Fields Institute Communications
Volume **33**, 2002

Approximate Roots

Patrick Popescu-Pampu
Université Paris 7 Denis Diderot
Institut de Mathématiques-UMR CNRS 7586
Equipe "Géométrie et Dynamique"
Case 7012
2, place Jussieu
75251-Paris Cedex 05
ppopescu@math.jussieu.fr

Abstract. Given an integral domain A, a monic polynomial P of degree n with coefficients in A and a divisor p of n, invertible in A, there is a unique monic polynomial Q such that the degree of $P - Q^p$ is minimal for varying Q. This Q, whose p-th power best approximates P, is called the *p-th approximate root* of P. If $f \in \mathbf{C}[[X]][Y]$ is irreducible, there is a sequence of *characteristic approximate roots* of f, whose orders are given by the singularity structure of f. This sequence gives important information about this singularity structure. We study its properties in this spirit and we show that most of them hold for the more general concept of *semiroot*. We show then how this local study adapts to give a proof of Abhyankar-Moh's embedding line theorem.

1 Introduction

The concept of *approximate root* was introduced and studied in [2] in order to prove (in [3]) what is now called the Abhyankar-Moh-Suzuki theorem: it states that the affine line can be embedded in a unique way (up to ambient automorphisms) in the affine plane. More precisely, formulated algebraically the theorem is:

Theorem *(Embedding line theorem)*
If $\mathbf{C}[X,Y] \rightarrow \mathbf{C}[T]$ is an epimorphism of $\mathbf{C}$-algebras, then there exists an isomorphism of $\mathbf{C}$-algebras $\mathbf{C}[U,V] \rightarrow \mathbf{C}[X,Y]$ such that the composed epimorphism $\mathbf{C}[U,V] \rightarrow \mathbf{C}[T]$ is given by $U = T, V = 0$.

This theorem, as well as other theorems about the group of automorphisms of $\mathbf{C}[X,Y]$, was seen to be an easy consequence of the following one, in which $d(P)$ denotes the degree of the polynomial P:

2000 *Mathematics Subject Classification.* Primary 32B30, 14B05; Secondary 14R15.

Theorem *(Epimorphism theorem)*
If $\mathbf{C}[X,Y] \to \mathbf{C}[T]$ *is an epimorphism of* $\mathbf{C}$*-algebras, given by* $X = P(T), Y = Q(T)$*, with* $d(P) > 0,\ d(Q) > 0$*, then* $d(P)$ *divides* $d(Q)$ *or vice-versa.*

Sometimes in the literature the names of the two theorems are permuted. The initial proofs ([3]) were simplified in [5]. Let us indicate their common starting point.

In order to prove the embedding line theorem, Abhyankar and Moh introduced the image curve of the embedding, whose equation is obtained by computing a resultant: $f(X,Y) = \mathrm{Res}_T(P(T) - X, Q(T) - Y)$. The curve $f(X,Y) = 0$ has only *one place at infinity* (see the general algebraic definition in [5]; in our context it means simply that the closure of the curve in the projective plane has only one point on the line at infinity and it is unibranch at that point). The fact that $\mathbf{C}[X,Y] \to \mathbf{C}[T]$ is an epimorphism is equivalent with the existence of a relation $T = \Psi(P(T), Q(T))$, where $\Psi \in \mathbf{C}[X,Y]$. This in turn is equivalent with the existence of Ψ such that the degree of $\Psi(P(T), Q(T))$ is equal to 1. Now, when Ψ varies, those degrees form a semigroup. This semigroup was seen to be linked with a semigroup of the unique branch of Ψ at infinity, which has a local definition. That is how one passes from a global problem to a local one.

To describe the situation near the point at infinity, in [3] the affine plane was not seen geometrically as a chart of the projective plane. The operation was done algebraically, making the change of variable $X \to \frac{1}{X}$. So from the study of the polynomial f one passed to the study of $\phi(X,Y) = f(X^{-1}, Y)$, seen as an element of $\mathbf{C}((X))[Y]$. That is why in [2] the local study was made for *meromorphic curves*, i.e., elements of $\mathbf{C}((X))[Y]$. The classical Newton-Puiseux expansions were generalized to that situation (see the title of [2]) as well as the notion of semigroup. In order to study this semigroup some special approximate roots of ϕ were used, which we call *characteristic approximate roots*. Their importance in this context lies in the fact that they can be defined globally in the plane, their local versions being obtained with the same change of variable as before: $X \to \frac{1}{X}$.

The proofs in [2] or in [5] of the local properties of approximate roots dealt exclusively with locally irreducible meromorphic curves. In [36] a generalization for possibly reducible polynomials was achieved, over an arbitrary non-archimedean valued field.

An introduction to Abhyankar's philosophy on curves and to his notations can be found in [9]. A gradual presentation of the general path of the proof of the epimorphism theorem was tried at an undergraduate level in [4]. See also the presentation done in [39]. Other applications to global problems in the plane are given in [6]. We quote here the following generalization of the embedding line theorem:

Theorem *(Finiteness theorem)*
Up to isomorphisms of the affine plane, there are only finitely many embeddings of a complex irreducible algebraic curve with one place at infinity in the affine plane.

The reference [6] also contains some conjectures in higher dimensions.

Here we discuss mainly the local aspects of approximate roots. We work in less generality, as suggested by the presentation of the subject made in [25]. Namely, we consider only polynomials in $\mathbf{C}[[X]][Y]$. This framework has the advantage of giving more geometrical insight, many computations being interpreted in terms of intersection numbers (see also [17]), a viewpoint that is lacking in the meromorphic case. This has also the advantage of allowing us to interpret the local properties of approximate roots in terms of the minimal resolution of f, a concept which has no analog in the case of meromorphic curves. We define the concept of *semiroots*, as being those curves that have the same intersection-theoretical properties as the characteristic approximate roots, and we show that almost all the local properties usually used for the characteristic roots are in fact true for semiroots.

First we introduce the notations for Newton-Puiseux parameterizations of a plane branch in arbitrary coordinates, following [25]. In section 3 we introduce the general notion of approximate roots. We explain the concept of semigroup of the branch and related notions in section 4. In section 5 we introduce the characteristic approximate roots of the branch, we state their main intersection-theoretical local properties (Theorem 5.1) and we add some corollaries. In section 6 we explain the main steps of the proof of Theorem 5.1. In sections 7 and 8 we give *the proofs* of Theorem 5.1, its corollaries and the auxiliary propositions stated in the text. We prefer to isolate the proofs from the main text, in order to help reading it. In the final section we indicate the changes one must make to the theory explained before in order to deal with the meromorphic curves and we sketch a proof of the embedding line theorem.

A forerunner of the concept of approximate root was introduced in an arithmetical context in [32] and [33] (see also [28] for some historical remarks on those papers). The existence of approximate roots is the content of exercise 13, §1, in [13]. The concept of semiroot is closely associated with that of curve having maximal contact with the given branch, introduced in [29] and [30]. More details on this last concept are given in the comments following Corollary 5.6. Approximate roots of elements of $\mathbf{C}[[X]][Y]$ are also used in [12] to study the local topology of plane curves. The approximate roots of curves in positive characteristic are studied in [40] using Hamburger-Noether expansions and the epimorphism theorem is generalized to this case under some restrictions. The approximate roots of meromorphic curves are used in [11] for the study of affine curves with only one irregular value. The projectivized approximate roots of a curve with one place at infinity are used in [16] in order to obtain global versions of Zariski's theory of complete ideals. In [23], the theorem 5.1 proved below and some of its corollaries are generalized to the case of quasi-ordinary singularities of hypersurfaces.

We would like to thank S.S.Abhyankar for the explanations he gave us in Saskatoon on approximate roots. We were also greatly helped in our learning of the subject by the article [25] of J.Gwoździewicz and A.Płoski. We thank B.Teissier, E.García Barroso and P.D.González Pérez for their comments on preliminary versions of this work and S.Kuhlmann and F.V.Kuhlmann for the invitation to talk on this subject in Saskatoon.

2 Notations

In what follows we do not care about maximal generality on the base field. We work over $\mathbf{C}$, the field of complex numbers. By $''a|b''$ we mean "a divides b", whose negation we note $''a \not| b''$. The greatest common divisor of $a_1, ..., a_m$ is denoted $\gcd(a_1, ..., a_m)$. If $q \in \mathbf{R}$, its integral part is denoted $[q]$.

We consider $f(X,Y) \in \mathbf{C}[[X]][Y]$, a polynomial in the variable Y, monic and irreducible over $\mathbf{C}[[X]]$, the ring of formal series in X:

$$f(X,Y) = Y^N + \alpha_1(X)Y^{N-1} + \alpha_2(X)Y^{N-2} + \cdots + \alpha_N(X)$$
where $\alpha_1(0) = \cdots = \alpha_N(0) = 0$.

If we embed $\mathbf{C}[[X]][Y] \hookrightarrow \mathbf{C}[[X,Y]]$, the equation $f(X,Y) = 0$ defines a germ of formal (or algebroïd) irreducible curve at the origin - we call it shortly *a branch* - in the plane of coordinates X, Y. We denote this curve by C_f.

Conversely, if a branch $C \hookrightarrow \mathbf{C}^2$ is given, the Weierstrass preparation theorem shows that it can be defined by a unique polynomial of the type just discussed, once the ambient coordinates X, Y have been chosen, with the exception of $C = Y$-axis. If we describe like this a curve by a polynomial equation f with respect to the variable Y, we call briefly its degree N in Y *the degree of* f, and we denote it by $d(f)$ or $d_Y(f)$ if we want to emphasize the variable in which it is polynomial. When C is *transverse* to the Y-axis (which means that the tangent cones of C and of the Y-axis have no common components), we have the equality $d(f) = m(C)$, where $m(C)$ denotes the multiplicity of C (see section 4).

From now on, each time we speak about the curve C, we mean the curve C_f, for the fixed f.

The curve C can always be parameterized in the following way (see [20], [46], [9], [44], [45]):

$$\begin{cases} X = T^N \\ Y = \sum_{j\geq 1} a_j T^j = \cdots + a_{B_1}T^{B_1} + \cdots + a_{B_2}T^{B_2} + \cdots + a_{B_G}T^{B_G} + \cdots \end{cases} \tag{2.1}$$

with $\gcd(\{N\} \cup \{j, a_j \neq 0\}) = 1$.

The exponents B_j, for $j \in \{1, ..., G\}$ are defined inductively:

$B_1 := \min\{j, a_j \neq 0, N \not| j\}$

$B_i := \min\{j, a_j \neq 0, \gcd(N, B_1, ..., B_{i-1}) \not| j\}$, for $i \geq 2$.

The number G is the least one for which $\gcd(N, B_1, ..., B_G) = 1$.

We define also: $B_0 := N = d(f)$. Then $(B_0, B_1, ..., B_G)$ is called the *characteristic sequence* of C_f in the coordinates X, Y. The B_i's are *the characteristic exponents* of C_f *with respect to* (X, Y).

A parameterization like (2.1) is called *a primitive Newton-Puiseux parameterization with respect to* (X, Y) of the plane branch C. Notice that X and Y cannot be permuted in this definition.

Let us explain why we added the attribute “primitive”. If we write $T = U^M$, where $M \in \mathbf{N}^*$, we obtain a parameterization using the variable U. In the new parameterization, the greatest common divisor of the exponents of the series $X(U)$ and $Y(U)$ is no longer equal to 1. In this case we say that the parameterization is *not primitive*. When we speak only of a “Newton-Puiseux parameterization”, we mean a primitive one.

We define now the sequence of greatest common divisors: $(E_0, E_1, ..., E_G)$ in the following way:

$$E_j = \gcd(B_0, ..., B_j) \text{ for } j \in \{0, ..., G\}.$$

In particular: $E_0 = N$, $E_G = 1$. Define also their quotients:

$$N_i = \frac{E_{i-1}}{E_i} > 1, \text{ for } 1 \leq i \leq G.$$

This implies:

$$E_i = N_{i+1}N_{i+2} \cdots N_G, \text{ for } 0 \leq i \leq G-1.$$

Let us introduce the notion of *Newton-Puiseux series of C with respect to* (X,Y). It is a series of the form:

$$\eta(X) = \sum_{j\geq 1} a_j X^{\frac{j}{N}} \tag{2.2}$$

obtained from (2.1) by replacing T by $X^{\frac{1}{N}}$. It is an element of $\mathbf{C}[[X^{\frac{1}{N}}]]$. One has then the equality $f(X,\eta(X)) = 0$, so $\eta(X)$ can be seen as an expression for a root of the polynomial equation in Y: $f(X,Y) = 0$. All the other roots can be obtained from (2.2) by changing $X^{\frac{1}{N}}$ to $\omega X^{\frac{1}{N}}$, where ω is an arbitrary N-th root of unity. This is a manifestation of the fact that the Galois group of the field extension $\mathbf{C}((X)) \to \mathbf{C}((X^{\frac{1}{N}}))$ is $\mathbf{Z}/N\mathbf{Z}$. From this remark we get another presentation of the characteristic exponents:

Proposition 2.1 The set $\{\frac{B_1}{N}, ..., \frac{B_G}{N}\}$ is equal to the set:

$$\{v_X(\eta(X) - \zeta(X)),\ \eta(X) \text{ and } \zeta(X) \text{ are distinct roots of } f\}.$$

Here v_X designates the order of a formal fractional power series in the variable X.

Given a Newton-Puiseux series (2.2), define for $k \in \{0, ..., G\}$:

$$\eta_k(X) = \sum_{1\leq j < B_{k+1}} a_j X^{\frac{j}{N}}.$$

It is the sum of the terms of $\eta(X)$ of exponents strictly less than $\frac{B_{k+1}}{N}$. We call $\eta_k(X)$ *a k-truncated Newton-Puiseux series of C with respect to* (X,Y). If the parameterization (2.1) is reduced, then $\eta_k(X) \in \mathbf{C}[[X^{\frac{E_k}{N}}]]$ and there are exactly $\frac{N}{E_k}$ such series.

Before introducing the concept of approximate root, we give an example of a natural question about Newton-Puiseux parameterizations, which will be answered very easily using that concept.

Motivating example

There are algorithms to compute Newton-Puiseux parameterizations of the branch starting from the polynomial f. If one wants to know only the beginning of the parameterization, one could ask if it is enough to know only some of the coefficients of the polynomial f. The answer is affirmative, as is shown by the following proposition:

Proposition 2.2 If f is irreducible with characteristic sequence $(B_0, ..., B_G)$, then the terms of the k-truncated Newton-Puiseux series of f depend only on $\alpha_1(X), ..., \alpha_{\frac{N}{E_k}}(X)$.

The proof will appear to be very natural once we know the concept of approximate root and Theorem 5.1. Let us illustrate the proposition by a concrete case.

Consider:

$f(X,Y) = Y^4 - 2X^3Y^2 - 4X^5Y + X^6 - X^7$.

One of its Newton-Puiseux parameterizations is:

$$\begin{cases} X = T^4 \\ Y = T^6 + T^7 \end{cases}$$

We get, using the proposition for $k = 1$, that every irreducible polynomial of the form:

$$g(X,Y) = Y^4 - 2X^3Y^2 + \alpha_3(X)Y + \alpha_4(X)$$

whose characteristic sequence is $(4, 6, 7)$, has a Newton-Puiseux series of the type:

$$Y = X^{\frac{3}{2}} + \gamma(X),$$

with $v_X(\gamma) \geq \frac{7}{4}$.

It is now the time to introduce the approximate roots...

3 The definition of approximate roots

Let A be an integral domain (a unitary commutative ring without zero divisors). If $P \in A[Y]$ is a polynomial with coefficients in A, we shall denote by $d(P)$ its degree.

Let $P \in A[Y]$ be monic of degree $d(P)$, and p a divisor of $d(P)$. In general there is no polynomial $Q \in A[Y]$ such that $P = Q^p$, i.e. there is no *exact root* of order p of the polynomial P. But one can ask for a *best approximation* of this equality. We speak here of approximation in the sense that the difference $P - Q^p$ is of degree as small as possible for varying Q. Such a Q does not necessarily exist. But it exists if one has the following condition on the ring A, verified for example in the case that interests us here, $A = \mathbf{C}[[X]]$: *p is invertible in A.*

More precisely, one has the following proposition:

Proposition 3.1 If p is invertible in A and p divides $d(P)$, then there is a unique monic polynomial $Q \in A[Y]$ such that:

$$d(P - Q^p) < d(P) - \frac{d(P)}{p}. \tag{3.1}$$

This allows us to define:

Definition 3.2 The unique polynomial Q of the preceding proposition is named the **p-th approximate root** of P. It is denoted $\sqrt[p]{P}$.

Obviously:

$$d(\sqrt[p]{P}) = \frac{d(P)}{p}.$$

Example: Let $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n$ be an element of $A[Y]$. Then, if n is invertible in A:

$$\sqrt[n]{P} = Y + \frac{\alpha_1}{n}.$$

We recognize here the *Tschirnhausen transformation* of the variable Y. That is the reason why initially (see the title of [2]) the approximate roots were seen as generalizations of the Tschirnhausen transformation.

We give now a proposition showing that in some sense the notation $\sqrt[p]{P}$ is adapted:

Proposition 3.3 If $p, q \in \mathbf{N}^*$ are invertible in A, then $\sqrt[q]{\sqrt[p]{P}} = \sqrt[pq]{P}$.

We see that approximate roots behave in this respect like usual d-th roots. The following construction shows another link between the two notions. We add it for completeness, since it will not be used in the sequel.

Let $P \in A[Y]$ be a monic polynomial. Consider $P_1 \in A[Z^{-1}]$, $P_1(Z) = P(Z^{-1})$. If we embed the ring $A[Z^{-1}]$ into $A((Z))$, the ring of meromorphic series with coefficients in A, the p-th root of P_1 exists inside $A((Z))$. It is the unique series P_2 with principal term $1 \cdot Z^{-\frac{n}{p}}$ such that $P_2^p = P_1$. We note:

$$P_1^{\frac{1}{p}} := P_2.$$

Consider the *purely meromorphic part* $M(P_1^{\frac{1}{p}})$ of $P_1^{\frac{1}{p}}$, the sum of the terms having Z-exponents ≤ 0.

We have $M(P_1^{\frac{1}{p}}) \in A[Z^{-1}]$, so:

$$Q(Y) = M(P_1^{\frac{1}{p}})(Y^{-1}) \in A[Y].$$

We can state now the proposition (see [35], [36]):

Proposition 3.4 If $Q \in A[Y]$ is defined as before, then $Q = \sqrt[p]{P}$.

4 The semigroup of a branch

Let $\mathcal{O}_C = \mathbf{C}[[X]][Y]/(f)$ be the local ring of the germ C at the origin. It is an integral local ring of dimension 1.

Let $\mathcal{O}_C \rightarrow \overline{\mathcal{O}}_C$ be the morphism of normalization of $\mathcal{O}_C$, i.e., $\overline{\mathcal{O}}_C$ is the integral closure of $\mathcal{O}_C$ in its field of fractions. This new ring is regular (normalization is a desingularization in dimension 1), and so it is *a discrete valuation ring of rank* 1. Moreover, there exists an element $T \in \overline{\mathcal{O}}_C$, called *a uniformizing parameter*, such that $\overline{\mathcal{O}}_C \simeq \mathbf{C}[[T]]$. Then the valuation is simply the T-adic valuation v_T, which associates to each element of $\overline{\mathcal{O}}_C$, seen as a series in T, its order in T.

Definition 4.1 The **semigroup** $\Gamma(C)$ of the branch C is the image by the T-adic valuation of the non zero elements of the ring $\mathcal{O}_C$:

$$\Gamma(C) := v_T(\mathcal{O}_C - \{0\}) \subset v_T(\overline{\mathcal{O}}_C - \{0\}) = \mathbf{N} = \{0, 1, 2, ...\}.$$

The set $\Gamma(C)$ is indeed a semigroup, which comes from the additivity property of the valuation v_T:

$$\forall \phi, \psi \in \mathcal{O}_C - \{0\}, v_T(\phi\psi) = v_T(\phi) + v_T(\psi).$$

The previous definition is intrinsic and it does not depend on the fact that the curve C is planar. Let us now turn to other interpretations of the semigroup.

First, our curve is given with a fixed embedding in the plane of coordinates (X, Y). Once we have chosen a uniformizing parameter T, we have obtained a *parameterization* of the curve: $\left\{ \begin{array}{l} X = X(T) \\ Y = Y(T) \end{array} \right.$.

For example, a Newton-Puiseux parameterization would work.

If $f' \in \mathcal{O}_C - \{0\}$, it can be seen as the restriction of an element of the ring $\mathbf{C}[[X]][Y]$, which we denote by the same symbol f'. The curve C' defined by the equation $f' = 0$ has an intersection number with C at the origin. We note it (f, f'), or (C, C'), to insist on the fact that this number depends only on the curves, and not on the coordinates or the defining equations. We have then the equalities:

$$v_T(f') = v_T(f'(X(T), Y(T))) = (f, f'),$$

which provides a geometrical interpretation of the semigroup of the branch C:

$$\Gamma(C) = \{(f, f'), f' \in \mathbf{C}[[X]][Y], f \not| f'\}.$$

From this viewpoint, the semigroup is simply the set of possible intersection numbers with curves not containing the given branch.

The minimal non-zero element of $\Gamma(C)$ is the *multiplicity* $m(C)$, noted also $m(f)$ if C is defined by f. It is the lowest degree of a monomial appearing in the Taylor series of f, and therefore also the intersection number of C with smooth curves passing through the origin and transverse to the tangent cone of C.

If $p_1, ..., p_l$ are elements of $\Gamma(C)$, the sub-semigroup $\mathbf{N}p_1 + \cdots + \mathbf{N}p_l$ they generate is denoted by:

$$\langle p_1, ..., p_l \rangle.$$

One has then the following result, expressing a set of generators of the semigroup in terms of the characteristic exponents:

Proposition 4.2 The degree N of the polynomial f is an element of $\Gamma(C)$, denoted $\overline{B}_0$. So, $\overline{B}_0 = B_0$. Define inductively other numbers $\overline{B}_i$ by the following property:

$$\overline{B}_i := \min\{j \in \Gamma(C), j \notin \langle \overline{B}_0, ..., \overline{B}_{i-1} \rangle\}.$$

Then this sequence has exactly $G+1$ terms $\overline{B}_0, ..., \overline{B}_G$, which verify the following properties for $0 \leq i \leq G$ (we consider by definition that $\overline{B}_{G+1} = \infty$):

1) $\overline{B}_i = B_i + \sum_{k=1}^{i-1} \frac{E_{k-1} - E_k}{E_{i-1}} B_k$.
2) $\gcd(\overline{B}_0, ..., \overline{B}_i) = E_i$.
3) $N_i \overline{B}_i < \overline{B}_{i+1}$.

A proof of this proposition is given in [49] for generic coordinates (see the definition below) and in [25] in this general setting. Other properties of the generators are given in [34], in the generic case (see the definition below). In fact the proof can be better conceptualized if one uses the notion of semiroot, more general than the notion of characteristic root. This notion is explained in section 6. When reading the proof of Proposition 4.2, one should become convinced that there is no vicious circle in the use of the $\overline{B}_k$'s.

The point is that it appears easier to define the $\overline{B}_k$'s by property 1) and then to prove the minimality property of the sequence. We have used the other way round in the formulation of Proposition 4.2 because at first sight the minimality definition seems more natural. One should also read the comments preceding Proposition 9.1.

The generators of the semigroup introduced in this proposition depend on the coordinates X, Y, but only in a loose way. Indeed, they are uniquely determined by the semigroup once the first generator $\overline{B}_0$ is known. This generator, being equal to the degree of the polynomial f, depends on X, Y. Geometrically, it is the intersection number (f, X). It follows from this that for *generic coordinates*, i.e. with the Y-axis transverse to the curve C, the generators are independent of the coordinates.

We can therefore speak of *generic characteristic exponents*. They are a complete set of invariants for the equisingularity and the topological type of the branch (see [49]). For the other discrete invariants introduced before, we speak in the same way of *generic* ones and we use lower case letters to denote them, as opposed to capital ones for the invariants in arbitrary coordinates. Namely, we use the following notations for the generic invariants:

$$\begin{array}{l} n \\ (b_0, ..., b_g) \\ (e_0, ..., e_g) \\ (n_1, ..., n_g) \\ (\overline{b}_0, ..., \overline{b}_g) \end{array} \quad .$$

This makes it easy to recognize in every context if we suppose the coordinates to be generic or not.

We call g the *genus* of the curve C.

The exponent b_0 is equal to the multiplicity $m(C)$ of C at the origin. When D is a curve passing through 0, we have $(C, D) = b_0$ if and only if D is smooth and transverse to C at 0.

The preceding proposition shows that in arbitrary coordinates the generators of the semigroup are determined by the characteristic exponents. But the relations can be reversed, and show that conversely, the characteristic exponents are determined by the generators of the semigroup. From this follows the invariance of the characteristic exponents with respect to the generic coordinates chosen for the computations. Moreover, like this one can easily obtain a proof of the classical *inversion formulae* for plane branches (see another proof in [1]). Let us state it in a little extended form.

Let (X, Y) and (x, y) be two systems of coordinates, the second one being generic for C. We consider the characteristic exponents $(B_0, ..., B_G)$ of C with respect to (X, Y).

Proposition 4.3 (Inversion formulae)

The first characteristic exponent B_0 can take values only in the set $\{lb_0, 1 \leq l \leq [\frac{b_1}{b_0}]\} \cup \{b_1\}$. The knowledge of its value completely determines the rest of the exponents in terms of the generic ones:

1) $B_0 = b_0 \Rightarrow G = g$ and:

$$(B_0, ..., B_G) = (b_0, ..., b_g).$$

2) $B_0 = lb_0$ with $2 \leq l \leq [\frac{b_1}{b_0}] \Rightarrow G = g + 1$ and:

$$(B_0, ..., B_G) = (lb_0, b_0, b_1 + (1 - l)b_0, ..., b_g + (1 - l)b_0).$$

3) $B_0 = b_1 \Rightarrow G = g$ and:

$$(B_0, ..., B_G) = (b_1, b_0, b_2 + b_0 - b_1, b_3 + b_0 - b_1, ..., b_g + b_0 - b_1).$$

Moreover, for $k \in \{1, ..., g\}$, the k-truncations of the Newton-Puiseux series with respect to (x, y) depend only on the $(k + \epsilon)$-truncation of the Newton-Puiseux series with respect to (X, Y), where $\epsilon = G - g \in \{0, 1\}$.

The name given classically to one form or another of this proposition comes from the fact it answers the question: *what can we say about the Newton-Puiseux series with respect to* (Y, X) *if we know it with respect to* (X, Y)? In this question, one simply *inverts* the coordinates.

We prove the statement on truncations using, as in the case of Proposition 4.2, the notion of *semiroot*, introduced in section 6.

5 The main theorem

As before, the polynomial $f \in \mathbf{C}[[X]][Y]$ is supposed to be irreducible. To be concise, we note in what follows:

$$f_k := \sqrt[E_k]{f}.$$

Next theorem is the main one, (7.1), in [2]. A different proof is given in [5], (8.2). Here we give a proof inspired by [25].

Theorem 5.1 The approximate roots f_k for $0 \leq k \leq G$, have the following properties:

1) $d(f_k) = \frac{N}{E_k}$ and $(f, f_k) = \overline{B}_{k+1}$.

2) The polynomial f_k is irreducible and its characteristic exponents in these coordinates are $\frac{B_0}{E_k}, \frac{B_1}{E_k}, ..., \frac{B_k}{E_k}$.

Theorem 5.1 gives properties of some of the approximate roots of f. One does not consider all the divisors of N, but only some special ones, computed from the knowledge of the characteristic exponents. For this reason, we name them *the characteristic approximate roots of f*.

We give now a list of corollaries. In fact these corollaries hold more generally for *semiroots*, see the comments made after Definition 6.4. The proofs of the theorem and of its corollaries are given in section 7. Before that, in section 6 we explain the main steps in the proof of Theorem 5.1

Corollary 5.2 The irreducible polynomial f being given, one can compute recursively its characteristic approximate roots in the following way. Compute the N-th root f_0 of f and put $E_0 = N$. If f_k was computed, put $(f, f_k) = \overline{B}_{k+1}$. As E_k has already been computed, take $E_{k+1} = \gcd(E_k, \overline{B}_{k+1})$ and compute $f_{k+1} = \sqrt[E_{k+1}]{f}$. One can then deduce the characteristic exponents from the characteristic roots.

This has been extended to the case of meromorphic curves in [10]. The preceding algorithm works only if f is irreducible. But it can be adapted to give a method of deciding whether a given f is indeed irreducible, as was done in [8]. See also the more elementary presentation given in [7]. A generalization of this criterion of irreducibility to the case of arbitrary characteristic is contained in [19].

Following the proof of the proposition, we add an example of application of the algorithm.

Corollary 5.3 For $0 \leq k \leq G$, the polynomials f and f_k have equal sets of k-truncations of their Newton-Puiseux series.

This, together with the remark following equation (8.1), gives an immediate proof of Proposition 2.2.

Corollary 5.4 Every $\phi \in \mathbf{C}[[X]][Y]$ can be *uniquely* written as a finite sum of the form:

$$\phi = \sum_{i_0, \ldots, i_G} \alpha_{i_0 \ldots i_G} f_0^{i_0} f_1^{i_1} \cdots f_G^{i_G}$$

where $i_G \in \mathbf{N}$, $0 \leq i_k < N_{k+1}$ for $0 \leq k \leq G-1$ and the coefficients $\alpha_{i_0 \ldots i_G}$ are elements of the ring $\mathbf{C}[[X]]$. Moreover:

1) the Y-degrees of the terms appearing in the right-hand side of the preceding equality are all distinct.

2) the orders in T of the terms

$$\alpha_{i_0 \dots i_{G-1} 0}(T^N) f_0(T^N, Y(T))^{i_0} \cdots f_{G-1}(T^N, Y(T))^{i_{G-1}}$$

are pairwise distinct, where $T \to (T^N, Y(T))$ is a Newton-Puiseux parameterization of f.

There is no a priori bound on i_G: this exponent is equal to $[\frac{d(\phi)}{N}]$. The orders in T appearing in 2) are the intersection numbers of f with the curves defined by the terms of the sum which are not divisible by f.

This corollary is essential for the applications of Theorem 5.1 to the proof of the embedding line theorem. Indeed, the point 2) allows one to compute (f, ϕ) in terms of the numbers $(f, \alpha_{i_0 \dots i_{G-1} 0} f_0^{i_0} f_1^{i_1} \cdots f_{G-1}^{i_{G-1}})$. But, as explained in the introduction, one is interested in the semigroup of f, composed of the intersection numbers (f, ϕ) for varying ϕ. This way of studying the semigroup of f is the one focused on in [2] and [5].

Corollary 5.5 The images of $X, f_0, f_1, ..., f_{G-1}$ into the graded ring $gr_{v_T} \mathcal{O}_C$ generate it as a $\mathbf{C}$-algebra. If the coordinates are generic, they form a minimal system of generators.

We have defined generic coordinates in the remark following Proposition 4.2. Here $gr_{v_T} \mathcal{O}_C$ is *the graded ring of* $\mathcal{O}_C$ *with respect to the valuation* v_T. This concept is defined in general, if A is a domain of integrity, $F(A)$ its field of fractions and ν a valuation of $F(A)$ that is positive on A. In this situation, we define first the semigroup of values $\Gamma(A)$ to be the image of $A - \{0\}$ by the valuation. If $p \in \Gamma(A)$, we define the following ideals of A:

$$I_p := \{x \in A, \nu(x) \geq p\},$$

$$I_p^+ := \{x \in A, \nu(x) > p\}.$$

The *graded ring of* A *with respect to the valuation* ν is defined in the following way:

$$gr_\nu A := \bigoplus_{p \in \Gamma(A)} I_p / I_p^+.$$

This viewpoint on the approximate roots is focused on in [42] and [43], where the general concept of *generating sequence* for a valuation is introduced. This concept generalizes the sequence of characteristic approximate roots, introduced before.

In the case of irreducible germs of plane curves, the spectrum of $gr_{v_T}(\mathcal{O}_C)$ is the so-called *monomial curve* associated to C. It was used in [22] in order to show that one could understand better the desingularization of C by embedding it in a space of higher dimension.

Before stating the next corollary, let us introduce some other notions. For more details one can consult [14], [31] and [42].

An *embedded resolution* of C is a proper birational morphism $\pi : \Sigma \to \mathbf{C}^2$ such that Σ is smooth and the total transform $\pi^{-1}(C)$ is a divisor with normal crossings. Such morphisms exist and they all factorize through a minimal one $\pi_m : \Sigma_m \to \mathbf{C}^2$ which can be obtained in the following way. Start from $C \hookrightarrow \mathbf{C}^2$ and blow-up the origin. Take the total transform divisor of C in the resulting surface. All its points are smooth or with normal crossings, with the possible exception of the point on the strict transform of C. If at this point the divisor is not with normal crossing,

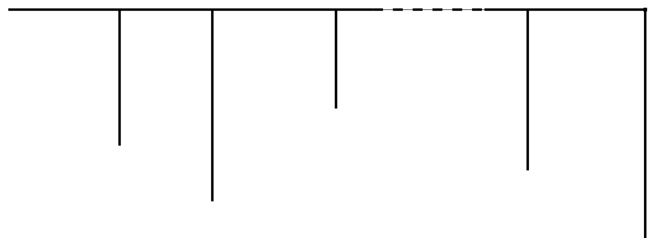

Figure 1 The Dual Graph

blow up the point. Then repeat the process. After a finite number of steps, one obtains the minimal embedded resolution of C.

The reduced exceptional divisor $\mathcal{E}$ of π_m is connected, which can be easily seen from the previous description by successive blowing-up. This phenomenon is much more general, and known under the name "Zariski's connectedness theorem" or "Zariski's main theorem", see [47], [37] and [27]. The components of $\mathcal{E}$ are isomorphic to $\mathbf{CP}^1$. We consider *the dual graph* $D(\pi_m)$ of $\mathcal{E}$, whose vertices are in bijection with the components of $\mathcal{E}$. Two vertices are connected by an edge if and only if the corresponding components intersect on Σ_m. The graph $D(\pi_m)$ is then a tree like in Figure 1, in which we represent only the underlying topological space of the graph and not its simplicial decomposition.

In this picture there are exactly g vertical segments, g being the genus of f (see its definition in the comments following Proposition 4.2). The first vertex on the left of the horizontal segment corresponds to the component of $\mathcal{E}$ created by the first blowing-up. The vertex of attachment of the horizontal segment and of the right-hand vertical segment corresponds to the component of $\mathcal{E}$ which cuts the strict transform of C.

If we consider also the strict transform of C on Σ_m, we represent it by an arrow-head vertex connected to the vertex of $D(\pi_m)$ which represents the unique component of $\mathcal{E}$ which it intersects. We denote this new graph by $D(\pi_m, f)$.

This graph as well as various numerical characters of the components of $\mathcal{E}$ can be computed from a generic Newton-Puiseux series for f. The first to have linked Newton-Puiseux series with the resolution of the singularity seems to be M.Noether in [38]. See also [20] for the viewpoint of the italian school.

Corollary 5.6 Let π_m be the minimal embedded resolution of C_f. We consider the characteristic approximate roots f_k, for $0 \leq k \leq g$ with respect to generic coordinates. Let us denote by C_k the curve defined by the equation $f_k = 0$. One has evidently $C_f = C_g$. Let us also denote by C'_k the strict transform of C_k by the morphism π_m. Then the curves C'_k are smooth and transverse to a unique component of the exceptional divisor of π_m. The dual graph of the total transform of $f_0 f_1 \cdots f_g$ is represented in Figure 2.

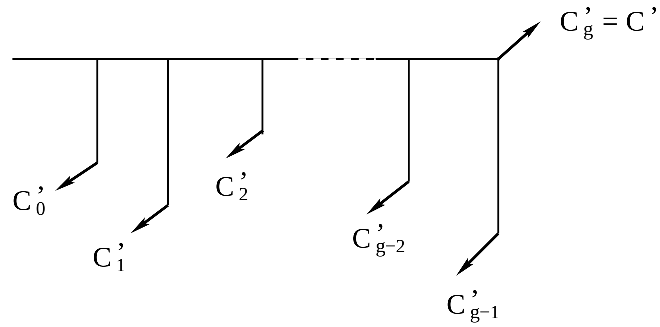

Figure 2 The Total Dual Graph

The previous corollary gives a topological interpretation of the characteristic approximate roots, showing how they can be seen as generalizations of smooth curves having maximal contact with C.

Such a generalization was already made in [29] and [30], where the notion of *maximal contact* with f was extended from smooth curves to singular curves having at most as many generic characteristic exponents as f. It was further studied in [15]. Let us explain this notion.

If D is a plane branch, let

$$\nu(D) := \frac{1}{m(D)} \sup_{D'}\{(D, D')\},$$

where the supremum is taken over all the choices of smooth D'. It is a finite rational number, with the exception of the case when D is smooth, which implies $\nu(D) = +\infty$.

Consider now the sequence of point blowing-ups which desingularizes C. For $i \in \{0, ..., g\}$, let D_i be the first strict transform of C that has genus $g - i$. One has $D_0 = C$. Define:

$$\nu_i(C) := \nu(D_i).$$

The sequence $(\nu_0(C), ..., \nu_g(C))$ was named in [29] *the sequence of Newton coefficients* of C. In characteristic 0 - for example when working over $\mathbf{C}$, as we do in this article - its knowledge is equivalent to the knowledge of the characteristic sequence. The advantage of the Newton coefficients is that they are defined in any characteristic.

Definition 5.7 If D is a branch of genus $k \in \{0, ..., g\}$, we say that D **has maximal contact** with C if $\nu_i(D) = \nu_i(C)$ for every $i \in \{0, ..., k\}$ and (C, D) is the supremum of the intersection numbers of C with curves of genus k having the previous property.

It can be shown with the same kind of arguments as those used to prove Corollary 5.6, that for every $k \in \{0, ..., g\}$, the curves having genus k and maximal contact with f are exactly the k-semiroots in generic coordinates.

In order to understand better Corollary 5.6, let us introduce another concept:

Definition 5.8 Let L be some component of the reduced exceptional divisor $\mathcal{E}$. A branch $D \hookrightarrow \mathbf{C}^2$ is called **a curvette** with respect to L if its strict transform by π_m is smooth and transversal to L at a smooth point of $\mathcal{E}$.

Let L_0 be the component of $\mathcal{E}$ created by the blowing-up of $0 \in \mathbf{C}^2$. For every $k \in \{1, ..., g\}$, let L_k be the component at the free end of the k-th vertical segment of $D(\pi_m)$. Let L_{g+1} be the component intersecting the strict transform of C.

Corollary 5.9 A characteristic approximate root of f in arbitrary coordinates is a curvette with respect to one of the components $L_0, L_1, ..., L_{g+1}$.

This corollary is an improvement of Corollary 5.6, which says this is true in generic coordinates. This more general property is important for the geometrical interpretations of approximate roots given in [16]. A deeper study of curvettes, for possibly multi-branch curve singularities can be found in [31].

6 The steps of the proof

In this section we explain only the main steps in the proof of Theorem 5.1, as well as a reformulation for the corollaries. The complete proofs are given in section 7.

First we have to introduce a new notion, fundamental for the proof, that of the *expansion of a polynomial* in terms of another polynomial. This is the notion mentioned in the title of [5].

Let A be an integral domain and let $P, Q \in A[Y]$ be monic polynomials such that $Q \neq 0$. We make the Euclidean division of P by Q and we keep dividing the intermediate quotients by Q until we arrive at a quotient of degree $< d(Q)$:

$$\begin{cases} P = q_0 Q + r_0 \\ q_0 = q_1 Q + r_1 \\ \vdots \\ q_{t-1} = q_t Q + r_t \end{cases} .$$

Here $q_t \neq 0$ and $d(q_t) < d(Q)$. Then we obtain an expansion of P in terms of Q:

$$P = q_t Q^{t+1} + r_t Q^t + r_{t-1} Q^{t-1} + \cdots + r_0.$$

All the coefficients $q_t, r_t, r_{t-1}, ..., r_0$ are polynomials in Y of degrees $< d(Q)$. This is the unique expansion having this property:

Proposition 6.1 One has a unique **Q-adic expansion of P**:

$$P = a_0 Q^s + a_1 Q^{s-1} + \cdots + a_s \tag{6.1}$$

where $a_0, a_1, ..., a_s \in A[Y]$ and $d(a_i) < d(Q)$ for all $i \in \{0, ..., s\}$.The Y-degrees of the terms $a_i Q^{s-i}$ in the right-hand side of equation (6.1) are all different and $s = [\frac{d(P)}{d(Q)}]$. One has $a_0 = 1$ if and only if $d(Q) \mid d(P)$. In this last situation, supposing that moreover s is invertible in A, one has $a_1 = 0$ if and only if $Q = \sqrt[s]{P}$.

Remark: One should note the analogy with the expansion of numbers in a basis of numeration. To obtain that notion, one needs only to take natural numbers in spite of polynomials. Then the a_i's are the digits of the expansion.

Definition 6.2 The polynomials P and Q are given as before, with $d(Q) \mid d(P)$. Let us suppose $s = \frac{d(P)}{d(Q)}$ is invertible in A. The **Tschirnhausen operator** τ_P of "completion of the s-power" is defined by the formula:

$$\tau_P(Q) := Q + \frac{1}{s} a_1.$$

Look again at the example given after Definition 3.2. The usual expression $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n$ is the Y-adic expansion of P and $\sqrt[n]{P}$ is exactly $\tau_P(Y)$. The following proposition generalizes this observation.

Proposition 6.3 Suppose $P \in A[Y]$ is monic and $p \mid d(P)$, with p invertible in A. The approximate roots can be computed by iterating the Tschirnhausen operator on arbitrary polynomials of the correct degree:

$$\sqrt[p]{P} = \underbrace{\tau_P \circ \tau_P \circ \ldots \circ \tau_P}_{d(P)/p}(Q)$$

for all $Q \in A[Y]$ monic of degree $\frac{d(P)}{p}$.

The steps of the proof of Theorem 5.1 are:

Step 1 Show that there exist polynomials verifying the conditions of Theorem 5.1, point 1).

Step 2 Show that those conditions are preserved by an adequate Tschirnhausen operator.

Step 3 Apply Proposition 6.3 to show inductively that the characteristic roots also satisfy those conditions.

Step 4 Show that the point 2) of Theorem 5.1 is true for all polynomials satisfying the conditions of point 1).

This motivates us to introduce a special name for the polynomials verifying the conditions of Theorem 5.1, point 1):

Definition 6.4 A polynomial $q_k \in \mathbf{C}[[X]][Y]$ is **a k-semiroot** of f if it is monic of degree $d(q_k) = \frac{N}{E_k}$ and $(f, q_k) = \overline{B}_{k+1}$.

The term of "semiroot" is taken from [8].

We show in fact that all the corollaries of the main theorem (Theorem 5.1), with the exception of the first one, are true for polynomials that are k-semiroots of f. That is why we begin the proofs of the corollaries 5.3, 5.4, 5.5, 5.6 and 5.9 by restating them in this greater generality. It is only in Corollary 5.2 that the precise construction of approximate roots is useful. In our context, the value of the approximate roots lies mainly in the fact that the definition is global and at the same time gives locally k-semiroots (see section 9).

We now formulate some propositions that are used in the proof of Theorem 5.1. The first one is attributed by some authors to M.Noether. Equivalent statements in terms of characteristic exponents can be found in [41], [26], [18], [48], [34].

Proposition 6.5 If $\phi \in \mathbf{C}[[X]][Y]$ is monic, irreducible and $K(f, \phi) :=$

$$= \max\{v_X(\eta(X) - \zeta(X)), \eta(X) \text{ and } \zeta(X) \text{ are Newton-Puiseux series of } f \text{ and } \phi\}$$

is *the coincidence exponent* of f and ϕ, then one has the formula:

$$\frac{(f, \phi)}{d(\phi)} = \frac{\overline{B}_k}{N_1 \cdots N_{k-1}} + \frac{N \cdot K(f, \phi) - B_k}{N_1 \cdots N_k}$$

where $k \in \{0, ..., G\}$ is the smallest integer such that $K(f, \phi) < \frac{B_{k+1}}{N}$.

This proposition allows one to translate information about intersection numbers into information about equalities of truncated Newton-Puiseux series and conversely. For example, from Definition 6.4 to Corollary 5.3, where in place of f_k we consider an arbitrary semiroot q_k.

Proposition 6.6 For each $k \in \{0, ..., G\}$, the minimal polynomial ϕ_k of a k-truncated Newton-Puiseux series $\eta_k(X)$ of f is a k-semiroot.

This gives us the Step 1 explained before.

Proposition 6.7 If $\phi \in \mathbf{C}[[X]][Y]$ and $d(\phi) < \frac{N}{E_k}$, then $(f, \phi) \in \langle \overline{B}_0, ..., \overline{B}_k \rangle$.

In other words, $\frac{N}{E_k}$ is the minimal degree for which one can obtain the value $\overline{B}_{k+1}$ in the semigroup $\Gamma(C)$.

Proposition 6.8 If ϕ is a k-semiroot and ψ is a $(k-1)$-semiroot, $k \in \{1, ..., G\}$, then $\tau_\phi(\psi)$ is a $(k-1)$-semiroot of f.

This gives Step 2 in the proof of Theorem 5.1.

7 The proofs of the main theorem and of its corollaries

Proof of Theorem 5.1

1) The first equality $d(f_k) = \frac{N}{E_k}$ is clear from the definition of approximate roots.

The main point is to prove that $(f, f_k) = \overline{B}_{k+1}$ for all $k \in \{0, ..., G\}$, where $\overline{B}_{G+1} = \infty$. We shall prove it by descending induction, starting from $k = G$. Then $f_G = f$ and so $(f, f_G) = \infty = \overline{B}_{G+1}$.

Let us suppose that $(f, f_k) = \overline{B}_{k+1}$, with $k \in \{1, ..., G\}$. Then we have by Proposition 3.3:

$$f_{k-1} = \sqrt[E_{k-1}]{f} = \sqrt[N_k E_k]{f} = \sqrt[N_k]{\sqrt[E_k]{f}}$$

and so: $f_{k-1} = \sqrt[N_k]{f_k}$.

By Proposition 6.3, we know that $\sqrt[N_k]{f_k} = \underbrace{\tau_{f_k} \circ \cdots \circ \tau_{f_k}}_{d(f_k)/N_k}(q_{k-1})$, where q_{k-1} is an arbitrary polynomial of degree $\frac{N}{E_{k-1}}$. We shall take for q_{k-1} an arbitrary $(k-1)$-semiroot, which exists by Proposition 6.6. By the induction hypothesis, f_k is a k-semiroot. By Proposition 6.8, if ψ is a $(k-1)$-semiroot of f, then $\tau_{f_k}(\psi)$ is again a $(k-1)$-semiroot. Starting with ϕ_{k-1} and applying the operator τ_{f_k} consecutively $\frac{d(f_k)}{N_k} = \frac{N}{E_{k-1}}$ times, we deduce that $\sqrt[N_k]{f_k}$ is a $(k-1)$-semiroot of f.

The induction step is completed, so we have proved the first part of the proposition.

2)We show that this is true generally for an arbitrary k-semiroot q_k. First we prove that q_k is irreducible.

Suppose this is not the case. Then $q_k = \prod_{i=1}^m r_i$, where $m \geq 2$ and $r_i \in \mathbf{C}[[X]][Y]$ are monic polynomials of degree at least 1. So, for all i, $d(r_i) < < d(q_k) = \frac{N}{E_k}$. By Proposition 6.7, $(f, r_i) \in \langle \overline{B}_0, ..., \overline{B}_k \rangle$ and so $(f, q_k) = = \sum_{i=1}^m (f, r_i) \in \langle \overline{B}_0, ..., \overline{B}_k \rangle$, which contradicts $(f, q_k) = \overline{B}_{k+1}$. This shows that q_k is irreducible.

We have to prove now the claim concerning its characteristic exponents. We apply Proposition 6.5, which expresses $\frac{(f,q_k)}{d(q_k)}$ in terms of the coincidence exponent of f and q_k.

First, we have directly by the property of being a k-semiroot: $\frac{(f,q_k)}{d(q_k)} = \frac{\overline{B}_{k+1}}{d(q_k)} = = \frac{\overline{B}_{k+1}}{N_1 \cdots N_k}$. So, by Proposition 6.5, one has $K(f, q_k) = B_{k+1}$, which implies that the k-truncated Newton-Puiseux series of f and q_k are equal. This means that the first k terms of the characteristic sequence of q_k are $l\frac{B_0}{E_k}, l\frac{B_1}{E_k}, ..., l\frac{B_k}{E_k}$, with $l \in \mathbf{N}^*$. So $d(q_k) = l\frac{B_0}{E_k} = l\frac{N}{E_k}$. But we know that $d(q_k) = \frac{N}{E_k}$, and this implies that $l = 1$, which in turn implies that q_k has no more characteristic exponents. $\square$

Proof of Corollary 5.2

The point here is to compute the characteristic approximate roots and the characteristic sequence without previously computing truncated Newton-Puiseux parameterizations.

The algorithm given in the statement works because

$$\gcd(\overline{B}_0, ..., \overline{B}_k) = \gcd(B_0, ..., B_k) = E_k,$$

which is part of Proposition 4.2.

Once the characteristic roots have been computed, by-products of the algorithm are the sequences $(\overline{B}_0, ..., \overline{B}_G)$ and $(E_0, ..., E_G)$. From the point 1 of Proposition 4.2 one deduces then the characteristic sequence $(B_0, ..., B_G)$. $\square$

Example: Take:

$$f(X,Y) = Y^4 - 2X^3Y^2 - 4X^5Y + X^6 - X^7,$$

an example already considered to illustrate Proposition 2.2. We suppose here we do not know a Newton-Puiseux parameterization for it. We suppose it is irreducible - indeed it is, and the elaborations of the algorithm alluded to in the text would show it - so we apply the algorithm:

$$\begin{aligned}
&N = B_0 = \overline{B}_0 = E_0 = 4\\
&f_0 = \sqrt[4]{f} = Y\\
&(f, f_0) = 6\\
&E_1 = \gcd(4,6) = 2\\
&f_1 = \sqrt[2]{f} = \tau_f \circ \tau_f(Y^2) = Y^2 - X^3\\
&(f, f_1) = 13\\
&E_2 = \gcd(E_1, \overline{B}_2) = \gcd(2, 13) = 1\\
&G = 2\\
&N_1 = \tfrac{E_1}{E_2} = 2\\
&B_2 = B_1 + \overline{B}_2 - N_1\overline{B}_1 = 6 + 13 - 2 \cdot 6 = 7.
\end{aligned}$$

So:

$$(B_0, B_1, B_2) = (4, 6, 7).$$

Proof of Corollary 5.3

The more general formulation is: *If q_k is a k-semiroot, f and q_k have equal k-truncated Newton-Puiseux series.* The proof is contained in that of Theorem 5.1, point 2, where it was seen that $K(f, q_k) = B_{k+1}$. $\square$

Proof of Corollary 5.4

We give first the more general formulation which we prove in the sequel:

Let $q_0, ..., q_G \in \mathbf{C}[[X]][Y]$ be monic polynomials such that for all i, $d(q_i) = \frac{N}{E_i}$. Then every $\phi \in \mathbf{C}[[X]][Y]$ can be uniquely written in the form:

$$\phi = \sum_{finite} \alpha_{i_0 \ldots i_G} q_0^{i_0} q_1^{i_1} \cdots q_G^{i_G}$$

where $i_G \in \mathbf{N}$, $0 \leq i_k < N_{k+1}$ for $0 \leq k \leq G-1$ and the coefficients $\alpha_{i_0 \ldots i_G}$ are elements of the ring $\mathbf{C}[[X]]$. Moreover:

1) the Y-degrees of the terms appearing in the right-hand side of the preceding equality are all distinct.

2) if for every $k \in \{0, ..., G\}$, q_k is a k-semiroot, then the orders in T of the terms

$$\alpha_{i_0 \ldots i_{G-1}}(T^N) q_0(T^N, Y(T))^{i_0} \cdots q_{G-1}(T^N, Y(T))^{i_{G-1}}$$

are pairwise distinct, where $T \to (T^N, Y(T))$ is a Newton-Puiseux parameterization of f.

Take first the q_G-adic expansion of ϕ:

$$\phi = \sum_{0 \leq i_G \leq [\frac{d(\phi)}{d(q_G)}]} \alpha_{i_G} q_G^{i_G}.$$

Here $\alpha_{i_G} \in \mathbf{C}[[X]][Y]$ and $d(\alpha_{i_G}) < d(q_G) = \frac{N}{E_G} = N$.

Take now the q_{G-1}-adic expansion of every coefficient α_{i_G}:

$$\alpha_{i_G} = \sum \alpha_{i_{G-1} i_G} q_{G-1}^{i_{G-1}}.$$

The coefficients $\alpha_{i_{G-1} i_G} \in \mathbf{C}[[X]][Y]$ have degrees $d(\alpha_{i_{G-1} i_G}) < d(q_{G-1})$ and the sum is over $i_{G-1} < N_G$.

Proceeding in this manner we get an expansion with the required properties. Before proving the unicity, we prove point 1), namely the inequality of the degrees.

Suppose there exist $(i_0, ..., i_G) \neq (j_0, ..., j_G)$ and

$$d(\alpha_{i_0 \ldots i_G} q_0^{i_0} q_1^{i_1} \cdots q_G^{i_G}) = d(\alpha_{j_0 \ldots j_G} q_0^{j_0} q_1^{j_1} \cdots q_G^{j_G}) \neq \infty.$$

This means:

$$\sum_{k=0}^{G} i_k \cdot \frac{N}{E_k} = \sum_{k=0}^{G} j_k \cdot \frac{N}{E_k}.$$

Let us define $p \in \{0, ..., G\}$ such that $i_k = j_k$ for $k \geq p+1$ and $i_p < j_p$. If such a p does not exist, simply interchange $(i_0, ..., i_G)$ and $(j_0, ..., j_G)$, then apply the preceding definition. We obtain:

$$\sum_{k=0}^{p-1} (i_k - j_k) \frac{N}{E_k} = (j_p - i_p) \frac{N}{E_p}.$$

But $j_p - i_p \geq 1$ and $\mid i_k - j_k \mid \leq N_{k+1} - 1$, so:

$$\begin{aligned} \frac{N}{E_p} \quad & \leq \textstyle\sum_{k=0}^{p-1} (N_{k+1} - 1) \frac{N}{E_k} = \sum_{k=0}^{p-1} (\frac{E_k}{E_{k+1}} - 1) \frac{N}{E_k} = \\ & = \textstyle\sum_{k=0}^{p-1} (\frac{N}{E_{k+1}} - \frac{N}{E_k}) = \frac{N}{E_p} - 1 \end{aligned}$$

which is a contradiction.

Now, this property of the degrees shows that $0 \in \mathbf{C}[[X]][Y]$ has only the trivial expansion, and this in turn shows the unicity.

Let us move to point 2). From now on, q_k is a k-semiroot. By the properties of intersection numbers recalled in section 4, $v_T(q_k(T^N, Y(T))) = (f, q_k) = \overline{B}_{k+1}$. So:

$$v_T(\alpha_{i_0 \dots i_{G-1} 0}(T^N) q_0(T^N, Y(T))^{i_0} \cdots q_{G-1}(T^N, Y(T))^{i_{G-1}}) = \sum_{k=-1}^{G-1} i_k \overline{B}_{k+1}.$$

Here $i_{-1} = v_X(\alpha_{i_0 \dots i_{G-1} 0}(X)) \in \mathbf{N}$.

Let us suppose we have $(i_0, ..., i_{G-1}) \neq (j_0, ..., j_{G-1})$ such that: $\sum_{k=-1}^{G-1} i_k \overline{B}_{k+1}$ $= \sum_{k=-1}^{G-1} j_k \overline{B}_{k+1}$. As before, we take $p \in \{0, ..., G-1\}$ with $i_k = j_k$ for $k \geq p+1$ and $i_p < j_p$. So: $(j_p - i_p)\overline{B}_{p+1} = \sum_{k=-1}^{p-1} (i_k - j_k) \overline{B}_{k+1}$ which gives: $E_p \mid (j_p - i_p)\overline{B}_{p+1}$. But $E_{p+1} = \gcd(E_p, \overline{B}_{p+1})$, by Proposition 4.2, and we get: $N_{p+1} = \frac{E_p}{E_{p+1}} \mid (j_p - i_p)$. As $0 < j_p - i_p < N_{p+1}$, we get a contradiction.

With this, point 2) is proved. $\square$

Proof of Corollary 5.5

We prove the following fact:

If $q_0, ..., q_G$ are semiroots of f, the images of $(X, q_0, ..., q_{G-1})$ in the graded ring $gr_{v_T}(\mathcal{O}_C)$ generate it. If the coordinates are generic, they form a minimal system of generators.

We take the notations explained in section 5, with $A = \mathcal{O}_C$. For every $p \in$ $\in \Gamma(C)$, $\dim_{\mathbf{C}}(I_p/I_p^+) = 1$. The vector space I_p/I_p^+ is generated by an arbitrary element $\phi \in \mathcal{O}_C$ such that $v_T(\phi) = p$. We obtain:

$$gr_{v_T}(\mathcal{O}_C) \simeq \bigoplus_{\{p \in \Gamma(C)\}} \mathbf{C} T^p.$$

We have: $v_T(X) = N$ and $v_T(q_k) = \overline{B}_{k+1}$, for $k \in \{0, ..., G-1\}$. To show that the images of $X, q_0, ..., q_{G-1}$ generate $gr_{v_T}(\mathcal{O}_C)$ is equivalent with the fact that every $\omega \in gr_{v_T}(\mathcal{O}_C)$ can be expressed as a polynomial $P_\omega(T^N, T^{\overline{B}_1}, ..., T^{\overline{B}_G})$. This comes in turn from Proposition 4.2. Indeed, it is shown that $\langle \overline{B}_0, \overline{B}_1, ..., \overline{B}_G \rangle =$ $= \Gamma(C)$ and so every $p \in \Gamma(C)$ can be written as $p = \sum_{k=-1}^{G-1} i_k \overline{B}_{k+1}$, which implies $T^p = (T^N)^{i_{-1}} (T^{\overline{B}_1})^{i_0} \cdots (T^{\overline{B}_G})^{i_{G-1}}$. An arbitrary $\omega \in gr_{v_T}(\mathcal{O}_C)$ is then a linear combination of such terms.

Another proof can use Corollary 5.4.

In case the coordinates are generic, $\overline{B}_0 = m(C)$, the multiplicity of C at the origin, and this is the smallest non-zero value in $\Gamma(C)$. Then $(\overline{b}_0, ..., \overline{b}_g)$ is a minimal system of generators of $\Gamma(C)$. Indeed, what prevented $(\overline{B}_0, ..., \overline{B}_G)$ from being minimal was the possibly non minimal value of $\overline{B}_0$ in $\Gamma(C) - \{0\}$ (see Proposition 4.2).

Now, the minimality for the algebra $gr_{v_T}(\mathcal{O}_C)$ comes from the minimality for the semigroup $\Gamma(C)$. $\square$

Remark: An equivalent statement (using the notion of maximal contact explained after Corollary 5.6, rather than the notion of semiroot), was proved by M. Lejeune-Jalabert. See the paragraph 1.2.3 in the Appendix of [49].

Proof of Corollary 5.6

Instead of the characteristic roots we consider arbitrary semiroots q_k and we show that the Corollary is also true in this greater generality. We sketch three proofs of the Corollary. The first one uses adequate coordinate systems to follow the strict transforms of C_f and C_{q_k} during the process of blowing-ups. The second and third one are more intrinsic.

1) Let us consider generic coordinates (X,Y) and Newton-Puiseux series $\eta(X)$, $\eta_k(X)$ for f, respectively q_k. We have:

$$\eta(X)=\sum_{j\geq n} a_j X^{\frac{j}{n}}.$$

If $\gamma_1 : S_1 \rightarrow \mathbf{C}^2$ is the blow-up of $0\in\mathbf{C}^2$, the strict transform C_f^1 of C_f in S_1 passes through the origin of a chart of coordinates (X_1,Y_1) such that:

$$\begin{cases} X=X_1 \\ Y=X_1(a_n+Y_1) \end{cases}.$$

The strict transform C_f^1 of C_f has in the coordinates (X_1,Y_1) a Newton-Puiseux series of the form:

$$\eta^{(1)}(X_1)=\sum_{j\geq n+1} a_j X_1^{\frac{j}{n}-1}.$$

The coordinates (X_1,Y_1) are generic for it if and only if $[\frac{b_1}{n}]\geq 2$. If this is the case, one describes the restriction of the next blowing-up to the chart containing the strict transform of C_f by the change of variables:

$$\begin{cases} X_1=X_2 \\ Y_1=X_2(a_{2n}+Y_2) \end{cases}.$$

One continues like this $s_1:=[\frac{b_1}{n}]$ times till one arrives in the chart (X_{s_1},Y_{s_1}) at a strict transform $C_f^{s_1}$ with Newton-Puiseux series:

$$\eta^{(s_1)}(X_{s_1})=\sum_{j\geq b_1} a_j X_{s_1}^{\frac{j}{n}-s_1}.$$

Now for the first time the coordinates are not generic with respect to the series. Let us look also at the strict transform $C_{q_0}^{s_1}$ of C_{q_0}. By Corollary 5.3, the branch C_{q_0} has a Newton-Puiseux series $\eta_0(X)$ such that:

$$\eta_0(X)=\sum_{j\geq 1} a'_j X^{\frac{j}{n}}$$

with $a'_j=a_j$ for $j<b_1$ and $n\mid j$ for all $j\in\mathbf{N}^*$.

The strict transform $C_{q_0}^{s_1}$ then has a Newton-Puiseux series of the form:

$$\eta_0^{s_1}(X_{s_1})=\sum_{j\geq b_1} a'_j X_{s_1}^{\frac{j}{n}-s_1}.$$

The series in the right-hand side has integral exponents, which shows that $C_{q_0}^{s_1}$ is smooth - which was evident, as C_{q_0} was already smooth. But, more important, $C_{q_0}^{s_1}$ is not tangent to $X_{s_1}=0$. This shows that it is transverse to $C_f^{s_1}$ and to the only component of the exceptional divisor passing through $(X_{s_1},Y_{s_1})=(0,0)$, which is defined by the equation: $X_{s_1}=0$.

The next blowing-up separates the strict transforms of C_f and C_{q_0}. The curve $C_{q_0}^{(s_1+1)}$ passes through a smooth point of the newly created component of the exceptional divisor.

This shows that the dual graph of the total transform of $f\cdot f_0$ is as drawn in Figure 3.

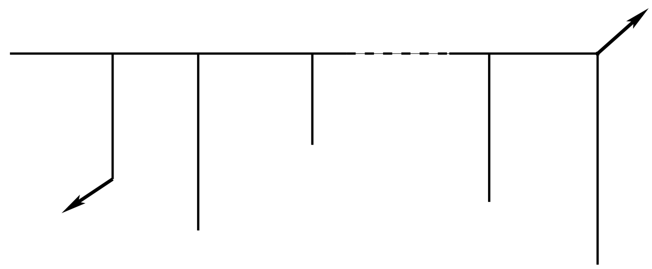

Figure 3 The Dual Graph of the Product

To continue, one needs to change coordinates after s_1 blowing-ups. Instead of considering the ordered coordinates (X_{s_1}, Y_{s_1}), we look at (Y_{s_1}, X_{s_1}). We now use the inversion formulae explained in Proposition 4.3. They allow to express the characteristic exponents of $C_f^{s_1}$ with respect to (Y_{s_1}, X_{s_1}) in terms of those with respect to (X_{s_1}, Y_{s_1}). Moreover, it follows from the property of truncations stated in Proposition 4.3 that, if one inverts simultaneously the strict transforms of $C_f, C_{q_0}, ..., C_{q_{g-1}}$, they keep having coinciding Newton-Puiseux series up to controlled orders. Repeating this process, one shows that after a number of inversions equal to the number of terms in the continuous fraction expansion of $\frac{b_1}{n}$, the initial situation is repeated, but with a curve having genus $(g-1)$. The strict transform of the semiroot q_k, for $k \in \{1, ..., g\}$ will be a $(k-1)$-semiroot for the strict transform of f, in the natural coordinates resulting from the process of blowing-ups. So, one can iterate the analysis made for q_0 and get the corollary. $\square$

2) Given two branches at the origin, from the knowledge of their characteristic exponents and of their coincidence exponent (see Proposition 6.5), one can construct the dual graph of resolution of their product. This is explained in [31] and proved in detail, as well as in the case of an arbitrary number of branches, in [21]. In our case this shows that the minimal embedded resolution of f, where q_k is an arbitrary semiroot for generic coordinates, is also an embedded resolution of $f \cdot q_k$. Moreover, the extended dual graph is obtained from the dual graph $D(\pi_m, f)$ attaching an arrow-head vertex at the end of the k-th vertical segment (see the explanations given after Corollary 5.6). We get from it the corollary. $\square$

3) If $l \in \mathbf{C}[[X, Y]]$ is of multiplicity 1, let $\pi_m^*(l)$ be its total transform divisor on Σ_m. If L is a component of $\mathcal{E}$, the exceptional divisor of π_m, let $\mu(L)$ be its multiplicity in $\pi_m^*(l)$. Let also $\phi(L)$ be its multiplicity in $\pi_m^*(f)$. These multiplicities can be computed inductively, following the order of creation of the components in the process of blowing-ups. In particular, if L_k is the component represented at the end of the k-th vertical segment of the dual graph, $\mu(L_k) = \frac{n}{e_{k-1}}$ for $k \in \{1, ..., g\}$, and $\phi(L_k) = \overline{b}_k$ (folklore).

Let us consider now the branch $C_{q_{k-1}}$. We know that $(f, q_{k-1}) = \overline{b}_k$ and $m(q_{k-1}) = \frac{n}{e_{k-1}}$, where $n = m(f)$. Then $\frac{(f, q_{k-1})}{m(q_{k-1})} = \frac{e_{k-1}\overline{b}_k}{n}$ and the lemma on the growth of coefficients of insertion in [31] shows that the strict transform of $C_{q_{k-1}}$ necessarily meets a component of the k-th vertical segment of $D(\pi_m)$. If $C'_{q_{k-1}}$ is the strict transform of q_{k-1} by π_m, we have:

$$(f, q_{k-1}) = (\pi_m^*(f), C'_{q_{k-1}}) = \sum_L \phi(L)(L, C'_{q_{k-1}})$$

the sum being taken over all the components of $\mathcal{E}$ which meet $C'_{q_{k-1}}$. Now it can be easily seen that ϕ strictly grows on a vertical segment of $D(\pi_m)$, from the end to the point of contact with the horizontal segment. This comes from the fact that those components of the exceptional divisor are created in this order - but not necessarily consecutively. As $\phi(L_k) = \overline{b}_k$ and $(f, q_{k-1}) = \overline{b}_k$, we see that:

$$\overline{b}_k = \sum_L \phi(L)(L, C'_{q_{k-1}}) \geq \sum_L \phi(L) m(C'_{q_{k-1}}) \geq \phi(L_k) \cdot 1 = \overline{b}_k.$$

This means that the inequalities are in fact equalities and shows that $C'_{q_{k-1}}$ is smooth, meets L_k transversely and meets no other component of $\mathcal{E}$. □

Proof of Corollary 5.9

We prove:

A semiroot q_k of f in arbitrary coordinates is a curvette with respect to one of the components L_k, L_{k+1}.

We analyze successively the three cases introduced in Proposition 4.3, using also some results of its proof.

1) $\underline{B_0 = b_0}$.

This is the case of generic coordinates. The affirmation is the same as Corollary 5.6. We get that q_k is a curvette with respect to L_{k+1}, for all $k \in \{0, ..., g\}$.

2) $\underline{B_0 = lb_0}$, with $2 \leq l \leq [\frac{b_1}{b_0}]$.

Then, by Proposition 4.3, $G = g + 1$.

The curve q_0 is smooth and so $m(q_0) = 1$.

Moreover, by the definition of semiroots, $(f, q_0) = \overline{B}_1 = \overline{b}_0 = m(f)$.

This shows that q_0 is smooth and transversal to f and so it is a curvette with respect to L_0.

If $k \in \{1, ..., G\}$, where by Proposition 4.3, $G = g + 1$, we have:

$$m(q_k) = b_0(q_k) = B_1(q_k) = \frac{B_1}{E_k} = \frac{b_0}{e_{k-1}},$$

$$(f, q_k) = \overline{B}_{k+1} = \overline{b}_k.$$

We have noted by $b_0(q_k)$ the corresponding characteristic exponent of q_k.

So, for $k \in \{1, ..., G-1\}$, the curve q_k is a $(k-1)$-semiroot with respect to generic coordinates and by Corollary 5.6, it is a curvette with respect to L_k.

3) $\underline{B_0 = b_1}$

By Proposition 4.3, we have $G = g$.

Again q_0 is smooth. Using Proposition 4.3 we obtain:

$$(f, q_0) = \overline{B}_1 = \overline{b}_0 = m(f).$$

As in the preceding case, q_0 is a curvette with respect to L_0.

If $k \in \{1, ..., G\}$, where $G = g$, we have:

$$m(q_k) = b_0(q_k) = B_1(q_k) = \frac{B_1}{E_k} = \frac{b_0}{e_k},$$

$$(f, q_k) = \overline{B}_{k+1} = \overline{b}_{k+1}.$$

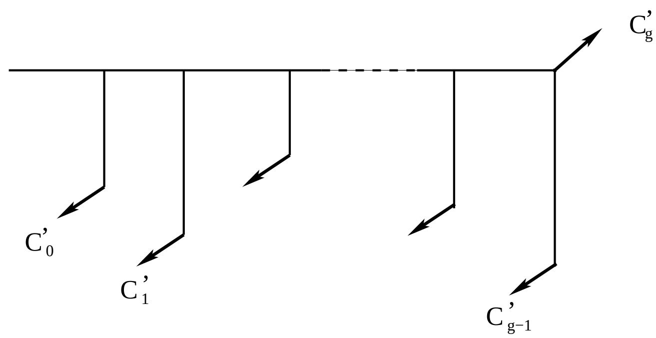

Figure 4 $B_0 = b_0$

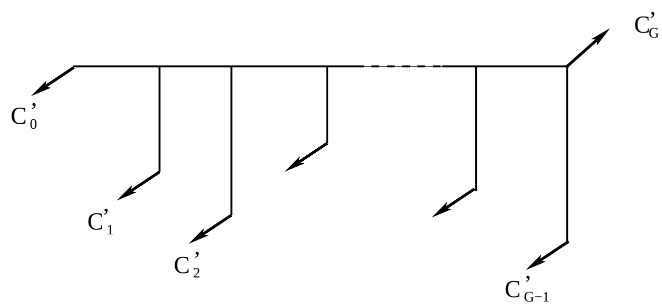

Figure 5 $B_0 = lb_0, l \geq 2$

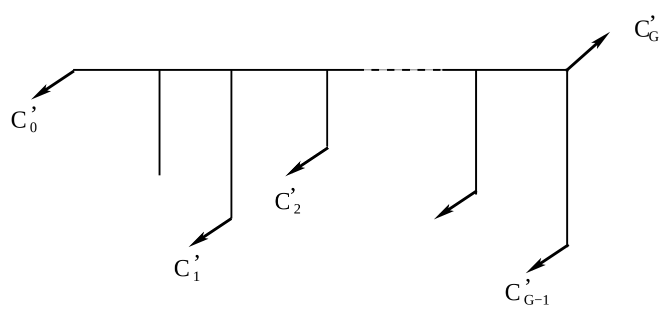

Figure 6 $B_0 = b_1$

So q_k is a k-semiroot with respect to generic coordinates, and by Corollary 5.6, it is a curvette with respect to L_{k+1}.

Let us summarize this study by drawing for each of the three cases the dual graph of the total transform of the product $q_0 \cdots q_G$. As in the statement of Corollary 5.6, we denote by C'_k the strict transform of q_k. We obtain the situations indicated in Figures 4, 5, 6. $\square$

8 The proofs of the propositions

Proof of Proposition 2.1

The series $\zeta(X)$ can be obtained from $\eta(X)$ by replacing $X^{\frac{1}{N}}$ by $\omega X^{\frac{1}{N}}$, where $\omega \in \mu_N$, the group of N-th roots of unity. One has the inclusions of cyclic groups: $\mu_{\frac{N}{E_0}} \subset \mu_{\frac{N}{E_1}} \subset \cdots \subset \mu_{\frac{N}{E_G}} = \mu_N$. Let $k \in \{0, ..., G\}$ be such that $\omega \in \mu_{\frac{N}{E_k}} - \mu_{\frac{N}{E_{k-1}}}$. Then:

$$v_X(\eta(X) - \zeta(X)) = \begin{cases} \infty, \text{ if } k = 0 \\ \frac{E_k}{N}, \text{ if } k \in \{1, ..., G\} \end{cases}.$$

□

Proof of Proposition 2.2

We start from $f = Y^N + \alpha_1(X)Y^{N-1} + \alpha_2(X)Y^{N-2} + \cdots + \alpha_N(X)$. Let us consider the approximate root $f_k = \sqrt[E_k]{f}$.

As is seen from equation (8.1) in the proof of Proposition 3.1, its coefficients depend only on $\alpha_1(X), ..., \alpha_{\frac{N}{E_k}}(X)$.

Corollary 5.3 shows that f and f_k have equal k-truncated Newton-Puiseux series. Combining these facts we see that the k-truncated Newton-Puiseux series of f depend only on $\alpha_1(X), ..., \alpha_{\frac{N}{E_k}}(X)$. □

Proof of Proposition 3.1

Let us put

$$Q = Y^{\frac{n}{p}} + a_1 Y^{\frac{n}{p}-1} + \cdots + a_{\frac{n}{p}}.$$

The inequality $d(P - Q^p) < d(P) - \frac{d(P)}{p}$ means that the coefficients of Y^n, $Y^{n-1}, ..., Y^{n-\frac{n}{p}}$ in the polynomial $P - Q^p$ are equal to 0. This gives the system of equalities:

$$\begin{cases} \alpha_1 = p a_1 \\ \alpha_2 = p a_2 + \begin{pmatrix} p \\ 2 \end{pmatrix} a_1^2 \\ \vdots \\ \alpha_k = p a_k + \sum_{i_1 + 2i_2 + \cdots + (k-1)i_{k-1} = k} c_{i_1 \ldots i_{k-1}} a_1^{i_1} \cdots a_{k-1}^{i_{k-1}}, \ 1 \leq k \leq \frac{n}{p} \end{cases} \tag{8.1}$$

Here the coefficients $c_{i_1 \ldots i_{k-1}}$ are integers, easily expressible in terms of binomial coefficients:

$$c_{i_1 \ldots i_{k-1}} = \begin{pmatrix} p \\ i_1 + \cdots + i_{k-1} \end{pmatrix} \frac{(i_1 + \cdots + i_{k-1})!}{i_1! \cdots i_{k-1}!}.$$

We see that from the relations (8.1) one can compute successively $a_1, a_2, ..., a_{\frac{n}{p}}$. One has only to divide at each step by p. That is the reason why in the definition of the approximate root we asked p to be invertible.

So $a_1, a_2, ..., a_{\frac{n}{p}}$ exist and are uniquely determined. Moreover, they depend only on $\alpha_1, ..., \alpha_{\frac{n}{p}}$. □

Proof of Proposition 3.3

Let us note $Q := \sqrt[p]{P}$ and $R := \sqrt[q]{Q}$.

We want to show that $R = \sqrt[pq]{P}$, i.e. that $d(P - R^{pq}) < d(P) - \frac{d(P)}{pq}$.

If $S := Q - R^q$, we know that $d(S) < d(Q) - \frac{d(Q)}{q} = \frac{d(P)}{p} - \frac{d(P)}{pq}$. Then: $P - Q^p = P - (R^q + S)^p = (P - R^{pq}) - \sum_{k=1}^p \begin{pmatrix} p \\ k \end{pmatrix} S^k R^{q(p-k)}$, and so:

$$P - R^{pq} = (P - Q^p) + \sum_{k=1}^{p} \begin{pmatrix} p \\ k \end{pmatrix} S^k R^{q(p-k)}$$

which implies:

$$d(P - R^{pq}) \leq \max(\{d(P - Q^p)\} \cup \{d(S^k R^{q(p-k)}), 1 \leq k \leq p\}).$$

We know that $d(P - Q^p) < d(P) - \frac{d(P)}{p}$, and for $1 \leq k \leq p$ we have:

$$\begin{aligned} d(S^k R^{q(p-k)}) &= kd(S) + q(p-k)d(R) < \\ &< k(\frac{d(P)}{p} - \frac{d(P)}{pq}) + q(p-k)\frac{d(P)}{pq} = \\ &= k\frac{d(P)}{p} - k\frac{d(P)}{pq} + d(P) - k\frac{d(P)}{p} = \\ &= d(P) - k\frac{d(P)}{pq} \leq d(P) - \frac{d(P)}{pq}. \end{aligned}$$

So finally:

$$d(P - R^{pq}) < \max\{d(P) - \frac{d(P)}{p}, d(P) - \frac{d(P)}{pq}\} = d(P) - \frac{d(P)}{pq}$$

which shows that $R = \sqrt[pq]{P}$. □

Proof of Proposition 3.4

If $P(Y) = Y^n + \alpha_1 Y^{n-1} + \alpha_2 Y^{n-2} + \cdots + \alpha_n$, then :

$$P_1(Z) = Z^{-n}(1 + \alpha_1 Z + \cdots + \alpha_n Z^n)$$

and so:

$$P_1^{\frac{1}{p}}(Z) = Z^{-\frac{n}{p}}(1 + \sum_{k \geq 1} c_k Z^k) = M(P_1^{\frac{1}{p}}) + H(P_1^{\frac{1}{p}})$$

where:

$$M(P_1^{\frac{1}{p}}) := Z^{-\frac{n}{p}} + c_1 Z^{1-\frac{n}{p}} + \cdots + c_{\frac{n}{p}},$$

$$H(P_1^{\frac{1}{p}}) := \sum_{k \geq 1} c_{k+\frac{n}{p}} Z^k.$$

Here the coefficients c_k are elements of A, uniquely determined polynomially by the coefficients of P. We get:

$$Q(Y) = Y^{\frac{n}{p}} + c_1 Y^{\frac{n}{p}-1} + \cdots + c_{\frac{n}{p}}.$$

Let us consider:

$$R(Y) := P(Y) - Q(Y)^p.$$

We want to show that $d(R) < n - \frac{n}{p}$, which is equivalent to $v_Z(R(Z^{-1})) \geq -n + \frac{n}{p} + 1$, v_Z designating the order of a series in $A((Z))$. But:

$$\begin{aligned} R(Z^{-1}) &= P(Z^{-1}) - Q(Z^{-1})^p = \\ &= P_1(Z) - (M(P_1^{\frac{1}{p}}))^p = \\ &= P_1 - (P_1^{\frac{1}{p}} - H(P_1^{\frac{1}{p}}))^p = \\ &= \sum_{k=1}^{p} (-1)^{k+1} \begin{pmatrix} p \\ k \end{pmatrix} P_1^{\frac{p-k}{p}} S^k. \end{aligned}$$

where we have noted $S := H(P_1^{\frac{1}{p}})$. We obtain:

$$v_Z(R(Z^{-1})) \geq \min_{1 \leq k \leq p}\{v_Z(P_1^{\frac{p-k}{p}} S^k)\} = \min_{1 \leq k \leq p}\{-n \cdot \frac{p-k}{p} + k \cdot 1\} = -n + \frac{n}{p} + 1$$

which is the inequality we wanted to prove.

So $d(P(Y) - Q(Y)^p) < n - \frac{n}{p}$, and this shows that $Q = \sqrt[p]{P}$. $\square$

Proof of Proposition 4.2

The degree $d(f)$ can be obtained as an intersection number: $N = d(f) = v_T(f(0,T)) = (f, X)$. So $N \in \Gamma(C)$.

We now *define* $\overline{b}_k$ by the relation given in point 2) of the proposition. We prove that the numbers defined in this way are indeed elements of the semigroup $\Gamma(C)$ and verify the minimality property used to define them in the text.

The important fact is that Proposition 6.5 is proved only using the formulas of the $\overline{B}_k$'s in terms of the B_k's. That is the reason why we can apply it in what follows.

Consider the minimal polynomials ϕ_k of the k-truncated Newton-Puiseux series $\eta_k(X)$, for $k \in \{0, ..., G-1\}$ (see Proposition 6.6 and its proof). Then $d(\phi_k) = = \frac{N}{E_k} = N_1 \cdots N_k$ and $K(f, \phi_k) = \frac{B_{k+1}}{N}$, so Proposition 6.5 gives: $\frac{(f,\phi_k)}{d(\phi_k)} = \frac{\overline{B}_{k+1}}{N_1 \cdots N_k}$. We get:

$$(f, \phi_k) = \overline{B}_k.$$

This shows that $\overline{B}_k \in \Gamma(C)$.

Consider now an arbitrary element $g \in \mathbf{C}[[X]][Y]$ and expand it in terms of $(\phi_0, ..., \phi_G)$ as explained in the proof of Corollary 5.4. Indeed, $(\phi_0, ..., \phi_G)$ are semiroots of f and we show in the proof that the corollary is true in this greater generality. Notice that the content of this corollary is true in our case, because we use only point 2) of Proposition 4.2 which, as well as point 3), results from point 1).

From Corollary 5.4 we get:

$$\begin{aligned} &(f, g) \\ &\quad = \quad \min_{(i_0, \dots, i_{G-1})}\{v_T(\alpha_{i_0 \dots i_{G-1} 0}(T^N)\phi_0(T^N, Y(T))^{i_0} \cdots \phi_{G-1}(T^N, Y(T))^{i_{G-1}})\} \\ &\quad = \quad \min_{(i_0, \dots, i_{G-1})}\{i_{-1}N + i_0 \overline{B}_1 + \cdots + i_{G-1}\overline{B}_G\} \end{aligned}$$

where $i_{-1} = v_X(\alpha_{i_0 \dots i_{G-1} 0})$.

This shows that $\Gamma(C) = \langle \overline{B}_0, ..., \overline{B}_G \rangle$.

Now, for every $k \in \{1, ..., G\}$, we have $\overline{B}_k \notin \langle \overline{B}_0, ..., \overline{B}_{k-1} \rangle$, because E_{k-1} does not divide $\overline{B}_k$.

Suppose $l \in \Gamma(C)$ and $l \notin \langle \overline{B}_0, ..., \overline{B}_{k-1} \rangle$. We already know that $l \in \langle \overline{B}_0, ..., \overline{B}_G \rangle$, so $l = i_{-1}N + i_0\overline{B}_1 + \cdots + i_{G-1}\overline{B}_G$ with $i_j \in \mathbf{N}$ for $j \in \{-1, ..., G-1\}$. As

$l \notin \langle \overline{B}_0, ..., \overline{B}_{k-1} \rangle$, we deduce that for some $j \geq k$, we have $i_j > 0$, which implies $l \geq \overline{B}_j \geq \overline{B}_k$. This proves the equality we were seeking:

$$\overline{B}_k = \min\{j \in \Gamma(C), j \notin \langle \overline{B}_0, ..., \overline{B}_{k-1} \rangle\}.$$

□

Proof of Proposition 4.3

In what follows we look at the functions as elements of $\hat{\mathcal{O}}_{\mathbf{C}^2,0}$. If the local coordinates X, Y are chosen, one obtains a natural isomorphism $\hat{\mathcal{O}}_{\mathbf{C}^2,0} \simeq \mathbf{C}[[X,Y]]$. If $f \in \mathbf{C}[[X]][Y]$, by definition (see section 4), $B_0 = d(f) = (f, X)$. Now, X is a regular function at the origin. We take other coordinates, $x, y \in \hat{\mathcal{O}}_{\mathbf{C}^2}$ generic for the functions f and X. By the implicit function theorem, we have $C_X = C_h$, where:

$$h(x,y) := y - \gamma(x),$$

with $\gamma \in \mathbf{C}[[x]]$. Take a Newton-Puiseux parameterization of C_f:

$$\begin{cases} x = T^{b_0} \\ y = y(T) \end{cases}.$$

Then: $B_0 = (f, X) = (f, h) = v_T(h(T^{b_0}, y(T))) = v_T(y(T) - \gamma(T^{b_0}))$.

The first exponent in $y(T)$ which is not divisible by b_0 is b_1. So, when we vary the choice of γ, we cannot obtain a value $v_T(y(T) - \gamma(T^{b_0}))$ greater than b_1. The value b_1 can be obtained if the truncations of $Y_1(T)$ and $\gamma(T^{b_0})$ coincide up to the order b_1 (not including it). When γ varies, we can also obtain all the values lb_0, with $lb_0 < b_1$, i.e., with $l \leq [\frac{b_1}{b_0}]$.

Once we know the degree B_0, by Proposition 4.2 we know that $\overline{B}_0 = B_0$ and that all the numbers $\overline{B}_1, ..., \overline{B}_G$ are uniquely determined by the minimality property from the semigroup, which is independent of the coordinates. Then one can compute, in this order, the sequences $(E_0, E_1, ..., E_G)$ and $(N_1, ..., N_G)$ and finally obtain all the sequence $(B_0, ..., B_G)$.

Let us treat successively the three cases distinguished in the statement of the proposition.

1) $\underline{B_0 = b_0}$.

This means that the Y-axis is transverse to C_f. Then it is immediate that $G = g$ and $(\overline{B}_0, ..., \overline{B}_G) = (\overline{b}_0, ..., \overline{b}_g)$. So:

$$(B_0, ..., B_G) = (b_0, ..., b_g).$$

2) $\underline{B_0 = l \cdot b_0}$, with $l \in \{2, ..., [\frac{b_1}{b_0}]\}$.

This means that the Y-axis is tangent to C_f but has not maximal contact with it (see the definition of this notion given after Corollary 5.6). Then $\overline{B}_0 = lb_0$. As b_0 is the minimal element of $\Gamma(C) - \{0\}$ and $b_0 < \overline{B}_0$, we see that $\overline{B}_1 = b_0$. Then $E_1 = b_0$ and so $\overline{B}_2 = b_1$. Continuing like this we get:

$$G = g + 1$$
$$(\overline{B}_0, \overline{B}_1, \overline{B}_2, ..., \overline{B}_G) = (l\overline{b}_0, \overline{b}_0, \overline{b}_1, ..., \overline{b}_g)$$
$$(E_0, E_1, E_2, ..., E_G) = (le_0, e_0, e_1, ..., e_g)$$
$$(N_1, N_2, N_3, ..., N_G) = (l, n_1, n_2, ..., n_g).$$

By proposition 4.2, point 1), we get : $B_k - B_{k-1} = \overline{B}_k - N_{k-1}\overline{B}_{k-1} = \overline{b}_{k-1} - N_{k-1}\overline{b}_{k-2}$, for all $k \in \{1, ..., G\}$.

For $k=2$, $B_2 - B_1 = \overline{b}_1 - l\overline{b}_0 = b_1 - lb_0$ which gives:

$$B_2 = b_1 + (1-l)b_0.$$

For $k \geq 3$, $N_{k-1} = n_{k-2}$ and so:

$$B_k - B_{k-1} = \overline{b}_{k-1} - n_{k-2}\overline{b}_{k-2} = b_{k-1} - b_{k-2}.$$

We obtain by induction:

$$(B_0, ..., B_G) = (lb_0, b_0, b_1 + (1-l)b_0, ..., b_g + (1-l)b_0).$$

3) $\underline{B_0 = b_1}$.

This means that the Y-axis has maximal contact with the branch C_f. The same kind of analysis as before shows that:

$$G = g$$
$$(\overline{B}_0, \overline{B}_1, \overline{B}_2, ..., \overline{B}_G) = (\overline{b}_1, \overline{b}_0, \overline{b}_2, ..., \overline{b}_g)$$
$$(E_0, E_1, E_2, ..., E_G) = (b_1, e_1, e_2, ..., e_g)$$
$$(N_1, N_2, N_3, ..., N_G) = (\frac{b_1}{e_1}, n_2, n_3, ..., n_g)$$
$$(B_0, ..., B_G) = (b_1, b_0, b_2 + b_0 - b_1, ..., b_g + b_0 - b_1).$$

In order to deal with truncations we use Proposition 6.5. Since we have two systems of coordinates, we note by $K^{(X,Y)}(f, \phi)$ the coincidence exponent of f and ϕ in the coordinates (X, Y). See Proposition 6.5 for its definition.

Let $\phi_{k+\epsilon}$ be the $(k+\epsilon)$-semiroot of f with respect to (X, Y) which is equal to the minimal polynomial of a $(k+\epsilon)$-truncated Newton-Puiseux series of f (see Proposition 6.6). Then we look at f and $\phi_{k+\epsilon}$ in the coordinates (x, y) and we compute $K^{(x,y)}(f, \phi_{k+\epsilon})$ using Proposition 6.5. This shows that some precisely determined truncations of their Newton-Puiseux series in these coordinates coincide. As $\phi_{k+\epsilon}$ is determined only by the $(k+\epsilon)$-truncation of the Newton-Puiseux series of f with respect to (X, Y), the computations done in each of the three cases give the result.

We give as an example only the treatment of the second case ($B_0 = lb_0$).

In this case $\epsilon = 1$. Let us consider $k \geq 1$ and the semiroot ϕ_{k+1}. We know, by Theorem 5.1, that $(X, \phi_{k+1}) = d(\phi_{k+1}) = \frac{N}{E_{k+1}}$ and $(f, \phi_{k+1}) = \overline{B}_{k+2}$. Then: $(x, \phi_{k+1}) = m(\phi_{k+1}) = \frac{B_1}{B_0} \cdot \frac{N}{E_{k+1}} = \frac{B_1}{E_{k+1}} = \frac{b_0}{e_k}$. So:

$$\frac{(f, \phi_{k+1})}{(x, \phi_{k+1})} = \frac{\overline{B}_{k+2} e_k}{b_0} = \frac{\overline{b}_{k+1} e_k}{b_0} = \frac{\overline{b}_{k+1}}{n_1 \cdots n_k}$$

and Proposition 6.5 applied in the coordinate system (x, y) gives the equality $K^{(x,y)}(f, \phi_{k+1}) = \frac{b_{k+1}}{n}$, which shows that f and ϕ_{k+1} have coinciding k-truncated Newton-Puiseux series in the coordinates (x, y). $\square$

Proof of Proposition 6.1

We consider expansions of the type (6.1):

$$P = a_0 Q^s + a_1 Q^{s-1} + \cdots + a_s$$

with $d(a_i) < d(Q)$ for all $i \in \{0, ..., s\}$.

Let us show that in such an expansion, *the degrees of the terms are all different.* More precisely, we show that:

$$d(a_i Q^{s-i}) > d(a_j Q^{s-j}) \text{ for } i < j. \tag{8.2}$$

Indeed, we have:

$$d(a_iQ^{s-i}) - d(a_jQ^{s-j}) = d(a_i) - d(a_j) + (j-i)d(Q) \geq d(a_i) - d(a_j) + d(Q) > 0.$$

From this property of the degrees, one deduces that a Q-adic expansion of $0 \in A[Y]$ is necessarily trivial, which in turn gives *the unicity of the expansion* for all monic $P \in A[Y]$.

Moreover, identifying the leading coefficients in both sides of equation (6.1), we see that a_0 is monic.

Then we have also: $d(P) = d(a_0Q^s) = d(a_0) + sd(Q)$, which implies:

$$\frac{d(P)}{d(Q)} = s + \frac{d(a_0)}{d(Q)}.$$

But $0 \leq \frac{d(a_0)}{d(Q)} < 1$, which gives the equality $s = [\frac{d(P)}{d(Q)}]$. Also, since a_0 is monic, $d(Q) \mid d(P) \Leftrightarrow d(a_0) = 0 \Leftrightarrow a_0 = 1$.

Let us suppose now we are in the case when $d(Q) \mid d(P)$. We have just seen that in this situation $a_0 = 1$. Then:

$$P - Q^s = \sum_{i=1}^{s} a_iQ^{s-i}$$

and, by the growth property of the degrees (8.2), we get:

$$d(P - Q^s) \leq d(a_2Q^{s-2}) \Leftrightarrow a_1 = 0.$$

But $d(a_2Q^{s-2}) = d(a_2) + (s-2)d(Q) < (s-1)d(Q) = d(P) - \frac{d(P)}{d(Q)}$ and $d(a_1Q^{s-1}) \geq (s-1)d(Q)$ if $a_1 \neq 0$, which implies:

$$d(P - Q^s) < d(P) - \frac{d(P)}{d(Q)} \Leftrightarrow a_1 = 0.$$

By the definition of approximate roots, we see that $a_1 = 0$ if and only if $Q = \sqrt[s]{P}$. □

Proof of Proposition 6.3

Let us take for Q a monic polynomial, $d(Q) = \frac{d(P)}{p}$. The Q-adic expansion of P is of the form:

$$P = Q^p + a_1Q^{p-1} + \cdots + a_p$$

with $d(a_i) < d(Q)$ for $1 \leq i \leq p$.

We consider also the $\tau_P(Q)$-adic expansion of P:

$$P = \tau_P(Q)^p + a'_1\tau_P(Q)^{p-1} + \cdots + a'_p.$$

We shall prove that if $a_1 \neq 0$, we have $d(a'_1) < d(a_1)$. This will show that after iterating τ_P at most $d(a_1)+1$ times, we arrive at the situation $a_1 = 0$, in which case $\tau_P(Q) = Q = \sqrt[p]{P}$. But $d(a_1) + 1 \leq d(Q) = \frac{d(P)}{p}$, which proves the proposition.

So, let us suppose $a_1 \neq 0$. Then:

$$P = (Q + \frac{1}{p}a_1)^p + \sum_{k=2}^{p} a_kQ^{p-k} - \sum_{k=2}^{p} \binom{p}{k} \frac{1}{p^k}a_1^kQ^{p-k}. \tag{8.3}$$

We study now the $\tau_P(Q)$-adic expansion of $P - \tau_P(Q)^p$ starting from equation (8.3). First, for $2 \leq k \leq p$, we have:

$$d(a_kQ^{p-k}) < d(Q) + (p-k)d(Q) \leq (p-1)d(Q)$$

$$d(a_1^k Q^{p-k}) < kd(Q) + (p-k)d(Q) = p \cdot d(Q).$$

But $d(\tau_P(Q)) = d(Q)$ and Proposition 6.1 shows that the $\tau_P(Q)$-adic expansion of $a_k Q^{p-k}$ has non-zero terms of the form $c_j \tau_P(Q)^j$ with $j \leq p-2$ and the $\tau_P(Q)$-adic expansion of $a_1^k Q^{p-k}$ of the form $c_j \tau_P(Q)^j$ with $j \leq p-1$.

Let $c_0^{(k)} \tau_P(Q)^{p-1}$ be the term corresponding to $\tau_P(Q)^{p-1}$ in the $\tau_P(Q)$-adic expansion of $a_1^k Q^{p-k}$. It is possible that $c_0^{(k)} = 0$. Then:

$$d(c_0^{(k)} \tau_P(Q)^{p-1}) \leq d(a_1^k Q^{p-k})$$

and so:

$$d(c_0^{(k)}) \leq k \cdot d(a_1) - k \cdot d(Q) + d(Q) \leq 2d(a_1) - d(Q) \leq d(a_1) - 1.$$

But the polynomial a_1' is a linear combination with coefficients in A of the polynomials $c_0^{(k)}$, which shows the announced inequality:

$$d(a_1') \leq d(a_1) - 1.$$

With this the proof is complete. □

Proof of Proposition 6.5

As stated in section 6, this result is classical. Recent proofs are contained in [34] (for generic coordinates) and [24] (for arbitrary coordinates). We give here a rather detailed proof in order to explain the origin of the formula for $\overline{B}_k$ in Proposition 4.2.

Let $N = d(f), M = d(\phi)$. Decompose $\phi \in \mathbf{C}[[X]][Y]$ as a product of terms of degree 1:

$$\phi(X,Y) = \prod_{i=1}^{M} (Y - \zeta_i(X))$$

where the $\zeta_i(X)$ are all the Newton-Puiseux series of ϕ with respect to (X,Y).

Let $T \to (T^N, Y(T))$ be a parameterization of f, obtained from a fixed Newton-Puiseux series $\eta(X)$. As $T = X^{\frac{1}{N}}$, we have: $Y(T) = \eta(X)$. Then, using the rules explained in section 4:

$$\begin{aligned}(f,\phi) &= v_T(\phi(T^N, Y(T))) = v_T(\textstyle\prod_{i=1}^{M}(Y(T) - \zeta_i(T^N))) = \\ &= v_{X^{\frac{1}{N}}}(\textstyle\prod_{i=1}^{M}(\eta(X) - \zeta_i(X))) = N v_X(\textstyle\prod_{i=1}^{M}(\eta(X) - \zeta_i(X))) = \\ &= N \textstyle\sum_{i=1}^{M} v_X(\eta(X) - \zeta_i(X)))\end{aligned}$$

Now we look at the possible values of $v_X(\eta(X) - \zeta_i(X)))$ when i varies, and for a fixed value we look how many times it is obtained.

If k is minimal such that $K(f,\phi) < \frac{B_{k+1}}{N}$, we get:

- the value $\frac{B_i}{N}$ is obtained $M \cdot \frac{E_{i-1} - E_i}{N}$ times, for $i \in \{1, ..., k\}$.
- the value $K(f,\phi)$ is obtained $M \cdot \frac{E_k}{N}$ times.

So:

$$(f,\phi) = N[\sum_{i=1}^{k} M \cdot \frac{E_{i-1} - E_i}{N} \cdot \frac{B_i}{N} + M \cdot \frac{E_k}{N} \cdot K(f,\phi)]$$

which implies:

$$\frac{(f,\phi)}{M} = \sum_{i=1}^{k} (E_{i-1} - E_i) \frac{B_i}{N} + E_k \cdot K(f,\phi).$$

Now recall the formula for $\overline{B}_k$ given in Proposition 4:

$$\overline{B}_k = B_k + \sum_{i=1}^{k-1} \frac{E_{i-1} - E_i}{E_{k-1}} B_i, \tag{8.4}$$

which gives:

$$\sum_{i=1}^{k-1} \frac{E_{i-1} - E_i}{B_i} = E_{k-1}\overline{B}_k - E_k B_k.$$

We get:

$$\frac{(f,\phi)}{M} = \frac{E_{k-1}\overline{B}_k}{N} - \frac{E_k B_k}{N} + E_k K(f,\phi),$$

which is the desired formula. $\square$

Remark: We had nothing to know about the relation of $\overline{B}_k$ with the semigroup $\Gamma(C)$. We only needed the fact it is given by formula (8.4). See also the comments made in the proof of Proposition 4.2.

Proof of Proposition 6.6

Let $\eta_k(X) = h_k(X^{\frac{E_k}{N}})$. Then $h_k(T) \in \mathbf{C}[[T]]$ and:

$$\begin{cases} X = T^{\frac{N}{E_k}} \\ Y = h_k(T) \end{cases}$$

is a *primitive* Newton-Puiseux parameterization of $(\phi_k = 0)$. So we have:

$$d(\phi_k) = \frac{N}{E_k}.$$

Now, using Proposition 6.5, since $K(f,\phi_k) = \frac{B_{k+1}}{N}$, we have:

$$\frac{(f,\phi_k)}{d(\phi_k)} = \frac{\overline{B}_{k+1}}{N_1 \cdots N_k} \Rightarrow (f,\phi_k) = \frac{N}{E_k} \cdot \frac{\overline{B}_{k+1}}{N_1 \cdots N_k} = \overline{B}_{k+1}.$$

We have obtained: $d(\phi_k) = \frac{N}{E_k}$ and $(f,\phi_k) = \overline{B}_{k+1}$, which shows that ϕ_k is a k-semiroot. $\square$

Proof of Proposition 6.7

We prove the proposition by induction on k.

For $k = 0$, we have $\phi \in \mathbf{C}[[X]]$, and so $\phi(X) = X^M u(X)$, where $u(0) \neq 0$, so: $(f,\phi) = M \cdot (f,x) = M \cdot d(f) \in \langle B_0 \rangle = \langle \overline{B}_0 \rangle$.

Suppose now the proposition is true for $k \in \{0, ..., G-1\}$. We prove it for $k+1$.

Consider $\phi \in \mathbf{C}[[X]][Y], d(\phi) < \frac{N}{E_{k+1}}$ and take a k-semiroot q_k of f, which exists by Proposition 6.6. Make the q_k-adic expansion of ϕ:

$$\phi = a_0 q_k^s + a_1 q_k^{s-1} + \cdots + a_s.$$

We prove that the intersection numbers $(f, a_i q_k^{s-i})$ are all distinct. Suppose by contradiction that $0 \leq j < i \leq s$ and $(f, a_i q_k^{s-i}) = (f, a_j q_k^{s-j})$. Then $(i-j)(f,q_k) = = (f,a_i) - (f,a_j) \in \langle \overline{B}_0, ..., \overline{B}_k \rangle$, by the induction hypothesis. So: $E_k \mid (i-j)\overline{B}_{k+1}$. But $E_{k+1} = \gcd(E_k, \overline{B}_{k+1})$, and so we obtain: $\frac{E_k}{E_{k+1}} \mid (i-j)$. Now, $\frac{E_k}{E_{k+1}} = N_{k+1}$ and $i - j \leq s = [\frac{d(\phi)}{d(q_k)}]$. As $\frac{d(\phi)}{d(q_k)} = \frac{E_k}{N} \cdot d(\phi) < \frac{E_k}{N} \cdot \frac{N}{E_{k+1}} = N_{k+1}$, we see that $s < N_{k+1}$, which gives a contradiction.

This shows that the numbers $(f, a_i q_k^{s-i})$ are all distinct and so:

$$(f,\phi) = \min_i\{(f, a_i q_k^{s-i})\} = \min_i\{(f,a_i) + (s-i)(f,q_k)\}.$$

But $(f, a_i) \in \langle \overline{B}_0, ..., \overline{B}_k\rangle$ by the induction hypothesis and $(f,\phi) = \overline{B}_{k+1}$, so: $(f,\phi) \in \langle \overline{B}_0, ..., \overline{B}_{k+1}\rangle$. With this, the step of induction is completed. □

Proof of Proposition 6.8

If ϕ is a k-semiroot and ψ a $(k-1)$-semiroot, then $d(\phi) = \frac{N}{E_k}$ and $d(\psi) = \frac{N}{E_{k-1}}$. So the ψ-expansion of ϕ is of the form:

$$\phi = \psi^{N_k} + a_1\psi^{N_k - 1} + \cdots + a_{N_k}. \tag{8.5}$$

We have $\tau_\phi(\psi) = \psi + \frac{1}{N_k} a_1$.

We are going to show that:

$$(f,\psi) < (f, a_1).$$

This will give $(f, \tau_\phi(\psi)) = (f,\psi) = \overline{B}_k$. But $d(a_1) < d(\psi)$ and so $d(\tau_\phi(\psi)) = = d(\psi)$, which shows that $\tau_\phi(\psi)$ is also a $(k-1)$-semiroot.

Exactly as in the proof of Proposition 6.7, we have that the intersection numbers $(f, a_i\psi^{N_k - i})$ are all distinct, for $i \in \{1, ..., N_k\}$. Using equation (8.5) we deduce:

$$(f, \phi - \psi^{N_k}) = \min_{1\leq i\leq N_k}\{(f, a_i\psi^{N_k-i})\} \leq (f, a_1\psi^{N_k-1}).$$

But, by Proposition 4.2, $(f,\phi) = \overline{B}_{k+1} > N_k\overline{B}_k = (f, \psi^{N_k})$ and so: $(f, \phi - \psi^{N_k}) = (f, \psi^{N_k})$. We obtain:

$$(f, a_1) + (N_k - 1)(f,\psi) \geq N_k(f,\psi)$$

which gives:

$$(f,\psi) \leq (f, a_1).$$

On the other hand, $d(a_1) < d(\psi) = \frac{N}{E_{k-1}}$, and Proposition 6.7 shows that $(f, a_1) \in \langle \overline{B}_0, ..., \overline{B}_{k-1}\rangle$. But $(f,\psi) = \overline{B}_k \notin \langle \overline{B}_0, ..., \overline{B}_{k-1}\rangle$, which shows that we cannot have the equality $(f,\psi) = (f,a_1)$.

Thus, we have proven the inequality $(f,\psi) < (f,a_1)$ and with it the proposition. □

9 The approximate roots and the embedding line theorem

We present the ideas of the proofs of the epimorphism theorem and of the embedding line theorem as they are given in [5].

It is in order to do these proofs that is developed in [5] the theory of Newton-Puiseux parameterizations and of local semigroups for elements of $\mathbf{C}((X))[Y]$, the *meromorphic curves*. This framework is more general than the one presented before, which concerned elements of $\mathbf{C}[[X]][Y]$, the *entire curves*. We have chosen to give before all the proofs for entire curves, first because they are in general used for the local study of plane curves and second in order to point out in this final section the differences between the two theories. A third type of curves, the *purely meromorphic* ones, will prove to be of the first importance.

Proof of the Epimorphism Theorem

We consider an *epimorphism* $\sigma : \mathbf{C}[X,Y] \to \mathbf{C}[T]$ and we note:

$$P(T) := \sigma(X), Q(T) := \sigma(Y),$$

$$N := d_T(P), M := d_T(Q).$$

We suppose that both degrees are non zero. The ideal $\ker(\sigma)$ is of height one in $\mathbf{C}[X,Y]$, so it is generated by one element. A privileged generator is given by:

$$F(X,Y) = \mathrm{Res}_T(P(T) - X, Q(T) - Y).$$

Here Res_T denotes the *resultant* of the two polynomials, seen as polynomials in the variable T.

From the determinant formula for the resultant, we obtain:

$$d_X(F) = M, d_Y(F) = N$$

and that F is monic if we see it as a polynomial in X or in Y.

Let us consider the set:

$$\Gamma(F) := \{d_T(G(P(T), Q(T))), G \in \mathbf{C}[X,Y] - (F)\}.$$

The set $\Gamma(F)$ is a sub-semigroup of $(\mathbf{N}, +)$. *The morphism σ is an epimorphism if and only if $T \in \mathrm{im}(\sigma)$, which is equivalent to $1 \in \Gamma(F)$, or $\Gamma(F) = \mathbf{N}$.*

Make now the change of variables: $x = X^{-1}, y = Y$. Take:

$$f(x,y) := F(x^{-1}, y) \in \mathbf{C}[x^{-1}][y].$$

The polynomial f is monic in y, of degree $d(f) = N$. By definition, the elements of $\mathbf{C}[x^{-1}][y]$ are called *purely meromorphic curves* (notation of [5]). As we have the embedding of rings $\mathbf{C}[x^{-1}] \hookrightarrow \mathbf{C}((x))$, we can also look at f as being a *meromorphic curve*, i.e. an element of $\mathbf{C}((x))[y]$. The theory of Newton-Puiseux expansions can be generalized to elements of $\mathbf{C}((x))[y]$, and so f has associated Newton-Puiseux series $\eta(x) \in \mathbf{C}((x^{\frac{1}{N}}))$ and Newton-Puiseux parameterizations of the form: $x = \tau^N, y = y(\tau) \in \mathbf{C}((\tau))$. It is important here that the exponent of τ in $x(\tau)$ is taken positive (see below).

From such a primitive Newton-Puiseux parameterization (see the definition in section 2), one can obtain a characteristic sequence of integers $(B_0, ..., B_G)$, where we put $B_0 = -N$ and the other B_i's are defined recursively as in the case of $\mathbf{C}[[x]][y]$, treated before. At the same time we define the sequence of greatest common divisors $(E_0, ..., E_G)$, which are elements of $\mathbf{N}^*$, and the sequences $(N_1, ..., N_G), (\overline{B}_0, ..., \overline{B}_G)$, as in section 2. Notice that $(B_0, ..., B_G)$ is again a strictly increasing sequence, but not necessarily $(\overline{B}_0, ..., \overline{B}_G)$.

If $\phi \in \mathbf{C}((x))[y]$, $f \not| \phi$, we define:

$$(f, \phi) := v_x(\mathrm{Res}_y(f, \phi)).$$

This construction extends the definition of the intersection number from $\mathbf{C}[[x]][y]$ to $\mathbf{C}((x))[y]$. It is again true with this definition that:

$$(f, \phi) = v_\tau(\phi(\tau^N, y(\tau))),$$

if $\tau \to (\tau^N, y(\tau))$ is a Newton-Puiseux parameterization of f (we understand here why it is important to take $x = \tau^N$ and not $x = \tau^{-N}$).

We define now:

$$\Gamma_{\mathbf{C}[x^{-1}]}(f) := \{(f, \phi), \phi \in \mathbf{C}[x^{-1}][y], f \not| \phi\}.$$

The set $\Gamma_{\mathbf{C}[x^{-1}]}(f)$ is a sub-semigroup of $(\mathbf{Z}, +)$. In fact we can say more. Indeed, if $\Phi(X,Y) = \phi(X^{-1}, Y) \in \mathbf{C}[X,Y]$, we have:

$$d_T(\Phi(P(T), Q(T))) = -(f, \phi),$$

which shows that:

$$\Gamma_{\mathbf{C}[x^{-1}]}(f) = -\Gamma(F).$$

We see in particular that the semigroup $\Gamma_{\mathbf{C}[x^{-1}]}(f)$ consists only of negative numbers.

As σ is an epimorphism, we get:

$$\Gamma_{\mathbf{C}[x^{-1}]}(f) = \mathbf{Z}_-.$$

Remark: If we consider intersections with elements of $\mathbf{C}((x))[y]$, we can define a second semigroup $\Gamma_{\mathbf{C}((x))}(f)$. We have obviously the inclusion $\Gamma_{\mathbf{C}[x^{-1}]} \subset \Gamma_{\mathbf{C}((x))}$, but in general this is not an equality.

Consider for example $f = y^2 - x^{-1}$. A Newton-Puiseux parameterization of f is $\tau \to (\tau^2, \tau^{-1})$. Take $\phi = y^2 - (x^{-1} - x) \in \mathbf{C}((x))[y] - \mathbf{C}[x^{-1}][y]$. Compute their intersection number: $(f, \phi) = v_\tau(\phi(\tau^2, \tau^{-1})) = 2 \notin \mathbf{Z}_- = \Gamma_{\mathbf{C}[x^{-1}]}(f)$.

Suppose now by contradiction that we are in a case where neither $N \mid M$ nor $M \mid N$. This implies easily that $B_1 = -M$. Indeed, $v_\tau(y) = (f, y) = = -d_T(Y(P(T), Q(T))) = -d_T(Q(T)) = -M$. Since $N \not| M$ we deduce by the definition of B_1 that $B_1 = v_\tau(y) = -M$.

Since $\Gamma_{\mathbf{C}[x^{-1}]}(f) = \mathbf{Z}_-$, we get in particular $-E_1 \in \Gamma_{\mathbf{C}[x^{-1}]}(f)$.

The contradiction is got in [5] from the properties:

$$B_0 = -N,\ B_1 = -M,\ -E_1 \in \Gamma_{\mathbf{C}[x^{-1}]}(f).$$

Here is the place in the proof where the approximate roots make their appearance. As in the case of $\mathbf{C}[[X]]$, from the sequences $(B_0, ..., B_G)$ and $(E_0, ..., E_G)$ one can define inductively a sequence $(\overline{B}_0, ..., \overline{B}_G)$ by the relations given in Proposition 4.2.

They are elements of $\Gamma_{\mathbf{C}((x))}(f)$, as they can be obtained by intersecting f with arbitrary semiroots of f, for example the ones got by truncating a Newton-Puiseux series of f (Proposition 6.6 generalizes to this context).

But, more important, $(\overline{B}_0, ..., \overline{B}_G)$ *are elements of* $\Gamma_{\mathbf{C}[x^{-1}]}(f)$. Indeed, $f_k = = \sqrt[E_k]{f} \in \mathbf{C}[x^{-1}][Y]$. Theorem 5.1 generalizes to this context and so: $(f, f_k) = = \overline{B}_{k+1}$, for $k \in \{0, ..., G\}$.

What is again true is that $(\overline{B}_0, ..., \overline{B}_G)$ form *a system of generators* of $\Gamma_{\mathbf{C}[x^{-1}]}(f)$. As $\Gamma_{\mathbf{C}[x^{-1}]}(f)$ is composed of negative numbers, we cannot speak any more about a minimal system of generators, as in Proposition 4.2. What remains true is that they are *a strict system of generators* (see [5]) in the following sense:

Proposition 9.1 Every element γ of $\Gamma_{\mathbf{C}[x^{-1}]}(f)$ can be expressed in a unique way as a sum:

$$\gamma = i_{-1}\overline{B}_0 + \cdots + i_{G-1}\overline{B}_G$$

where $i_{-1} \in \mathbf{N}$ and $0 \leq i_k < N_{k+1}$ for $k \in \{1, ..., G-1\}$.

To get this proposition, one proves first an analog of Corollary 5.4, obtained by replacing $\mathbf{C}[[X]]$ by $\mathbf{C}[x^{-1}]$. The proof follows the same path.

Now write the property $-E_1 \in \Gamma_{\mathbf{C}[x^{-1}]}(f)$ in terms of this strict sequence of generators:

$$-E_1 = i_{-1}\overline{B}_0 + \cdots + i_{G-1}\overline{B}_G.$$

Take $p := \max\{k \in \{0, ..., G\}, i_{k-1} \neq 0\}$. So:

$$E_1 = i_{-1} \mid \overline{B}_0 \mid + \cdots + i_{p-1} \mid \overline{B}_p \mid,$$

with $i_{p-1} \neq 0$.

If $p \geq 2$, we get: $E_{p-1} \mid (E_1 - i_{-1} \mid \overline{B}_0 \mid - \cdots - i_{p-2} \mid \overline{B}_{p-1} \mid)$ and so: $E_{p-1} \mid (i_{p-1} \mid \overline{B}_p \mid)$. Since $E_p = \gcd(E_{p-1}, \mid \overline{B}_p \mid)$, we get $N_p = \frac{E_{p-1}}{E_p} \mid i_{p-1}$, which contradicts the inequality $0 < i_{p-1} < N_p$.

So we obtain $p \leq 1$ and:

$$E_1 = i_{-1} \mid \overline{B}_0 \mid + i_0 \mid \overline{B}_1 \mid .$$

This implies: $1 = i_{-1} \frac{|\overline{B}_0|}{E_1} + i_0 \frac{|\overline{B}_1|}{E_1}$, which shows that $\frac{|\overline{B}_0|}{E_1} = 1$ or $\frac{|\overline{B}_1|}{E_1} = 1$. But, by the recursive relations giving the $\overline{B}_i$'s, $\overline{B}_0 = B_0 = -N$ and $\overline{B}_1 = B_1 = -M$, so:

$$\frac{N}{(M,N)} = 1 \text{ or } \frac{M}{(M,N)} = 1.$$

We get: $M \mid N$ or $N \mid M$, which contradicts our hypothesis. The theorem is proved. $\square$

Remark: One can also give a proof without using contradiction. In this case one cannot suppose from the beginning that $N \not| M$, and so it is not necessarily true that $B_1 = -M$. As one cannot hope to express in this case B_1 in terms of N and M, the preceding proof appears to get in trouble. This can be arranged if one modifies the definition of the characteristic sequence, taking for B_1 the minimal exponent appearing in $y(\tau)$, without imposing that it should not be divisible by N. This is the definition of characteristic sequence taken in a majority of Abhyankar's writings on curves, in particular [5], where the preceding proof is given with this modified definition.

Proof of the Embedding Line Theorem

If the epimorphism $\sigma : \mathbf{C}[X,Y] \to \mathbf{C}[T]$ is given by $X = P(T), Y = Q(T)$, put $N := d_T(P), M := d_T(Q)$ and write:

$$\begin{aligned} P(T) &= \alpha_0 T^N + \alpha_1 T^{N-1} + \cdots + \alpha_N, \\ Q(T) &= \beta_0 T^M + \beta_1 T^{M-1} + \cdots + \beta_M. \end{aligned}$$

(we consider here that $d_T(0) = 0$).

Suppose one of the degrees M, N is zero, for example $M = 0$. Then: $Q(T) = = \beta_0 \in \mathbf{C}$.

For all $G \in \mathbf{C}[X,Y]$, $d_T(G(P(T), Q(T)) \in N\mathbf{N}$. If σ is an epimorphism, there exists such a G with $d_T(G(P(T), Q(T)) = 1$, and this implies $N = 1$. So:

$$\begin{cases} P(T) = \alpha_0 T + \alpha_1, \ \alpha_0 \neq 0 \\ Q(T) = \beta_0 \end{cases} .$$

Consider the isomorphism of C-algebras $\sigma_1 : \mathbf{C}[U,V] \to \mathbf{C}[X,Y]$, given by:

$$\begin{cases} U = \frac{1}{\alpha_0} X - \frac{\alpha_1}{\alpha_0} \\ V = Y - \beta_0 \end{cases} .$$

Then $\sigma \circ \sigma_1 : \mathbf{C}[U,V] \to \mathbf{C}[T]$ is given by:

$$\begin{cases} U = T \\ V = 0 \end{cases}$$

and the theorem is proved in this case.

Suppose now that $M \geq 1, N \geq 1$. *By the epimorphism theorem*, $M \mid N$ or $N \mid M$. Suppose for example that $M \mid N$. Consider the isomorphism of $\mathbf{C}$-algebras $\sigma_1 : \mathbf{C}[U,V] \to \mathbf{C}[X,Y]$ given by:

$$\begin{cases} U = X - \alpha_0 \beta_0^{-\frac{N}{M}} Y^{\frac{N}{M}} \\ V = Y \end{cases}.$$

Then $\sigma \circ \sigma_1$ is given by:

$$\begin{cases} U = P(T) - \alpha_0 \beta_0^{-\frac{N}{M}} Q(T)^{\frac{N}{M}} \\ V = Q(T) \end{cases}.$$

We have: $d_T(P(T) - \alpha_0 \beta_0^{-\frac{N}{M}} Q(T)^{\frac{N}{M}}) < d_T(P(T))$ and so in the new coordinates (U,V), the sum of the degrees of the polynomials giving the embedding of the line in the plane is strictly less than in the coordinates (X,Y).

Repeating this process a finite number of times, we see that we arrive at the situation where one of the polynomials is a constant, the case first treated. This proves the theorem. $\square$

References

[1] Abhyankar, S.S. *Inversion and Invariance of Characteristic Pairs.* American Journal of Maths **89** (1967), 363-372.

[2] Abhyankar, S.S., Moh, T. *Newton-Puiseux Expansion and Generalized Tschirnhausen Transformation.* J. Reine Angew. Math. **260** (1973), 47-83; **261** (1973), 29-54.

[3] Abhyankar, S.S., Moh, T. *Embeddings of the Line in the Plane.* Ibid. **276** (1975), 148-166.

[4] Abhyankar, S.S. *Approximate Roots of Polynomials and Special Cases of the Epimorphism Theorem.* Preprint Purdue Univ. 1975.

[5] Abhyankar, S.S. *Expansion Techniques in Algebraic Geometry.* Tata Instit. Fund. Research, Bombay, 1977.

[6] Abhyankar, S.S. *On the Semigroup of a Meromorphic Curve (Part I).* International Symposium on Algebraic Geometry, Kyoto 1977(249-414), Kinokuniya Book-Store Co. Ltd. 1978.

[7] Abhyankar, S.S. *What is the Difference between a Parabola and a Hyperbola?* The Mathematical Intelligencer, vol.**10**, no.4 (1988).

[8] Abhyankar, S.S. *Irreducibility Criterion for Germs of Analytic Functions of Two Complex Variables.* Advances in Mathematics **74** (1989), 190-257.

[9] Abhyankar, S.S. *Algebraic Geometry for Scientists and Engineers.* Math. Surveys and Monographs, vol.35, AMS, 1990.

[10] Assi, A. *Deux remarques sur les racines approchées d'Abhyankar-Moh.* C. R. Acad. Sci. Paris, Ser. I **319** (1994), no.11, 1191-1196.

[11] Assi, A. *Meromorphic Plane Curves.* Math. Zeitschrift 230 (1999), 165-183.

[12] A'Campo, N., Oka, M. *Geometry of Plane Curves via Tschirnhausen Resolution Tower.* Osaka J. Math. **33** (1996), 1003-1033.

[13] Bourbaki, N. *Eléments de mathématiques. Algèbre, Livre II, 4: Polynômes et fractions rationnelles.* Deuxième édition, Hermann (1959).

[14] Brieskorn, E., Knörrer, H. *Plane Algebraic Curves.* Birkhäuser (1986), translation of the German Edition (1981).

[15] Campillo, A. *Algebroid Curves in Positive Characteristic.* LNM 813, Springer-Verlag (1980).

[16] Campillo, A., Piltant, O., Reguera-López, A.J. *Cones of Curves and of Line Bundles on Surfaces Associated with Curves Having one Place at Infinity.* Proc. London Math. Soc. (3) **84** (2002) no.3, 559-580.

[17] Chang, H-C., Wang, L-C. *An Intersection Theoretical Proof of the Embedding Line Theorem.* J. Algebra **161** (1993), 467-479.

[18] Coolidge, J.L. *A Treatise on Algebraic Plane Curves.* Oxford, 1931.

[19] Cossart, V., Moreno Socías, G. *Racines approchées, suites génératrices, suffisance des jets.* In preparation.

[20] Enriques, F., Chisini, O. *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche.* Zanichelli, 1915-1924.

[21] García Barroso, E. *Invariants des singularités de courbes planes et courbure des fibres de Milnor.* Thèse, Univ. de La Laguna, Tenerife (Espagne), LMENS-96-35, ENS, 1996.

[22] Goldin, R., Teissier, B. *Resolving Singularities of Plane Analytic Branches with One Toric Morphism.* In *Resolution of Singularities, A Research Textbook in Tribute to Oscar Zariski*, Birkhaüser, Progress in Math. No. 181, 2000, 315-340.

[23] González Pérez, P.D. *Quasi-Ordinary Singularities via Toric Geometry.* PhD-thesis, Univ. de La Laguna, Tenerife (Spain), sept.2000.

[24] Gwoździewicz, J., Płoski, A. *On the Merle Formula for Polar Invariants.* Bull. Soc. Sciences et lettres Łódź, vol.**XLI**, 7 (1991), 61-67.

[25] Gwoździewicz, J., Płoski, A. *On the Approximate Roots of Polynomials.* Annales Polonici Mathematici LX3 (1995), 199-210.

[26] Halphen, G.H., *Etude sur les points singuliers.* Appendix to Salmon, G. *Traité de géométrie analytique.* Gauthier-Villars, 1884.

[27] Hartshorne, R. *Algebraic Geometry.* Springer-Verlag, 1977.

[28] Kaplanski, I. *The Early Work of Saunders Mac Lane on Valuations and Fields.* In *Saunders Mac Lane Selected Papers.* Kaplansky, I. editor, Springer-Verlag, 1979, 519-524.

[29] Lejeune-Jalabert, M. *Sur l'équivalence des singularités des courbes algébroïdes planes (coefficients de Newton).* In *Introduction à la théorie des singularités I. Singularités et monodromie.* Lê, D.T. editor, Travaux en cours, Hermann, 1988, 49-125.

[30] Lejeune-Jalabert, M. *Contributions à l'étude des singularités du point de vue du polygone de Newton.* Thèse, Paris VII (1973).

[31] Lê, D.T., Michel, F., Weber, C. *Sur le comportement des polaires associées aux germes de courbes planes.* Compositio Mathematica **72** (1989), 87-113.

[32] MacLane, S. *A Construction for Absolute Values in Polynomial Rings.* Trans. Amer. Math. Soc. **40** (1936), 363-395.

[33] MacLane, S. *A Construction for Prime Ideals as Absolute Values of an Algebraic Field.* Duke Math. J. **2** (1936), 492-510.

[34] Merle, M. *Invariants polaires des courbes planes.* Inventiones Math. **41** (1977), 103-111.

[35] Moh, T.T. *On the Concept of Approximate Roots for Algebra.* J. Algebra **65** (1980), 347-360.

[36] Moh, T.T. *On Two Fundamental Theorems for the Concept of Approximate Roots.* J. Math. Soc. Japan **34** (1982), 637-652.

[37] Mumford, D. *Algebraic Geometry I, Complex Projective Varieties.* Grundlehren der math. Wissenschaften 221, Springer-Verlag, 1976.

[38] Noether, M. *Les combinaisons caractéristiques dans la transformation d'un point singulier.* Rend. Circ. Mat. Palermo **IV** (1890), 89-108, 300-301.

[39] Pinkham, H. *Courbes planes ayant une seule place à l'infini.* Sem. sur les singularités des surfaces, Ecole Polytechnique (1977).

[40] Russell, P. *Hamburger-Noether Expansions and Approximate Roots of Polynomials.* Manuscr. Math. **31** (1980), 25-95.

[41] Smith, H.J.S. *On the Higher Singularities of Plane Curves.* Proc. London Math. Soc. VI (1875), 153-182.

[42] Spivakovsky, M. *Valuations in Function Fields of Surfaces.* American Journal of Maths. **112** (1990), 107-156.

[43] Spivakovsky, M. *Resolución de singularidades y raíces aproximadas de Tschirnhausen.* Revista del Seminario Iberoamericano de Tordesillas, Fasc. **IV** (1997), 3-17.

[44] Teissier, B. *Introduction to Curve Singularities.* In *Singularity Theory.* Lê, D.T., Saito, M., Teissier, B. eds., World Scientific (1995), 866-893.

[45] Walker, R.J. *Algebraic Curves.* Princeton Univ. Press (1950).

[46] Zariski, O. *Algebraic Surfaces.* Springer-Verlag (1935); second supplemented edition (1971).

[47] Zariski, O. *The Connectedness Theorem for Birational Transformations.* In *A Symposium in Honor of S.Lefschetz.* Princeton, Princeton Univ. Press (1955).

[48] Zariski, O. *General Theory of Saturation and of Saturated Local Rings II.* Am. J. Math. **93** (1971), 872-964.

[49] Zariski, O. *Le problème des modules pour les branches planes.* Centre de Maths de l'X, 1973; réédition Hermann, 1986.