the least integer r such that $u^r \in \mathcal{U}(R)$ for any $u \in \mathcal{U}(\bar{R})$.

We can calculate this exponent. D.D. Anderson, D.F Anderson and M. Zafrullah call in [1] an atomic domain with almost all atoms prime a *generalized CK domain.* A CK domain is obviously a generalized CK domain. We can still assume $R \neq \bar{R}$. Then, if I is the conductor of R, we have the isomorphism $\mathcal{U}(\bar{R})/\mathcal{U}(R) \simeq \mathcal{U}(\bar{R}/I)/\mathcal{U}(R/I)$ by [11, Theorem 2] (the result was obtained for algebraic orders but a generalization to one-dimensional Noetherian domains R with integral closure which are finitely generated R-modules can be easily made). Since R is seminormal, I is a radical ideal in $\bar{R}$. After a reordering, write $I = \prod_{i=1}^{m} \bar{R}p_i$.

Then $\mathcal{U}(\bar{R})/\mathcal{U}(R) \simeq \prod_{i=1}^{m} \left[\mathcal{U}(\bar{R}/\bar{R}p_i)/\mathcal{U}(R/P_i)\right]$, where $P_i = R \cap \bar{R}p_i$ since $I = \prod_{i=1}^{m} P_i$ as an ideal of R.
Set $q_i = |R/P_i|$ and $k_i = [\bar{R}/\bar{R}p_i : R/P_i]$. Then $e_i = (q_i^{k_i} - 1)/(q_i - 1)$ is the order (and the exponent) of the finite cyclic group $\mathcal{U}(\bar{R}/\bar{R}p_i)/\mathcal{U}(R/P_i)$ and $e = \mathrm{lcm}(e_1, \dots , e_m)$.

We are now able to obtain all the factorizations into atoms of a nonzero nonunit element of a seminormal CK domain with the number of distinct factorizations into atoms. We can restrict to the local case by the following proposition.

Proposition 3.10. *Let R be a CK domain with maximal ideals $P_1, \dots , P_n$. Set $R_i = R_{P_i}$ and define $\eta_i(z)$ to be the number of distinct factorizations into atoms of R_i of a nonzero $z \in R_i$. Then $\eta(x) = \prod_{i=1}^{n} \eta_i(x/1)$ for a nonzero $x \in R$.*

Proof. By [2, Theorem 2.1 (2)], the atoms of R are primary and the atoms of R_i are the P_i-primary atoms of R. Moreover, if x is a nonzero nonunit element of R, then x is written in a unique way $x = x_1 \cdots x_n$, where x_i is a P_i-primary element of R for each $i = 1, \dots , n$ [7, Corollary 1.7]. Indeed, by [1, Corollary 5], a CK domain is *weakly factorial* (such that every nonunit is a product of primary elements), and a weakly factorial domain is a weakly factorial monoid for the multiplicative structure. So, we get $\eta(x) = \prod_{i=1}^{n} \eta(x_i)$ and $\eta(x_i) = \eta_i(x_i/1)$ for each i by [2, Theorem 2.1 (2)] since a factorization of x_i into atoms of R leads to a factorization of $x_i/1$ into atoms of R_i and conversely. □

To end, we give the form of atoms in a local seminormal CK domain.

Theorem 3.11. *Let R be a local seminormal CK domain with integral closure $\bar{R}$. Let $\bar{R}p$ be the maximal ideal of $\bar{R}$, with $p \in R$. Set $n = |\mathcal{U}(\bar{R})/\mathcal{U}(R)|$ and choose $u \in \mathcal{U}(\bar{R})$ such that $\bar{u}$ is a generator of the cyclic group $\mathcal{U}(\bar{R})/\mathcal{U}(R)$. Then*

1. *A set of all nonassociate atoms of R is $\{u^i p \mid i = 0, \dots, n-1\}$.*
2. *Let $x = vp^k$, $k \in \mathbb{N}^*$, $v \in \mathcal{U}(\bar{R})$. Let $r \in \{0, \dots, n-1\}$ be such that $\bar{v} = \bar{u}^r$. The number of nonassociated factorizations of x into atoms of R is equal to the number of solutions $(a_1, \dots, a_n) \in \mathbb{N}^n$ of the system of diophantine equations :*

$$(S) \qquad \begin{cases} \displaystyle\sum_{i=1}^{n} a_i = k \\ \displaystyle\sum_{i=1}^{n} \overline{ia_i} = \bar{r} \text{ in } \mathbb{Z}/n\mathbb{Z} \end{cases}$$

Proof. As above, we can assume $R \neq \bar{R}$. Then $\bar{R}p$ is the conductor of R so that $\bar{R}/\bar{R}p$ is a finite field by Theorem 2.1 (3) and $\mathcal{U}(\bar{R}/\bar{R}p)$ is a finite cyclic group. It follows that $\mathcal{U}(\bar{R})/\mathcal{U}(R) \simeq \mathcal{U}(\bar{R}/\bar{R}p)/\mathcal{U}(R/\bar{R}p)$ (Remark 3.9) is also a finite cyclic group. Let $u \in \mathcal{U}(\bar{R})$ be such that $\bar{u}$ is a generator of $\mathcal{U}(\bar{R})/\mathcal{U}(R)$.

(1) In view of Proposition 3.7, we can choose $\mathcal{A} = \{u^i p\}$, $i = 1, \dots, n$, as a set of nonassociate atoms of R since the u^i are the representatives of the elements of $\mathcal{U}(\bar{R})/\mathcal{U}(R)$ and $u^n p$ is an associate of p in R.

(2) Set $p_i = u^i p$, $i = 1, \dots, n$, and let x be a nonzero nonunit element of R which is not an atom. Then $x = vp^k$, $k > 1$ with a unique $v \in \mathcal{U}(\bar{R})$. A factorization of x into elements of $\mathcal{A}$ is of the form $x = w \displaystyle\prod_{i=1}^{n} p_i^{a_i}$, $w \in \mathcal{U}(R)$, $a_i \in \mathbb{N}$. This gives $x = w \displaystyle\prod_{i=1}^{n} (u^i p)^{a_i} = vp^k$ $(*)$, which implies, by identification in $\bar{R}$, the equalities

$$v = w \prod_{i=1}^{n} u^{ia_i} \text{ and } k = \sum_{i=1}^{n} a_i \qquad (**)$$

Consider another factorization $x = w' \displaystyle\prod_{i=1}^{n} p_i^{a'_i}$, $w' \in \mathcal{U}(R)$, $a'_i \in \mathbb{N}$. We get then $k = \displaystyle\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a'_i$ and $v = w \displaystyle\prod_{i=1}^{n} u^{ia_i} = w' \prod_{i=1}^{n} u^{ia'_i}$. These two factorizations coincide if and only if $a_i = a'_i$ for each i. In this case, we have $w = w'$.

In $\mathcal{U}(\bar{R})/\mathcal{U}(R)$ we have the relation $\bar{v} = \displaystyle\prod_{i=1}^{n} \bar{u}^{ia_i} = \bar{u}^r$ where $r \in \{0, \dots, n-1\}$ by $(**)$, that is $r \equiv \displaystyle\sum_{i=1}^{n} ia_i \pmod{n}$, or equivalently, $\bar{r} = \displaystyle\sum_{i=1}^{n} \overline{ia_i}$ in $\mathbb{Z}/n\mathbb{Z}$. Then $(a_1, \dots, a_n) \in \mathbb{N}^n$ is a solution of the system (S).

Conversely, let $(a'_1, \dots, a'_n) \in \mathbb{N}^n$ satisfying (S).

Set $x' = \displaystyle\prod_{i=1}^{n} p_i^{a'_i} = \prod_{i=1}^{n} (u^i p)^{a'_i} = u^{a'_1 + 2a'_2 + \cdots + na'_n} p^{a'_1 + a'_2 + \cdots + a'_n}$.

But $\sum_{i=1}^{n} ia'_i = r + sn,\ s \in \mathbb{Z}$, gives $x' = u^r(u^n)^s p^k$ and $\bar{v} = \bar{u}^r$ implies $u^r = w'v$, where $w' \in \mathcal{U}(R)$. So we get $x' = w'(u^n)^s vp^k = w'(u^n)^s x$, with $w'(u^n)^s \in \mathcal{U}(R)$ and $x \sim x'$ in R. We deduce that two distinct solutions of (S) give two distinct factorizations of x into atoms of R and the number of nonassociated factorizations of x into atoms of R is equal to the number of solutions $(a_1, \dots, a_n) \in \mathbb{N}^n$ of (S). □

We are going to calculate the number of solutions of such a system in the next section.

4. On the number of solutions of a system of two special diophantine equations

In this section, we use the following notation. Let $n, r \in \mathbb{N},\ k, s \in \mathbb{Z}$ with $n > 0$ and $0 \leq r \leq n-1$. We consider the following systems of diophantine equations in $(a_1, \dots, a_n) \in \mathbb{N}^n$:

$$S(n,k,r) \quad \begin{cases} \sum_{i=1}^{n} a_i = k \\ \\ \sum_{i=1}^{n} \overline{ia_i} = \bar{r} \text{ in } \mathbb{Z}/n\mathbb{Z} \end{cases} \qquad \text{and} \qquad S'(n,k,s) \quad \begin{cases} \sum_{i=1}^{n} a_i = k \\ \\ \sum_{i=1}^{n} ia_i = s \end{cases}$$

We denote respectively by $N(n,k,r)$ and $p(n,k,s)$ the numbers of solutions $(a_1, \dots, a_n) \in \mathbb{N}^n$ of $S(n,k,r)$ and $S'(n,k,s)$. Obviously, we have $N(n,k,r) = p(n,k,r) = 0$ for $k < 0$. It is easy to see that

$$N(n,k,r) = \sum_{i \geq 0} p(n,k,r+in) = \sum_{i=[\frac{k-r}{n}]}^{[k-\frac{r}{n}]} p(n,k,r+in)$$

At last, for $n, k \in \mathbb{N},\ k > 0$, we set :

$$F(n,k,x) = \frac{x^k(1-x^{n+k-1})(1-x^{n+k-2})\cdots(1-x^n)}{(1-x)(1-x^2)\cdots(1-x^k)}$$

where x is a variable.

Remark 4.1. It follows that $p(n,k,s)$ is also the number of partitions of s into k summands $b_j \in \mathbb{N}$ such that $1 \leq b_1 \leq \cdots \leq b_k \leq n$.

Proposition 4.2. *With the previous notation, for $k > 0$, we have $F(n,k,x) = \sum_{s \geq 0} p(n,k,s)x^s$. Moreover, $F(n,k,x)$ is a polynomial in x.*

Proof. The generating function for the numbers $p(n,k,s)$ is the two-variable series $\varphi(x,y) = \sum_{s,k \geq 0} p(n,k,s)x^s y^k = \frac{1}{(1-yx)(1-yx^2)\cdots(1-yx^n)}$ because of

$$\frac{1}{(1-yx)(1-yx^2)\cdots(1-yx^n)} = \prod_{i=1}^{n} \left(\sum_{a_i \geq 0} y^{a_i} x^{ia_i} \right) =$$

$$\sum_{a_1\geq 0,\dots,a_n\geq 0} y^{a_1+\cdots+a_n}x^{a_1+2a_2+\cdots+na_n} = \sum_{k\geq 0,s\geq 0} p(n,k,s)y^kx^s$$

We can write $\varphi(x,y) = \sum_{k\geq 0}\varphi_k(x)y^k$ with $\varphi_k(x) = \sum_{s\geq 0} p(n,k,s)x^s$, for all $k \geq 0$.

We can easily check that $(1-yx^{n+1})\varphi(x,xy) = (1-yx)\varphi(x,y)$, which implies $(1-x^k)\varphi_k(x) = (x-x^{n+k})\varphi_{k-1}(x)$ for $k>0$, so that

$$\varphi_k(x) = \frac{(x-x^{n+k})(x-x^{n+k-1})\cdots(x-x^{n+1})}{(1-x^k)(1-x^{k-1})\cdots(1-x)}\varphi_0(x), \text{ for } k>0.$$

But $\varphi_0(x)=1$. Hence $\varphi_k(x) = F(n,k,x)$ for $k>0$.

To end, F is a polynomial in x since $p(n,k,s)=0$ for large s. □

We can now calculate $N(n,k,r)$.

Theorem 4.3. *With the previous notation, for $k>0$, let $F_0,\dots,F_{n-1}$ be the n-components of $F(n,k,x)$, i.e. $F(n,k,x) = \sum_{r=0}^{n-1} x^rF_r(x^n)$. Then $N(n,k,r) = F_r(1)$.*

Proof. Write $F(n,k,x) = \sum_{j\geq 0} f_jx^j,\ f_j \in \mathbb{Q}$. Then
$F_r(x^n) = \sum_{i\geq 0} f_{r+in}x^{ni} = \sum_{i\geq 0} p(n,k,r+in)x^{ni}$ and $F_r(1) = \sum_{i\geq 0} p(n,k,r+in) = N(n,k,r)$. □

The value of $F_r(1)$ gives then the value of $N(n,k,r)$.

Theorem 4.4. *With the previous notation, set $d=\gcd(n,k)$ for $k,n>0$. Then*

$$N(n,k,r) = \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{k}\sum_{l=1}^{d-1}\left(\cos\left(\frac{2lr\pi}{d}\right)\prod_{1\leq j\leq k-1,d|jl}\left(\frac{n+j}{j}\right)\right)$$

In particular, $N(n,k,r) = \frac{1}{n}\binom{n+k-1}{k}$ for any $r\in\{0,\dots,n-1\}$ when $d=1$.

Proof. We use the relation $F(n,k,x) = \sum_{t=0}^{n-1} x^tF_t(x^n)$. We set $\alpha = e^{\frac{2i\pi}{n}}$. For all $r,m \in \{0,\dots,n-1\}$, we have $\alpha^{-rm}F(n,k,\alpha^m) = \sum_{t=0}^{n-1}\alpha^{tm-rm}F_t(\alpha^{nm}) = \sum_{t=0}^{n-1}\alpha^{(t-r)m}F_t(1)$.

Summing on m we get

$$\sum_{m=0}^{n-1}\alpha^{-rm}F(n,k,\alpha^m) = \sum_{m=0}^{n-1}\left(\sum_{t=0}^{n-1}\alpha^{(t-r)m}F_t(1)\right) =$$

$$\sum_{t=0}^{n-1}\left(\sum_{m=0}^{n-1}\alpha^{(t-r)m}F_t(1)\right) = \sum_{t=0}^{n-1}F_t(1)\left(\sum_{m=0}^{n-1}\alpha^{(t-r)m}\right) = \sum_{t=0}^{n-1}F_t(1)n\delta_{rt} = nF_r(1)$$

So we obtain $F_r(1) = \dfrac{1}{n}\displaystyle\sum_{m=0}^{n-1} \alpha^{-rm} F(n,k,\alpha^m)$.

Now, we have to calculate $u_m = F(n,k,\alpha^m)$, where

$$\begin{aligned} F(n,k,x) &= x^k \frac{(1-x^{n+k-1})(1-x^{n+k-2})\cdots(1-x^{n+1})(1-x^n)}{(1-x^{k-1})(1-x^{k-2})\cdots(1-x)(1-x^k)} \\ &= x^k \frac{x^n-1}{x^k-1}\prod_{j=1}^{k-1}\left(\frac{x^{n+j}-1}{x^j-1}\right) \end{aligned}$$

which is a polynomial in x, so that $F(n,k,\alpha^m)$ has a sense.

Using L'Hopital's rule, we are going to calculate the values of $\dfrac{x^n-1}{x^k-1}$ and $\dfrac{x^{n+j}-1}{x^j-1}$ for $j = 1,\ldots,k-1$, at $x = \alpha^m,\ m = 0,1,\ldots,n-1$.

- If $n \not| \, mk$, then $\dfrac{\alpha^{mn}-1}{\alpha^{mk}-1} = 0$.

If $n|mk$, then $\left[\dfrac{x^n-1}{x^k-1}\right]_{x=\alpha^m} = \displaystyle\lim_{x\to\alpha^m} \frac{nx^{n-1}}{kx^{k-1}} = \frac{n}{k}$. Moreover, in this case, $\alpha^{mk} = 1$.

Let $j \in \{1,\ldots,k-1\}$.

- If $n \not| \, mj$, then $\dfrac{\alpha^{m(n+j)}-1}{\alpha^{mj}-1} = 1$.

If $n|mj$, then $\left[\dfrac{x^{n+j}-1}{x^j-1}\right]_{x=\alpha^m} = \displaystyle\lim_{x\to\alpha^m} \frac{(n+j)x^{n+j-1}}{jx^{j-1}} = \frac{n+j}{j}$.

To sum up, we obtain $u_m = 0$ if $n \not| mk$ and $u_m = \dfrac{n}{k}\displaystyle\prod_{1\le j\le k-1, n|jm} \frac{n+j}{j}$ if $n|mk$.

In particular, $u_0 = \dfrac{n}{k}\displaystyle\prod_{j=1}^{k-1}\frac{n+j}{j} = \frac{n(n+1)\cdots(n+k-1)}{1\cdots(k-1)k} = \binom{n+k-1}{k}$.

Set $d = \gcd(n,k)$ and $n = n'd,\ k = k'd$ so that $\gcd(n',k') = 1$.
Then $n|mk \Leftrightarrow n'|mk' \Leftrightarrow n'|m$.

If $n' \not| m$, then $u_m = 0$

If $n'|m$, set $m = ln'$.

Then $n|mj \Leftrightarrow n'd|ln'j \Leftrightarrow d|lj$ so that $u_{ln'} = \dfrac{n}{k}\displaystyle\prod_{1\le j\le k-1, d|lj}\frac{n+j}{j}$.

This implies

$$\begin{aligned} N(n,k,r) &= \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{n}\sum_{l=1}^{d-1}\alpha^{-rln'}u_{ln'} \\ &= \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{n}\frac{n}{k}\sum_{l=1}^{d-1}\left(\alpha^{-rln'}\prod_{1\le j\le k-1, d|jl}\frac{n+j}{j}\right) \\ &= \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{k}\sum_{l=1}^{d-1}\left(e^{\frac{-2i\pi rln'}{n}}\prod_{1\le j\le k-1, d|jl}\frac{n+j}{j}\right) \end{aligned}$$

which is a real number.

So, we get $N(n,k,r) = \dfrac{1}{n}\dbinom{n+k-1}{k} + \dfrac{1}{k}\displaystyle\sum_{l=1}^{d-1}\left(\cos\left(\dfrac{2lr\pi}{d}\right)\prod_{1\leq j\leq k-1, d|jl}\dfrac{n+j}{j}\right)$.

In particular, if $d = 1$, we get $N(n,k,r) = \dfrac{1}{n}\dbinom{n+k-1}{k}$ since we have an empty sum. □

By the way, keeping the same notation, the following corollary results :

Corollary 4.5. *With the previous notation, we have* $\displaystyle\sum_{r=0}^{n-1} N(n,k,r) = \binom{n+k-1}{k}$.

Proof. It is enough to sum the formula of Theorem 4.4. We can also get it in view of $\displaystyle\sum_{r=0}^{n-1} N(n,k,r) = \sum_{r=0}^{n-1} F_r(1) = F(n,k,1) = \binom{n+k-1}{k}$. □

Remark 4.6. $N(n,k,r)$ is a d-periodic function in r.

Corollary 4.7. *With the previous notation, we have* $N(n,k,r) = N(k,n,r)$.

Proof. We use the formula of Theorem 4.4

$$N(n,k,r) = \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{k}\sum_{l=1}^{d-1}\left(\cos\left(\frac{2lr\pi}{d}\right)\prod_{1\leq j\leq k-1, d|jl}\left(\frac{n+j}{j}\right)\right)$$

where $d = \gcd(n,k)$. If $n = k$, there is nothing to prove. So, assume $n \neq k$.
• It is easily seen that $\dfrac{1}{n}\dbinom{n+k-1}{k} = \dfrac{1}{k}\dbinom{k+n-1}{n}$.
• The result is gotten if we prove that

$$\frac{1}{k}\prod_{1\leq j\leq k-1, d|jl}\left(\frac{n+j}{j}\right) = \frac{1}{n}\prod_{1\leq j\leq n-1, d|jl}\left(\frac{k+j}{j}\right)$$

for any $l \in \mathbb{N}$ such that $1 \leq l \leq d-1$.

For such an l and $a, b \in \mathbb{N}$, set $A(a,b) = \{j \in \mathbb{N} \mid a \leq j \leq b \text{ and } d|jl\}$. We may assume $n > k$. Then

$$\frac{1}{n}\prod_{1\leq j\leq n-1, d|jl}\left(\frac{k+j}{j}\right) = \frac{1}{n}\prod_{j\in A(1,n-1)}\left(\frac{k+j}{j}\right) = \frac{1}{n}\frac{\displaystyle\prod_{j\in A(1,n-1)}(k+j)}{\displaystyle\prod_{j\in A(1,n-1)} j}$$

But

$$\begin{aligned} A(1,n-1) &= A(1,n-k-1) \cup A(n-k+1,n-1) \cup \{n-k\} \\ &= A(k+1,n-1) \cup A(1,k-1) \cup \{k\} \end{aligned}$$

It follows that

$$\prod_{j\in A(1,n-1)}(k+j) = n\left(\prod_{j\in A(1,n-k-1)}(k+j)\right)\left(\prod_{j\in A(n-k+1,n-1)}(k+j)\right)$$

and

$$\prod_{j\in A(1,n-1)} j = k\left(\prod_{j\in A(k+1,n-1)} j\right)\left(\prod_{j\in A(1,k-1)} j\right)$$

Moreover, $j \in A(1, n-k-1) \Leftrightarrow k+j \in A(k+1, n-1)$ since $d|jl \Leftrightarrow d|(k+j)l$.
So we get $\displaystyle\prod_{j\in A(1,n-k-1)} (k+j) = \prod_{j\in A(k+1,n-1)} j$.
In the same way, we have $j \in A(n-k+1, n-1) \Leftrightarrow t = k+j-n \in A(1, k-1)$ since $d|jl \Leftrightarrow d|(k+j-n)l$.
So we get $\displaystyle\prod_{j\in A(n-k+1,n-1)} (k+j) = \prod_{t\in A(1,k-1)} (n+t) = \prod_{j\in A(1,k-1)} (n+j)$.

It follows that

$$\begin{aligned}
\frac{1}{n}\prod_{j\in A(1,n-1)}\binom{k+j}{j} &= \frac{n\left(\prod_{j\in A(k+1,n-1)} j\right)\left(\prod_{j\in A(n-k+1,n-1)} (k+j)\right)}{nk\left(\prod_{j\in A(k+1,n-1)} j\right)\left(\prod_{j\in A(1,k-1)} j\right)} \\
&= \frac{1}{k}\frac{\prod_{j\in A(n-k+1,n-1)} (k+j)}{\prod_{j\in A(1,k-1)} j} = \frac{1}{k}\frac{\prod_{j\in A(1,k-1)} (n+j)}{\prod_{j\in A(1,k-1)} j} \\
&= \frac{1}{k}\prod_{j\in A(1,k-1)}\binom{n+j}{j}
\end{aligned}$$

and we are done. □

When $\gcd(n,k) > 1$, we obtain a simpler evaluation for $N(n,k,r)$.

Theorem 4.8. *With the previous notation, set $d = \gcd(n,k)$ for $k,n > 0$ and assume $d > 1$. Then*

$$N(n,k,r) = \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{k}\sum_{1<\delta\le d,\delta|d}\frac{\varphi(\delta)\mu(\delta/\gcd(r,d))}{\varphi(\delta/\gcd(r,d))}\binom{\frac{n}{\delta}+\frac{k}{\delta}-1}{\frac{n}{\delta}}$$

where φ and μ are respectively the Euler function and the Möbius function.

In particular, we have

$$N(n,k,0) = \frac{1}{n}\binom{n+k-1}{k} + \frac{1}{k}\sum_{1<\delta\le d,\delta|d}\varphi(\delta)\binom{\frac{n}{\delta}+\frac{k}{\delta}-1}{\frac{n}{\delta}}$$

and

$$N(n,k,r) = \frac{1}{n}\binom{n+k-1}{n} + \frac{1}{k}\sum_{1<\delta\le d,\delta|d}\mu(\delta)\binom{\frac{n}{\delta}+\frac{k}{\delta}-1}{\frac{n}{\delta}}$$

when $r > 0$ and $\gcd(r,d) = 1$.

Proof. Set $S = \sum_{l=1}^{d-1} \left(\cos\left(\frac{2lr\pi}{d}\right) \prod_{1\leq j\leq k-1, d|jl} \binom{n+j}{j} \right)$ with the notation of Theorem 4.4. We can write

$$\begin{aligned} S &= \sum_{1\leq\delta'\leq d-1, \delta'|d} \left(\sum_{1\leq l\leq d-1, \gcd(l,d)=\delta'} \left(\cos\left(\frac{2lr\pi}{d}\right) \prod_{1\leq j\leq k-1, d|jl} \binom{n+j}{j} \right)\right) \\ &= \sum_{1<\delta\leq d, \delta|d} \sigma_\delta \end{aligned}$$

where $\delta = \frac{d}{\delta'}$ and

$$\sigma_\delta = \sum_{1\leq l\leq d-1, \gcd(l,d)=\delta'} \left(\cos\left(\frac{2lr\pi}{d}\right) \prod_{1\leq j\leq k-1, d|jl} \binom{n+j}{j} \right)$$

For $\delta' = \gcd(l,d)$, we have $d|jl$ and $1\leq j\leq k \Leftrightarrow \frac{d}{\delta'}$ divides $j\frac{l}{\delta'}$ and $1\leq j\leq k$ $\Leftrightarrow \delta$ divides j and $1\leq j\leq k \Leftrightarrow j = i\delta$ and $1\leq i\leq \frac{k}{\delta}$.

It follows that

$$\prod_{1\leq j\leq k-1, d|jl} \binom{n+j}{j} = \prod_{1\leq i\leq \frac{k}{\delta}-1} \binom{\frac{n}{\delta}+i}{i} = \binom{\frac{n}{\delta}+\frac{k}{\delta}-1}{\frac{n}{\delta}}$$

and

$$\sigma_\delta = \binom{\frac{n}{\delta}+\frac{k}{\delta}-1}{\frac{n}{\delta}} \sum_{1\leq l\leq d-1, \gcd(l,d)=\delta'} \cos\left(\frac{2lr\pi}{d}\right)$$

Consider

$$\begin{aligned} \tau_\delta &= \sum_{1\leq l\leq d-1, \gcd(l,d)=\delta'} \cos\left(\frac{2lr\pi}{d}\right) = \sum_{1\leq l\leq d-1, \gcd(l,d)=\delta'} \cos\left(\frac{2r\pi(\frac{l}{\delta'})}{\delta}\right) \\ &= \sum_{1\leq l'\leq \delta-1, \gcd(l',\delta)=1} \cos\left(\frac{2l'r\pi}{\delta}\right) \end{aligned}$$

where $l' = \frac{l}{\delta'}$.

But τ_δ is also the real part of the Ramanujan sum

$$c(r,\delta) = \sum_{1\leq l'\leq\delta-1, \gcd(l',\delta)=1} e^{\frac{2il'r\pi}{\delta}}$$

We have an explicite representation for $c(r,\delta)$ due to Hölder (see [13, Theorem 7.37, chapter 7, page 464]) by $c(r,\delta) = \frac{\varphi(\delta)\mu(m)}{\varphi(m)}$, where φ and μ are respectively the Euler function and the Möbius function, and where $m = d/\gcd(d, r\delta') = \delta/\gcd(r,\delta)$. Since $c(r,\delta)$ is a real number, we obtain $\tau_\delta = c(r,\delta)$ and the result is gotten.

In particular, we have the following two special cases

- $r = 0$ gives $\tau_\delta = \varphi(\delta)$

  and
- $\gcd(r,d) = 1$ with $r > 0$ gives $\tau_\delta = \mu(\delta)$. □

Example 4.9. We are going to find the distinct factorizations into atoms of an element of a local seminormal CK domain.

Let $\omega = (1+\sqrt{5})/2$ and consider the PID $\mathbb{Z}[\omega]$. Since 2 is inert in $\mathbb{Z}[\omega]$, the ring $S = \mathbb{Z}[2\omega]$ is weakly factorial and t-closed, and so is a generalized CK domain with conductor $2\mathbb{Z}[\omega]$, a maximal ideal in $\mathbb{Z}[\omega]$ [11, Theorem 2] and [12, Example (2), page 177]. Set $R = S_{2\mathbb{Z}[\omega]}$, which is a local seminormal CK domain and 2 is an atom in $\bar{R}$ and R. In view of [12, Theorem 1.2, Proposition 2.1 and Proposition 3.1], we have $|\mathcal{U}(\bar{R})/\mathcal{U}(R)| = 3$. Set $x = 32 = 2^5$. By Theorems 3.11 and 4.4, we get $\eta(x) = \dfrac{1}{3}\dbinom{7}{5} = 7$ since $\gcd(3,5) = 1$. As ω is the fundamental unit of $\mathbb{Z}[\omega]$, its class generates the cyclic group $\mathcal{U}(\bar{R})/\mathcal{U}(R)$. We can choose $p = 2,\ p' = 2\omega,\ p'' = 2\omega^2$ for the nonassociate atoms of R. The different nonassociated factorizations of x into atoms of R are the following:
$x = p^5 = \omega^{-3}p^3p'p'' = \omega^{-3}p^2p'^3 = \omega^{-6}p^2p''^3 = \omega^{-6}pp'^2p''^2 = \omega^{-6}p'^4p'' = \omega^{-9}p'p''^4$.

5. On the asymptotic behaviour of the number of distinct factorizations into atoms in a seminormal CK domain

As we saw in Section 3, we can restrict to the local case to evaluate the number of distinct factorizations into atoms of an element of a CK domain. To calculate this number for some special elements, we use results of Section 4.

Theorem 5.1. *Let R be a local seminormal CK domain with integral closure $\bar{R}$. Let $\bar{R}p$ be the maximal ideal of $\bar{R}$, with $p \in R$. Set $n = |\mathcal{U}(\bar{R})/\mathcal{U}(R)|$.*
Let $x = vp^k,\ k \in \mathbb{N}^*,\ v \in \mathcal{U}(\bar{R})$. The number of nonassociated factorizations of $x^m,\ m \in \mathbb{N}^*$ into atoms of R is of the form $\eta(x^m) = \dfrac{k^{n-1}}{n!}m^{n-1} + O(m^{n-2})$.

In particular, if x is an atom of R, then $\eta(x^m) = \dfrac{1}{n!}m^{n-1} + O(m^{n-2})$.

Proof. We can use Theorem 1.1 since its assumptions are satisfied by a CK domain. So $\eta(x^m)$ is of the form $\eta(x^m) = Am^d + O(m^{d-1})$ for $m \in \mathbb{N}^*$, where $A \in \mathbb{Q}$, $d \in \mathbb{N},\ A > 0$. Then, it is enough to find an equivalent of $\eta(x^m)$. For any $m \in n\mathbb{N}$, we have $v^m \in \mathcal{U}(R)$ and x^m is associated to p^{mk}, so that we can assume that n divides m to get A and d. In view of Theorem 3.11, we are led to calculate the number $N(n, km, 0) = \eta(x^m)$ of solutions $(a_1, \dots, a_n) \in \mathbb{N}^n$ of the system gotten in Theorem 4.4 :

$$(S) \quad \begin{cases} \displaystyle\sum_{i=1}^{n} a_i = km & (1) \\ \displaystyle\sum_{i=1}^{n} \overline{ia_i} = \bar{0} & (2) \quad \text{in } \mathbb{Z}/n\mathbb{Z} \end{cases}$$

But, by Corollary 4.7, we have, since $n = \gcd(n, mk)$

$$N(n, km, 0) = N(km, n, 0) =$$

$$\frac{1}{mk}\binom{mk+n-1}{n} + \frac{1}{n}\sum_{l=1}^{n-1}\left(\cos\left(\frac{2lr\pi}{n}\right)\prod_{1\le j\le n-1, n|jl}\left(\frac{mk+j}{j}\right)\right)$$

where $r = 0$.

First, we have

$$\frac{1}{mk}\binom{mk+n-1}{n} = \frac{(mk+n-1)\cdots(mk+1)}{n!} \sim \frac{(mk)^{n-1}}{n!} = m^{n-1}\frac{k^{n-1}}{n!}.$$

Now, consider $\displaystyle\frac{1}{n}\sum_{l=1}^{n-1}\left(\prod_{1\leq j\leq n-1, n|jl}\left(\frac{mk+j}{j}\right)\right)$ since $r=0$.

Because of $l \leq n-1 < n$, we cannot have $n|l$, so that $j \neq 1$ and we have at most $n-2$ factors in the product.

It follows that $\displaystyle\prod_{1\leq j\leq n-1, n|jl}\left(\frac{mk+j}{j}\right) \leq (mk+n)^{n-2} = O(m^{n-2})$. As we have a sum of $n-1$ terms, we get that $\eta(x^m) \sim \dfrac{k^{n-1}}{n!}m^{n-1}$. □

References

[1] D.D. Anderson, D.F. Anderson and M. Zafrullah, Atomic domains in which almost all atoms are prime, Comm. Algebra **20** (1992), 1447-1462.

[2] D.D. Anderson and J.L. Mott, Cohen-Kaplansky domains: Integral domains with a finite number of irreducible elements, J. Algebra **148** (1992), 17-41.

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

[4] I.S. Cohen and I. Kaplansky, Rings with a finite number of primes I, Trans. Amer. Math. Soc. **60** (1946), 468-477.

[5] D.E. Dobbs and M. Fontana, Locally pseudo-valuation domains, Annali Mat. Pura Appl. **134** (1983), 147-168.

[6] F. Halter-Koch, On the asymptotic behaviour of the number of distinct factorizations into irreducibles, Ark. Mat. **31** (1993), 297-305.

[7] F. Halter-Koch, Divisor theories with primary elements and weakly Krull domains, Boll. UMI, **9-B** (1995), 417-441.

[8] J.R. Hedstrom and E.G. Houston, Pseudo-valuation domains, Pac. J. Math. **75** (1) (1978), 137-147.

[9] G. Picavet and M. Picavet-L'Hermitte, Anneaux t-clos, Comm. Algebra **23** (1995), 2643-2677.

[10] M. Picavet-L'Hermitte, t-closed pairs, Lecture Notes in Pure and Appl. Math., Marcel Dekker, New York **185** (1997), 401-415.

[11] M. Picavet-L'Hermitte, Factorization in some orders with a PID as integral closure, Algebraic Number Theory and Diophantine Analysis, de Gruyter, New York (2000), 365-390.

[12] M. Picavet-L'Hermitte, Weakly factorial quadratic orders, Arab. J. Sci. Eng. **26** (2001), 171-186.

[13] D. Redmond, *Number Theory*, Marcel Dekker, New York (1996).

[14] R.G. Swan, On seminormality, J. Algebra **67** (1980), 210-229.

[15] A. Zaks, Half-factorial domains, Bull. Amer. Math. Soc. **82** (1976), 721-724.

Laboratoire de Mathématiques Pures, Université Blaise Pascal, 63177 Aubière-Cedex, France

E-mail address: Abdallah.Badra@math.univ-bpclermont.fr

Laboratoire de Mathématiques Pures, Université Blaise Pascal, 63177 Aubière-Cedex, France

E-mail address: Martine.Picavet@math.univ-bpclermont.fr