Combinatorics of singularities of some special curves and hypersurfaces

Ali Abbas

UNIVERSITE BRETAGNE LOIRE

université angers

Thèse de Doctorat

Ali ABBAS

Mémoire présenté en vue de l'obtention du
grade de Docteur de l'Université d'Angers
sous le sceau de l'Université Bretagne Loire

École doctorale : Sciences et technologies de l'information, et mathématiques

Discipline : Mathématiques et leurs interactions, section CNU 25
Unité de recherche : Laboratoire Angevin de Recherche en Mathématiques (LAREMA)

Soutenue le 11 Septembre 2017

Combinatoire des singularités de certaines courbes et hypersurfaces

JURY

Rapporteurs :	**M. Antonio CAMPILLO**, Professeur, Université de Valladolid, Espagne
	M. Mark SPIVAKOVSKY, Professeur, Université Paul Sabatier Toulouse 3
Examinateurs :	**M. Michel GRANGER**, Professeur, Université d'Angers
	M. Hussein MOURTADA, Maître de conférences, Université Paris VII
	M. Guillaume ROND, Maître de Conférences HDR, Université d'Aix Marseille
	M^{me} Monique LEJEUNE-JALABERT, Directeur de recherche au CNRS, Université de Versailles-Saint Quentin
Directeur de thèse :	**M. Abdallah ASSI**, Maître de Conférences HDR, Université d'Angers

Thèse

pour obtenir le grade de

Docteur ès Mathématiques

présentée à l'Université d'Angers par

Ali Abbas

Combinatoire des singularités de certaines courbes et hypersurfaces

---

soutenue le 11 Septembre 2017 devant le jury composé de :

M. Mark Spivakovsky	Professeur à l'Université de Paul Sabatier Toulouse 3	Rapporteur
M. Antonio Campillo	Professeur à l'Université de Valladolid	Rapporteur
M. Michel Granger	Professeur à l'Université d'Angers	Examinateur
M. Hussein Mourtada	Maître de conférences à l'Université de Paris VII	Examinateur
M. Guillaume Rond	Maître de conférences HDR à l'Université d'Aix Marseille	Examinateur
Mme. Monique Lejeune-Jalabert	Directeur de recherche au CNRS	Examinateur
M. Abdallah Assi	Maître de Conférences HDR à l'Université d'Angers	Directeur de thèse

préparée au **Larema - UMR CNRS 6093**

Remerciements

I would like to thank my advisor, Abdallah Assi for all his help and guiding through these years which led me to accomplish this work.

I would like to thank the committee members for their discussions and comments through this process.

I would like to thank my amazing family for all their support.

I'd like to thank all my friends especially Bachar Moughayt. I am very grateful for his help since the moment i arrived in Angers.

I would like to thank the soul of Dostoyevsky and other writers for what they gave to humanity. I undoubtedly could not have done anything in my life without them.

Finally, I would like to dedicate this thesis to my father and teacher in life, Hussein Abbas.

Table des matières

1

Introduction

The thesis is made up of two parts. In the first part we generalize the Abhyankar-Moh theory to a special kind of polynomials, called free polynomials. These polynomials generalize to $\mathbb{K}[[x_1, \ldots, x_e]][y]$ the well known results about polynomials of $\mathbb{K}[[x]][y]$, where $\mathbb{K}$ is an algebraically closed field of characteristic zero. More precisely, consider a polynomial :

$$f = y^n + a_1(x)y^{n-1} + \cdots + a_n(x)$$

in $\mathbb{K}[[x]][y]$, and assume that f is irreducible. The Newton-Puiseux theorem [25, 27] says that f admits a solution $y(x^{\frac{1}{n}})$ in the ring of fractional power series $\mathbb{K}[[x^{\frac{1}{n}}]]$. Moreover, we have :

$$f(x^n, y) = \prod_{i=1}^{n}(y - y(w_i x))$$

where $w_1, ..., w_n$ are the n-th roots of unity in $\mathbb{K}$. Furthermore, Abhyankar [2, 4] has proved that we can associate with f a sequence of integers $\{m_1, ..., m_h\}$ derived from the exponents of some root $y = \sum_p c_p x^p$ of $f(x^n, y) = 0$, and this sequence is independent of the choice of the solution. This set of integers is called the set of Newton-Puiseux exponents of f, and is constructed as follows : $m_0 = n = d_1$, and for all $k \geq 1$:

$$m_k = inf\{p \in \mathbb{N},\ such\ that\ c_p \neq 0,\ and\ d_k\ does\ not\ divide\ p\},\ d_{k+1} = gcd(d_k, m_k)$$

Then h is such that $d_{h+1} = 1$. We can also associate with f its semigroup of values which is defined to be the set :

$$\Gamma(f) = \{int(f, g) = O_x(g(x^n, y(x))),\ g \in \mathbb{K}[[x]][y] \backslash (f)\}$$

where $O_x(g(x^n, y(x)))$ denotes the smallest integer among the exponents of the power series $g(x^n, y(x))$. This semigroup is generated by the elements $r_0, r_1, ..., r_h$, defined by $r_0 = m_0 = n, r_1 = m_1$, and for all $2 \leq k \leq h$:

$$r_k = \frac{d_{k-1}}{d_k} r_{k-1} + m_k - m_{k-1}$$

Abhyankar proved in [4] that there exists a special king of polynomials $\{G_1, ..., G_h\}$, namely pseudo-roots of f, such that $deg(G_i) = \frac{n}{d_i}$ and $O(f, G_i) = r_i$. Moreover, he proves that $O(f, g_i) = r_i$ for all $i \in \{1, ..., h\}$ where $\{g_1, ..., g_h\}$ are the approximate roots of f (see Definition 4).
More generally let $f = y^n + a_1(x_1, ..., x_e)y^{n-1} + \cdots + a_n(x_1, ..., x_e)$ be a polynomial in y with coefficients $a_i(x_1, ..., x_e) \in \mathbb{K}[[x_1, ..., x_e]]$, the ring of formal power series in several variables, for all $1 \leq i \leq n$. Then, f is said to be quasi-ordinary if its discriminant $\Delta_y(f)$, which is defined to be the resultant in y of f and its y-derivative f_y, is of the form $\Delta_y(f) = x_1^{\alpha_1} \cdots x_e^{\alpha_e} \varepsilon(x_1, ..., x_e)$, where $\varepsilon(x_1, ..., x_e)$ is a unit in $\mathbb{K}[[x_1, ..., x_e]]$. If f

is irreducible then by the Abhyankar-Jung theorem [3, 18] f admits a solution $y(x_1,...,x_e)$ in $\mathbb{K}[[x_1^{\frac{1}{n}},...,x_e^{\frac{1}{n}}]]$. Moreover we have :

$$f(x_1^n,...,x_e^n,y)=\prod_{i=1}^{n}(y-y_i(x_1,...,x_e))$$

where $y_i(x_1,...,x_e)=y(\beta_1^i x_1,...,\beta_e^i x_e)$ are conjugates of y, where β_j^i is an n-th root of unity for all $1\leq i\leq n$, $1\leq j\leq e$. Now let $y=\sum_{(p_1,...,p_e)}c_{(p_1,...,p_e)}x_1^{p_1}\cdots x_e^{p_e}$ be a root of $f(x_1^n,...x_e^n,y)=0$, and define the support of f to be the set $Supp(f)=\{p\in\mathbb{N}^e,\ such\ that\ c_p\neq 0\}$. In [19], Lipman has proved that there exists a sequence of elements $m_1,...,m_h\in Supp(y)$ such that :
(i) $m_1<m_2<\cdots<m_h$ coordinate-wise.
(ii) If $m\in Supp(f)$, then $m\in(n\mathbb{Z})^e+\sum_{i=1}^{h}m_i\mathbb{Z}$
(iii) $m_i\notin(n\mathbb{Z})^e+\sum_{j<i}m_j\mathbb{Z}$ for all $i=1,...,h$.

The semigroup of f is defined to be the set $\Gamma(f)=\{O(f,g),\ g\in\mathbb{K}[[x_1,\ldots,x_e]][y]\backslash(f)\}$, where $O(f,g)$ is the lexiographical order of the the initial form of $g(x_1^n,...,x_e^n,y(x_1,...,x_e))$. Define the $\underline{D}$-sequence of f to be $D_1=n^e$, and for all $1\leq i\leq h$, D_i to be the gcd of the $e\times e$ minors of the matrix $[nI_e,m_1^T,...,m_i^T]$, where T denotes the transpose of the vector. We have $D_1>...>D_{h+1}=n^{e-1}$. We define the $\underline{e}$-sequence to be $e_i=\frac{D_i}{D_{i+1}}$ for all $1\leq i\leq h$, the $\underline{r}$-sequence $r_0^1,...,r_0^e,r_1,...,r_h$ to be :

$$r_i=e_{i-1}r_{i-1}+m_i-m_{i-1}$$

for all $1\leq i\leq h$, and $r_0^1,...,r_0^e$ to be the canonical basis of $\mathbb{Z}^e$. The sequence $\{r_0^1,...,r_0^e,r_1,...,r_h\}$ forms a system of generators of $\Gamma(f)$. Gonzàlez Pérez in [16] proved that for all $i\in\{1,...,h\}$ f admits an i-th semi-root, that is a polynomial g of degree $\frac{n}{d_i}$ such that $g(\underline{x}^n,y(\underline{x}))=\underline{x}^{r_i}\varepsilon$ for some ε unit in $\mathbb{K}[[\underline{x}]]$. Moreover, he proved that for all $i\in\{1,...,h\}$ the d_i-th approximate root of f is an i-th semi-root of f.

In sections 2 and 3 of the thesis we recall some preliminary facts about G-adic expansions, approximate roots, and affine semigroups. In section 4 we recall the Abhyankar-Jung theorem and the construction of the characteristic monomials of a quasi-ordinary branch done by Lipman [19], and the study of the semi-roots and approximate roots of a quasi-ordinary branch done by Gonzàlez Pérez in [16].

The aim of the first part of the thesis is to generalize these results from quasi-ordinary to a wider class of polynomials. Let $f(x_1,...,x_e,y)$ be a polynomial in y with coefficients in the polynomial ring $\mathbb{K}[x_1,...,x_e]$, McDonald proved in [21] that f admits a root in the ring of Puiseux power series with support in strongly convex polyhedral cone. Gonzàlez Pérez in [15] extended this result to polynomials with coefficients in the ring of Puiseux power series with support in a strongly convex polyhedral cone. Moreover, Aroca and Ilardi in [6] generalized McDonald results. Given $\omega\in\mathbb{R}^n$, they proved that the field of ω-positive Puiseux series is algebraically closed, where a ω-positive Puiseux series is a Puiseux series with support in a translate of a strongly convex rational polyhedral cone with $\omega.v\geq 0$ for all v in this cone.
In this work we take a polynomial $f=y^n+a_1(x_1,...,x_e)y^{n-1}+\cdots+a_n(x_1,...,x_e)$ in $\mathbb{K}[[x_1,...,x_e]][y]$ with a y-discriminant $\Delta_y(f)$(where the y-discriminant is defined to be the y-resultant of f and its y-derivative). By a preliminary change of variables we may assume that the homogeneous component of smallest degree of $\Delta_y(f)$ contains a power of x_1. Now by taking the change of variables :

$$x_1=X_1,x_2=X_2X_1,...,x_e=X_eX_1$$

we get a new polynomial $F(X_1,\ldots,X_e,y)$, which is quasi-ordinary, hence it has a root $y_N\in\mathbb{K}[[X_1^{\frac{1}{n}},...,X_e^{\frac{1}{n}}]]$. By taking the preimage we get a solution y of $f(x_1,\ldots,x_e,y)=0$, such that the support of y is in some line free cone C (where a line free cone C is a cone such that for all $x\in C$ we have $-x\notin C$). Thus y is in the set of fractional power series with exponents in the line free cone C, denoted by $\mathbb{K}_C[[x_1^{\frac{1}{n}},...,x_e^{\frac{1}{n}}]]$ (assuming that f is irreducible in $\mathbb{K}_C[[x_1,\ldots,x_e]][y]$). This set forms a ring under the usual addition and multiplication of

power series, moreover it is an integral domain.

The main idea of the birational change of variables above is the following : if f is irreducible in $\mathbb{K}_C[[x_1,\dots,x_e]][y]$ then F is an irreducible quasi-ordinay polynomial (see Theorem 4 and Lemma 17).
Since C is a line free cone, there exists an additive order $\leq$ on C which is compatible with C, i.e $\forall p \in C\cap\mathbb{Z}^e$ we have $p \geq (0,...,0)$. In particular every set $S \subseteq C\cap\mathbb{Z}^e$ has a minimal element with respect to this order, and so if we consider the support of y, then it can be arranged in an increasing order with respect to this order.
Let L be the fraction field of $\mathbb{K}_C[[x_1,...,x_e]]$, and let $L_n = L(x_1^{\frac{1}{n}},...,x_e^{\frac{1}{n}})$ be the field obtained by adjoining $x_1^{\frac{1}{n}},...,x_e^{\frac{1}{n}}$ to L, then a conjugate y_i of y is an element $\theta(y)$ for some automorphism θ of L_n over L. Note that y_i belongs to $\mathbb{K}_C[[x_1^{\frac{1}{n}},...,x_e^{\frac{1}{n}}]]$ also. We define the set of characteristic exponents of f to be :

$$\{O(y_i - y_j),\ \textit{such that } y_i, y_j \ \textit{ are distinct roots of } f\ \}$$

where $O(y_i - y_j)$ is the smallest element in $Supp(y_i - y_j)$ with respect to the order compatible with C. Similarly, for every $y_i \neq y_j$ let M_{ij} be the initial monomial of $y_i - y_j$. The obtained set $\{M_{ij}\}$ is called the set of characteristic monomials of f. Moreover, we prove that $L(y) = L(M_1,...,M_h)$.
Obviously the set of characteristic exponents of f is a finite subset in $C\cap\mathbb{Z}^e$, hence we can arrange them in an increasing order and write them as :

$$m_1 \leq \cdots \leq m_h.$$

Moreover we prove that :

(i) For all $m \in Supp(y)$, $m \in (n\mathbb{Z})^e + \sum_{i=1}^{h} m_i\mathbb{Z}$

(ii) $m_i \notin (n\mathbb{Z}^e) + \sum_{j=1}^{i-1} m_j\mathbb{Z}$

Let $D_1 = n^e$, and define D_{i+1} to be the gcd of the $e\times e$ minors of the matrix $(nI_e, m_1^T,...,m_i^T)$ for all $1 \leq i \leq h$, and set $e_i = \frac{D_i}{D_{i+1}}$. We obtain that $D_1 > \cdots > D_{h+1}$, and that the degree of extension of $L(M_1,...,M_i)$ over $L(M_1,...,M_{i-1})$ is equal to e_i. Consider the sequence $r_0^1,...,r_0^e,r_1,...,r_h$ by taking $r_0^1,...,r_0^e$ to be the canonical basis of $(n\mathbb{Z})^e$, and $r_i = e_{i-1}r_{i-1} + m_i - m_{i-1}$, then set $d_i = \frac{D_i}{n^{e-1}}$. Now define the semigroup of f to be the set $\Gamma(f) = \{O(f,g),\ g \in \mathbb{K}_C[[x_1,\dots,x_e]][[y]]\backslash(f)\}$, where $O(f,g)$ is the smallest element in $Supp(g(x_1^n,...,x_e^n,y(x_1,...,x_e)))$ with respect to the chosen order. As in the quasi-ordinary case, $\Gamma(f)$ is generated by $r_0^1,\dots,r_0^e,r_1,\dots,r_h$. Furthermore, there exists a special set of polynomials $g_1,...,g_h$(approximate roots of f), such that $O(f,g_i) = r_i$ for all $i = 1,...,h$.

In the second part of this theis we consider numerical semigroups and their ideals and we study their applications on one dimensional $\mathbb{K}$-algebras and the module of differentials of plane algebraic curves parametrized by polynomials. The aim of this part is to characterize these curves in terms of invariants such as Milnor number and Tjurina number.
A subset S of $\mathbb{N}$ is said to be a numerical semigroup if $0 \in S$ and for all $a,b \in S$ we have $a+b \in S$, and such that the set $G(S) = \mathbb{N}\backslash S$ is finite. Given a numerical semigroup S, we define the Frobenius number of S, denoted by $F(S)$, to be the maximum of the set $G(S)$. Note that every numerical semigroup admits a finite system of generators, that is, there exists $s_1,...,s_h \in S$ such that for all $s \in S$

$$s = \lambda_1 s_1 + \ldots + \lambda_h s_h$$

for some $\lambda_1,...,\lambda_h \in \mathbb{N}$. In this part we will be interested in a special class of numerical semigroups, called free numerical semigroups. Free numerical semigroups appear in the theory of singularities of algebraic plane curves and also in the theory of algebraic plane curves with one place at infinity. We aim to use the techniques developed in the theory of numerical semigroups and their ideals in order to characterize rational algebraic plane curves with one place at infinity with respect to invariants such as Milnor number and Tjurina number.
Let S be a numerical semigroup and let I be a subset of $\mathbb{N}$, then I is said to be a relative ideal of S if $I+S \subseteq I$ and for some $\alpha \in \mathbb{Z}$ we have $\alpha + I \subseteq S$. Note that for a relative ideal I there exists a set $\{a_1,...,a_l\} \subseteq I$ such that $I = \bigcup_{i=1}^{l}(a_i + S)$. This set is called a system of generators of I.

Let $\{f_1, ..., f_s\}$ be a set of elements in the polynomial ring $\mathbb{K}[t]$ and let $A = \mathbb{K}[f_1, ..., f_s]$, where $\mathbb{K}$ is a field. For every element $f \in \mathbb{K}[t]$ we denote by $d(f)$ the degree of f in t. Consider the set $d(A) = \{d(f),\ f \in A\}$ and suppose that the length $l(\mathbb{K}[t]/A) < +\infty$. Then $d(A)$ is a numerical semigroup. We say that $\{f_1, ..., f_s\}$ is a canonical basis of A if $\{d(f_1), ..., d(f_s)\}$ generates $d(A)$. It is proven that any $\mathbb{K}$-algebra A admits a canonical basis, moreover a basis can be obtained algorithmically form the elements $f_1, ..., f_s$ (see [10]).

Let $\{F_1, ..., F_r\}$ be a set of non zero elements in $\mathbb{K}[t]$, and let $M = \sum_{i=1}^{r} F_i A$ be the A-module generated by $F_1, ..., F_r$. Set

$$d(M) = \{d(F),\ F \in M\backslash\{0\}\}$$

Then $d(M)$ is a relative ideal of $d(A)$. We say that $\{F_1, ..., F_r\}$ is a canonical basis of M if $\{d(F_1), ..., d(F_r)\}$ is a system of generators of $d(M)$. Note that a basis of M can be obtained algorithmically from $\{F_1, ..., F_r\}$.

Let $\{f_1, ..., f_r\}$ be a set of polynomials of $\mathbb{K}[t]$. For all $i \in \{1, ..., r\}$ let $F_i = f_i'$ be the derivative of f_i with respect to t. Set $M = F_1 A + ... + F_r A$, then $I = d(M)$ is a relative ideal of $S = d(A)$. Note that if $g \in A$, then $g' \in M$, and so if $s \in d(A)$, then $s - 1 \in d(M)$. This leads to the definition of the set of non-exact elements of M, denoted by $NE(M)$, which is

$$NE(M) = \{a \in I,\ a + 1 \notin S\}.$$

We define $ne(M)$ to be the cardinality of $NE(M)$.

Suppose that $r = 2$, that is $A = \mathbb{K}[X(t), Y(t)]$ for some $X(t), Y(t) \in \mathbb{K}[t]$, and let $f(X, Y)$ be the smallest degree algebraic relation satisfied by $X(t)$ and $Y(t)$($f(X, Y)$ is the monic generator of the kernel of the morphism $\mathbb{K}[X, Y] \longmapsto \mathbb{K}[t]$, $\phi(X) = X(t), \phi(Y) = Y(t)$). Then f has one place at infinity (see [4]). Denote $d(A)$ by $\Gamma(f)$ and $F(\Gamma(f))$ by F. We can construct a set of generators $\{r_0, ..., r_h\}$ of $\Gamma(f)$ by taking the set of ranks of the vector spaces $\frac{\mathbb{K}[X,Y]}{(f,g)}$ where g runs over the set of approximate roots of f.
For all $i \in \{0, ..., h\}$ let $d_{i+1} = gcd(r_0, r_1, ..., r_i)$ and let $e_i = \frac{d_i}{d_{i+1}}$ for all $i \in \{1, ..., h\}$. Then $d_1 > d_2 > \cdots > d_{h+1} = 1$ and $e_i r_i \in \langle r_0, ..., r_{i-1}\rangle$ for all $i \in \{1, ..., h\}$. That is $\Gamma(f)$ is free with respect to the arrangement $(r_0, ..., r_h)$. Let f_X, f_Y be the derivatives of f with respect to X, Y. Let $\mu(f) = dim_{\mathbb{K}} \frac{\mathbb{K}[X,Y]}{(f_X, f_Y)}$ be the milnor number of f and $\nu(f) = dim_{\mathbb{K}} \frac{\mathbb{K}[X,Y]}{(f, f_X, f_Y)}$ be the Tjurina number of f. We use semigroup techniques in order to prove that $\mu(f) = \nu(f)$ if and only if $ne(M) = 0$, that is, every element of M is exact if and only if there exists an isomorphism $\mathbb{K}[X, Y] \mapsto \mathbb{K}[W, Z]$ such that the image of f by this isomorphism is of the form $W^n - Z^m$, with $gcd(n, m) = 1$ (Theorem 15, see also [7]). This theorem generalizes the local result of Saito for curves in [30] and also the result of Zariski in [31].

Suppose that $\mu(f) > \nu(f)$, that is $ne(M) > 0$. We prove in this case that $ne(M) > 2^{h-1}$ (see Proposition 66). Moreover we prove that if $ne(M) = 1$, then $S =< m, n >$ and $NE(M) = \{F - 1\}$. Moreover, if $ne(M) = 2$, then we have the following two cases (see Theorem 16) :

(i) $h = 1$ with $\Gamma(f) =< m, n >$ and we either have :
$\bullet NE(M) = \{F - 1, F - m - 1\}$ *or*
$\bullet NE(M) = \{F - 1, F - n - 1\}$.

(ii) $h = 2$ with $\Gamma(f) =< m, n, r_2 >$ and we either have :
• $NE(M) = \{F - 1, F - n - 1\}$ *or*,
• $NE(M) = \{F - 1, F - m - 1\}$ *or*,
• $NE(M) = \{F - 1, F - r_2 - 1\}$.
Finally we give a characterization of the semigroup $\Gamma(f)$ in case $ne(M) = 1$ or $ne(M) = 2$.

2

Free polynomials

2.1 G-adic Expansion and Approximate roots

In this section we introduce the notion of G-adic expansion of a polynomial with respect to a set of polynomials. We also introduce the notion of Tschirnhausen transform and that of approximate root of a polynomial. These notions will be used later in order to characterize the set of generators of the semigroup of a free polynomial.

2.1.1 Expansion of integers

Let $(m_0, ..., m_h)$ be an $(h+1)$-tuple of integers with $h \geq 1$. We set :
$d_1 = m_o, d_2 = \gcd(m_0, m_1), ..., d_i = \gcd(m_0, ..., m_{i-1}) = \gcd(d_{i-1}, m_{i-1})$, where gcd stands for the greatest common divisor. Suppose that $d_1 > d_2 > ... > d_{h+1}$, and let $e_i = \frac{d_i}{d_{i+1}}$ for all $i = 1, ..., h$.

Definition 1 *Let $\underline{m} = (m_0, m_1, ..., m_h)$ be a finite sequence of integers. A strict linear combination of $\underline{m}$ is an integer of the form :*

$$a_0 m_0 + a_1 m_1 + \cdots + a_h m_h$$

where $a_0 \in \mathbb{Z}$ and $0 \leq a_i < e_i$ for all $i = 1, ..., h$.

Proposition 1 *With the above notation, a given integer n can be expressed in at most one way as a strict linear combination $n = \sum_{i=0}^{h} a_i m_i$.*

Proof : Suppose $n = \sum_{i=0}^{h} a_i m_i = \sum_{i=0}^{h} b_i m_i$ with $a_0, b_0 \in \mathbb{Z}$ and $0 \leq a_i, b_i < e_i$ for all $i = 1, ..., h$. It is required to prove that $a_i = b_i$ for all i. Suppose to the contrary that it is not true, then there exists some j such that $a_j \neq b_j$, and $a_i = b_i \ \forall j < i \leq h$. Suppose that $a_j > b_j$. We have $\sum_{i=0}^{h} a_i m_i - \sum_{i=0}^{h} b_i m_i = \sum_{i=0}^{j} (a_i - b_i) m_i = 0$ with $0 < a_j - b_j < e_j$, and so $(a_j - b_j) m_j = \sum_{i=0}^{j-1} (b_i - a_i) m_i$.
Since d_j divides m_i for all $i = 0, ..., j-1$, then d_j divides $(a_j - b_j) m_j$, and so e_j divides $(a_j - b_j) \frac{m_j}{d_{j+1}}$, but e_j and $\frac{m_j}{d_{j+1}}$ are coprime, then e_j divides $a_j - b_j$, which is a contradiction since $a_j - b_j < e_j$. ■
As a corollary we get the following :

Corollary 1 *Let $u_1, ..., u_h$ be an h-tuple of distinct positive integers such that u_i divides u_{i+1} for all $1 \leq i \leq h-1$. If $\sum_{i=1}^{h} a_i u_i = \sum_{i=1}^{h} b_i u_i$ with $0 \leq a_i < \frac{u_{i+1}}{u_i}$ and $0 \leq b_i < \frac{u_{i+1}}{u_i}$ for all $i = 1, ..., h-1$ and a_h, b_h are non negative integers, then $a_i = b_i$ for all $1 \leq i \leq h$.*

Proof : Set $m_0 = u_h, m_1 = u_{h-1}, ..., m_{h-1} = u_1$, and let $d_i = gcd(m_0, ..., m_{i-1})$, then $d_1 = u_h, ..., d_h = u_1$. Now let $e_i = \frac{d_i}{d_{i+1}}$ for all $i = 1, ..., h-1$, then $a_1u_1 + \cdots + a_hu_h = a_hm_0 + a_{h-1}m_1 + \cdots + a_1m_{h-1}$ with $0 \leq a_{h-1} < \frac{u_h}{u_{h-1}} = \frac{d_1}{d_2} = e_1, ..., 0 \leq a_1 < \frac{u_2}{u_1} = \frac{d_{h-1}}{d_h} = e_{h-1}$ is a strict linear combination of $(m_0, ..., m_{h-1})$. By Proposition 1 this representation is unique, and so $a_i = b_i$ for all $1 \leq i \leq h$.■

2.1.2 G-adic expansion of a polynomial

Let $R[Y]$ be the polynomial ring in one variable, where R is a commutative unitary ring. For every element f in $R[Y]$, let $deg(f)$ be the degree of f in Y, with the convention that $\deg(0) = -\infty$.
Let $G = (G_1, ..., G_h)$ be an h-tuple of polynomials in $R[Y]$ satisfying the following conditions :
(i) The polynomial G_i is monic with $\deg(G_i) > 0$ for all $1 \leq i \leq h$.
(ii) $\deg(G_i)$ divides $\deg(G_{i+1})$ for all $1 \leq i \leq h-1$, and $\deg(G_1) = 1$.

Let $u_i = \deg(G_i)$ for $i = 1, ..., h$, and define the elements $n_1 = \frac{u_2}{u_1} = u_2, n_2 = \frac{u_3}{u_2}, ..., n_{h-1} = \frac{u_h}{u_{h-1}}$ and let $n_h = +\infty$. Let

$$A(G) = \{a = (a_1, ..., a_h) \in \mathbb{N}^h,\ 0 \leq a_i < n_i\ \forall 1 \leq i \leq h\}$$

and associate with each element a in $A(G)$ the polynomial $G^a = G_1^{a_1}...G_h^{a_h}$.

Definition 2 *Let f be a polynomial in $R[Y]$ and suppose that f can be written in the form $f = \sum_{a \in A(G), f_a \in R} f_a G^a$ for a finite number of a's. The expression $\sum_{a \in A(G)} f_a G^a$ is said to be a G-adic expansion of f.*

For every element $f = \sum_{a \in A(G)} f_a G^a$ we define $supp_G(f) = \{a \in A(G),\ f_a \neq 0\}$.

Proposition 2 *Let $R[G^A]$ be the R-submodule of $R[Y]$ generated by $G^A = \{G^a, a \in A(G)\}$. Then $R[G^A]$ is a free R-submodule.*

Proof : It is obvious that G^A is a system of generators of $R[G^A]$, and so it is required to prove that elements in G^A are linearly independent over R.
First of all, note that if a, b are distinct elements in $A(G)$, then $deg(G^a) \neq deg(G^b)$. In fact if $deg(G^a) = deg(G^b)$, then $\sum_{i=1}^{h} a_i u_i = \sum_{i=1}^{h} b_i u_i$, and so by Corollary 1 we get that $a = b$.
For linearly independence, suppose that $f = \sum_{a \in A(G)} f_a G^a = 0$ for some elements f_a in R, and suppose to the contrary that for some $a \in A(G)$ we have $f_a \neq 0$. Let $c \in supp_G(f)$ be such that $deg(G^c) = max\{deg(G^a), a \in Supp(f)\}$, then $deg(f) = deg(f_cG^c)$. If $c = 0$ in $\mathbb{N}^h$, then $f = f_cG^c = f_c = 0$, which contradicts our assumption. Otherwise, if $c \neq 0$, then $deg(G^c) = deg(f)$ is strictly positive, and so $f \neq 0$ which is impossible. Hence elements in G^A are linearly independent, and so G^A is a free R-basis of $R[G^A]$.■
From the above Proposition we conclude that if a polynomial $f \in R[G^A]$, then its G-adic expansion is unique. Moreover, there exists a unique $c \in supp_G(f)$ such that $deg(f) = deg(G^c) = max\{deg(G^a),\ a \in supp_G(f)\}$.

Lemma 1 *Let $a = (a_1, ..., a_h)$ be an element of $A(G)$. Suppose that $a_j \neq 0$ for some $1 \leq j \leq h$, and $a_i = 0$ for $i = j+1, ..., h$. Then $u_j \leq deg(G^a) < u_{j+1}$.*

Proof : Since $a_i \geq 0$ for all $1 \leq i < j$ and $a_j > 0$, then $a_j - 1 \geq 0$ and $a_1u_1 + ... + (a_j - 1)u_j \geq 0$, and so $deg(G^a) = \sum_{i=1}^{j} a_iu_i \geq u_j$. Concerning the right hand side of the inequality, we have $a_1 < n_1$ and so $a_1u_1 < n_1u_1 = u_2$. Now suppose that up to $j-1$ we have the inequality $\sum_{i=1}^{j-1} a_iu_i < u_j$, and consider $\sum_{i=1}^{j} a_iu_i$. We have $\sum_{i=1}^{j} a_iu_i = \sum_{i=1}^{j-1} a_iu_i + a_ju_j$ and $a_j < n_j$, and so $\sum_{i=1}^{j} a_iu_i < (a_j + 1)u_j \leq n_ju_j = u_{j+1}$. Finally $u_j \leq deg(G^a) < u_{j+1}$. ■

Lemma 2 *Let f be a non-constant polynomial in $R[G^A]$, then there exists some $j \in \{1, ..., h-1\}$ such that $u_j \leq deg(f) < u_{j+1}$. Moreover, for all $a \in supp_G(f)$, a can be written as $a = (a_1, ..., a_j, 0, ..., 0)$ with $0 \leq a_i < n_i$ for all $1 \leq i \leq j$.*

Proof : Let a be a non-zero element in $supp_G(f)$, then $a = (a_1, ..., a_k, 0, ..., 0)$ for some $1 < k \leq h$ and $a_k \neq 0$. Let $c = (c_1, ..., c_j, 0, ..., 0)$, with c_j non zero, be the unique element in $supp_G(f)$ such that $deg(f) = deg(G^c)$, then by Lemma 1 we have $u_j \leq deg(f) < u_{j+1}$. Also by Lemma 1 we have $u_k \leq deg(G^a) < u_{k+1}$, but $deg(G^a) < deg(G^c)$, then $u_k < u_{j+1}$, and so $k \leq j$. ■

Proposition 3 *Let $G = (G_1, ..., G_h)$ be a set of polynomials in $R[Y]$, such that $deg(G_1) = 1$ and $\deg(G_i)$ divides $\deg(G_{i+1})$ for all $i = 1, ..., h-1$, then every element f in $R[Y]$ is also in $R[G^A]$. In particular this expansion is unique.*

Proof : We will prove this by induction on the degree of f. If $deg(f) = 0$ or 1, then the assertion is clear. Suppose it is true for all polynomials h in $R[Y]$ with $deg(h) < n$, and let f be a polynomial of degree n. By Lemma 2, there exists some $j \in \{1, ..., h\}$ such that $u_j \leq deg(f) < u_{j+1}$. Since $u_{j+1} = n_ju_j$, then there exists some k, with $0 < k < n_j$, such that $ku_j \leq deg(f) < (k+1)u_j$. Now dividing f by G_j^k we get $f = qG_j^k + r$ with $deg(r) < deg(G_j^k) = ku_j \leq deg(f)$, and so by the induction hypothesis, r admits a G-adic expansion.
It remains to prove that qG_j^k admits a G-adic expansion. Since $deg(f) = deg(qG_j^k)$, then $deg(q) = deg(f) - ku_j < deg(f)$, hence q admits such an expansion, say $q = \sum_{a \in A(G)} q_aG^a, q_a \in R$, and so :

$$qG_j^k = \sum_{a \in supp(q)} q_aG^aG_j^k = \sum_{a \in supp(q)} q_aG_1^{a_1}...G_h^{a_h}G_j^k$$
$$= \sum_{a \in supp(q)} q_aG_1^{a_1}...G_{j-1}^{a_{j-1}}G_j^{a_j+k}G_{j+1}^{a_{j+1}}...G_h^{a_h}$$

Since $deg(q) < u_j$, then by the Lemma 2 every element $a \in Supp_G(q)$ has the form $a = (a_1, ..., a_{j-1}, 0, ..., 0)$, and so $supp_G(qG_j^k) = \{(a_1, ..., a_{j-1}, k, 0, ..., 0), a_1 < n_1, ..., a_{j-1} < n_{j-1}, k < n_j\}$, hence $\sum q_aG^aG_j^k$ is a G-adic expansion of qG_j^k, and so f admits a G-adic expansion.
From Proposition 2 we can easily see that the G-adic expansion of f is unique. ■

2.1.3 Tschirnhausen Transform

Let $g \in R[Y]$ be a monic polynomial with degree $m > 1$, and let $G = (G_1, G_2)$, where $G_1 = Y$ and $G_2 = g$. Let the notation be as before. In particular we have $n_1 = m = deg(g)$, $n_2 = \infty$ and $A(G) = \{a = (a_1, a_2)$, such that $0 \leq a_1 < m$ and $a_2 \in \mathbb{N}\}$.
According to Proposition 3 every polynomial $f(Y)$ in $R[Y]$ can be written in a unique way as follows :

$$f(Y) = \sum c_{i,j}Y^ig(Y)^j,\ 0 \leq i < m, c_{i,j} \in R.$$

Now for each j let $f_j(Y) = \sum_{i=1}^{m_j} c_{i,j} Y^i$, then f can be expressed as :

$$f = \sum_j f_j(Y) g(Y)^j$$

where $f_j(Y)$ are all zero except for a finite number of them and $\deg(f_j(Y)) < m$ for all j. Note that this expression is unique so that if f can be written as $\sum_k h_k g^k$ with $\deg(h_k) < deg(g)$, then $h_j = f_j$ for all j. This unique expansion of f in terms of g is called the **g-adic expansion** of f.

Lemma 3 *Let f be a monic polynomial in $R[Y]$ and consider another polynomial g such that g is monic and $\deg(g)$ divides $\deg(f)$, then the g-adic expansion of f is of the form :*

$$f = g^d + \sum_{i=0}^{d-1} c_f^{(i)}(Y) g^i, \text{ where } d = \frac{\deg(f)}{\deg(g)}$$

Proof : Let $f = \sum_{i=1}^{l} c_i g^i$, where $c_i \in R[Y]$ and $\deg(c_i) < \deg(g)$ for all $i = 1, ..., l$, be the g-adic expansion of f with respect to g. For all $i = 1, ..., l-1$ we have :

$$\deg(c_i g^i) = \deg(c_i) + i \deg(g) \leq \deg(c_i) + (l-1)\deg(g) < l \deg(g) \leq \deg(c_l g^l)$$

and so $\deg(f) = \deg(c_l g^l)$. Now write $\deg(f) = d \cdot \deg(g)$ for some strictly positive integer d. We have $\deg(c_l) + l.\deg(g) = d \cdot \deg(g)$, but $0 \leq \deg(c_l) < \deg(g)$, hence $\deg(c_l) = 0$ and $c_l \in R$. Moreover $l = d$. We have $\deg(f) = \deg(c_d g^d)$ and $\deg(f - c_d g^d) < \deg(f)$. But f and g are monic, then $c_d = 1$, and so the g-adic expansion of f with respect to g is :

$$f = g^d + \sum_{i=0}^{d-1} c_f^{(i)} g^i \ . \blacksquare$$

Definition 3 *Let f be a non-constant polynomial in $R[Y]$, let g be a monic polynomial such that $\deg(f) = d.\deg(g)$ for some integer d, and let $f = g^d + \sum_{i=0}^{d-1} c_f^{(i)} g^{d-i}$ be the g-adic expansion of f. Assume that $d^{-1} \in R$. The **Tschirnhausen transform** of g with respect to f is defined to be*

$$\tau_f(g) = g + d^{-1} c_f(g)$$

where $c_f(g) = c_f^{(d-1)}$ is the coefficient of g^{d-1} in the g-adic expansion of f ; it is called the Tschirnhausen coefficient.

Note that the Tschirnhausen transform is a monic polynomial with $\deg(\tau_f)(g) = \deg(g)$ since $\deg(c_f(g)) < \deg(g)$, and so we can define recursively by induction the i-th Tschirnhausen transform of g to be :

$$\tau_f^i(g) = \tau_f(\tau_f^{(i-1)}(g))$$

Now let $f = g^d + c_f(g) g^{d-1} + \sum_{i=0}^{d-2} c_f^i g^i$ be the g-adic expansion of f as above, and suppose that $c_f(g)$ is different from zero. Then $\deg(f - g^d) = \deg(c_f(g) g^{d-1}) = \deg(c_f(g)) + (d-1)\deg(g)$, and so

$$\deg(c_f(g)) = \deg(f - g^d) - (d-1)\deg(g).$$

Proposition 4 *Let the notation be as above, and let $\tau_f(g) = g + d^{-1} c_f(g)$ be the Tschirnhausen transform of g with respect to f. Then $\deg(c_f(\tau_f(g))) < \deg(c_f(g))$.*

Proof : Let $n = \deg(c_f(g))$ and $h = \tau_f(g) = g + d^{-1}c_f(g)$, then $h^d = g^d + c_f(g)g^{d-1} + r$, *where* $r = \sum_{i=2}^{d} C_d^i c_f(g)^i g^{d-i}$, and C_d^i represents the number of all i-combinations of d-elements. Now for all $2 \leq i \leq d$ write $i = j + 2, 0 \leq j \leq d-2$ then :

$$\begin{aligned}\deg((c_f(g))^i g^{d-i}) = i \cdot n + (d-i)\deg(g) &= (j+2)n + (d-2-j)\deg(g) \\ &= 2n + (d-2)\deg(g) + j(n - \deg(g))\end{aligned}$$

but $n < \deg(g)$, and so $\deg(c_f(g)^i g^{d-i}) \leq 2n + (d-2)\deg(g) < n + (d-1)\deg(g)$, hence $\deg(r) < n + (d-1)\deg(g)$.

We have $f - h^d = f - g^d - c_f(g)g^{d-1} - r = \sum_{i=0}^{d-2} c_f^i g^i - r$, but $\sum_{i=0}^{d-2} c_f^i g^i$ is the g-adic expansion of $f - g^d - c_f(g)g^{d-1}$, hence :

$$\deg(\sum_{i=0}^{d-2} c_f^i g^i) = \deg(c_f^{d-2}) + (d-2)\deg(g) < (d-1)\deg(g) \leq n + (d-1)\deg(g)$$

Finally we got that $\deg(\sum_{i=0}^{d-2} c_f^i g^i) < n + (d-1)\deg(g)$ and $\deg(r) < n + (d-1)\deg(g)$, hence $\deg(f - h^d) < n + (d-1)\deg(g)$. Since $\deg(c_f(\tau_f(g))) = \deg(f - h^d) - (d-1)\deg(h)$ and $\deg(g) = \deg(h)$, then

$$\deg(c_f(\tau_f(g))) < n = \deg(c_f(g)). \blacksquare$$

Definition 4 *Let f be a monic polynomial in $R[Y]$ of degree n, and let d be a divisor of n, a polynomial g in $R[Y]$ of degree $\frac{n}{d}$ is said to be a d-**th Approximate root** of f if $\deg(f - g^d) < n - \frac{n}{d}$. It is denoted by $App_d(f)$.*

Proposition 5 *Let f be a monic polynomial of degree n in $R[Y]$, and let d be a divisor of n. A monic polynomial g is an approximate root of f if and only if $deg(g) = \frac{n}{d}$ and $c_f(g) = 0$.*

Proof : Suppose that g is an approximate root of f. We have $deg(f) = n$ and $deg(f - g^d) < n - \frac{n}{d} < n$, then $deg(g^d) = deg(f) = n$ and so $deg(g) = \frac{n}{d}$. Since $deg(g)$ divides $deg(f)$, then by Lemma 3 the g-adic expansion of f is of the form :

$$f = g^d + \sum_{i=0}^{d-1} c_f^{(i)} g^i, \ \textit{with } 0 \leq deg(c_f^i) < deg(g) \ \forall i = 1, ..., d-1.$$

Since the g-adic expansion of a polynomial is unique and $deg(c_f^{(i)}) < deg(g)$ for all $i = 1, ..., d-1$, then $\sum_{i=0}^{d-1} c_f^{(i)} g^i$ is the g-adic expansion of $f - g^d$. If $c_f^{d-1} = c_f(g) \neq 0$, then $deg(f - g^d) = deg(c_f(g)) + (d-1)deg(g)$, and so $(d-1)deg(g) \leq deg(f - g^d)$. But this is impossible because $deg(f - g^d) < n - \frac{n}{d} = (d-1)deg(g)$, hence $c_f(g) = 0$.
Conversely suppose that $deg(g) = \frac{n}{d}$ and $c_f(g) = 0$, then the g-adic expansion of f is of the form

$$f = g^d + \sum_{i=0}^{d-2} c_f^i g^{d-i}$$

and so $\sum_{i=0}^{d-2} c_f^i g^{d-i}$ is the g-adic expansion of $f - g^d$, then :

$$deg(f - g^d) = deg(c_f^{d-2}) + (d-2)deg(g) < (d-1)deg(g) = (d-1)\frac{n}{d} = n - \frac{n}{d}$$

and so g is a d-th approximate root of f.$\blacksquare$

Proposition 6 *Let f be a monic polynomial of degree n in $R[Y]$, and let d be a divisor of n. Then f admits a d-th approximate root and this approximate root is unique. In particular $App_d(f) = \tau_f^{\frac{n}{d}}(g)$.*

Proof : Let g be any monic polynomial in $R[Y]$ of degree $\frac{n}{d}$. By Proposition 4 we have $deg(c_f(\tau_f(g))) < deg(c_f(g))$, and so for all $i \geq 2$ we get $deg(c_f(\tau_f^i(g))) < deg(c_f(\tau_f^{i-1}(g))) < deg(g) = \frac{n}{d}$. In particular if we take $i = \frac{n}{d}$, then $c_f(\tau_f^i(g)) = 0$. But $deg(\tau_f(g)) = deg(g)$, then by Proposition 5 $\tau_f^i(g)$ is an approximate root of f.
For uniqueness, let g_1 and g_2 be two d-th approximate roots of f with $deg(g_1) = deg(g_2) = \frac{n}{d}$. We have $deg(f - g_1^d) < n - \frac{n}{d}$ and $deg(f - g_2^d) < n - \frac{n}{d}$, and so :

$$deg(g_1^d - g_2^d) \leq max\{deg(f - g_1^d), deg(f - g_2^d)\} < n - \frac{n}{d}$$

But $g_1^d - g_2^d = (g_1 - g_2) \sum_{i+j=d-1} g_1^i g_2^j$. If $g_1 \neq g_2$, then :

$$deg(g_1^d - g_2^d) = deg(g_1 - g_2) + deg(\sum_{i+j=d-1} g_1^i g_2^j) \geq deg(g_1^i g_2^j) = (i+j)\frac{n}{d} = (d-1)\frac{n}{d} = n - \frac{n}{d}$$

which is a contradiction, and so $g_1 = g_2$, and the d-th approximate root of f is unique.■

Proposition 7 *Let f be a polynomial of of degree n in $R[y]$, and let $d_1 > ... > d_{h+1}$ be a set of divisors of n. For all $i \in \{1, ..., h\}$ set $e_i = \frac{d_i}{d_{i+1}}$. Then for all $i = 1, ..., h-1$ we have $App_{d_i}(f) = App_{e_i}(App_{d_{i+1}}(f))$.*

Proof : Let $i \in \{1, ..., h-1\}$. Set $g_i = App_{d_i}(f)$, $g_{i+1} = App_{d_{i+1}}(f)$, and $G_i = App_{e_i}(g_{i+1})$. Note that $deg_y(g_i) = \frac{n}{d_i}, \deg_y(g_{i+1}) = \frac{n}{d_{i+1}}$ and $\deg_y(G_i) = \frac{n}{d_i}$. Since $G_i = App_{e_i}(g_{i+1})$ then the G_i-adic expansion of g_{i+1} is of the form :

$$g_{i+1} = G_i^{e_i} + \alpha_2 G_i^{e_i-2} + \ldots + \alpha_{e_i-1} G_i + \alpha_{e_i}$$

Where $\alpha_j \in R[y]$ for all $j = 2, ..., e_i$ such that $\deg_y(\alpha_j) < \frac{n}{d_i}$. consider the g_{i+1}-adic expansion of f

$$f = g_{i+1}^{d_{i+1}} + \beta_2 g_{i+1}^{d_{i+1}-2} + \ldots + \beta_{d_{i+1}}$$

Where $\beta_k \in R[y]$ for all $k \in \{2, ..., d_{i+1}\}$ such that $\deg_y(\beta_k) < \frac{n}{d_{i+1}}$. Substituting the above value of g_{i+1} in the equation of f, by an easy calculation we can prove that $f = G_i^{d_i} + \psi$ where ψ is a polynomial in $R[y]$ such that $\deg_y(\psi) < \deg_y(G_i^{d_i-1}) = (d_i - 1)\frac{n}{d_i}$, and so the G_i-adic expansion of f is of the form

$$f = G_i^{d_i} + \gamma_2 G_i^{d_i-2} + \ldots + \gamma_{d_i}$$

With $deg_y(\gamma_l) < \frac{n}{d_i}$ for all $l \in \{2, ..., d_{i+1}\}$. It follows that $G_{i+1} = App_{d_i}(f) = g_i$.■

2.2 Affine semigroups

This section aims to give some general results about affine semigroups. These results will be used constantly in the next sections, since the semigroup associated with a free polynomial is an affine semigroup.

2.2.1 Free affine semigroups

Definition 5 *A **Semigroup** is a set S equipped with an associative binary operation $+$, such that for every x, y in S we have $x + y \in S$.*

A semigroup S is said to be finitely generated if there exists a finite number of elements $v_1, ..., v_e$ in S such that for every $v \in S$, we have $v = \lambda_1 v_1 + \cdots \lambda_e v_e$ with $\lambda_1, ..., \lambda_e \in \mathbb{N}$, in this case $\{v_1, ..., v_e\}$ is said to be a system of generators of S.

Definition 6 *A semigroup S is said to be an **Affine Semigroup** if it is a finitely generated semigroup of $\mathbb{Z}^e$ for some $e \in \mathbb{N}^*$.*

Definition 7 *A set $C \subset \mathbb{R}^e$ is said to be a cone if $\forall m \in C$ and $\lambda \geq 0$ we have $\lambda.m \in C$.*

If there exist some vectors $v_1, ..., v_n$ in $\mathbb{R}^e$ such that $C = \{\lambda_1.v_1 + ... + \lambda_n.v_n, \lambda_i \geq 0, \forall\ 1 \leq i \leq n\}$, then we say that C is finitely generated. Furthermore if the generating set $\{v_1, ..., v_n\}$ is a subset of $\mathbb{Z}^e$ then the cone is said to be rational. From now on all the considered cones are supposed to be rational finitley generated cones.
Let $\underline{v} = (v_1, ..., v_e, v_{e+1}, ..., v_{e+h})$ be a set of nonzero elements of $\mathbb{Z}^e$ and let

$$\Gamma(\underline{v}) = \{\sum_{i=1}^{e+h} a_i v_i,\ a_i \in \mathbb{N}\}, \quad G(\underline{v}) = \{\sum_{i=1}^{e+h} a_i v_i,\ a_i \in \mathbb{Z}\}$$

be the subsemigroup of $\mathbb{N}^e$ generated by $\underline{v}$, and the subgroup of $\mathbb{Z}^e$ generated by $\underline{v}$ respectively. Moreover, for every $0 \leq k \leq h$ let $G_k = \{\sum_{i=1}^{e+k} a_i v_i,\ a_i \in \mathbb{Z}\}$ be the subgroup of $\mathbb{Z}^e$ generated by $v_1, ..., v_{e+k}$, $\Gamma_k = \{\sum_{i=1}^{e+k} a_i v_i,\ a_i \in \mathbb{N}\}$ be the semigroup generated by $v_1, ..., v_{e+k}$, and $cone(v_1, ..., v_e)$ the convex cone generated by $v_1, ..., v_e$. More precisely

$$cone(v_1, ..., v_e) = \{\sum_{i=1}^{e} a_i v_i,\ a_i \in \mathbb{R}_+\}$$

Assume that the dimension of $cone(v_1, ..., v_e)$ is equal to e, i.e $\{v_1, ..., v_e\}$ generates $\mathbb{R}^e$ and that $v_{e+1}, ..., v_{e+h} \in cone(v_1, ..., v_e)$.
Let D_1 be the determinant of the matrix $(v_1^T, ..., v_e^T)$, where v_i^T denotes the transpose of the vector v_i, and for all $i = 2, ..., h+1$, let D_i be the *gcd* of the $e \times e$ minors of the matrix $[v_1^T, ..., v_e^T, v_{e+1}^T, ..., v_{e+i-1}^T]$. For all $i = 1, ..., h$ set $e_i = \frac{D_i}{D_{i+1}}$.

Definition 8 *Let $v_1, ..., v_{e+h} \in \mathbb{Z}^e$ and let $S = \Gamma(v_1, ..., v_e, v_{e+1}, ..., v_{e+h})$. Then S is said to be a free affine semigroup if the following two conditions are satisfied :*
(i) $D_1 > D_2 > \cdots > D_{h+1}$, equivalent to saying that for all $i = 1, ..., h$, v_{e+i} is not in the group generated by $v_1, ..., v_e, v_{e+1}, ..., v_{e+i-1}$.
(ii) For each $i = 1, ..., h$ we have $e_i v_{e+i} \in \Gamma(v_1, ..., v_{e+i-1})$.

2.2.2 Standard representation and the Frobenius vector.

Proposition 8 *Let $0 \leq k \leq h$ and $v \in G_k$. There exist unique integers $\lambda_1, ..., \lambda_e, \lambda_{e+1}, ..., \lambda_{e+k}$ such that $v = \sum_{i=1}^{e+k} \lambda_i v_i$ with $0 \leq \lambda_{e+i} < e_i$ for all $i = 1, ..., k$.*

Proof : Since $v \in G_k$, then $v = \sum_{i=1}^{e+k} c_i v_i$ where $c_i \in \mathbb{Z}$ for all $1 \leq i \leq e+k$. If $k = 0$, then the assertion is clear. Assume that $k \geq 1$, and that $c_{e+k} < 0$. Write $c_{e+k} = pe_k + \bar{c}_{e+k}$ with $0 \leq \bar{c}_{e+k} < e_k$, then

$$v = \sum_{i=1}^{e+k-1} c_i v_i + (pe_k + \bar{c}_{e+k}) v_{e+k}$$

Since $e_k v_{e+k} \in G_{k-1}$ then so is for $pe_k v_{e+k}$ and so we can write v as $v = \sum_{i=1}^{e+k-1} \tilde{c}_i v_i + \bar{c}_{e+k} v_{e+k}$ with $0 \leq \bar{c}_{e+k} < e_k$, and $\tilde{c}_i \in \mathbb{Z}$ for all $1 \leq i \leq e+k-1$. Now $\sum_{i=1}^{e+k-1} \tilde{c}_i v_i \in G_{k-1}$, and so we get the result by induction on k, hence the expression exists.
To prove the uniqueness, let $v = \sum_{i=1}^{e+k} a_i v_i = \sum_{i=1}^{e+k} b_i v_i$ where $0 \leq a_{e+i}, b_{e+i} < e_i$ for all $i = 1, ..., k$, and let α be the greatest integer such that $a_\alpha - b_\alpha \neq 0$. Suppose that $\alpha = e + j$ for some $j \geq 1$, and also that $a_\alpha - b_\alpha > 0$, then :

$$(a_{e+j} - b_{e+j}) v_{e+j} = \sum_{i=1}^{e} (b_i - a_i) v_i + (b_{e+1} - a_{e+1}) v_{e+1} + ... + (b_{e+j-1} - a_{e+j-1}) v_{e+j-1} \in G_{j-1}$$

and $0 < a_j - b_j < e_j$, which contradicts the hypothesis. ■

Definition 9 *Let v be a vector in G_k, The standard representation of v is defined to be $v = \sum_{i=1}^{e+k} \lambda_i v_i$ with $0 \leq \lambda_{e+i} < e_i$ for all $i = 1, ..., k$.*

Proposition 9 *Let $0 \leq k \leq h$, and consider a vector $v \in G_k$. Let*

$$v = \sum_{i=1}^{e+k} \lambda_i v_i$$

be its standard representation with respect to the vectors $v_1, ..., v_{e+k}$. The vector $v \in \Gamma_k$ if and only if $\lambda_i \geq 0$ for all $i = 1, ..., e$.

Proof : If $\lambda_i \geq 0$ for all $i = 1, ..., e$, then obviously $v \in \Gamma(v_1, ..., v_{e+k})$. Conversely suppose that $v \in \Gamma(v_1, ..., v_{e+k})$, then $v = \sum_{i=1}^{e+k} a_i v_i$ where $a_i \geq 0$ for all $1 \leq i \leq e+k$. If $0 \leq a_{e+i} < e_i$ for all $i = 1, ..., k$, then it is over. Otherwise, take j such that $a_{e+j} \geq e_j$ and $0 \leq a_{e+i} < e_i$ for all $i > j$. Write a_{e+j} as $a_{e+j} = me_j + b_j$, where $m \in \mathbb{N}^*$ and $0 \leq b_j \leq e_j$. But $e_j v_{e+j} \in \Gamma(v_1, ..., v_{e+j-1})$, and so $e_j v_{e+j} = \sum_{i=1}^{e+j-1} c_i v_i$, where $c_i \geq 0$ for all $1 \leq i \leq e+j-1$. Hence :

$$\begin{aligned} v &= \sum_{i=1}^{e+j-1} a_i v_i + (me_j + b_j) v_{e+j} + \sum_{i=e+j+1}^{k} a_i v_i \\ &= \sum_{i=1}^{e+j-1} (a_i + mc_i) v_i + b_j v_{e+j} + \sum_{i=e+j+1}^{k} a_i v_i \end{aligned}$$

Proceeding like this we can construct the standard representation of v, with $v = \sum_{i=1}^{e+k} \alpha_i v_i$, and $\alpha_i \geq 0$ for all $i = 1, ..., e$.■

Definition 10 *Let $\underline{v} = (v_1, ..., v_{e+h})$ be a set of non-zero vectors of $\mathbb{Z}^e$, and let the notation be as above. Let C be the topological interior of cone $(v_1, ..., v_e)$, i.e $C = \{\lambda_i v_i,\ \lambda_i \in \mathbb{R}_+^*\ \forall 1 \leq i \leq e\}$. The Frobenius vector of $\underline{v}$ is defined to be an element $w \in$ cone $(v_1, ..., v_e)$ such that $w \notin \Gamma(\underline{v})$, and for all $v \in w + (C - \{\underline{0}\})$ we have :*

$$v \in G(\underline{v}) \Longrightarrow v \in \Gamma(\underline{v})$$

Theorem 1 *Let the notation be as above with $\underline{v} = (v_1, ..., v_{e+h})$, and C the interior of cone$(v_1, ..., v_e)$. The frobenius vector of $\underline{v}$ is equal to :*

$$F(\underline{v}) = \sum_{k=1}^{h}(e_k - 1)v_{e+k} - \sum_{i=1}^{e} v_i$$

Proof : It is clear that $\sum_{k=1}^{h}(e_k - 1)v_{e+k} - \sum_{i=1}^{e} v_i$ is a standard representation, but the coefficients of $v_1, ..., v_e$ are negative. By Proposition 9 we get that $F(\underline{v}) \notin \Gamma(\underline{v})$.

Now let $u \in C - \{\underline{0}\}$, and consider the vector $v = F(\underline{v}) + u$. Assume that $v \in G(\underline{v})$, and let $v = \sum_{k=1}^{e+h} \alpha_k v_k$ be the standard representation of v with $0 \leq \alpha_{e+k} < e_k$ for all $k = 1, ..., h$. We have :

$$v = F(\underline{v}) + u \Longrightarrow \sum_{k=1}^{h}(e_k - 1 - \alpha_{e+k})v_{e+k} + u = (\alpha_1 + 1)v_1 + ... + (\alpha_e + 1)v_e$$

and since $\sum_{k=1}^{h}(e_k - 1 - \alpha_{e+k})v_{e+k} + u \in C$, then $\alpha_k + 1 > 0$ for all $k = 1, ..., e$, and so $\alpha_k \geq 0$ for all $k = 1, ..., e$. By Proposition 9 we obtain $v = F(\underline{v}) + u \in \Gamma(\underline{v})$.■

2.3 Quasi-Ordinary Polynomials

In this section we recall the notion of a quasi-ordinary polynomial and how to associate a semigroup to such a polynomial.

2.3.1 Abhyankar-Jung theorem

Definition 11 *Let $f = a_n x^n + ... + a_1 x + a_0$ and $g = b_m x^m + ... + b_1 x + b_0$ be two polynomials of degree n and m, respectively, in $R[x]$, where R is an arbitrary ring. The resultant of f and g, denoted by $R(f,g)$ is defined to be the determinant of the $(m+n) \times (m+n)$ matrix given by :*

$$\begin{pmatrix}
a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & \cdots & 0 \\
0 & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
\vdots & & & & & & & & & \vdots \\
0 & \cdots & 0 & a_n & \cdots & \cdots & \cdots & \cdots & a_1 & a_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & \cdots & \cdots & 0 \\
0 & b_m & \cdots & & b_1 & b_0 & 0 & \cdots & \cdots & 0 \\
\vdots & & & & \vdots & & & & & \vdots \\
0 & \cdots & & 0 & b_m & b_{m-1} & \cdots & & b_1 & b_0
\end{pmatrix}$$

where from the second row up to row m we shift the coefficients $a_n, ..., a_0$ of f one step to the right and zero elsewhere, and we do the same for $b_m, ..., b_0$ the coefficients of g from row $m+2$ up to row $m+n$.

Proposition 10 *Let $\mathbb{K}$ be an arbitrary field. Let $f = a_n x^n + ... + a_1 x + a_0$ and $g = b_m x^m + ... + b_1 x + b_0$ be polynomials in $\mathbb{K}[x]$ of degrees n and m, respectively. The resultant of f and g is given by :*

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{i=1}^{m} (y_i - z_j)$$

where $y_1, ..., y_n$ are the roots of f, and $z_1, ..., z_m$ are the roots of g in some extension field $\bar{\mathbb{K}}$ of $\mathbb{K}$.

Definition 12 *Let $f = a_n x^n + ... + a_1 x + a_0$ be a polynomial of degree n in $\mathbb{K}[x]$, and let $y_1, ..., y_n$ be its roots in some extension field of $\mathbb{K}$. The discriminant of f is defined to be :*

$$\Delta(f) = a_n^{2n-2} \prod_{1 \le i < j \le n} (y_i - y_j)^2$$

Note that we can also define the discriminant of f using the resultant of f and f_x, where f_x is the derivative of f with respect to x, more precisely we can prove that :

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \cdot a_n^{-1} R(f, f_x).$$

Let $\mathbb{K}$ be an algebraically closed field of characteristic 0, and let $\mathbb{K}[[x_1, ..., x_e]]$ be the ring of formal power series in $x_1, ..., x_e$. For simplicity we write $\underline{x}^\alpha$ Instead of $x_1^{\alpha_1} \cdots x_e^{\alpha e}$, where $\alpha = (\alpha_1, ..., \alpha_e) \in \mathbb{N}^e$.
Similarly for each $n \in \mathbb{N}^*$ we can define a ring of formal power series over $\mathbb{K}$ with fractional exponents denoted by $\mathbb{K}[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$. For simplicity we write $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ instead of $\mathbb{K}[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ and $\mathbb{K}[[\underline{x}]]$ instead of $\mathbb{K}[[x_1, ..., x_e]]$. Note that an element in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ is of the form $y(\underline{x}) = \sum_{m \in \mathbb{N}^e} c_m \underline{x}^{\frac{m}{n}}$, where $c_m \in \mathbb{K}$ and $\underline{x}^{\frac{m}{n}} = x_1^{\frac{m_1}{n}} ... x_e^{\frac{m_e}{n}}$, where $m = (m_1, ..., m_e) \in \mathbb{N}^e$.

Definition 13 *Let $f = y^n + a_1(\underline{x}) y^{n-1} + \cdots + a_{n-1}(\underline{x}) y + a_n(\underline{x})$ be a monic polynomial in $\mathbb{K}[[\underline{x}]][y]$, and suppose that $a_i(0) = 0$ for all $i = 1, ..., n$(such a polynomial is called a Weierstrass polynomial). Then f is said to be a **quasi-ordinary** polynomial if its discriminant in y, $\Delta_y(f)$ is of the form $x_1^{N_1} \cdots x_e^{N_e} u(x_1, ..., x_e)$, where $N_1, ..., N_e \in \mathbb{N}$ and $u(\underline{x})$ is a unit in $K[[\underline{x}]]$, i.e $u(\underline{x}) = c + v(\underline{x})$ for some formal power series $v(\underline{x})$ satisfying $v(\underline{0}) = 0$, and a constant $c \neq 0$.*

Theorem 2 ***Abhyankar-Jung Theorem*** *Let $f(\underline{x}, y)$ be a quasi-ordinary polynomial in $\mathbb{K}[[\underline{x}]][y]$. There exists a formal power series $y(x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}})$ in $\mathbb{K}[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ such that $f(\underline{x}, y(x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}})) = 0$ for some $n \in \mathbb{N}$. Furthermore if f is an irreducible polynomial of degree n, we have :*

$$f(x_1^n, ..., x_e^n, y) = \prod_{i=1}^{n} (y - y(w_1^i x_1, ..., w_e^i x_e))$$

where $(w_1^i, ..., w_e^i)_{1 \leq i \leq n}$ are distinct elements of $(U_n)^e$, where U_n is the set of n-th roots of unity in $\mathbb{K}$.

Definition 14 *Let $y(\underline{x}) = \sum_{p \in \mathbb{N}^e} c_p \underline{x}^{\frac{p}{n}} \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, for some integer n. We define the support of y, denoted $Supp(y)$, to be the set $Supp(y) = \{p \in \mathbb{N}^e,\ c_p \neq 0\}$.*

Note that if f is a polynomial in $\mathbb{K}[[\underline{x}]][y]$ that admits a root $y(\underline{x}) = \sum_{p \in \mathbb{N}^e} c_p \underline{x}^{\frac{p}{n}} \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, then for every $w_1, ..., w_e \in U_n$, $Supp(y(w_1^i x_1, ..., w_e^i x_e)) = Supp(y)$. We define the support of f to be $Supp(f) = Supp(y)$ for some root y of f.
Given $a = (a_1, ..., a_e), b = (b_1, ..., b_e) \in \mathbb{N}^e$, we say that $a \leq b$ (respectively $a < b$) coordinate-wise if $a_i \leq b_i$ (respectively $a_i < b_i$) for all $1 \leq i \leq n$.

2.3.2 Characteristic monomials of a quasi-ordinary polynomial

Proposition 11 *Let f be an irreducible quasi-ordinary polynomial of degree n, and let $\{y_i\}_{1 \leq i \leq n}$ be the set of roots of f. For all $i \neq j$ we have $y_i - y_j = M_{ij}\varepsilon_{ij}$ for some monomial $M_{ij} \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ and a unit ε_{ij} in $\mathbb{K}[[\underline{x}]]$.*

Proof : Let $\Delta(f)$ be the discriminant of f, then :

$$\Delta(f) = \prod_{i \neq j} (y_i - y_j) = M.h$$

where $M = x_1^{\frac{m_1}{n}} ... x_e^{\frac{m_e}{n}}$ and h is unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, i.e $h(\underline{0}) \neq 0$. Since $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ is a unique factorization domain, and $x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}$ are irreducible elements in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ then for each $1 \leq i, j \leq n$ with $i \neq j$ we have $y_i - y_j = x_1^{\frac{\alpha_1}{n}} ... x_e^{\frac{\alpha_e}{n}} \varepsilon_{ij} = M_{ij}\varepsilon_{ij}$, where $0 \leq \alpha_k \leq m_k$ are positive integers for all $1 \leq k \leq e$ that depends on y_i and y_j, and ε_{ij} a unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$.■

Definition 15 *Let the notation be as above with f a quasi-ordinary polynomial and $\{M_{ij}\}_{i \neq j}$ the set of monomials such that $y_i - y_j = M_{ij}\varepsilon_{ij}$ for some ε_{ij} unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$. The set $\{M_{ij}\}_{i \neq j}$ is said to be the set of characteristic monomials of f.*

Moreover, let $y = y_1$ be one of the roots of f, and let M_{ij} be one of the characteristic monomials of f. There exists some conjugate y_k of y such that $y - y_k = M_{ij}$.

Definition 16 *Let f be a quasi-ordinary polynomial in $\mathbb{K}[[\underline{x}]][y]$, and let $y(\underline{x}) \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ be a root of f. The element y is said to be a quasi-ordinary branch. We define the set of characteristic monomials of y to be the set of characteristic monomials of f.*

Note that if a quasi-ordinary branch $y \in \mathbb{K}[[\underline{x}]]$, then it has no characteristic monomials. If $y \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ for some $n > 1$ and z is a conjugate of y, then they both define the same set of characteristic monomials $\{M_1 = \underline{x}^{\frac{m_1}{n}}, ..., M_h = \underline{x}^{\frac{m_h}{n}}\}$ with $h \in \mathbb{N}$. The set $\{m_1, ..., m_h\} \subset \mathbb{N}^e$ is called the set of characteristic exponents of y.

Proposition 12 *Let f be an irreducible quasi-ordinary polynomial of degree n in $\mathbb{K}[[\underline{x}]][y]$ with a root $y \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$. The set of characteristic exponents of f is ordered with respect to the componentwise order.*

Proof : Let m_1, m_2 be two characteristic exponents of f, and let $M_1 = \underline{x}^{\frac{m_1}{n}}, M_2 = \underline{x}^{\frac{m_2}{n}}$ be the associated characteristic monomials, then there exists y_i, y_j two conjugates of y in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ such that $y - y_i = M_1\varepsilon_1$ and $y - y_j = M_2\varepsilon_2$ for some $\varepsilon_1, \varepsilon_2$ units in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, and so $y_i - y_j = (y - y_j) - (y - y_i) = M_2\varepsilon_2 - M_1\varepsilon_1$. By definition there exists a characteristic monomial M_{ij} such that $y_i - y_j = M_{ij}\varepsilon_{ij}$ with ε_{ij} is a unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, and we get that $M_2\varepsilon_2 - M_1\varepsilon_1 = M_{ij}\varepsilon_{ij}$, hence M_2 divides M_1 or M_1 divides M_2, and so $m_1 < m_2$ or $m_2 < m_1$ component-wise. We finally conclude that the set of characteristic exponents of y can be arranged as $m_1 < \cdots < m_h$ component-wise.■

Remark 1 *Let $f = y^n + a_1(\underline{x})y^{n-1} + \cdots + a_1(\underline{x})y + a_0(\underline{x})$ be a quasi-ordinary polynomial in $\mathbb{K}[[\underline{x}]][y]$. We have :*

$$f(\underline{0}, y) = \prod_{i=1}^{n}(y - y_i(0)) = y^n$$

Hence $y_i(0) = 0$, and so the conjugate y_i is a non unit in $k[[\underline{x}^{\frac{1}{n}}]]$ for all $1 \leq i \leq n$.
Conversely if y is a non-unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, and for every y_i conjugate of y we have $y - y_i = M_i\varepsilon_i$ for some monomial $M_i \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ and some unit ε_i, then for all $1 \leq j, k \leq n$ we will have $y_j - y_k = M_{jk}\varepsilon_{jk}$ for some M_{jk} monomial and ε_{jk} unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$. Take $f = \prod_i(y - y_i)$, then

$$\Delta(f) = \prod_{j\neq k}(y_j - y_k) = \prod_{j\neq k} M_{jk} \prod_{j\neq k} \varepsilon_{jk} = M.\varepsilon$$

where M is a monomial and ε is a unit, and so f is a quasi-ordinary polynomial.

From now on L denotes the fraction field of $\mathbb{K}[[\underline{x}]]$, and $L_n = L(x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}})$. It is well known that L_n is a Galois extension of L.

Proposition 13 *Let f be an irreducible quasi-ordinary polynomial in $\mathbb{K}[[\underline{x}]][y]$, and let y be one of its roots in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ with characteristic monomials $\{M_1, ..., M_h\}$. The field extensions $L(y)$ and $L(M_1, ..., M_h)$ coincide.*

Proof : Any automorphism of L_n over L that fixes y fixes all the monomials of y. In particular it fixes the characteristic monomials of y since they appear as terms in y, and so $L(M_1, ..., M_h) \subset L(y)$. On the other hand if an automorphism θ of L_n over L fixes all the characteristic monomials of y, then $\theta(y) = y$. Indeed if $\theta(y) - y \neq 0$, then $\theta(y) - y = \underline{x}^{\frac{m}{n}}.unit$ for some $m \in \mathbb{N}^e$, hence $\underline{x}^{\frac{m}{n}}$ is a characteristic monomial of y with $\theta(\underline{x}^{\frac{m}{n}}) \neq \underline{x}^{\frac{m}{n}}$ which contradicts our hypothesis. Hence $L(y) = L(M_1, ..., M_h)$.■

Lemma 4 *Let L be a field, and let α be an algebraic element over L. Then $L(\alpha) = L[\alpha]$.*

Proof : Since $L[\alpha] \subseteq L(\alpha)$ and $L(\alpha)$ is the smallest field containing α and L, it is enough to prove that $L[\alpha]$ is a field in order to deduce the equality.
Let f be the minimal polynomial of α over L, and suppose that $deg(f) = n$. Consider any nonzero polynomial $g \in L[x]$ with $deg(g) < n$. Since f is irreducible in $L[x]$, then f and g are coprime, and so there exists $h_1(x), h_2(x) \in L[x]$ such that $h_1(x)f(x) + h_2(x)g(x) = 1$, hence $h_2(\alpha)g(\alpha) = 1$, and so $g(\alpha)$ has a multiplicative inverse in $L[\alpha]$. If $deg(g) > n$, then dividing g by f we get $g = f.q + r$ for some $q, r \in L[x]$ with $deg(r) < n$. Obviously $g(\alpha) = r(\alpha)$, hence $g(\alpha)$ admits a multiplicative inverse in $L[\alpha]$, and so $L[\alpha]$ is a field. We finally get $L[\alpha] = L(\alpha)$. ■
More generally, let $\alpha_1, ..., \alpha_h$ be algebraic elements over L. By Lemma 4 we have $L(\alpha_1) = L[\alpha_1]$. Suppose that $L(\alpha_1, ..., \alpha_i) = L[\alpha_1, ..., \alpha_i]$ with $i < h$, then $L(\alpha_1, ..., \alpha_{i+1}) = L(\alpha_1, ..., \alpha_i)(\alpha_{i+1}) = L(\alpha_1, ..., \alpha_i)[\alpha_{i+1}] = L[\alpha_1, ..., \alpha_i][\alpha_{i+1}] = L[\alpha_1, ..., \alpha_{i+1}]$, and so $L(\alpha_1, ..., \alpha_h) = L[\alpha_1, ..., \alpha_h]$.

Proposition 14 *Let f be an irreducible quasi-ordinary polynomial with a root $y(\underline{x})$ as above, and a sequence of characteristic exponents $m_1, ..., m_h$ in $Supp(f)$ such that $m_1 < m_2 < \cdots < m_h$ coordinatewise. We have :*

(i) If $m \in Supp(f)$, then $m \in (n\mathbb{Z})^e + \sum_{i=1}^{h} m_i\mathbb{Z}$.

(ii) $m_i \notin (n\mathbb{Z})^e + \sum_{j<i} m_j\mathbb{Z}$ for all $i = 1, ..., h$.

Proof : Let $M = \underline{x}^{\frac{m}{n}}$ be a monomial of y with $m \in \mathbb{Z}^e$, where $y \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ is a root of f, then $M \in L(y)$, but $L(y) = L(M_1, ..., M_h) = L[M_1, ..., M_h]$. Hence $M = g(M_1, ..., M_h)$ for some $g = \frac{f_1}{g_1} M_1^{\alpha_1^1} ... M_h^{\alpha_h^1} + \cdots + \frac{f_l}{g_l} M_1^{\alpha_1^l} ... M_h^{\alpha_h^l}$, with $f_1, ..., f_l, g_1, ..., g_l \in \mathbb{K}[[\underline{x}]]$ and $l \in \mathbb{N}^*$, and so :

$$g_1 ... g_l M = f_1 g_2 ... g_l M_1^{\alpha_1^1} ... M_h^{\alpha_h^1} + \cdots + f_l g_1 ... g_{l-1} M_1^{\alpha_1^l} ... M_h^{\alpha_h^l}$$

Comparing both sides we can easily see that $M = \underline{x}^{\frac{m}{n}} = x_1^{a_1} \cdots x_e^{a_e} M_1^{p_1} \cdots M_h^{p_h}$ for some $a_1, ..., a_e, p_1, ..., p_h \in \mathbb{Z}$, hence $\frac{m}{n} \in \mathbb{Z}^e + \sum_{i=1}^{h} \frac{m_i}{n} \mathbb{Z}$, and obviously $m \in (n\mathbb{Z})^e + \sum_{i=1}^{h} m_i \mathbb{Z}$.

Now for the second part of the proposition, consider the characteristic monomial $M_i = \underline{x}^{\frac{m_i}{n}}$ of y, then by definition there exists an automorphism θ of L_n over L such that $y - \theta(y) = M_i \varepsilon_i$ with ε_i unit in $\mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$. Hence $\theta(M_j) = M_j$ for all $j = 1, ..., i-1$. On the other hand $\theta(M_i) \neq M_i$, thus M_i does not lie in $L(M_1, ..., M_{i-1})$, hence $m_i \notin (n\mathbb{Z})^e + \sum_{j<i} m_j \mathbb{Z}$. ■

Remark 2 *In general let $M_i = \underline{x}^{\frac{m_i}{n}}$ with $i = 1, ..., t$ be a set of monomials with fractional exponents, and $t \leq h$. Let $M = \underline{x}^{\frac{m}{n}}$ be an arbitrary monomial. Then $\underline{x}^{\frac{m}{n}}$ lies in $L(M_1, ..., M_t)$ if and only if $m \in (n\mathbb{Z})^e + \sum_{i=1}^{t} m_i \mathbb{Z}$.*

Let *glex* be the well-ordering on $\mathbb{N}^e$ defined as follows : $\underline{\alpha} <_{glex} \underline{\beta}$ if and only if $|\alpha| = \sum_{i=1}^{e} \alpha_i < |\beta| = \sum_{i=1}^{e} \beta_i$ or $|\alpha| = |\beta|$ and $\alpha <_{lex} \beta$(where *lex* denotes the lexicographical order).

Definition 17 *Let $u = \sum_p c_p \underline{x}^p$ in $\mathbb{K}[[\underline{x}]]$ be a non-zero formal power series. Let $u = u_d + u_{d+1} + ...$ be the decomposition of u into a sum of homogeneous components. We define the initial form of u to be $In(u) = u_d$.*

We set $O_x(u) = d$; this quantity is called the $\underline{x}$-order of u. We denote by $exp_{glex}(u)$ the smallest exponent of u with respect to *glex*. We denote by $inco_{glex}(u)$ the coefficient $c_{exp_{glex}}$, and we call it the initial coefficient of u. We finally set $M_{glex}(u) = inco_{glex}(u) \underline{x}^{exp_{glex}(u)}$, and we call it the initial monomial of u.

Remark 3 *Let $u(\underline{x})$ be a non-zero formal power series. Let $\prec$ be another well-ordering of $\mathbb{N}^e$. Define the leading exponent of u to be the leading exponent of $In(u)$ with respect to $\prec$. In this way we get a different notion of leading exponent (resp. initial coefficient, resp. initial monomial) of u.*

Let g be a non-zero element of $R[Y]$. The order of g with respect to f, denoted by $O_{glex}(f, g)$, is defined to be $exp_{glex}(g(x_1^n, ..., x_e^n, y(\underline{x}))$. Note that it is independent of the choice of the root $y(\underline{x})$ of $f(x_1^n, ..., x_e^n, y) = 0$. Indeed if y' is another root of f, then there exists some automorphism θ such that $\theta(y) = y'$. Hence $g(\underline{x}^n, y'(\underline{x})) = g(\underline{x}^n, \theta(y(\underline{x}))) = \theta(g(\underline{x}^n, y(\underline{x})))$, and so $g(\underline{x}^n, y'(\underline{x}))$ and $g(\underline{x}^n, y(\underline{x}))$ have the same support.

Definition 18 *The semigroup of f, denoted by $\Gamma(f)$, is the subsemigroup of $\mathbb{Z}^e$ defined by :*

$$\Gamma(f) = \{\ O_{glex}(f, g) |\ g \in \mathbb{K}[[\underline{x}]][y],\ g \notin (f)\ \}.$$

Proposition 15 *Let $n \in \mathbb{N}^*$ and let $Y(\underline{x}) = \sum_p c_p \underline{x}^{\frac{p}{n}} \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$, and suppose that there exists a finite sequence of elements $m_1, ..., m_h$, of $Supp(Y(\underline{x}))$ such that the following holds :*
(i) $m_1 < m_2 < ... < m_h$ componentwise.
(ii) If $p \in Supp(Y(\underline{x}))$, then $p \in (n\mathbb{Z})^e + \sum_{i=1}^{h} m_i \mathbb{Z}$.
(iii) $m_i \notin (n\mathbb{Z})^e + \sum_{j<i} m_j \mathbb{Z}$ for all $i = 1, ..., h$.
(iv) If $p \in Supp(Y)$ such that $p \in \mathbb{Z}^e + \sum_{i=1}^{j} m_i \mathbb{Z}$ and $p \notin \mathbb{Z}^e + \sum_{i=1}^{j-1} m_i \mathbb{Z}$ for some $j \in \{1, ..., h\}$ then $m_j \leq p$ coordinate wise.
Then $Y(\underline{x})$ is a quasi-ordinary branch.

Proof : For each $i = 1, ..., h$ define the set $G_i = M_i \backslash M_{i-1}$ and $G_0 = (n\mathbb{Z})^e \cap Supp(Y)$, and define for each $i = 0, ..., h$ the power series $H_i = \sum_{m \in G_i} c_m \underline{x}^{\frac{m}{n}}$, then $Y(\underline{x})$ can be written as $Y(\underline{x}) = H_0 + H_1 + ... + H_h$. If $m \in G_i$, then $m \in (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j\mathbb{Z}$ and $m \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j\mathbb{Z}$, hence by condition (iv) $m_i \leq m$, and so H_i can be written as $H_i = M_i\varepsilon_i$ with $M_i = \underline{x}^{\frac{m_i}{n}}$ and $\varepsilon_i(0) \neq 0$. Note that an automorphism θ of L_n over L fixes $H_0, ..., H_i$ if and only if it fixes the monomials $M_1, ..., M_i$. In fact if θ fixes H_j then it will obviously fix all monomials M of H_j, in particular it fixes M_j. On the other hand suppose that θ fixes all the monomials $M_1, ..., M_i$ and let $M = \underline{x}^{\frac{m}{n}}$ be a monomial of H_j for some $1 \leq j \leq i$, then $m \in G_j$, and it follows from Remark 2 that $M \in L(M_1, ..., M_j)$ but θ fixes $M_1, ..., M_j$ then it will fix M, hence H_j is fixed by θ. Now if θ is an automorphism that does not fix $y = H_0 + ... + H_h$, then θ does not fix all $H_1, ..., H_h$, and so there exists some $i \geq 0$ such that θ fixes $H_0, ..., H_i$ and does not fix H_{i+1}, hence $Y - \theta(Y) = M_{i+1}\varepsilon$ where $\varepsilon_i(0) \neq 0$. It follows from Remark 1 that Y is a quasi-ordinary branch. ■

2.3.3 Field extensions.

Lemma 5 *Let $m_1, ..., m_e, m$ be $(e+1)$ vectors in $\mathbb{Z}^e$, and let D be the determinant of the matrix $M = (m_1^t, ..., m_e^t)$ and D_i be the determinant of the matrix $M_i = (m_1^t, ..., m_{i-1}^t, m^t, m_{i+1}^t, ..., m_e^t)$ for all $i \in \{1, ..., e\}$. Then m can be written as $m = x_1m_1 + ... + x_em_e$ for some $x_1, ..., x_e \in \mathbb{Z}$ if and only if D divides D_i for all $1 \leq i \leq e$.*

Proof : Let X_i be the matrix obtained by replacing the $i-th$ column of the identity $(e \times e)$ matrix I_e by the vector x^t where $x = (x_1, ..., x_e)$, then we will have $M \cdot X_i = M_i$. Calculating the determinants we get $Det(M) \cdot Det(X_i) = Det(M_i)$, but the determinant of X_i is obviously x_i, hence $D \cdot x_i = D_i$, and so the equation $m = x_1m_1 + ... + x_em_e$ admits a solution if and only if $D \neq 0$, and the obtained solution will be $x_i = \frac{D_i}{D}$ for all $1 \leq i \leq e$. In particular $x_i \in \mathbb{Z}$ if and only if D divides D_i for all $1 \leq i \leq e$.■

Lemma 6 *Let M be a subgroup of $(n\mathbb{Z})^e$ generated by the elements $(B_1, ..., B_e)$. Consider another system of generators $\{v_1, ..., v_e\}$ of M. Then $Det(B_1^t, ..., B_e^t) = Det(v_1^t, ..., v_e^t)$.*

Proof : Consider the two matrices $V = (v_1^t, ..., v_e^t)$ and $B = (B_1^t, ..., B_e^t)$. For each of the e columns B_i^t of B, there exists a vector $x \in \mathbb{Z}^e$ such that $B_i^t = V \cdot x$, so there exists an $(e \times e)$ integer matrix U such that $B = V \cdot U$. Similarly, there exists an $(e \times e)$ integer matrix U' such that $V = B \cdot U'$, hence $B = V \cdot U = B(U' \cdot U)$, and so $B^TB = (U'U)^TB^TB(U'U)$ where B^T is the transpose of B.
Taking determinants, we get that $Det(B^TB) = (Det(U'U))^2Det(B^TB)$, and so $Det(U'U)^2 = 1$. Since U and U' are integer matrices, then $Det(U'U) = Det(U')Det(U) = \pm 1$, and so $Det(U) = \pm 1$. It follows that $Det(B) = Det(V)Det(U) = Det(V)$.■
We start with a technical Lemma :

Lemma 7 *Consider $M_0 = (n\mathbb{Z})^e$ with its canonical basis $A_1, ..., A_e$, let $A_{e+1} \in \mathbb{Z}^e$ be an arbitrary vector, and consider the group $M_1 = (n\mathbb{Z})^e + A_{e+1}\mathbb{Z}$. Then M_1 is a free group of rank e. Let D_1 be the GCD of the $(e \times e)$ minors of the matrix $A = (A_1, ..., A_e, A_{e+1})$, denoted by $GCDM(A_1, ..., A_e, A_{e+1})$ or $GCDM(A)$, and let D be the absolute value of the determinant of the matrix $(v_1, ..., v_e)$, where $v_1, ..., v_e$ is a basis of M_1. Then $D = D_1$.*

Proof : We have $(n\mathbb{Z})^e \subseteq M_1 \subseteq \mathbb{Z}^e$, but $\mathbb{Z}^e$ and $(n\mathbb{Z})^e$ are free abelian groups of rank e, then M_1 is a free abelian group of rank e. It is well known that a basis for M_1 is obtained by applying the following elementary operations on the columns of the matrix A :
(i) $A_i \leftarrow A_i + kA_j$, adding a multiple of a column to another column.
(ii) $A_i \leftrightarrow A_j$, interchanging two columns.
Each operation of the above will not affect the GCD of the minors of the obtained matrix, so at the end of the procedure we will obtain a matrix $C = (B_1, ..., B_e, \underline{0})$ where $B_1, ..., B_e$ is a basis of M_1 and $GCDM(A) = GCDM(C) = Det(B_1, ..., B_e)$, which is equal to D by Lemma 6.■

Definition 19 *Let f be a quasi-ordinary polynomial, and $m_1, ..., m_e$ be its set of characteristic exponents. Let $\underline{m}_0 = (m_0^1, ..., m_0^e)$ be the canonical basis of $(n\mathbb{Z}^e)$, and I_e the unit $e \times e$ matrix. The $\underline{D}-$sequence of f, $D_1, ..., D_{h+1}$, is defined to be the set of integers : $D_1 = n^e$, and D_{i+1} the gcd of the $e \times e$ minors of the matrix $(nI_e, m_1^T, ..., m_i^T)$.*

Proposition 16 *Let $M_i = (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j\mathbb{Z}$, and consider a nonzero vector v in $\mathbb{Z}^e$. Let $\tilde{D}$ be the gcd of the $e \times e$ minors of the matrix $(nI_e, m_1^T, ..., m_i^T, v^T)$. We have the following :*
(i) $v \in M_i$ if and only if $\tilde{D} = D_{i+1}$.
(ii) $\frac{D_{i+1}}{\tilde{D}}.v \in M_i$ and if $D_{i+1} > \tilde{D}$ then for all $1 \leq k < \frac{D_{i+1}}{\tilde{D}}, k.v \notin M_i$.

Proof : Let $v_1, ..., v_e$ be a basis of M_i, then obviously :

$$v \in M_i \text{ if and only if } v = \alpha_1 v_1 + ... + \alpha_e v_e, \text{ where } \alpha_i \in \mathbb{Z} \ \forall \ i = 1, ..., e.$$

Now let $D'_1, (D'_2, ..., D'_e)$ be the determinant of the matrix $(v, v_2, ..., v_e)((v_1, v, ..., v_e), ..., (v_1, ..., v_{e-1}, v))$ respectively, and D the determinant of the matrix $(v_1, ..., v_e)$. It follows from Lemma 7 that $D = D_{i+1}$, and that $\tilde{D}$ is equal to the GCD of the minors of the matrix $(v_1, ..., v_e, v)$.
By Proposition 5 we have : $v = \alpha_1 v_1 + ... + \alpha_e v_e$ if and only if D divides D'_k for all $1 \leq k \leq e$, if and only if D_{i+1} divides D'_k for all $1 \leq k \leq e$ which is equivalent to say $\tilde{D} = GCD(D_{i+1}, D'_1, ..., D'_e) = D_{i+1}$.
Concerning part (ii), let $1 \leq k \leq \frac{D_{i+1}}{\tilde{D}}$, and consider the vector $k.v$. Let A be the matrix $(v_1, ..., v_e, (k.v))$. The determinant of the minors of this matrix are clearly $k.D'_1, ..., k.D'_e, D_{i+1}$.Let $\bar{D}$ to be the GCD of the minors of the matrix A. If $k = \frac{D_{i+1}}{\tilde{D}}$, then :

$$\bar{D} = GCD(D_{i+1}\frac{D'_1}{\tilde{D}}, ..., D_{i+1}\frac{D'_e}{\tilde{D}}, D_{i+1}) = D_{i+1}GCD(\frac{D'_1}{\tilde{D}}, ..., \frac{D'_e}{\tilde{D}}, 1) = D_{i+1}$$

and so we can conclude that $k.v \in M_i$ from the first part. Now suppose that $D_{i+1} > \tilde{D}$, and let $1 \leq k < \frac{D_{i+1}}{\tilde{D}}$. If $k.v \in M_i$, then from part (i) we can conclude that $\bar{D} = D_{i+1}$, then D_{i+1} divides $kD'_1, ..., kD'_e, D_{i+1}$, hence it divides $k.D'_1, ..., k.D'_e, k.D_{i+1}$ and consequently divides $GCD(kD'_1, ..., kD'_e, kD_{i+1})$ but $GCD(kD'_1, ..., kD'_e, kD_{i+1}) = k.GCD(D'_1, ..., D'_e, D_{i+1}) = k.\tilde{D}$, which is a contradiction since $k.\tilde{D} < D_{i+1}$ by assumption.■
Now define the sequence $(e_i)_{1 \leq i \leq h}$ to be $e_i = \frac{D_i}{D_{i+1}}$ for all $1 \leq i \leq h$, which is called the $\underline{e}-$sequence associated with f. Let $M_0 = (n\mathbb{Z})^e$ and $M_i = (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j\mathbb{Z}$ for all $1 \leq i \leq h$, where $m_1, ..., m_h$ are the characteristic monomials of f, then $M_0 \subset M_1 \subset \cdots \subset M_h \subset \mathbb{Z}^e$ are free abelian subgroups of rank e for all $1 \leq i \leq h$.

Remark 4 *We have $m_{i+1} \notin M_i$, then by Proposition 16 we deduce that $D_{i+2} > D_{i+1}$, $e_{i+1}m_{i+1} \in M_i$, and $km_{i+1} \notin M_i$ for all $1 \leq k < e_{i+1}$.*

Let $F_0 = K((\underline{x}))$ and let $F_k = F_{k-1}(\underline{x}^{\frac{m_k}{n}})$ for all $k = 1, ..., h$. Obviously we have

$$F_0 \subset F_1 \subset ... \subset F_0(\underline{x}^{\frac{m_1}{n}}, ..., \underline{x}^{\frac{m_h}{n}}) = F_h.$$

Lemma 8 *For all $i = 1, ..., k$ the minimal polynomial of $\underline{x}^{\frac{m_k}{n}}$ over F_{k-1} is equal to $h_k = y^{e_k} - \underline{x}^{e_k\frac{m_k}{n}}$.*

Proof : The polynomial h_k belongs to $F_{k-1}[y]$, since $e_k m_k \in (n\mathbb{Z})^e + m_1\mathbb{Z} + \cdots m_{k-1}\mathbb{Z}$. obviously $h_k(\underline{x}^{\frac{m_k}{n}}) = 0$. Suppose to the contrary that h_k is not the minimal polynomial of $\underline{x}^{\frac{m_k}{n}}$. Then there exists some monic polynomial $f \in F_{k-1}[y]$ of degree $\alpha < e_k$ such that $f(\underline{x}^{\frac{m_k}{n}}) = 0$. Write $f = y^\alpha + a_{\alpha-1}y^{\alpha-1} + \cdots + a_0$ where $a_i \in F_{k-1}$ for all $i = 0, ..., \alpha - 1$. We have $f(\underline{x}^{\frac{m_k}{n}}) = 0$, and so :

$$\underline{x}^{\alpha\frac{m_k}{n}} + a_{\alpha-1}\underline{x}^{(\alpha-1)\frac{m_k}{n}} + \cdots + a_1\underline{x}^{\frac{m_k}{n}} + a_0 = 0$$

Hence there exists some $i \in \{0, ..., \alpha - 1\}$ such that one of the monomials of $a_i\underline{x}^{i\frac{m_k}{n}}$ is equal to $\underline{x}^{\alpha\frac{m_k}{n}}$. Let $\underline{x}^{\frac{a}{n}}$ be such monomial. Then $a = b + im_k$ for some $b \in \mathbb{Z}^e + \sum_{j=1}^{k-1} m_j\mathbb{Z}$, and so $\alpha m_k = b + im_k$, hence $(\alpha - i)m_k = b \in \mathbb{Z}^e + \sum_{j=1}^{k-1} m_j\mathbb{Z}$. But $0 < \alpha - i < e_i$, which is a contradiction.■

Proposition 17 *Let the notation be as above. We have the following :*
(i) For all $k = 1, ..., h$, F_k is an algebraic extension of degree e_k of F_{k-1}.
(ii) For all $k = 1, ..., h$, F_k is an algebraic extension of degree $e_k.e_{k-1}...e_1$ of F_0.
(iii) $n = deg_y(f) = e_1...e_h = \frac{D_1}{D_{h+1}} = \frac{n^e}{D_{h+1}}$. In particular $D_{h+1} = n^{e-1}$.

Proof : (i) By Lemma 8 we have that for all $1 \leq k \leq h$, the polynomial $h_k = y^{e_k} - \underline{x}^{e_k \frac{m_k}{n}}$ is the minimal polynomial of $\underline{x}^{\frac{m_k}{n}}$ over F_{k-1}, which is a polynomial of degree e_k. Hence F_k is an algebraic extension of degree e_k of F_{k-1}.
(ii) It follows from part (i) that F_k is an algebraic extension of F_{k-1} of degree e_k for all $1 \leq k \leq h$, and so F_k is an algebraic extension of F_0 of degree $e_k...e_1$.
(iii) By Proposition 13, we have $F_h = F_0(y)$, but $[F_0(y); F_0] = deg(f) = n$, then $[F_h, F_0] = n$. By part (ii) we have that F_h is an algebraic extension of degree $e_h...e_1$ of F_0, and so $n = deg_y(f) = e_1...e_h = \frac{D_1}{D_2} \cdots \frac{D_h}{D_{h+1}} = \frac{D_1}{D_{h+1}} = \frac{n^e}{D_{h+1}}$. It follows that $D_{h+1} = n^{e-1}$.■

2.3.4 Semi-roots and approximate roots of a quasi-ordinary polynomial.

Let f, g be two non zero polynomials, of degrees n, m respectively, in $\mathbb{K}[[\underline{x}]][y]$ such that $f.g$ is a quasi-ordinary polynomial. Then $\Delta_y(f.g) = \underline{x}^{\lambda}.\epsilon$ for some ϵ unit in $\mathbb{K}[[\underline{x}]]$. It follows that f and g are quasi ordinary polynomials. Let $\{y_i\}_{i=1,...,n}$ and $\{z_j\}_{j=1,...,m}$ be the roots of f and g respectively. Then by Proposition 11 for all $i = 1, ..., n$ and $j = 1, ..., m$ we have $y_i - z_j = \underline{x}^{\lambda_{ij}} \varepsilon_{ij}$ where ε_{ij} is a unit. Moreover the exponents λ_{ij} are ordered with respect to the component-wise order. In this case we say that f and g are comparable. This leads to the following definition.

Definition 20 *Let f and g be two comparable polynomials with $\{\lambda_{ij}\}_{i=1,...,n}^{j=1,...,m}$ as above. The order of coincidence of f and g is defined to be the largest element λ_{ij} where $i \in \{1, ..., n\}$ and $j \in \{1, ..., m\}$ with respect to the component-wise order.*

We define the sequence $(d_1, d_2, ..., d_{h+1})$ by $d_i = \frac{D_i}{D_{h+1}}$, in particular $d_1 = n$ and $d_{h+1} = 1$. This sequence is called the $\underline{d}-$sequence associated with f. Let $(r_0^1, ..., r_0^e) = (m_0^1, ..., m_0^e)$ be the canonical basis of $(n\mathbb{Z})^e$ and define the sequence $(r_k)_{1 \leq k \leq h}$ by $r_1 = m_1$ and :

$$r_{k+1} = e_k r_k + m_{k+1} - m_k$$

For all $1 \leq k \leq h-1$. We call $(r_0^1, ..., r_0^e, r_1, ..., r_h)$ the $\underline{r}-$sequence associated with f.

Remark 5 *Each of the sequences $(m_k)_{1 \leq k \leq h}$ and $(r_k)_{1 \leq k \leq h}$ determines the other. More precisely $m_1 = r_1$ and $r_k d_k = m_1 d_1 + \sum_{j=2}^{k} (m_j - m_{j-1}) d_j$ (resp $m_k = r_k - \sum_{j=1}^{k-1} (e_j - 1) r_j$) for all $2 \leq k \leq h$. Hence we have $M_k = (n\mathbb{Z})^e + \sum_{j=1}^{k} m_j \mathbb{Z} = (n\mathbb{Z})^e + \sum_{j=1}^{k} r_j \mathbb{Z}$ and $e_k r_k \in (n\mathbb{Z})^e + \sum_{j=1}^{k-1} r_j \mathbb{Z}$ for all $k = 1, ..., h$.*

Definition 21 *Let y be a quasi-ordinary branch, and let $(r_0^1, ..., r_0^e, r_1, ..., r_h)$ be the $\underline{r}$-sequence associated to y. The semigroup of y is defined to be $(n\mathbb{N})^e + \sum_{i=1}^{h} r_i \mathbb{N}$, and denoted by Γ_y.*

From now on we denote by $\Gamma_0 = (n\mathbb{N})^e$ and $\Gamma_j = (n\mathbb{N})^e + \sum_{i=1}^{j} r_i \mathbb{N}$ for all $j = 1, ..., h$.

Lemma 9 *Let the notation be as above. Then we have the following :*
(1) $e_i r_i < r_{i+1}$ for all $i = 1, ..., h-1$ (where $<$ means $\leq$ component wise but not equal).
(2) For all $i \in \{1, ..., h\}$. If $u \in M_j \cap \mathbb{N}^e$, then $u + e_j r_j \in \Gamma_j$.
(3) $e_{i+1} r_{i+1} \in \Gamma_i$ for all $i = 1, ..., h-1$, that is Γ_y is a free affine semigroup.

Proof : (1) We have $r_{j+1} = e_j r_j + (m_{j+1} - m_j)$. Then

$$\begin{aligned} e_{j+1}r_{j+1} - e_j r_j &= e_{j+1}e_j r_j + e_{j+1}(m_{j+1} - m_j) - e_j r_j \\ &= e_j(e_{j+1} - 1)r_j + e_{j+1}(m_{j+1} - m_j) \\ &> (e_{j+1} - 1)(e_j r_j + m_{j+1} - m_j) \\ &= (e_{j+1} - 1)r_{j+1} \end{aligned}$$

It follows that $e_j r_j < r_{j+1}$.
(2) For $i = 1$, it is obvious. Suppose that it is true up to $j-1$ and let $u \in M_j \cap \mathbb{N}^e$. Then u can be written in a unique way as $u = \alpha r_j + u'$ with $0 \leq \alpha < e_j$ and $u' \in M_{j-1}$. Let $v = u' + e_j r_j - e_{j-1}r_{j-1}$. since $e_j r_j \in M_{j-1}$, then $v \in M_{j-1}$. On the other hand $e_j r_j - e_{j-1}r_{j-1} > (e_j - 1)r_j \geq \alpha r_j$ component wise, and so $e_j r_j - e_{j-1}r_{j-1} = \alpha r_j + \omega$ for some $\omega \in \mathbb{N}^e$, then $v = u' + e_j r_j - e_{j-1}r_{j-1} = u' + \alpha r_j + \omega = u + \omega \in \mathbb{N}^e$, hence $v \in M_{j-1} \cap \mathbb{N}^e$, then by the induction hypothesis $v + e_{j-1}r_{j-1} = u' + e_j r_j \in \Gamma_{j-1}$. But $u + e_j r_j = \alpha r_j + (u' + e_j r_j)$, and so it belongs to Γ_j.
(3) For all $i = 1, ..., h-1$ we have $e_{i+1}r_{i+1} = e_{i+1}e_i r_i + e_{i+1}(m_{i+1} - m_i)$. But $m_{i+1} - m_i \in \mathbb{N}^e$ since $m_i \leq m_{i+1}$ coordinate wise, and $e_{i+1}m_{i+1} \in M_i$, then $e_{i+1}(m_{i+1} - m_i) \in M_i \cap \mathbb{N}^e$. Hence by part (2) we get $e_i r_i + e_{i+1}(m_{i+1} - m_i) \in \Gamma_i$, whence $e_{i+1}r_{i+1} \in \Gamma_i$.■
Let $d_1, ..., d_{h+1}$ be the $\underline{d}$ sequence associated to y. Note that for all $i = 1, ..., h$ we have $e_i = \frac{d_i}{d_{i+1}}$, and so $d_i = d_{i+1}e_i = ... = d_{h+1}e_h...e_i = e_i...e_h$. Hence $\frac{n}{d_i} = \frac{e_1...e_h}{e_i...e_h} = e_1...e_{i-1}$.

Definition 22 *Let the notation be as above, and let $i \in \{1, ..., h\}$. A polynomial $g \in \mathbb{K}[[\underline{x}]][y]$ is said to be an $i-th$ semi-root of f if $deg_y(g) = \frac{n}{d_i}$ and $g(\underline{x}^n, y) = \underline{x}^{r_i}\varepsilon$ for some ε unit in $\mathbb{K}[[\underline{x}]]$.*

Remark 6 *Let $\sigma = \langle a^1, ..., a^e \rangle$ be a cone in $\mathbb{R}^e_{\geq 0}$ with $a^i = (a^i_1, ..., a^i_e) \in \mathbb{N}^e$ for each $i = 1, ..., e$. This cone defines a homomorphism of rings $\psi :\ \mathbb{K}[[x_1, ..., x_e]] \mapsto \mathbb{K}[[t_1, ..., t_e]]$ defined by :*

$$\begin{aligned} x_1 &\mapsto t_1^{a_1^1} \cdots t_e^{a_1^e} \\ x_2 &\mapsto t_1^{a_2^1} \cdots t_e^{a_2^e} \\ &\cdots \\ x_1 &\mapsto t_1^{a_e^1} \cdots t_e^{a_e^e} \end{aligned}$$

Let $M = x_1^{\alpha_1} \cdots x_e^{\alpha_e} = \underline{x}^{\alpha}$ be a monomial, then $\psi(M) = t_1^{\beta_1} \cdots t_e^{\beta_e}$ is a monomial, with $(\beta_1, ..., \beta_e) = (< a^1, \alpha >, ..., < a^e, \alpha >)$ and denoted by $\psi(\alpha)$, where $< a, b >$ is the dot product of two vectors in $\mathbb{R}^e$. Also ψ extends to a homomorphism from $\mathbb{K}[[\underline{x}]][y]$ to $\mathbb{K}[[\underline{t}]][y]$, by sending each $g = a_n y^n + \cdots + a_1 y + a_0$ in $\mathbb{K}[[\underline{x}]][y]$ to $\psi(g) = \psi(a_n)y^n + \cdots + \psi(a_1)y + \psi(a_0)$ in $\mathbb{K}[[\underline{t}]][y]$. It is easy to see that ψ sends a unit to another unit.

Lemma 10 *Let $f \in \mathbb{K}[[\underline{x}]][y]$ be an irreducible quasi-ordinary polynomial of degree n and let $\{m_1, ..., m_h\}$ be its set of characteristic exponents. Then $\psi(f)$ is an irreducible quasi-ordinary polynomial in $\mathbb{K}[[\underline{t}]][y]$ and $\{\psi(m_i)\}_{i=1,...,h}$ is its set of characteristic exponents.*

Proof : Since f is a quasi-ordinary polynomial then $\Delta_y(f) = \underline{x}^m.unit$. But $\Delta_y(\psi(f)) = \psi(\Delta_y(f))$, then $\Delta_y(\psi(f)) = \psi(\underline{x}^m).unit$, hence $\psi(f)$ is a quasi-ordinary polynomial. Let $\{y_1, ..., y_n\}$ be the roots of f, then $\{\psi(y_1), ..., \psi(y_n)\}$ are the roots of $\psi(f)$. By definition the characteristic exponents of $\psi(f)$ are obtained by taking the difference of its roots. In particular $\psi(y_i) - \psi(y_j) = \psi(y_i - y_j) = \psi(\underline{x}^{m_i}.unit) = \psi(\underline{x}^{m_{ij}}).unit = \underline{x}^{\psi(m_{ij})}.unit$ where m_{ij} is a characteristic exponent of f. Then the characteristic exponents of $\psi(f)$ are the images of the characteristic exponents of f by ψ.■

Remark 7 *we can rewrite the $\underline{r}$ sequence of f as :*

$$\begin{aligned} r_k &= m_k + (e_{k-1} - 1)m_{k-1} + (e_{k-2} - 1)e_{k-1}m_{k-2} + ... + (e_1 - 1)e_2...e_{k-1}m_1 \\ &= n\frac{m_k}{n} + n(e_{k-1} - 1)\frac{m_{k-1}}{n} + n(e_{k-2} - 1)e_{k-1}\frac{m_{k-2}}{n} + ... + n(e_1 - 1)e_2...e_{k-1}\frac{m_1}{n} \\ &= e_1...e_{k-1}[e_k...e_h\frac{m_k}{n} + e_k...e_h(e_{k-1} - 1)\frac{m_{k-1}}{n} + \cdots + e_k...e_h(e_1e_2...e_{k-1} - e_2...e_{k-1})\frac{m_1}{n}] \\ &= e_1...e_{k-1}[d_k\frac{m_k}{n} + (d_{k-1} - d_k)\frac{m_{k-1}}{n} + \cdots + (d_1 - d_2)\frac{m_1}{n}] \end{aligned}$$

for all $k = 1, ..., h$.

Definition 23 *Let $y = \sum c_p \underline{x}^p$ be a formal power series in $\mathbb{K}[[\underline{x}]]$. The Newton polyhedron of y is defined as the convex hull of the set $H = \bigcup_{p \in Supp(y)} (p + \mathbb{N}^e)$, that is the smallest convex subset of $\mathbb{R}^e$ containing H, and it is denoted by $N(y)$.*

Let f be a quasi-ordinary polynomial, and let $g \in \mathbb{K}[[\underline{x}]][y]$. If y_1, y_2 are two roots of f, then $supp(y_1) = supp(y_2)$. Consequently $N(g(\underline{x}, y_1)) = N(g(\underline{x}, y_2))$. Moreover if g is quasi-ordinary of degree m, and $\{z_1 = z, z_2, ..., z_m\}$ are its roots. Then :

$$N(\prod_{i=1}^{n} g(\underline{x}, y_i)) = deg(f) N(g(\underline{x}, y)) = N(\prod_{j=1}^{m} (f(\underline{x}, z_j))) = deg(g) N(f(\underline{x}, z)) = N(Res_y(f, g)) \tag{2.1}$$

Proposition 18 *Let g be an irreducible quasi-ordinary polynomial in $\mathbb{K}[[\underline{x}]][y]$ of degree $m = \frac{n}{d_i} (i \in \{1, ..., h\})$. Then g is an $i-$th semi root of f if and only if the order of coincidence between f and g is equal to $\frac{m_i}{n}$.*

Proof : Let $\{z_1, ..., z_m\}$ be the roots of g. We have $g(\underline{x}, Z) = \prod_{j=1}^{m} (Z - z_j)$. Now suppose that g is an i-th semi root, then by definition we have $g(\underline{x}, y(\underline{x})) = \underline{x}^{r_i} \varepsilon$ for some unit ε. Since $N(\prod_{i=1}^{n} g(\underline{x}, y_i(\underline{x}))) = deg(f) N(g(\underline{x}, y(\underline{x})))$ and $g(\underline{x}, y(\underline{x})) = \prod_{j=1}^{m} (y(\underline{x}) - z_j)$, then $y_i(\underline{x}) - z_j(\underline{x}) = \underline{x}^{\alpha_{ij}} \varepsilon_{ij}$ for some unit ε_{ij}, for all $i = 1, ..., n$ and $j = 1, ..., m$. Hence the order of coincidence between f and g is defined. Let α be the order of coincidence between f and g, and suppose without loss of generality that $y(\underline{x}) - z(\underline{x}) = \underline{x}^{\alpha} \omega$ for some unit ω. Remember that $\{m_1, ..., m_h, \alpha\}$ is an ordered set with respect to the component wise order because $f.g$ is quasi ordinary. Now let m_k be the greatest characteristic exponent of z which is smaller than α (which is also a characteristic exponent of y). For all $r = 1, ..., h$ we have $y_r(\underline{x}) - z(\underline{x}) = (y_r(\underline{x}) - y(\underline{x})) + (y(\underline{x}) - z(\underline{x}))$, and so $y_r(\underline{x}) - z(\underline{x}) = \underline{x}^{\alpha}.unit$ if and only if $y_r(\underline{x}) - y(\underline{x}) = \underline{x}^{\frac{m_j}{n}} \cdot (unit)$ for some $j > k$, that is y_j is the image of y by some automorphism of $L(y)$ over L that fixes $\underline{x}^{\frac{m_1}{n}}, ..., \underline{x}^{\frac{m_k}{n}}$. The number of roots satisfying this property is equal to $[L(y) : L(\underline{x}^{\frac{m_1}{n}}, ..., \underline{x}^{\frac{m_k}{n}})]$ which is equal to $e_{k+1}...e_h = d_{k+1}$. Moreover for all $j = 1, ..., k$ we have :

$$\begin{aligned}
\#\{y_j,\ y_j - z = \underline{x}^{\frac{m_j}{n}}.unit\} &= \#\{y_j,\ y_j - y = \underline{x}^{\frac{m_j}{n}}.unit\} \\
&= [L(y) : L(\underline{x}^{\frac{m_1}{n}}, ..., \underline{x}^{\frac{m_{j-1}}{n}})] - [L(y) : L(\underline{x}^{\frac{m_1}{n}}, ..., \underline{x}^{\frac{m_j}{n}})] \\
&= e_j...e_h - e_{j+1}...e_h \\
&= d_j - d_{j+1}.
\end{aligned}$$

Since g_i is an $i-$th semi-root, by equation (2.1) and similary to Remark 7 we get

$$r_i = e_1...e_{i-1}[(d_1 - d_2)\frac{m_1}{n} + \cdots + (d_k - d_{k+1})\frac{m_k}{n} + d_{k+1}\alpha] \tag{2.2}$$

If $k+1 > i$, then from Remark 7 we get $r_i > r_i$, which is a contradiction and so $k+1 \leq i$. If $k+1 < i$ or $\alpha \leq$ all the characteristic exponents of z, we deduce that $\alpha \geq \frac{m_i}{n}$, and so $\frac{m_{i-1}}{n} < \alpha$ and $\frac{m_{i-1}}{n}$ is a characteristic exponent of z, which is a contradiction. Hence $k+1 = i$, and so by Remark 7 we easily deduce that $\alpha = \frac{m_i}{n}$. Conversely if the order of coincidence between f and g is equal to $\frac{m_i}{n}$, then it follows easily from equation (2.2) that g is an i-th semi root of f.■
In what follows we will prove that every $j-$th semi-root of f is irreducible.

Definition 24 *Let $y \in \mathbb{K}[[\underline{x}]]$ and let $N(y)$ be its Newton polyhedron. The Newton initial polynomial of y is defined to be the sum of the terms of y lying on the compact faces of $N(y)$, and is denoted by $in_N(y)$.*

Recall that Γ_j represents the semigroup generated by $(r_0^1, ..., r_0^e, r_1, ..., r_j)$. Let $\mathbb{K}[\Gamma_j]$ be the ring of polynomials $f = \sum_p c_p \underline{x}^p$, with $supp(f)$ a finite subset of Γ_j.

Proposition 19 *Let the notations as before. Let g be a polynomial in $\mathbb{K}[[\underline{x}]][y]$. If $deg(g) = 0$, then $in(g(\underline{x}^n, y)) \in \mathbb{K}[\Gamma_0]$. Otherwise for all $j = 1, ..., h$ if $deg(g) < e_1...e_j = \frac{n}{d_{j+1}}$, then $in(g(\underline{x}^n, y)) \in \mathbb{K}[\Gamma_j]$.*

Proof : If $deg(g) = 0$, then $g = a(\underline{x})$ for some $a(\underline{x}) \in \mathbb{K}[[\underline{x}]]$, and so $g(\underline{x}, y) = a(\underline{x})$, then obviously $in(g(\underline{x}, y)) \in \mathbb{K}[\Gamma_0]$. Suppose that the assumption is true for polynomials of degrees $< e_1...e_{j-1}$ and let g be a polynomial of degree $< e_1...e_j$. Consider g_j to be a $j-$th semi-root of f, and let

$$g = a_0 + a_1 g_j + \cdots + a_{d_j} g_j^{dj}$$

be the g_j-adic expansion of g. where $a_i \in \mathbb{K}[[\underline{x}]][y]$ and $deg(a_i) < \frac{n}{d_j} = e_1...e_{j-1}$ for all $i = 0, ..., d_j$. By induction hypothesis we have $in(a_i(\underline{x}, y)) \in \mathbb{K}[\Gamma_{j-1}]$ for all $i = 0, ..., d_j$. Since terms of the polynomials $a_l \underline{x}^{lr_i}$ and $a_k \underline{x}^{kr_i}$ can not cancel each other for all $0 \leq l \neq k \leq d_j$, then the terms of the polynomial $in(g)$ are terms of the polynomials $a_l \underline{x}^{lr_j}$, $j = 0, ..., d_j$. Hence $in(g) \in \mathbb{K}[\Gamma_j]$.■

Proposition 20 *Let f be a quasi-ordinary polynomial and let $g \in \mathbb{K}[[\underline{x}]][y]$ be an $i-$th semi root of f. Then g is an irreducible polynomial.*

Proof : suppose to the contrary that g is not irreducible then there exists $g_1, g_2 \in \mathbb{K}[[\underline{x}]][y]$ such that $g = g_1.g_2$ with $deg(g_j) < \frac{n}{d_i}$ for $j = 1, 2$. By Proposition 19 we have $in(g_j) \in \mathbb{K}[\Gamma_{i-1}]$ for $j = 1, 2$. But r_i is an exponent in the polynomial $in(g_1) + in(g_2)$, then $r_i \in \mathbb{K}[\Gamma_{i-1}]$. This is a contradiction.■

Lemma 11 *Let the notation be as above with f a quasi-ordinary polynomial. Then for all $i = 1, ..., h$, f admits an i-th semiroot.*

Proof : Let y be a root of f, and write $y = H_0 + H_1 + \cdots + H_h$ as in Proposition 15. For each $i = 1, ...h$, let g_{i+1} be the minimal polynomial of $H_0 + \cdots + H_i$. Then g_i is a quasi-ordinary polynomial with characteristic exponents $\{m_1, ..., m_i\}$, and it is obviously irreducible. We have $deg(g_i) = [L(M_1, ..., M_i) : L] = e_1...e_i = \frac{n}{d_{i+1}}$. Obviously the order of coincidence between f and g_{i+1} is equal to $\frac{m_{i+1}}{n}$, then by Proposition 18 g_{i+1} is an $(i+1)$-st semi-root of f.■

Proposition 21 *Let the notation be as above with f an irreducible quasi-ordinary polynomial. For each $i = 1, ..., h+1$ let $g_i = App_{d_i}(f)$ be the d_i-th approximate root of f. Then g_i is an $i-th$ semi root of f.*

Proof : For $i = h+1$, $g_i = App_{d_{h+1}}(f) = f$ and so the assumption is true since $f(\underline{x}^n, y) = 0$ and $r_{h+1} = \infty$. Suppose that the assumption is true for $i+1$ and let us prove it for i. We have $App_{d_i}(f) = App_{e_i}(App_{d_{i+1}}(f))$. Let g be a polynomial of degree $\frac{n}{d_i}$, then by Proposition 6, we have $App_{d_i}(f) = \tau_{g_{i+1}}^{\frac{n}{d_i}}(g)$, where τ represents the Tschirnhausen transform. In order to prove that g_i is an $i-th$ semi-root, it is enough to prove that if g is an $i-$th semi-root then $\tau_{g_{i+1}}(g)$ is an i-th semi-root. Now suppose that g is an i-th semi-root, and let

$$g_{i+1} = g^{e_i} + a_1 g^{e_i - 1} + \cdots + a_{e_i}$$

be the g-adic expansion of g_{i+1} with $a_i \in \mathbb{K}[[\underline{x}]][y]$ and $deg(a_i) < deg(g)$ for all $i = 1, ..., e_i$. By the induction hypothesis we have $g_{i+1}(\underline{x}^n, y) = \underline{x}^{r_{i+1}}.unit$. It follows that

$$N(a_1(\underline{x}^n, y) g^{e_i - 1}(\underline{x}^n, y) \subseteq N(g_{i+1}(\underline{x}^n, y))$$

But g is an $i-$th semi-root of f, and so $g(\underline{x}^n, y) = \underline{x}^{r_i}.unit$. Hence if m is an exponent of $in(a_1(\underline{x}^n, y))$, then $m + (e_i - 1)r_i \in N(g_{i+1}(\underline{x}^n, y))$, and so $m + (e_i - 1)r_i \geq r_{i+1}$. Finally we get that $m \geq r_{i+1} - (e_i - 1)r_i > r_i$. Hence $\tau_{g_{i+1}} g(\underline{x}^n, y) = g(\underline{x}^n, y) + \frac{1}{e_i} a_1(\underline{x}^n, y) = \underline{x}^{r_i}.unit$, that is $\tau_{g_{i+1}}(g)$ is an i-th semi root.■

Proposition 22 *Let the notation be as above with f an irreducible quasi-ordinary polynomial. Let g be an $i-$th semi-root of f with $i \in \{1, ..., h\}$. Then g is a quasi-ordinary polynomial.*

Proof : Let $\Delta_Y(g)$ be the discriminant of g, and let $N(\Delta_y(g))$ be its newton polyhedron. Let $\sigma = \langle a^1, ..., a^e \rangle$ be a regular cone such that $\sigma \subseteq \mathbb{R}^e_{\geq 0}$ and σ is compatible with $\mathbb{N}(\Delta_y(g))$. That is there exists a unique $\omega \in N(\Delta_y(g))$ such that :

$$\langle a^i, \omega \rangle = \inf_{v \in N(\Delta_y(g))} \langle a^i, v \rangle.$$

for all $i \in \{1, ..., e\}$. Now let the notations be as in Remark 6, then the discriminant of $\psi(g)$ is $\psi(\Delta_y(g))$. Moreover if $\underline{x}^v = x_1^{v_1} \dots x_e^{v_e}$ is a monomial of $\Delta_y(g)$ for some $v \in \mathbb{N}^e$, then $\psi(\underline{x}^v) = x_1^{<a^1,v>} \dots x_e^{<a^e,v>}$ is a monomial of $\psi(\Delta_y(g))$. Furthermore, $\psi(\underline{x}^\omega) = x_1^{<a^1,\omega>} \dots x_e^{<a^e,\omega>}$, but $\langle a^i, \omega\rangle \leq \langle a^i, v\rangle$ for all $i \in \{1, ..., e\}$. It follows that the discriminant $\psi(\Delta_y(g))$ of $\psi(g)$ is of the form

$$\psi(\Delta_y(g)) = \underline{x}^{\psi(\omega)}.unit.$$

It follows that $\psi(g)$ is a quasi-ordinary polynomial. Since f is a quasi-ordinary irreducible polynomial, then by Lemma 10 we get that $\psi(f)$ is a quasi-ordinary irreducible polynomial. Moreover, the set of characteristic exponents of $\psi(f)$ is $\{\psi(m_1), ..., \psi(m_h)\}$. Since $\psi(g)$ is the the $i-$th semi root of $\psi(f)$, then by Proposition 20 we get that $\psi(g)$ is irreducible, and by Proposition 18 we get that the order of coincidence between $\psi(f)$ and $\psi(g)$ is $\psi(m_i)$. Now since $\psi(g)$ is an irreducible quasi-ordinary polynomial, it admits some root $z(\underline{x})$ and its set of characteristic exponents is equal to $\{\psi(m_1), ..., \psi(m_{i-1})\}$.
It follows that the element ω does not depend on the chosen cone σ since it is determined by the characteristic exponents $m_1, ..., m_{i-1}$ of f. Hence $N(\Delta_y(g))$ has a unique vertex. Thus g is a quasi-ordinary polynomial.■

Proposition 23 *Let the notation be as above with f an irreducible quasi-ordinary polynomial. Let g be an approximate root of f. Then g is an irreducible quasi-ordinary polynomial.*

Proof : Since g is an approximate root of f, then by Proposition 21 we get that g is a semi root of f. It follows from Proposition 20 and Proposition 22 that g is an irreducible quasi-ordinary polynomial.■

2.4 Free polynomials

In this section we generalize the results of section 4 to a free polynomial (see Definition 29). We also show that we can generalize Abhyankar-Moh theory to such a polynomial.

2.4.1 Line Free Cones.

The material of this subsection can be found in [24].
In this subsection we will consider the set of formal power series with exponents in some line free cone C with a non-empty interior, denoted by $\mathbb{K}_C[[\underline{x}]]$, and we will prove that this set is a ring. Also we will prove that we can find some order on $C \cap \mathbb{Z}^e$ such that for each element $y \in \mathbb{K}_C[[\underline{x}]]$, the exponents of y can be written in increasing order.

Definition 25 *Let C be a cone, then C is said to be a line-free cone if $\forall v \in C - \{0\}$ we have $-v \notin C$.*

Lemma 12 ***(Dickson's lemma)*** *Let S be a subset of $\mathbb{N}^e$. Then there exists a finite set of elements $H = \{s_1, ..., s_k\}$ in S such that $S \subseteq \bigcup_{i=1}^{k}(s_i + \mathbb{N}^e)$.*

Proof : We will proceed by induction on e. For $e = 1$ S is a subset of $\mathbb{N}$, so take s to be the minimal element of S, then in this case $H = \{s\}$, and lemma is true for $e = 1$.
Suppose that the lemma is true up to $e - 1$ and consider a subset S of $\mathbb{N}^e$. Let $c = (c_1, ..., c_e)$ be any element in S. If $\alpha = (\alpha_1, ..., \alpha_e) \in S$ with $\alpha_i \geq c_i$ for all $1 \leq i \leq e$, then $\alpha \in (c + \mathbb{N}^e)$. Otherwise there exists some $1 \leq i \leq e$ such that $\alpha_i \leq c_i$. For each $1 \leq i \leq e$ and $0 \leq a \leq c_i$ define the set $A_{i,a} = \{(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_e) \in \mathbb{N}^{e-1}$ such that $(\alpha_1, ..., \alpha_{i-1}, a, \alpha_{i+1}, ..., \alpha_e) \in S\}$. By the induction hypothesis there exists a finite subset $B_{i,a} \subseteq A_{i,a}$ such that for every $(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_e) \in A_{i,a}$ there exists $(\beta_1, ..., \beta_{i-1}, \beta_{i+1}, ..., \beta_e) \in B_{i,a}$ with $(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_e) \in (\beta_1, ..., \beta_{i-1}, \beta_{i+1}, ..., \beta_e) + \mathbb{N}^{e-1}$. Hence $(\alpha_1, ..., \alpha_{i-1}, a, \alpha_{i+1}, ..., \alpha_e) \in (\beta_1, ..., \beta_{i-1}, a, \beta_{i+1}, ..., \beta_e) + \mathbb{N}^e$, and so the desired finite subset is
$H = \{c\} \cup \{(\beta_1, ..., \beta_{i-1}, a, \beta_{i+1}, ..., \beta_e),$ *with* $(\beta_1, ..., \beta_{i-1}, \beta_{i+1}, ..., \beta_e) \in B_{a,i},\ 1 \leq i \leq e$ *and* $0 \leq a \leq c_i\}$.■

Lemma 13 *Fix a line-free cone C in $\mathbb{R}^e$ with a non-empty interior. Let S be any subset of $C \cap \mathbb{Z}^e$. Then there exists a finite subset $F = \{\alpha_1, ..., \alpha_n\}$ of S such that $S \subseteq \bigcup_{i=1}^{n}(\alpha_i + C)$.*

Proof : Consider a set of generators $\{v_1, ..., v_k\}$ of the cone C where $v_1, ..., v_k \in \mathbb{Z}^e$. Let $s \in S$. The element s can be written as $s_1v_1 + ... + s_kv_k$ for some $s_1, ..., s_k \in \mathbb{R}^+$. Since $s \in \mathbb{Z}^e$, $s_1, ..., s_k$ are non negative elements in $\mathbb{Q}$. Define the set

$$B = \{b_1v_1 + ... + b_kv_k,\ b_i \in [0, 1]\ \forall 1 \leq i \leq k\}$$

Since B is bounded, $B \cap \mathbb{Z}^e$ is finite. Say $B = \{c_1, ..., c_l\}$ for some $l \in \mathbb{N}$. Then every $s = s_1v_1 + ... + s_kv_k \in S$ can be written as $s = a_1v_1 + ... + a_kv_k + c_i$ where $a_j \in \mathbb{N}$ is the integer part of s_j for all $j \in \{1, ..., k\}$ and c_i is some element in B. Now for each $1 \leq i \leq l$, let N_i be the set of elements $(a_1, ..., a_k) \in \mathbb{N}^e$ such that $a_1v_1 + ... + a_kv_k + c_i \in S$ for some $1 \leq i \leq l$. By Dickson's Lemma there exists a finite set $H_i \subseteq N_i$ such that for every $(a_1, ..., a_k) \in N_i$ there is some $(h_1, ..., h_k) \in H_i$ such that $(a_1, ..., a_k) \in (h_1, ..., h_k) + \mathbb{N}^e$, and so $(a_1 - h_1)v_1 + ... + (a_k - h_k)v_k \in C$ since $(a_i - h_i) \geq 0$ for all $1 \leq i \leq k$, hence $a_1v_1 + ... + a_kv_k + c_i \in h_1v_1 + ... + h_kv_k + c_i + C$, then the desired set F is equal to

$$\bigcup_{i=1}^{l}\{h_1v_1 + ... + h_kv_k + c_i,\ (h_1, ..., h_k) \in H_i\}$$

which is obviously finite, say $F = \{\alpha_1, ..., \alpha_n\}$ for some $n \in \mathbb{N}$. We finally get $S \subseteq \bigcup_{i=1}^{n}(\alpha_i + C)$. ■

Definition 26 *Let $\leq$ be a total order on $\mathbb{Z}^e$. The order $\leq$ is said to be additive if for all $m, n, k \in \mathbb{Z}^e$ we have : $m \leq n \implies m + k \leq n + k$.*

Let $\leq$ be an additive order on a cone $C \subset \mathbb{R}^e$. The order $\leq$ is called compatible with C if for all $m \in C \cap \mathbb{Z}^e$ we have $m \geq \underline{0}$, where $\underline{0} := (0, ..., 0)$. Note that if we have an additive order $\leq$, then for all $m, n \in \mathbb{Z}^p$ with $m, n \geq \underline{0}$, we get $am + bn \geq \underline{0}$ for all $a, b \in \mathbb{N}$.

Proposition 24 *Let C be a line-free cone of dimension e. Then there exists an additive total order $\leq$ which is compatible with C.*

Proof : Consider any vector $x = (x_1, ..., x_e) \in \mathbb{R}^e$ such that its components are linearly independent over $\mathbb{Q}$, and define the order on $\mathbb{Z}^e$ as follows : for $m, n \in \mathbb{Z}^e$, $n \leq_x m \iff n \cdot x \leq m \cdot x$, where "$\cdot$" refers to the scalar product on $\mathbb{R}^e$. It is clear that this is an additive total order on $\mathbb{Z}^e$ since if $n \cdot x \leq m \cdot x$, then $(n + n') \cdot x \leq (m + n') \cdot x$ for any $n' \in \mathbb{Z}^e$, and so $n + n' \leq m + n'$. It is antisymmetric since the coordinates of x are linearly independent over $\mathbb{Q}$, indeed for all $m = (m_1, ..., m_e), n = (n_1, ..., n_e) \in \mathbb{Z}^e$ if we have $m \leq_x n$ and $n \leq_x m$, then $n \cdot x = m \cdot x$, and we get $(n_1 - m_1)x_1 + ... + (n_e - m_e)x_e = 0$, and so $n_i = m_i$ for all $1 \leq i \leq e$ hence $m = n$.
To prove that there exists some order relation which is compatible with C, we have to prove that there exists some $x \in \mathbb{R}^e$ such that $0 \leq_x n$ for all $n \in C$. Since C is a line-free cone it is enough to choose x to be in the dual cone of C. This proves our assertion. ■

Proposition 25 *Let C be a cone, and let $\leq$ be an additive total order which is compatible with C. Then $\leq$ is a well-founded order on $C \cap \mathbb{Z}^e$, i.e, every subset of $C \cap \mathbb{Z}^e$ contains a minimal element with respect to the chosen order. Moreover this minimal element is unique.*

Proof : Let $S \subset C \cap \mathbb{Z}^e$. By Lemma 13, we can find a finite subset $\{s_1, ..., s_n\}$ of S such that $S \subset \bigcup_{i=1}^{n} (s_i + C)$.
Since $\leq$ is compatible with C it follows that for every $m, n \in \mathbb{Z}^e$ such that $m \in n + C$, then $m \leq n$. So the minimal element of S is the minimal element of the set $\{s_1, ..., s_n\}$ which exists since $\leq$ is a total order. ■
Let $\mathbb{K}$ be an algebraically closed field. Consider infinite formal power series in several variables of the form $y(\underline{x}) = \sum c_a \underline{x}^a$, where $c_a \in \mathbb{K}$, and $a = (a_1, ..., a_e)$ ranges in $\mathbb{Z}^e$, and $\underline{x}^a$ denotes the monomial $x_1^{a_1} \cdots x_e^{a_e}$. We set $Supp(y(\underline{x})) = \{a, c_a \neq 0\}$.
If we consider any two series y, z of this form, then $y + z$ is naturally defined, while their multiplication does not exist in general. For that reason the support of these series should be restricted to be in the same line-free cone.

Definition 27 *Let C be a line-free cone in $\mathbb{R}^e$. We define the set of formal power series with exponents in C to be $\mathbb{K}_C[[\underline{x}]] := \{y(\underline{x}) = \sum_{p \in \mathbb{Z}^e} c_p \underline{x}^p,\ Supp(y(\underline{x})) \subseteq C\}$*

Proposition 26 *Let C be a cone, and let $\leq$ be an additive order on $\mathbb{Z}^e$. Let $\{v_1, ..., v_k\}$ be a set of generators of C. C is compatible with $\leq$ if and only if $v_i \geq 0$ for all $i = 1, ..., k$.*

Proof : If C is compatible with $\leq$, then $v \geq 0$ for all $v \in C$. In particular $v_i \geq 0$ for all $1 \leq i \leq k$. On the other hand, suppose that $v_i \geq 0$ for all $1 \leq i \leq k$, and let $v \in C \cap \mathbb{Z}^e$, then $v = a_1 v_1 + \cdots + a_e v_e$ for some $a_1, .., a_e \in \mathbb{R}^+$. Since $\leq$ is an additive order then $v = a_1 v_1 + \cdots + a_e v_e \geq 0$. Hence $v \geq 0$ for all $v \in C$. ■

Remark 8 *Let $\leq$ be an additive order on $\mathbb{Z}^e$, and consider two cones C, C' in $\mathbb{Z}^e$ which are compatible with $\leq$. Let $\{v_1, ..., v_k\}$ be a set of generators of C, and let $\{w_1, ..., w_h\}$ be a set of generators of C'. By Proposition 26 $v_i, w_j \geq 0$ for all $1 \leq i \leq k$ and $1 \leq j \leq h$. But $\{v_1, ..., v_k, w_1, ..., w_h\}$ is a set of generators of $C + C'$, hence by Proposition 26, $C + C'$ is compatible with $\leq$.*

In what follows we shall give some results in order to prove that $\mathbb{K}_C[[\underline{x}]]$ is a ring, where C is a line free cone in $\mathbb{Z}^e$.

Proposition 27 *Let $K \subseteq \mathbb{R}^e$ be a closed and convex set. The set K is unbounded if and only if there exists some $u \in K$ and a non zero vector $v \in \mathbb{R}^e$, such that the ray $R = \{u + \lambda v\}_{\lambda \geq 0} \subseteq K$. Moreover for all $u, u' \in K$ we have $\{u + \lambda v\}_{\lambda \geq 0} \subseteq K \iff \{u' + \lambda v\}_{\lambda \geq 0} \subseteq K$.*

Proof : If K contains a ray then it is obvious that K is unbounded.
Now suppose that K is unbounded. Let $u \in K$, and let S be the unit sphere in $\mathbb{R}^e$ centered at the origin. For each $\lambda > 0$ consider the map $\pi : \ u + \lambda S \to u + S$ defined by $\pi(u + x) = u + \frac{x}{\|x\|}$ and define the family of sets $\{P_\lambda = \pi((u + \lambda S) \cap K)\}_{\lambda > 0}$. Since π is continuous and bijective. $u + \lambda S$ is homeomorphic to $u + S$, and so $u + \lambda S$ is closed and bounded, hence compact. Since K is closed, $K \cap (u + \lambda S)$ is compact and so P_λ is compact for all $\lambda > 0$. Since K is unbounded, we have $P_\lambda \neq \phi$ for all $\lambda > 0$.
For all $\lambda' \leq \lambda$ we have $P_\lambda \subset P_{\lambda'}$. Indeed, let $u + s = \pi(u + \lambda s) \in P_\lambda$ for some $s \in S$. As $\lambda \geq \lambda'$ we have $t = \frac{\lambda - \lambda'}{\lambda} \geq 0$, and so $u + \lambda' s = tu + (1 - t)(u + \lambda s)$ belongs to the segment $[u, u + \lambda s]$. Since K is convex we have $u + \lambda' s \in K$, hence $u + s = \pi(u + \lambda' s) \in P_{\lambda'}$, and so $P_\lambda \subset P_{\lambda'}$. Now the family $\{P_\lambda\}_{\lambda > 0}$ is a decreasing nested sequence of non-empty compact subsets. By Cantor's intersection theorem :

$$\bigcap_{\lambda > 0} P_\lambda \neq \phi.$$

Let p be any vector in this intersection. For all $\lambda > 0$ there exists $s_\lambda \in S$ such that $u + \lambda s_\lambda \in K$ and $p = \pi(u + \lambda s_\lambda) = u + s_\lambda$, and so $s_\lambda = p - u$ for all $\lambda > 0$, hence by letting $v = p - u$ we will have $R = \{u + \lambda v\}_{\lambda \geq 0} \subseteq K$.
Concerning the last statement of the Proposition, let $u \in K$ be such that $\{u + \lambda v\}_{\lambda \geq 0} \subseteq K$, and let u' be another point in K. We want to prove that $u' + \lambda v \in K$ for all $\lambda \geq 0$. Fix $\lambda \geq 0$, and for each $n \in \mathbb{N}^*$, consider the point $x_n = (1 - \frac{1}{n})u' + \frac{1}{n}(u + \lambda n v)$. Since $u', u + (\lambda n)v \in K$ and $\frac{1}{n} \in [0, 1]$, and by the fact that K is convex, we get that $x_n \in K$ for all $n \in \mathbb{N}^*$. On the other hand $x_n = (1 - \frac{1}{n})u' + \frac{1}{n}u + \lambda v$ converges to $u' + \lambda v$ as $n \to \infty$, but K is closed then $u' + \lambda v \in K$. Hence $u' + \lambda v \in K$ for all $\lambda \geq 0$. ■

Lemma 14 *Let $C \subset \mathbb{R}^e$ be a line free cone, and let B be a closed and convex set in $\mathbb{R}^e$ such that $C \cap B = \{0\}$. Then for all $k \in \mathbb{R}^e$ the set $C \cap (k + B)$ is bounded.*

Proof : Let $A = C \cap (k + B)$ for some $k \in \mathbb{R}^e$. Since C and $k + B$ are closed and convex, A is closed and convex. Suppose that A is unbounded, then by Proposition 27, there exists $u \in A$ and a non zero vector $v \in \mathbb{R}^e$ such that $\{u + \lambda v\}_{\lambda \geq 0} \subseteq A$.
Since $u \in A$, then $u \in C$. But $0 \in C$. Applying Proposition 27 to u and 0 we get

$$\{u + \lambda v\}_{\lambda \geq 0} \subseteq C \Longleftrightarrow \{\lambda v\}_{\lambda \geq 0} \subseteq C$$

and so $\lambda v \in C$ for all $\lambda \geq 0$. In particular $v \in C$ for $\lambda = 1$.
On the other hand $u \in A$, and so $u \in k + B$. But $k \in k + B$ since $0 \in B$. Applying Proposition 27 to u and k we get

$$\{u + \lambda v\}_{\lambda \geq 0} \subseteq k + B \Longleftrightarrow \{k + \lambda v\}_{\lambda \geq 0} \subseteq k + B$$

hence $k + v \in k + B$, and so $v \in B$.
We obtained that $v \in C \cap B$, which is a contradiction since $v \neq 0$. Therefore A is bounded. ■

Remark 9 *Let C be a line free cone in $\mathbb{Z}^e$ and let $k \in \mathbb{Z}^e$. We have $C \cap -C = \{0\}$, where $-C = \{-x, \ x \in C\}$. By Lemma 14 we get that $C \cap (k - C)$ is a bounded set in $\mathbb{Z}^e$, and so it is finite.*

Remark 10 *Let C be a line free cone and let $\leq_x$ be the total additive order compatible with C given by Propostion 24. Then for all $i \in C$ the set of elements $j \in C$ such that $j \leq_x i$ is finite. Indeed, let $B = \{\alpha \in \mathbb{R}^e, \ \alpha \cdot x \leq 0\}$. Since $j \leq_x i$, then $j = i + \alpha$ for some $\alpha \in B$, and so $j \in i + B$. For all $a \in C$ we have $a \cdot x \geq 0$, then $C \cap B = \{0\}$. It follows from Proposition 14 that $C \cap (i + B)$ is bounded in $\mathbb{R}^e$, and so $C \cap (i + B) \cap \mathbb{Z}^e$ is finte. Hence the set of elements $j \in C$ such that $j \leq_x i$ is finite.*

Proposition 28 *Let C be a line-free cone in $\mathbb{R}^e$. The set $K_C[[\underline{x}]]$ is a ring.*

Proof : The neutral elements 0 and 1 are obviously in $K_C[[x]]$. It is easy to see that addition is well defined. Concerning the multiplication, let $f(\underline{x}) = \sum_i a_i \underline{x}^i$ and $g(\underline{x}) = \sum_j b_j \underline{x}^j$ be two elements of $K_C[[\underline{x}]]$, the natural definition of multiplication of f and g is :

$$f(\underline{x}).g(\underline{x}) = \sum_k (\sum_{i+j=k} a_i b_j) \underline{x}^k$$

Each k in $Supp(f.g)$ is of the form $i+j$ for some $i \in supp(f)$ and $j \in Supp(g)$, and since $Supp(f)$ and $Supp(g)$ are both in the same cone C then $i+j=k \in C$ also, hence $Supp(f.g) \subset C$. In order to show that multiplication is well defined, the coefficient of each $\underline{x}^k$ which is $\sum_{i+j=k} a_i b_j$ must be a finite sum. By Remark 9 we get that for each k in $Supp(f.g)$ the set $C \cap (k-C)$ contains only a finite number of points in $\mathbb{Z}^e$, hence the sum is finite. ■

Lemma 15 *(Principle of Noetherian Induction) : Let C be a set and let $\leq$ be a well founded order on C. To prove that a property $p(x)$ is true for all $x \in C$. It is enough to prove that $p(x)$ is true for minimal elements and for every $x \in C$ we have*

$$(I): \ p(y) \text{ is true for all } y < x \implies p(x) \text{ is true}$$

Proof : Suppose to the contrary that (I) is true but $p(z)$ is not true for some $z \in C$. Let N be the set of all elements such that $p(z)$ is false. Since $\leq$ is a well founded order on C and N is a non empty set, then N admits a minimal element, say m. Now let $y \in C$ such that $y < m$. Since m is a minimal element in N, then $y \notin N$, and so $p(y)$ is true. We get that $p(y)$ is true for all $y < m$. It follows from our hypothesis (I) that $p(m)$ is true. This is a contradiction. ■

Theorem 3 *Let $y(\underline{x}) = \sum_a c_a \underline{x}^a$ be an element of $\mathbb{K}_C[[\underline{x}]]$, where C is a line free cone in $\mathbb{R}^e$. There exists $z(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$ such that $y(\underline{x}).z(\underline{x}) = 1$ if and only if $c_0 \neq 0$.*

Proof : In fact if $c_0 = 0$, it is impossible to find a multiplicative inverse for y, since for any $z(\underline{x}) = \sum_i d_i \underline{x}^i \in \mathbb{K}_C[[\underline{x}]]$, the constant term of $y(\underline{x})z(\underline{x})$ will be $c_0 d_0 = 0$ while it should be equal to 1.
Conversely if $c_0 \neq 0$, then we can construct a power series $z(\underline{x}) = \sum_i d_i \underline{x}^i$, with $d_0 = \frac{1}{c_0}$. Now consider an additive order $\leq$ on $\mathbb{Z}^e$ that is compatible with, which exists since C is line free-cone, then it is a well founded order on C. We will prove our statement by noetherian induction. Suppose that the coefficients d_i of $z(\underline{x})$ can be chosen in a unique way for all $i < k$, and let us prove that d_k can be chosen in a unique way. We have :

$$y(\underline{x})z(\underline{x}) = \sum_k \Big(\sum_{i,j \in C, i+j=k} c_i d_j \Big) \underline{x}^k$$

So the coefficient of $\underline{x}^k$ is equal to $\sum_{i+j=k} c_i d_j = c_0 d_k + \sum_{i \neq 0} c_i d_{k-i}$. Let $i > 0$, then $-i < 0$ since the order is additive. It follows that $j = k - i < k$, and so by the induction hypothesis d_{k-i} are obtained in a unique way. Since the coefficient of $\underline{x}^k$ should be equal to zero, then it is enough to take $d_k = -\frac{1}{c_0} \sum_{i \neq 0} c_i d_{k-i}$.
It follows from the principle of noetherian induction that for all $k \in C$ we can choose d_k in a unique way. Hence we get the result.■
As we can see, $\mathbb{K}[[\underline{x}]]$ is a special case of $\mathbb{K}_C[[\underline{x}]]$ when C is the cone generated by the canonical basis of $\mathbb{N}^e$, and the properties of $\mathbb{K}[[\underline{x}]]$ generalize to rings of the form $\mathbb{K}_C[[\underline{x}]]$ for any line-free cone C.

2.4.2 Fractional power series solutions

We will define a kind of polynomials, namely free polynomials. They are polynomials in $\mathbb{K}_C[[\underline{x}]][y]$ that admit a fractional power series solution in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$, where C is some line free cone, and n is the degree of the polynomial. We will prove also that a polynomial f of degree n in $\mathbb{K}[[\underline{x}]][y]$ admits a fractional power series solution in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ after some change of variables. Hence it is free.
Consider the polynomial :

$$f(x_1, ..., x_e, y) = f(\underline{x}, y) = y^n + a_1(\underline{x})y^{n-1} + \cdots + a_{n-1}(\underline{x})y + a_n(\underline{x}).$$

Then f is a polynomial in y with coefficients in the multivariate formal power series ring $\mathbb{K}[[\underline{x}]]$, where $\mathbb{K}$ is an algebraically closed field of characteristic zero. Let Δ be the discriminant of f in y, and write $\Delta(x_1, ..., x_e) = \sum_{p \in \mathbb{N}^e} c_{(p_1,...,p_e)} x_1^{p_1} ... x_e^{p_e} \in K[[\underline{x}]]$. Set :

$$Supp(\Delta) = \{p = (p_1, ..., p_e) \in \mathbb{N}^e, c_{(p_1,...,p_e)} \neq 0\}.$$

Write $\Delta = \sum_{d\geq 0} u_d(x_1,...,x_e)$ where $u_d(x_1,...,x_e) = \sum_{p_1+...+p_e=d} c_{(p_1,...,p_e)} x_1^{p_1}\dots x_e^{p_e}$ is the homogeneous component of Δ of degree d. Let $a = inf\{d,\ u_d \neq 0\}$. Note that if $a = 0$, then f is a quasi-ordinary polynomial. Suppose that $a \neq 0$. Then u_a is a non constant polynomial in $\mathbb{K}[[\underline{x}]]$, say $u_a = \sum \lambda_{(a_1,...,a_e)} x_1^{a_1}\dots x_e^{a_e}$. Moreover, suppose without loss of generality that x_1 appears in u_a.

Remark 11 *Consider the mapping*

$$\xi :\ \mathbb{K}[[x_1,...,x_e]] \mapsto \mathbb{K}[[X_1,...,X_e]]$$

defined by $\xi(x_1) = X_1$ *and* $\xi(x_i) = X_i + t_iX_1$ *for all* $i \in \{2,...,e\}$, *where* t_i *is a parameter to be determined. For all* $y = \sum c_a x_1^{a_1}\dots x_e^{a_e}$ *in* $\mathbb{K}[[x_1,...,x_e]]$ *we have* $\xi(y) = y(X_1, X_2+t_2X_1,\dots, X_e+t_eX_1) = \sum c_a X_1^{a_1}(X_2+t_2X_1)^{a_2}\dots(X_e+t_eX_1)^{a_e}$. *It is obvious that* ξ *is a homomorphism of rings. Morover consider the mapping* $\phi :\ \mathbb{K}[[X_1,...,X_e]] \mapsto \mathbb{K}[[x_1,...,x_e]]$ *defined by* $\phi(Y) = Y(x_1, x_2 - t_2x_1,...,x_e - t_ex_1) = \sum a_p x_1^{p_1}(x_2 - t_2x_1)^{p_2}\dots(x_e - t_ex_1)^{p_e}$ *for all* $Y(\underline{X}) = \sum a_p X_1^{p_1}\dots X_e^{p_e}$, *then*

$$\xi\circ\phi(Y) = \sum a_p X_1^{p_1}(X_2 - t_2X_1 + t_2X_1)^{p_2}\dots(X_e - t_eX_1 + t_eX_1)^{p_e} = \sum a_p X_1^{p_1}X_2^{p_2}\dots X_e^{p_e} = Y.$$

It follows that for all $y(\underline{x}) \in \mathbb{K}[[x_1,...,x_e]]$ *and* $Y(\underline{X}) \in \mathbb{K}[[X_1,...,X_e]]$ *we have* $\phi\circ\xi(y) = y$ *and* $\xi\circ\phi(Y) = Y$. *Hence* ϕ *is the inverse of* ξ *and so* ξ *is an isomorphism.*

Let $\psi :\ \mathbb{K}[[\underline{x}]][y] \mapsto \mathbb{K}[[\underline{X}]][y]$ be the extension of the map ξ in Remark 11. That is for all $f = a_n(\underline{x})y^n + \dots + a_1(\underline{x})y + a_0(\underline{x})$ in $\mathbb{K}[[\underline{x}]][y]$ we have $\psi(f) = \xi(a_n(\underline{x}))y^n + \dots + \xi(a_1(\underline{x}))y + \xi(a_0(\underline{x}))$. Then ψ is an isomorphism between $\mathbb{K}[[\underline{x}]][y]$ and $\mathbb{K}[[\underline{X}]][y]$.

Now let the notation be as above and let $\Delta(\psi(f))$ be the discriminant of $\psi(f)$. Then

$$\Delta(\psi(f)) = \sum c_{(p_1,...,p_e)} X_1^{p_1}(X_2 + t_2X_1)^{p_2}...(X_e + t_eX_1)^{p_e}.$$

Moreover, $\Delta(\psi(f)) = \sum_{d\geq 0} u_d(X_1, X_2+t_2X_1,..., X_e+t_eX_1)$. For all $d \geq 0$ let $v_d(X_1,\dots,X_e) = u_d(X_1, X_2 + t_2X_1,..., X_e + t_eX_1)$. Then

$$v_d(X_1,...,X_e) = \sum_{p_1+...+p_e=d} c_{(p_1,...,p_e)} X_1^{p_1}(X_2 + t_2X_1)^{p_2}\dots(X_e + t_eX_1)^{p_e}$$

$$= \varepsilon_d(t_2,\dots,t_e)X_1^{p_1+...+p_e} + v'_d(X_1,\dots,X_e) = \varepsilon_d(t_2,\dots,t_e)X_1^d + v'_d(X_1,\dots,X_e)$$

where v'_d is a homogeneous polynomial of degree d, and $\varepsilon_d(t_2,\dots,t_e)$ is a polynomial in $t_2,\dots,t_e$. Since $\mathbb{K}$ is an infinite field, we can choose $t_2,\dots,t_e \in \mathbb{K}$ such that $\varepsilon_d(t_2,\dots,t_e) \neq 0$.
Note that $\epsilon_d(t_2,\dots,t_e) = \sum_{p_1+...+p_e=d} c_{(p_1,...,p_e)} t_2^{p_2}\dots t_e^{p_e}$, hence this polynomial cannot be identically zero. This is clear if $u_d(x_1,\dots,x_e)$ is a monomial. Otherwise, since $p_1+\dots+p_e = d$ for all $(p_1,\dots,p_e) \in \mathrm{Supp}(u_d)$, all elements in $\mathrm{Supp}(\epsilon_d)$ are pairwise distinct.

Example 1 *Let* $\Delta = x_1x_2 - x_1x_3$. *Then the change of variables* $X_1 = X_1, X_2 = X_1 + X_2, x_3 = X_1 + X_3$ *gives us the new polynomial* $X_1(X_1 + X_2) - X_1(X_1 + X_3) = X_1X_2 - X_1X_3$. *This justifies the above use of the variables* $t_2,\dots,t_e$ *since we need the new discriminant to contain a power of* X_1

Let $a = \mathrm{in}f\{d : u_d \neq 0\}$. By the above change of variables we may assume that the following condition holds :

(1) The polynomial u_a contains x_1^a with a nonzero constant.

From now on we suppose that f is a polynomial in $\mathbb{K}[[\underline{x}]][y]$ that satisfies the above condition.

Theorem 4 *Consider a polynomial* $f(\underline{x}, y)$ *in* $K[[\underline{x}]][y]$ *and assume that* f *satisfies condition* (1). *Then the polynomial*

$$F(X_1,...,X_e,y) = f(X_1, X_2X_1,\dots, X_eX_1, y)$$

is a quasi-ordinary polynomial.

Proof : Let $\Delta = \sum_p c_{(p_1,...,p_e)} x_1^{p_1} \dots x_e^{p_e}$ be the discriminant of f. Consider the change of variables :

$$x_1 = X_1, x_2 = X_2X_1, ..., x_e = X_eX_1$$

The new discriminant Δ_N of $F(X_1, ..., X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y)$ is $\Delta_N = \Delta(X_1, X_2X_1, \dots, X_eX_1)$. Write $\Delta = \sum_{d\geq 0} u_d$, where u_d is the homogeneous component of degree d of Δ. Let $a = inf\{d : u_d \neq 0\}$. By hypothesis $u_a = c_a x_1^a + ...$ with $c_a \neq 0$. Then

$$u_a(X_1, X_2X_1, \dots, X_eX_1) = x_1^a(c_a + \epsilon_a(X_1, \dots, X_e))$$

with $\epsilon(0, \dots, 0) = 0$. On the other hand, if $u_d = \sum c_{(d_1,...,d_e)} x_1^{d_1} \dots x_e^{d_e}$ then

$$u_d(X_1, X_2X_1, \dots, X_eX_1) = X_1^d u_d(1, X_2, \dots, X_e) = X_1^d \varepsilon_d(X_1, ..., X_e)$$

with $\epsilon_d(X_1, \dots, X_e) \neq 0$. We finally obtain that

$$\Delta_N = X_1^a(c + \varepsilon(X_1, \dots, X_e))$$

with $c \neq 0$ and $\varepsilon(0, \dots, 0) = 0$. That is, F is a quasi-ordinary polynomial. ■
In the following we will introduce a line free cone which is independent of the choice of the polynomial f. However, we should keep in mind that in order to use this cone, the given polynomial should satify condition (1).

Proposition 29 *Let the notation be as above. Consider the set C defined by :*

$$C = \{(c_1, ..., c_e) \in \mathbb{R}^e, c_1 \geq -(c_2 + \dots + c_e),\ c_i \geq 0\ \forall\ 2 \leq i \leq e\}$$

Then C is a line free convex cone.

Proof : Let $c = (c_1, ..., c_e) \in C$ and $\lambda \geq 0$, then $c_1 \geq -(c_2 + \dots + c_e)$ and $c_i \geq 0$ for all $2 \leq i \leq e$, and so $\lambda c_1 \geq -\lambda(c_2 + \dots + c_e) = -(\lambda c_2 + \dots + \lambda c_e)$ and $\lambda c_i \geq 0$ for all $i \in \{2, ..., e\}$. It follows that $\lambda.c \in C$, hence C is a cone. Now consider $c = (c_1, ..., c_e), c' = (c'_1, ..., c'_e) \in C$, then $c_i + c'_i \geq 0$ for all $2 \leq i \leq e$ and $c_1 + c'_1 \geq -(c_2 + c'_2 + \dots + c_e + c'_e)$, and so $c + c' \in C$. In particular, if $c, c' \in C$ and $0 \leq \lambda \leq 1$, then $\lambda c + (1 - \lambda)c' \in C$, and so C is a convex cone.
Finally to prove that C is a line free cone, let $c = (c_1, ..., c_e) \in C$ such that $c \neq \underline{0}$, and let us prove that $-c = (-c_1, ..., -c_e) \notin C$. We have $c_i \geq 0$ for all $i \in \{2, ..., e\}$. If $c_i > 0$ for some $i \in \{2, ..., e\}$, then obviously $-c = (-c_1, ..., -c_e) \notin C$. If $c_i = 0$ for all $i \in \{2, ..., e\}$, then $c_1 \geq -(c_2 + \dots + c_e) = 0$, but $c \neq \underline{0}$, then $c_1 > 0$, and so $-c = (-c_1, 0, ..., 0) \notin C$. Hence C is a line free cone.■
From now on C denotes the cone defined in Proposition 29 unless otherwise specified.

Lemma 16 *Let $Y(X_1, ..., X_e)$ be an element of $\mathbb{K}[[\underline{X}]] = \mathbb{K}[[X_1, ..., X_e]]$. Consider :*

$$y(x_1, ..., x_e) = Y(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}).$$

We have $y \in \mathbb{K}_C[[\underline{x}]]$.

Proof : Write $Y(X_1, ..., X_e) = \sum_{(a_1,...,a_e)} \gamma_{(a_1,...,a_e)} X_1^{a_1} \dots X_e^{a_e}$. We have :

$$\begin{aligned} y(x_1, ..., x_e) &= \sum_{(a_1,...,a_e)} \gamma_{(a_1,...,a_e)} x_1^{a_1} (x_2x_1^{-1})^{a_2} \dots\ (x_ex_1^{-1})^{a_e} \\ &= \sum_{(a_1,...,a_e)} \gamma_{(a_1,...,a_e)} x_1^{a_1-(a_2+...+a_e)} x_2^{a_2} \dots\ x_e^{a_e} \end{aligned}$$

Let $Supp(Y)$ be the support of Y, then

$$Supp(y) = \{(a_1 - (a_2 + \dots + a_e), a_2, ..., a_e), (a_1, ..., a_e) \in supp(Y)\}.$$

Now let $q = (q_1, q_2, ..., q_e) = (a_1 - (a_2 + \dots + a_e), a_2, ..., a_e)$ be an element of $Supp(y)$, where $(a_1, ..., a_e) \in supp(Y)$. Since $Y(\underline{X}) \in \mathbb{K}[[\underline{X}]]$, then $(a_1, ..., a_e) \geq \underline{0}$ componentwise. Hence $q_1 = a_1 - (a_2 + \dots + a_e) \geq -(a_2 + \dots + a_e) = -(q_2 + \dots + q_e)$ and $q_i = a_i \geq 0$ for all $2 \leq i \leq e$, and so $q \in C$. It follows that $y \in \mathbb{K}_C[[\underline{x}]]$.■

Definition 28 *Let $n, e \in \mathbb{N}^*$. We define the ring $\mathbb{K}_C[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$, denoted by $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$, to be the set of formal power series of the form $\sum_{p=(p_1,...,p_e)\in C} c_p \underline{x}^{\frac{p}{n}} = \sum_{p=(p_1,...,p_e)} c_p x_1^{\frac{p_1}{n}} \dots x_e^{\frac{p_e}{n}}$.*

Lemma 17 *Let f be a polynomial in $\mathbb{K}[[\underline{x}]][y]$. Then f is irreducible in $\mathbb{K}_C[[\underline{x}]][y]$ if and only if $F(x_1, ..., x_e, y) = f(x_1, x_2x_1, ..., x_ex_1, y)$ is irreducible in $\mathbb{K}[[\underline{x}]][y]$, where polynomials are considered as polynomials in the variable y.*

Proof : Suppose that f is irreducible in $\mathbb{K}_C[[\underline{x}]][y]$ and suppose to the contrary that F is reducible in $\mathbb{K}[[\underline{x}]][y]$. There exists some monic polynomials $G, H \in \mathbb{K}[[\underline{x}]][y]$ such that $F = G.H$ and $0 < deg_y(G), deg_y(H) < n$. But $f(x_1, ..., x_e, y) = F(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$. Then :

$$f(x_1, ..., x_e, y) = G(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y).H(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$$

Let $g(\underline{x}, y) = G(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$ and $h(\underline{x}, y) = H(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$. Let $m = deg_y(G)$ and write $G(\underline{x}, y) = y^m + a_1(\underline{x})y^{m-1} + ... + a_m(\underline{x})$, where $a_i(\underline{x}) \in \mathbb{K}[[\underline{x}]]$ for all $i = 1, ..., m$. Then :

$$g(\underline{x}, y) = y^m + a_1(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})y^{m-1} + ... + a_m(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})$$

Since $a_i(\underline{x}) \in \mathbb{K}[[\underline{x}]]$ for all $i = 1, ..., m$, then by Lemma 16 we get that $a_i(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}) \in \mathbb{K}_C[[\underline{x}]]$ for all $i = 1, ..., m$. It follows that $g \in \mathbb{K}_C[[\underline{x}]][y]$. Similarly we can prove that $h \in \mathbb{K}_C[[\underline{x}]][y]$. Hence $f = g.h$ with $0 < deg_y(g) = deg_y(G) < n$ and $0 < deg_y(h) = deg_y(H) < n = deg_y(f)$, and so f is reducible in $\mathbb{K}_C[[\underline{x}]][y]$, which is a contradiction. It follows that F is irreducible in $\mathbb{K}[[\underline{x}]][y]$.
Conversely Let F be an irreducible polynomial in $\mathbb{K}[[\underline{x}]][y]$, and let $f = F(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$. Since $F \in \mathbb{K}[[\underline{x}]][y]$, then F is a polynomial in y with coefficients in $\mathbb{K}[[\underline{x}]]$. It follows from lemma 16 that f is a polynomial in y with coefficients in $\mathbb{K}_C[[\underline{x}]]$, and so $f \in \mathbb{K}_C[[\underline{x}]][y]$. Now suppose to the contrary that f is reducible in $\mathbb{K}_C[[\underline{x}]][y]$, that is there exists $h_1, h_2 \in \mathbb{K}_C[[\underline{x}]][y]$ such that $f = h_1h_2$ with $deg_y(h_1), deg_y(h_2) < deg_y(g)$.
Now let $a(x_1, ..., x_e) = \sum c_a x_1^{a_1} \dots x_e^{a_e}$ be an element in $\mathbb{K}_C[[\underline{x}]]$, then

$$a(x_1, x_2x_1, ..., x_ex_1) = \sum c_a x_1^{a_1}(x_2x_1)^{a_2} \dots (x_ex_1)^{a_e} = \sum c_a x_1^{a_1+a_2+...+a_e} x_2^{a_2} \dots x_e^{a_e}$$

Since $a(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$, then $a_1 \geq -(a_2 + \dots + a_e)$ for all $(a_1, ..., a_e) \in Supp(a(\underline{x}))$. It follows that $a_1 + a_2 + \dots + a_e \geq 0$ for all $(a_1, ..., a_e) \in Supp(a(\underline{x}))$. Hence, $a(x_1, x_2x_1, ..., x_ex_1) \in \mathbb{K}[[\underline{x}]]$. Then $h_1(x_1, x_2x_1, ..., x_ex_1, y)$, $h_2(x_1, x_2x_1, ..., x_ex_1, y) \in \mathbb{K}[[\underline{x}]][y]$. But

$$F(x_1, ..., x_e, y) = f(x_1, x_2x_1, ..., x_ex_1, y) = h_1(x_1, x_2x_1, ..., x_ex_1, y)h_2(x_1, x_2x_1, ..., x_ex_1, y).$$

Hence F is reducible in $\mathbb{K}[[\underline{x}]][y]$, which is a contradiction.■

Definition 29 *Let f be a polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$. Then f is said to be a free polynomial if f is irreducible in $\mathbb{K}_C[[\underline{x}]][y]$ and if it admits a solution in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$.*

Theorem 5 *Let $f(\underline{x}, y) = y^n + a_1(\underline{x})y^{n-1} + \dots + a_{n-1}(\underline{x})y + a_n(\underline{x})$ be a polynomial of $\mathbb{K}[[\underline{x}]][y]$ that satisfies condition (1). Suppose that f is irreducible in $\mathbb{K}_C[[\underline{x}]][y]$, then f is free.*

Proof : By Theorem 4 the polynomial F defined by

$$F(X_1, ..., X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y)$$

is a quasi-ordinary polynomial of $\mathbb{K}[[\underline{X}]][y]$.
By Lemma 17 we get that F is an irreducible quasi-ordinary polynomial in $\mathbb{K}[[\underline{X}]][y]$ of degree n, then by the Abhyankar-Jung theorem there exists a formal power series $Z(X_1, ...X_e) = \sum_{(a_1,...,a_e)} \gamma_{(a_1,...,a_e)} X_1^{\frac{a_1}{n}} ... X_e^{\frac{a_e}{n}}$ in $\mathbb{K}[[X_1^{\frac{1}{n}}, ..., X_e^{\frac{1}{n}}]]$ such that $F(X_1, ..., X_e, Z(X_1, ..., X_e)) = 0$. But :

$$F(X_1, ..., X_e, Z(X_1, ..., X_e)) = f(X_1, X_2X_1, \dots, X_eX_1, Z(X_1, ..., X_e))$$

Then $f(x_1, x_2, ..., x_e, Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})) = 0$. It follows that $Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})$ is a solution of $f(x_1, ..., x_e, y) = 0$. Since $Z(X_1, ..., X_e) \in \mathbb{K}[[\underline{X}^{\frac{1}{n}}]]$, then by Lemma 16 we deduce that $Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})$ belongs to $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. This proves our assertion.■

Proposition 30 *Let the notation be as above, with f a free polynomial of degree n in $\mathbb{K}[[\underline{x}]][y]$ that satisfies condition (1). Let d be a divisor of n. Then the d-th approximate root of f is free.*

Proof : By Theorem 4 and Lemma 17 the polynomial F defined by

$$F(X_1, ..., X_e, y) = f(X_1, X_2X_1, \ldots, X_eX_1, y)$$

is a quasi-ordinary irreducible polynomial of $\mathbb{K}[[\underline{X}]][y]$. Let G be the d-th approximate root of F, and let

$$F = G^d + C_1(\underline{X}, y)G^{d-1} + \ldots + C_d(\underline{X}, y)$$

be the G-adic expansion of F, with $deg_y(C_i) < \frac{n}{d}$ for all $i \in \{1, ..., d\}$. Since G is the d-th approximate root of F, then by Proposition 5 we get that $C_1(\underline{X}, y) = 0$. Hence :

$$\begin{aligned} f(x_1, ..., x_e, y) &= F(x_1, x_2x_1^{-1}, \ldots, x_ex_1^{-1}, y) \\ &= g^d(\underline{x}, y) + C'_2(\underline{x}, y)g^{d-1}(\underline{x}, y) + \ldots + C'_d(\underline{x}, y) \end{aligned}$$

Where $g(\underline{x}, y) = G(x_1, x_2x_1^{-1}, \ldots, x_ex_1^{-1}, y)$ and $C'_i(\underline{x}, y) = C_i(x_1, x_2x_1^{-1}, \ldots, x_ex_1^{-1}, y)$ for all $i \in \{2, ..., d\}$. By Lemma 16 we have $g \in \mathbb{K}_C[[\underline{x}]][y]$ and $C'_i \in \mathbb{K}_C[[\underline{x}]][y]$ for all $i \in \{2, ..., n\}$. Since $deg_y(C'_i) < \frac{n}{d}$ for all $i \in \{2, ..., d\}$ and $deg_y(g) = \frac{n}{d}$, then again by Proposition 5 we get that g is the $d-$th approximate root of f in $\mathbb{K}_C[[\underline{x}]][y]$. By Proposition 6, f admits a unique $d-$th approximate root in $\mathbb{K}_C[[\underline{x}]][y]$, but $f \in \mathbb{K}[[\underline{x}]][y]$ and $\mathbb{K}[[\underline{x}]][y] \subseteq \mathbb{K}_C[[\underline{x}]][y]$, then g is the $d-$th approximate root of f in $\mathbb{K}[[\underline{x}]][y]$.
Since G is the approximate root of an irreducible quasi-ordinary polynomial then by Proposition 23 it is an irreducible quasi-ordinary polynomial, hence by the Abhyankar-Jung theorem G admits a root in $\mathbb{K}[[\underline{x}^{\frac{1}{\frac{n}{d}}}]]$. But $g(\underline{x}, y) = G(x_1, x_2x_1^{-1}, \ldots, x_ex_1^{-1}, y)$, then by a similar discussion as in Theorem 5 we get that g admits a root in $\mathbb{K}_C[[\underline{x}^{\frac{1}{\frac{n}{d}}}]]$. Moreover g is irreducible in $\mathbb{K}_C[[\underline{x}]][y]$ by Lemma 17. Hence g is free with respect to C.■

2.4.3 Characteristic exponents

Let the notation be as above where $f \in \mathbb{K}_C[[\underline{x}]][y]$ is a free polynomial with a root $y \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. We will study a special set of exponents of y, namely the set of characteristic exponents, with their properties.
Let L be the field of fractions of $\mathbb{K}_C[[\underline{x}]]$. Moreover set :

$$L_1 = L(x_1^{\frac{1}{n}}), L_2 = L_1(x_2^{\frac{1}{n}}), ..., L_n = L_{n-1}(x_e^{\frac{1}{n}}) = L(x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}})$$

The field L_i is obtained by adjoining the root $x_i^{\frac{1}{n}}$ of the irreducible polynomial $Y^n - x_i$ to L_{i-1}, and L_n is a Galois extension of L of degree n^e. Let U_n be the set of n^{th} roots of unity in $\mathbb{K}$. The conjugates of $x_i^{\frac{1}{n}}$ over L are $\omega.x_i^{\frac{1}{n}}$ with $\omega \in U_n$.

Definition 30 *Let $z(\underline{x}) = \sum c_p\underline{x}^{\frac{p}{n}} \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. The support of z, denoted by $Supp(z)$, is defined to be the set $\{p \in \mathbb{Z}^e, c_p \neq 0\}$. Obviously $Supp(z) \subseteq C \cap \mathbb{Z}^e$.*

Let $\theta \in Aut(L_n/L)$. For all $i = 1, ..., e$ we have $\theta(x_i^{\frac{1}{n}}) = \omega_i x_i^{\frac{1}{n}}$ for some $\omega_i \in U_n$. Then :

$$\theta(\underline{x}^{\frac{p}{n}}) = \theta(x_1^{\frac{1}{n}})^{p_1} \ldots\ \theta(x_e^{\frac{1}{n}})^{p_e} = \omega_1^{p_1}x_1^{\frac{p_1}{n}} \ldots\ \omega_e^{p_e}x_e^{\frac{p_e}{n}} = \omega_1^{p_1} \ldots\ \omega_e^{p_e}\underline{x}^{\frac{p}{n}} = k.\underline{x}^{\frac{p}{n}}$$

where k is a non-zero element in $\mathbb{K}$.
Now let $Roots(f) = \{y_i\}_{1 \leq i \leq n}$ be the conjugates of y over L, with the assumption that $y_1 = y = \sum c_p\underline{x}^{\frac{p}{n}}$. Then for all $2 \leq i \leq n$ there exists some automorphism $\theta \in Aut(L_n/L)$ such that $y_i = \theta(y)$. Hence :

$$y_i = \theta(y) = \theta(\sum c_p\underline{x}^{\frac{p}{n}}) = \sum c_p\theta(\underline{x}^{\frac{p}{n}}) = \sum c_pk_p\underline{x}^{\frac{p}{n}},\ k_p \in \mathbb{K}^*.$$

Since $k_p \in \mathbb{K}^*$ for all $p \in Supp(y)$, we have $Supp(y) = Supp(y_i)$ for all $i = 1, ..., h$.
By Proposition 24, there exists an order $\leq$ on $\mathbb{Z}^e$ which is compatible with C. Hence for all $z(\underline{x})$ in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$, $Supp(z(\underline{x}))$ can be arranged as an increasing sequence. We define the following notion : the order of z to be : $O(z) = inf(Supp(z))$ if $z \neq 0$, and $O(z) = \infty$ for $z = 0$. We set $LM(z) = \underline{x}^{\frac{p}{n}}$ where $p = O(z)$, and we call it the leading monomial of z. We set $LC(z) = c_{O(z)}$ and we call it the leading coefficient of z.

Definition 31 *Let the notation be as above with $\{y_1, ..., y_n\} = Roots(f)$ and $y_1 = y$. The set of Characteristic exponents of y is defined by :*

$$\{O(y_i - y_j),\ y_i, y_j \in Roots(f) \text{ and } y_i \neq y_j\}.$$

Similarly we define the set of Characteristic monomials of y to be : $\{LM(y_i - y_j), y_i \neq y_j\}$. Note that this set depends on the order that we are using.

Proposition 31 *Let the notation be as above. Then the set of Characteristic exponents of y is equal to the set $\{O(y_k - y), y_k \neq y\}$.*

Proof : For every $1 \leq i \neq j \leq n$ let $c_{ij} = LC(y_i - y_j)$ and $M_{ij} = LM(y_i - y_j)$, then :

$$y_i - y_j = c_{ij}M_{ij} + \epsilon_{ij}$$

where $\epsilon_{ij} \in L_n$ with $O(\epsilon_{ij}) > O(M_{ij})$. Now let $\theta \in Aut(L_n/L)$ be the automorphism such that $\theta(y_j) = y$. Then $\theta(y_i) = y_k$ for some $1 \leq k \leq n$, and $\theta(y_i - y_j) = \theta(y_i) - \theta(y_j) = y_k - y = c_{k1}M_{k1} + \epsilon_{k1}$ with $O(\epsilon_{k1}) > O(M_{k1})$. On the other hand $\theta(y_i - y_j) = \theta(c_{ij}M_{ij} + \epsilon_{ij}) = c_{ij}\alpha M_{ij} + \theta(\epsilon_{ij})$ with $\alpha \neq 0$ and $O(\theta(\epsilon_{ij})) > O(M_{ij})$. Hence $M_{k1} = M_{ij} = LM(y_i - y_j)$, and so we get :

$$\{O(y_i - y_j), y_i \neq y_j \text{ are conjugates of } y\} = \{O(y_k - y), y_k \neq y\}. \ \blacksquare$$

It follows from Proposition 31 that the set of characteristic monomials of y is given by :

$$\{LM(y_i - y_j), y_i \neq y_j\} = \{M_k = LM(y_k - y),\ k = 2, ..., n\} = \{LM(\theta(y) - y), \theta(y) \neq y,\ \theta \in Aut(L_n/L)\}.$$

Note that if $n \geq 2$, then the characteristic monomial M_k does not belong to L for all $k = 2, ..., n$. Indeed, for each M_k there exists an element $\theta \in Aut(L_n/L)$ such that $\theta(y) - y = c_kM_k + \epsilon_k$ where c_k is a non zero constant in $\mathbb{K}$ and $O(\epsilon_k) > O(M_k)$. Since $Supp(y) = Supp(\theta(y))$ then M_k is a monomial of y. Moreover we have :

$$y = p + cM_k + q$$

where c is a non zero constant and p, q are in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ such that $O(p) < O(M_k) < O(q)$, then $\theta(y) - y = (\theta(p) - p) + c(\theta(M_k) - M_k) + (\theta(q) - q)$. It follows that $\theta(p) - p = 0$ and $\theta(M_k) - M_k \neq 0$, hence $\theta(M_k) \neq M_k$ and so $M_k \notin L$.
Now we write the characteristic monomials in an increasing order and we reindex them as :

$$M_1 < M_2 < ... < M_h$$

Proposition 32 *Let the notation be as above with $\{M_1, ..., M_h\}$ the set of characteristic monomials of y. The two field extensins $L(y)$ and $L(M_1, ..., M_h)$ are equal.*

Proof : Let $\theta \in Aut(L_n/L(y))$, then θ is an L-automorphism of L_n with $\theta(y) = y$. But if $\theta(y) = y$ then $\theta(y) = \theta(\sum c_p\underline{x}^{\frac{p}{n}}) = \sum c_p\theta(\underline{x}^{\frac{p}{n}}) = \sum c_pk_p\underline{x}^{\frac{p}{n}} = y = \sum c_p\underline{x}^{\frac{p}{n}}$, with $k_p \neq 0\ \forall p \in supp(y)$, and so $\theta(\underline{x}^{\frac{p}{n}}) = \underline{x}^{\frac{p}{n}}$. Hence $\underline{x}^{\frac{p}{n}} \in L(y)\ \forall\ p \in supp(y)$. In particular $M_1, ..., M_h$ are monomials of y, then $M_1, ..., M_h \in L(y)$, and so $L(M_1, ..., M_h) \subset L(y)$.
Conversely $y \in L(M_1, ..., M_h)$. Since if $\theta \in Aut(L_n/L(M_1, .., M_h))$, i.e if θ is an L automorphism of L_n such that $\theta(M_i) = M_i\ \forall\ i = 1, ..., h$, then $\theta(y) = y$. In fact if $\theta(y) \neq y$ then $\theta(y) - y = cM_i + \epsilon_i$ for some characteristic monomial M_i, hence for this i we have $\theta(M_i) \neq M_i$ which contradicts the hypothesis. Then $L(y) \subset L(M_1, ..., M_h)$, and so $L(y) = L(M_1, ..., M_h)$. $\blacksquare$
Note that for all $k = 1, ..., h$ the characteristic monomials of y are of the form $M_k = \underline{x}^{\frac{m_k}{n}}$ for some $m_k \in C$. Moreover $\underline{x}^{\frac{m_k}{n}}$ is a root of the polynomial $Y^n - \underline{x}^{m_k}$ which belongs to $L[Y]$ since $\underline{x}^{m_k} \in L$, and so M_k is algebraic over L. Hence $L(M_1, ..., M_i) = L[M_1, ..., M_i]$ for all $i = 1, ..., h$.

Proposition 33 *Let the notation be as above with $\{m_1, ..., m_h\}$ the set of characteristic exponents of y. Let $m \in \mathbb{Z}^e$ be an element of $Supp(y)$, then $m \in (n\mathbb{Z})^e + \sum_{i=1}^{h} m_i\mathbb{Z}$.*

Proof : Write $M = \underline{x}^{\frac{m}{n}}$. Since M is a monomial of y, then $M \in L(y) = L(M_1, ..., M_h) = L[M_1, ..., M_h]$. Hence :

$$M = \frac{f_1}{g_1} M_1^{\alpha_1^1} \dots M_h^{\alpha_h^1} + \dots + \frac{f_l}{g_l} M_1^{\alpha_1^l} \dots M_h^{\alpha_h^l}.$$

for some $f_1, ..., f_l, g_1, ..., g_l \in \mathbb{K}_C[[\underline{x}]]$ and $l \in \mathbb{N}^*$, and so :

$$g_1 \dots g_l M = f_1 g_2 \dots g_l M_1^{\alpha_1^1} \dots M_h^{\alpha_h^1} + \dots + f_l g_1 \dots g_{l-1} M_1^{\alpha_1^l} \dots M_h^{\alpha_h^l}$$

Comparing both sides we get that $LM(g_1 \dots g_l M) = \underline{x}^a M_1^{\alpha_1^i} \dots M_h^{\alpha_h^i}$ for some $i \in \{1, ..., l\}$ and $a \in \mathbb{Z}^e$. Now write $LM(g_1 \dots g_l) = \underline{x}^b$ for some $b \in \mathbb{Z}^e$, then $nb + m = na + \alpha_1^i m_1 + ... + \alpha_h^i m_h$, and so $m = n(a-b) + \alpha_1^i m_1 + ... + \alpha_h^i m_h$. It follows that $m \in (n\mathbb{Z})^e + \sum_{i=1}^h m_i \mathbb{Z}$.■

Now we define the following fields :

$$F_0 = L$$
$$F_i = L[M_1, ..., M_i] = F_{i-1}[M_i] \text{ for all } i = 1, ..., h.$$

We also set :

$$G_i = (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j \mathbb{Z}$$

for all $i = 1, ..., h$, and we write $G_0 = (n\mathbb{Z})^e$. Similar to Proposition 33 we can prove that for any monomial $M = \underline{x}^{\frac{m}{n}}$ with $m \in C$, we have $M \in F_i \Leftrightarrow m \in G_i$.

Definition 32 *Let the notation be as above with $y = \sum c_p \underline{x}^{\frac{p}{n}}$ a root of f in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. Let $\{m_1, ..., m_h\}$ be the set of characteristic exponents of y. We define the following sequences :*
• *The GCD-sequence $\{D_i\}_{1 \le i \le h+1}$, with $D_1 = n^e$ and for all $i \in \{2, ..., h\}$ $D_{i+1} = gcd(nI_e, m_1^T, ..., m_i^T)$, the gcd of the (e, e) minors of the $e \times (e+i)$ matrix $A = (nI_e, m_1^T, ..., m_i^T)$, where I_e is the identity $e \times e$ matrix.*
• *The $d-$sequence $\{d_i\}_{1 \le i \le h+1}$ with $d_i = \frac{D_i}{D_{h+1}}$.*
• *The e-sequence $\{e_i\}_{1 \le i \le h}$ with $e_i = \frac{D_i}{D_{i+1}} = \frac{d_i}{d_{i+1}}$.*
• *The $r-$sequence $\{r_0^1, ..., r_0^e, r_1, ..., r_h\}$ by $(r_0^1, ...r_0^e)$ the canonical basis of $(n\mathbb{Z})^e$, $r_1 = m_1$, and for all $k \in \{1, ..., h-1\}$ $r_{k+1} = e_k \cdot r_k + m_{k+1} - m_k$.*
Note that we also have the following

$$\begin{aligned} r_{k+1} \cdot D_{k+1} &= D_{k+1} \cdot e_k \cdot r_k + (m_{k+1} - m_k) \cdot D_{k+1} = D_k \cdot r_k + (m_{k+1} - m_k) \cdot D_{k+1} \\ &= m_1 \cdot D_1 + \sum_{i=2}^{k+1} (m_i - m_{i-1}) D_i. \end{aligned}$$

Proposition 34 *Let the notation be as in Definition 32 and let v be a non zero vector in $\mathbb{Z}^e$. Let $\tilde{D}$ be the gcd of the $e \times e$ minors of the matrix $(nI_e, m_1^T, ..., m_i^T, v^T)$. Then $v \in (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$ if and only if $\tilde{D} = D_{i+1}$. Moreover, $\frac{D_{i+1}}{\tilde{D}}.v \in (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$ and if $D_{i+1} > \tilde{D}$ then for all $1 \le k < \frac{D_{i+1}}{\tilde{D}}, k.v \notin (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$.*

Proof : Same as the proof of Proposition 16.■

Definition 33 *Let $a, b \in C$. We say that $\underline{x}^{\frac{a}{n}} < \underline{x}^{\frac{b}{n}}$ if $a < b$.*

Proposition 35 *For all $i = 1, ..., h-1$ let H_i be the algebraic extension of L obtained by adjoining all the monomials M of y such that $M < M_{i+1}$ then :*
(i) $F_i = H_i$ and M_i does not belong to F_{i-1}
(ii) The degree $[F_i : F_{i-1}]$ of the field extension $F_{i-1} \subset F_i$ is equal to e_i.

Proof : (i) Since $m_j < m_{i+1}$ for all $j = 1, ..., i$, then $M_1, ..., M_i \in H_i$, and so $F_i \subseteq H_i$. In order to prove that $H_i \subseteq F_i$, consider a monomial M of y such that $M < M_{i+1}$. For each $\theta \in Aut(L_n/F_i)$, θ is an L automorphism of L_n and $\theta(M_j) = M_j$ for all $j < i+1$. Hence $LM(\theta(y) - y) \geq M_{i+1}$, and so $\theta(M) = M$ for all $M < M_{i+1}$, hence $M \in F_i$. Finally we get that $H_i = F_i$. Now to prove that $m_i \notin F_{i-1}$, let $\theta \in Aut(L_n \backslash L)$ such that $\theta(y) - y = cM_i + \varepsilon$ with $O(\varepsilon) > m_i$ and c a non zero constant(such θ obviously exists since M_i is a characteristic monomial of y), then $\theta(M_j) = M_j$ for all $j = 1, ..., i-1$ and $\theta(M_i) \neq M_i$, and so $\theta \in Aut(L_n \backslash F_{i-1})$ with $\theta(M_i) \neq M_i$, hence M_i does not belong to F_{i-1}.
Note that (i) is equivalent to say that between all the exponents m of y, m_i is the samllest one which does not belong to G_{i-1}.
(ii) Since $M_i \notin F_{i-1}$, then $m_i \notin G_{i-1}$, and so $D_i > D_{i+1}$. Moreover $e_i m_i \in G_{i-1}$ and for all $0 < \alpha < e_i$ we have $\alpha \cdot m_i \notin G_{i-1}$. Now let $g = y^l + a_1 y^{l-1} + ... + a_l$ with $a_k \in F_{i-1}$ for all $i = 1, ..., l$ be the minimal polynomial of M_i over F_{i-1} and suppose that $l < e_i$. Since $g(M_i) = 0$, then there exists some $k \in \{0, ..., l-1\}$ such that $\underline{x}^{l\frac{m_i}{n}} = \underline{x}^{\frac{\alpha}{n}} . \underline{x}^{\frac{km_i}{n}}$ for some $\alpha \in G_{i-1}$, and so $(l-k)m_i = \alpha \in G_{i-1}$ with $0 < l - k < e_i$ which is a contradiction. Hence the degree of the minimal polynomial of m_i is at least e_i. It follows easily that $Y^{e_i} - x^{e_i \cdot \frac{m_i}{n}}$ is the minimal polynomial of $x^{\frac{m_i}{n}}$ over F_{i-1}, hence $[F_i : F_{i-1}] = e_i$.■

Proposition 36 *Let f be a free polynomial of degree n, and let $\{m_1, ..., m_h\}$, $\{r_1, ..., r_h\}$ and $\{e_1, ..., e_h\}$ be its sequence of characteristic exponents, its $r-$sequence, and its $e-$sequence respectively. Then for all $i \in \{1, ..., h\}$ we have $e_i r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ and $\alpha r_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ for all $1 \leq \alpha < e_i$.*

Proof : Note that each of the sequences $(m_k)_{1 \leq k \leq h}$ and $(r_k)_{1 \leq k \leq h}$ can be obtained from the other. In particular the $r-$sequence can be rearranged in the following way : $r_1 = m_1$,$r_2 = e_1 \cdot r_1 + m_2 - m_1 = e_1 \cdot m_1 + m_2 - m_1 = m_2 + m_1(e_1 - 1)$ and so we get that $r_k = m_k + m_{k-1}(e_{k-1} - 1) + m_{k-2}(e_{k-2} - 1)e_{k-1} + ... + m_1(e_1 - 1)e_2 ... e_{k-1}$. Hence $(n\mathbb{Z})^e + \sum_{j=1}^{i} r_j \mathbb{Z} \subseteq (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j \mathbb{Z}$ for all $i \in \{1, ..., h\}$.
On the other hand we have $m_1 = r_1$ and $m_2 = r_2 - (e_1 - 1)r_1$. Suppose that $m_k = r_k + (e_{k-1} - 1)r_{k-1} + \ldots + (e_1 - 1)r_1$ up to some k with $k \geq 2$, and let us prove it for $k+1$. We have

$$\begin{aligned} r_{k+1} &= e_k r_k + m_{k+1} - m_k \\ &= m_{k+1} + (e_k - 1)r_k + (e_{k-1} - 1)r_{k-1} + \ldots + (e_1 - 1)r_1. \end{aligned}$$

Hence $m_{k+1} = r_{k+1} - (e_k - 1)r_k + \ldots + (e_1 - 1)r_1$, and so it is true for all $k \in \{2, ..., h\}$. It follows that $(n\mathbb{Z})^e + \sum_{j=1}^{i} r_j \mathbb{Z} = (n\mathbb{Z})^e + \sum_{j=1}^{i} m_j \mathbb{Z}$ for all $i \in \{1, ..., h\}$.
We have proved that for any $\alpha \in \mathbb{N}$ we have $\alpha m_i = \alpha r_i - \alpha(e_{i-1} - 1)r_{i-1} - \ldots - \alpha(e_1 - 1)r_1$ and that $(n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z} = (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_{j-1} \mathbb{Z}$. It follows easily that $\alpha r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ if and only if $\alpha m_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$.
Now let $i \in \{1, ..., h\}$ and let $M_i = \underline{x}^{\frac{m_i}{n}}$ be the characteristic monomials. We have $m_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$. Otherewise, we will get that $m_i = \alpha_1 m_0^1 + \ldots + \alpha_e m_0^e + \beta_1 m_1 + \ldots + \beta_{i-1} m_{i-1}$ for some $\alpha_1, \ldots, \alpha_e, \beta_1, \ldots, \beta_e \in \mathbb{Z}$. It follows that $\underline{x}^{\frac{m_i}{n}} = x_1^{\alpha_1} \ldots x_e^{\alpha_e} M_1^{\beta_1} \ldots M_{i-1}^{\beta_{i-1}} \in L(M_1, ..., M_{i-1})$. Which is a contradiction. It follows from Proposition 34 that $e_i m_i = \frac{D_i}{D_{i+1}} m_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$ and $\beta m_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$ for all $1 \leq \beta < e_i$. It follows directly that $e_i r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ and $\alpha r_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ for all $1 \leq \alpha < e_i$■.

Remark 12 *Since $[L(y) : L] = n$, it follows from Proposition 35 that $[L(y) : L] = e_1 \ldots e_h = \frac{D_1}{D_{h+1}}$. But $[L(y) : L] = n$ and $D_1 = n^e$, hence $D_{h+1} = n^{e-1}$. Moreover $d_1 = n$ and $d_{h+1} = 1$.*

Now we define the following sets :

$$\begin{aligned} Q(i) &= \{\theta \in Aut(L_n/L), \quad such\ that\ O(y - \theta(y)) < m_i\} \\ R(i) &= \{\theta \in Aut(L_n/L), \ such\ that\ O(y - \theta(y)) \geqslant m_i\} \\ S(i) &= \{\theta \in Aut(L_n/L), \ such\ that\ O(y - \theta(y)) = m_i\} \end{aligned}$$

Proposition 37 *Let the notation be as above with $\{D_i\}_i$ the GCD-sequence associated to y, then $\#S(i) = D_i - D_{i+1}$, where $\#S(i)$ is the cardinality of the set $S(i)$.*

Proof : Since L_n is an extension of degree n^e of L, then $\#Aut(L_n/L) = [L_n : L] = n^e$. We have

$$\theta \in R(i) \Leftrightarrow O(y - \theta(y)) \geqslant m_i \Leftrightarrow \theta(M_j) = M_j \ \forall j < i \Leftrightarrow \theta \in Aut(L_n/L(M_1, ..., M_{i-1}))$$

Hence $\#R(i) = \#Aut(L_n/L(M_1, ..., M_{i-1})) = [L_n : L(M_1, ..., M_{i-1})] = [L_n : F_{i-1}]$. By Proposition 35 we have :

$$\begin{aligned}[F_{i-1} : L] &= [F_{i-1} : F_{i-2}] \cdots [F_1 : L] = e_{i-1} \cdots e_1 \\ &= \frac{D_1}{D_2} \cdot \frac{D_2}{D_3} \cdots \frac{D_{i-1}}{D_i} = \frac{D_1}{D_i} = \frac{n^e}{D_i}\end{aligned}$$

But $[L_n : L] = [L_n : F_{i-1}] \cdot [F_{i-1} : L] = n^e$, then $[L_n : F_{i-1}] = D_i$, and so $\#(R(i)) = D_i$. Now let $\theta \in R(i+1)$, then $O(y - \theta(y)) \geqslant m_{i+1}$, but $m_{i+1} > m_i$, then $O(y - \theta(y)) \geqslant m_i$, and so $\theta \in R(i)$, hence $R(i+1) \subset R(i)$. Moreover $\theta \in S(i)$ if and only if $O(y - \theta(y)) = m_i$ if and only if $\theta \in R(i)$ and $\theta \notin R(i+1)$. It follows that $\#S(i) = \#R(i) - \#R(i+1)$, and so $\#S(i) = D_i - D_{i+1}$. ■

2.4.4 The initial form of the minimal polynomial of $y_{<m_i}$

Let f be a free polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$, and let $y = \sum c_p \underline{x}^{\frac{p}{n}} \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ be a root of f. Let $\{m_1, ..., m_h\}$ and $\{r_1, ..., r_h\}$ be the set of characteristic exponents and the $r-$squence of y respectively. For all $i \in \{1, ..., h\}$ we will define a specific polynomial G_i called the $i-$th pseudo-root of f. We will prove that $O(G_i(\underline{x}, y(\underline{x}))) = r_i$. Moreover, we will prove that G_i is a free polynomial in $\mathbb{K}_C[[\underline{x}]][y]$ for all $i \in \{1, ..., h\}$, and we will find the relation between the characteristic exponents of f and those of G_i.

Definition 34 *Let the notation be as above, and let m be one of the exponents of y. Then an $m-$truncation of y is defined to be $y_{<m} := \sum_{p<m} c_p \underline{x}^{\frac{p}{n}}$ with $p \in Supp(y)$.*

By $p < m$ we mean that $p \leq m$ with respect to the defined order on C and $p \neq m$. Note that since C is a line free cone, $y_{<m}$ is a finite sum of monomials, and it is obviously an element in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]] \subset L_n$.

Definition 35 *Let the notation be as above with $\{m_1, ..., m_h\}$ the set of characteristic exponents of y. For all $i = 1, ..., h$ let $y_{<m_i}$ be the m_i-truncation of y, then the i-th pseudo-root of f is defined to be the minimal polynomial of $y_{<m_i}$ over L.*

Proposition 38 *Let the notation be as above. For all $i = 1, ..., h$ let G_i be i-th pseudo-root of f, then $deg_y(G_i) = \frac{n^e}{D_i} = \frac{n}{d_i}$.*

Proof : By Proposition 35 we have $L(y_{<m_i}) = L(M_1, .., M_{i-1})$. By a similar argument as in the proof of Proposition 37, we get :

$$deg_y(G_i) = [L(y_{<m_i}) : L] = [L(M_1, ..., M_{i-1}) : L] = \frac{n^e}{D_i}. \blacksquare$$

For all $i = 1, ..., h$ the $i - th$ pseudo-root G_i splits completely in L_n. Moreover the conjugates of $y_{<m_i}$ over L are $\theta(y_{<m_i})$, with $\theta \in Aut(L_n/L)$, which are elements of $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$, then G_i has $\frac{n^e}{D_i}$ roots in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. Let $z_1, ..., z_{\frac{n^e}{D_i}}$ be the roots of G_i, then

$$G_i = \prod_{i=1}^{\frac{n^e}{D_i}} (y - z_i) \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]][y]$$

but $G_i \in L$, hence $G_i \in \mathbb{K}_C[[\underline{x}]][y]$.

Proposition 39 *Let the notation be as above with f a free polynomial of degree n and $y = y(\underline{x}^{\frac{1}{n}})$ a root of f, then :*

$$f(\underline{x}, Y)^{n^{e-1}} = \prod_{\theta \in Aut(L_n/L)} (Y - \theta(y))$$

Proof : Let $\{y_1, ..., y_n\}$ be the conjugates of y over L. For all $i = 1, .., n$ set :

$$A_i = \{\theta \in Aut(L_n/L), \theta(y) = y_i\} \text{ and } a_i = \#(A_i).$$

We have $\theta \in A_1$ if and only if $\theta \in Aut(L_n/L)$ and $\theta(y) = y_1 = y$ if and only if $\theta \in Aut(L_n/L(y))$, hence :

$$\#(A_1) = \#Aut(L_n/L(y)) = [L_n : L(y)].$$

But $[L_n : L(y)][L(y) : L] = [L_n : L]$ with $[L_n : L] = n^e$ and $[L(y) : L] = deg(f) = n$, then $[L_n : L(y)] = \frac{n^e}{n} = n^{e-1}$ and so $a_1 = \#(A_1) = n^{e-1}$.
Write $A_1 = \{\beta_1, ..., \beta_{n^{e-1}}\}$ and we want to prove that $\#(A_i) = \#(A_1) = n^{e-1}$ for all $i = 1, .., n$. Let y_i be a conjugate of y other than y. Since L_n/L is a normal extension then there existes some $\alpha_i \in Aut(L_n/L)$ such that $\alpha_i(y) = y_i$. For all $i = 1, ..., n^{e-1}$ we have $\alpha_i \circ \beta_j(y) = \alpha_i(y) = y_i$ and so $\alpha_i \circ \beta_j \in A_i$. Moreover, if $j \neq k$, then $\alpha_i \circ \beta_j \neq \alpha_i \circ \beta_k$, hence $a_i = \#(A_i) \geq \#(A_1) = a_1 = n^{e-1}$. If $a_l > a_1 = n^{e-1}$ for some $l = 2, ..., n$, then $\sum_{l=1}^{n} a_l > n^e$, but $\sum_{l=1}^{n} a_l = n^e$, this is a contradiction. It follows that for all $i = 1, ..., n$ we have $a_i = a_1 = n^{e-1}$.
Hence for all $i = 1, ..., n$ A_i can be written as

$$A_i = \{\theta_i^j, 1 \leq j \leq n^{e-1}\}$$

Hence :

$$\prod_{\theta \in Aut(L_n/L)} (Y - \theta(y)) = \prod_{j=1}^{n^{e-1}} \prod_{i=1}^{n} (Y - \theta_i^j(y)) = \prod_{j=1}^{n^{e-1}} \prod_{i=1}^{n} (Y - y_i) = \prod_{j=1}^{n^{e-1}} f = f^{n^{e-1}}$$

Hence the proof is completed. ■

Proposition 40 *Let the notation be as above. For all $i = 1, ..., h$ let $G_i(\underline{x}, Y)$ be the i-th pseudo root of f. Then*

$$(G_i(\underline{x}, Y))^{D_i} = \prod_{\theta \in Aut(L_n/L)} (Y - \theta(y_{<m_i}))$$

Proof : Let $y_1, ..., y_{\frac{n^e}{D_i}}$ be the conjugates of $y_{<m_i}$ with $y_1 = y_{<m_i}$. For all $i = 1, ..., \frac{n^e}{D_i}$ set :

$$A_j = \{\theta \in Aut(L_n/L),\ \theta(y_{<m_i}) = y_j\} \text{ and } a_j = \#A_j$$

For each $j = 1, ..., \frac{n^e}{D_i}$ there exists $\alpha_j \in Aut(L_n/L)$ such that $\alpha_j(y_1) = y_j$, so we define the set $\{\alpha_j \circ \theta, \theta \in A_1\}$ and we denote it by $\alpha_j \circ A_1$. We want to prove that $A_j = \alpha_j \circ A_1$.
Let $\theta \in A_1$, we have $\theta(y_1) = y_1$, hence $\alpha_j \circ \theta(y_1) = \alpha_j(y_1) = y_j$. But $\alpha_j, \theta \in Aut(L_n/L)$, then $\alpha_j \circ \theta \in Aut(L_n/L)$, and so $\alpha_j \circ \theta \in A_j$ this implies that $\alpha_j \circ A_1 \subset A_j$.
Now let $\beta \in A_j$, then $\beta(y_1) = y_j$. Write $\beta = \alpha_j \circ (\alpha_j^{-1} \circ \beta)$. Then :

$$\alpha_j((\alpha_j^{-1} \circ \beta)(y_1)) = \beta(y_1) = y_j = \alpha_j(y_1)$$

But α_j is injective, then $(\alpha_j^{-1} \circ \beta)(y_1) = y_1$, hence $\alpha_j^{-1} \circ \beta \in A_1$. It follows that $\beta = \alpha_j \circ (\alpha_j^{-1} \circ \beta) \in \alpha_j \circ A_1$. Then $A_j \subset \alpha_j \circ A_1$. Finally we get that $A_j = \alpha_j \circ A_j$.
Now $A_1 = \{\theta \in Aut(L_n/L), \theta(y_{<m_i}) = y_{<m_i}\} = Aut(L_n/L(y_{<m_i})) = Aut(L_n/L(M_1, ..., M_{i-1}))$ by Proposition 35. Hence $a_1 = \#A_1 = \#Aut(L_n/L(M_1, ..., M_{i-1})) = D_i$ but since $\forall \theta_1, \theta_2 \in A_1$ and $\theta_1 \neq \theta_2$ we have $\alpha_j \circ \theta_1 \neq \alpha_j \circ \theta_2$ then $a_j = \#A_j = \#A_1 = a_1 = D_i$. Write $A_j = \{\theta_j^k, 1 \leq k \leq D_i\}$, we get :

$$\prod_{\theta \in Aut(L_n/L)} (Y - \theta(y_{<m_i})) = \prod_{k=1}^{D_i} \prod_{j=1}^{\frac{n^e}{D_i}} (Y - \theta_j^k(y_{<m_i})) = \prod_{k=1}^{D_i} \prod_{j=1}^{\frac{n^e}{D_i}} (Y - y_j) = \prod_{k=1}^{D_i} G = G^{D_i}. \blacksquare$$

Lemma 18 *Let the notation be as above with $y \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ a root of a free polynomial $f \in \mathbb{K}_C[[\underline{x}]][y]$, and let $\{m_1, ..., m_h\}$ be the set of characteristic exponents of y and $\{D_1, ..., D_{h+1}\}$ be its GCD sequence. For all $1 \leq i \leq h$ set $S_i = m_1 \cdot D_1 + \sum_{j=1}^{i}(m_j - m_{j-1})D_j$ then we have :*

$$O(\prod_{\theta \in Q(i)}(y - \theta(y))) = S_{i-1} - m_{i-1} \cdot D_i.$$

Proof : We have $\theta \in Q(i)$ if and only if $O(y - \theta(y)) < m_i$ if and only if $O(y - \theta(y)) = m_j$ for some $j \in \{1, ..., i-1\}$. It follows that $Q(i) = \cup_{j=1}^{i-1} S(j)$. Hence

$$\prod_{\theta \in Q(i)}(y - \theta(y)) = \prod_{j=1}^{i-1}\prod_{\theta \in S(j)}(y - \theta(y)).$$

By Proposition 37 we have $\#(S(j)) = D_j - D_{j+1}$, and so for all $j = 1, ..., i-1$ we have :

$$O(\prod_{\theta \in S(j)}(y - \theta(y))) = (D_j - D_{j+1})m_j.$$

Hence :

$$\begin{aligned} O(\prod_{\theta \in Q(i)}(y - \theta(y))) &= (D_1 - D_2)m_1 + (D_2 - D_3)m_2 + ... + (D_{i-1} - D_i)m_{i-1} \\ &= D_1 m_1 + D_2(m_2 - m_1) + ... + D_{i-1}(m_{i-1} - m_{i-2}) + D_i m_{i-1} \\ &= S_{i-1} - m_{i-1} \cdot D_i. \blacksquare \end{aligned}$$

Definition 36 *Let y be a formal power series in $\mathbb{K}_C[[\underline{x}]]$. Let $\leq$ be an order which is compatible with C, and let $LM(y)$ and $LC(y)$ be the leading monomial and the leading coefficient of y with respect to this order. The initial form of y with respect to this order is defined to be : $Info(y) := LC(y) \cdot LM(y)$.*

Definition 37 *Let the notation be as above with $\{m_1, ..., m_h\}$ the set of characteristic exponents of y, and $Z \neq 0$ an indeterminate. Let $i \in \{1, ..., h\}$, by an (i, Z)-deformation of y we mean an element $y^* \in \mathbb{K}'(Z)_C[[\underline{x}^{\frac{1}{n}}]]$ where $\mathbb{K}'$ is an overfield of $\mathbb{K}$, such that $Info(y^* - y_{<m_i}) = Z \cdot \underline{x}^{\frac{m_i}{n}}$. Note that the initial form is taken with respect to the chosen order on C.*

Proposition 41 *Let f be a free polynomial with a root y. Let $\{m_1, ..., m_h\}$ be the set of characteristic exponents of y, and for all $1 \leq i \leq h$ let G_i be the i-th pseudo root of f and y^* be an (i, Z) deformation of y. Then :*

$$Info(G_i(\underline{x}, y^*)) = c \cdot Z \cdot \underline{x}^{\frac{r_i}{n}}.$$

Where $c \in \mathbb{K}$ is a non zero constant.

Proof : By Proposition 40 we have :

$$G_i(\underline{x}, y^*)^{D_i} = \prod_{\theta \in Aut(L_n/L)}(y^* - \theta(y_{<m_i})).$$

Since $Aut(L_n/L)$ is the disjoint union of $R(i)$ and $Q(i)$), then :

$$\begin{aligned} Info(G_i(\underline{x}, y^*))^{D_i} &= Info(\prod_{\theta \in Aut(L_n/L)}(y^* - \theta(y_{<m_i}))) \\ &= Info(\prod_{\theta \in Q(i))}(y^* - \theta(y_{<m_i}))) \cdot Info(\prod_{\theta \in R(i)}(y^* - \theta(y_{<m_i}))). \end{aligned}$$

Consider the equation :

$$y^* - \theta(y_{<m_i}) = (y^* - y_{<m_i}) + (y_{<m_i} - y) + (y - \theta(y)) + (\theta(y) - \theta(y_{<m_i}))$$

For all $\theta \in Aut(L_n/L)$ we have $O(\theta(y) - \theta(y_{<m_i})) = O(\theta(y - y_{<m_i})) = O(y - y_{<m_i}) = m_i$, also by the definition of the deformation y^*, we have $O(y^* - y_{<m_i}) = m_i$. Then :

(i) If $\theta \in Q(i)$, we have $Info(y^* - \theta(y_{<m_i})) = Info(y - \theta(y))$, and using Lemma 18 we get :

$$Info \prod_{\theta \in Q(i)} (y^* - \theta(y_{<m_i})) = Info \prod_{\theta \in Q(i)} (y - \theta(y)) = \lambda \cdot \underline{x}^{\frac{S_{i-1} - m_{i-1}D_i}{n}} \tag{2.3}$$

Where λ is a non zero constant in $\mathbb{K}$.

(ii) If $\theta \in R(i)$, then $\theta(y_{<m_i}) = y_{<m_i}$, and so $Info(y^* - \theta(y_{<m_i})) = Info(y^* - y_{<m_i}) = Z \cdot \underline{x}^{\frac{m_i}{n}}$. But $card(R(i)) = D_i$, then :

$$Info \prod_{\theta \in R(i)} (y^* - \theta(y_{<m_i})) = \prod_{\theta \in R(i)} Info(y^* - \theta(y_{<m_i})) = \prod_{i=1}^{D_i} (Z \cdot \underline{x}^{\frac{m_i}{n}}) = Z^{D_i} \cdot \underline{x}^{\frac{m_i D_i}{n}}$$

Combining (i) and (ii) we get :

$$\begin{aligned} Info(G_i(\underline{x}, y^*))^{D_i} &= Info \prod_{\theta \in Q(i)} (y^* - \theta(y_{<m_i})) \cdot Info \prod_{\theta \in R(i)} (y^* - \theta(y_{<m_i})) \\ &= \lambda \cdot \underline{x}^{\frac{S_{i-1} - m_{i-1}D_i}{n}} \cdot Z^{D_i} \cdot \underline{x}^{\frac{m_i D_i}{n}} \\ &= \lambda \cdot Z^{D_i} \cdot \underline{x}^{\frac{S_{i-1} - m_{i-1}D_i + m_i D_i}{n}} = \lambda \cdot Z^{D_i} \cdot \underline{x}^{\frac{S_i}{n}} = \lambda \cdot Z^{D_i} \cdot \underline{x}^{\frac{r_i D_i}{n}} \end{aligned}$$

Hence $Info(G_i(\underline{x}, y^*)) = c \cdot Z \cdot \underline{x}^{\frac{r_i}{n}}$ for some $c \in \mathbb{K}^*$. Moreover, $O(G_i(\underline{x}, y^*)) = r_i$.■
As a corollary of Proposition 41 we get the following :

Corollary 2 *Let the notation be as in Proposition* 41. *We have* $O(G_i(\underline{x}, y(x))) = r_i$.

Proof : In fact, $y(\underline{x}) = y^*(\underline{x})|_{Z=1}$. Hence the result follows.

Proposition 42 *Let* f *be a free polynomial in* $\mathbb{K}_C[[\underline{x}]][y]$, *and let* G_i *be the* i*-th pseudo root of* f, *where* $i \in \{1, ..., h\}$. *Then* G_i *is a free polynomial. In particular its root* $y_{<m_i} \in \mathbb{K}_C[[\underline{x}^{\frac{1}{\frac{n}{d_i}}}]]$ *and its characteristic exponents are* $\frac{m_1}{d_i}, ..., \frac{m_{i-1}}{d_i}$.

Proof : We want to prove that $y_{<m_i} \in \mathbb{K}_C[[\underline{x}^{\frac{1}{\frac{n}{d_i}}}]]$. Let $\underline{x}^{\frac{\lambda}{n}}$ be a monomial of $y_{<m_i}$, then $\lambda \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$. Let D be the *gcd* of the minors of the matrix $(m_0^1, ..., m_0^e, m_1, ..., m_{i-1}, \lambda)$, then by Proposition 16 we have $D = D_i$. For all $l \in \{1, ..., e\}$ the matrix $A_l = (m_0^1, ..., m_0^{l-1}, \lambda, m_0^{l+1}, ..., m_e)$ is one of the minors of the matrix $(m_0^1, ..., m_0^e, m_1, ..., m_{i-1})$, then D_i divides $Det(A_l)$ for all $l \in \{1, .., e\}$. Write $\lambda = (\lambda_1, ..., \lambda_e)$, then obviously $Det(A_l) = n^{e-1}\lambda_l$, and so D_i divides $n^{e-1}\lambda_l$ for all $l \in \{1, ..., e\}$. It follows that D_i divides $n^{e-1}\lambda$, and so $\frac{n^{e-1}\lambda}{D_i} = \frac{\lambda}{d_i} \in \mathbb{Z}^e$. Moreover, since $\lambda \in C$, and $\frac{1}{d_i} \geq 0$, then $\frac{\lambda}{d_i} \in C$. It follows that $\underline{x}^{\frac{\lambda}{n}} = \underline{x}^{\frac{\lambda'}{\frac{n}{d_i}}}$ where $\lambda' = \frac{\lambda}{d_i}$, and so $\underline{x}^{\frac{\lambda}{n}} \in \mathbb{K}_C[[\underline{x}^{\frac{1}{\frac{n}{d_i}}}]]$.
Let $\theta(y_{<m_i})$ be a conjugate of $y_{<m_i}$, then obviously $LM(\theta(y_{<m_i}) - y_{<m_i}) = \underline{x}^{\frac{m_j}{n}}$ for some $j \in \{1, ..., i-1\}$. But $\frac{m_j}{n} = \frac{\frac{m_j}{d_i}}{\frac{n}{d_i}}$, hence the set of characteristic monomials of $y_{<m_i}$ is $\{\frac{m_1}{d_i}, ..., \frac{m_{i-1}}{d_i}\}$.■

2.4.5 The initial form of the approximate roots of f

Let the notation be as above with f a free polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$ and let $y(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$ be a root of $f(\underline{x}^n, y) = 0$. Let $g \in \mathbb{K}_C[[\underline{x}]][y]$ such that f does not divide g. From now on we will write $O(f, g)$ for the smallest element in the set $Supp(g(\underline{x}^n, y(\underline{x})))$ with respect to the given order on the cone. Note that if $z(\underline{x})$ is another root of f, then $z = \theta(y)$ for some $\theta \in Aut(L_n \backslash L)$, and so $g(\underline{x}^n, z(\underline{x})) = g(\underline{x}^n, \theta(y(\underline{x}))) = \theta(g(\underline{x}^n, y(\underline{x})))$. But $Supp(g(\underline{x}^n, y(\underline{x}))) = Supp(\theta(g(\underline{x}^n, y(\underline{x}))))$. It follows that $O(f, g)$ does not depend on the choice of the root of f. Note also that if g_1, g_2 are nonzero elements of $\mathbb{K}_C[[\underline{x}]][y]$, which are not divisible by f, then $O(f, g_1 g_2) = O(f, g_1) + O(f, g_2)$.
Now for each polynomial g such that f does not divide g, we will consider $O(f, g)$. We will prove that the set of such elements form a semigroup. Moreover, if $\deg_y(g) < \frac{n}{d_i}$, then $O(f, g) \in < r_0^1, ..., r_0^e, r_1, ..., r_{i-1} >$. For all $i \in \{1, ..., h\}$ we will take g_i to be the d_i-th approximate root of f, where $\{d_1, ..., d_h\}$ is the $d-$sequence of f. We will prove that $r_i = O(f, g_i)$ for all $i \in \{1, ..., h\}$. The following Proposition shows that $O(f, G_i) = r_i$ if G_i is the i-th pseudo-root of f.

Proposition 43 *Let $i \in \{1, \ldots, h\}$ and let G_i be the i-th pseudo-root of f. We have $O(f, G_i) = r_i$.*

Proof : This is an immediate consequence of Corollary 2.

Proposition 44 *Let f be a free polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$, and let $\{G_1, ..., G_h\}$ be the set of pseudo roots of f. Let $i \in \{1, ..., h\}$, then we have $O(G_i, G_j) = \frac{r_j}{d_i}$ for all $j \in \{1, ..., i-1\}$.*

Proof : Let $y \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ be a root of f, and let $\{m_1, ..., m_h\}$ be its set of characteristic exponents, and let $\{d_1, ..., d_h\}$ be its $d-$sequence. For all $j = 1, ..., i-1$ the $\frac{m_j}{d_i}$ truncation of $y_{<m_i}$ is obviously $y_{<m_j}$. By Proposition 42 we have that $\frac{m_1}{d_i}, ..., \frac{m_{i-1}}{d_i}$ are the characteristic exponents of G_i. It follows directly that the pseudo-roots of G_i are $\{G_1, ..., G_{i-1}\}$. Let $D'_1, ..., D'_i$ be the $GCD-$sequence of G_i. Then

$$D'_j = GCD(\frac{r_0^1}{d_i}, ..., \frac{r_0^e}{d_i}, \frac{m_1}{d_i}, ..., \frac{m_{i-1}}{d_i}) = \frac{1}{d_i} D_j$$

for all $j \in \{1, ..., i\}$. Let $\{e'_j\}_{1 \leq j \leq i-1}$ be the $e-$sequence of G_i. We have $d'_j = \frac{D'_j}{D'_i} = \frac{\frac{D_j}{d_i}}{\frac{D_i}{d_i}} = \frac{D_j}{D_i}$. Hence $e'_j = \frac{D'_j}{D'_{j+1}} = \frac{D_j}{D_{j+1}} = e_j$. Let $\{\alpha_0^1, ..., \alpha_0^e, r'_1, ..., r'_{i-1}\}$ be the $r-$sequence of G_i where $\{\alpha_0^1, ..., \alpha_0^e\}$ is the canonical basis of $(\frac{n}{d_i}\mathbb{Z})^e$. Then $\alpha_0^1 = \frac{r_0^1}{d_i}, ..., \alpha_0^e = \frac{r_0^e}{d_i}$ and $r'_1 = m'_1 = \frac{m_1}{d_i} = \frac{r_1}{d_i}$. Suppose that $r'_k = \frac{r_k}{d_i}$ for $k = 1, ..., j$, then

$$r_{j+1} = e'_j r'_j + m'_{j+1} - m'_j = e_j \frac{r_j}{d_i} + \frac{m_{j+1}}{d_i} - \frac{m_j}{d_i} = \frac{1}{d_i}(e_j r_j + m_{j+1} - m_j) = \frac{r_{j+1}}{d_i}.$$

It follows that the $r-$sequence of G_i is equal to $\{\frac{r_0^1}{d_i}, ..., \frac{r_0^e}{d_i}, \frac{r_1}{d_i}, ..., \frac{r_{i-1}}{d_i}\}$. Finally by Proposition 43 we get $O(G_i, G_j) = \frac{r_j}{d_i}$ for all $j \in \{1, ..., i-1\}$.■
Recall that for all $H \in \mathbb{K}_C[[\underline{x}]][y]$ the expansion of H with respect to $(G_1, ..., G_h, f)$ is given by :

$$H = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \ldots G_h^{\theta_h} f^{\theta_{h+1}}$$

Where $\underline{\theta} = (\theta_1, ..., \theta_{h+1})$ with $0 \leq \theta_i < e_i = \frac{d_i}{d_{i+1}}$ for all $i = 1, ..., h$ and $\theta_{h+1} \in \mathbb{N}$. Moreover we have the following proposition :

Lemma 19 *Let f a free polynomial in $\mathbb{K}_C[[\underline{x}]][y]$, and let $g \in \mathbb{K}_C[[\underline{x}]][y]$ be such that g is not a multiple of f. Let $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \ldots G_h^{\theta_h} f^{\theta_{h+1}}$ be the expansion of g with respect to $(G_1, ..., G_h, f)$. Then there exists a unique $\underline{\theta} \in A$ such that $O(f, g) = O(f, c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \ldots G_h^{\theta_h} f^{\theta_{h+1}})$.*

Proof : Note that the expansion of g with respect to $(G_1, ..., G_h, f)$ is given by $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h} f^{\theta_{h+1}}$ with $\underline{\theta} = (\theta_1, ..., \theta_{h+1}) \in A = \{(\beta_1, ..., \beta_{h+1}),\ \ 0 \leq \beta_j < e_j\ \forall j = 1, ..., h,\ \theta_{h+1} \in \mathbb{N}\}$. Let $c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h}$, $c_{\underline{\theta'}}(\underline{x}) G_1^{\theta'_1} \dots G_h^{\theta'_h}$ be two distinct elements of g, and let $\underline{\theta}_0 = O(f, c_{\underline{\theta}}(\underline{x}))$ and $\underline{\theta}'_0 = O(f, c_{\underline{\theta'}}(\underline{x}))$. Suppose that $O(f, c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h}) = O(f, c_{\underline{\theta'}}(\underline{x}) G_1^{\theta'_1} \dots G_h^{\theta'_h})$, that is $\underline{\theta}_0 + \sum_{i=1}^h \theta_i r_i = \underline{\theta}'_0 + \sum_{i=1}^h \theta'_i r_i$ and let j be the greatest element such that $\theta_j \neq \theta'_j$, and suppose that $\theta_j > \theta'_j$. Then

$$(\theta_j - \theta'_j) r_j = (\underline{\theta}'_0 - \underline{\theta}_0) + \sum_{k=1}^{j-1} (\theta'_k - \theta_k) r_k$$

with $0 < \theta_j - \theta'_j < e_j$, which is a contradiction because e_j is the smallest positive integer α such that $\alpha r_j \in (n\mathbb{Z})^e + \sum_{k=1}^{j-1} r_k \mathbb{Z}$ (see Proposition 36). Now If $\theta_{h+1} \neq 0$ for all $\underline{\theta}$ with $c_{\underline{\theta}}(\underline{x}) \neq 0$, then $g = h.f$ for some $h \in \mathbb{K}_C[[\underline{x}]][y]$, and so f divides g which contradicts the hypothesis. It follows that there exists at least an element $\underline{\theta} \in A$ with $c_{\underline{\theta}}(\underline{x}) \neq 0$ which is of the form $(\theta_1, ..., \theta_h, 0)$, and by the above discussion we conclude that there exists a unique $c_\gamma(\underline{x}) G_1^{\gamma_1} \dots G_h^{\gamma_h}$ such that

$$O(f, g) = O(f, c_\gamma(\underline{x}) G_1^{\gamma_1} \dots G_h^{\gamma_h}) = \gamma_0 + \sum_{i=1}^h \gamma_i r_i = inf\{O(f, c_{\underline{\theta}} G_1^{\theta_1} \dots G_h^{\theta_h}),\ c_{\underline{\theta}} \neq 0\}$$

by the additive property of O, where $\gamma_0 = O(f, c_\gamma(\underline{x})) = \sum_{i=1}^e \lambda_0^i r_0^i$ for some $\lambda_0^1, ..., \lambda_0^e \in \mathbb{Z}$.■

Remark 13 *Note that Lemma* 19 *is equivalent to saying that if f is a free polynomial and f does not divide g, there exist unique $\lambda_0^1, ..., \lambda_0^e, \lambda_1, ..., \lambda_h \in \mathbb{Z}$ such that $O(f, g) = \sum_{i=1}^e \lambda_0^i r_0^i + \sum_{i=1}^h \lambda_i r_i$ with $0 \leq \lambda_i < e_i$ for all $i \in \{1, ..., h\}$.*

Proposition 45 *Let the notation be as above, and consider a non zero polynomial F in $\mathbb{K}_C[[\underline{x}]][y]$ such that $deg_y(F) < \frac{n}{d_i}$ for some $1 \leq i \leq h$. Then $O(f, F) \in (n\mathbb{Z})^e + r_1\mathbb{N} + \ldots + r_{i-1}\mathbb{N}$.*

Proof : Since $deg_y(F) < \frac{n}{d_i}$, then the expansion of F with respect to $(G_1, ..., G_h, f)$ is given by :

$$F = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} ... G_{i-1}^{\theta_{i-1}}.$$

Where $\underline{\theta} = (\theta_1, ..., \theta_{i-1}) \in B = \{(\beta_1, ..., \beta_{i-1}),\ \ 0 \leq \beta_j < e_j = \frac{d_j}{d_{j+1}}\ \forall j = 1, ..., i-1\}$. Similar to Lemma 19, we can prove that there exists a unique $c_\gamma(\underline{x}) G_1^{\gamma_1} \dots G_{i-1}^{\gamma_{i-1}}$ such that

$$O(f, F) = O(f, c_\gamma(\underline{x}) G_1^{\gamma_1} \dots G_{i-1}^{\gamma_{i-1}}) = \gamma_0 + \sum_{i=1}^{i-1} \gamma_i r_i = inf\{O(f, c_{\underline{\theta}} G_1^{\theta_1} \dots G_{i-1}^{\theta_{i-1}}),\ c_{\underline{\theta}} \neq 0\}$$

where $\gamma_0 = O(f, c_\gamma(\underline{x})) = \sum_{i=1}^e \lambda_0^i r_0^i$ for some $\lambda_0^1, ..., \lambda_0^e \in \mathbb{Z}$. Hence we get the result.■

Proposition 46 *Let the notation be as above with $\{G_1, ..., G_h\}$ the set of pseudo-roots of f. Let $g \in \mathbb{K}_C[[\underline{x}]][y]$ such that $deg_y(g) < \frac{n}{d_i}$ for some $i \in \{1, ..., h\}$. Then $O(f, g) = d_i O(G_i, g)$.*

Proof : Let $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h} f^{h+1}$ be the expansion of g with respect to $(G_1, ..., G_h, f)$. Since $deg_y(g) < deg_y(G_i) = \frac{n}{d_i}$, then the expansion of g with respect to $(G_1, ..., G_h, f)$ coincides with the expansion of g with respect to $(G_1, ..., G_{i-1})$. In particular for all $\underline{\theta}$ such that $c_{\underline{\theta}}(\underline{x}) \neq 0$ we have $\underline{\theta} = (\theta_1, ..., \theta_{i-1}, 0, ..., 0)$. Since $deg_y(g) < \frac{n}{d_i}$, then by Proposition 45 there exists a unique $c_{\underline{\theta}^0}(\underline{x}) G_1^{\theta_1^0} \dots G_{i-1}^{\theta_{i-1}^0}$ such that :

$$O(f, g) = O(f, c_{\underline{\theta}^0}(\underline{x}) G_1^{\theta_1^0} \dots G_{i-1}^{\theta_{i-1}^0}) = O(f, c_{\underline{\theta}^0}(\underline{x})) + \sum_{j=1}^{i-1} \theta_j^0 r_j$$

Also by Proposition 45 we have

$$O(G_i, g) = inf\{O(G_i, c_{\underline{\theta}} G_1^{\theta_1} \dots G_{i-1}^{\theta_{i-1}}),\ c_{\underline{\theta}} \neq 0\}$$

By Proposition 44 we have $O(G_i, G_j) = \frac{r_j}{d_i}$ for all $j \in \{1, ..., i-1\}$, also we have $O(G_i, c_{\underline{\theta}}(\underline{x})) = \frac{1}{d_i} O(f, c_{\underline{\theta}}(\underline{x}))$, then $O(G_i, g) = O(G_i, c_{\underline{\theta}^0}(\underline{x})) + \sum_{j=1}^{i-1} \theta_j \frac{r_j}{d_i} = \frac{1}{d_i}(O(f, c_{\underline{\theta}}(\underline{x})) + \sum_{j=1}^{i-1} \theta_j r_j) = \frac{1}{d_i} O(f, g)$.■
Let f be a polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$, and let $d_1 > \ldots > d_{h+1}$ be the set of divisors of n. For all $i \in \{1, ..., h\}$ set $e_i = \frac{d_i}{d_{i+1}}$. Let $i \in \{1, ..., h\}$ and consider a monic polynomial G_i of degree $\frac{n}{d_i}$. Let

$$f = G_h^{d_h}(\underline{x}, y) + C_1(\underline{x}, y) G_h^{d_h - 1}(\underline{x}, y) + \ldots + C_{d_h}(\underline{x}, y).$$

be the G_i-adic expansion of f. Recall that, with the notation and results of Section 2.3, the Tshirnhausen transform of G_i with respect to f, denoted by $\tau_f(G_i)$ is the polynomial

$$\tau_f(G_i) = G_i + \frac{1}{d_i} C_1$$

Obviously $\deg_y(\tau_f(G_i)) = \frac{n}{d_i}$. Hence we can define for all $j \geq 2$, the $j-th$ Tshirnhausen transform of G_i with respect to f, denoted by $\tau_f^j(G_i) = \tau_f(\tau_f^{j-1}(G_i))$.
Also recall that for all $i \in \{1, ..., h\}$, there exists a unique polynomial g_i of degree $\frac{n}{d_i}$ such that $\deg(f - g_i^{d_i}) < n - \frac{n}{d_i}$, this polynomial is called the d_i-th approximate root of f, and denoted by $App_{d_i}(f)$. Moreover, recall that, by Proposition 6 $App_{d_i}(f)$ exists and it is unique for all $i \in \{1, \ldots, h\}$.

Proposition 47 *Let f be a free polynomial of degree n in $\mathbb{K}_C[[\underline{x}]][y]$, and let $\{d_i\}_{1 \leq i \leq h}$ and $\{r_i\}_{1 \leq i \leq h}$ be its $d-$sequence and $r-$sequence respectively. Let $\{g_1, ..., g_h\}$ be the set of approximate roots of f. Then for all $i \in \{1, ..., h\}$ we have $O(f, g_i) = r_i$.*

Proof : Let $\{G_1, ..., G_h\}$ be the set of pseudo-roots of f. Let $i = h$ and consider the G_h-adic expansion of f :

$$f = G_h^{d_h}(\underline{x}, y) + C_1(\underline{x}, y) G_h^{d_h - 1}(\underline{x}, y) + \ldots + C_{d_h}(\underline{x}, y).$$

where $C_k(\underline{x}, y) \in \mathbb{K}_C[[\underline{x}]][y]$ with $deg_y(C_k(\underline{x}, y)) < \frac{n}{d_h}$ for all $k = 1, ..., d_h$. Consider the Tschirnhausen transform of G_h with respect to f

$$\tau_f G_h(\underline{x}, y) = G_h(\underline{x}, y) + d_h^{-1} C_1(\underline{x}, y).$$

We have $O(f, G_h) = r_h$. We want to prove that $O(f, C_1) > r_h$. Taking $C_0 = 1$ we get that $f(\underline{x}, y) = \sum_{k=0}^{d_h} C_k(\underline{x}, y) \cdot G_h(\underline{x}, y)^{d_h - k}$.
For all $\alpha \neq k \in \{0, ..., d_h - 1\}$ we have $O(f, C_\alpha G_h^{d_h - \alpha}) \neq O(f, C_k G_h^{d_h - k})$. In fact, suppose that $O(f, C_\alpha G_h^{d_h - \alpha}) = O(f, C_k G_h^{d_h - k})$, that is $O(f, C_\alpha) + (d_h - \alpha) r_h = O(f, C_k) + (d_h - k) r_h$. Suppose that $\alpha > k$, then $(\alpha - k) r_h = O(f, C_\alpha) - O(f, C_k)$. But $deg_y(C_\alpha), deg_y(C_k) < \frac{n}{d_h}$, then by proposition 45 we get $O(f, C_\alpha), O(f, C_k) \in (n\mathbb{Z})^e + r_1\mathbb{Z} + \ldots + r_{h-1}\mathbb{Z}$, and so $(\alpha - k) r_h \in (n\mathbb{Z})^e + r_1\mathbb{Z} + \ldots + r_{h-1}\mathbb{Z}$, with $0 < \alpha - k < d_h$. But by Remark 12 we have $d_{h+1} = 1$, and so $e_h = \frac{d_h}{d_{h+1}} = d_h$, hence $0 < \alpha - k < e_h$. Which is a contradiction since $j r_h \notin (n\mathbb{Z})^e + r_1\mathbb{Z} + \ldots + r_{h-1}\mathbb{Z}$ for all $0 < j < e_h$ (see Proposition 36).
Similarly, for all $k \in \{1, ..., d_h - 1\}$ we have $0 \leq d_h - k < d_h = e_h$ and $O(f, C_k) \in (n\mathbb{Z})^e + r_1\mathbb{Z} + \ldots + r_{h-1}\mathbb{Z}$. Hence $O(f, C_k G_h^{d_h - k}) = O(f, C_k) + (d_h - k) r_h \neq O(f, C_{d_h})$, otherwise we will get that $(d_h - k) r_h = O(f, C_{d_h}) - O(f, C_k) \in (n\mathbb{Z})^e + r_1\mathbb{Z} + \ldots + r_{h-1}\mathbb{Z}$, which is a contradiction again by Proposition 36. For all $k \in \{0, ..., d_h\}$ Let $M_k = LM(C_k G_h^{d_h - k}(\underline{x}^n, y(\underline{x})))$ and suppose that for some $l \in \{1, ..., d_h - 1\}$ we have $0 \neq M_l < M_{d_h}$. Moreover suppose that M_l is the smallest element in the set $M_1, ..., M_{d_h - 1}$. Since $M_l \neq M_k$ for all $k \in \{0, ..., d_h\}$ with $k \neq l$, it follows that $M_l = LM(f(\underline{x}^n, y(\underline{x})))$, but $f(\underline{x}^n, y(\underline{x})) = 0$, which is a contradiction. Hence $M_1 < M_k$ for all $k \in \{1, ..., d_h - 1\}$, but $f(\underline{x}^n, y(\underline{x})) = 0$, and so $M_1 = M_{d_h}$. It follows that

$$O(f, G_h^{d_h}) = O(f, C_{d_h})\ and\ O(f, G_h^{d_h}) < O(f, C_k G_h^{d_h - k}) \forall k \in \{1, ..., d_h - 1\}$$

In particular $O(f, G_h^{d_h}) = d_h r_h < O(f, C_1 G_h^{d_h-1}) = O(f, C_1) + (d_h - 1)r_h$, and so $O(f, C_1) > r_h$. It follows that

$$O(f, \tau_f G_h) = O(f, G_h + \frac{1}{d_h} C_1) = O(f, G_h) = r_h.$$

Applying the same process as above to f and $\tau_f(G_h)$ instead of f and G_h we get that $O(f, \tau_f^2 G_h) = r_h$. Repeating this process consecutively, we get that $O(f, \tau_f^\lambda G_h) = r_h$ for all $\lambda \geq 1$. But $g_h = App_{d_h}(f) = \tau_f^{d_h}(G_h)$. Hence we get that $O(f, g_h) = r_h$.
Now suppose that $O(f, g_{i+1}) = r_{i+1}, ..., O(f, g_h) = r_h$, and let us prove that $O(f, g_i) = r_i$. By Proposition 7 we have that $g_i = App_{e_i}(g_{i+1})$. Since $\deg_y(G_i) = \frac{n}{d_i} = \frac{\deg_y(g_{i+1})}{e_i}$, then $g_i = App_{e_i}(g_{i+1}) = \tau_{g_{i+1}}^{e_i}(G_i)$. Let

$$g_{i+1} = G_i^{e_i}(\underline{x}, y) + \beta_1(\underline{x}, y) G_i^{e_i-1}(\underline{x}, y) + \ldots + \beta_{e_i}(\underline{x}, y) \tag{2.4}$$

be the G_i-adic expansion of g_{i+1}. We are given that $O(f, G_i) = r_i$ since G_i is a pseudo-root. Then by a similar discussion as above, and since we have by our hypothesis that $O(f, g_{i+1}) = r_{i+1}$ and $r_{i+1} \notin < r_0^1, ..., r_0^e, r_1, ..., r_i >$. We get that $O(f, G_i^{e_i}) = O(f, \beta_{e_i}) = e_i r_i$ and $O(f, \beta_1 G_i^{e_i-1}) > O(f, G_i^{e_i}) = e_i r_i$. Hence $O(f, \beta_1) + (e_i - 1)r_i > e_i r_i$, and so $O(f, \beta_1) > r_i$. It follows that

$$O(f, \tau_{g_{i+1}}(G_i)) = O(f, G_i + \frac{1}{e_i}\beta_1) = r_i$$

Applying the same process to f and $\tau_{g_{i+1}}(G_i)$ instead of f and G_i. We get that $O(f, \tau_{g_{i+1}}^2(G_i)) = r_i$. Repeating the same process we get that $O(f, g_i) = O(f, \tau_{g_{i+1}}^{e_i}(G_i)) = r_i$. It follows that $O(f, g_i) = r_i$ for all $i \in \{1, ..., h\}$. This completes the proof.■

Definition 38 *Let $f \in \mathbb{K}_C[[\underline{x}]][y]$ be a free polynomial. The semigroup of f is defined to be the set :*

$$\Gamma(f) = \{O(f, g),\ g \in \mathbb{K}_C[[\underline{x}]][y],\ f \text{ does not divide } g\}.$$

The fact that this set is a semigroup follows from the additive property of the order O.

Proposition 48 *Let $f \in \mathbb{K}_C[[\underline{x}]][y]$ be a free polynomial, and let $r_0^1, ..., r_0^e, r_1, ..., r_e$ be the $\underline{r}$-sequence associated to f. Then $\Gamma(f)$ is generated by the elements $r_0^1, ..., r_0^e, r_1, ..., r_e$.*

Proof : Let $g \in \mathbb{K}_C[[\underline{x}]][y]$ be a polynomial which is not a multiple of f, and let $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) g_1^{\theta_1} \ldots g_h^{\theta_h} f^{\theta_{h+1}}$ be the expansion of g with respect to $(g_1, ..., g_h, f)$, where $\{g_1, ..., g_h\}$ is the set of approximate roots of f. Then similar to Proposition 45, we can prove that there exists a unique $\lambda_0^1, ..., \lambda_0^e, \lambda_1, ..., \lambda_h$ such that $O(f, g) = \sum_{i=1}^e \lambda_0^i r_0^i + \sum_{i=1}^h \lambda_i r_i$ with $0 \leq \lambda_i < e_i$ for all $i \in \{1, ..., h\}$.■

3

Canonical bases of modules over one dimensional $\mathbb{K}$-algebras

3.1 Numerical semigroups and ideals.

3.1.1 Numerical semigroups.

Let $\{a_1, ..., a_n\}$ be a set of non-negative integers, and let $b \in \mathbb{N}$. Numerical semigroups arise in a natural way in the study of non-negative integer solutions to Diophantine equations of the form :

$$a_1x_1 + \cdots + a_nx_n = b$$

Note that $x_1, ..., x_n$ is a solution of the above Diophantine equation if and only if $x_1, ..., x_n$ is a solution of the Diophantine equation $\frac{a_1}{d}x_1 + \cdots + \frac{a_n}{d}x_n = \frac{b}{d}$, where $d = gcd(a_1, ..., a_n)$ is the greatest common divisor of $a_1, ..., a_n$. Hence the problem of finding solutions to Diophantine equations is reduced to the case where $gcd(a_1, ..., a_n) = 1$.

Definition 39 *Let S be a subset of $\mathbb{N}$. The set S is a submonoid of $\mathbb{N}$ if the following holds :*
(i) $0 \in S$.
(ii) If $a, b \in S$, then $a + b \in S$.

Clearly, $\{0\}$ and $\mathbb{N}$ are submonoids of $\mathbb{N}$. Also, if a is an element of S, then $\lambda a \in S$ for all $\lambda \in \mathbb{N}$. Hence if $S \neq \{0\}$, then S is an infinite set.

Definition 40 *Let S be a submonoid of $\mathbb{N}$, and let $G = \{\sum_{i=1}^{s} \lambda_i a_i,\ \lambda_i \in \mathbb{Z},\ a_i \in S\}$ be the subgroup of $\mathbb{Z}$ generated by S. If $1 \in G$, then we say that S is a numerical semigroup.*

Proposition 49 *Let S be a submonoid of $\mathbb{N}$. Then S is a numerical semigroup if and only if $\mathbb{N}\backslash S$ is a finite set.*

Proof : Let S be a numerical semigroup, and let $G = \{\sum_{i=1}^{s} \lambda_i a_i,\ \lambda_i \in \mathbb{Z},\ a_i \in S\}$ be the subgroup generated by S in $\mathbb{Z}$. In order to prove that $\mathbb{N}\backslash S$ is a finite set, its enough to find some integer m such that for all $n \geq m$, $n \in S$. Since S is a numerical semigroup then there exist some integeres $\lambda_1, ..., \lambda_k \in \mathbb{Z}^*$ and $a_1, ..., a_k \in S$ such that $1 = \sum_{i=1}^{k} \lambda_i a_i$. Without loss of generality, suppose that $\lambda_1, ..., \lambda_h < 0$ and $\lambda_{h+1}, ..., \lambda_k > 0$, and let $s = \sum_{i=1}^{h}(-\lambda_i a_i)$. Obviously $s \in S$, and $s+1 = \sum_{i=h+1}^{k} \lambda_i a_i \in S$. Now take $m = (s-1)(s+1)$, and let n be any integer such that $n \geq m$, and write $n = qs+r$ with $r < s$. Since $r \leq s-1$ and $n = qs+r \geq m = (s-1)s+(s-1)$, then $q \geq s-1$, and so $q \geq r$. But $n = qs + r = qs - rs + rs + r = (q-r)s + r(s+1)$. Hence $n \in S$ for all $n \geq m$, and so $\mathbb{N}\backslash S$ is a finite set.
Conversely, suppose that $\mathbb{N}\backslash S$ is a finite set, then there exists some $s \in S$ such that $s + 1 \in S$. Hence $1 = s + 1 - s \in G$.■

Definition 41 *Let S be a numerical semigroup. The set of gaps of S is defined to be the set $\mathbb{N}\backslash S$, denoted by $G(S)$. Moreover the cardinality of $G(S)$ is called the genus of S, and denoted by $g(s)$.*

We set $F(S) = Max(G(S))$, and we call it the Frobenius number of S. We define $C(S) = F(S) + 1$. Note that $C(S)$ is the smallest integer in S, such that for all $n \geq C(S)$, we have $n \in S$. Finally we define $m(S) = inf(S\backslash\{0\})$ to be the least positive integer in S which is called the multiplicity of S.
Even though any numerical semigroup S has infinitely many elements, there exists a finite number of elements in S, such that any other element in S can be written as a linear combination with non-negative integer coefficients in terms of theses elements.

Definition 42 *Let S be a numerical semigroup. A subset $\boldsymbol{A}$ of S is said to be a system of generators of S, written as $S = \langle \boldsymbol{A} \rangle$, if for all $s \in S$ there exists $\lambda_1, ..., \lambda_h \in \mathbb{N}$ and $a_1, ..., a_h \in \boldsymbol{A}$ such that $s = \sum_{i=1}^{h} \lambda_i a_i$.*

Moreover, S is said to be finitely generated if there exists a finite subset $\mathbf{A} = \{a_1, ..., a_h\}$ of S, such that $S = \langle \mathbf{A} \rangle = \langle a_1, ..., a_h \rangle$.

Proposition 50 *Let S be a numerical semigroup. Then S is finitely generated.*

Proof : Let $\mathbf{A}$ be any system of generators of S, and note that such a system of generators always exist since S is a system of generators of itself. Let m be the multiplicity of S, then obviously $m \in \mathbf{A}$ since its the least non zero element in S. Let a be an element of $\mathbf{A}$, and let b be any element of $\mathbf{A}$ which is congruent to a modulo m with $b > a$, then $b = km + a$ for some $k \in \mathbb{N}^*$, and so we can find a new system of generators of S by excluding all such elements b from $\mathbf{A}$. At the end of this process we will have at most one element in each congruence class modulo m. Hence we obtain a finite system of generators of S.■
Let $\{a_1, ..., a_h\}$ be a system of generators of a numerical semigroup S. We say that $\{a_1, ..., a_h\}$ is a minimal system of generators of S if $a_i \notin \langle a_1, ..., a_{i-1}, a_{i+1}, ..., a_h \rangle$ for all $i = 1, ..., h$.

Definition 43 *Let S be a numerical semigroup, and let $n \in S^*$. The Apéry set of S with respect to n, denoted by $Ap(S, n)$, is defined to be the set :*

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

Proposition 51 *Let S be a numerical semigroup and let $n \in S^*$. For all $i = 1, ..., n$ let $\omega(i)$ be the smallest element of S such that $\omega(i) \equiv i \ mod \ n$. Then :*

$$Ap(S, n) = \{0, \omega(1), ..., \omega(n-1)\}.$$

Proof : Let $i \in \{1, ..., n\}$. By definition $\omega(i) \in S$ and $\omega(i) = \lambda n + i$ for some $\lambda \in \mathbb{N}$, then $\omega(i) - n = (\lambda - 1)n + i$, and so $\omega(i) - n \equiv i \bmod n$, but $\omega(i) - n < \omega(i)$, then $\omega(i) - n \notin S$. Hence $\omega(i) \in Ap(S, n)$ for all $i = 1, ..., n$. Since $\omega(i) + (\lambda - 1)n \in S$ for all $\lambda > 0$, then $\omega(i) + \lambda n \notin Ap(S, n)$ for all $\lambda > 0$. Now let $\alpha \in Ap(S, n)$, then $\alpha \in S$, and $\alpha = \omega(i) + \lambda n$ for some $\lambda \geq 0$ and $i \in \{0, ..., n-1\}$, hence $\lambda = 0$, and so $\alpha = \omega(i)$. Finally we get the equality.■
Moreover for all $n \in S^*$, S is generated by the set $A = \langle n, \omega(1), ..., \omega(n-1) \rangle$.

Proposition 52 *Let S be a numerical semigroup and let $n \in S^*$. Then $F(S) = max(Ap(S, n)) - n$.*

Proof : Since $max(Ap(S, n))$ is an element in $Ap(S, n)$, then $max(Ap(S, n)) - n \notin S$. Now let $x \in \mathbb{N}$ with $x > max(Ap(S, n)) - n$ then $x + n > max(Ap(S, n))$. Let us prove that $x \in S$. Write $x + n = kn + i$ with $k \in \mathbb{N}$ and $i \in \{0, ..., n-1\}$, and let $\omega(i) \in Ap(S, n)$ be the smallest element of S which is congruent to i modulo n, then $\omega(i) = \lambda n + i$ for some $\lambda \in \mathbb{N}$, and so $x + n = kn + i = (k - \lambda)n + \lambda n + i = (k - \lambda)n + \omega(i)$, but $x + n > \omega(i)$, then $k - \lambda > 0$. Hence $x = (k - \lambda - 1)n + \omega(i)$ with $(k - \lambda - 1) \in \mathbb{N}$, and so $x \in S$. ■
Consider the set $\{x \in \mathbb{N},\ x \leq F(S)\}$. The cardinality of this set is obviously equal to $F(S) + 1$. Let $n(S)$ be the cardinality of the set $\{s \in S,\ s \leq F(S)\}$. We deduce the following Lemma :

Lemma 20 *Let S be a numerical semigroup, then $n(S) \leq g(S)$. Moreover we have $g(S) \geq \frac{F(S)+1}{2}$.*

Proof : Let $s \in S$, then $F(S)-s \notin S$. Indeed, suppose that $F(s)-s \in S$, then we get $(F(S)-s)+s = F(S) \in S$ which is a contradiction. We conclude that $n(S)$ is smaller than or equal to $g(S)$. But $n(S)+g(S) = F(S)+1$, hence $g(S) \geq \frac{F(S)+1}{2}$. ■

Definition 44 *Let the notation be as above. Then a numerical semigroup S is said to be symmetric if $g(S) = \frac{F(S)+1}{2}$.*

We will be interested in a special class of numerical semigroups, namely free numerical semigroups. The definition is as follows.

Definition 45 *Let $S = \langle r_0, r_1, ..., r_h \rangle$ be a numerical semigroup, and let $d_{i+1} = gcd(r_0, r_1, ..., r_i)$ for all $i \in \{0, ..., h\}$(in particular $d_1 = r_0$ and $d_{h+1} = 1$), and let $e_i = \frac{d_i}{d_{i+1}}$ for all $i \in \{1, ..., h\}$. We say that S is free for the arrangement $(r_0, ..., r_h)$ if the following conditions hold :*
(i) $d_1 > d_2 > \cdots > d_{h+1} = 1$.
(ii) $e_i r_i \in \langle r_0, ..., r_{i-1} \rangle$ for all $i \in \{1, ..., h\}$.

Note that the notion of freeness depends on the arrangement of the generators. For example, $S = \langle 4, 6, 13 \rangle$ is free for the arrangement $(4, 6, 13)$ but it is not free for the arrangement $(13, 4, 6)$.

If S is a numerical semigroup generated by $a_0, ..., a_n$, then an element $s \in S$ may be expressed in different ways as a linear combination with integer coefficients in terms of $a_0, ..., a_n$. While if S is free with respect to the arrangement $(a_0, ..., a_n)$, then each element in S has a unique representation in terms of this system in case we impose some bounds on the coefficients. This representation is called the standard representation. The following Lemmas are special cases of the Lemmas proved in the section about Affine Semigroups.

Lemma 21 *Let S be a free numerical semigroup with respect to the arrangement $(a_0, ..., a_h)$. Then for all $x \in \mathbb{Z}$, x can be written in a unique way as :*

$$x = \lambda_0 a_0 + \cdots + \lambda_h a_h$$

where $0 \leq \lambda_k < e_k$ for all $k = 1, ..., h$ and $\lambda_0 \in \mathbb{Z}$.

Lemma 22 *Let S be a free numerical semigroup for the arrangement $(a_0, ..., a_h)$. Let $x \in \mathbb{N}$ and let $\sum_{k=0}^{h} \lambda_k a_k$ be its standard representation. Then $x \in S$ if and only if $\lambda_0 \geq 0$.*

Proposition 53 *Suppose that S is a free numerical semigroup with respect to the arrangement $(a_0, ..., a_h)$. Then we have :*
(i) $F(S) = \sum_{k=1}^{h} (e_k - 1)a_k - a_0$
(ii) S is symmetric, that is $g(S) = \frac{F(S)+1}{2}$.

Proof : (i) Let $r = \sum_{k=1}^{h} (e_k - 1)a_k - a_0$. Obviously $r \notin S$. Let $s > r$ and write $s = \lambda_0 a_0 + \lambda_1 a_1 + \cdots + \lambda_h a_h$ with $0 \leq \lambda_i < e_i$ for all $i = 1, ..., h$ and $\lambda_0 \in \mathbb{Z}$. Since $s > r$, then $(\lambda_0 + 1)a_0 > \sum_{k=1}^{h} (e_k - 1 - \lambda_k)a_k$, but $\lambda_k \leq e_k - 1$ for all $k = 1, ..., h$, then $(\lambda_0 + 1)a_0 > 0$, and so $\lambda_0 + 1 > 0$ and $\lambda_0 \geq 0$. Hence $s \in S$, thus the frobenius number $F(S)$ of S is equal to $\sum_{k=1}^{h} (e_k - 1)a_k - a_0$.
(ii) Let $a, b \in \mathbb{N}$ such that $a + b = F(S)$, and let us prove that if $a \notin S$ then $b \in S$. Write $a = \alpha_0 a_0 + \alpha_1 a_1 + \cdots + \alpha_h a_h$ and $b = \beta_0 a_0 + \beta_1 a_1 + \cdots + \beta_h a_h$ with $\alpha_0, \beta_0 \in \mathbb{Z}^e$ and $0 \leq \alpha_i, \beta_i < e_i$ for all $i = 1, ..., h$. We have $(\alpha_0 + \beta_0)a_0 + \sum_{i=1}^{h} (\alpha_i + \beta_i)a_i = -a_0 + \sum_{i=1}^{h} (e_i - 1)a_i$. suppose that $\alpha_h + \beta_h \geq e_h$, then $e_h \leq \alpha_h + \beta_h \leq 2e_h - 2$, and so $\alpha_h + \beta_h = e_h + \gamma_h$ for some $0 \leq \gamma_h \leq e_h - 2$. Hence $a + b = \gamma_0 a_0 + \sum_{i=1}^{h} \gamma_i a_i$ with $\gamma_0 \in \mathbb{Z}$, $0 \leq \gamma_i < e_i$ for all $i = 1, ..., h - 1$ and $0 \leq \gamma_h \leq e_h - 2$, which is a contradiction since $a + b = -a_0 + \sum_{i=1}^{h} (e_i - 1)a_i$ and this representation is unique. Hence $\alpha_h + \beta_h = e_h - 1$. Similarly, we can prove that $\alpha_i + \beta_i = e_i - 1$ for all $i = 1, ..., h$ and $\alpha_0 + \beta_0 = -1$. If $a \notin S$ then $\alpha_0 < 0$ but $\alpha_0 + \beta_0 = -1$, then $\beta_0 \geq 0$, and so $b \in S$.
Now let $n(S)$ be the cardinality of the set $\{s \in S,\ s \leq F(S)\}$. By our discussion, we have proved that $g(S) \leq n(S)$, but $n(S) \leq g(S)$ by Lemma 20. It follows that $n(S) = g(S)$, but $n(S) + g(S) = F(S) + 1$. Hence $g(S) = \frac{F(S)+1}{2}$.■

3.1.2 Ideals of numerical semigroups

Definition 46 *Let S be a numerical semigroup, and let I be a subset of $\mathbb{Z}$. The set I is said to be a relative ideal of S if for all $a \in I$ and $s \in S$ we have $a+s \in I$ (in short $I+S \subseteq I$), and there exists some $d \in \mathbb{Z}$ such that $d+I \subseteq S$. The second condition implies that I has a minimum.*

Definition 47 *Let I be a relative ideal of a numerical seimgroup S, and let $A \subseteq I$. The set A is said to be a system of generators of I if $I = A+S$. Moreover I is said to be finitely generated if it admits a system of generators A which is finite.*

Let $a \in \mathbb{Z}$, we write $a+S$ to represent the sum $\{a\}+S$. The following proposition shows that every relative ideal is finitely generated :

Proposition 54 *Let S be a numerical semigroup, and let I be a relative ideal of S, then there exists a finite set $\{a_1, ..., a_l\} \subseteq I$ such that $I = \cup_{i=1}^{l}(a_i + S)$.*

Proof : Since I is a relative ideal of S, then $I+S \subseteq I$, but $I \subseteq I+S$, then $I+S = I$, and so I is a system of generators of I. Let $C(S)$ be the conductor of the semigroup S, and let m be the minimal element of I. For all $a \in I$ such that $a > m + C(S)$, we have $a = m + C(S) + n$ for some $n \geq 1$. Since $C(S) + n > C(S)$ then $C(S) + n \in S$, hence $a \in m + S$. Define the set $A = \{a \in I,\ a < m + C(S)\}$. Since I has a minimum then A is a finite set, say $A = \{a_1 = m, a_2, ..., a_l\}$. Finally we get $I = \cup_{i=1}^{l}(a_i + S)$.■
Let I be a relative ideal of S with a system of generators $\{a_1, ..., a_l\}$. If furthermore $a_k \notin \cup_{i \neq k}(a_i + S)$, then we say that $a_1, ..., a_l$ is a minimal system of generators of I.

Remark 14 *Obviously any relative ideal I admits a minimal system of generators. Moreover, let $\leq_S$ be the order defined on S as $a \leq_S b$ if $b = a + s$ for some $s \in S$, then $Min_{\leq_S}(I)$ is a minimal set of generators of I. Indeed, let $m(S)$ be the multiplicity of the semigroup S, and define for $i = 0, ..., m(S)-1$ the integer a_i to be the smallest integer in I which is congruent to i, which obviously exist. Let $a+s$ be an element in I, with $a \in I$ and $s \in S$, then there exists some $0 \leq i \leq m(S)-1$ and $\lambda \in \mathbb{N}$ such that $a = \lambda m(S) + a_i$, then $a + s = a_i + (\lambda m(S) + s) \in a_i + S$. Hence $I = \cup_{i=0}^{m(S)-1}(a_i + S)$. If for some $0 \leq j \leq m(S)-1$ $a_j \notin Min_{\leq_S}\{a_0, ..., a_{m(S)-1}\}$, then $a_j = a_i + s$ for some $i \neq j$ and $s \in S$, and so $a_j + S \subseteq a_i + S$. We conclude that the set $Min_{\leq_S}\{a_0, ..., a_{m(S)-1}\}$ is a minimal set of generators of I.*

Corollary 3 *Let I and J be two relative ideals of a numerical semigroup S, then $I \cap J$ is a relative ideal.*

Proof : It is required to prove that $(I \cap J) + S \subseteq I \cap J$. Let $a \in I \cap J$, and let $s \in S$. Since I, J are relative ideals of S then $a + s \in I$ and $a + s \in J$, and so $a + s \in I \cap J$. Hence $I \cap J$ is a relative ideal.■
In particular, given $a, b \in \mathbb{N}$, $(a+S) \cap (b+S)$ is a relative ideal. Assume that $\{a_1, ..., a_r\}$ is the set of minimal generators of $(a+S) \cap (b+S)$. We set

$$R(a,b) = \{(a_k - a, a_k - b),\ k = 1, ..., r\}$$

Example 2 *Let $S = \langle 3, 4\rangle = \{0, 3, 4, 6, 7, \rightarrow\}$, and let $a = 3, b = 5$. We have $3 + S = \{3, 6, 7, 9, 10, \rightarrow\}$ and $5 + S = \{5, 8, 9, 11, 12, \rightarrow\}$. Hence $(3+S) \cap (5+S) = \{9, 11, 12, \rightarrow\} = (9+S) \cup (11+S)$. Note that $\{9, 11\}$ is the set of minimal elements of $(3+S) \cap (5+S)$ with respect to $\leq_S$ and that $R(3,5) = \{(6,4), (8,6)\}$.*

Let $S = \langle \alpha_1, ..., \alpha_n\rangle$ be a numerical semigroup, and let I be a relative ideal of S. Let $\{a_1, ..., a_r\}$ be a minimal system of generators of I. Let $\mathbb{K}$ be a field and consider the algebra $A = \mathbb{K}[t^{\alpha_1}, ..., t^{\alpha_n}] = \mathbb{K}[S]$. Let $M = t^{a_1}A + \cdots + t^{a_r}A$ and let

$$\phi : A^r \mapsto M,\quad \phi(f_1, ..., f_r) = t^{a_1}f_1 + \cdots + t^{a_r}f_r.$$

The kernel $ker(\phi)$ is a submodule of A^r. The following result gives explicitly a generating system for $ker(\phi)$.

Theorem 6 *Let the notation be as above where I is the relative ideal generated by $\{a_1, ..., a_r\}$. For all $1 \leq i, j \leq r$ with $i \neq j$ write $R(a_i, a_j) = \{(\alpha_k^{ij}, \beta_k^{ij}),\ 1 \leq k \leq c_{ij}\}$. Then $ker(\phi)$ is generated by $\{t^{\alpha_k^{ij}} e_i - t^{\beta_k^{ij}} e_j,\ 1 \leq i \neq j \leq r,\ 1 \leq k \leq c_{ij}\}$, where $\{e_1, ..., e_r\}$ denotes the canonical basis of A^r.*

Proof : Let $(f_1, ..., f_r) \in ker(\phi)$, then $\sum_{i=1}^r t^{a_i} f_i = 0$. Let $s_i = \deg(f_i)$ denotes the degree of f_i in t which obviously belongs to S for all $i = 1, ..., r$, and let $s = \max\{\deg(t^{a_i} f_i),\ i = 1, ..., r\}$, then there exists at least $i, j \in \{1, ..., r\}$ with $i \neq j$ and $s = a_i + s_i = a_j + s_j$. Without loss of generality suppose that $s = a_1 + s_1 = \cdots = a_h + s_h$ for some $2 \leq h \leq r$ and $s \neq a_i + s_i$ for all $h < i \leq r$. For all $i = 1, ..., h$ write $f_i = c_i t^{s_i} + \overline{f_i}$ with $\deg(\bar{f_i}) < s_i$, then

$$\sum_{i=1}^{h} c_i t^{a_i} t^{s_i} = 0.$$

There exists some $(\alpha^{12}, \beta^{12}) \in R(a_1, a_2)$ and $s_{12} \in S$ such that $(a_1+s_1, a_2+s_2) = (a_1+s_{12}+\alpha^{12}, a_2+s_{12}+\beta^{12})$, Hence :

$$c_1 t^{s_1} t^{a_1} + c_2 t^{s_2} t^{a_2} = c_1 t^{s_{12}} (t^{\alpha^{12}} t^{a_1} - t^{\beta^{12}} t^{a_2}) + (c_2 + c_1) t^{s_2} t^{a_2}$$

Now we restart with $(c_2 + c_1) t^{s_2} t^{a_2} + \sum_{i=3}^h c_i t^{s_i} t^{a_i}$, which is obviously equal to 0. We finally get that :

$$\sum_{i=1}^{h} c_i t^{s_i} t^{a_i} = \sum_{i,j} \overline{c}_{ij} t^{s_{ij}} (t^{\alpha^{ij}} t^{a_i} - t^{\beta^{ij}} t^{a_j})$$

where for all (i, j), $(\alpha^{ij}, \beta^{ij}) \in R(a_i, a_j)$. We have :

$$\sum_{i=1}^{r} t^{a_i} f_i = \sum_{i,j} \overline{c}_{ij} t^{s_{ij}} (t^{\alpha^{ij}} t^{a_i} - t^{\beta^{ij}} t^{a_j}) + \sum_{i=1}^{h} t^{a_i} \overline{f}_i + \sum_{i=h+1}^{r} t^{a_i} f_i$$

with $\sum_{i=1}^h t^{a_i} \overline{f}_i + \sum_{i=h+1}^r t^{a_i} f_i = 0$ and $\max_{i, \overline{f}_i \neq 0}(\deg(\overline{f}_i + a_i)) < s$ and $\deg(\sum_{i=h+1}^r t^{a_i} f_i) < s$. Then we restart with $\sum_{i=1}^h t^{a_i} \overline{f}_i + \sum_{i=h+1}^r t^{a_i} f_i$. This process will eventually stop, proving our assertion.■

Example 3 *Let $S = \langle 3, 4 \rangle$ and let $I = (3 + S) \cup (5 + S)$. Let $A = \mathbb{K}[t^3, t^4]$ and consider $\phi : A^2 \mapsto t^3 \mathbb{K}[t^3, t^4] + t^5 \mathbb{K}[t^3, t^4]$, defined by $\phi(f_1, f_2) = t^3 f_1 + t^5 f_2$. Then $ker(\phi)$ is generated by $(t^6, -t^4), (t^8, -t^6)$.*

3.2 Basis of $\mathbb{K}$-Algebra

Let $\mathbb{K}$ be a field and let $f_1(t), ..., f_s(t)$ be s polynomials of $\mathbb{K}[t]$. Let $A = \mathbb{K}[f_1, ..., f_s]$ be a subalgebra of $\mathbb{K}[t]$, and assume, without loss of generality, that f_i is monic for all $i = 1, ..., s$. Given $f(t) = \sum_{i=0}^{p} c_i t^i \in A$, with $c_p \neq 0$, we set $d(f) = p$ and $M(f) = c_p t^p$, the degree and leading monomial, respectively.
Let f be a polynomial in $\mathbb{K}[t]$, we define the support of f to be the set $supp(f) = \{i,\ c_i \neq 0\}$. The set $d(A) = \{d(f),\ f \in A\}$ is a submonoid of $\mathbb{N}$. We shall assume that $l(\mathbb{K}[t]/A) < \infty$. In this case $d(A)$ is a numerical semigroup.

Definition 48 *Let $A = \mathbb{K}[f_1, ..., f_s]$ be a subalgebra of $\mathbb{K}[t]$. $\{f_1, ..., f_s\}$ is said to be a basis of A if $\{d(f_1), ..., d(f_s)\}$ generates the numerical semigroup $d(A)$.*

Let $\mathbb{K}[M(f), f \in A]$ be the polynomial ring generated by the leading monomials of the polynomials in A, then clearly $\{f_1, ..., f_s\}$ is a basis of A if and only if $\mathbb{K}[M(f), f \in A] = \mathbb{K}[M(f_1), ..., M(f_s)]$.

Proposition 55 *Let $A = \mathbb{K}[f_1, ..., f_s]$ be a subalgebra of $\mathbb{K}[t]$. Consider $f(t) \in \mathbb{K}[t]$, then there exist $g(t) \in A$ and $r(t) \in \mathbb{K}[t]$ such that the following conditions hold :*
(i) $f(t) = g(t) + r(t) = \sum_{\underline{\alpha}} c_{\underline{\alpha}} f_1^{\alpha_1} \cdots f_s^{\alpha_s} + r(t)$, *with* $\underline{\alpha} = (\alpha_1, ..., \alpha_s) \in \mathbb{N}^s$.
(ii) If $g(t) \neq 0$ (respectively $(r(t)) \neq 0$), then $d(g) \leq d(f)$ (respectively $d(r) \leq d(f)$)
(iii) If $r(t) \neq 0$, then $supp(r(t)) \subseteq \mathbb{N}\backslash\langle d(f_1), ..., d(f_s)\rangle$.

Proof : If $f \in \mathbb{K}$, then the assertion is clear. Suppose that $f \notin \mathbb{K}$, and let $f(t) = \sum_{i=0}^{p} c_i t^i$ with $p = d(f) > 0$. If $p \notin \langle d(f_1), ..., d(f_s)\rangle$, then we set $g^1 = 0$, $r_1 = c_p t^p$ and $f^1 = f - c_p t^p$. Otherwise if $p \in \langle d(f_1), ..., d(f_s)\rangle$, then there exists $\underline{\theta} = (\theta_1, ..., \theta_s) \in \mathbb{N}^s$ such that $p = \theta_1 d(f_1) + \cdots + \theta_s d(f_s)$, and so $c_p t^p = c_{\underline{\theta}} M(f_1)^{\theta_1} \cdots M(f_s)^{\theta_s}$ with $c_{\underline{\theta}} \in \mathbb{K}$ (Note that this expression is not unique). In this case we set $g^1 = c_{\underline{\theta}} f_1^{\theta_1} \cdots f_s^{\theta_s}$, $r^1 = 0$ and $f^1 = f - g^1$.
Finally we get $f = f^1 + g^1 + r^1$, with $g^1 \in A$ and the following conditions hold :
(1) If $r^1 \neq 0$, then $supp(r^1) \subseteq \mathbb{N}\backslash\langle d(f_1), ..., d(f_s)\rangle$.
(2) If $f^1 \notin \mathbb{K}$, then $d(f^1) < d(f)$.
Then we restart with f^1 and apply the same process. In each step we will obtain $f^{i+1} = f^i + g^i + r^i$, with $g^i \in A$ and f^1, r^1 satisfying the above two conditions. Since $d(f^{i+1}) < d(f^i)$, then clearly there exists some $k \geq 1$ such that $d(f^k) = 0$, and so $f^k \in \mathbb{K}$. We set $g = g^1 + \cdots g^k + f^k$ and $r = r^1 + \cdots + r^k$, which proves our assertion.■
The polynomial $r(t)$ obtained in the above proposition is called the remainder of f with respect to $\{f_1, ..., f_s\}$, and it is not unique. We denote this polynomial by $R(f, \{f_1, ..., f_s\})$.

Proposition 56 *Let $A = \mathbb{K}[f_1, ..., f_s]$ be a subalgebra of $\mathbb{K}[t]$, then $\{f_1, ..., f_s\}$ is a basis of A if and only if $R(f, \{f_1, ..., f_s\}) = 0$ for all $f \in A$.*

Proof : Suppose that $\{f_1, ..., f_s\}$ is a basis of A. Let $f \in A$, then $f(t) = g(t) + r(t)$ where $g(t)$ and $r(t) = R(f, \{f_1, ..., f_s\})$ are as in Proposition 55, and so $r(t) \in A$. If $r \neq 0$ then $d(r) \in \langle d(f_1), ..., d(f_s)\rangle$, because $f_1, ..., f_s$ is a basis of A. This is a contradiction.
Conversely, suppose that $R(f, \{f_1, ..., f_s\}) = 0$ for all $f \in A$. Take $f \neq 0$, if $d(f) \notin \langle d(f_1), ..., d(f_s)\rangle$, then by Proposition 55 we have $R(f, \{f_1, ..., f_s\}) \neq 0$, which is a contradiction.■

Proposition 57 *Let the notation be as above and let $\{f_1, ..., f_s\}$ be a basis of A. Let $f \in \mathbb{K}[t]$, then $R(f, \{f_1, ..., f_s\})$ is unique.*

Proof : Let $f \in \mathbb{K}[t]$, and suppose that $f = g_1 + r_1 = g_2 + r_2$, where g_1, g_2 and r_1, r_2 are as in Proposition 55. Suppose that $r_1 \neq r_2$. We have $r_2 - r_1 = g_1 - g_2 \in A$, then $d(r_2 - r_1) \in \langle d(f_1), ..., d(f_s)\rangle$, which is a contradiction since $supp(r_i) \subseteq \mathbb{N}\backslash\langle d(f_1), ..., d(f_s)\rangle$ for $i = 1, 2$.■
Let $A = \mathbb{K}[f_1, ..., f_s]$, and consider the homomorphism :

$$\phi :\ \mathbb{K}[X_1, ..., X_s] \mapsto \mathbb{K}[t],\ \phi(X_i) = M(f_i),\quad for\ all\ \ i = 1, ..., s.$$

Let $\{F_1, ..., F_r\}$ be a system of generators of the kernel of ϕ, then F_i is a binomial for all $i = 1, ..., r$. To each $F_i = X_1^{\alpha_1^i} \cdots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \cdots X_s^{\beta_s^i}$ in $ker(\phi)$, we associate the polynomial $S_i = f_1^{\alpha_1^i} \cdots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \cdots f_s^{\beta_s^i}$. The polynomials $S_1, ..., S_r$ are called the $S-$ polynomials associated with $\{f_1, ..., f_s\}$. Since $F_i \in ker(\phi)$ for all $i = 1, ..., r$, then obviously $\sum_{k=1}^{s} \alpha_k^i d(f_k) = \sum_{k=1}^{s} \beta_k^i d(f_k) = d$, and so $d(S_i) < d$.

Theorem 7 *let $A = \mathbb{K}[f_1, ..., f_s]$ and let $\{S_i\}_{i=1,...,r}$ be the $S-$polynomials associated to $\{f_1, ..., f_s\}$. Then $\{f_1, ..., f_s\}$ is a basis of A if and only if $R(S_i, \{f_1, ..., f_s\}) = 0$ for all $i = 1, ..., r$.*

Proof : Suppose that $\{f_1, ..., f_s\}$ is a basis of A, then $R(f, \{f_1, ..., f_s\}) = 0$ for all $f \in A$. In particular $S_i \in A$ for all $i = 1, ..., r$, then $R(S_i, \{f_1, ..., f_s\}) = 0$.
Conversely suppose that $R(S_i, \{f_1, ..., f_s\}) = 0$ for all $i = 1, ..., r$, and let us prove that $\{f_1, ..., f_s\}$ is a basis of A. Let $f \in A$, and suppose to the contrary that $d(f) \notin \langle d(f_1), ..., d(f_s)\rangle$. Write :

$$f = \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1} \cdots f_s^{\theta_s}$$

For all $\underline{\theta} = (\theta_1, ..., \theta_s)$ such that $c_{\underline{\theta}} \neq 0$, we set $p_{\underline{\theta}} = d(f_1^{\theta_1} \cdots f_s^{\theta_s}) = \sum_{i=1}^{s} \theta_i d(f_i)$. Let $p = \max\{p_{\underline{\theta}},\ c_{\underline{\theta}} \neq 0\}$, then there exists $\{\underline{\theta}^1, ..., \underline{\theta}^l\}$ with $c_{\underline{\theta}^i} \neq 0$ and $d(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) = p$ for all $i = 1, ..., l$. Obviously $\sum_{i=1}^{l} c_{\underline{\theta}^i} M(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) = 0$, otherwise we will have $d(f) = p \in \langle d(f_1), ..., d(f_s)\rangle$, which contradicts our hypothesis. Hence :
$\sum_{i=1}^{l} c_{\underline{\theta}^i} M(f_1)^{\theta_1^i} \cdots M(f_s)^{\theta_s^i} = 0$, and so $\sum_{i=1}^{l} c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} \in ker(\phi)$. Then :

$$\sum_{i=1}^{l} c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} = \sum_{k=1}^{r} \lambda_k F_k$$

with $\lambda_k \in \mathbb{K}[X_1, ..., X_s]$ and $d(\lambda_k F_k) = p$ for all $k = 1, ..., r$. Substituting f_i in X_i for all $i = 1, ..., r$ we get :

$$\sum_{i=1}^{l} c_{\underline{\theta}^i} f_1^{\theta_1^i} \cdots f_s^{\theta_s^i} = \sum_{k=1}^{r} \lambda_k(f_1, ..., f_s) S_k$$

with $d(S_k) + d(\lambda_k) < p$ for all $k = 1, ..., r$. By hypothesis, we have $R(S_k, \{f_1, ..., f_s\}) = 0$ for all $k = 1, ..., r$, then by Proposition 55 S_k can be written as :

$$S_k = \sum_{\underline{\beta}} c_{\underline{\beta}} f_1^{\beta_1} \cdots f_s^{\beta_s}$$

with $d(f_1^{\beta_1} \cdots f_s^{\beta_s}) \leq d(S_k)$ for all $\underline{\beta}$ such that $c_{\underline{\beta}} \neq 0$. Hence we can write :

$$f = \sum_{\underline{\theta'}} c_{\underline{\theta'}} f_1^{\theta'_1} \cdots f_s^{\theta'_s}$$

with $\max\{d(f_1^{\theta'_1} \cdots f_s^{\theta'_s}),\ c_{\underline{\theta'}} \neq 0\} < p$. We apply the same process to the new expression of f. After applying this process more than p times, we will get a contradiction.■
The following algorithm explains how to find a basis for an algebra $A = \mathbb{K}[f_1, ..., f_s]$.

Algorithm 1

Let $A = \mathbb{K}[f_1, ..., f_s]$, and let $S_1, ..., S_r$ be the $S-$polynomials associated to $\{f_1, ..., f_s\}$. Then :
(1) If $R(S_k, \{f_1, ..., f_s\}) = 0$ for all $k = 1, ..., r$, then $\{f_1, ..., f_s\}$ is a basis of A.
(2) If $r(t) = R(S_k, \{f_1, ..., f_s\}) \neq 0$ for some $1 \leq k \leq r$, then we set $f_{s+1} = r(t)$, and we restart with $\{f_1, ..., f_{s+1}\}$. We will have $\langle d(f_1), ..., d(f_s)\rangle \subsetneq \langle d(f_1), ..., d(f), d(f_{s+1})\rangle$.

Since $\mathbb{N}\backslash\langle d(f_1), ..., d(f_s)\rangle$ is finite, then this process will stop obtaining a subset $\{f_1, ..., f_s, f_{s+1}, ..., f_{s+h}\}$ of A. If $\{S'_1, ..., S'_n\}$ are the $S-$polynomials of $\{f_1, ..., f_{s+h}\}$, then we have $R(S'_i, \{f_1, ..., f_{s+h}\}) = 0$ for all $i = 1, ..., n$. Obviously we have $A = \mathbb{K}[f_1, ..., f_{s+h}]$. Finally by Theorem 7 we get that $\{f_1, ..., f_{s+h}\}$ is a basis of A.

Definition 49 *Let $A = \mathbb{K}[f_1, ..., f_s]$ where $\{f_1, ..., f_s\}$ is a basis of A. Then $\{f_1, ..., f_s\}$ is said to be a minimal basis of A if $\{d(f_1), ..., d(f_s)\}$ is a minimal system of generators of the semigroup $d(A)$. Moreover we say that $\{f_1, ..., f_s\}$ is a reduced basis of A if $supp(f_i(t) - M(f_i)) \subseteq \mathbb{N}\backslash d(A)$ for all $i = 1, ..., s$.*

An algebra A can have many different bases, since if $\{f_1, ..., f_s\}$ is a basis of A, then if we take any polynomial $f \in A$ with $f \neq f_i$ for all $i = 1, ..., s$, then obviously $\{f_1, ..., f_s, f\}$ is also a basis of A. Now suppose that $\{f_1, ..., f_s\}$ is a basis of A. If $d(f_i) \in \langle d(f_1), ..., d(f_{i-1}), d(f_{i+1}), ..., d(f_s)\rangle$ for some $i \in \{1, ..., s\}$, then $\{f_1, ..., f_{i-1}, f_{i+1}, ..., f_s\}$ is also a basis of A. After repeating this process we obtain a minimal basis of A, which is not unique.

Remark 15 *Suppose that $\{f_1, ..., f_s\}$ and $\{g_1, ..., g_t\}$ are two minimal basis of A. The two sets $\langle d(f_1), ..., d(f_s)\rangle$ and $\langle d(g_1), ..., d(g_t)\rangle$ are minimal sets of generators of the numerical semigroup $d(A)$, which is unique. Then $s = t$ and for each $i \in \{1, ..., s\}$ there exists a unique $j \in \{1, ..., s\}$ such that $M(f_i) = M(g_j)$. Thus two minimal basis of A have the same cardinality. The following corollary shows that a minimal reduced basis of A is unique.*

Corollary 4 *Let the notation be as above. Then A has a unique minimal reduced basis up to constants.*

Proof : Let $\{f_1, ..., f_s\}$ be a minimal basis of A. Applying the division process of Proposition 55 to $f_i - M(f_i)$ for each $i \in \{1, ..., s\}$, we will obtain a reduced minimal basis of A. For uniqueness, let $\{f_1, ..., f_s\}$ and $\{g_1, ..., g_t\}$ be two minimal reduced basis of A, moreover we can suppose that these polynomials are monic. By Remark 15, we have $s = t$. Without loss of generality suppose that $M(f_i) = M(g_i)$ for all $i = 1, ..., s$. We have $d(f_i) = d(g_i)$, if $f_i - g_i \neq 0$, then $d(f_i - g_i) \in d(A)$. But $d(f_i - g_i) \subseteq supp(f_i(t) - M(f_i)) \cup supp(g_i(t) - M(g_i))$. This is a contradiction since the bases are reduced. Finally we get $f_i = g_i$ for all $i = 1, ..., s$, and so A admits a unique minimal reduced basis.■

Example 4 *Let $f_1 = t^4 + t^2$ and $f_2 = t^3$, and compute the reduced minimal basis of $A = \mathbb{K}[f_1, f_2]$. First we start by computing the kernel of $\phi_1 : \mathbb{K}[X_1, X_2] \mapsto \mathbb{K}[t]$, with $\phi_1(X_1) = t^4$ and $\phi_1(X_2) = t^3$. The kernel of ϕ_1 is generated by $F_1 = X_1^3 - X_2^4$. Hence we check the $S-$polynomial $S_1 = f_1^3 - f_2^4 = 3t^{10} + 3t^8 + t^6$. We get $R(S_1, \{f_1, f_2\}) = 0$. Then $\{f_1, f_2\}$ is a reduced basis of A and $d(A) = \langle 3, 4\rangle$.*

Example 5 *Let $f_1 = t^4 + 5t^3$ and $f_2 = t^2$, and compute the reduced minimal basis of $A = \mathbb{K}[f_1, f_2]$. First we start by computing the kernel of $\phi_1 : \mathbb{K}[X_1, X_2] \mapsto \mathbb{K}[t]$, with $\phi_1(X_1) = t^4$ and $\phi_1(X_2) = t^2$. The kernel of ϕ_1 is generated by $F_1 = X_1 - X_2^2$. Hence we check the $S-$polynomial $S_1 = f_1 - f_2^2 = 5t^3$. We get $R(S_1, \{f_1, f_2\}) = 5t^3$. Then we add $f_3 = t^3$ to obtain a new generating set $\{f_1, f_2, f_3\}$. Hence $A = \mathbb{K}[f_1, f_2, f_3] = \mathbb{K}[t^4 + 5t^3, t^2, t^3] = \mathbb{K}[t^2, t^3]$*
Now we consider $\phi_2 : \mathbb{K}[X_1, X_2] \mapsto \mathbb{K}[t]$, defined by $\phi_2(X_1) = t^3, \phi_2(X_2) = t^2$. We get $ker(\phi_2) = (F_2 = X_2^3 - X_1^2)$. The associated $S-$polynomial to F_2 is $S_2 = 0$. Hence $\{t^2, t^3\}$ is a reduced basis of A and $d(A) = \langle 2, 3\rangle$.

3.3 Modules over $\mathbb{K}$-Algebras

Let $A = \mathbb{K}[f_1, ..., f_s]$ be the subalgebra of $\mathbb{K}[t]$ generated by $\{f_1, ..., f_s\}$. Let $F_1, ..., F_r$ be a set of nonzero elements of $\mathbb{K}[t]$, and consider the $\mathbf{A}-$module $\mathbf{M}$ generated by $F_1, ..., F_r$:

$$M = \sum_{i=1}^{r} F_i A.$$

We set $d(M) = \{d(F),\ F \in \mathbf{M}\backslash\{0\}\}$ and $d(A) = \{d(f),\ f \in \mathbf{A}\backslash\{0\}\}$. Let $i \in d(M)$ and $s \in d(A)$, then $i = d(F)$ and $s = d(f)$ for some $F \in M$ and $f \in A$. Write $F = \sum_{i=1}^{r} F_i g_i$ for some $g_1, ..., g_r \in A$, then $F.f = \sum_{i=1}^{r} F_i(g_i f) \in M$. It follows that $i+s = d(F)+d(f) = d(F+f) \in d(M)$. Hence $d(M)+d(A) \subseteq d(M)$, and so $d(M)$ is a relative ideal of $d(A)$. From now on we denote by I the relative ideal $d(M)$, and by S the numerical semigroup $d(A)$.

Definition 50 *Let the notation be as above. Then $\{F_1, ..., F_r\}$ is said to be a basis of $\mathbf{M}$ if $I = \cup_{i=1}^{r}(d(F_i) + S)$. In other words $\{F_1, ..., F_r\}$ is a basis of $\mathbf{M}$ if $\{d(F_1), ..., d(F_r)\}$ is a basis of the relative ideal I of S.*

Theorem 8 *Let $F_1, ..., F_r \in \mathbb{K}[t]$ and consider the A-module $M = \sum_{i=1}^{r} F_i A$. Let F be a non zero element in $\mathbb{K}[t]$, then there exists $g_1, ..., g_r, R \in A$ satisfying the following conditions :*
(1) *$F = \sum_{i=1}^{r} g_i F_i + R$.*
(2) *For all $i = 1, ..., r$, if $g_i \neq 0$, then $d(g_i) + d(F_i) \leq d(F)$.*
(3) *If $R \neq 0$, then $d(R) \leq d(F)$ and $d(R) \in \mathbb{N}\backslash \cup_{i=1}^{r} (d(F_i) + S)$.*

Proof : If $F \in \mathbb{K}$, then the assertion is clear. Let F be a non constant polynomial in $\mathbb{K}[t]$ with $d(F) = p > 0$, and write $F = \sum_{i=0}^{p} c_i t^i$. If $p \notin \cup_{i=1}^{r}(d(F_i) + S)$, then we set $g^1 = ... = g^r = 0, r^1 = c_p t^p$ and $F^1 = F - c_p t^p$. Otherwise if $p \in \cup_{i=1}^{r}(d(F_i) + S)$, then $p \in d(F_i) + S$ for some $i \in \{1, ..., r\}$, and so $p = d(F_i) + s_i$ for some $s_i \in S$, hence $c_p t^p = ct^{s_i} M(F_i)$ with $c \in \mathbb{K}$. Choose some $g \in A$ such that $M(g) = ct^{s_i}$ which obviously exists. Set $g_i^1 = g$ and $g_j^1 = 0$ for all $j \neq i$, $R^1 = 0$ and $F^1 = F - gF_i$. Now we have $F = F^1 + \sum_{i=1}^{r} g_i^1 F_i + R^1$, and the following conditions hold :
(1) $g_i^1 \in A$ for all $i \in \{1, ..., r\}$.
(2) If $R^1 \neq 0$, then $supp(R^1) \subseteq \mathbb{N}\backslash \cup_{i=1}^{r} (d(F_i) + S)$.
(3) If $F^1 \notin \mathbb{K}$, then $d(F^1) < d(F) = p$.
Now we apply the same procedure for F^1 as in the case of F. In each step we will obtain F^k such that $d(F^{k+1}) < d(F^k)$, and so there exists some $k \geq 1$ such that $F^k \in \mathbb{K}$. We set $g_i = g_i^1 + \cdots + g_i^k$ for all $i \in \{1, ..., r\}$ and $R = R^1 + \cdots + R^k + F^k$. ■
From now on we denote the polynomial R of Theorem 8 by $R_A(F, \{F_1, ..., F_r\})$.

Proposition 58 *Let $M = F_1 A + \cdots + F_r A$ with $F_1, ..., F_r \in \mathbb{K}[t]$. Then $\{F_1, ..., F_r\}$ is a basis of M if and only if $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in M$.*

Proof : Suppose that $\{F_1, ..., F_r\}$ is a basis of M. Let $F \in M$, then by Theorem 8 $F = \sum_{i=1}^{r} g_i F_i + R$ where $g_1, ..., g_r, R$ satisfies the conditions of that theorem. We have $R_A(F, \{F_1, ..., F_r\}) = R = F - \sum_{i=1}^{r} g_i F_i \in M$. If $R \neq 0$, then $d(R) \in \mathbb{N}\backslash \cup_{i=1}^{r} (d(F_i) + S)$, which is a contradiction.
Conversely suppose that $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in M$. Let $F \in M$, and suppose to the contrary that $d(F) \notin \cup_{i=1}^{r}(d(F_i) + S)$, then by Theorem 8 we have $R_A(F, \{F_1, ..., F_r\}) \neq 0$. This is a contradiction.■
Let the notation be as before with $F_1, ..., F_r \in \mathbb{K}[t]$. Assume without loss of generality that $F_1, ..., F_r$ are monic, and let $M(F_i) = t^{a_i}$ for all $i = 1, ..., r$. Consider the homomorphism of $A-$modules ϕ defined by :

$$\phi :\ A^r \mapsto M = F_1 A + \cdots + F_r A,\ \phi(f_1, ..., f_r) = \sum_{i=1}^{r} f_i M(F_i)$$

Let $(s_i, s_j) \in R(a_i, a_j)$, then $s_i, s_j \in d(A)$ with $a_i + s_i = a_j + s_j$. Hence there exists some $g_i, g_j \in A$ with $d(g_i) = s_i$ and $d(g_j) = s_j$(note that these polynomials are not unique). Write $M(g_i) = c_{g_i} t^{s_i}$ and $M(g_j) = c_{g_j} t^{s_j}$. Obviously we have $t^{s_i} M(F_i) - t^{s_j} M(F_j) = 0$, and so $t^{s_i} e_i - t^{s_j} e_j \in ker(\phi)$ where $\{e_1, ..., e_r\}$ is the canonical basis of A^r. Set :

$$F = c_{g_j} g_i F_i - c_{g_i} g_j F_j$$

Since $M(c_{g_j}g_iF_i) = M(c_{g_i}g_jF_j)$, then $d(F) < d(g_iF_i) = a_i+s_i = d(g_jF_j) = a_j+s_j$. We call F an S-polynomial of $(F_1, ..., F_r)$. Every element of $Ker(\phi)$ gives rise to an S-polynomial. The set of all S-polynomials is denoted by $SP(F_1, ..., F_r)$ and is constructed in the above way.

Theorem 9 *Let the notation be as above, in particular $F_1, ..., F_r \in \mathbb{K}[t]$ and $M = \sum_{i=1}^r F_iA$. Then $\{F_1, ..., F_r\}$ is a basis of M if and only if $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in SP(F_1, ..., F_r)$.*

Proof : Suppose that $\{F_1, ..., F_r\}$ is a basis of M, then $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in M$. But $SP(F_1, ..., F_r) \subseteq M$, then $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in SP(F_1, ..., F_r)$.
Conversely, let $F \in M - \{0\}$ and suppose to the contrary that $R = R_A(F, \{F_1, ..., F_r\}) \neq 0$. Since $R \in M$, then there exists $g_1, ..., g_r \in A$ such that $R = g_1F_1 + \cdots + g_rF_r$. Let

$$p = max_{i,g_i\neq 0}(d(g_i) + d(F_i)).$$

Since $R \neq 0$, then by Theorem 8 $d(R) \notin \cup_{i=1}^r(d(F_i)+d(A))$, and so $p \neq d(R)$. In particular $p > d(R)$. Suppose without loss of generality that $p = d(g_i) + d(F_i)$ for $i = 1, ..., l$ and $p > d(g_i) + d(F_i)$ for $i = l + 1, ..., r$. Clearly $l \geq 2$. We shall prove by induction on l that we can rewrite R as $R = g'_1F_1 + \cdots + g'_rF_r$ with $p > max_{i,g'_i\neq 0}(d(g'_i) + d(F_i))$.
(i) Suppose that $l = 2$, that is $d(g_1) + d(F_1) = d(g_2) + d(F_2) = p$ and $d(g_i) + d(F_i) < p$ for all $i = 3, ..., r$. Let $M(g_1) = c_{g_1}t^{\alpha_1}$, $M(g_2) = c_{g_2}t^{\alpha_2}$. By our hypothesis, we have $M(g_1f_1) = -M(g_2f_2)$ and so $c_{g_2} = -c_{g_1}$ and $a_1 + \alpha_1 = a_2 + \alpha_2 \in (a_1 + S) \cap (a_2 + S)$, and so there exists $(s_1, s_2) \in R(a_1, a_2)$ such that $\alpha_1 = s + s_1$ and $\alpha_2 = s + s_2$. hence we have :

$$c_{g_1}t^{\alpha_1}t^{a_1} + c_{g_2}t^{\alpha_2}t^{a_2} = t^s(c_{g_1}t^{s_1}t^{a_1} - c_{g_1}t^{s_2}t^{a_2})$$

The polynomial $t^s(c_{g_1}t^{s_1}t^{a_1} - c_{g_1}t^{s_2}t^{a_2})$ gives rise to the $S-$polynomial

$$h = \tilde{g}_1F_1 + \tilde{g}_2F_2$$

with $\tilde{g}_1, \tilde{g}_2 \in A$ such that $M(\tilde{g}_1) = c_{g_1}t^{s_1}$ and $M(\tilde{g}_2) = c_{g_2}t^{s_2} = -c_{g_1}t^{s_1}$. We have $d(\tilde{g}_1F_1) = d(\tilde{g}_2F_2) = s_1 + a_1 = \alpha_1 + a_1 - s = p - s$ and $M(\tilde{g}_1F_1) = -M(\tilde{g}_2F_2)$, and so $d(h) < p - s$. Since h is an $S-$polynomial, then by our hypothesis $R_A(h, \{F_1, ..., F_r\}) = 0$, then h can be written as

$$h = \bar{g}_1F_1 + \cdots + \bar{g}_rF_r$$

with $d(\bar{g}_iF_i) \leq d(h) < p - s$ for all $i = 1, ..., r$. Hence

$$\begin{aligned} R &= g_1F_1 + g_2F_2 + t^s\tilde{g}_1F_1 - t^s\tilde{g}_1F_1 + t^s\tilde{g}_2F_2 - t^s\tilde{g}_2F_2 + \sum_{i=3}^r g_iF_i \\ &= (g_1 - t^s\tilde{g}_1)F_1 + (g_2 - t^s\tilde{g}_2)F_2 + t^s(\tilde{g}_1F_1 + \tilde{g}_2F_2) + \sum_{i=3}^r g_iF_i \end{aligned}$$

Since $d((g_1 - t^s\tilde{g}_1)F_1) < p$ and $d((g_2 - t^s\tilde{g}_2)F_2) < p$ and $d(t^s(\tilde{g}_1F_1 + \tilde{g}_2F_2)) = d(t^s\sum_{i=1}^r \tilde{g}_iF_i) < s + p - s = p$, then R is of the form $R = \sum_{i=1}^r \hat{g}_iF_i$ with $d(\hat{g}_iF_i) < p$ for all $i \in \{1, ..., r\}$.
(ii) Suppose that the hypothesis is true up to $l-1$, and let us prove it for l. For all $i = 1, ..., r$ set $M(g_i) = c_{g_i}t^{s_i}$. Write :

$$R = \sum_{i=1}^r g_iF_i = g_1F_1 - \frac{c_{g_1}}{c_{g_2}}g_2F_2 + (\frac{c_{g_1}}{c_{g_2}} + 1)g_2F_2 + \sum_{i=3}^r g_iF_i$$

The polynomial $g_1F_1 - \frac{c_{g_1}}{c_{g_2}}g_2F_2$ satisfies the conditions of part (i), and so there exists $\bar{g}_1, ..., \bar{g}_r \in A$ such that $g_1F_1 - \frac{c_{g_1}}{c_{g_2}}g_2F_2 = \bar{g}_1F_1 + \cdots + \bar{g}_rF_r$ with $max_{i,\bar{g}_i\neq 0}d(\bar{g}_iF_i) < p$. Hence R can be written as $R = \tilde{g}_1F_1 + \cdots + \tilde{g}_rF_r$ with $\tilde{g}_1 = \bar{g}_1$ and where the set $\{i,\ d(\tilde{g}_iF_i) = p\}$ has at most $l - 1$ elements. It follows from the induction hypothesis that

$$\tilde{g}_1F_1 + \sum_{i=2}^r \tilde{g}_iF_i = \tilde{g}_1F_1 + \sum_{i=1}^r \hat{g}_iF_i$$

with $d(\hat{g}_iF_i) < p$ for all i such that $\hat{g}_i \neq 0$ and we have that $d(\tilde{g}_1F_1) < p$. This proves our assertion.■

Algorithm 2

Let the notation be as above. In particular $M = \sum_{i=1}^{r} F_i A$.
(1) If $R_A(F, \{F_1, ..., F_r\}) = 0$ for all $F \in SP(F_1, ..., F_r)$, then by Theorem 9 $\{F_1, ..., F_r\}$ is a basis of M.
(2) If $R_A(F, \{F_1, ..., F_r\}) \neq 0$ for some $F \in SP(F_1, ..., F_r)$, then we set $F_{r+1} = R_A(F, \{F_1, ..., F_r\})$ and we restart with $\{F_1, ..., F_r, F_{r+1}\}$.

Since the set $\mathbb{N} \setminus \cup_{i=1}^{r} (d(F_i + S))$ is finite, then the process (2) in the algorithm cannot be infinite. Hence we get a basis of M, after a finite number of steps.

3.4 Curves with one place at infinity.

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero, and let $\mathbb{K}((x))$ denote the field of meromorphic series in x.

Theorem 10 *(Newton Puiseux Theorem) Let $f(x,y) \in \mathbb{K}((x))[y]$ be a polynomial in y with coefficients in $\mathbb{K}((x))$ and suppose that f is irreducible. Then there exists an element $y(t) \in \mathbb{K}((t))$ such that $f(t^n, y(t)) = 0$. Moreover :*
(i) $f(t^n, y) = \prod_{\omega^n=1}(y - y(\omega t))$.
(ii) $y(\omega t) \neq y(\omega' t)$ for all ω, ω' distinct n-th roots of unity.
(iii) $gcd(n, Supp(y(t))) = 1$.

To an irreducible polynomial $f \in \mathbb{K}((x))[y]$, we will associate a special sequences of integers, namely the characteristic sequences of f. Suppose that f is of degree n, then by Newton Puiseux theorem there exists an element $y(t) \in \mathbb{K}((t))$ such that $f(t^n, y(t)) = 0$. Write $y(t) = \sum_p c_p t^p$. Let $d_1 = n = deg_y(f)$ and set :

$$m_1 = \inf\{p \in Supp(y(t)),\ d_1 \nmid p\} \quad and\ d_2 = gcd(d_1, m_1).$$

Suppose we have defined $m_1, ..., m_{i-1}$ and $d_1, ..., d_i$ and set :

$$m_i = \inf\{p \in Supp(y(t)),\ d_i \nmid p\} \quad and\ d_{i+1} = gcd(d_i, m_i).$$

Then there exists some $h \geq 1$ such that $d_{h+1} = 1$. This sequence $\underline{m} = (m_1, ..., m_h)$ is called the set of Newton-Puiseux exponents of f. Now for all $i = 1, ..., h$ we set $e_i = \frac{d_i}{d_{i+1}}$. Finally we define the $\underline{r} = (r_0, ..., r_h)$ sequence associated to f as follows :

$$\begin{aligned} &r_0 = n, r_1 = m_1 \\ &r_i = e_{i-1} r_{i-1} + m_i - m_{i-1} \quad for\ all\ i = 2, ..., h. \end{aligned}$$

The sequences $\underline{m}$, $\underline{r}$ and $\underline{d} = (d_1, ..., d_{h+1})$ are the characteristic sequences associated to f.
Moreover the set of Newton-Puiseux exponents of f can be defined in a similar manner to that in the case of quasi-ordinary polynomials.
Now for all $y \in \mathbb{K}((t))$, let $O_t(y)$ represent the order of y in t, that is the smallest element in $supp(y)$, which is obviously in $\mathbb{Z}$.

Lemma 23 *Let f be an irreducible polynomial in $\mathbb{K}((x))[y]$ of degree n, and let $y(t) \in \mathbb{K}((t))$ be such that $f(t^n, y(t)) = 0$. Let $\{m_1, ..., m_h\}$ be the set of characteristic exponents of f. Then :*
(i) $\{m_1, ..., m_h\} = \{ord_t(y(t) - y(\omega t)),\ \omega^n = 1 \text{ and } \omega \neq 1\}$
(ii) The cardinality of the set $\{y(\omega t), ord_t(y(t) - y(\omega t)) > m_k\}$ is equal to d_{k+1}.
(iii) The cardinality of the set $\{y(\omega t), ord_t(y(t) - y(\omega t)) = m_k\}$ is equal to $d_k - d_{k+1}$.

Definition 51 *Let f be as above with $y(t) \in \mathbb{K}((t))$ such that $f(t^n, y(t)) = 0$. Consider a nonzero polynomial g in $\mathbb{K}((x))[y]$. The intersection multiplicity of f and g, denoted by $int(f,g)$, is defined to be $int(f,g) = ord_t(g(t^n, y(t)))$.*

Note that if ω is an n-th root of unity in $\mathbb{K}$, then $ord_t(g(t^n, y(t))) = ord_t(g(t^n, y(\omega t)))$. Thus the definition of intersection multiplicity of f with a polynomial g is independent of the choice of the root of $f(t^n, y) = 0$.

Theorem 11 *Let the notation be as above, and let $\underline{d} = (d_1, ..., d_{h+1})$ be the gcd-sequence associated to f. For all $i = 1, ..., h$ let $App_{d_i}(f)$ be the d_i-th approximate root of f, then $int(f, App_{d_i}(f)) = r_i$.*

For all $i = 1, ..., h$ let $g_i = App_{d_i}(f)$, which is obviously a monic polynomial of degree $\frac{n}{d_i}$. Let $g \in \mathbb{K}((x))[y]$ and remember that the expansion of g with respect to $(g_1, ..., g_h, f)$ is defined to be :

$$g = \sum_{\theta} c_\theta(x) g_1^{\theta_1} ... g_h^{\theta_h} . f^{\theta_{h+1}}$$

where $\theta = (\theta_1, ..., \theta_{h+1}) \in \mathbb{N}^{h+1}$ with $0 \leq \theta_k < e_k$ for all $k = 1, ..., h$, and $c_\theta(x) \in \mathbb{K}((x))$.

Proposition 59 *Let the notation be as above, and let $g \in \mathbb{K}((x))[y]$ such that $g \notin (f)$. Then $int(f,g) = \sum_{k=0}^{h} \lambda_k r_k$ for some $\lambda_0 \in \mathbb{Z}$ and $0 \leq \lambda_i < e_k$ for all $k = 1, ..., h$.*

Lemma 24 *Let the notation be as above. Then for all $i = 1, ..., h$ we have :*

$$e_i r_i = \sum_{j=0}^{i-1} \lambda_j r_j$$

with $\lambda_j \in \mathbb{N}$ for all $j = 0, ..., i-1$.

Now suppose that f is an irreducible polynomial in $\mathbb{K}[[x]][y]$, then $App_{d_i}(f) \in \mathbb{K}[[x]][y]$ for all $i = 1, ..., h$. Moreover, $r_i = int(f, App_{d_i}(f)) \in \mathbb{N}$ for all $i = 1, ..., h$.

Definition 52 *Let f be as above. The semigroup of values of f is defined to be :*

$$\Gamma(f) = \{int(f,g),\ g \notin (f)\}.$$

Proposition 60 *Let f be an irreducible polynomial in $\mathbb{K}[[x]][y]$, and let $\underline{r} = (r_0, ..., r_h)$ be its associated $\underline{r}$-sequence. Then $\Gamma(f)$ is a numerical seimgroup generated by $r_0, ..., r_h$. Moreover it is free with respect to the arrangement $(r_0, ..., r_h)$ and $e_k r_k < r_{k+1}$ for all $k = 1, ..., h$ where $e_k = \frac{d_k}{d_{k+1}}$.*

Theorem 12 *Let the notation be as above with f an irreducible polynomial in $\mathbb{K}[[x]][y]$, and $\Gamma(f)$ its free semigroup. Let $C(\Gamma(f))$ be the conductor of $\Gamma(f)$, then $int(f_x, f_y) = C(\Gamma(f))$.*

Proof : Let f_x, respectively f_y, be the derivative of f with respect to x, respectively y. Write

$$f_y = H_1^{\alpha_1} ... H_s^{\alpha_s}$$

where H_i is irreducible of degree n_i for all $i \in \{1, ..., s\}$. By the Newton-Puiseux theorem $H_i = \prod_{j=1}^{n_i}(y - z_j^i(t))$, where $z_j^i \in \mathbb{K}((t))$ for all $i \in \{1, ..., s\}$ and $j \in \{1, ..., n_i\}$. Using the chain rule of derivatives, we get that for all $i \in \{1, ..., s\}$ we have :

$$\frac{d}{dt} f(t^{n_i}, z_1^i) = \frac{df}{dx}(t^{n_i}, z_1^i(t)).(n_i t^{n_i - 1}) + \frac{df}{dy}(t^{n_i}, z_1^i(t))(z'(t)) = \frac{df}{dx}(t^{n_i}, z_1^i(t)).(n_i t^{n_i - 1})$$

Hence $int(f, H_i) - 1 = int(f_x, H_i) + n_i - 1$ for all $i \in \{1, ..., s\}$. It follows that :

$$\begin{aligned} int(f, f_y) &= int(f, H_1^{\alpha_1} ... H_s^{\alpha_s}) \\ &= \sum_{i=1}^{s} \alpha_i int(f, H_i) = \sum_{i=1}^{s} \alpha_i int(f_x, H_i) + \sum_{i=1}^{s} \alpha_i n_i \\ &= \sum_{i=1}^{s} int(f_x, H_1^{\alpha_1} ... H_s^{\alpha_s}) + deg(f_y) = int(f_x, f_y) + n - 1. \end{aligned}$$

Now write $f(t^n, y) = \prod_{i=1}^{n}(y - y_i(t))$. Then $f_y(t^n, y) = \sum_{i=1}^{n} \prod_{k \neq i}(y - y_k(t))$, and so $f_y(t^n, y_1(t)) = \prod_{k=2}^{n}(y_1(t) - y_k(t))$. Hence

$$int(f, f_y) = \sum_{k=2}^{n} ord_t(y_1(t) - y_k(t)) = \sum_{k=1}^{h}(d_k - d_{k+1}) m_k = \sum_{k=1}^{h}(e_k - 1) r_k = int(f_x, f_y) + n - 1.$$

It follows that $int(f_x, f_y) = \sum_{k=1}^{h}(e_k - 1) r_k - n + 1$. But $C(\Gamma(f)) = \sum_{k=1}^{h}(e_k - 1) r_k - n + 1$ since $\Gamma(f)$ is free, and so $C(\Gamma(f)) = int(f_x, f_y)$.■

Consider a polynomial $f(x, y) \in \mathbb{K}[x][y]$ of degree n and assume that after a change of variable, f can be written as

$$f = y^n + \sum_{i,j, i+j<n} c_{ij} x^i y^j$$

Definition 53 *Let the notation be as above and let $C = \{f = 0\}$ be the curve defined by f in $\mathbb{K}^2$. The projective closure of C is defined to be the curve $\bar{C} = \{H_f = 0\}$ in $\mathbb{P}^2_{\mathbb{K}}$, where $H_f = y^n + \sum c_{ij} u^{n-i-j} x^i y^j \in \mathbb{K}[u, x, y]$.*

Definition 54 *Let the notation be as above. Then f is said to be a curve with one place at infinity if $f_\infty(u, y) = H(u, 1, y)$ is irreducible in $\mathbb{K}[[u]][y]$.*

To every polynomial $f \in \mathbb{K}[x][y]$ we associate the polynomial $F(x, y) = f(x^{-1}, y)$. Obviously $F(x, y) \in \mathbb{K}[x^{-1}][y] \subseteq \mathbb{K}((x))[y]$.

Proposition 61 *Let the notation be as above. Then $F(x, x^{-1}y) = x^{-n} f_\infty(x, y)$, moreover f has one place at infinity if and only if $F(x, y)$ is irreducible in $\mathbb{K}((x))[y]$.*

Proof : Write $f = y^n + \sum_{i+j<n} c_{ij} x^i y^j$, then $F(x, y) = f(x^{-1}, y) = y^n + \sum_{i+j<n} c_{ij} x^{-i} y^j$, Hence :

$$\begin{aligned} F(x, x^{-1}y) &= (x^{-1}y)^n + \sum_{i+j<n} c_{ij} x^{-i} (x^{-1}y)^j = x^{-n} y^n + \sum_{i+j<n} c_{ij} x^{-i-j} y^j \\ &= x^{-n}(y^n + \sum_{i+j<n} c_{ij} x^{n-(i+j)} y^j) = x^{-n} f_\infty(x, y). \end{aligned}$$

Now we want to prove that f_∞ is irreducible in $\mathbb{K}[[x]][y]$ if and only if $F(x, y)$ is irreducible in $\mathbb{K}((x))[y]$. Suppose that f_∞ is not irreducible in $\mathbb{K}[[x]][y]$, then there exists $f_1, f_2 \in \mathbb{K}[[x]][y]$ such that $f_\infty = f_1.f_2$ and $deg(f_i) = n_i < deg(f_\infty)$ for $i = 1, 2$. We have

$$F(x, x^{-1}y) = x^{-n} f_\infty(x, y) = x^{-(n_1+n_2)} f_1(x, y).f_2(x, y) = x^{-n_1} f_1(x, y).x^{-n_2} f_2(x, y).$$

Hence :

$$F(x, y) = x^{-n_1} f_1(x, xy).x^{-n_2} f_2(x, xy).$$

Setting $F_1 = x^{-n_1} f_1(x, xy)$ and $F_2 = x^{-n_2} f_2(x, xy)$, we get that $F = F_1.F_2$ with $F_1, F_2 \in \mathbb{K}((x))[y]$ and $deg(F_i) < deg(F)$ for $i = 1, 2$, hence F is not irreducible in $\mathbb{K}((x))[y]$. Similarly we can prove that if F is not irreducible in $\mathbb{K}((x))[y]$, then f_∞ is not irreducible in $\mathbb{K}[[x]][y]$.■

Definition 55 *Let the notation be as above. The semigroup of F is defined to be the set*

$$\Gamma(F) = \{int(F, G) = O_t G(t^n, y(t)),\ G(x, y) \in \mathbb{K}[x^{-1}][y]\}$$

Now let $f, g \in \mathbb{K}[x][y]$. Note that the intersection multiplicity between f and g is the rank of the $\mathbb{K}-$vector space $\frac{\mathbb{K}[x,y]}{(f,g)}$, and its denoted by $Int(f, g)$.

Theorem 13 *Let the notation be as above with $f = y^n + \sum_{i+j<n} a_{ij} x^i y^j$. Consider a polynomial $g \in \mathbb{K}[x, y]$, and suppose that g can be written as $g = y^p + \sum_{i+j<p} x^i y^j$ and let $F(x, y) = f(x^{-1}, y)$ and $G(x, y) = g(x^{-1}, y)$, then $Int(f, g) = -int(F, G)$.*

Proof : Let $y(t)$ be a root of $F(t^n, y(t)) = 0$. By Proposition 61 we have :

$$f_\infty(x, y) = x^n F(x, x^{-1}y) \text{ and } g_\infty(x, y) = x^p G(x, x^{-1}y)$$

Hence $f_\infty(t^n, t^n y(t)) = t^{n^2} F(t^n, t^{-n} t^n y(t)) = t^{n^2} F(t^n, y(t)) = 0$, and so $t^n y(t)$ is a root of $f_\infty(t^n, y) = 0$. Hence :

$$\begin{aligned} int(f_\infty, g_\infty) &= ord_t g_\infty(t^n, t^n y(t)) = ord_t((t^n)^p G(t^n, t^{-n} t^n y(t))) \\ &= ord_t(t^{np}) + ord_t(G(t^n, y(t))) = np + int(F, G). \end{aligned}$$

On the other hand by Bezout's Theorem we have :

$$int(f_\infty, g_\infty) + Int(f, g) = np$$

Comparing both equations we get $Int(f, g) = -int(F, G)$.■
More generally we can prove that if f is a curve with one place at infinity, then $Int(f, g) = -int(F, G)$ for all $g \in \mathbb{K}[x, y]$ where $F(x, y) = f(x^{-1}, y)$ and $G(x, y) = g(x^{-1}, y)$.

Definition 56 *Let the notation be as above with $f \in \mathbb{K}[x,y]$ a curve with one place at infinity. The semigroup of f is defined to be :*

$$\Gamma(f) = \{Int(f,g),\ g \in \mathbb{K}[x,y] \text{ and } g \notin (f)\}$$

Proposition 62 *Let f be a polynomial in $\mathbb{K}[x,y]$ with one place at infinity, and let $F(x,y) = f(x^{-1},y)$. Let $(r_0,...,r_h)$ be the $\underline{r}-$sequence associated to F, then according to the previous propositions $\Gamma(f)$ is a free numerical semigroup with respect to the arrangement $(r_0,...,r_h)$.*

3.5 Kahler Differentials

Let $\{f_1, ..., f_r\}$ be a set of polynomials of $\mathbb{K}[t]$, and let $A = \mathbb{K}[f_1, ..., f_r]$ be the algebra generated by $f_1, ..., f_r$. Set :

$$S = d(A) = \{d(f),\ f \in A\}$$

We shall assume that S is a numerical semigroup. For all $i = 1, ..., r$ set $F_i(t) = f_i'(t)$, the derivative of f_i with respect to t, and let $M = F_1A + ... + F_rA$. Now let $I = d(M) = \{d(F),\ F \in M\}$, then obviously I is a relative ideal of S. Moreover, let $g \in A$, then $g = \sum_\alpha c_\alpha f_1^{\alpha_1}...f_r^{\alpha_r}$, and so $g' = \sum_\alpha c_\alpha(\sum_{i=1}^r \alpha_i f_1^{\alpha_1}...f_i^{\alpha_i - 1}...f_r^{\alpha_r} f_i')$, hence $g' \in M$. Note that $d(g') = d(g) - 1$. It follows that for all $s \in S$ we have $s - 1 \in I$. This leads to the following definition :

Definition 57 *Let the notation be as above. An element $s \in I$ is said to be an exact element if $s + 1 \in S$. Other elements are called non exact elements of I, and they are denoted by $NE(M)$, i.e*

$$NE(M) = \{i \in I,\ i + 1 \notin S\}.$$

Note that if $s \in NE(M)$, then $s + 1 \in G(S)$ where $G(S)$ is the set of gaps of S. Since S is a numerical semigroup, then $G(S)$ is a finite set, and so the number of non exact elements in I is finite. We denote the cardinality of the set $NE(M)$ by $ne(M)$. It follows that :

$$ne(M) \leq g(s)$$

In what follows we will be interested in the case where $r = 2$. We will also use the notation of $x(t), y(t)$ for $f_1(t), f_2(t)$.
Now write $x(t) = t^n + a_1t^{n-1} + ... + a_n$ and $y(t) = t^m + b_1t^{m-1} + ... + b_m$, and suppose without loss of generality that $m < n$. Consider the map :

$$\psi : \mathbb{K}[X, Y] \mapsto \mathbb{K}[t],\ \psi(X) = x(t),\ \psi(Y) = y(t).$$

and let $f \in \mathbb{K}[X, Y]$ be the monic generator of the kernel of this map. Then f is a curve with one place at infinity. In this case we will denote $S = d(A) = d(\mathbb{K}[x(t), y(t)])$ by $\Gamma(f)$. Note that for any nonzero polynomial $g(X, Y) \in \mathbb{K}[X, Y]$, the element $deg_t(g(x(t), y(t)))$ of $\Gamma(f)$ coincides with the rank over $\mathbb{K}$ of the $\mathbb{K}$-vector space $\frac{\mathbb{K}[X,Y]}{(f,g)}$.
Let $\mathbb{K}$ be an algebraically closed field, and let $f(X, Y)$ be an irreducible plane curve in $A = \mathbb{K}[X, Y]$, where A is the ring of polynomials in two variables over $\mathbb{K}$. Let $\Theta = \frac{\mathbb{K}[X,Y]}{(f)}$ be the coordinate ring of f, and let $\phi :\ \mathbb{K}[X, Y] \mapsto \frac{\mathbb{K}[X,Y]}{(f)}$ be the canonical homomorphism defined by f. Let $x = \phi(X)$ and $y = \phi(Y)$, then $\Theta \cong \mathbb{K}[x, y]$.

Definition 58 *The module of Kahler differentials of Θ is defined to be the Θ-module generated by dx and dy and subject to the relation $f_x dx + f_y dy = 0$, where f_x, respectively f_y represents the partial derivative of f with respect to x, respectively y. This module is denoted by $\Theta d\Theta$.*

Note that elements in $\Theta d\Theta$ are of the form $gdx + hdy$ for some $g, h \in \mathbb{K}[x, y]$. Moreover the module of Kahler differentials associated to f is isomorphic to $M = x'(t)A + y'(t)A$, where $A = \mathbb{K}[x(t), y(t)]$. From now on we write $l(N)$ for the length of an Θ-module N.

Definition 59 *The torsion module of $\Theta d\Theta$ is defined to be the set :*

$$T = \{\omega \in \Theta d\Theta,\ g\omega = 0,\ \textit{for some non zero element}\ \ g \in \Theta\}$$

Definition 60 *The Tjurina number of f is defined to be $l(\frac{\mathbb{K}[X,Y]}{(f, f_X, f_Y)}) = l(\frac{\Theta}{(f_x, f_y)})$, and is denoted by $\nu(f)$. Moreover, the jacobian ideal of Θ is defined as $J := \Theta f_x + \Theta f_y$, hence $\nu(f) = l(\frac{\Theta}{J})$.*

Lemma 25 *Define the set $U = \{g \in \Theta,\ gf_x = h_g f_y$ for some $\ h_g \in \Theta\}$. Then*

$$l(T) = l(\frac{U}{\Theta.f_y}).$$

Proof : Note that for each $g \in U$, there is a unique $h_g \in \Theta$ such that $gf_x = h_g f_y$. Hence we can define the Θ-homomorphism :

$$\varphi : \ U \mapsto \Theta d\Theta$$

by setting $\varphi(g) = h_g dx + g dy$. For all $g \in U$, we have :

$$f_x \cdot \varphi(g) = f_x h_g dx + f_x g dy = f_x h_g dx + h_g f_y dy = h_g(f_x dx + f_y dy) = 0$$

Similarly we can prove that $f_y \cdot \varphi(g) = 0$. Supposing that f is non constant then $f_x \neq 0$ or $f_y \neq 0$, hence $\varphi(g) \in T$.
Conversely let $hdx + gdy \in T$, then there exists some $\lambda \in \Theta$ such that $\lambda(hdx + gdy) = 0 = k(f_x dx + f_y dy)$ for some $k \in \Theta$. Hence $\lambda \cdot h = k \cdot f_x$ and $\lambda \cdot g = k \cdot f_y$, and consequently $\lambda(h \cdot f_y) = \lambda(g \cdot f_x) = k \cdot f_x \cdot f_y$. Hence $h \cdot f_y = g \cdot f_x$, and so $g \in U$ and $\varphi(g) = hdx + gdy$. Whence $Im(\varphi) = T$.
On the other hand if $g \in Ker(\varphi)$, then $\varphi(g) = h_g dx + g dy = 0$, and so $h_g dx + g dy = \gamma(f_x dx + f_y dy)$ for some $\gamma \in \Theta$, hence $g = \gamma \cdot f_y \in \Theta \cdot f_y$. Conversely if $g \in \Theta \cdot f_y$, then $g = \lambda \cdot f_y$ for some $\lambda \in \Theta$, and so $g.f_x = (\lambda.f_x).f_y$, hence $\varphi(g) = \lambda.f_x dx + g dy = \lambda(f_x dx + f_y dy) = 0$. Thus $Ker(\varphi) = \Theta.f_y$. Finally we get :

$$T \cong \frac{U}{\Theta.f_y}.$$

Consequently $l(T) = l(\frac{U}{\Theta.f_y})$.■.

Proposition 63 *Let the notation be as above, where T is the torsion module of $\Theta d\Theta$. Then*

$$l(T) = \nu(f).$$

Proof : Define the following Θ-homomorphisms :

$$\psi_1 : \Theta \mapsto \Theta.f_x, \ \psi(h) = h.f_x \ \forall h \in \Theta.$$
$$\psi_2 : \Theta.f_x \mapsto \frac{\Theta.f_x}{\Theta.f_x \cap \Theta.f_y}, \quad \textit{to be the canonical surjection.}$$

Since $\frac{\Theta.f_x}{\Theta.f_x \cap \Theta.f_y} \cong \frac{J}{\Theta.f_y}$. Then we set the $\Theta-$homomorphism defined by :

$$\psi = \psi_2 \circ \psi_1 : \ \Theta \mapsto \frac{J}{\Theta.f_y}, \quad \textit{to be the composition of } \psi_2 \textit{ and } \psi_1.$$

We have $\omega \in Ker(\psi)$ if and only if $\omega.f_x = 0$ in $\frac{J}{\Theta.f_y}$ if and only if $\omega.f_x \in \Theta.f_y$ if and only if $\omega \in U$. Hence $\frac{\Theta}{U} \cong \frac{J}{\Theta.f_y}$. It follows that :

$$l(\frac{\Theta}{U}) = l(\frac{J}{\Theta.f_y}). \tag{3.1}$$

Since $\Theta.f_y \subset J \subset \Theta$, then $l(\frac{\Theta}{J}) = l(\frac{\Theta}{\Theta.f_y}) - l(\frac{J}{\Theta.f_y})$. Also $\Theta.f_y \subset U \subset \Theta$, then $l(\frac{\Theta}{U}) = l(\frac{\Theta}{\Theta.f_y}) - l(\frac{U}{\Theta.f_y})$, and so $l(\frac{U}{\Theta.f_y}) = l(\frac{\Theta}{\Theta.f_y}) - l(\frac{\Theta}{U})$. It follows from Equation 3.1 that $l(\frac{\Theta}{J}) = l(\frac{U}{\Theta.f_y})$. Hence by Lemma 25 we get that $\nu(f) = l(\frac{\Theta}{J}) = l(\frac{U}{\Theta.f_y}) = l(T)$.■
Let $\bar{\Theta}$ be the integral closure of Θ, and let $\bar{\Theta}d\bar{\Theta}$ be the module of kahler differentials of $\bar{\Theta}$ regarded as an Θ- module. Note that if $(x(t), y(t))$ is a parametrization of the curve f, then $\Theta = \mathbb{K}[x(t), y(t)]$. Moreover $\bar{\Theta} = \mathbb{K}[t]$. In this case $\bar{\Theta}d\bar{\Theta} = \mathbb{K}[t]dt$, and an element $hdx + gdy \in \ \Theta d\Theta$ can be regarded as an element in $\bar{\Theta}d\bar{\Theta}$ by taking $h(x(t), y(t))d(x(t)) + g(x(t), y(t))d(y(t))$, keeping in mind that $d(t^n) = nt^{n-1}dt$ for all $n \in \mathbb{N}^*$.
We define the conductor ideal of Θ in its integral closure $\bar{\Theta}$ to be the set $\Im_f = \{g \in \bar{\Theta}, \ g\bar{\Theta} \subset \Theta\}$, and we write c for its length.
Now let $(f-\lambda)_{\lambda \in \mathbb{K}}$ be the family of translates of f, and for all $\lambda \in \mathbb{K}$ let $V(f-\lambda) = \{P \in \mathbb{K}^2, \ (f-\lambda)(p) = 0\}$ be the curve of $\mathbb{K}^2$ defined by $f - \lambda$.

Definition 61 *Let $\lambda \in \mathbb{K}$ and $p = (a, b) \in V(f - \lambda)$. Let M_p be the maximal ideal defined by p, that is $M_p = (X - a, X - b)$, and let $F = \mathbb{K}[X, Y]_{M_p}$ be the localization of $\mathbb{K}[X, Y]$ at M_p. The local Milnor number of $(f - \lambda)$ at p, denoted by μ_p^λ, is defined to be the rank of the $\mathbb{K}$-vector space $\frac{F}{(f_X, f_Y)}$, where (f_X, f_Y) is the ideal generated by f_X, f_Y considered as elements in F.*

Note that a point $p \in V(f-\lambda)$ is said to be a singular point of $f-\lambda$ if $\mu_p^\lambda > 0$, otherwise p is a smooth point of $f-\lambda$.

Definition 62 *Let $\lambda \in \mathbb{K}$. Then $f-\lambda$ is said to be singular if $\mu_p^\lambda > 0$ for some $p \in V(f-\lambda)$.*

In our setting if $f-\lambda$ is singular, then it has only a finite number of singular points. Moreover, there is only a finite number of λ such that $f-\lambda$ is singular. Note that if $\mu(f) = dim_{\mathbb{K}} \frac{K[X,Y]}{(f_X, f_Y)}$ is the Milnor number of f, then $\mu(f)$ is the sum of local Milnor numbers at the singular points of the translates of f. That is

$$\mu(f) = \sum_{\lambda \in \mathbb{K}} \sum_{p \in V(f-\lambda)} \mu_p^\lambda.$$

Lemma 26 (Berger's Formula) *Let the notations be as above, where Θ is the coordinate ring of f, and $\bar{\Theta}$ its integral closure. Then :*

$$\nu(f) = l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta}) + \frac{c}{2} = l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta}) + \frac{\mu(f)}{2}.$$

Let v denotes the natural valuation on $\bar{\Theta}$. The valuation of an element g in Θ is the valuation of g regarded as an element of $\bar{\Theta}$. Moreover $v(g(t)dh(t)) = v(g(t)) + v(h(t)) - 1$. Now we define the following sets :
$\Gamma(f) = \{v(g),\ g \ \ non\ constant\ element\ in\ \Theta\}$, *the set of values of elements in the coordinate ring.*
$\Gamma'(f) = \{v(g)-1,\ g \ \ non\ constant\ element\ in\ \Theta\}$, *the set of values of exact differential forms.*
$\Gamma^*(f) = \{v(\omega),\ \omega \in \Theta d\Theta\}$, *the set of values of Kahler differentials.*

Theorem 14 *Let the notation be as above, where $\nu(f)$ is the Tjurina number of f, and c is the length of the conductor ideal of Θ. Then :*

$$\nu(f) \leq c.$$

Proof : Note that the number of missing integers in $\Gamma(f)$, (cardinality of $\mathbb{N}\backslash\Gamma(f)$), is equal to $l(\frac{\bar{\Theta}}{\Theta}) = \frac{c}{2}$, which is obviously equal to the cardinality of $\mathbb{N}\backslash\Gamma'(f)$. Now consider an integer $s-1 = v(g)-1 \in \Gamma'(f)$ for some $g \in \Theta$, then $s-1 = v(dg)$, but $dg \in \Theta d\Theta$, hence $s-1 \in \Gamma^*(f)$, and so $\Gamma'(f) \subseteq \Gamma^*(f)$. Hence $\mathbb{N}\backslash\Gamma^*(f) \subseteq \mathbb{N}\backslash\Gamma^{'}(f)$, and consequently :

$$l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta}) = \#(\mathbb{N}\backslash\Gamma^*(f)) \leq \#(\mathbb{N}\backslash\Gamma^{'}(f)) = \frac{c}{2}$$

It follows from Bergers formula that $\nu(f) = l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta}) + \frac{c}{2} \leq \frac{c}{2} + \frac{c}{2} = c$.■
Note that $\nu(f) = c$ if and only if $l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta}) = \frac{c}{2}$, that is every integer in $\Gamma^*(f)$ is of the form $v(g)-1$ for some $g \in \Theta$. Hence if ω is a differential form then there exists some $g_1 \in \Theta$ such that $v(\omega) = v(dg_1)$, moreover we can choose g_1 such that $\omega_1 = \omega - dg_1$ satisfies $v(\omega_1) < v(\omega)$, then we choose some $g_2 \in \Theta$ such that $v(\omega_1) = v(dg_2)$ and $v(\omega_2 = \omega_1 - dg_2) < v(\omega_1)$. We finally get a sequence $g_1, ..., g_n \in \Theta$ with $\omega = d(g_1 + \cdots + g_n)$, hence ω is an exact differential form. Finally we conclude the following proposition :

Proposition 64 *Let the notations be as above, with $c = l(\Im_f)$ and $\nu(f)$ the Tjurina number of f. Then $\nu(f) = c$ if and only if every differential form is exact.*

Note that if $g(x,y) \in \mathbb{K}[x,y]$, then $\frac{d}{dt} g(x(t), y(t)) \in M$, and so $d(\frac{d}{dt} g(x(t), y(t))) \in I$. It follows that $\{s-1,\ s \in \Gamma(f)\} \subseteq I$ and $d(\frac{d}{dt} g(x(t), y(t)))$ is an exact element. In particular, $l(\frac{\bar{\Theta} d\bar{\Theta}}{\Theta d\Theta})$ is the cardinality of the set $\{s \in G(\Gamma(f)),\ s-1 \notin S\}$. This cardinality is equal to

$$g(\Gamma(f)) - ne(M) = \frac{\mu(f)}{2} - ne(M)$$

It follows from the Berger's formula that

$$\nu(f) = \frac{\mu(f)}{2} - ne(M) + \frac{\mu(f)}{2} = \mu(f) - ne(M)$$

Let the notation be as above with $x(t) = t^n + a_1t^{n-1} + ... + a_n$ and $y(t) = t^m + b_1t^{n-1} + ... + b_n$, and $\Gamma(f) = d(\mathbb{K}[x(t), y(t)])$. Obviously $n, m \in \Gamma(f)$. Suppose without loss of generality, that $m < n$ and also (by taking the change of variables $t_1 = t + \frac{b_1}{n}$) that $b_1 = 0$. Recall that a set of generators of $\Gamma(f)$ is constructed as follows : $r_0 = m = d_1$ and $r_1 = n$, then we take $d_2 = gcd(d_1, r_1)$ and we let $g_2 = App_{d_2}(f)$ to be the d_2-th approximate root of f, we get that $r_2 = d(g_2(x(t), y(t)))$. Suppose that $r_0, r_1, ..., r_i$ and $d_1, ..., d_i$ are constructed, and let $d_{i+1} = gcd(r_i, d_i)$, then we take $g_{i+1} = App_{d_{i+1}}(f)$ and $r_{i+1} = d(g_{i+1}(x(t), y(t)))$. Consequently we get a finite system of generators $r_0, ..., r_h$ such that $\Gamma(f) = \langle r_0, ..., r_h \rangle$. Moreover, $\Gamma(f)$ is free with respect to this arrangement.

Lemma 27 *Let $q(t) = t + \sum_{i\geq 1} c_i t^{-i} \in \mathbb{K}((t))$ and consider the map $l : \mathbb{K}((T)) \mapsto \mathbb{K}((t))$ defined by $l(\alpha(T)) = \alpha(q(t))$ for all $\alpha(T) \in \mathbb{K}((T))$. In particular $l(T) = q(t)$. Then l is an isomorphism.*

Proof : Let $\alpha(T), \beta(T) \in \mathbb{K}((T))$, then clearly we have $l(\alpha(T)+\beta(T)) = l(\alpha(T))+l(\beta(T))$ and $l(\alpha(T)\beta(T)) = l(\alpha(T))l(\beta(T))$. Furthermore, $l(1) = 1$ and $ker(l) = \{0\}$. In order to prove that l is an isomorphism we are going to construct the inverse of l. More precisely we are going to prove that $t = l(T + b_1T^{-1} + b_2T^{-2} + \ldots)$ for some $T + b_1T^{-1} + b_2T^{-2} + \ldots \in \mathbb{K}((T))$. We shall prove this by induction on $k \geq 1$. That is for all $k \geq 1$, we shall prove that there exists $b_k \in \mathbb{K}$ such that

$$deg_t(t - l(T + b_1T^{-1} + \ldots + b_kT^{-k})) \leq -k - 1.$$

Note that for all $k \in \mathbb{Z}$, we have

$$l(T^k) = t^k + \sum_{i\geq 1} c_i^k t^{k-i-1}.$$

If $k = 1$, then we set $b_1 = -c_1$. We get

$$\begin{aligned} t - l(T + b_1T^{-1}) &= t - q(t) - b_1 l(T^{-1}) \\ &= t - (t + c_1t^{-1} + c_2t^{-2} + \ldots) - b_1(t^{-1} + c_1^{-1}t^{-3} + c_2^{-1}t^{-4} + \ldots) \\ &= (-c_1 - b_1)t^{-1} - \sum_{i\geq 1} \gamma_i^1 t^{-1-i} = \sum_{i\geq 1} \gamma_i^1 t^{-1-i}. \end{aligned}$$

Where $\gamma_i^1 \in \mathbb{K}$ for all $i \geq 1$. It follows that $deg(t - l(T + b_1T^{-1})) \leq -2$. Hence the assertion is clear for $k = 1$. Suppose that the assertion is true for k and let us prove it for $k + 1$. By hypothesis we have

$$t - l(T + b_1T^{-1} + \ldots + b_kT^{-k}) = \sum_{i\geq 1} \gamma_i^k t^{-k-i}.$$

Where $\gamma_i^k \in \mathbb{K}$ for all $i \geq 1$. Then we set $b_{k+1} = \gamma_1^k$. But $l(T^{-k-1}) = t^{-k-1} + \sum_{i\geq 1} c_i^{-k-1} t^{-k-i-2}$, and so $b_{k+1}l(T^{-k-1}) = b_{k+1}t^{-k-1} + \sum_{i\geq 1} b_{k+1}c_i^{-k-1}t^{-k-i-2}$. It follows that

$$\begin{aligned} t - l(T + b_1T^{-1} + \ldots + b_{k+1}T^{-k-1}) &= t - l(T + b_1T^{-1} + \ldots + b_kT^{-k}) - b_{k+1}l(T^{-k-1}) \\ &= \sum_{i\geq 1} \gamma_i^k t^{-k-i} - b_{k+1}t^{-k-1} - \sum_{i\geq 1} b_{k+1}c_i^{-k-1}t^{-k-i-2} \\ &= (\gamma_1^k - b_{k+1})t^{-k-1} + \sum_{i\geq 2} \gamma_i^k t^{-k-i} - \sum_{i\geq 1} b_{k+1}c_i^{-k-1}t^{-k-i-2} \\ &= \sum_{i\geq 1} \gamma_i^{k+1} t^{-k-1-i} \end{aligned}$$

Hence $deg_t(t - l(T + b_1T^{-1} + \ldots + b_{k+1}T^{-k-1})) \leq -k - 2$. This proves the assertion for $k + 1$.
Let $q_1(T) = T + \sum_{k\geq 1} b_kT^{-k}$ and let us define the mapping

$$l_1 : \mathbb{K}((t)) \mapsto \mathbb{K}((T))$$

by setting $l_1(\beta(t)) = \beta(q_1(T))$ (in particular $l_1(t) = q_1(T)$). Since $deg_t(t - l(q_1(T))) \leq -k$ for all $k \geq 0$, then $t = l(q_1(T))$. This proves that l is surjective, hence an isomorphism. Note that $l_1 = l^{-1}$ because $l(l_1(t)) = t$.■

Now let us make the following change of variables, $y(t) = \bar{y}(T) = T^m$, that is :

$$T = t(1 + b_2 t^{-2} + ... + b_m t^{-m})^{\frac{1}{m}} = t(1 + \frac{1}{m} b_2 t^{-2} + \ldots) = q(t).$$

This change of variables defines a map $l : \mathbb{K}((T)) \mapsto \mathbb{K}((t))$, with $l(T) = q(t)$. It follows from Lemma 27 that l is an isomorphism. Let $\bar{x}(T) = x(l^{-1}(t))$, then $\bar{x}(T) = T^n + \sum_{p<n} c_p T^p$. Note that for all $g \in \mathbb{K}[X, Y]$ we have $d(g(x(t), y(t))) = d(g(\bar{x}(T), \bar{y}(T)))$. Furthermore the Newton-Puiseux exponents of f are constructed as follows :
Let $m_1 = -n$, and let $D_2 = gcd(n, m) = d_2$. Then for all $i \geq 2$ set :

$$m_i = inf\{-p,\ p \in supp(\bar{x}(T))\ and\ D_i \nmid p\},\ and\ D_{i+1} = gcd(D_i, m_i).$$

Note that $D_{h+1} = 1$ and $D_i = d_i$ for all $i = 1, ..., h$. Moreover, the sequence $\{r_0, ..., r_h\}$ is related to the Newton-Puiseux exponents of f as follows : $r_0 = m, r_1 = n$, and for all $k \geq 1$ we have :

$$-r_{k+1} = -e_k r_k + (m_{k+1} - m_k).$$

where $e_k = \frac{d_k}{d_{k+1}}$ for all $i = 1, ..., h$.
Now write $x(T) = T^n + c_\lambda T^\lambda + ...$ *and* $y(T) = T^m$, where $\lambda = \max\{p,\ p < n, c_p \neq 0\}$ and suppose that $\lambda > -\infty$, that is $x(t)$ is not of the form $x(T) = T^n$. Define the following differential form :

$$W(T) = mx'(T)y(T) - ny'(T)x(T)$$

which is equal to :

$$\begin{aligned} W(T) &= mT^m(nT^{n-1} + \lambda c_\lambda T^{\lambda-1} + ...) - nmT^{m-1}(T^n + c_\lambda T^\lambda + ...) \\ &= (mnT^{m+n-1} + m\lambda c_\lambda T^{m+\lambda-1} + ...) - (nmT^{m+n-1} + nmc_\lambda T^{m+\lambda-1} + ...) \\ &= (\lambda - n)mc_\lambda T^{m+\lambda-1} + \quad terms\ of\ lower\ degree. \end{aligned}$$

It follows that if $m + \lambda \notin \Gamma(f)$, then $W(T)$ is a non exact element of M. On the other hand if $m + \lambda \in \Gamma(f)$ we have the following proposition :

Proposition 65 *Let the notation be as above, with $W(T) = mx'(T)y(T) - ny'(T)x(T)$. Suppose that $m + \lambda \in \Gamma(f)$, then $\lambda \neq -m_2$. Moreover, $m + \lambda = an + bm$ for some $a, b \in \mathbb{N}$ with $a \leq 1$.*

Proof : Suppose to the contrary that $\lambda = -m_2$. In this case $m + \lambda$ is of the form $an + bm + cr_2$ for some $a, b, c \in \mathbb{N}$. We have $-r_2 = -e_1 r_1 + m_2 - m_1$, then $r_2 = e_1 r_1 + m_1 - m_2$, but $r_1 = -m_1$, and so $r_2 = (e_1 - 1)r_1 - m_2$ and $-m_2 = r_2 - (e_1 - 1)r_1$. Hence $m - m_2 = m + r_2 - (e_1 - 1)r_1 = an + bm + cr_2$, and so $m - (e_1 - 1)r_1 = am + bm + (c - 1)r_1$. If $c \geq 1$, then $m - (e_1 - 1)r_1 \geq 0$, but $m - (e_1 - 1)r_1 = m - (e_1 - 1)n < 0$ since $m < n$, which is a contradiction. It follows that $c = 0$ and $m + r_2 - (e_1 - 1)r_1 = an + bm$, hence $r_2 = (a + e_1 - 1)n + (b - 1)m$, and so $d_2 = gcd(n, m)$ divides r_2 which is a contradiction. We conclude that $\lambda \neq -m_2$, and so $\lambda > -m_2$ and λ is in the group generated by n, m, hence $m + \lambda = an + bm$ for some $a, b \in \mathbb{N}$. We have $n > m > \lambda$ and $\lambda = (a - 1)n + bm + (n - m)$, so if $a > 1$ it follows that $\lambda > n$, which is a contradiction, hence $a \leq 1$.■

Theorem 15 *Let $x(t) = t^n + a_1 t^{n-1} + ... + a_n$ and $y(t) = t^m + b_1 t^{m-1} + ... + b_m$ be the equations of a polynomial curve in $\mathbb{K}^2$, and let f be as above. Let $M = x'(t)A + y'(t)A$ be the A-module generated by $x'(t), y'(t)$. Then the following conditions are equivalent :*
(i) $\mu(f) = \nu(f)$.
(ii) Every element in $d(M)$ is exact.
(iii) There exists an isomorphism $\mathbb{K}[x, y] \mapsto \mathbb{K}[X, Y]$ thats sends f to the polynomial $X^m - Y^n$, with $gcd(m, n) = 1$.

Proof : The equivalence between (i) and (ii) is due to the fact that $\mu(f) = C(\Gamma(f)) = c(f)$ where $c(f)$ is the length of the conductor ideal, and Proposition 64.
Now let us prove that (ii) is equivalent to (iii). For the necessary condition, suppose that every element in $d(M)$ is exact, and let the notations be as in Proposition 65 with $x(T) = T^n + c_\lambda T^\lambda + ...$ and $y(T) = T^m$. By assumption we have $W(T)$ is exact, and so $m + \lambda \in \Gamma(f)$, then by Proposition 65 we have $m + \lambda = an + bm$ for some $a, b \in \mathbb{N}$ with $a \leq 1$. We will distinguish two cases :
(I) Suppose that $a = 1$, then $\lambda = n + (b-1)m$. If $b \geq 1$ we will get $\lambda \geq n$ which is not true, hence $b = 0$ in this case and $m + \lambda = n$. Now let $\tilde{y}(T) = y(T) + \alpha$ with $\alpha \in \mathbb{K}^*$. We have :

$$\begin{aligned}
\bar{W}(T) &= mx'(T)\tilde{y}(T) - n\tilde{y}'(T)x(T) \\
&= (m.nT^{n-1} + m\lambda c_\lambda T^{\lambda-1} + ...)(T^m + \alpha) - nmT^{m-1}(T^n + c_\lambda T^\lambda + ...) \\
&= (\alpha mn + m\lambda c_\lambda - nmc_\lambda)T^{m+\lambda-1} + ... \\
&= m(\alpha n + c_\lambda(\lambda - n))T^{m+\lambda-1} + ...
\end{aligned}$$

Then if we choose $\alpha = \frac{c_\lambda(n-\lambda)}{n}$, then $d(\bar{W}) < m+\lambda-1$. Now let $\bar{y} = \tilde{T}^m = T^m + \alpha$, then $\tilde{x} = \tilde{T}^n + c_{\lambda_1}\tilde{T}^{\lambda_1} + ...$ with $\lambda_1 < \lambda$.
(II) Now suppose that $a = 0$, then $m + \lambda = bm$, and so $\lambda = (b-1)m$. Consider the change of variables $\bar{x} = x - c_\lambda y^{b-1}$ and $\bar{y} = y$. We will get $\bar{x} = (T^n + c_\lambda T^\lambda + ...) - c_\lambda T^{(b-1)m}$, hence we will get either $\bar{x} = T^n$ or $\bar{x} = T^n + c_{\lambda'}T^{\lambda'} + ...$ with $\lambda' < \lambda$.
Following these two process we will get a new parametrization $(\bar{x}, \bar{y})$ with

$$(\bar{x}, \bar{y}) = (T^n, T^m) \text{ or } (\bar{x}, \bar{y}) = (T^n + c_{\lambda'}T^{\lambda'} + \ldots, T^m)$$

We shall prove that these two processes will eventually stop. In case (I), it is clear since $\lambda = n - m > 0$, so we are constructing a decreasing sequence of nonnegative integers. In case (II), if $h \geq 2$, then this is clear since the set of integers in the interval $[\lambda, -m_2]$ is finite. Suppose that $h = 1$, that is $\gcd(m, n) = 1$. If the process is infinite, then after a finite number of steps we will obtain a new parametrization of the curve of the form $\tilde{x} = T^n + \alpha T^{-l} + \ldots, \tilde{y} = T^m$ with $l > nm$, which is a contradiction.
It follows that either we will finally get a parametrization $(x(T) = T^n, y(T) = T^m)$, or a parametrization $(x(T), y(T))$ such that $W = mx'(T)y(T) - ny'(T)x(T)$ is non exact. By our assumption we have that every element is exact, and so the new parametrization must be of the form (T^n, T^m). Hence the equation of the curve is of the form $X^m - Y^n$ with $gcd(m, n) = 1$.
For the sufficient condition, suppose that $x(T) = T^n$ and $y(T) = T^m$. To prove that every element in M is exact it is enough to prove that elements of the form $x^i y^j x'$ and $x^i y^j y'$ are exact for all $i, j \in \mathbb{N}$. We have :

$$\begin{aligned}
(x^{i+1}y^j)' &= (T^{n(i+1)}T^{mj})' = n(i+1)T^{n(i+1)-1}T^{mj} + mjT^{n(i+1)}T^{mj-1} \\
&= (n(i+1) + mj)T^{n(i+1)+mj-1} \\
&= (n(i+1) + mj)(T^n)^i(T^m)^j T^{n-1} = \frac{n(i+1) + mj}{n}x^i y^i(nT^{n-1}) \\
&= \frac{n(i+1) + mj}{n}x^i y^i x'
\end{aligned}$$

Hence $x^i y^j x' = (\frac{n}{n(i+1)+mj}x^{i+1}y^j)'$, and so it is exact. Similarly we can prove that :

$$x^i y^j y' = (\frac{m}{ni + (j+1)m}x^i y^{j+1})'.$$

It follows that every element in M is exact.■

Proposition 66 *Let the notation be as above with $x(T) = T^n + c_\lambda T^\lambda + ...$ and $y(T) = T^m$. Suppose that $ne(M) > 0$, then $ne(M) \geq 2^{h-1}$.*

Proof : Let $\omega = mx'y - ny'x$, then $d(\omega) = m + \lambda - 1$ with $m + \lambda \notin S$. Furthermore $\lambda \geq -m_2$. We are going to distinguish two cases

(i) $\lambda = -m_2$. Since $m + \lambda \notin S$, then $m + \lambda = m - m_2 = -am + bn + cr_2$ with $a, b, c \in \mathbb{N}$ and $a > 0, 0 \leq b < e_1, 0 < c < e_2$. But $-m_2 = r_2 - (e_1 - 1)r_1$ and $r_1 = n$, then $m + r_2 - (e_1 - 1)n = -am + bn + cr_2$, and so $(c-1)r_2 = (a+1)m - (e_1 - 1 + b)n$. If $c \geq 1$, then $d_2 = gcd(m, n)$ divides $(c-1)r_2$ which is a contradiction since $c < e_2$. Hence $c = 1$, and $(a+1)m = (e_1 - 1 + b)n$. If $b = 0$, then m divides $(e_1 - 1)n$, which is a contradiction, hence $b \geq 1$, and so $e_1 - 1 + b \geq 2$. It follows that we should have $a \geq 2$. Finally we get :

$$m + \lambda = -am + bn + r_2 \text{ with } a \geq 2.$$

Consider the following elements $g_3^{\alpha_3} \cdots g_h^{\alpha_h} w$ of M with $\alpha_i \in \mathbb{N}$ and $0 \leq \alpha_i < e_i$ for all $i = 3, ..., h$, then $d(g_3^{\alpha_3} \cdots g_h^{\alpha_h} w) + 1 = m + \lambda + \alpha_3 r_3 + ... + \alpha_h r_h = -am + bn + r_2 + \alpha_3 r_3 + ... + \alpha_h r_h$. Since $a > 0$, then $d(g_3^{\alpha_3} \cdots g_h^{\alpha_h} w) + 1 \notin S$ for all $\alpha_3, ..., \alpha_h$. Since $e_i \geq 2$ for all $i = 3, ..., h$, then the cardinality of such elements is at least 2^{h-2}.
Moreover $d(y\omega) + 1 = -(a-1)m + bn + r_2$ with $a \geq 2$, then $y\omega$ is not exact. Then we can prove similarly that $y g_3^{\alpha_3} \cdots g_h^{\alpha_h} \omega$ are non exact elements, and the cardinality of such elements is at least 2^{h-2}. It follows that $ne(M) \geq 2^{h-1}$.
(ii) $\lambda > -m_2$. In this case $m + \lambda = -am + bn$ with $a, b \in \mathbb{N}$, $a > 0$ and $0 \leq b < e_1$. Consider the elements $g_2^{\alpha_2} \cdots g_h^{\alpha_h} \omega$ with $\alpha_i \in \mathbb{N}$ and $0 \leq \alpha_i < e_i$ for all $i = 2, ..., h$. We have $d(g_2^{\alpha_2} \cdots g_h^{\alpha_h} \omega) + 1 = d(\omega) + 1 + \alpha_2 r_2 + ... + \alpha_h r_h = -am + bn + \alpha_2 r_2 + ... + \alpha_h r_h \notin S$. Since $e_i \geq 2$ for all $i = 2, ..., h$, it follows that the number of such elements is at least 2^{h-1}. Hence $ne(M) \geq 2^{h-1}$.■

Corollary 5 *Let the notation be as above, and suppose that $ne(M) = 1$. Then $S = d(A) =< m, n >$ with $gcd(m, n) = 1$. Moreover let $F(S)$ be the Frobenius number of S, then $NE(M) = \{F(S) - 1\}$.*

Proof : Suppose that $ne(M) = 1$. By Proposition 66, we have $2^{h-1} \leq ne(M)$, and so $2^{h-1} = 1$. It follows that $h = 1$ and the gcd sequence of f is $(d_1 = m, d_2 = 1)$, and so $S =< m, n >$ with $gcd(m, n) = d_2 = 1$ and $e_1 = d_1 = m$. Let $\omega = mx'y - nxy' = cT^{m+\lambda-1} + \cdots$. By Theorem 15 we can suppose that $d(\omega) + 1 = \lambda + m \notin S$. Hence it is of the form $\lambda + m = -am + bn$ for some $a, b \in \mathbb{N}$ with $a \geq 1$ and $0 \leq b \leq e_1 - 1 = m - 1$. Note that we have $F(S) = -m + (m-1)n$. Now if $a > 1$, then $d(y\omega) + 1 = -am + bn + m = -(a+1)m + bn \notin S$, and so $y\omega$ is a non exact element different from ω, which is a contradiction. Hence $a = 1$. If $b < m - 1$, then $d(x\omega) + 1 = -am + bn + n = -m + (b+1)n \notin S$ since $b + 1 \leq m - 1$, and consequently $x\omega$ is a non exact element different from ω, which is again a contradiction. It follows that $b = m - 1$, and so $d(\omega) + 1 = -am + bn = -m + (m-1)n = F(S)$. Hence $d(\omega) = F(S) - 1$ and $NE(M) = \{F(S) - 1\}$.■
Suppose that $ne(M) = 1$, that is we have one non exact element. In this case $h = 1$, $\Gamma(f) =< m, n >$ with $m < n$ and $gcd(m, n) = 1$. Furthermore, $m + \lambda = F(S) = -m + (m-1)n < m + n$ because $\lambda < n$. This implies that $(m-2)n < 2m < 2n$. In particular $m < 4$. If $m = 2$, then $n = 2p + 1$ for some $p \geq 1$. If $m = 3$, then $n < 2m = 6$ and $n > m = 3$ implies that either $n = 4$ or $n = 5$.

Proposition 67 *Let the notation be as above, and suppose that $ne(M) = 2$. One of the following two conditions holds :*
(i) $h = 1$. In this case $S =< m, n >$ with $gcd(m, n) = 1$. Moreover $NE(M) = \{F(S) - 1, F(S) - m - 1\}$ or $NE(M) = \{F(S) - 1, F(S) - n - 1\}$.
(ii) $h = 2$. In this case $S =< m, n, r_2 >$ with $d_3 = 1$. Moreover we will have $NE(M) = \{F(S) - 1, F(S) - r_2 - 1\}$ or $NE(M) = \{F(S) - 1, F(S) - m - 1\}$ or $NE(M) = \{F(S) - 1, F(S) - n - 1\}$.

Proof : By Proposition 66, we have $2^{h-1} \leq ne(M)$, and so $2^{h-1} = 1$ or $2^{h-1} = 2$, hence $h = 1$ or $h = 2$. Let ω be a non exact element with $d(\omega) + 1 < F(S)$, and let $d(\omega)$ be minimal in $NE(M)$.
(i) $h = 1$. Since ω is non exact, then $d(\omega) + 1 = -am + bn$ for some $a \geq 1$ and $0 \leq b \leq m - 1$. If $a \geq 2$ and $b < m - 1$, then $d(y\omega) + 1 = -(a-1)m + bn \notin S$ and $d(x\omega) = -am + (b+1)n \notin S$, and so ω,$x\omega$ and $y\omega$ are three non exact elements, but $ne(M) = 2$. This is a contradiction. Hence we have :
(1) $a = 1$ and $b < m - 1$. Hence, $x\omega, ..., x^{m-b-1}\omega$ are non exact elements, but $ne(M) = 2$, then $b = m - 2$, and so $d(\omega) + 1 = -m + (m-2)n = F(S) - n$ and $d(x\omega) + 1 = -m + (m-1)n = F(S)$. Finally we get :

$$NE(M) = \{d(\omega), d(y\omega)\} = \{F(S) - 1, F(S) - n - 1\}.$$

(2) $a \geq 2$ and $b = m-1$. Hence, $y\omega, ..., y^{a-1}\omega$ are non exact elements, but $ne(M) = 2$, then $a = 2$, and so $d(\omega)+1 = -2m+(m-1)n$ and $d(y\omega)+1 = -m+(m-1)n = F(S)$. Hence :

$$NE(M) = \{F(S)-1, F(S)-m-1\}.$$

(ii) $h = 2$. In this case $S =< m, n, r_2 >$ with $d_3 = 1$. Furthermore $d(\omega)+1 = -am+bn+cr_2$ with $a \geq 1$, $0 \leq b \leq e_1-1$, and $0 \leq c \leq e_2-1$. If $a \geq 3$ then $y\omega$ and $y^2\omega$ are non exact elements, and so $ne(M) \geq 3$, which is a contradiction. Hence $a = 1$ or $a = 2$.
(1) $a = 1$. If $b < e_1-1$ and $c < e_2-1$, then $x\omega$ and $g_2\omega$ are non exact elements, which is a contradiction. Hence we have :
• $a = 1, b = e_1-1$ and $c < e_2-1$. By a similar discussion as above, we get that the only possible condition to get $ne(M) = 2$ is $c = e_2-2$. In this case ω and $g_2\omega$ are non exact elements, and $d(g_2\omega)+1 = -m+(e_1-1)r_1+(e_2-1)r_2 = F(S)$ and $d(\omega)+1 = -m+(e_1-1)r_1+(e_2-2)r_2 = F(S)-r_2$. Hence :

$$NE(M) = \{F(S)-1, F(S)-r_2-1\}.$$

• $a = 1, b < e_1-1$ and $c = e_2-1$. As above we get $b = e_1-2$. In this case ω and $x\omega$ are non exact elements with $d(\omega)+1 = -m+(e_1-2)n+(e_2-1)r_2 = F(S)-n$ and $d(x\omega)+1 = -m+(e_1-1)n+(e_2-1)r_2 = F(S)$. Hence :

$$NE(M) = \{F(S)-1, F(S)-n-1\}.$$

(2) $a = 2$. If $b < e_1-1$ or $c < e_2-1$, then $y\omega, x\omega$ are non exact, or $y\omega$ $g_2\omega$ are non exact, which is a contradiction. We get that $a = 2, b = e_1-1$ and $c = e_2-1$. In this case ω and $y\omega$ are non exact elements with $d(\omega)+1 = -2m+(e_1-1)r_1+(e_2-1)r_2 = F(S)-m$ and $d(y\omega)+1 = -m+(e_1-1)r_1+(e_2-1)r_2 = F(S)$. Hence :

$$NE(M) = \{F(S)-1, F(S)-m-1\}.\blacksquare$$

Let the notations be as above and suppose that $d(M)$ admits two non exact elements. We are going to describe the semigroup S under this condition :

Suppose that h=1 : In this case, $S =< m, n >$ with $m < n$ and $gcd(m, n) = 1$. By Proposition 67 we have $m+\lambda \in \{F(S), F(S)-n, F(S)-m\}$. We distinguish the three different cases :
• If $m+\lambda = F(S) = -m+(m-1)n$, then $\lambda = -2m+(m-1)n$. But $\lambda < n$, then $-2m+(m-2)n < 0$. We have $-2m+(m-2)n = m(n-2)-2n = (n-2)(m-2)-4$, and so $(n-2)(m-2) < 4$. It follows that $m = 2$ or $m = 3$. If $m = 2$ then $n = 2k+1$ for some $k \geq 1$ since $gcd(m, n) = 1$. Hence :

$$S =< 2, 2k+1 > .$$

If $m = 3$, then $(n-2) < 4$ and $m < n$ implies that $n = 4$ or $n = 5$. Hence :

$$S =< 3, 4 > \ \ or\ S =< 4, 5 > .$$

• If $m+\lambda = F(S)-m = -2m+(m-1)n$. Hence $\lambda = -3m+(m-1)n < n$. It follows that $(n-3)(m-2) < 6$, and so $m = 2$ or $m = 3$ or $m = 4$. Similar calculations as above leads to :

$$S =< 2, 2k+1 > \ k \geq 1,\ or\ S =< 3, 4 > \ or\ S =< 3, 5 > \ or\ S =< 4, 5 > .$$

• If $m+\lambda = F(S)-n = -m+(m-2)n$. Similar calculations as above implies that $(n-2)(m-3) < 4$, and so $m = 2$ or $m = 3$ or $m = 4$. It follows that :

$$S =< 2, 2k+1 > \ k \geq 1,\ or\ S =< 3, n > \ with\ gcd(m, n) = 1,\ or\ S =< 4, 5 > .$$

Suppose that h=2 : Let $S =< m, n, r_2 >$. In this case $m+\lambda \in \{F(S), F(S)-m, F(S)-n, F(S-r_2)\}$. We will distinguish the four cases :
• Suppose that $m+\lambda = F(S) = -m+(e_1-1)n+(e_2-1)r_2$. Since $e_2 \neq 1$, then $\lambda = -m_2 = r_2-(e_1-1)n$. Hence :

$$m+\lambda = m+r_2-(e_1-1)n = -m+(e_1-1)n+(e_2-1)r_2$$

and so $(e_2-2)r_2 = 2m-2(e_1-1)n$, then $d_2 = gcd(m, n)$ divides $(e_2-2)r_2$. But $d_2 \nmid ir_2$ for all $i = 1, ..., e_2-1$, and so $(e_2-2)r_2 = 0$. It follows that $m = (e_1-1)n$, which is a contradiction.

• If $m+\lambda = F(S) - r_2 = -m + (e_1-1)n + (e_2-2)r_2$. If $e_2 \neq 2$, then $\lambda = -m_2 = r_2 - (e_1-1)n$, and so $m + r_2 - (e_1-1)n = -m + (e_1-1)n + (e_2-2)r_2$. It follows that :

$$(e_2-3)r_2 = 2m - 2(e_1-1)n$$

Hence $d_2 = gcd(m,n)$ divides $(e_2-3)r_2$, but $d_2 \nmid ir_2$ for all $i = 1, ..., e_2-1$. Hence $(e_2-3)r_2 = 0$, which is a contradiction. It follows that $e_2 = 2, d_2 = e_2 = 2$ and $e_1 = \frac{d_1}{d_2}$, then $m+\lambda = -m+(e_1-1)n = -m+(\frac{m}{2}-1)n$. But $m+\lambda < m+n$. It follows that :

$$-2\frac{m}{2} + (\frac{m}{2}-2)\frac{n}{2} < 0$$

By similar calculations as above we obtain the inequality : $(\frac{m}{2}-2)(\frac{n}{2}-2) < 4$. Hence $(\frac{m}{2}, \frac{n}{2})$ is either $(2, 2k+1)$ with $k \geq 1$, or $(3,4)$ or $(3,5)$. Since $d_2 = 2 \nmid r_2$, then r_2 is odd. Moreover we (m,n,r_2) satisfies one of the following conditions :
(i) $m = 4, n = 4k+2, r_2 = 2p+1$ with $2p+1 < 8k+4$
(ii) $m = 6, n = 8, r_2 = 2p+1$ and $2p+1 < 24$.
(iii) $m = 6, n = 10, r_2 = 2p+1$ and $2p+1 < 30$.
• If $m+\lambda = F(S) - m = -2m + (e_1-1)n + (e_2-1)r_2$. Since $e_2 \neq 1$, then $\lambda = -m_2 = r_2 - (e_1-1)n$. This implies that $m+\lambda = m + r_2 - (e_1-1)n = -2m + (e_1-1)n + (e_2-1)r_2$. Hence :

$$(e_2-2)r_2 = 3m - 2(e_1-1)n \tag{3.2}$$

It follows that $d_2 = gcd(m,n)$ divides $(e_2-2)r_2$, and so $(e_2-2)r_2 = 0$. Hence $e_2 = 2$, $d_2 = e_2 = 2$ and $e_1 = \frac{d_1}{d_2} = \frac{m}{2}$. Since $(e_2-2)r_2 = 0$, then by Equation (3.2), we get that $3m - 2(\frac{m}{2}-1)n = 0$, and so $3\frac{m}{2} - \frac{m}{2}n + n = 0$, hence $(\frac{m}{2}-1)(n-3) = 3$. If $\frac{m}{2} \geq 4$, then $n > m \geq 8$, and so $(\frac{m}{2}-1)(n-3) > 15$, which is a contradiction. Hence $\frac{m}{2} = 2$, and so $m = 4$ and $n = 6$, and it is the only solution. Moreover $r_2 = 2p+1$ with $r_2 < 12$.
• If $m+\lambda = F(S) - n = -m + (e_1-2)n + (e_2-1)r_2$. Since $e_2 \neq 1$, then $\lambda = -m_2 - (e_1-1)n$. It follows that :

$$(e_2-2)r_2 = 2m - (2e_1-3)n \tag{3.3}$$

Hence $e_2 = d_2 = 2$ and $e_1 = \frac{m}{2}$. Using Equation (3.3) we get that $2m-(m-3)n = 0$, and so $(m-3)(n-2) = 6$. The only possible case is $m = 4$ and $n = 8$.

These results can be summarized into the following theorem.

Theorem 16 *Let $X(t) = t^n + a_1t^{n-1} + \ldots + a_n$, $Y(t) = t^m + b_1t^{m-1} + \ldots + b_m$ and assume that $m < n$ and that $gcd(m,n) < m$. Let $f(x,y)$ be the monic polynomial of $\mathbb{K}[X,Y]$ such that $f(X(t),Y(t)) = 0$ and let $\Gamma(f)$ be the semigroup associated with f. Assume that $\Gamma(f)$ is a numerical semigroup and let $\Gamma(f) = \langle m = r_0, n = r_1, \ldots, r_h \rangle$ where $r_2, ..., r_h$ are constructed as above. Let $\mu(f)$ and $\nu(f)$ be the Milnor number and the Tjurina number of f respectively. Assume that $\mu(f) > \nu(f)$. We have the following :*
(i) If $\mu(f) = \nu(f) + 1$, then $h = 1$.
(ii) If $\mu(f) = \nu(f) + 2$, then $h = 1, 2$.
Furthermore we have :
(1)If $\mu(f) = \nu(f) + 1$, then $\Gamma(f) =< m, n >$ and one of the following conditions holds :
• $(m,n) = (2, 2p+1)$, $p \geq 1$.
• $(m,n) = (3,4)$.
• $(m,n) = (3,5)$.
(2) If $\mu(f) = \nu(f) + 2$ and $h = 1$ then $\Gamma(f) =< m, n >$ and one of the following conditions holds :
• $(m,n) = (2, 2p+1)$, $p \geq 1$.
• $(m,n) = (3,4)$.
• $(m,n) = (3,5)$.
• $(m,n) = (4,5)$.
• $(m,n) = (3,n)$ *with* $gcd(3,n) = 1$.
(3) If $\mu(f) = \nu(f) + 2$ and $h = 2$ then $\Gamma(f) =< m, n, r_2 >$ and one of the following conditions holds :
• $(m,n,r_2) = (4, 4p+2, 2q+1)$, $p \geq 1$ *and* $8p+4 > 2q+1$.
• $(m,n,r_2) = (6, 8, 2p+1)$, $p \leq 11$.

- $(m, n, r_2) = (6, 10, 2p + 1),\ p \leq 14.$
- $(m, n, r_2) = (4, 6, 2p + 1),\ p \leq 5.$

Bibliographie

[1] S.S Abhyankar, Approximate Roots of Polynomials and Special Cases of the Epimorphism Theorem. preprint Purdue Univ. 1975.

[2] S.S. Abhyankar, Expansion Techniques in Algebraic Geometry, Lecture Notes of the Tata Institute Bombay, 57, (1977). 9

[3] S. S. Abhyankar, On the ramification of algebraic functions, Amer. J. Math., 77, (1955), 575-592. 10

[4] S.S. Abhyankar, On the semigroup of a meromorphic curve, Part 1, in Proceedings of International Symposium on Algebraic Geometry, Kyoto, (1977), 240-414. 9, 12

[5] S.S. Abhyankar, T.T. Moh, Newton-Puiseux expansion and generalized Tschirnhausen transformation. I, II. J. Reine Angew. Math. 260 (1973), 47-83 ; ibid. 261 (1973), 29-54.

[6] F. Aroca, G. Ilardi, A family of algebraically closed fields containing polynomials in several variables, Communications in Algebra, 37 : 1284-1296, 2009. 10

[7] A. Assi, A. Sathaye, On quasi-homogenous curves, Affine Algebraic Geometry, Osaka Univ. Press, Osaka (2007), 33-56. 12

[8] A. Assi, Irreducibility criterion for quasi-ordinary polynomials, Journal of Singularities Volume 4 (2012), 23-34.

[9] A. Assi, Meromorphic plane curves, Math. Z. 230 (1999), no. 1, 165-183.

[10] A. Assi, P.A García-Sánchez, Algorithms for curves with one place at infinity, J. Symbolic Comput. 74 (2016), 475-492. 12

[11] A. Assi, P.A García-Sánchez, Numerical Semigroups and Applications, RSME Springer Series I, 2016.

[12] A. Assi, P.A García-Sánchez, V. Micale. Bases of subalgebras of $\mathbb{K}[x]$ and $\mathbb{K}[[x]]$. J. Symbolic Comput. 79 (2017), part 1, 4-22.

[13] A. Assi, The Frobenius vector of a free affine semigroup. J. Algebra Appl. 11 (2012), no. 4, 1250065, 10 pp.

[14] R. Berger, differentialmoduln eindimensionaler lokaler Ringe, Math. Z. 81 (1963), 326-354.

[15] P.D. Gonzàlez Pérez, Singularités quasi-ordinaires toriques et polyédre de newton du discriminant. Canad. J. Math., 52, (2000), no. 2, 348-368. 10

[16] P.D. Gonzàlez Pérez, The semigroup of a quasi-ordinary hypersurface, Journal of the Institute of Mathematics of Jussieu, no 2 (2003), 383-399. 10

[17] B. Grunbaum, Convex Polytopes, John Wiley, 1967.

[18] H. E. W. Jung, Darstellung der Funktionen eines algebraischen Körpers zweier unabhängiger Varänderlichen x, y in der Umbebung einer Stelle x = a, y = b. J. Reine Angew. Math., 133, (1908), 289-314. 10

[19] J. Lipman, Quasi-ordinary singularities of embedded surfaces, Thesis, Harvard University (1965). 10

[20] F. Lucas, J. J. Madden, D. Schaub, M. Spivakovsky On connectedness of sets in the real spectra of polynomial rings.

[21] J. McDonald, Fiber polytopes and fractional power series, Journal of Pure and Applied Algebra 104 (1995) 213-233. 10

[22] V. Micale, G. Molica, B. Torrisi, Order bases of subalgebras of $\mathbb{K}[[X]]$. Commutative rings, 193-199, Nova Sci. Publ., Hauppauge, NY, 2002.

[23] V. Micale, Order bases of subalgebras of power series rings, Comm. Algebra 31 (2003), no. 3, 1359-1375.

[24] A. Monforte, M. Kauers, Formal Laurent series in several variables, Expo. Math. 31 (2013) 350-367. 35

[25] I. Newton. The mathematical papers of Isaac Newton. Vol. III : 1670-1673. Edited by D. T. Whiteside, with the assistance in publication of M. A. Hoskin and A. Prag. Cambridge University Press, London, 1969. 9

[26] P. Popescu-Pampu, Approximate roots, 1991 Mathematics Subject Classification. 32B30, 14B05.

[27] V. Puiseux. Recherches sur les fonctions algébriques. J. de math. pures et appl., 15 :365-480, 1850. 9

[28] L. Robbiano and M. Sweedler, Subalgebra bases. Commutative algebra (Salvador, 1988), 61-87, Lecture Notes in Math., 1430, Springer, Berlin, 1990.

[29] J.C Rosales, P.A García-Sánchez, Numerical semigroups, Developments in Mathematics, 20. Springer, New York, 2009.

[30] K. Saito, Quasihomogene isolierte Singularitäten von Hyperfächen, Invent. Math. 14 (1971), 123-142. 12

[31] O. Zariski, Characterization of plane algebroid curves whose module of differentials has maximum torsion. Proc. Nat. Acad. Sci. U.S.A. 56 1966 781-786. 12

[32] M. Zurro, The Abhyankar-Jung theorem revisited, Journal of Pure and Applied Algebra 90 (1993) 275-282.

UNIVERSITE BRETAGNE LOIRE

université angers

Thèse de Doctorat

Ali ABBAS

Combinatoire des singularités de certaines courbes et hypersurfaces

Combinatorics of singularities of some curves and hypersurfaces

Résumé

La thèse est constituée de deux parties. Dans la première partie on généralise la Théorie d'Abhyankar-Moh à un type special de polynômes, les polynômes libres. Soit f un polynôme non nul de $\mathbb{K}[[x_1, ..., x_e]][y]$ et supposons, moyennement un changement des variables élémentaire, que la composante homogène de plus bas degré du discriminant de f contient une puissance de x_1. Une transformation monômiale dans $\mathbb{K}[[x_1, ..., x_e]]$ transforme f en un polynôme quasi-ordinaire avec une racine dans $\mathbb{K}[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$, $n \in \mathbb{N}$. En prenant la Préimage de f par le morphisme, nous obtenons une solution $y \in \mathbb{K}_C[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ de $f(x_1, ..., x_e, y) = 0$, où $\mathbb{K}_C[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ est l'anneau des séries fractionnaires dont le support appartient à un cône convexe C. Ceci nous permet de construire l'ensemble des exposants caractéristiques de y, et de généraliser certains des résultats concernant les polynômes quasi-ordinaire au polynôme f. Dans la deuxiéme partie, nous donnons un algorithme pour calculer le monoïde des degrés du module $M = F_1A + \ldots + F_rA$ oú $A = \mathbb{K}[f_1(t), \ldots, f_s(t)]$ et $F_1, \ldots, F_r \in \mathbb{K}[t]$. Nous donnons ensuite des applications concernant le probléme de la classification des courbes polynômiales (C'est-á-dire, des courbes algébriques paramétrées par des polynômes) par rapport à certains de leurs invariants, en utilisant le module de différentielles Kähleriennes.

Mots clés

Polynômes quasi-ordinaires, Cônes sans droites, Racines approchées, Semigroupes numériques, Nombre de Milnor, Nombre de Tjurina

Abstract

The thesis is made up of two parts. In the first part we generalize the Abhyankar-Moh theory to a special kind of polynomials, called free polynomials. We take a polynomial f in $\mathbb{K}[[x_1, ..., x_e]][y]$ and by a preliminary change of variables we may assume that the leading term of the discriminant of f contains a power of x_1. After a monomial transformation we get a quasi-ordinary polynomial with a root in $\mathbb{K}[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ for some $n \in \mathbb{N}$. By taking the preimage of f we get a solution $y \in \mathbb{K}_C[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ of $f(x_1, ..., x_e, y) = 0$, where $\mathbb{K}_C[[x_1^{\frac{1}{n}}, ..., x_e^{\frac{1}{n}}]]$ is the ring of formal fractional power series with support in a specific line free cone C. Then we construct the set of characteristic exponents of y, and we generalize some of the results concerning quasi-ordinary polynomials to f. In the second part, we give a procedure to calculate the monoid of degrees of the module $M = F_1A + \ldots + F_rA$ where $A = \mathbb{K}[f_1, ..., f_s]$ and $F_1, \ldots, F_r \in \mathbb{K}[t]$. Then we give some applications to the problem of the classification of plane polynomial curves (that is, plane algebraic curves parametrized by polynomials) with respect to some of their invariants, using the module of Kähler differentials.

Key Words

Quasi-ordinary polynomials, Line-free cones, Approximate roots, Numerical semigroups, Tjurina number, Milnor number.