MASTER'S THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

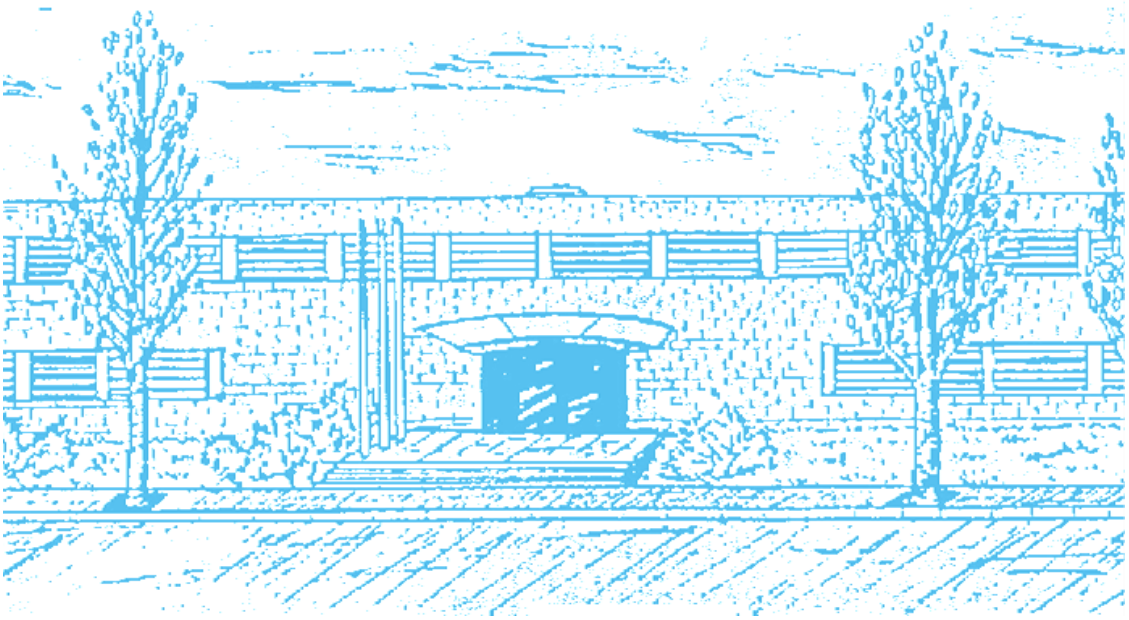
Title: Prime ideals in three dimensional regular local rings

Author: Laura González Hernández

Advisors: Francesc Planas Vilanova

Department: Mathematics

Academic year: 2019/2020



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Master degree thesis
Facultat de Matemàtiques i Estadística
Universitat Politècnica de Catalunya

Prime ideals in three dimensional regular local rings

Author: Laura González Hernández
Advisor: Francesc Planas Vilanova

June 2020

In the first place, I would like to thank my advisor Francesc Planas for all the knowledge he has provided me with, his unconditional support and excellent supervision. Secondly, thanks to my lockdown and life partners Oriol and Aina for their help and love.

Prime ideals in three dimensional regular local rings

Abstract

The aim of this work is twofold. First we study a family of prime ideals, in the power series ring in three variables over a field, which need arbitrarily high number of generators. This family was introduced by T. T. Moh in the seventies. Second, and having in mind to generalize this phenomenon to any three dimensional regular local ring, we study the proof of the existence of a prime ideal minimally generated by four elements, in any regular local ring. This fact was recently stated by F. Planas. We conclude the present dissertation by extending this result to a prime ideal minimally generated by five elements.

Key words: Moh's primes, power series rings, regular local rings, Hilbert-Burch Theorem.

Contents

Introduction

The study of prime ideals is a classical and long-standing algebraic problem. In particular, the analysis of generators of prime ideals. F.S. Macaulay, in 1916, gave a first approach to the problem of bounding the minimal number of generators of prime ideals. He found a set of prime ideals $\{P_m\}$, in the polynomial ring in three variables, so that every P_m needs at least m generators. Later on, S.S. Abhyankar provided a more precise discussion on Macaulay's prime ideals. In 1973, T.T. Moh adapted Macaulay's examples to the power series ring in three variables. He proved that there exists a family $\{P_n\}$ of prime ideals, in the power series ring in three variables, where each $\{P_n\}$ is minimally generated by at least n elements. Furthermore, he proved in 1979, that P_n is generated by exactly $n+1$ elements.

This work has two main purposes. The first one is to describe and understand Moh's examples. We will study the construction of these prime ideals and delve into Moh's proof, in order to understand the reason why these ideals need exactly $n+1$ generators. The second purpose is to try to generalize this family of prime ideals to any regular three dimensional local rings.

The structure of the present dissertation is the following. In Chapter 1, we prove the following result:

THEOREM. *Let k be a field of characteristic zero. Let $k[[x,y,z]]$ be the power series ring in three variables over k. Then, for an odd positive integer n, there exists a family of prime ideals $\{Pn\}$ such that each P_n needs exactly $n+1$ generators.*

Having this result in mind, in Sections 1 and 2, we introduce the theoretical background regarding binomial vectors and numerical semigroups. In Section 3, we dig into Moh's prime ideals. We prove the first half of his result, namely, that each P_n needs at least n generators.
Then, in Section 4, we prove the whole aforementioned Theorem.
Last section of Chapter 1, shows that these prime ideals can be generated by the $n \times n$ subdeterminants of a $n \times (n+1)$ matrix.
Chapter 2 considers the problem of Moh, but in any regular local ring of Krull dimension three. In Section 1, we follow the recent article of F. Planas, [**6**]. There it is shown the

existence of a prime ideal minimally generated by four elements, in any regular local ring of dimension three.
This result provides us with an idea of how to find a prime ideal minimally generated by more elements. We display this general process in Section 2. Finally, in Section 3, we prove the existence of a prime ideal in a regular local ring of dimension three, minimally generated by five elements.
We finally present our conclusions and ideas for further work.

CHAPTER 1

Generators of prime ideals in power series rings of three variables

The purpose of this chapter is to give a family of prime ideals $\{P_n\}$, in the power series ring $k[[x, y, z]]$, such that P_n needs at least n generators. We follow the articles of Moh [**4**] and [**5**]. Before proving the main result about generators in prime ideals, we will need some general notions on binomial vectors and semigroups.

1. Binomial vectors

In this section we present the main tools on binomial vectors that will be used subsequently in Section 3. We reproduce the definitions and the structure of Moh [**5**]. When necessary, we add some observations and examples for comprehension purposes, as well as some remarks to clarify the most difficult points.
Let k be a field of characteristic zero. Therefore, k contains a copy of $\mathbb{Z}$, $\mathbb{Z} \hookrightarrow k$. Let k^∞ and k^m be the k-vector spaces of dimension ∞ and m.

NOTATION 1.1. The binomial coefficients are defined as follows:

$$b_{i,j} := \binom{i}{j} = \tfrac{i!}{j!(i-j)!}\,, \text{ for } i \geq j\,;$$
$$b_{i,j} := 0\,, \text{ for } i < j\,.$$

The binomial coefficients are positive integers that can be thought in k, through the inclusion $\mathbb{Z} \hookrightarrow k$.

DEFINITION 1.2. For a fixed integer $n \geq 0$, the n-th *binomial vector* b_n is defined as

$$b_n := (b_{n,0}, \ldots, b_{n,n}, 0, \ldots) \in k^\infty.$$

EXAMPLE 1.3. The first binomial vectors are: $b_0 = (1, 0, \ldots)$, $b_1 = (1, 1, 0, \ldots)$, $b_2 = (1, 2, 1, 0, \ldots)$, $b_3 = (1, 3, 3, 1, 0, \ldots)$, $b_4 = (1, 4, 6, 4, 1, 0, \ldots)$, and so on.

Let $T = \{t_1, \ldots, t_m\}$ be a set of m non-negative integers. We can always suppose that they are labelled so that, $t_1 < \ldots < t_m$. We can consider then, the binomial vectors associated to the set of integers in T. Let us give a basis of the k-vector space $k^{\mathrm{Card}(T)}$ in terms of these binomial vectors.

DEFINITION 1.4. For the k-vector spaces k^∞ and k^m, we consider the following map projections:

$$\begin{array}{ccccc} k^\infty & \xrightarrow{\rho_m} & k^m & , & k^\infty & \xrightarrow{\rho'_m} & k^{m-1} \\ (\lambda_1,\ldots,\lambda_m,\ldots) & \mapsto & (\lambda_1,\ldots,\lambda_m) & & (\lambda_1,\ldots,\lambda_m,\ldots) & \mapsto & (\lambda_2,\ldots,\lambda_m) \end{array} .$$

Following Moh's framework, we define some matrices, which will be used to prove some subsequent lemmas and propositions.

DEFINITION 1.5. Given $m \geq 0$ and $T = \{t_1, \ldots, t_m\}$,

- $B_{t_1,\ldots,t_m}$ is the $m \times m$ matrix whose rows are the vectors $\rho_m(b_{t_1}), \ldots, \rho_m(b_{t_m})$. That is,

$$B_{t_1,\ldots,t_m} := (\rho_m(b_{t_1}), \ldots, \rho_m(b_{t_m})) = \begin{pmatrix} b_{t_1,0} & \cdots & b_{t_1,m-1} \\ \vdots & & \vdots \\ b_{t_m,0} & \cdots & b_{t_m,m-1} \end{pmatrix} .$$

- The matrix ${}_iA$ is the identity $m \times m$ matrix with -1 in the position $(i, i+1)$. That is,

$${}_iA := \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ & & \ddots & & & & \\ & \cdots & \cdots & 1 & -1 & \cdots & 0 \\ & & & & \ddots & & \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} .$$

- The matrix A_m is the product of all ${}_iA$, $A_m := \prod_{i=1}^{m-1} {}_iA$.

EXAMPLE 1.6. Let us take $T = \{1, 2, 5, 7\}$. Then the matrices $B_{t_1,\ldots,t_m}$, ${}_2A$ and A_m are as follows:

$$B_{1,2,5,7} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 5 & 10 & 10 \\ 1 & 7 & 21 & 35 \end{pmatrix} , \quad {}_2A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \quad A_4 = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

In order to prove the main theorem of this section we need three lemmas.

LEMMA 1.7. [**4**, Lemma 2.1.] *For $t_1 > 0$,*

$$B_{t_1,\ldots,t_m} \cdot A_m = B_{t_1-1,\ldots,t_m-1} .$$

Moreover, $\det(B_{t_1,\ldots,t_m}) = \det(B_{t_1-1,\ldots,t_m-1})$.

PROOF. Note that

$$b_{t_i,0} = b_{t_i-1,0}\,,$$
$$b_{t_i,j} - b_{t_i-1,j-1} = b_{t_i-1,j}\,.$$

The first equality is clear by definition, since $b_{t_i,0} = \binom{t_i}{0} = 1$, for any t_i. The second one, follows directly from the definition. Indeed:

$$b_{t_i,j} - b_{t_i-1,j-1} = \frac{t_i!}{j!(t_i-j)!} - \frac{(t_i-1)!}{(j-1)!((t_i-1-j+1)!} =$$
$$\frac{t_i! - j(t_i-1)!}{j!(t_i-j)(t_i-j-1)!} = \frac{(t_i-1)!}{j!(t_i-1-j)!} = b_{t_i-1,j}\,.$$

Now we compute the product of the matrices $B_{t_1,\ldots,t_m} \cdot {}_1A \cdot \ldots \cdot {}_{m-1}A$:

$$\begin{pmatrix} b_{t_1,0} & \cdots & b_{t_1,m-1} \\ \vdots & & \vdots \\ b_{t_m,0} & \cdots & b_{t_m,m-1} \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix} \cdot {}_2A \cdot \ldots \cdot {}_{m-1}A\,.$$

Multiplying the first two matrices, we obtain the matrix

$$\begin{pmatrix} b_{t_1,0} & b_{t_1,1} - b_{t_1-1,0} & \cdots & b_{t_1,m-1} \\ \vdots & \vdots & & \vdots \\ b_{t_m,0} & b_{t_m,1} - b_{t_m-1,0} & \cdots & b_{t_m,m-1} \end{pmatrix}.$$

Applying the second aforementioned equality involving the subtraction of two binomial vectors, we get:

$$\begin{pmatrix} b_{t_1,0} & b_{t_1-1,1} & \cdots & b_{t_1,m-1} \\ \vdots & \vdots & & \vdots \\ b_{t_m,0} & b_{t_m-1,1} & \cdots & b_{t_m,m-1} \end{pmatrix}.$$

Then, multiplying this matrix by ${}_2A$, we will obtain some sums of $b_{i,j}$ for the third column and the rest of the matrix will remain the same. So, applying the previous relations for the third column, we obtain the following matrix:

$$\begin{pmatrix} b_{t_1,0} & b_{t_1-1,1} & b_{t_1-1,2} & \cdots & b_{t_1,m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{t_m,0} & b_{t_m-1,1} & b_{t_m-1,2} & \cdots & b_{t_m,m-1} \end{pmatrix}.$$

Recursively, multiplying and also applying the first equality involving binomial numbers to the first column, we arrive to the matrix

$$\begin{pmatrix} b_{t_1-1,0} & \cdots & b_{t_1-1,m-1} \\ \vdots & & \vdots \\ b_{t_m-1,0} & \cdots & b_{t_m-1,m-1} \end{pmatrix},$$

which is precisely $B_{t_1-1,\dots,t_m-1}$. The determinant equality follows directly by applying determinants to this matrix equality. We use that the product of determinants is the determinant of the product and that the determinant of each ${}_iA$ equals 1. □

For a better understanding of the proofs, we illustrate it with an example.

EXAMPLE 1.8. Let us take T, as before, $T = \{1, 2, 5, 7\}$. Then $B_{1,2,5,7} \cdot A_4$:

$$B_{1,2,5,7} \cdot A_4 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 5 & 10 & 10 \\ 1 & 7 & 21 & 35 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 4 & 6 & 4 \\ 1 & 6 & 15 & 20 \end{pmatrix} = B_{0,1,4,6}\,.$$

LEMMA 1.9. [**4**, Lemma 2.2.] *Suppose $t_1 = 0$. Then,*

$$\det(B_{t_1,\dots,t_m}) = \det(\rho'_m(b_{t_2}), \dots, \rho'_m(b_{t_m}))\,.$$

PROOF. Clearly if $b_{t_1} = b_0 = (1, 0, \dots, 0)$, we can develop the determinant of $B_{t_1,\dots,t_m}$ by the first row. So we need to compute the determinant of the following matrix:

$$\begin{pmatrix} b_{t_2,1} & \cdots & b_{t_2,m-1} \\ \vdots & & \vdots \\ b_{t_m,1} & \cdots & b_{t_m,m-1} \end{pmatrix}.$$

This determinant is precisely the determinant of the matrix $(\rho'_m(b_{t_2}), \dots, \rho'_m(b_{t_m}))$. □

EXAMPLE 1.10. Suppose that $T = \{0, 2, 3, 4\}$. Then

$$\det(B_{0,2,3,4}) = \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \\ 1 & 4 & 6 & 4 \end{pmatrix} = 4\,.$$

On the other hand,

$$\det(\rho'_m(2), \rho'_m(3), \rho'_m(4)) = \det \begin{pmatrix} 2 & 1 & 0 \\ 3 & 3 & 1 \\ 4 & 6 & 4 \end{pmatrix} = 4\,.$$

LEMMA 1.11. [**4**, Lemma 2.3.] *We have,*

$$\det(\rho'_m(b_{t_2}), \dots, \rho'_m(b_{t_m})) = \frac{(t_2 \cdots t_m)}{(m-1)!} \det(B_{t_2-1,\dots,t_m-1})\,.$$

PROOF. To prove this equality, it is enough to consider the following fact:

$$b_{t_i,j} = \frac{t_i!}{j!(t_i-j)!} = \frac{t_i(t_i-1)!}{j(j-1)!(t_i-j)!} = \frac{t_i}{j} b_{t_i-1,j-1}\,.$$

Multiplying each entry (i,j) of the matrix $B_{t_2-1,\ldots,t_m-1}$by $\frac{t_{i+1}}{j}$, we get the matrix

$$(\rho'_m(b_{t_2}),\ldots,\rho'_m(b_{t_m}))\,.$$

The previous multiplication can be seen as multiplying the i-th row by t_{i+1} and the j-th column by $\frac{1}{j}$. So, by taking determinants and applying their properties, we get:

$$\det(\rho'_m(b_{t_2}),\ldots,\rho'_m(b_{t_m})) = \frac{(t_2\cdots t_m)}{(m-1)!}\det(B_{t_2-1,\ldots,t_m-1})\,.$$

□

Example 1.12. To illustrate this lemma, take $T=\{1,2,5,7\}$ and compute the determinant matrices:

$$\begin{aligned}\det(\rho'_m(2),\rho'_m(5),\rho'_m(7)) &= \begin{vmatrix} 2 & 1 & 0\\ 5 & 10 & 10\\ 7 & 21 & 35\end{vmatrix} = 175\,;\\ \frac{2\cdot 5\cdot 7}{3!}\det(B_{2-1,5-1,7-1}) &= \frac{5\cdot 7}{3}\cdot\begin{vmatrix} 1 & 1 & 0\\ 1 & 4 & 6\\ 1 & 6 & 15\end{vmatrix} = 175\,.\end{aligned}$$

Now we are in position to prove the main theorem of this section.

Theorem 1.13. [**4**, Theorem 2.1.] *The set* $\{\rho_m(b_{t_1}),\ldots,\rho_m(b_{t_m})\}$ *forms a basis for* k^m.

Proof. Let us proceed by induction on m.
For $m=1$, $\rho_1(b_{t_1})=(1)$, which clearly defines a basis of k. Let us suppose that the result holds for $m-1$ and let us prove the case m. We proceed now by induction on t_1. If $t_1=0$, by Lemmas 1.9 and 1.11, we have the following equality:

$$\det(B_{t_1,\ldots,t_m}) = \frac{(t_2\cdots t_m)}{(m-1)!}\det(B_{t_2-1,\ldots,t_m-1})\,.$$

By induction, the right hand side of the equation is different from zero. Therefore

$$\det(B_{t_1,\ldots,t_m})\neq 0\,.$$

The set $\{\rho_m(b_{t_1}),\ldots,\rho_m(b_{t_m})\}$ is linearly independent and is a basis of the k-vector space k^m. Let us assume that it is proved for $t_1\geq 0$ and prove it for t_1+1. Let us consider the labelled set $\{t_1+1,t_2,\ldots,t_m\}$ with $t_1+1<t_2<\ldots<t_m$. By Lemma 1.7, we have the following equality:

$$\det(B_{t_1+1,\ldots,t_m}) = \det(B_{t_1+1-1,t_2-1,\ldots,t_m-1}) = \det(B_{t_1,t_2-1,\ldots,t_m-1})\,.$$

By induction, the rightmost term on the equality is different from 0. Therefore, the leftmost term is also different from zero. Hence $\{\rho_m(b_{t_1}),\ldots,\rho_m(b_{t_m})\}$, with $t_1\geq 0$, forms a basis of k^m. □

EXAMPLE 1.14. Continuing with the previous example given by $T = \{1, 2, 5, 7\}$, let us see that a basis of k^4 is

$$\{\rho_m(b_1), \rho_m(b_2), \rho_m(b_5), \rho_m(b_7)\},$$

where $m = 4$. Thus, the vectors $\{(1, 1, 0, 0), (1, 2, 1, 0), (1, 5, 10, 10), (1, 7, 21, 35)\}$ must generate k^4 and be linearly independent. Since the dimension of the k-vector space k^4 is 4, we just have to prove that they are linearly independent, i.e. the determinant of the matrix formed by the coordinates of these vectors is different from 0. Indeed, this is the case:

$$\det B_{1,2,5,7} = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 5 & 10 & 10 \\ 1 & 7 & 21 & 35 \end{vmatrix} = 60 \neq 0\,.$$

2. Numerical semigroups

REMARK 2.1. Moh uses the notion of semigroup to refer to what we currently know as numerical semigroups. We follow the definitions and the results in [**7**, Chapter 1] which, by now, have become standard in this area.

DEFINITION 2.2.

- A *semigroup* $(S, +)$ is a set S with a binary associative operation $+$ on S.
- A semigroup S is a *monoid* if it has an identity element with respect to its operation.
- A subset of a semigroup (monoid) closed under the operation is called *subsemigroup (submonoid).*

DEFINITION 2.3. A *numerical semigroup* S is a submonoid of $\mathbb{N}$ with finite complement. Here, we understand $0 \in \mathbb{N}$ and $0 \in S$. Thus $a + b \in S$ for all $a, b \in S$ and $\mathbb{N} \setminus S$ is finite.

The next proposition gives us an alternative way of finding numerical semigroups for generated monoids.

PROPOSITION 2.4. *Let A be a nonempty subset of $\mathbb{N}$. Then the monoid $\langle A \rangle$ generated by this subset is a numerical semigroup if, and only if,* $\gcd(A) = 1$.

PROOF. We follow the proof of [**7**, Lemma 2.1.] For the forward implication, we denote $d = \gcd(A)$. As $\langle A \rangle$ is a numerical semigroup, $\mathbb{N} \setminus \langle A \rangle$ is finite. Therefore, it exists a positive integer $n \in A$ such that $n + 1 \in A$. So d divides n and $n + 1$, thus $d = 1$.

To prove the converse, it is enough to prove that the complement of $\langle A\rangle$ is finite. As $1 = \gcd(A)$, there exist $a_1, \ldots, a_n \in A$ and $z_1, \ldots, z_n \in \mathbb{Z}$ such that

$$1 = z_1 a_1 + \ldots + z_n a_n \,.$$

We can assume, without loss of generality, that the first l coefficients z_i are positive and that the next ones are negative. Therefore, we have the following equality:

$$z_1 a_1 + \ldots + z_l a_l = 1 - z_{l+1} a_{l+1} - \ldots - z_n a_n =: 1 + s \,,$$

where $s = -z_{l+1} a_{l+1} - \ldots - z_n a_n \geq 0$, $s \in \langle A\rangle$ and $s + 1 = z_1 a_1 + \ldots + z_l a_l \in \langle A\rangle$.
Claim: Given an n such that $n \geq (s-1)s + (s-1)$, then $n \in \langle A\rangle$.
Clearly, from the Claim, it follows that $\mathbb{N} \setminus \langle A\rangle \subseteq \{z \in \mathbb{N} | z < (s-1)s + (s-1)\}$ and so $\mathbb{N} \setminus \langle A\rangle$ is finite.
To prove the Claim, divide n by s so that

$$n = qs + r \,,$$

with $q \in \mathbb{N}$ and $0 \leq r \leq s - 1$. So

$$n = qs + r = qs + r + rs - rs = r(s+1) - (q-r)s \,.$$

If we prove that $q - r \geq 0$, since s and $s + 1$ are in $\langle A\rangle$, it would follow that $n \in \langle A\rangle$. So let us see that $q - r \geq 0$. Using the hypothesis of the Claim and that $0 \leq r \leq s - 1$, we obtain

$$qs + r = n \geq (s-1)s + (s-1) \geq (s-1)s + r \,.$$

Therefore $qs \geq (s-1)s$ and $q \geq s - 1 \geq r$. Hence $q - r \geq 0$. □

Example 2.5. Let us give an example of a numerical semigroup. Let us consider the set $A = \{2, 7, 9\}$. Clearly $\langle A\rangle \subset \mathbb{N}$ and is closed. It remains to see that its complementary is finite. It is easy to see that $\langle A\rangle$ contains all the even numbers and all the odd ones bigger than 7. Thus

$$\mathbb{N} \setminus \langle A\rangle = \{1, 3, 5\} \,.$$

We can check that the theorem holds, as $\gcd(A) = \gcd(2, 7, 9) = 1$.

Once we have established these concepts we can define the *Frobenius number*. This number is used as an assumption in Moh's article.

Definition 2.6. If S is a numerical semigroup, the *Frobenius number* is defined as

$$F(S) = \max\{n \in \mathbb{N} | n \notin S\} \,.$$

The set of *gaps* of S is defined as

$$G(S) = \mathbb{N} \setminus S \,.$$

The *genus* of S is defined as

$$g(S) = \mathrm{Card}(G(S))\,.$$

DEFINITION 2.7. Let S be a numerical semigroup and $n \in S, n \neq 0$, the *Apéry set* of n in S is defined as the following set:

$$\mathrm{Ap}(S,n) := \{s \in S : s - n \notin S\}\,.$$

LEMMA 2.8. *The Apéry Set of n in a numerical semigroup S is equal to*

$$\mathrm{Ap}(S,n) = \{w(0), \ldots, w(n-1)\}\,,$$

where $w(i)$ is the least element of S congruent with i mod n, $i \in \{0, \ldots, n-1\}$.

PROOF. See [**7**, Lemma 2.4.]. □

EXAMPLE 2.9. Let $S = \langle 2, 7, 9\rangle$ be a numerical semigroup. Then,

$$\mathrm{Ap}(S,7) = \{0, 8, 2, 10, 4, 12, 6\}\,.$$

The next proposition will provide a way to find the Frobenius number and the genus of a given numerical semigroup.

PROPOSITION 2.10. *Let S be a numerical semigroup and let $n \neq 0$ be an element of S. Then*

$$F(S) = \max \mathrm{Ap}(S,n) - n\,; \qquad g(S) = \frac{1}{n}\left(\sum_{w \in Ap(S,n)} w\right) - \frac{n-1}{2}\,.$$

PROOF. First, let us see that the element $\max \mathrm{Ap}(S,n) - n$ is not in S. This is clear by the definition of the Apéry set. So we just have to check that there is not an integer greater than $\max \mathrm{Ap}(S,n) - n$ that is not in S.
Let x be such that $x > \max \mathrm{Ap}(S,n) - n$. That is, $x + n > \max \mathrm{Ap}(S,n)$. Let $\overline{x} = \overline{i} \in \mathbb{Z}/(n\mathbb{Z})$, with $i \in \{0, \ldots, n-1\}$. Therefore, $x + n$ is congruent with $i + 1$ mod n. Let us take the element $w(i+1) \in \mathrm{Ap}(S,n)$, which is congruent to $i + 1$ mod n. Since $x + n > \max \mathrm{Ap}(S,n)$, $x + n$ is congruent with $w(i+1)$ mod n. Therefore

$$x + n = w(i+1) + \lambda n \Leftrightarrow x = w(i+1) + (\lambda - 1)n\,.$$

As S is a numerical semigroup, i.e. is closed under the sum, $x \in S$.
To prove the second part, we consider the Apéry set of n in S,

$$\mathrm{Ap}(S,n) = \{w(0) = 0, w(1) = 1 + k_1 n + \ldots, w(n-1) = n - 1 + k_{n-1} n\}\,.$$

An integer x, congruent with i, does not belong to S if, and only if, $w(i) \geq x$. Therefore, for each $i \in \{0, \cdots, n-1\}$, there are k_i integers not in S. Thus

$$g(S) = k_1 + \ldots + k_{n-1} = \frac{1}{n}(1 + k_1 n + \ldots + n - 1 + k_{n-1} n) - \frac{\sum_{i=1}^{n-1} i}{n} = \frac{1}{n}\left(\sum_{w \in Ap(S,n)} w\right) - \frac{n-1}{2}\,.$$

□

Example 2.11. Let $S = \langle 2, 7, 9\rangle$ be a numerical semigroup. Let us compute its Frobenius number and its genus.

$$S = \{0, 2, 4, 6, \mapsto\} \qquad \mathbb{N} \setminus S = \{1, 3, 5\}\,.$$

Therefore $F(S) = 5$ and $g(S) = 3$. Let us check that the proposition follows,

$$F(S) = \max \mathrm{Ap}(S, 7) - 7 = 12 - 7 = 5\,;$$
$$g(S) = \tfrac{1}{7} \cdot 21 = 3\,.$$

Let us focus on 2−generated numerical semigroups.

Proposition 2.12. *Let a, b be two non-negative integers such that* $\gcd(a, b) = 1$. *Let $S = \langle a, b\rangle$ be the numerical semigroup generated by a and b. Then,*

$$F(S) = ab - b - a\,; \qquad g(S) = \frac{ab - a - b + 1}{2} = \frac{F(S) + 1}{2}\,.$$

Proof. By Lemma 2.8, we know that the Apéry set of a in S is formed by the least elements of S congruent with $1, \ldots, a-1$. Therefore,

$$\mathrm{Ap}(S, a) = \{0, b, 2b, \ldots, (a-1)b\}\,.$$

So, by Proposition 2.10,

$$F(S) = \max \mathrm{Ap}(S, a) - a = (a-1)b - a = ab - b - a\,.$$

For the genus we just apply the formula given above. □

Notation 2.13. From now on, we denote $\mathbb{Z}_L = \{i \in \mathbb{N} | 0 \leq i \leq L\}$.

Remark 2.14. Let $S = \langle a, b\rangle$ be the numerical semigroup generated by a and b, with $\gcd(a, b) = 1$. Let A be

$$A = \{n \in S | n \leq F(S)\} = S \cap \mathbb{Z}_{F(S)}\,.$$

Clearly $A \subseteq \mathbb{Z}_{F(S)}$. By Definition 2.6,

$$\mathbb{N} \setminus S \subseteq \mathbb{Z}_{F(S)}\,,$$

and its cardinal is the genus, $g(S)$. Therefore,

$$\mathrm{Card}(A) = F(S) + 1 - g(S) = \frac{F(S) + 1}{2} = g(S)\,.$$

Now, we are the position to understand Moh's [**4**, Section 4].

DEFINITION 2.15. For a positive integer n, a numerical semigroup S is *residuely equally distributed mod* n, if

$$\mathrm{Card}(S \cap \{i + n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) = \frac{F(S)+1}{2n} \quad , \quad \text{for all } i \in \{0, \ldots, n-1\}.$$

REMARK 2.16. Let $S = \langle a, b\rangle$ with $\gcd(a, b) = 1$. Then S is equally distributed mod 1. Recall the definition of A in the previous remark. When $n = 1$, then $\{i + 1\mathbb{Z}\} = \mathbb{Z}$. Therefore,

$$A = \{n \in S | n \leq F(S)\} = S \cap \mathbb{Z} \cap \mathbb{Z}_{F(S)} = S \cap \mathbb{Z}_{F(S)}\,.$$

Taking cardinalities,

$$\frac{F(S)+1}{2} = \mathrm{Card}(A) = \mathrm{Card}(S \cap \mathbb{Z}_{F(S)})\,.$$

THEOREM 2.17. [**4**, Theorem 3.1.] *Let n be an odd positive integer. The semigroup $S = \langle n+1, n+2\rangle$ is residually equally distributed mod n.*

PROOF. We are going to follow the proof of [**4**, Theorem 3.1.]. First, we can apply the previous propositions because $(n+1, n+2) = 1$. So, by Proposition 2.4, S is a numerical semigroup. Let us write the set $\{i \in \mathbb{N} | 0 \leq i \leq F(S)\}$ in a matricial way. Let D be the $n \times (n+1)$ matrix defined as:

$$D = (d_{i,j}) = \begin{pmatrix} 0 & 1 & \ldots & n \\ n+1 & n+1+1 & \ldots & n+1+n \\ \vdots & \vdots & & \vdots \\ (n-1)(n+1) & (n-1)(n+1)+1 & \cdots & (n-1)(n+1)+n \end{pmatrix}.$$

Claim: If $i \geq j$, then $d_{i,j} \in S$. Indeed,

$$d_{i,j} = (i-1)(n+1) + (j-1) = (i-j)(n+1) + (j-1)(n+2)\,.$$

Since $i - j \geq 0$ and $j - 1 \geq 0$, then $d_{ij} \in S$. By the previous remark 2.14,

$$\mathrm{Card}(S \cap \mathbb{Z}_{F(S)}) = \frac{F(S)+1}{2} = \frac{(n+1)(n+2) - (n+2) - (n+1) + 1}{2} = \frac{n(n+1)}{2}\,,$$

which is the number of $d_{i,j} \in S$, when $i \geq j$. Therefore, we can conclude that

$$\text{if } i < j \Rightarrow d_{i,j} \notin S\,.$$

To finish the proof we find the set of elements in the following intersection:

$$\mathbb{Z}_{F(S)} \cap \{i + n\mathbb{Z}\}\,.$$

So we look into the entries of the matrix that can be written as $i + \lambda n$ for $\lambda \in \mathbb{Z}$. We find the following elements:

$$\{d_{1,i+1}, d_{2,i}, d_{3,i-1}, \ldots, d_{i+1,1}, d_{i+1,n+1}, \ldots, d_{n,i+2}\} = \{i, i+n, \ldots, i+in, i+(i+1)n, \ldots, i+nn\}\,.$$

The next element of the set $\{i + n\mathbb{Z}\}$ is $i + (n+1)n$. However, this one is not in $\mathbb{Z}_{F(S)}$. Finally, we check which of the elements of this set are in S, *i.e.* $i \geq j$. Let us suppose that $i+1$ is even. The first $\frac{i+1}{2}$ elements are not in S, but the next $\frac{i+1}{2}$ elements do are. The following $\frac{n-i}{2}$ elements are not in S and the last $\frac{n-i}{2}$ elements are. Let us suppose now that $i+1$ is odd. In this case, the first $\frac{i}{2}$ elements are not in S, the following $\frac{i}{2}+1$ elements are in S, the next $\frac{n-i-1}{2}+1$ are not in S and the last $\frac{n-i-1}{2}$ are. In both cases, the number of elements in S is $\frac{n+1}{2}$. Therefore,

$$\mathrm{Card}(S \cap \{i + n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) = \frac{n+1}{2} = \frac{n(n+1) - 1 + 1}{2n} = \frac{F(S)+1}{2n}\,.$$

□

Example 2.18. Let us give an example to illustrate the proof. Let $S = \langle 4, 5\rangle$ and let $n = 3$. Then,

$$S = \{0, 4, 5, 8, 9, 10, 12, \to\} \text{ and } \mathbb{N} \setminus S = \{1, 2, 3, 6, 7, 11\}\,.$$

The Frobenius number of S is 11. Let us compute the intersection for $i = 2$ and $n = 3$:

$$S \cap \{2, 5, 8, 11, \ldots\} \cap \mathbb{Z}_{11} = \{5, 8\}\,.$$

Therefore,

$$\mathrm{Card}(S \cap \{2 + 3\mathbb{Z}\} \cap \mathbb{Z}_{11}) = 2 = \frac{11+1}{2 \cdot 3}\,.$$

3. Generators in prime ideals

In this section we prove the main theorem of the chapter. Let $k[[x, y, z]]$ be the power series ring in the variables x, y, z over a field k. Let us define a collection of prime ideals P_n, $n \geq 1$, in $k[[x, y, z]]$. For an odd integer n, set $m = \frac{n+1}{2}$. Let λ be an integer such that $\lambda > n(n+1)m$ and $\gcd(\lambda, m) = 1$. Let ρ be the following ring morphism:

$$\begin{array}{rccc} \rho: & k[[x,y,z]] & \longrightarrow & k[[t]] \\ & x & \mapsto & t^{nm} + t^{nm+\lambda} \\ & y & \mapsto & t^{m(n+1)} \\ & z & \mapsto & t^{m(n+2)}\,. \end{array}$$

Notice that the ring morphism ρ has nothing to do with the projection map ρ_m defined in Section 1. We will keep this notation just to match the one used by Moh.

Definition 3.1. Let P_n be defined as

$$P_n = \ker \rho\,.$$

Note that P_n is a prime ideal because $k[[t]]$ is an integral domain and

$$k[[x, y, z]]/\ker \rho \cong \mathrm{Im}\rho \subseteq k[[t]]\,.$$

Let σ be the following ring morphism:

$$\begin{array}{rccc} \sigma: & k[[x,y,z]] & \longrightarrow & k[[x,y,z]] \\ & x & \mapsto & x^n \\ & y & \mapsto & y^{n+1} \\ & z & \mapsto & z^{n+2} \end{array}$$

We proceed to establish some definitions related to this mapping.

DEFINITION 3.2. The *order* of an element $f = \sum_{i=0}^{\infty} \sum_{i+j+k=r} a_{i,j,k} x^i y^j z^k \in k[[x,y,z]]$, for $f \neq 0$ is

$$\text{ord}\,(f) = \min\{i+j+k | a_{i,j,k} \neq 0\}\,.$$

The *leading form* of f is defined as

$$\text{LF}(f) = \sum a_{i,j,k} x^i y^j z^k \text{ such that } i+j+k = \text{ord}\,(f)\,.$$

A series f is *homogeneous* if $f = \text{LF}(f)$.

REMARK 3.3. If necessary, we fix an ordering on the set of monomials in three variables x, y, z; for instance, the degrevlex, with $x < y < z$, we have:

$$1 < x < y < z < x^2 < xy < xz < y^2 < yz < z^2 < \\ < x^3 < x^2y < x^2z < xy^2 < xyz < y^3 < y^2z < yz^2 < z^3 < \dots$$

The number of monomials of degree r in 3 variables is $b_{r+2,r} = \binom{r+2}{r}$ and the number of monomials of degree less than or equal to r in 3 variables is $b_{r+3,r} = \binom{r+3}{r}$. In particular, the number of monomials of degree less than or equal to $r-1$ in 3 variables is $b_{(r-1)+3,r-1} = \binom{r+2}{3}$. Every series $f \in k[[x,y,z]]$ is uniquely determined by its *coefficient sequence*, that is, the sequence $c_f : \mathbb{N} \to k$ of its coefficients placed according to the aforementioned ordering, namely:

$$c_f = (c_{f,1}, c_{f,2}, c_{f,3}, \dots) = (a_{0,0,0}, a_{1,0,0}, a_{0,1,0}, a_{0,0,1}, a_{2,0,0}, a_{1,1,0}, a_{1,0,1}, a_{0,2,0}, \dots) \in k^\infty.$$

Of course, for $\lambda, \mu \in k$, we have $c_{\lambda f + \mu g} = \lambda c_f + \mu c_g$. Let us consider the map defined in Section 1, $\rho_m : k^\infty \to k^m$. Then

$$\text{ord}\,(f) = r \Leftrightarrow \rho_{b_{r+2,3}}(c_f) = 0 \text{ and } \rho_{b_{r+3,3}}(c_f) \neq 0.$$

Similarly,

$$\text{ord}\,(f) \geq r \Leftrightarrow \rho_{b_{r+2,3}}(c_f) = 0.$$

DEFINITION 3.4. Let $f(x,y,z) \in k[[x,y,z]]$.

- The *σ-order* of $f(x,y,z)$ is defined as $\sigma\text{ord}\,(f(x,y,z)) = \text{ord}\,(\sigma(f(x,y,z)))$.
- The *σ-leading form* of $f(x,y,z)$ is $\sigma\text{LF}(f(x,y,z)) = \sigma^{-1}(\text{LF}(f(x,y,z)))$, where LF is the leading form of a power series.

· $f(x,y,z)$ is *σ-homogeneous* if $f(x,y,z) = \sigma\mathrm{LF}(f(x,y,z))$.

Remark 3.5. Clearly a σ-homogeneous (or homogeneous) power series must be a polynomial. Let us suppose that the σ-order (or order) of a σ-homogeneous power series (or homogeneous) is r. Each monomial appearing in $\sigma\mathrm{LF}(f)$ must have degree r (or the monomials appearing in $\mathrm{LF}(f)$). Since there are a finite number of monomials $a_{\alpha\beta\gamma}x^\alpha y^\beta z^\gamma$ verifying $\alpha n + \beta(n+1) + \gamma(n+2) = r$ (or $\alpha+\beta+\gamma = r$). It follows that if $f(x,y,z)$ is σ-homogeneous, then $f = \sigma\mathrm{LF}(f)$ is a polynomial.

Next, we give an example to better understand these concepts.

Example 3.6. Let us consider the power series $f(x,y,z) = xy^2 + z^3 + xyz + y^4$. Let us compare its order and leading form with its σ-order and σ-leading form.

$$\sigma(f(x,y,z)) = x^n y^{2(n+1)} + z^{3(n+2)} + x^n y^{n+1} z^{n+2} + y^{4(n+1)}\,.$$

Then,

$$\begin{aligned} &\sigma\mathrm{ord}\,(f(x,y,z)) = 3n+2\,; && \mathrm{ord}\,(f(x,y,z)) = 3\,;\\ &\sigma\mathrm{LF}(f(x,y,z)) = xy^2\,; && \mathrm{LF}(f(x,y,z)) = xy^2 + z^3 + xyz\,. \end{aligned}$$

Neither the σ-leading form nor the leading form of $f(x,y,z)$ match with itself, therefore it is not σ-homogeneous or homogeneous. Let us give an example of a σ-homogeneous power series. Let $g(x,y,z) = xy^2 + x^3z$. Then

$$\sigma(g(x,y,z)) = x^n y^{2(n+1)} + x^{3n} z^{n+2}\,.$$

Then, $\sigma\mathrm{ord}\,(g(x,y,z)) = 3n+2$, so $\sigma\mathrm{LF}(g(x,y,z)) = xy^2 + zx^3z = g(x,y,z)$. Therefore, $g(x,y,z)$ is σ-homogeneous.

Notation 3.7. Let W_r be the k-vector space defined as:

$$W_r = \{f(x,y,z) \in k[[x,y,z]] \,|\, f(x,y,z) \text{ is } \sigma\text{-homogeneous of } \sigma\mathrm{ord}\ = r\} \cup \{0\}\,.$$

Proposition 3.8. *The dimension of W_r is finite.*

Proof. Let E be the k-vector space defined as follows:

$$E = \langle x^\alpha y^\beta z^\gamma \,|\, \alpha,\beta,\gamma \le r\rangle\,.$$

Clearly $W_r \subseteq E$. The dimension of E is finite, therefore the dimension of W_r must be finite. □

Let $\overline{U}_r := W_r \cap k[[y,z]]$. Let $d_r = \dim W_r$ and $e_r = \dim \overline{U}_r$. Recall the notation in Section 2, where $S = \langle n+1, n+2\rangle$ is the numerical semigroup generated by the integers $n+1$ and $n+2$, and $\mathbb{Z}_L = \{i \in \mathbb{Z} \text{ such that } 0 \le i \le L\}$.

Remark 3.9. Let (β,γ) be a couple of integers such that $\beta,\gamma \ge 0$, and let $S = \langle n+1, n+2\rangle$. For a fixed $r \ge 0$ and some $\alpha \in \mathbb{N}$, the following statements are equivalent:

- $\beta(n+1)+\gamma(n+2)=r-\alpha n$,
- $\beta(n+1)+\gamma(n+2)\in S\cap\{r+n\mathbb{Z}\}\cap\mathbb{Z}_r$.

THEOREM 3.10. [**4**, Theorem 4.1.] *With the previous notations, in particular n is a fixed odd integer and $m=\frac{n+1}{2}$. We obtain:*

(1) $d_r=\sum_i e_i$, *where* $i\in S\cap\{r+n\mathbb{Z}\}\cap\mathbb{Z}_r$.

Especially

(2) $d_r\leq m$, *if* $r<n(n+1)$.
(3) $d_r=m+s$, *if* $n(n+s)\leq r<n(n+s+1)$ *and* $r<(n+1)(n+2)$, *for any* $s\geq 1$.

PROOF. Notice that the generators of W_r are the monomials $x^\alpha y^\beta z^\gamma$ such that,

$$\alpha n+\beta(n+1)+\gamma(n+2)=r\,.$$

Let

$$W_{r,\alpha}:=W_r\cap x^\alpha k[[y,z]]\,,$$
$$\overline{U}_{r,\alpha}:=\overline{U}_r\cap W_{r,\alpha}\,.$$

We have the following $1-1$ correspondence:

$$\begin{array}{ccc} W_{r,\alpha} & \longleftrightarrow & \overline{U}_{r,\alpha} \\ x^\alpha y^\beta z^\gamma & \to & y^\beta z^\gamma \\ x^\alpha y^\delta z^\epsilon & \leftarrow & y^\delta z^\epsilon\,. \end{array}$$

$W_{r,\alpha}$ is also generated by the monomials $x^\alpha y^\beta z^\gamma$, where the α is fixed and α and β satisfy the following equation:

$$\beta(n+1)+\gamma(n+2)=r-\alpha n\,.$$

Let us check that this correspondence is well defined. Given the monomial $x^\alpha y^\beta z^\gamma$ of $W_{r,\alpha}$, we have to prove that its image is contained in $\overline{U}_{r,\alpha}$. Clearly $y^\beta z^\gamma\in k[[y,z]]$. So we just have to see that its σ-order is $r-\alpha n$.

$$\begin{aligned}\text{Thus, } x^\alpha y^\beta z^\gamma\in W_r &\Rightarrow \alpha n+\beta(n+1)+\gamma(n+2)=r \\ &\Rightarrow \beta(n+1)+\gamma(n+2)=r-\alpha n\Rightarrow y^\beta z^\gamma\in W_{r-\alpha n}\,.\end{aligned}$$

Let us prove now that the inverse map is also well defined. Take $y^\delta z^\epsilon\in\overline{U}_{r,\alpha}$ and let us prove that, for a fixed α, the monomial $x^\alpha y^\delta z^\epsilon\in W_{r,\alpha}$. Clearly, it is contained in $x^\alpha k[[x,y]]$, so we have to prove that its σ-order is r. This is clear since $\overline{U}_{r,\alpha}=W_r\cap x^\alpha k[[x,y,z]]\cap k[[y,z]]$. Then,

$$\delta(n+1)+\epsilon(n+2)=r-\alpha n\,.$$

Therefore $\sigma\text{ord}\,(x^\alpha y^\delta z^\epsilon) = r$ and $x^\alpha y^\delta z^\epsilon \in W_{r,\alpha}$. To finish the proof of (1), we use the previous remark. Then we have this isomorphism:

$$\bigoplus_\alpha \overline{U}_{r,\alpha} \cong \bigoplus \overline{U}_i \text{ where } i \in S \cap \{r+\mathbb{Z}\} \cap \mathbb{Z}_r\,.$$

Since there exits a $1-1$ correspondence between $W_{r,\alpha}$ and $\overline{U}_{r-\alpha n}$. We obtain the following collection of isomorphisms:

$$\begin{aligned} W_r &= \bigoplus_\alpha W_{r,\alpha} \\ &\cong \bigoplus_\alpha \overline{U}_{r-\alpha n} \\ &= \bigoplus \overline{U}_i \text{ where } i \in S \cap \{r+\mathbb{Z}\} \cap \mathbb{Z}_r\,. \end{aligned}$$

Therefore $d_r = \sum e_i$ where $i \in S \cap \{r+n\mathbb{Z}\} \cap \mathbb{Z}_r$. This proves statement (1).
We now turn to the proof of (2) and (3). Suppose that $r < (n+1)(n+2)$. In particular $r < n(n+1)$. Let (β,γ) and (ϵ,δ) such that, for a fixed $0 \le \alpha \le r$, one has

$$\beta(n+1)+\gamma(n+2) = r-\alpha n = \epsilon(n+1)+\delta(n+2)\,.$$

So $(\beta-\epsilon)(n+1) = (\delta-\gamma)(n+2)$. Hence

$$\beta-\epsilon = u(n+2) \text{ and } \delta-\gamma = v(n+1)\,, \text{ for some } u,v \in \mathbb{N}\,.$$

Thus

$$\beta = u(n+2)+\epsilon \ge u(n+2)\,.$$

Then

$$\begin{aligned} r \ge r-\alpha n = \beta(n+1)+\gamma(n+2) &\ge u(n+2)(n+1)+\gamma(n+2) \\ &= (u(n+1)+\gamma)(n+2)\,. \end{aligned}$$

Therefore

$$(u(n+1)+\gamma)(n+2) \le r < (n+1)(n+2)\,.$$

It follows that $nun+1)+\gamma < n+1$ and necessarily $u=0$, so $\beta=\epsilon$ and $\gamma=\delta$.
This fact ensures that $e_i = \dim \overline{U}_i = 1$, for all $i < (n+1)(n+2)$. Then

$$d_r = \sum e_i = \text{Card}(S \cap \{r+n\mathbb{Z}\} \cap \mathbb{Z}_r)\,.$$

Now, let us prove (2). Take $r < n(n+1)$, which is equivalent to $r \le F(S)$. Indeed, recall from Section 2, that the Frobenius number of $S = \langle n+1, n+2\rangle$ is $n(n+1)-1$. Applying now Theorem 2.17, we have:

$$\text{Card}(S \cap \{r+n\mathbb{Z}\} \cap \mathbb{Z}_r) \le \text{Card}(S \cap \{r+n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) = \frac{F(S)+1}{2n} = \frac{n(n+1)}{2n}\,.$$

This proves the statement (2).
To prove (3), we assume $n(n+s) \le r < n(n+s+1)$ and $r < (n+1)(n+2)$ for

some $s \geq 1$. We already know that $d_r = \mathrm{Card}(S \cap \{r + n\mathbb{Z}\} \cap \mathbb{Z}_r)$. Since $s \geq 1$, then $r \geq n(n+s) \geq n(n+1) > F(S)$, where $F(S) = n(n+1) - 1$. Then

$$\mathrm{Card}(S \cap \{r + n\mathbb{Z}\} \cap \mathbb{Z}_r) = \\ \mathrm{Card}(S \cap \{r + n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) + \mathrm{Card}(S \cap \{r + n\mathbb{Z}\} \cap \{i : F(S) < i \leq r\}) \,.$$

Since $F(S)$ is the least positive integer not in S, the set $\{i : F(S) < i \leq r\} \subseteq S$. So, to end the proof it is enough to compute $\mathrm{Card}(\{r + \mathbb{Z}\} \cap \{i : F(S) < i \leq r\})$. Let us take an element i in the intersection of $\{r + n\mathbb{Z}\}$ with $\{i \,|\, F(S) < i \leq r\}$. So $i = r - un$ for some $u \in \mathbb{N}$, because i must be smaller than or equal to r. Since $F(S) < i$ and $F(S) = n(n+1) - 1$, then

$$n(n+1) \leq r - un \,.$$

Therefore $un \leq r - n(n+1)$. Dividing by n and using $r < n(n+s+1)$, then

$$u \leq \frac{r}{n} - \frac{n(n+1)}{n} < \frac{n(n+s+1)}{n} - (n+1) = s \,.$$

This proves,

$$\{r + n\mathbb{Z}\} \cap \{i \,|\, F(S) < i \leq r\} \subseteq \{r - un \,|\, 0 \leq u < s\} \,.$$

The other inclusion is clear, therefore

$$d_r = \mathrm{Card}(S \cap \{r + \mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) + \mathrm{Card}(S \cap \{r + \mathbb{Z}\} \cap \{i : F(S) < i \leq r\}) = m + s \,.$$

□

Definition 3.11. Let us consider the monomial $x^\alpha y^\beta z^\gamma$,

· The *associated binomial vector* is:

$$b(x^\alpha y^\beta z^\gamma) := (b_{\alpha,0}, \ldots, b_{\alpha,\alpha}, 0, \ldots) = b_\alpha \in k^\infty.$$

· The *associated binomial m-vector* is:

$$b_m(x^\alpha y^\beta z^\gamma) := \rho_m(b(x^\alpha y^\beta z^\gamma)) = (b_{\alpha,0}, \ldots, b_{\alpha,m}) \in k^m.$$

Let $\sum a_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma$ be σ-homogeneous. Then,

$$b(\sum a_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma) = \sum a_{\alpha\beta\gamma} b(x^\alpha y^\beta z^\gamma) \text{ and } b_m(\sum a_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma) = \sum a_{\alpha\beta\gamma} b_m(x^\alpha y^\beta z^\gamma) \,.$$

In general, let $f(x, y, z)$ be a power series,

· its associated binomial vector is:

$$b(f(x,y,z)) = b(\sigma\mathrm{LF}(f(x,y,z))) \,,$$

· and its associated binomial m-vector is:

$$b_m(f(x,y,z)) = \rho_m(b(f(x,y,z))) \,.$$

PROPOSITION 3.12. [**4**, Proposition 4.1.] *Let $f(x,y,z) \in P = P_n$. Then*

$$b_m(f(x,y,z)) = 0\,,$$

where n is a fixed odd integer and $m = \frac{n+1}{2}$.

PROOF. Assume $\sigma\text{ord}\,(f(x,y,z)) = r$. Consider the decomposition of f as the sum of its σ-leading form and the rest, $f(x,y,z) = g(x,y,z) + h(x,y,z)$, where $\sigma\text{LF}(f) = g(x,y,z)$. Let $a_{\alpha\beta\gamma}x^\alpha y^\beta z^\gamma$ be a monomial of $g(x,y,z)$. Therefore,

$$\rho(a_{\alpha\beta\gamma}x^\alpha y^\beta z^\gamma) = a_{\alpha\beta\gamma}t^{\alpha mn}(1+t^\lambda)^\alpha t^{m(n+1)\beta}t^{m(n+2)\gamma}\,.$$

Since that $\sigma\text{ord}\,(a_{\alpha\beta\gamma}x^\alpha y^\beta z^\gamma) = r$, then $\alpha n + \beta(n+1) + \gamma(n+2) = r$. By applying the Binomial Theorem, we obtain the following:

$$\rho(a_{\alpha\beta\gamma}x^\alpha y^\beta z^\gamma) = a_{\alpha\beta\gamma}t^{rm}(b_{\alpha,0}t^\lambda + \ldots + b_{\alpha,m-1}t^{\lambda(m-1)} + \ldots)\,.$$

We do the same for a monomial $a_{\epsilon\delta\mu}x^\epsilon y^\delta z^\mu$ of $h(x,y,z)$, whose order is $s > r$. Then

$$\rho(a_{\epsilon\delta\mu}x^\epsilon y^\delta z^\mu) = a_{\epsilon\delta\mu}t^{sm}(b_{\epsilon,0}t^\lambda + \ldots + b_{\epsilon,m-1}t^{\lambda(m-1)} + \ldots)\,.$$

Claim: The terms of the form $t^{rm+u\lambda}$ with $u < m$, only come from the σ-leading form of $f(x,y,z)$. Thus suppose that $t^{rm+u\lambda} = t^{sm+v\lambda}$. Since $s > r$, then $v < u < m$. On the other hand the equality implies $rm + u\lambda = sm + v\lambda \Leftrightarrow (s-r)m = (u-v)\lambda$. Since $(\lambda, m) = 1$ and $\lambda > m$, then $m|(u-v)$. Therefore $m < u - v < u < m$ and we arrive to a contradiction. So the elements of the form $t^{rm+u\lambda}$ can only be cancelled among them, in addition if $t^{rm+u\lambda} = t^{rm+v\lambda}$ implies $u = v$.
Let us compute $\rho(f(x,y,z))$:

$$\begin{aligned}\rho(f(x,y,z)) &= \rho(g(x,y,z)) + \rho(h(x,y,z)) \\ &= \sum a_{\alpha\beta\gamma}t^{rm}(b_{\alpha,0}t^\lambda + \ldots + b_{\alpha,m-1}t^{\lambda(m-1)}) \\ &\quad + \{\text{ the rest of the terms of } \rho(g(x,y,z)) \text{ and } \rho(h(x,y,z))\}\,.\end{aligned}$$

As we mentioned before, the terms of the first sum can only be cancelled among them, so the rest of the terms do not interfere in the sum. Since $f(x,y,z) \in P$, then $\rho(f(x,y,z)) = 0$. Thus, one must have

$$\sum a_{\alpha\beta\gamma}t^{rm}(b_{\alpha,0}t^\lambda + \ldots + b_{\alpha,m-1}t^{\lambda(m-1)}) = 0\,.$$

Hence

$$\sum a_{\alpha\beta\gamma}b_{\alpha,i} = 0\,.\text{ for } i \leq m-1\,,$$

and by definition,

$$b_m(f(x,y,z)) = 0.$$

□

Let us consider de k-vector space $V_r = W_r \cap (\{\sigma\text{-leading forms of elements in } P_n\} \cup \{0\})$. We denote $c_r = \dim V_r$.

THEOREM 3.13. [**4**, Theorem 4.2.] *With the previous notations, in particular n is a fixed odd integer and $m = \frac{n+1}{2}$. The vector space V_r is the kernel of the mapping*

$$b_m : W_r \longrightarrow k^m .$$

Moreover,

(1) $c_r = 0$ *if* $r < n(n+1)$.
(2) $c_r = d_r - m$ *if* $r \geq n(n+1)$.
(3) $c_r = 1$ *if* $n(n+1) \leq r < n(n+2)$.

PROOF. Remark that W_r is generated by the monomials $\{x^\alpha y^\beta z^\gamma\}$ such that:

$$\alpha n + \beta(n+1) + \gamma(n+2) = r .$$

Considering the proof given in Theorem 3.10, for $r < (n+1)(n+2)$ since $x^\alpha y^\beta z^\gamma = x^\alpha y^\epsilon z^\delta$, then $\beta = \epsilon$ and $\gamma = \delta$. Therefore, the elements of $\{x^\alpha y^\beta z^\gamma\}$ are determined by the α index. Thus,

$$d_r = \dim W_r = \mathrm{Card}(\{x^\alpha y^\beta z^\gamma\}_{\alpha n+\beta(n+1)+\gamma(n+2)=r}) = \mathrm{Card}(\{\rho_m b_\alpha\}) .$$

By Theorem 3.10, we know that $dr < m$. Then, by Theorem 1.13, we affirm that $\{\rho_m b_\alpha\}$ is a set of linearly independent vectors. Just by applying the previous definitions, we conclude that the set of associated m-binomial vectors $\{b_m(x^\alpha y^\beta z^\gamma)\}$ are linear independent. The map

$$b_m : W_r \longrightarrow k^m ,$$

is injective since $\{b_m(x^\alpha y^\beta z^\gamma)\}$ are linear independent vectors. By Proposition 3.12,

$$V_r \subset \ker b_m = 0 \Rightarrow V_r = 0 = \ker b_m .$$

Now, let us prove (2) and (3). First, let us prove that b_m is surjective. We consider an element $s \in S \cap \{r + n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}$, where S is the numerical semigroup, $S = \langle n+1, n+2\rangle$. Then,

$$s = \beta_i(n+1) + \gamma_i(n+2) \qquad \beta_i , \gamma_i \in \mathbb{N} .$$

Therefore for some $\alpha_i \in \mathbb{N}$, we have

$$\beta_i(n+1) + \gamma_i(n+2) = r - \alpha_i n \Leftrightarrow \alpha_i n + \beta_i(n+1) + \gamma_i(n+2) = r .$$

Thus, $x^{\alpha_i} + y^{\beta_i} + z^{\gamma_i} \in W_r$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. We can consider the family of elements of W_r given by $\{x^{\alpha_i} y^{\beta_i} z^{\gamma_i}\}$, such that $\beta_i(n+1)+\gamma_i(n+2)$ is an element of $S \cap \{r+n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}$. Clearly,

$$\mathrm{Card}(b_{\alpha_i}) = \mathrm{Card}(S \cap \{r + n\mathbb{Z}\} \cap \mathbb{Z}_{F(S)}) = m .$$

By applying Theorem 1.13, the set $\{\rho_m b_{\alpha_i}\}$ forms a basis of k^m. Considering the definition of associated m-binomial vector,

$$\{\rho_m b_{\alpha_i}\} = \{b_m(x^{\alpha_i}y^{\beta_i}z^{\gamma_i})\}\,.$$

The previous discussion tell us that the monomials $\{x^{\alpha_i}y^{\beta_i}z^{\gamma_i}\}_{0\leq i\leq m}$ are contained in W_r and are part of the generators of W_r. Then, the set $\{b_m(x^{\alpha_i}y^{\beta_i}z^{\gamma_i})\}$ is in the image of b_m, which is contained in k^m. Therefore,

$$m = \mathrm{Card}(\{b_m(x^{\alpha_i}y^{\beta_i}z^{\gamma_i})\}) \leq dim\mathrm{Im}(b_m) \leq m\,,$$

and b_m is surjective. Applying the Theorem of Dimension for vector spaces, we have the following equation:

$$d_r = \dim W_r = m + \dim\ker b_m\,.$$

By showing that $Vr = \ker b_m$, we end the proof of the theorem. Clearly $V_r \subseteq \ker b_m$, so it is enough to prove the other inclusion. Let $f(x,y,z) \in \ker b_m$ and let us see that $f(x,y,z) \in V_r$, i.e. is a σ-leading form of an element of P_n. Let us find a family of power series $\{g_i\}$ for $i \geq rm + m\lambda$, such that:

(1) ord $\rho(g_i(x,y,z)) = s \geq i\,.$
(2) ord $\rho(g_{i+1}(x,y,z) - g_i(x,y,z)) \geq i\,.$
(3) $\sigma\mathrm{LF}(g_i(x,y,z)) = f(x,y,z)\,.$
(4) ord $(g_{i+1}(x,y,z) - g_i(x,y,z)) \geq \frac{i-m\lambda}{m(n+2}\,.$

Let us proceed by induction, $i = rm + m\lambda$, $g_i(x,y,z) = f(x,y,z)$. Clearly,

$$\rho(f(x,y,z)) = \sum a_{\alpha,\beta,\gamma}b_{\alpha,m}t^{rm+m\lambda} + \dots\,,$$

where the terms of order less than $rm + m\lambda$, are cancelled out because $b_m(f(x,y,z)) = 0$. So ord $\rho(f(x,y,z)) \geq rm + m\lambda = i$. Since $f(x,y,z)$ is σ-homogeneous, then $\sigma\mathrm{LF}(f) = f$. Therefore conditions (1) and (3) are satisfied. In this first step, conditions (2) and (4) are void. For the general case, let us suppose that there exist an element $g_i(x,y,z)$ for $i \geq rm + m$ verifying the previous conditions. Now let us construct the element g_{i+1}. Let $s =$ ord $(\rho(g_i(x,y,z)))$, we can assume that $s \in u\lambda + m\mathbb{Z}$, with $0 \leq u < m$. Then,

$$s - (u\lambda + rm) \geq rm - m\lambda - (u\lambda + rm) = (m-u)\lambda \geq \lambda > n(n+1)m\,,$$

recall that the last inequality comes by the choice of λ. Observe that the last integer not in S is

$$F(S) = n(n+1) - 1\,.$$

So we can assure that $s - (u\lambda + rm) \in mS$. Therefore, there exist $\beta, \gamma \in \mathbb{N}$ such that

$$s - (u\lambda + rm) = \beta(n+1)m + \gamma(n+2)m\,.$$

Then we conclude that ord $\rho(y^\beta z^\gamma) = s - (u\lambda + rm)$. Now, since $b_m : W_r \longrightarrow k^m$ is surjective, there exist $h(x,y,z) \in W_r$ such that $b_m(h(x,y,z)) = (0,\ldots,1,0,\ldots,0)$, where 1 is in the position $u+1$. I.e. the binomial coefficients verify that $b_{i,\alpha} = 0$ for $i \neq u$ and ord $(\rho(h(x,y,z)) = rm + u\lambda$. Then,

$$\text{ord }(\rho(y^\beta z^\gamma h(x,y,z))) = s \text{ and } \sigma\text{ord }(y^\beta z^\gamma h(x,y,z)) = \sigma\text{ord }(y^\beta z^\gamma) + (\sigma\text{ord }(h(x,y,z)) < r\,.$$

For some $a \in k$, we have constructed $g_{i+1}(x,y,z) = g_i(x,y,z) + ay^\beta z^\gamma h(x,y,z) \in k[[x,y,x]]$, such that:

(1) ord $(\rho(g_i(x,y,z) + ay^\beta z^\gamma h(x,y,z))) \geq s$.
(2) ord $(\rho(g_{i+1}(x,y,z) - g_i(x,y,z))) =$ ord $(\rho(ay^\beta z^\gamma h(x,y,z))) = s \geq i$.
(3) $\sigma\text{LF}((g_{i+1}(x,y,z)) = \sigma\text{LF}((g_i(x,y,z)) = f(x,y,z)$.
(4)

$$\text{ord }(g_{i+1}(x,y,z) - g_i(x,y,z)) = \text{ord }(ay^\beta z^\gamma h(x,y,z)) =$$
$$\beta + \gamma + \text{ord }(h(x,y,z)) = \frac{(\beta + \gamma + \text{ord }(h(x,y,z)))(n+2)m}{(n+2)m}$$
$$\geq \frac{s - (rm + u\lambda) + rm}{m(n+2} \geq \frac{i - m\lambda}{m(n+2)}\,.$$

Let us note the floor function for of $\frac{i-m\lambda}{m(n+2)}$ as r_i. There exist a uniquely determined power series $g(x,y,z) \in k[[x,y,z]]$ verifying the following conditions:

· ord $\rho(g - g_i) \geq i$.
· $\sigma\text{LF}(g) = f(x,y,z)$.
· ord $(g - g_i) \geq r_i$.

The construction of g is not evident so we will clarify it in a remark at the end of the proof. Now let us prove that $\rho(g(x,y,z)) = 0$. We proceed by contrapositive, supposing $\rho(g) \neq 0$. Then, for some $N \in \mathbb{N}$, ord $\rho(g(x,y,z)) = N$. Let us take $g_{N+1}(x,y,z)$ with ord $\rho(g_{N+1}) \geq N+1 > N$. According to the construction of g,

$$\text{ord }\rho(g - g_{N+1}) \geq N+1\,.$$

Therefore $\rho(g)$ and $\rho(g_{N+1})$ agree up to order N. Since $\rho(g)$ has order N, then ord $\rho(g_{N+1}) = N$, which is a contradiction. Thus,

$$\rho(g(x,y,z)) = 0\,.$$

So, we can affirm that $f(x,y,z) \in V_r$. Therefore,

$$\ker b_m = V_r \text{ and } c_r = d_r - m\,.$$

The statement (3) is proved by considering (3) of Theorem 3.10 and take $s = 1$. Therefore,

$$c_r = d_r - m = m + 1 - m = 1\,.$$

□

REMARK 3.14. Let $f \in k[[x,y,z]]$ be a σ-homogeneous power series of σ-order $r \geq 1$. Let $\{r_i\}_{i\geq 1}$ be an ascending chain of integer numbers which tends to infinity. Let $\{g_i\}_{i\geq 1}$ be a sequence of power series such that $\sigma\text{LF}(g_i) = f$, ord $(g_{i+1} - g_i) \geq r_i$, ord $(\rho(g_i)) \geq i$ and ord $(\rho(g_{i+1} - g_i)) \geq i$. Then there exists a uniquely determined power series $g \in k[[x,y,z]]$ with $\sigma\text{LF}(g) = f$ and ord $(g - g_i) \geq r_i$. Moreover ord $(\rho(g - g_i)) \geq i$.
To describe g in a uniquely way, it is enough to describe its coefficient sequence c_g. According to the remark 3.3,

$$\text{ord } (g_{i+1} - g_i) \geq r_i \Leftrightarrow \rho_{b_{r_i+2,3}}(c_{g_{i+1}}) = \rho_{b_{r_i+2,3}}(c_{g_i}). \tag{1}$$

Thus, from 1 to $b_{r_1+2,3}$, let the coefficients of g be those of g_1. Concretely, $\rho_{b_{r_1+2,3}}(c_g) = \rho_{b_{r_1+2,3}}(c_{g_1})$. In other words, g and g_1 agree up to order $r_1 - 1$. From $b_{r_1+2,3} + 1$ to $b_{r_2+2,3}$, let the coefficients of g be equal to those of g_2. In fact, using (1), this is equivalent to say that the coefficients of g and g_2 agree up to the $b_{r_2+2,3}$-th term, because the first $b_{r_1+2,3}$ coefficients of g_1 and g_2 agree. Recursively, let the coefficients of g from $b_{r_i+2,3} + 1$ to $b_{r_{i+1}+2,3}$ be those of g_{i+1}. In other words, the series g and g_{i+1} agree up to order $r_{i+1} - 1$ and so ord $(g - g_{i+1}) \geq r_{i+1}$.
From this construction, it seems reasonable to think that ord $(\rho(g - g_i)) \geq i$. From here we deduce that $\rho(g)$ tends to infinity. However the proof is not clear. We assume this results from Moh's claim. He defined the power series $g = \lim_{i\to\infty} g_i$ and he assert that ord $(\rho(g)) = \infty$.

In order to understand and prove the next theorem we stablish the following notations. First, let us generalize the concept of the order of a mapping. Let α be

$$\begin{array}{rccc} \alpha: & k[[x,y,z]] & \longrightarrow & k[[x,y,z]] \\ & x & \mapsto & x^{\beta_1} \\ & y & \mapsto & y^{\beta_2} \\ & z & \mapsto & z^{\beta_3} \end{array}$$

We define the concepts of α-order, α-leading form and α-homogeneous as in Definition 3.4. The α-order of $f(x,y,z) \in k[[x,y,z]]$ is $\alpha\text{ord } (f(x,y,z)) = \text{ord } (\alpha(f(x,y,z)))$. The α-leading form of $f(x,y,z)$ is $\alpha\text{LF}(f(x,y,z)) = \alpha^{-1}(\text{LF}(f(x,y,z)))$. Finally, a power series is α-homogeneous if $f(x,y,z) = \alpha\text{LF}(f(x,y,z))$.
Let $\beta = \min(\beta_1, \beta_2, \beta_3)$ and let w_r be defined as follows:

$$w_r = \{f(x,y,z) \in k[[x,y,z]] | f(x,y,z) \text{ is } \alpha\text{-homogeneous and } \alpha\text{ord } (f(x,y,z)) = r\}.$$

The following lemma will be used in the proof of Theorem 3.16.

LEMMA 3.15. *Let us consider a set of power series* $\{f_1, \ldots, f_n\}$. *Let* $\{h_1, \ldots, h_n\}$ *be their* α*-leading forms. Let* $s = \min\{\alpha\text{ord}\,(f_i)\}$, *if*

$$g(x,y,z) = \sum g_i(x,y,z) f_i(x,y,z)\,, \text{ where } g_i(x,y,z) \in k[[x,y,z]] \text{ and } s < \alpha\text{ord}\,(g) < s+\beta.$$

Then,

$$\alpha\text{LF}(g(x,y,z)) = \sum g_i h_i(x,y,z)\,, \qquad g_i \in k\,.$$

PROOF. First, let us consider that $\alpha\text{ord}\,(g(x,y,z)) = s$. We want to see the shape of its α-leading form. Therefore, we choose the elements of g with α-order r. The only possible candidates are the α-leading forms of the f_i with α-order r, multiplied by a constant $g_i(0,0,0)$. The rest of the elements have greater α-order. Therefore,

$$\alpha\text{LF}(g(x,y,z)) = \sum g_i h_i(x,y,z)\,; \qquad g_i \in k\,.$$

Where $g_i = g_i(0,0,0)$ for i such that $\alpha\text{ord}\,(h_i) = r$ and $g_i = 0$ for i such that $\alpha\text{ord}\,(h_i) > r$. Now let us take $\alpha\text{ord}\,(g) = s+1$. Our candidates for the α-leading form are:

(1) $\overline{g_i}(x,y,z)h_i$ where ord $(h_i) = s$.
(2) $g_i(0,0,0)h_i$ where ord $(h_i) = s+1$.

Let us see that the first candidate is not good enough. The power series $\overline{g_i}(x,y,z)$ is composed by some monomials of $g(x,y,z)$. The condition to be in the $\alpha\text{LF}(g)$ is the following:

$$\alpha\text{ord}\,(\overline{g_i}h_i) = s+1\,.$$

However,

$$\alpha\text{ord}\,(\overline{g_i}h_i) = \alpha\text{ord}\,(\overline{g_i}) + \alpha\text{ord}\,(h_i) = \alpha\text{ord}\,(\overline{g_i}) + s\,.$$

This means that $\alpha\text{ord}\,(\overline{g_i}) = 1$, nevertheless $\alpha\text{ord}\,(\overline{g_i}) \geq \beta$. So $\alpha\text{ord}\,(\overline{g_i}h_i) \geq \beta + s > 1 + s$. Thus,

$$\alpha\text{LF}(g(x,y,z)) = \sum g_i h_i(x,y,z)\,, \text{ where } g_i \in k \text{ for } i \text{ such that } \alpha\text{ord}\,(h_i) > s\,.$$

Where the constants g_i are zero when $\alpha\text{ord}\,(h_i) > s+1$. Recursively, we apply the same reasoning when the α-order of g is growing up to $s+\beta$. We obtain that for each $g(x,y,z)$,

$$\alpha\text{LF}(g(x,y,z)) = \sum g_i h_i(x,y,z)\,, \text{ where } g_i \in k\,, \text{ for } i \text{ such that } \alpha\text{ord}\,(h_i) > s+j-1\,.$$

Remark that the constants g_i are zero when $\alpha\text{ord}\,(h_i) > s+j$. □

THEOREM 3.16. [**4**, Theorem 4.3.] *Let* Q *be an ideal of* $k[[x,y,z]]$. *Let*

$$s = \min\{\alpha\text{ord}\,(f(x,y,z)) | f(x,y,z) \in Q\}\,.$$

Let N *be the minimum number of generators of* Q, *let*

$$v_r = w_r \cap \{\alpha\text{- leading forms of } Q\} \cup \{0\}\,.$$

Then,

$$N \geq r = \sum_i \dim v_i \,, \qquad s \leq i < s + \beta \,.$$

PROOF. We want to build inductively a system of generators for Q with N elements. So that the α- order of each element increases and letting $N \geq \sum \dim(vi)$ for $s \leq i < s+\beta$. Let $\{g_1, \ldots, g_N\}$ be at system of generators of Q and let $\{h_1, \ldots, h_N\}$ be their α- leading forms. Then, let us consider a set of elements in Q, $\{g_{i,1}, \ldots, g_{i,d_i}\}$, such that their α-leading forms $\{h_{i,1}, \ldots h_{i,d_i}\}$ constitute a basis for the v_i. For the first case $i = s$, we can express the elements $\{g_{s,1}, \ldots, g_{s,d_s}\}$ as a combination of $\{g_1, \ldots, g_N\}$:

$$g_{s,j} = \sum_{i=1}^{N} u_{i,j}(x,y,z) g_i(x,y,z) \quad \forall 1 \leq j \leq d_s \,.$$

Then, we consider the α-leading forms of each part of the equality. By applying Lemma 3.15, we obtain the following:

$$h_{s,j} = \sum_{i=1}^{N} u_{i,j} h_i(x,y,z) \,,$$

the $u_{i,j}$ are equal to zero when $\alpha\text{ord}\,(h_i) > s$. Therefore, the set $\{h_1, \ldots h_{d_s}\}$ forms a basis for v_s. This tells us that at least the set $\{g_1, \ldots, g_N\}$ must have d_s elements, in other words $N \geq d_s$. Finally, we must assure that the α-order of the following $g_j(x,y,z)$ increases. By definition the set $\{h_1(x,y,z), \ldots, h_{d_s}(x,y,z)\}$ generate the α-leading forms of α-order s. Then, there exists $a_{i,j} \in k$ such that

$$\alpha\text{LF}(g_j(x,y,z)) = \sum_{i=1}^{d_s} a_{i,j} h_i(x,y,z) \quad \forall j > d_s \,.$$

Replacing the $g_j(x,y,z)$ when $j > d_s$ by $g_j(x,y,z) + \sum_{i=1}^{d_s} a_{i,j} g_i(x,y,z)$, we force the new $g_j(x,y,z)$ to have α-order greater than s. Inductively for $s' > s$, the system of generators $\{g_1(x,y,z), \ldots, g_N(x,y,z)\}$ verifies:

- $\{h_j(x,y,z) \mid \sum_{s \leq i < d_{\overline{s}}} d_i < j \leq \sum_{s \leq i < d_{\overline{s}+1}} d_i\}$ forms a basis for $v_{\overline{s}}$, for all $\overline{s} < s'$.
- $N \geq \sum_{s \leq i < s'} d_s$.
- $\alpha\text{ord}\,(g_j(x,y,z)) > s' - 1$ for all $j > \sum_{s \leq i < s'} d_i$.

Let us prove that the inductive process works, i.e. for $s'+1$ the previous statements are true. Let us consider the set $\{g_{s',1}, \ldots, g_{s',d_{s'}}\}$, we can express each $g_{s',j}$ as follows:

$$g_{s',j} = \sum_{i=1}^{N} u_{i,j}(x,y,z) g_i(x,y,z) \quad \forall 1 \leq j \leq d_s \,.$$

Let us suppose that for some $i \leq \sum_{s\leq i<s'} d_i$, $u_{i,j}(x,y,z)$ is a unit. Then by taking

$$M = \min\{(g_j(x,y,z) \,|\, u_{i,j}(x,y,z) = 1\}\,,$$

we have the following:

$$\alpha\text{ord}\,(g_{s',j}(x,y,z)) = \alpha\text{ord}\,(g_M(x,y,z))\,.$$

However, by construction of the $\{g_j(x,y,z)\}_{1\leq j\leq \sum_{s\leq i<s'} d_i}$, the α-order of $g_M(x,y,z)$ is less than s' but the order of $g_{s',j}$ is exactly s', so we arrive to a contradiction. Therefore,

$$u_{i,j}(x,y,z) \neq 1 \text{ and } \alpha\text{ord}\,(u_{i,j}(x,y,z)g_i(x,y,z)) \geq \beta + s > s' \quad \forall i \leq \sum_{s\leq i<s'} d_i\,.$$

Now, let us consider the α-leading forms of $g_{s',j}(x,y,z)$. By applying again Lemma 3.15, we get to:

$$h_{s',j} = \sum_{i=1}^{N} u_{i,j} h_i(x,y,z)\,,$$

where $u_{i,j}$ are constants equal to zero, when $\alpha\text{ord}\,(h_i) > s'$. Therefore, the set

$$\{h_j(x,y,z) \,|\, \sum_{s\leq i<d_{s'}} d_i < j \leq \sum_{s\leq i<d_{s'+1}} d_i\}\,,$$

forms a basis for v'_s, proving the first statement. Clearly, there must exist at least, $\sum_{s\leq i<s'} d_i$ of $g_j(x,y,z)$, such that their α-leading forms are a basis for $v_s,\ldots,v'_s$. That implies $N \geq \sum_{s\leq i<s'} d_i$. Finally, we can assume the existence of some $a_{i,j} \in k$ verifying the following:

$$\sum a_{i,j} h_i(x,y,z) = \{\text{ the monoids of } \alpha(g_j) \text{ with } \alpha\text{-order}s\}\,,$$

for $\sum_{s\leq i<s'} d_i < i \leq \sum_{s\leq i<s'+1} d_i$ and $\forall j > \sum_{s\leq i<s'+1} d_i$. For $j > \sum_{s\geq i<s'+1} d_i$, we replace $g_j(x,y,z)$ by $g_j(x,y,z) + \sum a_{i,j} g_i(x,y,z)$. Then,

$$\alpha\text{ord}\,(g_j(x,y,z)) > s'\,.$$

We have proved that the inductive process works. Therefore letting $s' = s + \beta$ we have proved that $N \geq \sum_{s\leq i<s+\beta} d_i = r$. □

Now we have enough tools to state the main result of this chapter.

THEOREM 3.17. [**4**, Theorem 4.4.] *There are at least n generators for P_n.*

PROOF. Let us consider Theorem 3.16 and the following modified notation:

$$\alpha = \sigma\,, \quad Q = P\,, \quad \omega_r = W_r\,,$$
$$\beta = n\,, \quad d_i = c_i\,.$$

By Theorem 3.13, we know that the minimum σ-order of the elements in P_n is $n(n+1)$. Below these orders $c_i = 0$, which implies $V_i = \{0\}$. Therefore, by Theorem 3.16,

$$\text{the minimum number of generators of } P_n \geq \sum c_i \,,$$

where $n(n+1) \leq i < n(n+1) + n$. Applying again Theorem 3.13 and summing up all together, we obtain

$$\text{the minimum number of generators of } P_n \geq \sum c_i = \sum 1 = n \,.$$

□

4. Minimal generators of P_n

In the previous section we have set that P_n needs at least n generators. This section contains the proof that there are exactly $n+1$ elements generating P_n. We keep the notation of Section 3. First of all, let us state a key lemma . Let us consider the mapping

$$\rho : k[[x, y, z]] \longrightarrow k[[t]] \,,$$

where $P_n = ker\rho$.

REMARK 4.1. Let J be an ideal of $k[[x, y, z]]$. The σ-leading ideal of J is, by definition,

$$\sigma\text{LI}(J) = \langle \sigma\text{LF}(f) | f \in J \rangle \,.$$

In particular, $\sigma\text{LI}(P_n) = \langle h_1, \ldots, h_n \rangle$ where h_i are the generators of the k-vector spaces V_i.

LEMMA 4.2. [**5**, Lemma 2.1.] *Let $f_1, \ldots, f_s$ elements be in P_n with σ-leading forms generating the σ-leading ideal of P_n. Then,*

$$(f_1, \ldots, f_s) = P_n \,.$$

PROOF. Set

$$\sigma\text{LF}(f_i) = h_i = \sigma\text{-leading form of } f_i \,,$$
$$\sigma\text{LI}(P_n) = \text{ the } \sigma\text{-leading ideal of } P_n \,.$$

Thus, by hypotheses $\sigma\text{LI}(P_n) = \langle \sigma\text{LF}(f) | f \in P_n \rangle = \langle h_1, \ldots, h_s \rangle$. Let $g(x, y, z) \in P_n$. Therefore its σ-leading form is in the ideal $\sigma\text{LI}(P_n)$, so

$$\sigma\text{LF}(g(x, y, z)) = \sum_{i=0}^{s} g_i(x, y, z) h_i(x, y, z) \,,$$

$g_i(x, y, z) \in k[[x, y, z]]$. Let $G(x, y, z)$ such that

$$G(x, y, z) = g(x, y, z) - \sum g_i(x, y, z) f_i(x, y, z) \,.$$

Moreover, we can assume that no term of G is divisible by h_i. Otherwise there would exist at least a term of G of the form $G_i h_i$. Therefore we can consider the following construction:

$$g(x,y,z) = \sum_{j=1}^{s} g'_j(x,y,z) f_j(x,y,z) + G'(x,y,z)\,.$$

Where $g'_j = g_j \quad \forall j \neq i$ and $g'_i = g_i + G_i$. And $G' = G - G_i h_i - G_i(f_i - h_i)$. In particular, if $G \neq 0$ we can assume that its σ-leading form is not divisible by $h_i(x,y,z)$. On the other hand, since P_n is an ideal and $g\,, \sum g_i f_i \in P_n$ then $G \in P_n$. Therefore, $\sigma\mathrm{LF}(G) = (h_1, \ldots, h_s)$ which implies $G = 0$. □

THEOREM 4.3. [**5**, Theorem 2.1.] *The prime ideal P_n needs at least $n+1$ generators. In particular there are $f_1, \ldots, f_{n+1} \in P_n$ such that:*

(1) The σ-leading forms of f_i are in $V_{n(n+1)+i-1}$, for $i = 1, \ldots, n$.
(2) The subspace $V_{n(n+2)}$ is generated by $x \cdot \sigma\mathrm{LF}(f_1)$ and f_{n+1}.

Moreover any $f_1, \ldots, f_{n+1}$ satisfying this two conditions generate P_n.

PROOF. Let us consider a set of generators of P_n, $\{g_1, \ldots, g_s\}$. By theorem 3.16 and 3.17, there exist $\{f_1, \ldots, f_n\}$ such that:

- The σ-leading form of f_i, generates the subspace V_i, for $n(n+1) \leq i < n(n+2)$.
- $\sigma\mathrm{ord}\,(f_i) = n(n+1) + (i-1)$ for all $i \in \{1, \ldots, n\}$.
- The set $\{f_1, \ldots, f_n, g_{n+1}, \ldots, g_s\}$ is a set of generators for P_n. Such that

$$\sigma\mathrm{ord}\,(g_j) \geq n(n+2) \text{ for all } j \in \{n+1, \ldots, s\}\,.$$

Let us prove (2). The subspace $V_{n(n+2)}$ has dimension 2, recall Theorem 3.13. Let us consider all the possibles σ-leading forms of the set $\{f_1, \ldots, f_n\}$, and let us take an element $f(x,y,z) \in k[[x,y,z]]$. We want to prove that only one of the generators of $V_{n(n+2)}$ is of the form,

$$f(x,y,z)\sigma\mathrm{LF}(f_i), \quad i \in \{1, \ldots n\}\,.$$

Therefore, the second generator must be the σ-leading form of the element f_{n+1}. The condition to be a generator of $V_{n(n+2)}$ is $\sigma\mathrm{ord}\,(f(x,y,z)h_i) = n(n+2)$. The only possibles candidates are h_1 and $f(x,y,z) = ax + \ldots$. Then, (2) has been proved, by construction implies (1). Therefore, P_n needs at least $n+1$ generators. Finally, we want to prove that any $f_1, \ldots, f_{n+1}$ verifying conditions (1) and (2), generate P_n. Let us recall the previous lemma, 4.2. It is enough to prove that their σ-leading forms $\{h_1, \ldots, h_{n+1}\}$, generate the σ-leading ideal of P_n. Clearly, $\{h_1, \ldots, h_{n+1}\}$ generates the vector spaces $V_{n(n+1)}, \ldots, V_{n(n+2)}$. Therefore, it is enough to prove that V_r for $r > n(n+2)$ can be generated by $\{h_1, \ldots h_{n+1}\}$. We distinguish two cases,

(1) The V_r where $n(n+2) < r < (n+1)(n+2)$.

(2) The V_r where $r \geq (n+1)(n+2)$.

Let us start by (1). Let us consider the semigroup $S = \langle n+1, n+2 \rangle$. Then, we consider the elements of S with residue $r-1$ mod n, i.e. the elements of the form $tn + (r-1)$ where $t \in \mathbb{Z}$. By Theorem 2.17,

$$\mathrm{Card}(S \cap \{(r-1) + n\mathbb{Z}\} \cap \mathbb{Z}_{n(n+1)-1}) = m\,.$$

Therefore, we can consider m elements $d_{i_1 j_1}, \ldots, d_{i_m j_m}$ of S, with residue $r-1$. We can express them as follows:

$$d_{i_s j_s} = \beta_s(n+1) + \gamma_s(n+2) \text{ for } j = 1, \ldots, m\,.$$

This elements must be positive, so $\beta_s, \gamma_s \geq 0$. Moreover, we can assume $0 \leq d_{ij} \leq n(n+1)$. Let us denote the elements $d_{ij} = r - 1 + tn$, $t \in \mathbb{Z}$. Summing up all together, we obtain the followings inequalities:

$$n(n+2) < d_{ij} - tn + 1 = r \leq n(n+1) - tn + 1\,;$$
$$n(t+1) < 1\,.$$

Therefore $t \leq -1$. Now, let us consider the monomials $x^{\alpha_1} y^{\beta_1+1} z^{\gamma_1}, \ldots, x^{\alpha_m} y^{\beta_m+1} z^{\gamma_m}$ of W_r. We can assume $\alpha_i > 0$ for $i = 1, \ldots, m$:

$$\alpha_i n + \beta_i(n+1) + n + 1 + \gamma_i(n+2) = r\,;$$
$$\alpha_i n + n + 1 + d_{ij} = r\,;$$
$$\alpha_i n + n + 1 + r - 1 + tn = r\,;$$
$$(\alpha_i + t + 1)n = 0\,.$$

Therefore, $\alpha_i = -t - 1 > 1 - 1 = 0$. Moreover ,this α_i are different between them. This idea follows from fixing the β_i, γ_i as we explain in Proposition 3.12. Next we consider the morphism

$$b_m : W_r \longrightarrow k^m\,.$$

By Theorem 1.13 and Definition 3.11, the set $\{b_m(x^{\alpha_1} y^{\beta_1+1} z^{\gamma_1}), \ldots, b_m(x^{\alpha_m} y^{\beta_m+1} z^{\gamma_m})\}$ forms a basis of k^m. Let us consider an element of W_r, this element can be expressed as a linear combination of the monomials generators of W_r:

$$f(x,y,z) = \sum a_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma\,.$$

Therefore, without lose of generality we can follow the proof for a monomial $x^\alpha y^\beta z^\gamma \in W_r$. Moreover, we can assume that either α or β are greater than zero. Otherwise $\alpha = \beta = 0$. Therefore

$$\alpha n + \beta(n+1) + \gamma(n+2) = r\,,$$
$$\gamma(n+2) = r\,.$$

Considering the bounds of r, $n(n+2) < r < (n+1)(n+2)$, then we obtain:

$$n < \gamma < n+1\,,$$

which is a contradiction. Finally, we build an element of $\ker b_m$, starting with the monomial $x^\alpha y^\beta z^\gamma$. We can assume that any element of the kernel has this structure. The image of this monomial can be expressed as a linear combination of $\{b_m(x^{\alpha_i} y^{\beta_i+1} z^{\gamma_i})\}_{i=1,\dots,m}$, in the following way:

$$b_m(x^\alpha y^\beta z^\gamma) = \sum a_{\alpha_i} b_m(x^{\alpha_i} y^{\beta_i+1} z^{\gamma_i})\,.$$

Therefore,

$$x^\alpha y^\beta z^\gamma - \sum a_{\alpha_i} x^{\alpha_i} y^{\beta_i+1} z^{\gamma_i} \in \ker b_m = V_r \text{ (see Theorem 3.13) }.$$

Let us suppose $\alpha > 0$. This allows to divide by x, $\alpha_i - 1 \geq 1$ and $\alpha - 1 \geq 0$. Therefore, dividing the previous expression by x, we obtain an element of V_{r-n}. On the other hand, let us suppose $\beta > 0$, then dividing by y we obtain an element of V_{r-n-1}. So any element of V_r can be expressed as an element of V_{r-n}, V_{r-n-1} by multiplying by x or y. This means that, every element of V_r for $n(n+2) < r < (n+1)(n+2)$ can be generated by $\{h_1, \dots, h_{n+1}\}$.

Let us prove case (2). Here we apply a similar reasoning. In this case let us take the elements $d_{i_1 j_1}, \dots, d_{i_m j_m}$ of $S = \langle n+1, n+2\rangle$ with residue $r-3$. By the same argument as before, we can assume the existence of m elements in the set

$$S \cap \{r - 3 + n\mathbb{Z}\} \cap \mathbb{Z}_{n(n+1)-1}\,.$$

Let us express this elements as follows:

$$d_{i_t j_t} = \beta_j(n+1) + \gamma_j(n+2)\,; \qquad \forall j = 1, \dots, m\,.$$

We denote $d_{ij} = r - 3 + tn$. Summing all up, we get the following inequalities:

$$(n+1)(n+2) \leq d_{ij} - tn + 3 \leq n(n+1) - tn + 3\,;$$
$$(2+t)n \leq 1\,.$$

Therefore, $t \leq -2$. Now, let us consider the monomials $x^{\alpha_1} y^{\beta_1+1} z^{\gamma_1+1}, \dots, x^{\alpha_m} y^{\beta_m+1} z^{\gamma_m+1}$. Each $\alpha_i > 0$. This follows from this relation:

$$\alpha_i n + \beta_i(n+1) + n + 1 + \gamma_i(n+2) + n + 2 = r\,;$$
$$\alpha_i n + 2n + 3 + d_{ij} = r\,;$$
$$\alpha_i + 2n + 3 + r - 3 + tn = r\,.$$

Therefore $\alpha_i = -2 - t$ which implies $\alpha_i > 0$. We can assume that the α_i are distinct. As we did for the previous case, the elements $\{b_m(x^{\alpha_1} y^{\beta_1+1} z^{\gamma_1+1}), \dots, b_m(x^{\alpha_m} y^{\beta_m+1} z^{\gamma_m+1})\}$ form a basis of k^m. Similarly, we can consider a monomial $x^\alpha y^\beta z^\gamma \in W_r$, and assume that

for any element of W_r the proof follows. Then, we can assume that α, β or γ are different from zero. By taking the monomial $x^\alpha y^\beta z^\gamma$, we construct an element of the kernel of b_m :

$$x^\alpha y^\beta z^\gamma - \sum a_{\alpha_i} x^{\alpha_i} y^{\beta_i+1} z^{\gamma_i+1} \in \ker b_m = V_r \text{ (see Theorem 3.13) } .$$

Let us suppose $\alpha > 0$, dividing by x we obtain an element of V_{r-n}. Let $\beta > 0$ dividing by y we obtain an element of V_{r-n-1} and dividing by z an element of V_{r-n-2}. This means that any element of V_r can by expressed as an element of V_{r-n}, V_{r-n-1} or V_{r-n-2} multiplying by x, y, z respectively. Therefore the σ -leading forms $h_1, \ldots, h_{n+1}$ generates the elements of V_r for all r.
We have proved in case (1) and in case (2) that,

$$\sigma\mathrm{LI}(P_n) = (h_1, \ldots, h_{n+1}) .$$

Therefore, $(f_1, \ldots, f_{n+1}) = P_n$. □

5. Determinantal ideals

Our goal in this section is to express the ideal P_n as an ideal generated by $n \times n$ subdetermintants of an $n \times (n+1)$ matrix. We will follow the next process. First, we find a system of equations for the generators $f_1, \ldots, f_{n+1}$. Then we consider the matrix associated to these equations and we check if the power series $f_1, \ldots, f_{n+1}$ can be generated by the subdeterminants of this matrix.
Let us begin by stating the following lemma. Recall that n is an odd positive integer and $m = \frac{n+1}{2}$.

Lemma 5.1. [**5**, Lemma 3.1.] *With the notations,*

$$V_r = W_r \cap (\{\sigma\text{-leading forms of the elements in } P_n\} \cup \{0\}) ;$$
$$c_r = \dim V_r .$$

we have,

$$c_r = 2 , \qquad \text{for } r = n^2 + 2n + 2, \ldots, n^2 + 3n - 1 ;$$
$$c_r = 3 , \qquad \text{for } r = n^2 + 3n, n^2 + 3n + 1 .$$

Proof. Recall from Theorem 3.13 that $c_r = d_r - m$. Then by applying Theorem 3.10 we get

$$d_r = m + s , s \geq 1 \text{ and } n(n+s) \leq r < n(n+s+1) .$$

We take $s = 2$. Then ,

$$c_r = m + 2 - m = 2 \text{ for } r = n^2 + 2n + 2, \ldots, n^2 + 3n - 1 .$$

Finally, by letting $s = 3$. We obtain,

$$c_r = m + 3 - m = 3 \text{ for } r = n^2 + 3n, n^2 + 3n + 1 .$$

□

Now, we will find a system of equations for the power series $f_1, \ldots, f_{n+1}$. The power series zf_1, yf_2 and xf_3 have σ-order n^2+2n+2. Then $\sigma\mathrm{LF}(zf_1)$, $\sigma\mathrm{LF}(yf_2)$, $\sigma\mathrm{LF}(xf_3) \in V_{n^2+2n+2}$. By Lemma 5.1, a basis of V_{n^2+2n+2} has only two elements. Therefore the elements

$$\sigma\mathrm{LF}(zf_1),\, \sigma\mathrm{LF}(yf_2),\, \sigma\mathrm{LF}(xf_3)\,,$$

satisfy a non trivial relation,

$$a_{1,1}z\sigma\mathrm{LF}(f_1) + a_{1,2}y\sigma\mathrm{LF}(f_2) + a_{1,3}x\sigma\mathrm{LF}(f_3) = 0$$
$$\text{where } a_{1,i} \in k\,, a_{1,i} \neq 0 \text{ for } i = 1,2,3\,.$$

Clearly, the power series $a_{1,1}zf_1 + a_{1,2}yf_2 + a_{1,3}xf_3 \in P_n$. Therefore, they can be expressed as a combination of the generators of P_n,

$$a_{1,1}zf_1 + a_{1,2}yf_2 + a_{1,3}xf_3 = \sum_{i=1}^{n+1} b_i f_i\,, \quad b_i \in k[[x,y,z]]\,.$$

By abuse of notation,

$$a_{1,1} = a_{1,1}z - b_1\,, \quad a_{1,2} = a_{1,2}y - b_2\,, \quad a_{1,1} = a_{1,3}x - b_3\,,$$
$$a_{1,i} = -b_i \text{ for } 4 \leq i \leq n+1\,.$$

Therefore we obtain one equation for $f_1, \ldots, f_{n+1}$,

$$a_{1,1}zf_1 + a_{1,2}yf_2 + a_{1,3}xf_3 + a_{1,4}f_4 + \ldots + a_{1,n+1}f_{n+1} = 0\,.$$

We can repeat this process for $1 \leq j \leq n-2$. The power series zf_j, yf_{j+1} and xf_{j+2} have σ-order $n^2+2n+j+1$. Then their σ-leading forms are in $V_{n^2+2n+j+1}$. Applying again Lemma 5.1, since the dimension of $V_{n^2+2n+j+1}$ is two, then $z\sigma\mathrm{LF}(f_j)\,, y\sigma\mathrm{LF}(f_{j+1})\,, x\sigma\mathrm{LF}(f_{j+2})$ satisfy the following non trivial relation:

$$a_{j,j}z\sigma\mathrm{LF}(f_j) + a_{j,j+1}y\sigma\mathrm{LF}(f_{j+1}) + a_{j,j+2}x\sigma\mathrm{LF}(f_{j+2}) = 0$$
$$\text{for } a_{j,i} \in k\,, a_{j,i} \neq 0 \text{ for } i = j, j+1, j+2\,.$$

Once more, the power series $a_{j,j}zf_j\,, a_{j,j+1}yf_{j+1}\,, a_{j,j+2}xf_{j+2} \in P_n$. Then, repeating the same process, we get a system of $n-1$ equations for $f_1, \ldots, f_{n+1}$,

$$\sum_{i=1}^{j-1} a_{j,i}f_i + a_{j,j}zf_j + a_{j,j+1}yf_{j+1} + a_{j,j+2}xf_{j+2} + \sum_{i=j+3}^{n+1} a_{j,i}f_i = 0\,.$$

Finally, we repeat this reasoning for $j = n-1, n$. The power series $x^2f_1\,, zf_{n-1}\,, yf_n\,, xf_{n+1}$ have σ-order n^2+3n. On the other hand, the elements $xyf_1\,, x^2f_2\,, zf_n\,, yf_{n+1}$ have σ-order n^2+3n+1. Lemma 5.1 tells us that the dimension of V_{n^2+3n} and of V_{n^2+3n+1} is 3. Therefore, $x^2\sigma\mathrm{LF}(f_1)\,, z\sigma\mathrm{LF}(f_{n-1})\,, y\sigma\mathrm{LF}(f_n)\,, \sigma\mathrm{LF}(xf_{n+1})$ satisfy a non-trivial relation among them. Similarly, $xy\sigma\mathrm{LF}(f_1)\,, x^2\sigma\mathrm{LF}(f_2)\,, z\sigma\mathrm{LF}(f_n)\,, y\sigma\mathrm{LF}(f_{n+1})$ satisfy a

non-trivial relation. Proceeding as before, we obtain two equations for the power series $f_1, \ldots, f_{n+1}$:

$$a_{n-1,1}x^2 f_1 + \sum_{i=2}^{n-2} a_{n-1,i} f_i + a_{n-1,n-1} z f_{n-1} + a_{n-1,n} y f_n + a_{n-1,n+1} x f_{n+1} = 0 \quad ,$$

$$a_{n,1} xy f_1 + a_{n,2} x^2 f_2 + \sum_{i=3}^{n-1} a_{n,i} f_i + a_{n,n} z f_n + a_{n,n+1} y f_{n+1} = 0 \, .$$

At the end, we get a system of n equations for $f_1, \ldots, f_{n+1}$. Considering its associated matrix system, we can write:

$$\begin{pmatrix} a_{1,1}z & a_{1,2}y & a_{1,3}z & a_{1,4} & \ldots & a_{1,n+1} \\ a_{2,1} & a_{2,2}z & a_{2,3}y & a_{2,4}x & \ldots & a_{2,n+1} \\ \vdots & & & & & \vdots \\ a_{n-1,1}x^2 & \ldots & \ldots & \ldots & a_{n-1,n}y & a_{n-1,n+1}x \\ a_{n,1}xy & a_{n,2}x^2 & \ldots & \ldots & a_{n,n}z & a_{n,n+1}y \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} .$$

Now our goal is to apply Cramer's rule. Let Δ_i be the $n \times n$ subdeterminant of the matrix above, omitting the i-th column and affected with the sign $(-1)^{(n+1)-i}$:

$$\Delta_i = (-1)^{(n+1)-i} \begin{vmatrix} a_{1,1}z & \ldots & a_{1,i-1} & a_{1,i+1} & \ldots & a_{1,n+1} \\ \vdots & & & & & \vdots \\ a_{n,1}xy & \ldots & a_{n,i-1} & a_{n,i+1} & \ldots & a_{n,n+1}y \end{vmatrix} .$$

Let us prove that $\Delta_{n+1} \neq 0$ and its σ-order is n^2+2n. Let us consider the subdeterminant $\overline{\Delta}_{n+1}$ by taking $a_{i,j}(0,0,0)$. It is enough to prove that $\overline{\Delta}_{n+1} \neq 0$ and has σ-order n^2+2n. The subdeterminat $\overline{\Delta}_{n+1}$ can be written as follows:

$$\begin{vmatrix} a_{1,1}z & a_{1,2}y & a_{1,3}x & 0 & \ldots & 0 \\ 0 & a_{2,2}z & a_{2,3}y & a_{2,4}x & \ldots & 0 \\ 0 & 0 & a_{3,3}z & a_{3,4}y & \ldots & 0 \\ \vdots & & & & & \vdots \\ a_{n,1}xy & a_{n,2}x^2 & 0 & \ldots & 0 & a_{n,n}z \end{vmatrix} .$$

The element from the diagonal Az^n, where $A = \prod_{i=1}^{n} a_{i,i}$, can not be vanished by any other element. Therefore $\overline{\Delta}_{n+1} \neq 0$ and moreover $\sigma\text{ord}\,(\overline{\Delta}_{n+1}) = \sigma\text{ord}\,(z^n) = n(n+2)$. Since $\Delta_{n+1} \neq 0$, we have the following system of equations:

$$\begin{pmatrix} a_{1,1}z & a_{1,2}y & a_{1,3}z & a_{1,4} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2}z & a_{2,3}y & a_{2,4}x & \ldots & a_{2,n} \\ \vdots & & & & & \vdots \\ a_{n-1,1}x^2 & \ldots & \ldots & \ldots & a_{n-1,n-1}z & a_{n-1,n}y \\ a_{n,1}xy & a_{n,2}x^2 & \ldots & \ldots & \ldots & a_{n,n}z \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ \vdots \\ f_n \end{pmatrix} = - \begin{pmatrix} a_{1,n+1} \\ a_{2,n+1} \\ \vdots \\ a_{n-1,n+1}x \\ a_{n,n+1}y \end{pmatrix} f_{n+1} \, .$$

Using Cramer's rule and applying some determinants properties we obtain f_1 in terms of the subdeterminants:

$$f_1 = \frac{-f_{n+1}}{\Delta_{n+1}} \begin{vmatrix} a_{1,n+1} & a_{1,2}z & \dots & \dots & \dots & a_{1,n} \\ \vdots & & & & & \vdots \\ a_{n,n+1}y & a_{n,2}x^2 & \dots & \dots & \dots & a_{n,n}z \end{vmatrix} = \frac{f_{n+1}}{\Delta_{n+1}}\Delta_1 \,.$$

Proceeding similarly for the rest of power series $f_2, \dots, f_n$, we get:

$$f_2 = \frac{f_{n+1}}{\Delta_{n+1}}\Delta_2 \,, \dots \,, f_n = \frac{f_{n+1}}{\Delta_{n+1}}\Delta_n \,.$$

Clearly, $f_{n+1} = \lambda\Delta_{n+1}$ where λ is an element from the quotient field of $k[[x,y,z]]$. It is left to show that $\lambda \in k[[x,y,z]]$. This fact should be deduced from $\sigma\text{ord}\,(\Delta_{n+1}) = \sigma\text{ord}\,(f_{n+1}) = n^2 + 2n$. Let $g \in P_n$, we can express g as

$$g = \sum_{i=1}^{n+1} b_i f_i \text{ for some } b_i \in k[[x,y,z]] \,.$$

Substituting the f_i for the relations obtained using Cramer's rule, we obtain:

$$g = \sum_{i=1}^{n+1} \lambda\Delta_i \,.$$

Then,

$$(f_1, \dots, f_{n+1}) = \lambda(\Delta_1, \dots, \Delta_{n+1}) \,.$$

Clearly λ has to be invertible, otherwise the ideal P_n of height 2, would be contained in an ideal of height 1 which is a contradiction. Therefore,

$$(f_1, \dots, f_{n+1}) = (\Delta_1, \dots, \Delta_{n+1}) \,.$$

So we have proved that $P_n = I_n(\varphi)$, where $I_n(\varphi)$ is the ideal generated by the subdeterminats of the matrix φ. In our case,

$$\varphi = \begin{pmatrix} a_{1,1}z & a_{1,2}y & a_{1,3}z & a_{1,4} & \dots & a_{1,n+1} \\ a_{2,1} & a_{2,2}z & a_{2,3}y & a_{2,4}x & \dots & a_{2,n+1} \\ \vdots & & & & & \vdots \\ a_{n-1,1}x^2 & \dots & \dots & \dots & a_{n-1,n}y & a_{n-1,n+1}x \\ a_{n,1}xy & a_{n,2}x^2 & \dots & \dots & a_{n,n}z & a_{n,n+1}y \end{pmatrix} .$$

An interesting observation is that we can prove this result in another way, using Hilbert-Burch Theorem [**1**, Theorem 1.4.17.].

THEOREM 5.2. *The ideal P_n verifies the following equality:*

$$P_n = I_n(\varphi) \,,$$

where $I_n(\varphi)$ is the ideal generated by the subdeterminats of an $(n+1) \times n$ matrix with entries in $R = k[[x,y,z]]$.

PROOF. The ideal P_n is a prime ideal of height 2 because $\dim R/P_n = 1$. Since R is a regular local ring, $\text{grade}(P_n) = \text{ht}(P_n) = 2$. Since R is a regular local ring of dimension 3, all the prime ideals are perfects. Therefore, there exists a free resolution of R/I of length 2. Thus, we have the following exact sequence:

$$0 \to R^n \xrightarrow{\varphi} R^{n+1} \to R \to R/P_n \to 0\,,$$

where $n+1$ is the minimum number of generators of P_n and the rank mus be n (see [**1**, Theorem 1.4.13.]). Therefore, we have a free resolution

$$0 \to R^n \to R^{n+1} \to P_n \to 0\,.$$

By the Hilbert-Burch Theorem [**1**, Theorem 1.4.17.], we deduce that $P_n = aI_n(\varphi)$, where a is a R-regular element. Since R is regular, R is a domain therefore a is not a zero divisor. Moreover, a must be invertible, otherwise the height 2 prime ideal P_n would be included in a height 1 ideal. Thus,

$$P_n = I_n(\varphi)\,.$$

□

CHAPTER 2

Generators of primes ideals in a three-dimensional regular local ring

The goal of this chapter is to try to generalize the ideas of Moh, in the articles[**4**] and [**5**], for any regular local ring R of Krull dimension 3. We follow the result of the article [**6**], where F. Planas finds a prime ideal minimally generated by 4 elements. Our aim is to define a prime ideal minimally generated by 5 elements proceeding as in [**6**, Lemma 2.]. We distribute this chapter in three sections. In the first one, we state Lemma 2 of [**6**] and we explain in detail the proof. In the second one, we stablish a general criterion to find prime ideals minimally generated by n elements. Finally, on the third one, we give an original example of a prime ideal minimally generated by 5 elements.

1. A prime ideal minimally generated by four elements

In this section we explain Lemma 2 of the article [**6**]. This result shows a method about finding prime ideals, in a regular local ring of dimension three, minimally generated by n elements. The proof of the lemma uses commutative algebra theory, therefore we will reference many of the definitions and results. However, we start by proving a lemma and recalling a definition.

LEMMA 1.1. *Let $(R, \mathfrak{m})$ be a regular local ring. Denote $(\widehat{R}, \widehat{\mathfrak{m}})$ to its completion. Let I be an ideal of R. If its completion $\widehat{I}$ is prime then I is also prime.*

PROOF. Let us consider the completion morphism

$$R \longrightarrow \widehat{R}\,.$$

By this morphism the ideal $\widehat{I}$ is defined as follows:

$$\widehat{I} = I\widehat{R}\,.$$

The completion $\widehat{R}$ is flat and faithfully flat over R. Therefore $R \subset \widehat{R}$ and $I = I\widehat{R} \cap R$ [**3**, page 63]. Then, if $\widehat{I}$ is prime, I is also prime. □

DEFINITION 1.2. An ideal I is called *grade unmixed* if for all $\mathfrak{p} \in \mathrm{Ass}(R/I)$,

$$\mathrm{grade}(I) = \mathrm{grade}(\mathfrak{p})\,.$$

Now we will state and prove Lemma 2 of [**6**]. The idea of the proof is to find a possible prime ideal I generated by 4 elements. To verify that I is prime, we take $\mathfrak{p}$, an associated prime to I, and we check $I = \mathfrak{p}$.

THEOREM 1.3. [**6**, Lemma 2.] *Let $(R, \mathfrak{m}, k)$ a regular local ring of Krull dimension 3. Let x, y, z be a regular system of parameters. Let I be the ideal of R generated by*

$$f_1 = y^3 - x^4\,,\ f_2 = xyz - z^3 + x^4 - xy^3\,,$$
$$f_3 = x^2y + y^2z - xz^2 - x^3 \text{ and } f_4 = xy^2 - yz^2 - x^2y^2 + x^3z\,.$$

Then I is a height two prime ideal minimally generated by four elements.

PROOF. By Lemma 1.1, we can assume $(R, \mathfrak{m})$ to be complete. Observe that f_1, f_2, f_3, f_4 are, up to a change of sign, the 3×3 subdeterminants of the 4×3 matrix φ_2,

$$\varphi_2 = \begin{pmatrix} x & xy & z \\ x & y & 0 \\ -z & -x^2 & -y \\ -y & -z & x \end{pmatrix}.$$

Therefore, $I = I_3(\varphi_2)$, where $I_3(\varphi_2)$ denote the ideal generated for the subdeterminants of φ_2. Check that $(f_1, f_2, x) = (x, y^3, z^3)$, then $\operatorname{grade}(f_1, f_2, x) = 3$. By [**1**, Corollary 1.6.19.], f_1, f_2 is a R-regular sequence in $I_3(\varphi_2)$. Then $\operatorname{grade}(I(\phi_2)) \geq 2$. Therefore, by applying the converse of the Hilbert-Burch Theorem, see [**1**, Theorem 1.4.17.],

$$0 \to R^3 \xrightarrow{\varphi_2} R^4 \xrightarrow{\varphi_1} R \to R/I \to 0\,,$$

is a free resolution of R/I. Note that φ_1 is the 1×4 matrix defined as (f_1, f_2, f_3, f_4). (It is a minimal resolution since $\varphi_2(R^3) \subset \mathfrak{m}R^4$ and $\varphi_1(R^4) = I \subset \mathfrak{m}$.) Therefore,

$$2 \leq \operatorname{grade}(I) \leq \operatorname{proj\,dim}_R(R/I) \leq 2\,,$$

the inequalities are equalities and I is a perfect ideal [**1**, Definition 1.4.17.] of grade 2. Moreover, I is grade *unmixed*. This implies that $\mathfrak{m}$ is not an associated prime of I. The aim of the proof is to find a relation for $\operatorname{length}(R/(xR + I))$ and $\operatorname{length}(R/(xR + \mathfrak{p}))$, in the following way:

$$m = \operatorname{length}(R/(xR + I)) \geq \operatorname{length}(R/(xR + \mathfrak{p}) \geq m\,,\ \text{where } m \in \mathbb{N}\,.$$

We start by computing $\operatorname{length}(R/(xR+I))$. Let $S = R/xR$, be a local ring with maximal $\mathfrak{n} = (y, z)$. By the third isomorphism theorem,

$$\frac{R/xR}{(xR + I)/xR} \simeq R/(xR + I)\,.$$

Observe that $\mathfrak{n}^3 = (xR + I)/xR$, then $R/(xR + I) \simeq S/\mathfrak{n}^3$. Let us notice the following $1 - 1$ correspondence:

$$\{ \text{ Submodules of } R \text{ that contain } xR + I\} \longleftrightarrow \{ \text{ Submodules of } S \text{ that contain } \mathfrak{n}^3\} .$$

Therefore, $\text{length}_R(R/(xR + I)) = \text{length}_S(S/\mathfrak{n}^3)$. Since y, z are a S-regular sequence, there exist a graded isomorphism $S/\mathfrak{n}[y, z] \simeq G(\mathfrak{n})$, see [**1**, Theorem 1.1.8.]. Now, we can compute the length of $S/\mathfrak{n}^3$ with the following exact sequences:

$$0 \to \mathfrak{n}^i/\mathfrak{n}^{i+1} \to S/\mathfrak{n}^{i+1} \to S/\mathfrak{n}^i \to 0 , \quad \text{for } i = 1, 2 .$$

Since $\mathfrak{n}^i/\mathfrak{n}^{i+1}$ are k-vector spaces for $k = S/\mathfrak{n}$ and the length is additive then,

$$\text{length}(S/\mathfrak{n}^3) = \dim_k(S/\mathfrak{n}) + \dim_k(\mathfrak{n}/\mathfrak{n}^2) + \dim_k(\mathfrak{n}^2/\mathfrak{n}^3) = 6 .$$

Therefore $\text{length}(R/(xR + I)) = 6$.
Now, let us see that $\text{length}(R/(xR + \mathfrak{p})) \geq 6$. We consider the one dimensional complete Noetherian local domain $D = R/\mathfrak{p}$, see [**3**, page 63]. Let V be its integral closure. V is a one dimensional integrally closed Noetherian local domain, therefore V is a discrete valuation ring (DVR). Moreover, V is complete, see [**9**, Theorem 4.3.4.]. Set $\nu(x) = \nu_x$, $\nu(y) = \nu_y$ and $\nu(z) = \nu_z$. Since$f_1 = 0$ in V, then by applying ν to the equality $x^4 - y^3 = 0$, we obtain

$$4\nu_x = 3\nu_y .$$

Therefore, $\nu_x = 3q$ for some integer $q \geq 1$. Let us prove that $q > 1$ by supposing $q = 1$. Then $\nu_x = 3$ and $\nu_y = 4$. Since $f_2 = 0$ in V then $z^3 = x(xy + x^3 - y^3)$. Applying the valuation to this equation we get,

$$3\nu_z \geq \min(12, 7 + \nu_z) .$$

If $7 + \nu_z \geq 12$, then $3\nu_z \geq 12$ and $\nu_z \geq 4$. Otherwise, $3\nu_z \geq 12 + \nu_z$, then $\nu_z \geq 4$. In both cases the inequality is true so we can assume $\nu_z \geq 4$. Since $f_3 = 0$ in V, then we have the following equality:

$$x^2y = -y^2z + xz^2 + x^3y .$$

Applying ν to this equality, we get

$$10 \geq \min(12, 11, 13) ,$$

which is a contradiction. Therefore $q > 1$ and $\nu_x \geq 6$.
Since

$$R/(xR + \mathfrak{p}) \simeq (R/\mathfrak{p})/(xR/\mathfrak{p}) = D/xD ,$$

then, $\text{length}_R(R/(xR+\mathfrak{p}) = \text{length}_D(D/xD)$. Our propose is to compute $\text{length}_D(D/xD)$. Since f_1, f_2 are zero in D, $z^3, y^3 \in xD$. Therefore x is a system of parameters, i.e. xD is an

$\mathfrak{m}/\mathfrak{p}$-primary ideal of the Cohen-Macaulay local domain $(D, \mathfrak{m}/\mathfrak{p}, k)$. By [**9**, Proposition 11.1.10.] we get the following equality:

$$\text{length}_D(D/Dx) = e_D(xD; D)\,,$$

where $e_D(xD; D)$ is the multiplicity of xD in D. Let K be the quotient field of D. Since V is the integral closure of D in K, then, by definition, V is contained in K. In particular, the quotient field K_V of V is contained in K (because it is the minimal field containing V). Hence

$$D \subset V \subset K_V \subseteq K\,.$$

Again, since K is the minimal field containing D, then $K_V = K$. Thus, D and V have the same field of fractions. By definition, V is a finitely generated Cohen-Macaulay D-module of $\text{rank}_D(V) = 1$. As $K = S^{-1}D \subseteq S^{-1}V \subseteq K$,

$$\text{rank}(V \otimes_D K) = \text{rank}(S^{-1}V) = \text{rank}(K) = 1\,.$$

Applying [**1**, Corollary 4.7.11.] we obtain,

$$\text{length}_D(V/xV) = e_D(xD; D)\text{rank}_D(V) = e_D(xD; D)\,.$$

Finally we need to compute $\text{length}_D(V/xV)$. By [**8**, Lemma 10.51.12.],

$$\text{length}_D(V/xV) = [k_V : k]\text{length}_V(V/xV)\,,$$

where $[k_v : k]$ is de degree of the extension $k \to k_v$. Now, it is left to compute $\text{length}_V(V/xV)$. As V is a DVR and $x \in V \setminus V^*$, then $x \in (t)$, where (t) is the maximal of V. So $x = ut^r$ with u a positive integer. Therefore, we can consider the following unrefinable chain of submodules,

$$0 \subset (t)^{r-1}/(t)^r \subset \ldots \subset (t)/(t)^r \subset V/t^r\,.$$

Then $\text{length}_V(V/xV) = r = \nu(ut^r) = \nu(x) = \nu_x$. Summing up all together we get,

$$\text{length}_R(R/(xR + \mathfrak{p})) = \text{length}_D(D/xD) = e_D(xD; D) = \text{length}_D(V/xV) =$$
$$[k_V : k]\text{length}_V(V/xV) = [k_v : k]\nu_x \geq 6\,.$$

Since $xR + I \subseteq xR + \mathfrak{p}$, then

$$6 = \text{length}(R/(xR + I)) \geq \text{length}(R/(xR + \mathfrak{p})) = [k_V : k]\nu_x \geq 6\,.$$

Therefore,

$$\text{length}(R/(xR + I)) = \text{length}(R/(xR + \mathfrak{p}))$$

Let us consider the following short exact sequences,

$$0 \to xR + I \to R \to R/(xR + I) \to 0 \quad \text{and} \quad 0 \to xR + \mathfrak{p} \to R \to R/(xR + \mathfrak{p}) \to 0\,.$$

By the additivity of the length, $\text{length}(xR+I) = \text{length}(xR+\mathfrak{p})$. Since $xR+I \subseteq xR+\mathfrak{p}$, then $xR + I = xR + \mathfrak{p}$.

Note that $x \notin \mathfrak{p}$. Otherwise, $(f_1, f_2, x) \subset xR + I \subset \mathfrak{p}$ and $\mathfrak{p} = \mathfrak{m}$. But the maximal is not an associated prime to I. Therefore $\mathfrak{p} \cap xR = x\mathfrak{p}$. Let us consider the following short exact sequence:

$$0 \to \mathfrak{p}/I \to R/I \to R/\mathfrak{p} \to 0\,.$$

We tensor the previous short exact sequence by $\otimes_R R/xR$, and we get

$$\begin{aligned}\mathrm{Tor}_1(\mathfrak{p}/I, R/xR) \to \mathrm{Tor}_1(R/(xR+I), R/xR) \to \mathrm{Tor}_1(R/(xR+\mathfrak{p}), R/xR)\\ \to \mathfrak{p}/I \otimes R/xR \to R/(xR+I) \to R/(xR+\mathfrak{p}) \to 0\,.\end{aligned}$$

Since $\mathfrak{p} \cap xR = x\mathfrak{p}$, then $\mathrm{Tor}_1(R/(xR+\mathfrak{p}), R/xR) = xR \cap \mathfrak{p}/x\mathfrak{p} = 0$. Applying some properties of the tensorial product, we get to the following short exact sequence

$$0 \to L/xL \to R/(xR+I) \to R/(xR+\mathfrak{p}) \to 0\,.$$

where $L = \mathfrak{p}/I$. Since $xR + I = xR + \mathfrak{p}$, $L = xL$. Therefore by Nakayama's Lemma, $L = 0$ and $\mathfrak{p} = I$.
We conclude that I is a prime ideal. Since the aforementioned resolution of R/I is minimal, then I is minimally generated by 4 elements. □

2. Generalisation of the proof

In the previous result, we have seen a process to build a prime ideal minimally generated by 4 elements. In this section, we will explain the general scheme of this process. We keep the notation of Theorem 1.3.
The first step is to find an ideal I generated by $n+1$ elements, $f_1, \ldots, f_{n+1}$. Moreover, we ask this functions to be the $n \times n$ subderterminants of a $(n+1) \times n$ matrix. This ideal is our candidate to be prime.
Let $I = (f_1, \ldots, f_{n+1})$ and let φ_2 be the matrix whose subdeterminats are f_i up to sign.
The next step is to check if for any of x, y or z, there exist f_i, f_j such that

$$\mathrm{grade}(f_i, f_j, x_i) = 3\,,$$

where $x_i = x, y$ or z. To simplify the notation, we are going to take $x_i = x$. Then by [**1**, Corollary 1.6.19.], f_i, f_j is a R regular sequence. and $\mathrm{grade}(I_3(\varphi_2)) \geq 2$.
Then, we can apply the converse of the Hilbert-Burch Theorem, see [**1**, Theorem 1.4.17.],

$$0 \to R^n \to R^{n+1} \to R \to R/I \to 0\,,$$

is a free resolution of R/I, moreover it is a minimal resolution since $\varphi_1(R^{n+1}) = I \subset \mathfrak{m}$ and $\varphi_2(R^n) \subset \mathfrak{m}R^{n+1}$. So I is a perfect ideal of dimension 2 and it is grade unmixed. As we concluded before, the maximal is not an associated prime of I.
The following step is to take $\mathfrak{p} \in \mathrm{Ass}(R/I)$. We want to find a non negative integer k, verifying

$$k = \mathrm{length}_R(R/(xR+I) \geq \mathrm{length}_R(R/(xR+\mathfrak{p}) \geq k\,.$$

To compute $\text{length}_R(R/(xR+I)$, it is enough to find a non negative integer m, such that $\mathfrak{n}^m = (xR+I)/xR$, where $\mathfrak{n}$ is the maximal of the local ring $D = R/xR$. Therefore, we can conclude that $\text{length}_R(R/(xR+I) = k$.
The next step is to to check if $\text{length}_R(R/(xR+\mathfrak{p}) \geq k$. To prove it, it is enough to see if $\nu_x \geq k$. The idea of this proof is to check if $x^m - x_i^r \in I$, for $x_i = y, z$ and $r, m \in \mathbb{N}$. Now, proceeding similarly as in the above-mentioned proof, we should be able to achieve $\nu_x \geq k$. Once we get to this point, the rest of the proof holds. Therefore

$$k = \text{length}_R(R/(xR+I) \geq \text{length}_R(R/(xR+\mathfrak{p}) \geq k\,.$$

And applying Nakayama's Lemma we conclude that I is a prime ideal.
Since the resolution of R/I is minimal, then I is minimally generated by $n+1$ elements.

3. A prime ideal minimally generated by five elements

In this section we are going to give an example of a prime ideal, in a regular local ring of dimension 3, minimally generated by 5 elements. This ideal is inspired on Moh's primes. More precisely on [**2**, Example 3.6.]. The common idea is to consider the following ring morphism,

$$\begin{array}{rccc} \rho: & k[[X,Y,Z]] & \to & k[[t]] \\ & X & \mapsto & t^a \\ & Y & \mapsto & t^{b_1}+t^{b_2} \\ & Z & \mapsto & t^c\,. \end{array}$$

Therefore, our first candidate to be the prime ideal I, minimally generated by 5 elements is the kernel of ρ. Our example is done in a regular local ring R of Krull dimension 3. We substitute the variables X, Y and Z for the regular parameters x, y, z. Then, by taking $a = 10$, $b_1 = 11$, $b_2 = 16$ and $c = 12$, our ideal I would be the kernel of ρ. Subsequently, using Singular (see [**10**]), we calculate a resolution of ideal I,

$$0 \to R^4 \xrightarrow{\varphi} R^5 \to I \to 0\,.$$

We replace in φ, the ± 2 and ± 3 for ± 1 to avoid characteristic problems. Then, by considering the modified matrix φ_2 we obtain our final candidate $I = I_3(\varphi_2)$.

THEOREM 3.1. *Let $(R, \mathfrak{m}, k)$ be a regular local ring of Krull dimension 3. Let x, y, z be a regular system of parameters. Let I be the ideal of R generated by*

$$f_1 = y^2z^2 - xz^3 - x^4y + x^2z^3\,,\ f_2 = -y^3z + xyz^2 + x^5 - z^5\,,$$
$$f_3 = y^4 - 2xy^2z + x^2z^2 - x^3z^2 + yz^4\,,\ f_4 = -xy^3 + x^2yz + z^4 - xz^4\,,$$
$$f_5 = x^2y^2 - x^3z - yz^3 + x^4z\,.$$

Then I is a height 2 prime ideal minimally generated by five elements.

PROOF. By Lemma 1.1, we can assume $(R, \mathfrak{m})$ complete. Observe that f_1, f_2, f_3, f_4, f_5 are the 4×4 subdeterminants of the 5×4 matrix φ_2,

$$\varphi_2 = \begin{pmatrix} 0 & z & -y & x^2 \\ 0 & -y & x & -z^2 \\ z & x & 0 & 0 \\ -y & 0 & 0 & -z+xz \\ x & 0 & -z & y \end{pmatrix}.$$

Therefore $I = I_3(\varphi_2)$. We check the following equality:

$$(f_3, f_4, x) = (y^4, z^4, x)\,.$$

Thus, $\operatorname{grade}(f_3, f_4, x) = 3$. By [**1**, Corollary 1.6.19.], f_3, f_4 is a R-regular sequence and $\operatorname{grade}(I(\varphi_2)) \geq 2$. Therefore, by applying the converse of the Hilbert-Burch Theorem, see [**1**, Theorem 1.4.17.],

$$0 \to R^4 \xrightarrow{\varphi_2} R^5 \xrightarrow{\varphi_1} R \to R/I \to 0\,.$$

is a free resolution of R/I, where φ_1 is the 1×5 matrix defined as $(f_1, f_2, f_3, f_4, f_5)$. (The resolution is minimal since $\varphi_2(R^4) \subset \mathfrak{m}R^5$ and $\varphi_1(R^5) \subset I \subset \mathfrak{m}$). Therefore,

$$2 \leq \operatorname{grade}(I) \leq \operatorname{proj\,dim}_R(R/I) \leq 2\,,$$

so the inequalities are equalities and I is a perfect ideal [**1**, Definition 1.4.16.] of grade 2. Moreover, I is grade *unmixed*. This implies that $\mathfrak{m}$ is not an associated prime of I.
Following the proof of Theorem 1.3, we compute $\operatorname{length}(R/(xR+I))$. Let $S = R/xR$, be a local ring with maximal $\mathfrak{n} = (y, z)$. By the third isomorphism theorem,

$$R/xR/(xR+I)/xR \simeq R/(xR+I)\,.$$

We check that $\mathfrak{n}^4 = (xR+I)/xR$, therefore $R/(xR+I) \simeq S/\mathfrak{n}^4$. Moreover, there exists a one an one correspondence

$$\{\text{ Submodules of } R \text{ that contain } xR+I\} \longleftrightarrow \{\text{ Submodules of } S \text{ that contain } \mathfrak{n}^4\}\,.$$

In this sense, we arrive to the equality $\operatorname{length}_R(R/(xR+I)) = \operatorname{length}_S(S/\mathfrak{n}^4)$. Since y, z are a S-regular sequence, there exist a graded isomorphism $S/\mathfrak{n}[y,z] \simeq G(\mathfrak{n})$, see [**1**, Theorem 1.1.8.]. Now, we can compute the length of $S/\mathfrak{n}^4$ with the following exact sequences:

$$0 \to \mathfrak{n}^i/\mathfrak{n}^{i+1} \to S/\mathfrak{n}^{i+1} \to S/\mathfrak{n}^i \to 0\,, \quad \text{for } i = 1, 2, 3\,.$$

Since $\mathfrak{n}^i/\mathfrak{n}^{i+1}$ are k-vector spaces for $k = S/\mathfrak{n}$ and the length is additive then,

$$\operatorname{length}(S/\mathfrak{n}^4) = \dim_k(S/\mathfrak{n}) + \dim_k(\mathfrak{n}/\mathfrak{n}^2) + \dim_k(\mathfrak{n}^2/\mathfrak{n}^3) + \dim_k(\mathfrak{n}^3/\mathfrak{n}^4) = 10\,.$$

Therefore $\operatorname{length}(R/(xR+I)) = 10$.
Now, let us see that $\operatorname{length}(R/(xR+\mathfrak{p})) \geq 10$. Let us consider the one dimensional complete Noetherian local domain $D = R/\mathfrak{p}$, see [**3**, page 63]. Let V be its integral

closure. V is a one dimensional integrally closed Noetherian local domain. Therefore V is a discrete valuation ring (DVR). Moreover V is complete see [**9**, Theorem 4.3.4.]. Set $\nu(x) = \nu_x$, $\nu(y) = \nu_y$ and $\nu(z) = \nu_z$. The element $z^5 - x^6 = -x(f_2) + z(f_4)$, therefore $z^5 - x^6 \in I$. Since $z^5 - x^6 = 0$ in V. By applying ν we get,

$$6\nu_x = 5\nu_z\,,$$

therefore $\nu_x = 5q$ where q is an integer, $q \geq 1$. Let us prove that $q > 1$. Let us suppose that $q = 1$ then $\nu_x = 5$ and $\nu_z = 6$. Since $f_1 = 0$ in V then $y^2z^2 = x(z^3 + x^3y + xz^3)$. Applying ν to this equation we get,

$$2\nu_y + 2\nu_z \geq \nu_x + \min(18, 15 + \nu_y)\,.$$

If $\nu_y + 15 \leq 18$ then, $\nu_y \leq 3$ and $\nu_y \geq 8$, it is a contradiction. Therefore $\nu_y + 15 > 18$, $\nu_y > 3$ and

$$2\nu_y + 12 \geq 5 + 18\,.$$

Thus $2\nu_y \geq 11$. Since $f_5 = 0$ in V, we obtain the equation

$$x^3z(-1 + x) = y(-x^2y + z^3)\,.$$

Applying ν we get,

$$3\nu_x + \nu_z \geq \nu_y + \min(10 + \nu_y, 18)\,.$$

Remark that $\nu(-1 + x) = 0$ because $x - 1$ does not belong to the maximal of V. Let us suppose $18 \leq 10 + \nu_y$. Then,

$$3\nu_x + \nu_z \geq \nu_y + 18\,,$$

and $\nu_y \leq 3$, it is a contradiction. Therefore $18 \geq 10 + \nu_y$,

$$3\nu_x + \nu_z \geq 2\nu_y + 10\,,$$

$$11 \geq 2\nu_y\,,$$

which is a contradiction. Thus $q > 1$ and $\nu_x \geq 10$. From here and as we did in Theorem 1.3, we deduce:

$$10 = \text{length}(R/(xR + I)) \geq \text{length}(R/(xR + \mathfrak{p})) = [k_V : k]\nu_x \geq 10\,.$$

Therefore $\text{length}(R/(xR + I)) = \text{length}(R/(xR + \mathfrak{p}))$. Again, proceeding as in Theorem 1.3 we arrive to $\mathfrak{p} = I$.

We conclude that I is a prime ideal. Since the aforementioned resolution of R/I is minimal, then I is minimally generated by 5 elements. □

Conclusions and Further work

The purpose of this thesis is to study the family of prime ideals introduced by T.T. Moh in the seventies and, subsequently, to extend his ideas to any three dimensional regular local ring.

Our main achievements are the following:

- A detailed explanation and proof of the construction of Moh's primes. Namely, the existence of a family of prime ideals, in the power series ring in three variables, minimally generated by $n+1$ elements.
- These prime ideals are determinantal ideals. More precisely, they are the ideals of the $n \times n$ minors of an $n \times (n+1)$ matrix with entries in the power series ring. This phenomenon is the starting point to extend this result to any three dimensional regular local ring, as shown in a recent example for four generators stated by F. Planas.
- We study with great care the aforementioned example.
- We propose a general scheme that would allow to find a prime ideal, in any three dimensional regular local ring, minimally generated by an arbitrarily high number of generators.
- Following this scheme we give an original example of a prime ideal, in a three dimensional regular local ring, minimally generated by five elements.

An interesting fact that we would like to emphasize is the following. While Moh's primes are constructed for an odd non-negative integer number n, we realise that there are prime ideals in a three dimensional regular local ring, minimally generated by four and five elements. Therefore, Moh's restriction seems to be unessential.
Some interesting further work would be the following:

- Using the method described in Section 2, we would like to investigate the existence of prime ideals minimally generated by six and seven elements. Although this may represent a remarkable increase in the complexity of the computations, we guess that this is a short, middle-term available result.
- Of course, the low number cases would be just an excuse to address the general problem. That is to say, given a three dimensional regular local ring, and given

any non-negative integer $n \geq 1$, our purpose is to find a prime ideal minimally generated by n elements.

Bibliography

[1] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, 2nd ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1998.

[2] C. Huneke, *Hilbert functions and symbolic powers*, Michigan Math. J. **34** (1987), no. 2, 293–318.

[3] H. Matsumura, *Commutative Ring Theory* (Translate by M. Reids, ed.), Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1987.

[4] T.T. Moh, *On the unboundedness of generators of prime ideals in powerseries rings of three variables*, Journal of the Mathematical Society of Japan **26** (1974), no. 4, 722–734.

[5] ———, *On generators of ideals*, Proceedings of the American Mathematical Society **77** (1979), no. 3, 309–312.

[6] F. Planas-Vilanova, *Noetherian rings of low global dimension and syzygetic prime ideals*, arXiv preprint arXiv:1910.01550 (2019).

[7] J.C. Rosales and P.A. García-Sánchez, *Numerical semigroups*, Vol. 20, Springer Science & Business Media, 2009.

[8] The Stacks Project Authors, *Stacks Project* (2018), `https://stacks.math.columbia.edu`. Last accessed in May 2020.

[9] I. Swanson and C. Huneke, *Integral closure of ideals, rings, and modules*, Vol. 13, Cambridge University Press, 2006.

[10] W. Decker; G.-M.Greuel; G. Pfister and H.Schönemann, SINGULAR *4-1-2 — A computer algebra system for polynomial computations*, 2019.