



Semigroup associated with a free polynomial

Abbas Ali, Assi Abdallah

► To cite this version:

| Abbas Ali, Assi Abdallah. Semigroup associated with a free polynomial. 2019. hal-02281623

HAL Id: hal-02281623

<https://hal.science/hal-02281623>

Preprint submitted on 9 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Semigroup associated with a free polynomial

Abbas Ali and Assi Abdallah *

Abstract

Let \mathbb{K} be an algebraically closed field of characteristic zero and let $\mathbb{K}_C[[x_1, \dots, x_e]]$ be the ring of formal power series in several variables with exponents in a line free cone C . We consider irreducible polynomials $f = y^n + a_1(\underline{x})y^{n-1} + \dots + a_n(\underline{x})$ in $\mathbb{K}_C[[x_1, \dots, x_e]][y]$ whose roots are in $\mathbb{K}_C[[x_1^{\frac{1}{n}}, \dots, x_e^{\frac{1}{n}}]]$. We generalize to these polynomials the theory of Abhyankar-Moh. In particular we associate with any such polynomial its set of characteristic exponents and its semigroup of values. We also prove that the set of values can be obtained using the set of approximate roots. We finally prove that polynomials of $\mathbb{K}[[\underline{x}]]$ fit in the above set for a specific line free cone (see Section 4).

Introduction

Let \mathbb{K} be an algebraically closed field of characteristic zero and let $\mathbb{K}[[\underline{x}]]$ be the ring of formal power series in $\underline{x} = (x_1, \dots, x_e)$ over \mathbb{K} . Let $f = y^n + a_1(\underline{x})y^{n-1} + \dots + a_n(\underline{x})$ be a nonzero polynomial of degree n in $\mathbb{K}[[\underline{x}]]$. Suppose that f is a quasi-ordinary polynomial, i.e its discriminant $\Delta_y(f)$ (the y -resultant of f and its y -derivative), is of the form $\Delta_y(f) = \underline{x}^\alpha \cdot \varepsilon(\underline{x})$, where $\varepsilon(\underline{x})$ is a unit in $\mathbb{K}[[\underline{x}]]$ (Note that this is always the case if $e = 1$). If f is irreducible then, by the Abhyankar-Jung theorem, there exists $y = \sum_p c_p \underline{x}^{\underline{p}} \in \mathbb{K}[[\underline{x}^{\frac{1}{n}}]]$ such that $f(\underline{x}, y) = 0$. Define the support of y to be the set $\text{Supp}(y) = \{p \in \mathbb{N}^e | c_p \neq 0\}$. In [7], Lipman proved that there exists a sequence of elements $\frac{m_1}{n}, \dots, \frac{m_h}{n} \in \text{Supp}(y)$ such that:

(i) $m_1 < m_2 < \dots < m_h$ coordinate wise.

(ii) If $\frac{m}{n} \in \text{Supp}(y)$, then $m \in (n\mathbb{Z})^e + \sum_{i=1}^h m_i \mathbb{Z}$. Moreover, $m_i \notin (n\mathbb{Z})^e + \sum_{j < i} m_j \mathbb{Z}$ for all $i = 1, \dots, h$.

The semigroup of f is defined to be the set $\Gamma(f) = \{O(f, g), g \in \mathbb{K}[[\underline{x}]] \setminus \{0\}\}$, where $O(f, g)$ is the order of the initial form of the y -resultant of f and g with respect to a fixed order on \mathbb{N}^e (we also have $O(f, g) = ng(\underline{x}, y(\underline{x}))$). Now we can associate with f the following sequences: the \underline{D} -sequence of f is defined to be $D_1 = n^e$, and for all $1 \leq i \leq h$, D_i is the gcd of the (e, e) minors of the matrix $[nI_e, m_1^T, \dots, m_i^T]$, where T denotes the transpose of a vector. We have $D_1 > \dots > D_{h+1} = n^{e-1}$. Then

*LAREMA, Angers university, 2 Bd Lavoisier, 49045 Angers cedex 01, emails: ali.abbas@math.univ-angers.fr and assi@math.univ-angers.fr

Keywords: Semigroup, Formal power series, Newton-Puiseux expansions

AMS Classification: 05E40, 20M14

we define the \underline{e} -sequence to be $e_i = \frac{D_i}{D_{i+1}}$ for all $1 \leq i \leq h$, and the \underline{r} -sequence $r_0^1, \dots, r_0^e, r_1, \dots, r_e$ to be $r_1 = m_1, r_i = e_{i-1}r_{i-1} + m_i - m_{i-1}$ for all $2 \leq i \leq h$, and r_0^1, \dots, r_0^e is the canonical basis of \mathbb{Z}^e . The sequence $\{r_0^1, \dots, r_0^e, r_1, \dots, r_h\}$ is a system of generators of $\Gamma(f)$. Moreover, there exists a special set of polynomials g_1, \dots, g_h (the approximate roots of f), such that $O(f, g_i) = r_i$ for all $i \in \{1, \dots, h\}$ (see [5]).

The aim of this article is to generalize these results to a wider class of polynomials. Namely let C be a line free rational convex cone in \mathbb{R}^e and let $\mathbb{K}_C[[\underline{x}]]$ be the ring of power series whose exponents are in C . Let $f = y^n + a_1(\underline{x})y^{n-1} + \dots + a_n(\underline{x})$ be a nonzero polynomial of $\mathbb{K}_C[[\underline{x}]][[y]]$. We say that f is free if it is irreducible in $\mathbb{K}_C[[\underline{x}]][[y]]$ and if it has a root (then all its roots) $y(\underline{x}) \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. Note that irreducible quasi-ordinary polynomials are free with respect to the cone \mathbb{R}_+^e . In general, we associate with a free polynomial f its set of characteristic exponents and characteristic sequences. We also associate with f its set of pseudo-approximate roots and we prove that the set of orders (with respect to a fixed order on $\mathbb{Z}^e \cap C$) of these polynomials generate the semigroup of f , which is defined to be the set of orders of polynomials of $\mathbb{K}_C[[\underline{x}]][[y]]$. Finally we prove that the semigroup is also generated by the set of orders of approximate roots of f (see Section 3). Note that the semigroup is free in the sense of [6]. This explain the notion of free polynomial. In Section 4 we apply our results to polynomials of $\mathbb{K}[[\underline{x}]][[y]] = \mathbb{K}_{\mathbb{R}_+^e}[[\underline{x}]][[y]]$. An irreducible polynomial $f \in \mathbb{K}[[\underline{x}]][[y]]$ is not free in general. Our main result is that f becomes free in $\mathbb{K}_C[[\underline{x}]][[y]]$ for a specific cone, after a preparation result. More precisely let $\Delta_y(f)$ be the y -discriminant of f . If f is a prepared polynomial (in the sense of Remark 4) then f is equivalent, modulo a birational transformation, to a quasi-ordinary polynomial F . This transformation is used in order to go from roots of F to roots of f , and these roots are in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ for the cone introduced in Proposition 17.

1 G-adic expansion and Approximate roots

In this section we recall the notion of G -adic expansion and the notion of approximate roots (see [1]). Let $R[Y]$ be the polynomial ring in one variable over an integral domain R .

Proposition 1 *Let f be a polynomial of degree n in $R[Y]$ and let d be a divisor of n . Let g be a monic polynomial of degree $\frac{n}{d}$, then there exist unique polynomials $a_1, \dots, a_d \in R[Y]$ with $\deg_Y(a_i) < \frac{n}{d}$ for all $i \in \{1, \dots, d\}$ such that $a_i \neq 0$, and $f = g^d + a_1g^{d-1} + \dots + a_d$.*

This expression is called the g -adic expansion of f . The **Tschirnhausen transform** of g with respect to f is defined to be $\tau_f(g) = g + d^{-1}a_1$. Note that the $\tau_f(g)$ is a monic polynomial of degree $\frac{n}{d}$ and so we can define recursively the i^{th} Tschirnhausen transform of g to be $\tau_f^i(g) = \tau_f(\tau_f^{(i-1)}(g))$ with $\tau_f^1(g) = \tau_f(g)$. By [2], $\tau_f(g) = g$ if and only if $a_1 = 0$ if and only if $\deg(f - g^d) < n - \frac{n}{d}$. In this case g is said to be the d^{th} approximate root of f . For every divisor d of n there exists a unique d^{th} approximate root of f . We denote it by $App(f, d)$.

More generally let $n = d_1 > d_2 > \dots > d_h$ be a sequence of integers such that d_{i+1} divides d_i for all $i \in \{1, \dots, h-1\}$, and set $e_i = \frac{d_i}{d_{i+1}}, 1 \leq i \leq h-1$, and $e_h = +\infty$. For all $i \in \{1, \dots, h\}$ let G_i be a polynomial of degree $\frac{n}{d_i}$ (in particular $\deg_Y G_1 = 1$) and let $G = (G_1, \dots, G_h)$. Let $B = \{\underline{b} = (b_1, \dots, b_h) \in \mathbb{N}^h, 0 \leq b_i < e_i \forall 1 \leq i \leq h\}$. Then f can be written in a unique way as $f = \sum_{\underline{b} \in B} c_{\underline{b}} G_1^{b_1} \dots G_h^{b_h}$. We call this expression the G -adic expansion of f .

2 Line Free Cones

In this section we recall the notion of line free cones, which will be used later in the paper. Let $C \subseteq \mathbb{R}^e$. We say that C is a cone if for all $s \in C$ and for all $\lambda \geq 0$, $\lambda s \in C$. A cone C is said to be finitely generated if there exists a finite subset $\{s_1, \dots, s_k\}$ of C such that for all $s \in C$,

$$s = \lambda_1 s_1 + \dots + \lambda_k s_k$$

for some $\lambda_1, \dots, \lambda_k \in \mathbb{R}$. If s_1, \dots, s_k can be chosen to be in \mathbb{Q}^e , then C is said to be rational. From now on we suppose that all considered cones are finitely generated and rational.

Definition 1 *Let C be a cone, then C is said to be a line free cone if $\forall v \in C - \{0\}$, $-v \notin C$.*

Given a line free cone, we can define the set of formal power series in several variables with exponents in C , denoted $\mathbb{K}_C[[\underline{x}]]$. More precisely an element $y \in \mathbb{K}_C[[\underline{x}]]$ is of the form $y = \sum_{\underline{p}=(p_1, \dots, p_e) \in C} \alpha_{\underline{p}} x_1^{p_1} \dots x_e^{p_e}$. It follows from [8] that this set is a ring.

Definition 2 *Let \leq be a total order on \mathbb{Z}^e , then \leq is said to be additive if for all $m, n, k \in \mathbb{Z}^e$ we have : $m \leq n \implies m + k \leq n + k$. An additive order on \mathbb{Z}^e is said to be compatible with a cone C if $m \geq \underline{0} = (0, \dots, 0)$ for all $m \in C \cap \mathbb{Z}^e$.*

With these notations we have the following:

Proposition 2 *(see [8]) Let C is a line free cone. There exists an additive total order \leq which is compatible with C . Moreover, if \leq is such an total orde, 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, and this minimal element is unique.*

Let $y = \sum_{\underline{p}} c_{\underline{p}} \underline{x}^{\underline{p}}$ be an element in $\mathbb{K}_C[[\underline{x}]]$. The support of y , denoted $\text{Supp}(y)$, is defined to be the set of elements $\underline{p} \in C$ such that $c_{\underline{p}} \neq 0$. It results from Proposition 2 that elements in $\text{Supp}(y)$ can be written as an increasing sequence with respect to the chosen additive order on C .

We shall now introduce the notion of free polynomials.

Definition 3 *Let C be a line free cone and let $f = y^n + a_1(\underline{x})y^{n-1} + \dots + a_n(\underline{x}) \in \mathbb{K}_C[[\underline{x}]] [y]$. Then f is said to be a free polynomial if f is irreducible in $\mathbb{K}_C[[\underline{x}]] [y]$ and if it has a root $y(\underline{x})$ in $\mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$.*

3 Characteristic sequences of a free polynomial

In this section we will introduce the set of characteristic sequences associated with a free polynomial as well as its semigroup. Let C be a line free cone and let \leq be an additive order on \mathbb{Z}^e compatible with C . Let $f \in \mathbb{K}_C[[\underline{x}]] [y]$ be a free polynomial and let $y \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$ be a root of f . Let L be the field of fractions of $\mathbb{K}_C[[\underline{x}]]$ and set $L_1 = L(x_1^{\frac{1}{n}}), L_2 = L(x_2^{\frac{1}{n}}), \dots, L_n = L_{n-1}(x_e^{\frac{1}{n}}) = L(x_1^{\frac{1}{n}}, \dots, x_e^{\frac{1}{n}})$. Then L_n is a galois extension of L of degree n^e . Let finally U_n be the set of n^{th} roots of unity in \mathbb{K} .

Let $\theta \in \text{Aut}(L_n/L)$. For all $i = 1, \dots, e$ we have $\theta(x_i^{\frac{1}{n}}) = \omega_i x_i^{\frac{1}{n}}$ for some $\omega_i \in U_n$. Then $\theta(\underline{x}^{\frac{p}{n}}) = k \underline{x}^{\frac{p}{n}}$, where k is a non zero element of \mathbb{K} . Let $\text{Roots}(f) = \{y_1, \dots, y_n\}$ 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 an automorphism $\theta \in \text{Aut}(L_n/L)$ such that $y_i = \theta(y)$, hence $y_i = \theta(y) = \sum c_p k_p \underline{x}^{\frac{p}{n}}$, $k_p \in \mathbb{K}^*$, and consequently $\text{Supp}(y) = \text{Supp}(y_i)$.

Let $z(\underline{x}) \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. Then $\text{Supp}(z(\underline{x}))$ can be arranged into an increasing sequence with respect to \leq . We define the order of z , denoted $O(z)$, to be $O(z) = \inf_{\leq}(\text{Supp}(z))$ if $z \neq 0$, and $O(0) = -\infty$. We set $LM(z) = \underline{x}^{\frac{p}{n}}$ where $\underline{p} = O(z)$, 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 . We finally set $\text{Info}(z) = LC(z)LM(z)$ and we call it the initial form of y .

Definition 4 Let the notations be as above with $\{y_1, \dots, y_n\} = \text{Roots}(f)$ and $y_1 = y$. The set of characteristic exponents of f is defined to be $\{O(y_i - y_j), y_i \neq y_j\}$. Similarly we define the set of characteristic monomials of f to be $\{LM(y_i - y_j), y_i \neq y_j\}$.

Next we will give some properties of the set of characteristic exponents.

Proposition 3 Let the notations be as above. Then the set of characteristic exponents of f is equal to the set $\{O(y_k - y), y_k \neq y\}$. In particular the set of characteristic monomials of f is given by $\{LM(y_k - y), k = 2, \dots, n\} = \{LM(\theta(y) - y), \theta(y) \neq y, \theta \in \text{Aut}(L_n/L)\}$.

Proof. We only need to prove that any characteristic exponent is of the form $O(y_k - y)$ for some k . Let $1 \leq i \neq j \leq n$ and 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 $\epsilon_{ij} \in L_n$ and $O(\epsilon_{ij}) > O(M_{ij})$. Let $\theta \in \text{Aut}(L_n/L)$, such that $\theta(y_j) = y$, then $\theta(y_i) = y_k$ for some $1 \leq k \leq n$, and $\theta(y_i - y_j) = \theta(y_i) - \theta(y_j) = y_k - y = c_{k1}M_{k1} + \epsilon_{k1} = \theta(c_{ij}M_{ij} + \epsilon_{ij}) = c_{ij}\alpha M_{ij} + \theta(\epsilon_{ij})$ with $\alpha \neq 0$, $O(\epsilon_{k1}) > O(M_{k1})$, and $O(\theta(\epsilon_{ij})) > O(M_{ij})$. Hence $M_{k1} = M_{ij} = LM(y_i - y_j)$. This proves our assertion. ■

Let $\{M_1, \dots, M_h\}$ be the set of characteristic monomials of f and write $M_i = \underline{x}^{\frac{m_i}{n}}$. Then $\{m_1, \dots, m_h\}$ is the set of characteristic exponents of f . We shall suppose that $m_1 < m_2 < \dots < m_h$.

Proposition 4 Let the notations be as above. We have $L(y) = L(M_1, \dots, M_h)$.

Proof. Let $\theta \in \text{Aut}(L_n/L(y))$, then θ is an L -automorphism of L_n with $\theta(y) = y$. We have $\theta(y) = \theta(\sum c_p \underline{x}^{\frac{p}{n}}) = \sum c_p \theta(\underline{x}^{\frac{p}{n}}) = \sum c_p k_p \underline{x}^{\frac{p}{n}} = y = \sum c_p \underline{x}^{\frac{p}{n}}$, with $k_p \neq 0$ for all $\underline{p} \in \text{Supp}(y)$, and so $\theta(\underline{x}^{\frac{p}{n}}) = \underline{x}^{\frac{p}{n}}$. Hence $\underline{x}^{\frac{p}{n}} \in L(y)$ for all $\underline{p} \in \text{Supp}(y)$. In particular, since M_1, \dots, M_h are monomials of y , then $M_1, \dots, M_h \in L(y)$, and so $L(M_1, \dots, M_h) \subset L(y)$. Conversely, if $\theta \in \text{Aut}(L_n/L(M_1, \dots, M_h))$, i.e if θ is an L automorphism of L_n such that $\theta(M_i) = M_i \forall i = 1, \dots, h$, 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 $\theta(M_i) \neq M_i$ which contradicts the hypothesis. This proves our assertion. ■

Note that for all $i \in \{1, \dots, h\}$, $L(M_1, \dots, M_i) = L[M_1, \dots, M_i]$ since M_i is algebraic over L .

Proposition 5 Let the notations be as above. If $m \in \mathbb{Z}^e \cap \text{Supp}(y)$ 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 $M \in L(y) = L[M_1, \dots, M_h]$, 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 $f_1, \dots, f_l, g_1, \dots, g_l \in \mathbb{K}_C[[\underline{x}]]$ 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 $\underline{x}^b = LM(g_1 \dots g_l M) = \underline{x}^a M_1^{\alpha_1^i} \dots M_h^{\alpha_h^i}$ for some $i \in \{1, \dots, l\}$ and $a \in \mathbb{Z}^e$. In particular $nb + m = na + \alpha_1^i m_1 + \dots + \alpha_h^i m_h$, and so $m = n(a - b) + \alpha_1^i m_1 + \dots + \alpha_h^i m_h \in (n\mathbb{Z})^e + \sum_{i=1}^h m_i \mathbb{Z}$. ■

Remark 1 Write $F_0 = L$ and for all $i \in \{1, \dots, h\}$, $F_i = L[M_1, \dots, M_i] = F_{i-1}[M_i]$. Also let $G_0 = (n\mathbb{Z})^e$ and for all $i \in \{1, \dots, h\}$, $G_i = (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$. As in Proposition 5, we can prove that for any monomial $M = \underline{x}^{\frac{m}{n}}$ with $m \in C$, we have $M \in F_i \Leftrightarrow m \in G_i$.

Next we will define the set of characteristic sequences associated with f .

Definition 5 Let the notations be as above and let $\{m_1, \dots, m_h\}$ be the set of characteristic exponents of f . Let I_e be the $e \times e$ identity matrix. We shall introduce the following sequences:

- The GCD-sequence $\{D_i\}_{1 \leq i \leq h+1}$, where $D_1 = n^e$ and for all $i \in \{1, \dots, h\}$, $D_{i+1} = \gcd(nI_e, m_1^T, \dots, m_i^T)$, the gcd of the (e, e) minors of the $e \times (e + i)$ matrix $(nI_e, m_1^T, \dots, m_i^T)$.
- The d -sequence $\{d_i\}_{1 \leq i \leq h+1}$, where $d_i = \frac{D_i}{D_{h+1}}$.
- The e -sequence $\{e_i\}_{1 \leq i \leq h}$, where $e_i = \frac{D_i}{D_{i+1}} = \frac{d_i}{d_{i+1}}$.
- The r -sequence $\{r_0^1, \dots, r_0^e, r_1, \dots, r_h\}$, where (r_0^1, \dots, r_0^e) is the canonical basis of $(n\mathbb{Z})^e$, $r_1 = m_1$, and for all $i \in \{2, \dots, h\}$ $r_i = e_{i-1} r_{i-1} + m_i - m_{i-1}$. Note that for all $i \in \{2, \dots, h\}$, $r_i d_i = r_1 d_1 + \sum_{k=2}^i (m_k - m_{k-1}) d_k = \sum_{k=1}^{i-1} (d_k - d_{k+1}) m_k + m_i d_i$.

Remark 2 Let the notations be as in Definition 5 and let v be a non zero vector in \mathbb{Z}^e . Let \tilde{D} be the gcd of the (e, e) minors of the matrix $(nI_e, m_1^T, \dots, m_i^T, v^T)$, then $v \in (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$ if and only if $D_{i+1} = \tilde{D}$. More generally, $\frac{D_{i+1}}{D} \cdot v \in (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$ and if $D_{i+1} > \tilde{D}$ then for all $1 \leq k < \frac{D_{i+1}}{D}$, $kv \notin (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$.

Proposition 6 For all $i = 1, \dots, h-1$ let $H_i = L(M = \underline{x}^{\frac{m}{n}}, m \in \text{Supp}(y), m < m_{i+1})$. Then we have

- (i) $F_i = H_i$ and m_i does not belong to F_{i-1}
- (ii) $[F_i : F_{i-1}]$, the degree of extension of F_i over F_{i-1} , is equal to e_i .

Proof. (i) Since $m_j < m_{i+1}$ for all $j = 1, \dots, i$, then $m_1, \dots, m_i \in H_i$, 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 $\theta \in \text{Aut}(L_n/F_i)$, 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 $\theta \in \text{Aut}(L_n \setminus L)$ such that $\theta(y) - y = cM_i + \varepsilon$ with $O(\varepsilon) > m_i$ and c a non zero constant (such a θ obviously exists since M_i is a characteristic monomial of f), then $\theta(M_j) = M_j$ for all $j = 1, \dots, i-1$ and $\theta(M_i) \neq M_i$, and so $\theta \in \text{Aut}(L_n \setminus F_{i-1})$ with $\theta(M_i) \neq M_i$, hence M_i does not belong to F_{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 $\alpha m_i \notin G_{i-1}$. Now let $g = y^l + a_1 y^{l-1} + \dots + a_l$ 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 $k \in \{0, \dots, l-1\}$ such that $\underline{x}^{l \frac{m_i}{n}} = \underline{x}^{\frac{\alpha}{n}} \underline{x}^{\frac{k m_i}{n}}$ 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 $l \geq e_i$. But g divides $Y^{e_i} - x^{e_i \cdot \frac{m_i}{n}}$. Hence $g = Y^{e_i} - x^{e_i \cdot \frac{m_i}{n}}$, and consequently $[F_i : F_{i-1}] = e_i$. ■

Proposition 7 *Let the notations be as above. For all $i \in \{1, \dots, h\}$ we have $e_i r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$. Moreover, $\alpha r_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ for all $1 \leq \alpha < e_i$.*

Proof. We can easily prove that $r_i = m_i + \sum_{j=1}^{i-1} (e_j - 1)r_j$ for all $i \in \{2, \dots, h\}$, hence 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 and $(n\mathbb{Z})^e + \sum_{j=1}^i r_j \mathbb{Z} = (n\mathbb{Z})^e + \sum_{j=1}^i m_j \mathbb{Z}$ for all $i \in \{1, \dots, h\}$. In particular, for all $\alpha \in \mathbb{N}$, $\alpha r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ if and only if $\alpha m_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$. Let $i \in \{1, \dots, h\}$. By Remark 2, $e_i m_i = \frac{D_i}{D_{i+1}} m_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$ and $\alpha m_i \notin (n\mathbb{Z})^e + \sum_{j=1}^{i-1} m_j \mathbb{Z}$ for all $1 \leq \alpha < e_i$. Hence $e_i r_i \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{Z}$ 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 3 *Since $[L(y) : L] = n$, then it follows from proposition 6 that $[L(y) : L] = e_1 \dots e_h = \frac{D_1}{D_{h+1}}$. But $[L(y); L] = n$ and $D_1 = n^e$, hence $D_{h+1} = n^{e-1}$. It follows that $d_1 = n$ and $d_{h+1} = 1$.*

For all $i \in \{1, \dots, h\}$, define the following sets: $Q(i) = \{\theta \in \text{Aut}(L_n/L) \mid O(y - \theta(y)) < m_i\}$, $R(i) = \{\theta \in \text{Aut}(L_n/L) \mid O(y - \theta(y)) \geq m_i\}$ and $S(i) = \{\theta \in \text{Aut}(L_n/L) \mid O(y - \theta(y)) = m_i\}$. With these notations we have the following:

Proposition 8 *$\#R(i) = D_i$ and $\#S(i) = D_i - D_{i+1}$, where $\#$ stand for the cardinality.*

Proof. We have $\theta \in R(i) \Leftrightarrow \theta(M_j) = M_j$ for all $j < i \Leftrightarrow \theta \in \text{Aut}(L_n/L(M_1, \dots, M_{i-1}))$, hence $\#R(i) = \#\text{Aut}(L_n/L(M_1, \dots, M_{i-1})) = [L_n : L(M_1, \dots, M_{i-1})] = [L_n : F_{i-1}]$. By proposition 6 we have $[F_{i-1} : L] = [F_{i-1} : F_{i-2}] \dots [F_1 : L] = e_{i-1} \dots e_1 = \frac{D_1}{D_i} = \frac{n^e}{D_i}$. But $[L_n : L] = [L_n : F_{i-1}][F_{i-1} : L] = n^e$, then $[L_n : F_{i-1}] = D_i$, and so $\#R(i) = D_i$. Now $R(i+1) \subset R(i)$ and $\theta \in S(i)$ if and only if $O(y - \theta(y)) = m_i$ if and only if $\theta \in R(i)$ and $\theta \notin R(i+1)$, hence $\#S(i) = D_i - D_{i+1}$. ■

The statement and the proof of Proposition 8 imply the following: for all $i \in \{1, \dots, h\}$, let $\tilde{R}(i) = \{y_k \mid O(y - y_k) \geq m_i\}$ and $\tilde{S}(i) = \{y_k \mid O(y - y_k) = m_i\}$. We have:

Proposition 9 *$\#\tilde{R}(i) = d_i$ and $\#\tilde{S}(i) = d_i - d_{i+1}$.*

3.1 Pseudo roots, semigroup, and approximate roots of a free polynomial

Let the notations be as above. For all $i \in \{1, \dots, h\}$ we will define a specific free polynomial G_i , called the i^{th} pseudo root of f such that $O(G_i(\underline{x}, y(\underline{x}))) = r_i$. Also we will define the semigroup $\Gamma(f)$ of f and we will construct a system of generators of $\Gamma(f)$. Finally we will prove that $O(f, \text{App}(f, d_i)) = r_i$ for all $i \in \{1, \dots, h\}$. Let $y(x) = \sum c_p \underline{x}^{\frac{p}{n}}$ be a root of f and let $m \in \text{Supp}(y)$. We set $y_{<m} = \sum_{p < m} c_p \underline{x}^{\frac{p}{n}}$ and we call $y_{<m}$ the m -truncation of y .

Definition 6 *For all $i \in \{1, \dots, h\}$, we define the i^{th} pseudo root of f to be the minimal polynomial of $y_{<m_i}$ over L . We denote it by G_i .*

In the following we shall study the properties of G_i . In particular we shall prove that $O(f, G_i) = r_i$.

Proposition 10 *Let the notations be as above. For all $i = 1, \dots, h$, $\deg_y(G_i) = \frac{n^e}{D_i} = \frac{n}{d_i}$.*

Proof. By proposition 6 we have $L(y_{<m_i}) = L(M_1, \dots, M_{i-1})$. In particular $\deg_y(G_i) = [L(y_{<m_i}) : L] = [L(M_1, \dots, M_{i-1}) : L] = \frac{n^e}{D_i} = \frac{n}{d_i}$. ■

Proposition 11 *The polynomial G_i is free, and its characteristic exponents are $\frac{m_1}{d_i}, \dots, \frac{m_{i-1}}{d_i}$.*

Proof. The polynomial G_i is free from the definition. We shall prove that $y_{<m_i} \in \mathbb{K}_C[[x^{\frac{1}{d_i}}]]$. 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 $(m_0^1, \dots, m_0^e, m_1, \dots, m_{i-1}, \lambda)$, then $D = D_i$. For all $l \in \{1, \dots, e\}$ the matrix $A_l = (m_0^1, \dots, m_0^{l-1}, \lambda, m_0^{l+1}, \dots, m_0^e)$ is one of the minors of the matrix $(m_0^1, \dots, m_0^e, m_1, \dots, m_{i-1})$, then D_i divides $\text{Det}(A_l)$. Write $\lambda = (\lambda_1, \dots, \lambda_e)$, then obviously $\text{Det}(A_l) = n^{e-1} \lambda_l$, and so D_i divides $n^{e-1} \lambda_l$ for all $l \in \{1, \dots, e\}$. It follows that $\frac{n^{e-1} \lambda}{D_i} = \frac{\lambda}{d_i} \in \mathbb{Z}^e$. Moreover, since $\lambda \in C$, and $\frac{1}{d_i} \geq 0$, then $\frac{\lambda}{d_i} \in C$.

Hence $\underline{x}^{\frac{\lambda}{n}} = \underline{x}^{\frac{\lambda'}{d_i}}$ where $\lambda' = \frac{\lambda}{d_i}$, and so $\underline{x}^{\frac{\lambda}{n}} \in \mathbb{K}_C[[x^{\frac{1}{d_i}}]]$.

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 $j \in \{1, \dots, i-1\}$. But $\frac{m_j}{n} = \frac{\frac{m_j}{d_i}}{\frac{n}{d_i}}$, hence the set of characteristic monomials of G_i is $\{\frac{m_1}{d_i}, \dots, \frac{m_{i-1}}{d_i}\}$. ■

Proposition 12 *Let the notations be as above. For all $i \in \{1, \dots, h\}$, we have $O(f(\underline{x}, y_{<m_i}(\underline{x}))) = \frac{r_i d_i}{n}$.*

Proof. We have $f(\underline{x}, y_{<m_i}) = \prod_{k=1}^n (y_{<m_i} - y_k)$ with the assumption that $y = y_1$. Clearly $O(y_{<m_i} - y_k) = O(y_1 - y_k)$ if $O(y_1 - y_k) < \frac{m_i}{n}$ and $\frac{m_i}{n}$ otherwise. It follows from Proposition 9 that $O(\prod_{k=1}^n (y_{<m_i} - y_k)) = \frac{1}{n} (\sum_{k=1}^{i-1} (d_k - d_{k+1}) m_k + d_i m_i)$, which is equal to $\frac{r_i d_i}{n}$ by Definition 5. ■

Let $g = y^m + b_1(\underline{x})y^{m-1} + \dots + b_m(\underline{x})$ be free polynomial of $\mathbb{K}_C[[\underline{x}]][[y]]$ and let z_1, \dots, z_m be the set of roots of g in $\mathbb{K}[[x^{\frac{1}{m}}]]$. We set $O(f, g) = \sum_{i=1}^n O(g(\underline{x}, y_i(\underline{x})))$. Clearly $O(f, g) = \sum_{j=1}^m O(f(\underline{x}, z_j(\underline{x}))) = O(g, f) = O(\text{Res}_y(f, g))$, where Res stand for the y -resultant of f, g . As a corollary of Proposition 12 we get the following:

Corollary 1 *With the notations above, we have $O(f, G_i) = r_i$*

Proof. In fact, $O(f, G_i) = O(G_i, f) = \frac{n}{d_i} O(f(\underline{x}, y_{<m_i})) = r_i$. ■

As a corollary we get the following:

Proposition 13 *Let $\{G_1, \dots, G_h\}$ be the set of pseudo roots of f . Let $i \in \{1, \dots, h\}$, then we have $O(G_i, G_j) = \frac{r_j}{d_i}$ for all $j \in \{1, \dots, i-1\}$.*

Proof. This is an immediate consequence of Corollary 1 because G_1, \dots, G_{i-1} is the set of pseudo-approximate roots of G_i and the \underline{r} sequence of G_i is given by $\frac{r_0^1}{d_i}, \dots, \frac{r_0^e}{d_i}, \frac{r_1}{d_i}, \dots, \frac{r_{i-1}}{d_i}$. ■

Definition 7 *Given $g \in \mathbb{K}_C[[\underline{x}]][[y]]$, $f \nmid g$, we set $O(f, g) = \sum_{i=1}^n O(g(\underline{x}, y_i)) = nO(g(\underline{x}, y(\underline{x})))$. Clearly $O(f, g_1 g_2) = O(f, g_1) + O(f, g_2)$. It follows that $\Gamma(f) = \{O(f, g) | g \in \mathbb{K}_C[[\underline{x}]][[y]] \setminus (f)\}$ is a subsemigroup of \mathbb{Z}^e . We call it the semigroup associated with f .*

In the following we will prove that $(r_0^1, \dots, r_0^e, r_1, \dots, r_h)$ is a system of generators of $\Gamma(f)$. We shall need the following result:

Lemma 1 *Let the notations be as above and let $\underline{\alpha} = (\alpha_0^1, \dots, \alpha_0^e, \alpha_1, \dots, \alpha_h), \underline{\beta} = (\beta_0^1, \dots, \beta_0^e, \beta_1, \dots, \beta_h)$ be two elements of $\mathbb{Z}^e \times \mathbb{N}^h$ such that $0 \leq \alpha_i, \beta_i < e_i$ for all $i \in \{1, \dots, h\}$. If $a = \sum_{i=1}^e \alpha_0^i r_0^i + \sum_{j=1}^h \alpha_j r_j = \sum_{i=1}^e \beta_0^i r_0^i + \sum_{j=1}^h \beta_j r_j$ then $\underline{\alpha} = \underline{\beta}$.*

Proof. Suppose that $\underline{\alpha} \neq \underline{\beta}$ and let k be the smallest integer ≥ 1 such that $\alpha_i = \beta_i$ for all $i \geq k+1$. Suppose that $\alpha_k > \beta_k$. We have $(\alpha_k - \beta_k)r_k = \sum_{i=1}^e (\beta_0^i - \alpha_0^i)r_0^i + \sum_{j=1}^{k-1} (\beta_j - \alpha_j)r_j$. This contradicts Proposition 7. ■

Lemma 2 *Let $g \in \mathbb{K}_C[[x]][y]$ and suppose that $f \nmid g$. There exists a unique $\underline{\theta} = (\theta_0^1, \dots, \theta_0^e, \theta_1, \dots, \theta_h) \in \mathbb{Z}^e \times \mathbb{N}^h$ such that $0 \leq \theta_j < e_j$ for all $j \in \{1, \dots, h\}$ and $O(f, g) = \sum_{i=1}^e \theta_0^i r_0^i + \sum_{j=1}^h \theta_j r_j$. In particular $\Gamma(f)$ is generated by $r_0^1, \dots, r_0^e, r_1, \dots, r_h$.*

Proof. Let $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h} f^{\theta_{h+1}}$ be the expansion of g with respect to (G_1, \dots, G_h, f) and recall that for all $\underline{\theta}$, if $c_{\underline{\theta}} \neq 0$ then $\underline{\theta} = (\theta_1, \dots, \theta_{h+1}) \in \{(\beta_1, \dots, \beta_{h+1}) \in \mathbb{N}^{h+1}, 0 \leq \beta_j < e_j \forall j = 1, \dots, h\}$. The hypothesis implies that there exists at least one $\underline{\theta}$ such that $c_{\underline{\theta}} \neq 0$ and $\theta_{h+1} = 0$. Let $M = c_{\underline{\theta}}(\underline{x}) G_1^{\theta_1} \dots G_h^{\theta_h}$, $N = c_{\underline{\theta}'}(\underline{x}) G_1^{\theta_1'} \dots G_h^{\theta_h'}$ be two distinct monomials of g . It follows from Lemma 1 that $O(f, M) \neq O(f, N)$. Hence there exists a unique monomial \tilde{M} of g such that $O(f, g) = O(f, \tilde{M})$. This proves our assertion. ■

Remark 4 *In the Lemma above, if $\deg_y g < \frac{n}{d_i}$ for some $i \in \{1, \dots, h\}$, then $O(f, g) \in (n\mathbb{Z})^e + \sum_{k=1}^{i-1} r_k \mathbb{N}$. Moreover, $O(f, g) = d_i O(G_i, g)$. In fact, in this case, any monomial M of the expansion of g with respect to (G_1, \dots, G_h, f) is a monomial in G_1, \dots, G_{i-1} . Hence this expansion coincides with that of g with respect to $(G_1, \dots, G_{i-1}, G_i)$. If M is the unique monomial such that $O(f, g) = O(f, M)$ then M is the unique monomial such that $O(G_i, g) = O(G_i, M)$. But $O(f, M) = d_i O(G_i, M)$. This proves our assertion. ■*

The next Proposition shows that we can calculate a system of generators of $\Gamma(f)$ only with the set of approximate roots of f .

Proposition 14 *For all $i \in \{1, \dots, h\}$, let $g_i = \text{App}(f, d_i)$. We have $O(f, g_i) = r_i$.*

Proof. Let $i = h$ and consider the G_h -adic expansion of f , $f = G_h^{d_h} + C_1(\underline{x}, y) G_h^{d_h-1} + \dots + C_{d_h}(\underline{x}, y) = \sum_{k=0}^{d_h} C_k(\underline{x}, y) G_h^{d_h-k}$ where $C_0 = 1$ and $C_k(\underline{x}, y) \in \mathbb{K}_C[[x]][y]$ with $\deg_y(C_k(\underline{x}, y)) < \frac{n}{d_h}$ for all $k = 1, \dots, d_h$. Consider the Tschirnhausen transform of G_h with respect to f given by $\tau_f(G_h) = G_h + d_h^{-1} C_1(\underline{x}, y)$. We have $O(f, G_h) = r_h$, hence we need to prove that $O(f, C_1) > r_h$.

Let $k \in \{0, \dots, d_h - 1\}$. For all $\alpha \neq k$, 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 Remark 4, $O(f, C_{\alpha}), O(f, C_k) \in (n\mathbb{Z})^e + r_1\mathbb{Z} + \dots + r_{h-1}\mathbb{Z}$, and so $(\alpha - k)r_h \in (n\mathbb{Z})^e + r_1\mathbb{N} + \dots + r_{h-1}\mathbb{N}$, with $0 < \alpha - k < d_h = e_h$. This contradicts Proposition 7. Now a similar argument shows that

$O(f, C_k G_h^{d_h-k}) = O(f, C_k) + (d_h - k)r_h \neq O(f, C_{d_h})$. As $f(\underline{x}, y(\underline{x})) = 0$, we get that $O(f, C_{d_h}) = O(f, G_h^{d_h}) = r_h d_h < O(C_k G_h^{d_h-k})$, hence $O(f, C_k) > k r_h$. This is true for $k = 1$, consequently $O(f, C_1) > r_h$, and $O(f, \tau_f(G_h)) = r_h$. Repeating this process, we get that $O(f, \tau_f^l(G_h)) = r_h$ for all $l \geq 1$. But $g_h = \text{App}(f, d_h) = \tau_f^{l_0}(G_h)$ for some l_0 . Hence $O(f, g_h) = r_h$. Now suppose that $O(f, g_k) = r_k$ for all $k > i$, and let us prove that $O(f, g_i) = r_i$. Note that $g_i = \text{App}(g_{i+1}, e_i)$. Let

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

be the G_i -adic expansion of g_{i+1} and consider $O(f, g_{i+1})$. For all $k \in \{1, \dots, e_i\}$, $O(f, \beta_k G_i^{e_i-k}) = O(f, \beta_k) + (e_i - k)r_i$. But $O(f, \beta_k) \in (n\mathbb{Z})^e + \sum_{j=1}^{i-1} r_j \mathbb{N}$ because $\deg_y \beta_k < \frac{n}{d_i}$, and $r_{i+1} \notin (n\mathbb{Z})^e + \sum_{j=1}^i r_j \mathbb{N}$. Now a similar argument as above shows that $r_i e_i = O(f, G_i^{e_i}) = O(f, \beta_{e_i}) < O(\beta_1 G_i^{e_i-1})$. Hence $O(f, \beta_1) > r_i$. In particular

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

Applying the same process to f and $\tau_{g_{i+1}}(G_i)$ instead of f and G_i . We get that $O(f, \tau_{g_{i+1}}^2(G_i)) = r_i$. But $g_i = \tau_{g_{i+1}}^{l_i}(G_i)$ for some l_i , hence $O(f, g_i) = O(f, \tau_{g_{i+1}}^{e_i}(G_i)) = r_i$. This proves our assertion. ■

Remark 5 *The semigroup $\Gamma(f)$ is a free affine semigroup with respect to the arrangement $(r_0^1, \dots, r_0^e, r_1, \dots, r_h)$ (see [6] for the definition and properties of free affine semigroup). This explains the notion of free polynomials introduced in the paper.*

4 Solutions of formal power series

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 degree n in $\mathbb{K}[[\underline{x}]][[y]]$. In this Section we shall prove that, modulo an automorphism of $\mathbb{K}[[\underline{x}]][[y]]$, and under an irreducibility condition, f is free in $\mathbb{K}_C[[\underline{x}]][[y]]$ for some specific line free cone C . Let $\Delta(\underline{x})$ be the discriminant of f in y , and write $\Delta(\underline{x}) = \sum_{p \in \mathbb{N}^e} c_p \underline{x}^p = \sum_{d \geq 0} u_d(\underline{x})$ where for all $d \geq 0$, u_d is the homogeneous component of degree d of Δ . Let $a = \inf\{d, u_d \neq 0\}$. If $a = 0$, then f is a quasi-ordinary polynomial. Suppose that $a > 0$, and, without loss of generality, that $u_a \notin \mathbb{K}[[x_2, \dots, x_e]]$. In the next remark we will show how to prepare our polynomial so that the smallest homogeneous component u_a of Δ contains a monomial in x_1 .

Remark 6 (Preparation) *Consider the mapping $\xi : \mathbb{K}[[\underline{x}]] \mapsto \mathbb{K}[[\underline{x}]]$, defined by $\xi(x_1) = X_1$ and $\xi(x_i) = X_i + tX_1$ for all $i \in \{2, \dots, e\}$, where t is a parameter to be determined. Let $\psi : \mathbb{K}[[\underline{x}]][[y]] \mapsto \mathbb{K}[[\underline{X}]][[y]]$ be the map defined as follows: if $H = h_0(\underline{x})y^m + \dots + h_{m-1}(\underline{x})y + h_m(\underline{x}) \in \mathbb{K}[[\underline{x}]][[y]]$ then $\psi(H) = \xi(h_0(\underline{x}))y^m + \dots + \xi(h_{m-1}(\underline{x}))y + \xi(h_m(\underline{x}))$. Then we easily prove that ψ is an isomorphism. If Δ' is the discriminant of $\psi(f)$ and if $v_d(\underline{X}) = u_d(X_1, X_2 + tX_1, \dots, X_e + tX_1)$ then $\Delta' = \sum_{d \geq a} v_d$. But $v_d(\underline{X}) = \varepsilon_d(t)X_1^d + v'_d$, where v'_d is a homogeneous polynomial of degree d , and $\varepsilon_d(t)$ is a polynomial in t . Since \mathbb{K} is an infinite field, then we can choose $t \in \mathbb{K}$ such that $\varepsilon_a(t) \neq 0$.*

In the following we shall say that a polynomial f is prepared if it satisfies the condition of Remark 6, i.e. its discriminant is of the form $\Delta = \sum_{d \geq 0} u_d$ such that the smallest homogeneous component is of the form $u_a = c_a x_1^a + u'_a$ with $c_a \neq 0$ and $u'_a \in \mathbb{K}[[x_2, \dots, x_e]]$. The next proposition shows that a prepared polynomial is birationally equivalent to a quasi-ordinary polynomial.

Proposition 15 *With the notations above, if f is a prepared polynomial then $F(X_1, \dots, X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y)$ is a quasi-ordinary polynomial.*

Proof. Let Δ be the discriminant of f . The discriminant Δ_N of F is $\Delta_N = \Delta(X_1, X_2X_1, \dots, X_eX_1)$. Write $\Delta = \sum_{d \geq a} u_d$, where u_d is the homogeneous component of degree d of Δ and $u_a \neq 0$, then $\Delta_N = \sum_{d \geq a} w_d(\underline{X})$ with $w_d(\underline{X}) = u_d(X_1, X_2X_1, \dots, X_eX_1)$. For all $d \geq a$, we have

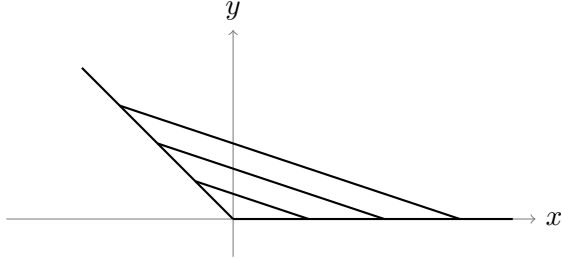
$$w_d(\underline{X}) = X_1^d u_d(1, X_2, \dots, X_e) = X_1^d (c_d + \varepsilon_d(X_1, \dots, X_e)) = X_1^a X_1^{d-a} (c_d + \varepsilon_d(X_1, \dots, X_e))$$

where $c_d \in \mathbb{K}$ and $\varepsilon_d(0, \dots, 0) = 0$. Since f is prepared, then $c_a \neq 0$, hence $\Delta_N = X_1^a (c_a + \varepsilon(\underline{X}))$ and $\varepsilon(\underline{X})$ is a non unit in $\mathbb{K}[[\underline{X}]]$. So F is a quasi-ordinary polynomial. ■

We will now introduce the following line free cone.

Proposition 16 *The set $C = \{(c_1, \dots, c_e) \in \mathbb{R}^e, c_1 \geq -(c_2 + \dots + c_e), c_i \geq 0 \forall 2 \leq i \leq e\}$ is a line free convex cone.*

Proof. Let $c = (c_1, \dots, c_e) \in C$ and $\lambda \geq 0$, then obviously $\lambda c \in C$, hence C is a cone. Moreover, if $c = (c_1, \dots, c_e), c' = (c'_1, \dots, c'_e) \in C$, then $c + c' \in C$, and so C is a convex cone. Let $c = (c_1, \dots, c_e) \in C$ such that $c \neq \underline{0}$, and let us prove that $-c = (-c_1, \dots, -c_e) \notin C$. We have $c_i \geq 0$ for all $i \in \{2, \dots, e\}$. If $c_i > 0$ for some $i \in \{2, \dots, e\}$, then obviously $-c = (-c_1, \dots, -c_e) \notin C$. If $c_i = 0$ for all $i \in \{2, \dots, e\}$, then $c_1 \geq -(c_2 + \dots + c_e) = 0$, but $c \neq \underline{0}$, then $c_1 > 0$, and so $-c = (-c_1, 0, \dots, 0) \notin C$. Hence C is a line free cone. ■



Along this Section, C will denote the cone defined in proposition 16.

Lemma 3 *Let $Y(\underline{X})$ be an element of $\mathbb{K}[[\underline{X}]]$. If $y(\underline{x}) = Y(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})$ then $y(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$.*

Proof. Write $Y(\underline{X}) = \sum_{\underline{a}} \gamma_{\underline{a}} \underline{X}^{\underline{a}}$, then $y(\underline{x}) = \sum_{\underline{a}} \gamma_{\underline{a}} x_1^{a_1 - (a_2 + \dots + a_e)} x_2^{a_2} \dots x_e^{a_e}$. In particular $\text{Supp}(y) = \{(a_1 - (a_2 + \dots + a_e), a_2, \dots, a_e), \underline{a} \in \text{Supp}(Y)\}$. As $a_1 \geq 0$, we have $(a_1 - (a_2 + \dots + a_e)) \geq -(a_2 + \dots + a_e)$, hence $y(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$. ■

The following proposition characterizes the irreducibility of elements of $\mathbb{K}[[\underline{x}]] [y]$ in $\mathbb{K}_C[[\underline{x}]] [y]$.

Proposition 17 *With the notations above, f is irreducible in $\mathbb{K}_C[[\underline{x}]] [y]$ if and only if $F(X_1, \dots, X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y)$ is irreducible in $\mathbb{K}[[\underline{X}]] [y]$.*

Proof. Suppose that f is irreducible in $\mathbb{K}_C[[\underline{x}]] [y]$. If F is reducible in $\mathbb{K}[[\underline{X}]] [y]$, then there exist monic polynomials $G, H \in \mathbb{K}[[\underline{X}]] [y]$ such that $F = GH$ and $0 < \deg_y(G), \deg_y(H) < n$. But $f(x_1, \dots, x_e, y) = F(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}, y)$. Then:

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

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 $G(\underline{X}, y) = y^m + a_1(\underline{X})y^{m-1} + \dots + a_m(\underline{X})$, where $a_i(\underline{X}) \in \mathbb{K}[[\underline{X}]]$ for all $i = 1, \dots, m$. We have:

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

Since $a_i(\underline{X}) \in \mathbb{K}[[\underline{X}]]$ for all $i = 1, \dots, m$, then by Lemma 3 we get that $a_i(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}) \in \mathbb{K}_C[[\underline{x}]]$ for all $i = 1, \dots, m$. 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 $f = gh$ 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. Conversely suppose that F is an irreducible polynomial in $\mathbb{K}[[\underline{X}]][[y]]$. If f is reducible in $\mathbb{K}_C[[\underline{x}]][[y]]$, then there exist $h_1, h_2 \in \mathbb{K}_C[[\underline{x}]][[y]]$ such that $f = h_1h_2$ with $0 < \deg_y(h_1), \deg_y(h_2) < \deg_y(f)$. Given $a(\underline{x}) = \sum c_a x_1^{a_1} \dots x_e^{a_e} \in \mathbb{K}_C[[\underline{x}]]$, we have

$$a(X_1, X_2X_1, \dots, X_eX_1) = \sum c_a X_1^{a_1} (X_2X_1)^{a_2} \dots (X_eX_1)^{a_e} = \sum c_a X_1^{a_1+a_2+\dots+a_e} X_2^{a_2} \dots X_e^{a_e}$$

Since $a(\underline{x}) \in \mathbb{K}_C[[\underline{x}]]$, then $a_1 \geq -(a_2 + \dots + a_e)$ for all $(a_1, \dots, a_e) \in \text{Supp}(a(\underline{x}))$. It follows that $a_1 + a_2 + \dots + a_e \geq 0$ for all $(a_1, \dots, a_e) \in \text{Supp}(a(\underline{x}))$. Hence, $a(X_1, X_2X_1, \dots, X_eX_1) \in \mathbb{K}[[\underline{X}]]$. Then $h_1(X_1, X_2X_1, \dots, X_eX_1, y), h_2(X_1, X_2X_1, \dots, X_eX_1, y) \in \mathbb{K}[[\underline{X}]][[y]]$. But

$$F(X_1, \dots, X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y) = h_1(X_1, X_2X_1, \dots, X_eX_1, y)h_2(X_1, X_2X_1, \dots, X_eX_1, y).$$

This contradicts the hypothesis. ■

In the following we give a characterization for the polynomial f to be free.

Proposition 18 *Suppose that f is a prepared polynomial. If f is irreducible in $\mathbb{K}_C[[\underline{x}]][[y]]$, then it is free.*

Proof. By Proposition 15, $F(X_1, \dots, X_e, y) = f(X_1, X_2X_1, \dots, X_eX_1, y)$ is a quasi-ordinary polynomial of $\mathbb{K}[[\underline{X}]][[y]]$, and by Proposition 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 in $\mathbb{K}[[X_1^{\frac{1}{n}}, \dots, X_e^{\frac{1}{n}}]]$ such that $F(\underline{X}, Z(\underline{X})) = 0$. But $F(\underline{X}, Z(\underline{X})) = f(X_1, X_2X_1, \dots, X_eX_1, Z(\underline{X}))$, then $f(x_1, x_2, \dots, x_e, Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})) = 0$. It follows that $Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1})$ is a solution of $f(x_1, \dots, x_e, y) = 0$. Since $Z(\underline{X}) \in \mathbb{K}[[X_1^{\frac{1}{n}}]]$, then by Lemma 3 we deduce that $Z(x_1, x_2x_1^{-1}, \dots, x_ex_1^{-1}) \in \mathbb{K}_C[[\underline{x}^{\frac{1}{n}}]]$. This proves our assertion. ■

Remark 7 *In Propositions 17 and 18, if $F(\underline{X}) = f(X_1, X_2X_1, \dots, X_eX_1)$ is not irreducible, then it decomposes into quasi-ordinary polynomials, hence f itself decomposes into free polynomials in $\mathbb{K}_C[[\underline{x}]][[y]]$. As for reducible quasi-ordinary polynomials, we can associate with f the set of characteristic sequences of its irreducible components as well as a semigroup defined from the set of semigroups of these components.*

Next we prove that the approximate roots of a prepared free polynomial are free polynomials.

Proposition 19 *Suppose that f is prepared and let d be a divisor of n . If f is free in $\mathbb{K}_C[[\underline{x}]][[y]]$ then $\text{App}(f, d)$ is also free.*

Proof. By Propositions 15, 18 and Lemma 17, the polynomial $F(\underline{X}, y) = f(X_1, X_2 X_1, \dots, X_e X_1, y)$ is an irreducible quasi-ordinary polynomial of $\mathbb{K}[[\underline{X}]] [y]$. Let $G = \text{App}(F, d)$. We have $F = G^d + C_2(\underline{X}, y)G^{d-2} + \dots + C_d(\underline{X}, y)$, with $\deg_y(C_i) < \frac{n}{d}$ for all $i \in \{2, \dots, d\}$. Hence, $f(x_1, \dots, x_e, y) = F(x_1, x_2 x_1^{-1}, \dots, x_e x_1^{-1}, y) = g^d(\underline{x}, y) + C'_2(\underline{x}, y)g^{d-1}(\underline{x}, y) + \dots + C'_d(\underline{x}, y)$ where $g(\underline{x}, y) = G(x_1, x_2 x_1^{-1}, \dots, x_e x_1^{-1}, y)$ and $C'_i(\underline{x}, y) = C_i(x_1, x_2 x_1^{-1}, \dots, x_e x_1^{-1}, y)$ for all $i \in \{2, \dots, d\}$. By lemma 3 we have $g, C'_i \in \mathbb{K}_C[[\underline{x}]] [y]$ for all $i \in \{2, \dots, n\}$. Since $\deg_y(C'_i) < \frac{n}{d}$ for all $i \in \{2, \dots, d\}$ and $\deg_y(g) = \frac{n}{d}$ we get that $g = \text{App}(f, d)$ 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 $g = \text{App}(f, d)$ in $\mathbb{K}[[\underline{x}]] [y]$. Since G is the approximate root of an irreducible quasi-ordinary polynomial then it is an irreducible quasi-ordinary polynomial, and G admits a root in $\mathbb{K}[[\underline{x}^{\frac{1}{d}}]]$. But $g(\underline{x}, y) = G(x_1, x_2 x_1^{-1}, \dots, x_e x_1^{-1}, y)$, then by a similar argument as in Proposition 18 we get that g admits a root in $\mathbb{K}_C[[\underline{x}^{\frac{1}{d}}]]$. Moreover g is irreducible in $\mathbb{K}_C[[\underline{x}]] [y]$ by lemma 17. Hence g is free. ■

References

- [1] S.S. Abhyankar, Expansion Techniques in Algebraic Geometry, Lecture Notes of the Tata Institute Bombay, 57, (1977).
- [2] S.S. Abhyankar, On the semigroup of a meromorphic curve, Part 1, in Proceedings of International Symposium on Algebraic Geometry, Kyoto, (1977), 240-414.
- [3] S.S. Abhyankar, T.T. Moh, Newton-Puiseux expansion and generalized Tschirnhausen transformation. I, II. J. Reine Angew. Math. 260 (1973), 47—83 and 261 (1973), 29—54.
- [4] S.S. Abhyankar, Approximate Roots of Polynomials and Special Cases of the Epimorphism Theorem. preprint Purdue Univ. 1975.
- [5] A. Assi, Irreducibility criterion for quasi-ordinary polynomials, Journal of Singularities Volume 4 (2012), 23—34.
- [6] A. Assi, The Frobenius vector of a free affine semigroup. J. Algebra Appl. 11 (2012), no. 4, 1250065, 10 pp.
- [7] J. Lipman, Quasi-ordinary singularities of embedded surfaces, Thesis, Harvard University (1965).
- [8] A. Monforte, M. Kauers, Formal Laurent series in several variables, Expo. Math. 31 (2013) 350—367.
- [9] J. McDonald, Fiber polytopes and fractional power series, Journal of Pure and Applied Algebra 104 (1995) 213—233.
- [10] M. Zurro, The Abhyankar-Jung theorem revisited, Journal of Pure and Applied Algebra 90 (1993) 275-282.