COMPOSITIO MATHEMATICA

DOMINIQUE DUVAL

Rational Puiseux expansions

Compositio Mathematica, tome 70, n° 2 (1989), p. 119-154

<http://www.numdam.org/item?id=CM_1989__70_2_119_0>

Compositio Mathematica **70**: 119–154, 1989.

Rational Puiseux expansions

DOMINIQUE DUVAL
Institut Fourier, B.P.74, F-38402 Saint-Martin-d'Hères Cedex, France

Received 7 January 1988; accepted in revised form 21 September 1988

Abstract. The aim of this paper is to define and study "rational" Puiseux expansions of a plane curve, and to describe a variant of Newton's algorithm to compute them. The rational Puiseux expansions of a curve give the same information as the classical ones, and in addition they give results of arithmetical nature about the curve. One major result is the easy determination of the residual field of the places of a curve over a non-algebraically closed field. This leads for example to a simple description of the real branches of curves defined over the real numbers.

My goal when I began studying Puiseux expansions simply was to implement Newton's algorithm on a computer algebra system. It happens that the rational Puiseux expansions are much easier to compute than the classical ones, mainly because less algebraic numbers are needed.

Introduction

Let $F(X, Y)$ denote a polynomial with coefficients in a field $\mathbb{K}$ of characteristic 0. Let us assume that F is monic in Y and *absolutely irreducible*, i.e., irreducible in $\bar{\mathbb{K}}[X, Y]$ for any algebraic closure $\bar{\mathbb{K}}$ of $\mathbb{K}$. It is a classical fact due to Newton [Ne], that the roots of F (considered as a Y-polynomial) are *Puiseux series* in X, i.e., formal series in $X^{1/e}$ (for some positive integer e) with coefficients in $\bar{\mathbb{K}}$.

For example, if $\mathbb{K}$ is the field $\mathbb{Q}$ of rational numbers, the roots of the Y-polynomial

$$F = (X^2 + Y^2)^3 - 4X^2Y^2$$

are 6 Puiseux series, beginning as follows:

$$\bar{y}_1 = \tfrac{1}{2}X^2 + \ldots, \qquad \bar{y}_2 = -\tfrac{1}{2}X^2 + \ldots,$$

$$\bar{y}_3 = \sqrt{2}X^{1/2} + \ldots, \qquad \bar{y}_4 = i\sqrt{2}X^{1/2} + \ldots,$$

$$\bar{y}_5 = -\sqrt{2}\,X^{1/2} + \ldots, \qquad \bar{y}_6 = -i\sqrt{2}X^{1/2} + \ldots.$$

In this case, the rational Puiseux expansions of F give a description of these roots by pairs of formal series with rational coefficients:

$\bar{y}_1$ by $(\tilde{x}_1 = T, \tilde{y}_1 = \frac{1}{2}T^2 + \ldots)$, $\bar{y}_2$ by $(\tilde{x}_2 = T, \tilde{y}_2 = -\frac{1}{2}T^2 + \ldots)$,

$\bar{y}_3$ and $\bar{y}_5$ by $(\tilde{x}_3 = \frac{1}{2}T^2, \tilde{y}_3 = T + \ldots)$,

$\bar{y}_4$ and $\bar{y}_6$ by $(\tilde{x}_4 = -\frac{1}{2}T^2, \tilde{y}_4 = T + \ldots)$.

In Section 1, the notion of a system of rational Puiseux expansions of F over $\mathbb{K}$ is defined, and it is proved that it easily gives the classical Puiseux expansions of F. These rational Puiseux expansions of F correspond *bijectively* to the *branches* of the plane curve of equation $F(x, y) = 0$ which pass through a point $(0, \beta)$ of the curve, i.e. to the *places* of the field $\bar{\mathbb{K}}(X)[Y]/(F(X, Y))$ which lie above the place $\mathfrak{p}_0$ of $\bar{\mathbb{K}}(X)$ corresponding to $0 \in \bar{\mathbb{K}}$. But the existence of systems of rational Puiseux expansions of F over $\mathbb{K}$ is not proved in this section.

In the two following sections, we show that rational Puiseux expansions give more information than the classical ones:

Complete factorization of F as a Y-polynomial is obtained over any algebraic closure $\overline{\bar{\mathbb{K}}((X))}$ of $\bar{\mathbb{K}}((X))$, and over $\bar{\mathbb{K}}((X))$, from classical Puiseux expansions of F. It is proved in Section 2 that from rational Puiseux expansions of F is got complete factorization of F over $\overline{\bar{\mathbb{K}}((X))}$, $\bar{\mathbb{K}}((X))$, *and* $\mathbb{K}((X))$.

In section 3 are considered the places of $\bar{\mathbb{K}}(X)[Y]/(F(X, Y))$. We have yet noticed that they correspond bijectively to the rational Puiseux expansions of F. In addition,

- two such places are *conjugated* over $\mathbb{K}$ if and only if the corresponding rational Puiseux expansions are conjugated over $\mathbb{K}$, and thus the places of the field $\mathbb{K}(X)[Y]/(F(X, Y))$ correspond bijectively to the conjugacy classes over $\mathbb{K}$ of the rational Puiseux expansions of F;
- the *ramification index* of a place of either $\bar{\mathbb{K}}(X)[Y]/(F(X, Y))$ or $\mathbb{K}(X)[Y]/(F(X, Y))$ is obtained as easily as in the classical case;
- and the *residual field* of a place of $\mathbb{K}(X)[Y]/(F(X, Y))$ is, up to $\mathbb{K}$-isomorphism, the extension field of $\mathbb{K}$ that is generated by the coefficients of any of the corresponding rational Puiseux expansions.

In the example above, the curve

$$(5x^2 + y^2)^3 - 4x^2y^2 = 0$$

has 4 branches at (0, 0) over $\bar{\mathbb{Q}}$, or over $\mathbb{C}$. Two of them are unramified, the two others have ramification index 2, and each branch corresponds to

exactly one place over $\mathbb{Q}$, with residual field $\mathbb{Q}$, since all coefficients are rational.

In Section 4 is described a variant of Newton's algorithm for computing Puiseux expansions, and it is proved that this "rational" Newton's algorithm computes a system of rational Puiseux expansions of F over $\mathbb{K}$, thereby proving its existence. In addition, this rational algorithm is cheaper than the classical one because the coefficients of the series are in a smaller extension field of $\mathbb{K}$.

The implementation of the rational Newton algorithm has been performed on the computer algebra system Reduce, using the D5 method (cf. [D–D]) to handle algebraic numbers. This method does not use any factorization algorithm, and actually no such algorithm is needed as long as one asks only for results over $\bar{\mathbb{K}}$. For results over $\mathbb{K}$, factorization algorithms may be needed (for example when $\mathbb{K} = \mathbb{Q}$), but Sturm sequences are sufficient when $\mathbb{K} = \mathbb{R}$. These points are detailed on examples in section 4, too.

In Section 5, we prove that the number of elementary operations over $\mathbb{K}$ that are needed for the computation of a system of rational Puiseux expansions of F is "polynomial", when the D5 method is used.

Basic references are: Walker [Wa] for parameterizations and classical Puiseux expansions, Fulton [Fu] for a more geometric point of view, and Chevalley [Ch] for arithmetical points.

Contents

1. Classical and rational Puiseux expansions

From now on, $\mathbb{K}$ denotes a field of zero characteristics, $\bar{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, $F(X, Y)$ a bivariate polynomial with coefficients in $\mathbb{K}$, monic in Y, irreducible in $\bar{\mathbb{K}}[X, Y]$, and M (resp. N) the degree of F in X (resp. in Y), with $N > 0$. Actually, these assumptions may be much weakened, as explained in the conclusion.

Generally, F will be considered as a Y-polynomial with coefficients in $\mathbb{K}[X]$

$$F(X, Y) = \sum_{i=0}^{N} a_i(X)Y^i \quad \text{with} \quad a_i(X) = \sum_{j=0}^{M} a_{i,j}X^j$$

where the $a_i(X)$'s are in $\mathbb{K}[X]$, the $a_{i,j}$'s in $\mathbb{K}$, and by assumption $a_N(X) = 1$.

As usual, the power series field in one variable T and with coefficients in some field $\mathbb{L}$ is denoted by $\mathbb{L}((T))$. And the domain formed by the elements of $\mathbb{L}((T))$ of non-negative T-order by $\mathbb{L}[[T]]$. For every positive integer q, a root $X^{1/q}$ of X of order q is chosen in an algebraic closure of $\mathbb{K}(X)$, in such a way that $(X^{1/q_1q_2})^{q_2} = X^{1/q_1}$.

DEFINITION: The *Puiseux series field* $\mathfrak{K}$ over $\bar{\mathbb{K}}$ is the union of all the fields $\bar{\mathbb{K}}((X^{1/q}))$. It is an algebraically closed field, by Puiseux theorem [Wa, 4 *thm* 3.1.].

DEFINITION: The (*classical*) *Puiseux expansions* of $F(X, Y)$ are the roots of the Y-polynomial F in the field $\mathfrak{K}$.

Since F is irreducible in $\bar{\mathbb{K}}(X)[Y]$ (by Gauss' lemma) and since $\mathfrak{K}$ is algebraically closed and of characteristic 0, the Y-polynomial F has N distinct classical Puiseux expansions. They are denoted

$$\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_N \quad \text{with} \quad \bar{y}_k = \sum_{h=1}^{+\infty} \alpha_{k,h} X^{n_{k,h}/\bar{e}_k}.$$

It will always be assumed that each $\bar{e}_k$ is as small as possible, i.e. that $\bar{e}_k$ and the $n_{k,h}$ (for $h \geqslant 1$) have no common factor greater than 1. This $\bar{e}_k$ is called the *ramification index* of the series $\bar{y}_k$. In addition, $\bar{y}_k$ is in $\bar{\mathbb{K}}[[X^{1/\bar{e}_k}]]$ because F has been assumed monic in Y.

Let us now recall the definition of the parametrizations of the plane affine curve C of equation $F(x, y) = 0$ over $\bar{\mathbb{K}}$, following Walker [Wa, 4-2].

DEFINITION: A *parametrization* of the curve C is a pair $(\tilde{x}, \tilde{y})$ of elements of $\bar{\mathbb{K}}[[T]]$ for some new variable T, such that $F(\tilde{x}, \tilde{y}) = 0$ in $\bar{\mathbb{K}}[[T]]$, and $\tilde{x}$ and $\tilde{y}$ are not both in $\bar{\mathbb{K}}$.

The *center* of the parametrization $(\tilde{x}, \tilde{y})$ is the point (x_0, y_0) of the affine plane such that x_0 (*resp.* y_0) is the constant term of the series $\tilde{x}$ (*resp.* $\tilde{y}$). It is a point of the curve C. The parametrization $(\tilde{x}, \tilde{y})$ is *irreducible* if there is no integer $k > 1$ such that both $\tilde{x}$ and $\tilde{y}$ are in $\bar{\mathbb{K}}[[T^k]]$. And two parametrizations $(\tilde{x}_1, \tilde{y}_1)$ and $(\tilde{x}_2, \tilde{y}_2)$ are *equivalent* if there is some

$z \in \bar{\mathbb{K}}[[T]]$, of T-order 1, such that $\tilde{x}_2(T) = \tilde{x}_1(z(T))$ and $\tilde{y}_2(T) = \tilde{y}_1(z(T))$. If such is the case they have the same center, but the reciprocal is false.

In addition, the *coefficient field* of $(\tilde{x}, \tilde{y})$ over $\mathbb{K}$ is the extension field of $\mathbb{K}$ generated by all the coefficients of the series $\tilde{x}$ and $\tilde{y}$. It is a subfield of $\bar{\mathbb{K}}$.

A *branch* of C is then defined as an equivalence class of irreducible parametrizations of C, and its center as the common center of the parametrizations of the class. We say that a branch of C *lies above* a point x_0 of $\bar{\mathbb{K}}$ if the center of the branch is (x_0, y_0) for some y_0 in $\bar{\mathbb{K}}$.

For each classical Puiseux expansion

$$\bar{y}_k = \sum_{h=1}^{+\infty} \alpha_{k,h} X^{n_{k,h}/\bar{e}_k}$$

of F, let

$$u_k(T) = T^{\bar{e}_k} \text{ and } v_k(T) = \sum_{h=1}^{+\infty} \alpha_{k,h} T^{n_{k,h}}.$$

Since $\bar{y}_k = v_k(X^{1/\bar{e}_k})$, it follows that $F(u_k(X^{1/\bar{e}_k}), v_k(X^{1/\bar{e}_k})) = F(X, \bar{y}_k) = 0$ in $\mathfrak{R}$. The pair $(u_k(T), v_k(T))$ is thus a parametrization of C, which is irreducible because $\bar{e}_k$ has been chosen minimal. We say that $(u_k(T), v_k(T))$ is the parametrization of C *corresponding* to the Puiseux expansion $\bar{y}_k$. And that two classical Puiseux expansions of F are *equivalent* if their corresponding parametrizations are equivalent.

If $\bar{\zeta}_k$ denotes a primitive root of unity of order $\bar{e}_k$ in $\bar{\mathbb{K}}$, the classical Puiseux expansions of F that are equivalent to $\bar{y}_k$ are the

$$v_k(\bar{\zeta}_k^i X^{1/\bar{e}_k}) \text{ for } i = 0, 1, \ldots, \bar{e}_k - 1 \text{ or } i = 1, 2, \ldots, \bar{e}_k.$$

All of them have the same ramification index $\bar{e}_k$.

Thus is obtained a partition of the set $\{\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_N\}$ in equivalence classes, which are in one-to-one correspondence with the branches of C lying above 0. Let $\bar{g}$ be the number of these classes, and assume that the numbering of the Puiseux expansions is such that $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_{\bar{g}}$ are in different classes. It follows that

$$N = \sum_{k=1}^{\bar{g}} \bar{e}_k.$$

DEFINITION: As above, let $\bar{g}$ denote the number of branches of C lying above 0. A *system of rational Puiseux expansions of* F over $\mathbb{K}$ is a set

$$\{(\tilde{x}_1, \tilde{y}_1), (\tilde{x}_2, \tilde{y}_2), \ldots, (\tilde{x}_{\bar{g}}, \tilde{y}_{\bar{g}})\}$$

of $\bar{g}$ pairwise non-equivalent irreducible parametrizations of C, which is invariant under the action of the Galois group $\mathcal{G}$ of $\bar{\mathbb{K}}$ over $\mathbb{K}$, and such that, for each k, $\tilde{x}_k$ is a monomial $\lambda_k T^{e_k}$ with $e_k > 0$ and $\lambda_k \neq 0$.

The fact that such systems exist will be proved in section 4. For a given F, there are different systems of rational Puiseux expansions of F: for example if $F = Y^2 - X$ there are

$$\{(T^2, T)\} \text{ and } \{(T^2, -T)\}.$$

It must be noticed that the parametrizations $(u_k(T), v_k(T))$ (for $1 \leqslant k \leqslant \bar{g}$) defined above from classical Puiseux expansions usually do *not* form a system of rational Puiseux expansions of F, because they do not form an invariant set under the action of $\mathcal{G}$:

In the example of the introduction, the only classical Puiseux expansion equivalent to

$$(u_3(T), v_3(T)) = (T^2, \sqrt{2}T + \ldots)$$

$$\text{is } (u_5(T), v_5(T)) = (T^2, -\sqrt{2}T + \ldots),$$

which is conjugated to (u_3, v_3) over $\mathbb{K} = \mathbb{Q}$.

On the contrary, it is very easy to determine the classical Puiseux expansions of F from a system of rational Puiseux expansions: Let

$$\left(\tilde{x}_k = \lambda_k T^{e_k}, \tilde{y}_k = \sum_{h=1}^{+\infty} \alpha_{k,h} T^{n_{k,h}}\right)$$

(for $1 \leqslant k \leqslant \bar{g}$) be a system of rational Puiseux expansions of F over $\mathbb{K}$, let ζ_k denote a primitive root of unity of order e_k in $\bar{\mathbb{K}}$, and λ_k^{-1/e_k} a root of order e_k of λ_k^{-1} in $\bar{\mathbb{K}}$ for each k. Then:

THEOREM 1: *The classical Puiseux expansions of F are the series*

$$\tilde{y}_k(\zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k})$$

for $k = 1, 2, \ldots, \bar{g}$ *and* $i = 1, 2, \ldots, e_k$.

The ramification index of $\tilde{y}_k(\zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k})$ *is exactly* e_k.

Proof: Consider some k between 1 and $\bar{g}$. Then

$$0 = F(\tilde{x}_k, \tilde{y}_k) = F\left(\lambda_k T^{e_k}, \sum_{h=1}^{+\infty} \alpha_{k,h} T^{n_{k,h}}\right) \text{ in } \bar{\mathbb{K}}((T)).$$

Now if we set $X = \lambda T^e$, i.e., $T = \zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k}$ for some i, we get

$$F\left(X, \sum_{h=1}^{+\infty} \alpha_{k,h} (\zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k})\right) = 0 \text{ in } \mathfrak{R}.$$

This proves that each of the

$$\tilde{y}_k(\zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k})$$

for $1 \leqslant k \leqslant \bar{g}$ and $1 \leqslant i \leqslant e_k$ is a classical Puiseux expansion of F.

They are mutually distinct: for different k because the rational Puiseux expansions are pairwise non-equivalent, and for the same k and different i because the rational Puiseux expansions are irreducible as parametrizations of C. For the same reason, e_k is the ramification index of $\tilde{y}_k(\zeta_k^i \lambda_k^{-1/e_k} X^{1/e_k})$ for any i.

The fact that every classical Puiseux expansion of F is obtained in this way now comes from the identity $N = \Sigma_{k=1}^{\bar{g}} e_k$, and thus theorem 1 is proved.

Now, let g denote the number of $\mathscr{G}$-orbits in a given system of rational Puiseux expansions of F over $\mathbb{K}$, and suppose that $(\tilde{x}_k, \tilde{y}_k)$ are in different orbits for $1 \leqslant k \leqslant g$. For each k from 1 to g, let us denote by $\mathbb{L}_k$ the coefficient field of $(\tilde{x}_k, \tilde{y}_k)$. Because of the $\mathscr{G}$-invariance property of the set $\{(\tilde{x}_k, \tilde{y}_k)\}_{1 \leqslant k \leqslant \bar{g}}$, the field $\mathbb{L}_k$ is a finite extension of $\mathbb{K}$. Let f_k denote the dimension of $\mathbb{L}_k$ over $\mathbb{K}$, i.e., the number of k' in $\{1, 2, \ldots, \bar{g}\}$ such that $(\tilde{x}_{k'}, \tilde{y}_{k'})$ is in the $\mathscr{G}$-orbit of $(\tilde{x}_k, \tilde{y}_k)$, and let $\{\sigma_1, \sigma_2, \ldots, \sigma_{f_k}\}$ be the set of $\mathbb{K}$-isomorphisms from $\mathbb{L}_k$ into $\bar{\mathbb{K}}$. For every j from 1 to f_k, let $\lambda_{k,j} = \sigma_j(\lambda_k)$ and $\tilde{y}_{k,j} = \sigma_j(\tilde{y}_k) = \Sigma_{h=1}^{+\infty} \sigma_j(\alpha_{k,h}) T^{n_{k,h}}$. By definition, the given system of rational Puiseux expansions of F over $\mathbb{K}$ is made of the

$$(\lambda_{k,j} T^{e_k}, \tilde{y}_{k,j}(T))$$

for $1 \leqslant k \leqslant g$ and $1 \leqslant j \leqslant f_k$, and theorem 1 can be expressed as follows:

THEOREM 1 *bis*: *The classical Puiseux expansions of F are the*

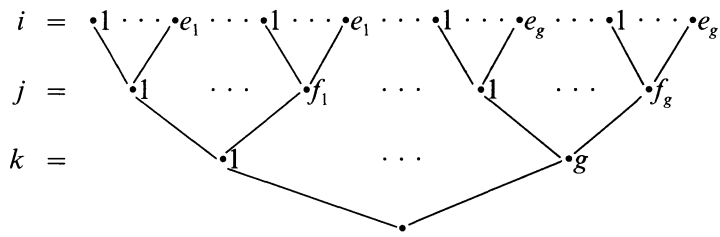
$$\tilde{y}_{k,j}(\zeta_k^i \lambda_{k,j}^{-1/e_k} X^{1/e_k})$$

for $1 \leqslant k \leqslant g$, $1 \leqslant j \leqslant f_k$, *and* $1 \leqslant i \leqslant e_k$. *The ramification index of the expansion above is* e_k.

It follows that $g = \Sigma_{k=1}^{g} f_k$ and that

$$N = \sum_{k=1}^{g} e_k f_k.$$

In the following diagram, the first line corresponds to the N classical Puiseux expansions of F, the second line to their $\tilde{g}$ equivalence classes, or to a system of rational Puiseux expansions of F over $\mathbb{K}$, and the third line to the g orbits of this system under the action of $\mathcal{G}$:



2. Factorization of F over series fields

By definition of the classical Puiseux expansions of F, the factorization of F in $\mathfrak{K}[Y]$ is

$$F(X, Y) = \prod_{k=1}^{N} (Y - \bar{y}_k) = \prod_{k=1}^{N} (Y - v_k(X^{1/\bar{e}_k})).$$

And if the classical Puiseux expansions are grouped according to equivalence, a refinement of the above factorization is obtained:

$$F(X, Y) = \prod_{k=1}^{\tilde{g}} \bar{F}_k(X, Y)$$

where

$$\bar{F}_k(X, Y) = \prod_{i=1}^{\bar{e}_k} (Y - v_k(\bar{\zeta}_k^i X^{1/\bar{e}_k})) \in \bar{\mathbb{K}}((X))[Y].$$

In addition, this factorization over $\bar{\mathbb{K}}((X))$ is *complete* in the sense that each $\bar{F}_k(X, Y)$ is irreducible in $\bar{\mathbb{K}}((X))[Y]$: If the *norm* in the field extension

$\bar{\mathbb{K}}((X^{1/\bar{e}_k}))/\bar{\mathbb{K}}((X))$ is extended to polynomials, then $\bar{F}_k(X, Y)$ is the norm of $(Y - \bar{y}_k)$, which is irreducible in $\bar{\mathbb{K}}((X^{1/\bar{e}_k}))[Y]$, and it follows that $\bar{F}_k(X, Y)$ is a power of some irreducible polynomial of $\bar{\mathbb{K}}((X))[Y]$ [Tr1, *thm* 2.1]. But $\bar{F}_k(X, Y)$ has distinct roots in $\mathfrak{K}$, and thus it is irreducible in $\bar{\mathbb{K}}((X))[Y]$.

REMARK: If some classical Puiseux expansion of F is "finite", say $\bar{y}_k \in \bar{\mathbb{K}}[X^{1/\bar{e}_k}]$, then $\bar{F}_k \in \bar{\mathbb{K}}[X, Y]$, and since F is absolutely irreducible it follows that $F = F_k$ and $\bar{g} = 1$.

Thus, complete factorization of F over $\mathfrak{K}$ and over $\bar{\mathbb{K}}((X))$ is obtained from the classical Puiseux expansions of F. The next result proves that it can also be obtained from a system of rational Puiseux expansions of F over $\mathbb{K}$, together with the complete factorization of F over $\mathbb{K}((X))$.

THEOREM 2: *With the notations of section 1, the complete factorization of F (as a Y-polynomial)* over the fields $\mathbb{K}((X))$, $\bar{\mathbb{K}}((X))$ and $\mathfrak{K}$, is given by:

$$F(X, Y) = \prod_{k=1}^{g} F_k(X, Y) \text{ in } \mathbb{K}((X))[Y],$$

$$F_k(X, Y) = \prod_{j=1}^{f_k} F_{k,j}(X, Y) \text{ in } \bar{\mathbb{K}}((X))[Y],$$

$$F_{k,j}(\lambda_{k,j}X, Y) = \prod_{i=1}^{e_k} (Y - \tilde{y}_{k,j}(\zeta_k^i X^{1/e_k})) \text{ in } \mathfrak{K}[Y].$$

REMARK: The last equality can also be written:

$$F_{k,j}(X, Y) = \prod_{i=1}^{e_k} (Y - \tilde{y}_{k,j}(\zeta_k^i \lambda_{k,j}^{-1/e_k} X^{1/e_k})).$$

Proof: Theorem 1 *bis* proves that the complete factorization of F over $\mathfrak{K}$ is

$$F(X, Y) = \prod_{k=1}^{g} \prod_{j=1}^{f_k} \prod_{i=1}^{e_k} (Y - \tilde{y}_{k,j}(\zeta_k^i \lambda_{k,j}^{-1/e_k} X^{1/e_k})).$$

But notations are such that a set of $\bar{g}$ non-equivalent classical Puiseux expansions of F is given by the $\tilde{y}_k(\lambda_{k,j}^{-1/e_k} X^{1/e_k})$ for $1 \leqslant k \leqslant g$ and $1 \leqslant j \leqslant f_k$, and thus the $F_{k,j}$'s for $1 \leqslant k \leqslant g$ and $1 \leqslant j \leqslant f_k$ are exactly

the $\bar{F}_k$'s for $1 \leqslant k \leqslant \bar{g}$. So, it has been proved above that the complete factorization of F over $\bar{\mathbb{K}}((X))$ is

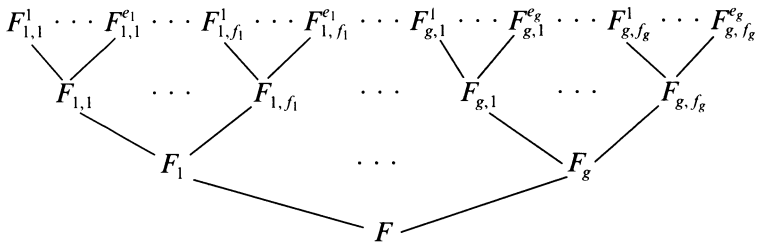
$$F(X, Y) = \prod_{k=1}^{g} \prod_{j=1}^{f_k} F_{k,j}(X, Y).$$

Now, for a given k between 1 and g, if σ_1 is the identity of Σ_k, then $F_k(X, Y)$ is the norm of $F_{k,\sigma_1}(X, Y)$ in the extension $\mathbb{L}_k((x))/\mathbb{K}((X))$. It follows, as above, that $F_k(X, Y)$ is a power of some irreducible polynomial of $\mathbb{K}((X))[Y]$, and that it is itself irreducible in $\mathbb{K}((X))[Y]$ since it has distinct roots in $\mathfrak{R}$. Thus the complete factorization of F over $\mathbb{K}((X))$ is

$$F(X, Y) = \prod_{k=1}^{g} F_k(X, Y)$$

and theorem 2 is proved.

Those different factorizations of F can be visualized by the following diagram, where $F_{k,j}^i = Y - \tilde{y}_{k,j}(\zeta_k^i \lambda_{k,j}^{-1/e_k} X^{1/e_k})$, and where the first line corresponds to the factorization in $\mathfrak{R}[Y]$, the second line over $\bar{\mathbb{K}}((X))[Y]$, and the third line over $\mathbb{K}((X))[Y]$:



3. The places of $\bar{\mathbb{K}}(C)$ and of $\mathbb{K}(C)$

Since F is irreducible over $\bar{\mathbb{K}}$, the quotient $\bar{\mathbb{K}}(X)[Y]/(F(X, Y))$ is an extension field of $\bar{\mathbb{K}}(X)$ of degree N, that will be denoted by $\bar{\mathbb{K}}(C)$. This notation comes from the interpretation of $\bar{\mathbb{K}}(C)$ as the function field of the plane curve C of equation $F(x, y) = 0$. The extension $\bar{\mathbb{K}}(C)/\bar{\mathbb{K}}(X)$ corresponds to the projection of C on the "x-axis" [Fu, 6-3]. In the same way, since F is also irreducible over $\mathbb{K}$, the quotient $\mathbb{K}(X)[Y]/(F(X, Y))$ is a field $\mathbb{K}(C)$, extension of $\mathbb{K}(X)$ of degree N.

The branches of C have been defined in section 1 as the equivalence classes of irreducible parametrizations of C. To each parametrization $(\tilde{x}, \tilde{y})$ of C are associated two subsets $\bar{\mathcal{O}}$ and $\bar{\mathfrak{P}}$ of $\bar{\mathbb{K}}(C)$, such that $\bar{\mathcal{O}}$ is a ring and $\bar{\mathfrak{P}}$ a maximal ideal of $\bar{\mathcal{O}}$. By definition, $\bar{\mathfrak{P}}$ is a *place* of $\bar{\mathbb{K}}(C)$ and $\bar{\mathcal{O}}$ is *the ring of* $\bar{\mathfrak{P}}$. They may be defined as follows:

Consider the $\bar{\mathbb{K}}$-algebra homomorphism

$$\varphi\colon \bar{\mathbb{K}}[X, Y] \to \bar{\mathbb{K}}[[T]]\colon G \mapsto G(\tilde{x}, \tilde{y}).$$

Notice that $Ker(\varphi)$ contains no non-zero element of $\bar{\mathbb{K}}[X]$: If $\varphi(G) = 0$ with $G \in \bar{\mathbb{K}}[X]$ and $G \neq 0$, then $\tilde{x}$ would be a root of G in $\bar{\mathbb{K}}$, and $\tilde{y}$ would be a root of the univariate polynomial $F(\tilde{x}, Y)$ of $\bar{\mathbb{K}}[Y]$ of positive degree N. But then $\tilde{y}$ would be in $\bar{\mathbb{K}}$ too, which contradicts the definition of a parametrization.

It is thus possible to extend φ to a $\bar{\mathbb{K}}$-algebra homomorphism still denoted by φ:

$$\varphi\colon \bar{\mathbb{K}}(X)[Y] \to \bar{\mathbb{K}}((T)).$$

Since $(\tilde{x}, \tilde{y})$ is a parametrization of C, the polynomial F is contained in $Ker(\varphi)$. And since F is irreducible in the principle ring $\bar{\mathbb{K}}(X)[Y]$, we get $Ker(\varphi) = (F)$.

Thus is obtained an injective $\bar{\mathbb{K}}$-algebra homomorphism

$$\Phi\colon \bar{\mathbb{K}}(C) = \bar{\mathbb{K}}(X)[Y]/(F) \to \bar{\mathbb{K}}((T)).$$

Now, $\bar{\mathcal{O}}$ and $\bar{\mathfrak{P}}$ are defined by

$$\bar{\mathcal{O}} = \Phi^{-1}(\bar{\mathbb{K}}[[T]]) \text{ and } \bar{\mathfrak{P}} = \Phi^{-1}(T\bar{\mathbb{K}}[[T]]).$$

Two parametrizations of C gives the same $\bar{\mathcal{O}}$ and $\bar{\mathfrak{P}}$ if and only if they are equivalent, which proves that each branch of C corresponds to exactly one place of $\bar{\mathbb{K}}(C)$.

Actually, we do not get in this way all places of $\bar{\mathbb{K}}(C)$. We should have, in addition, considered parametrizations centered at the "points at infinity" of C in order to get all places of $\bar{\mathbb{K}}(C)$. It does not matter here, because we are only interested in the places of $\bar{\mathbb{K}}(C)$ that "lie above" $\mathfrak{p}_0$ (*cf.* below), and all of them are finite since F is monic in Y.

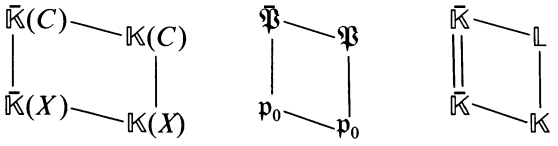
In the case of $F = Y$, we have $\bar{\mathbb{K}}(C) = \bar{\mathbb{K}}(X)$. The curve C is the x-axis, and has only one branch lying above 0. One of its parametrizations is $(\tilde{x}_0, \tilde{y}_0) = (T, 0)$, and the corresponding ring and place are respectively $\bar{\mathbb{K}}[X]$ and $\bar{\mathfrak{p}}_0 = X\bar{\mathbb{K}}[X]$.

In the general case, a place $\bar{\mathfrak{P}}$ of $\bar{\mathbb{K}}(C)$ *lies above* the place $\bar{\mathfrak{p}}_0$ of $\bar{\mathbb{K}}(X)$ if $\bar{\mathfrak{P}} \cap \bar{\mathbb{K}}[X] = \bar{\mathfrak{p}}_0$. Those places correspond to the branches of C lying above 0. We have seen that such a branch of C is the equivalence class of e classical Puiseux expansions of F, each with ramification index e. This integer e is called the *ramification index* of the corresponding place $\bar{\mathfrak{P}}$.

The *places* of $\mathbb{K}(C)$ are now defined as the intersections $\mathfrak{P} \cap \mathbb{K}(C)$ of the places of $\bar{\mathbb{K}}(C)$ with $\mathbb{K}(C)$. In this situation too, we say that $\mathfrak{P}$ *lies above* $\mathfrak{P} \cap \mathbb{K}(C)$. Let $\bar{\mathfrak{P}}_1$ and $\bar{\mathfrak{P}}_2$ be two places of $\bar{\mathbb{K}}(C)$ lying above the place $\bar{\mathfrak{p}}_0$ of $\bar{\mathbb{K}}(X)$. It is not easy to decide, from classical Puiseux expansions of F, whether $\bar{\mathfrak{P}}_1$ and $\bar{\mathfrak{P}}_2$ lie above the same place of $\mathbb{K}(C)$. But we shall see in theorem 3 that, on the contrary, it is very easily done from any system of rational Puiseux expansions of F over $\mathbb{K}$.

If $\mathfrak{P}$ is a place of $\mathbb{K}(C)$, $\bar{\mathfrak{P}}$ a place of $\bar{\mathbb{K}}(C)$ lying above $\mathfrak{P}$, and if $\mathcal{O} = \bar{\mathcal{O}} \cap \mathbb{K}(C)$ where $\bar{\mathcal{O}}$ is the ring of $\bar{\mathfrak{P}}$, then $\mathbb{L} = \mathcal{O}/\mathfrak{P}$ is a field. It is a finite extension of $\mathbb{K}$, called the *residual field* of $\mathfrak{P}$, and its degree f is the *residual degree* of $\mathfrak{P}$. This integer f is also equal to the number of places $\bar{\mathfrak{P}}$ of $\bar{\mathbb{K}}(C)$ lying above $\mathfrak{P}$. If $F = Y$, then $\mathfrak{p}_0 = X\mathbb{K}[X]$ is a place of $\mathbb{K}(X)$; the only place of $\bar{\mathbb{K}}(C)$ lying above $\mathfrak{p}_0$ is $\bar{\mathfrak{p}}_0$, and the residual field of $\mathfrak{p}_0$ is $\mathbb{K}$. Now, when $\mathfrak{P}$ is a place of $\mathbb{K}(C)$ lying above $\mathfrak{p}_0$, we shall see that $\mathbb{L}$ and f are easily obtained from a set of rational Puiseux expansions of F over $\mathbb{K}$, which is not true for classical Puiseux expansions.

fields of functions places residual fields



Let us denote by $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_{g^*}$, the places of $\mathbb{K}(C)$ lying above the place $\mathfrak{p}_0$ of $\mathbb{K}(X)$. For $1 \leqslant k \leqslant g^*$, let e_k^* be the ramification index, f_k^* the residual degree, and $\mathbb{L}_k^*$ the residual field of $\mathfrak{P}_k$. The integers e_k^* and f_k^* are related to N by the formula

$$N = \sum_{k=1}^{g^*} e_k^* f_k^*.$$

The following result proves that the *'s are useless:

THEOREM 3: For $k = 1, 2, \ldots, g$, *let* e_k, f_k and $\mathbb{L}_k$ *be defined as in section 2, from a set* $\{(\tilde{x}_k, \tilde{y}_k)\}_{1 \leqslant k \leqslant g}$ *of representatives of the* $\mathcal{G}$*-orbits in a system of rational Puiseux expansions of* F *over* $\mathbb{K}$.

For $k = 1, 2, \ldots, g^*$, *let* e_k^*, f_k^* *and* $\mathbb{L}_k^*$ *be defined as above, from the places* $\{\mathfrak{P}_k\}_{1 \leq k \leq g^*}$ *of* $\mathbb{K}(C)$ *lying above* $\mathfrak{p}_0$.

Then $g^* = g$, *and (up to reordering the places* $\mathfrak{P}_k$*)* $e_k^* = e_k, f_k^* = f_k$, *and* $\mathbb{L}_k^*$ *is* $\mathbb{K}$*-isomorphic to* $\mathbb{L}_k$ *for* $k = 1, 2, \ldots, g$.

Proof: (*using Chevalley's book* [Ch]).

It has been proved in theorem 2 that the complete factorization of F in $\mathbb{K}((X))[Y]$ is $F = \Pi_{k=1}^{g} F_k$. It follows, by the Chinese remainder theorem, that the $\mathbb{K}((X))$-algebras

$$\mathbb{K}((X))[Y]/(F) \quad \text{and} \quad \prod_{k=1}^{g} \mathbb{K}((X))[Y]/(F_k)$$

are isomorphic, and that each $\mathbb{K}((X))[Y]/(F_k)$ is a field.

On the other hand, $\mathbb{K}((X))[Y]/(F(X, Y))$ is equal to the $\mathfrak{p}_0$-adic completion $\mathbb{K}(C) \otimes_{\mathbb{K}(X)} \mathbb{K}((X))$ of $\mathbb{K}(C)$, it is thus isomorphic to the product of the $\mathfrak{P}_k$-adic completions of $\mathbb{K}(C)$ for $k = 1$ to g^*, which are fields.

This proves that $g^* = g$, and that the places $\mathfrak{P}_k$ can be numbered in such a way that $\mathbb{K}((X))[Y]/(F_k)$ is the $\mathfrak{P}_k$-adic completion of $\mathbb{K}(C)$.

The fact that F_k is the product of f_k irreducible factors of the same degree e_k in $\bar{\mathbb{K}}((X))[Y]$ proves that there are f_k places of $\bar{\mathbb{K}}(C)$ lying above $\mathfrak{P}_k$, each of them with ramification index e_k. This means that f_k is the residual degree of $\mathfrak{P}_k$ and e_k its ramification index, i.e. that $f_k^* = f_k$ and $e_k^* = e_k$.

It remains to prove that the coefficient field $\mathbb{L}_k$ of $(\tilde{x}_k, \tilde{y}_k)$ is $\mathbb{K}$-isomorphic to the residual field $\mathbb{L}_k^*$ of $\mathfrak{P}_k$. Since we have just proved that they both have the same degree over $\mathbb{K}$, we only have to get an injective $\mathbb{K}$-algebra homomorphism from $\mathbb{L}_k^*$ into $\mathbb{L}_k$. From now on, a $\mathbb{K}$-algebra homomorphism is always one that preserves 1. Thus, since $\mathbb{L}_k^*$ is a field, we only need a $\mathbb{K}$-algebra homomorphism from $\mathbb{L}_k^*$ in $\mathbb{L}_k$. This is given by the following lemma:

LEMMA: *Let* $\mathfrak{P}$ *be a place of* $\mathbb{K}(C)$ *and* $\mathbb{L}^*$ *its residual field. Let* $(\tilde{x}, \tilde{y})$ *be a parametrization of any place* $\mathfrak{P}$ *of* $\bar{\mathbb{K}}(C)$ *lying above* $\mathfrak{P}$, *and let* $\mathbb{L}$ *be the coefficient field of* $(\tilde{x}, \tilde{y})$.

Then there is a $\mathbb{K}$*-algebra homomorphism from* $\mathbb{L}^*$ *into* $\mathbb{L}$.

Proof: Let us come back to the $\bar{\mathbb{K}}$-algebra homomorphism

$$\varphi\colon \bar{\mathbb{K}}[X, Y] \to \bar{\mathbb{K}}[[T]]\colon G \mapsto G(\tilde{x}, \tilde{y}).$$

The restriction ψ of φ to $\mathbb{K}[X, Y]$ is a $\mathbb{K}$-algebra homomorphism with values in $\mathbb{L}[[T]]$. As for φ, it induces a $\mathbb{K}$-algebra homomorphism

$$\Psi\colon \mathbb{K}(C) \to \mathbb{L}((T)),$$

and if $\mathcal{O}$ is the ring of $\mathfrak{P}$ then $\Psi(\mathcal{O}) \subset \mathbb{L}[[T]]$.

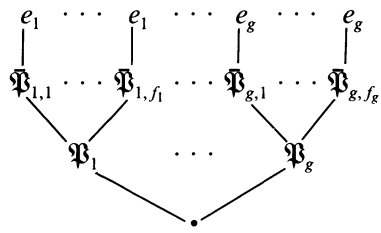
On the other hand, the application

$$\Theta\colon \mathbb{L}[[T]] \to \mathbb{L} \text{ such that } \Theta\left(\sum_{i=0}^{+\infty} \lambda_i T^i\right) = \lambda_0$$

is a $\mathbb{K}$-algebra homomorphism. And since the $\mathbb{K}$-algebra homomorphism $\Theta \circ \Psi|_{\mathcal{O}}$ from $\mathcal{O}$ to $\mathbb{L}$ has $\mathfrak{P}$ in its kernel, it induces a $\mathbb{K}$-algebra homomorphism from $\mathcal{O}/\mathfrak{P} = \mathbb{L}^*$ to $\mathbb{L}$. This proves the lemma, and theorem 3.

REMARK: The fact that the $\mathcal{G}$-orbits of rational Puiseux expansions of F are in one-to-one correspondence with the places of $\mathbb{K}(C)$ lying above $\mathfrak{p}_0$ is simply a different statement of theorem 2.

In the following diagram, ramification indices are on the first line, places of $\bar{\mathbb{K}}(C)$ lying above $\bar{\mathfrak{p}}_0$ are on the second line, and places of $\mathbb{K}(C)$ lying above $\mathfrak{p}_0$ on the third line:



In addition, theorem 3 proves that the residual field of a place is $\mathbb{K}$-isomorphic to the coefficient field of any rational Puiseux expansion of F in the corresponding $\mathcal{G}$-orbit. Among the consequences of this property are:

- The fact that the coefficient field of the rational Puiseux expansion of a given branch of C is "the smallest one" among the coefficient fields of the parametrizations of this branch (by the lemma above). It will be seen in section 4 that the computations can be made in this field.
- When $\mathbb{K}$ is the field $\mathbb{R}$ of real numbers, since a branch of a complex curve (defined by a real polynomial) is real if and only if its residual fields is the field of reals, we get the following result:

COROLLARY: *Let $F(X, Y)$ be a bivariate polynomial with real coefficients, and $\{(\tilde{x}_k, \tilde{y}_k)\}_k$ a system of rational Puiseux expansions of F over $\mathbb{R}$. Then for each k, the branch of C parametrized by $(\tilde{x}_k, \tilde{y}_k)$ is real if and only if the coefficient of $\tilde{x}_k$ and every coefficient of $\tilde{y}_k$ are real numbers.*

This corollary leads to a simple determination of the real branches of C, since it can be decided whether every coefficient of $\tilde{x}_k$ and of $\tilde{y}_k$ is real with a *finite* computation (*cf.* section 4).

EXAMPLES: Let us come back to $F = (X^2 + Y^2)^3 - 4X^2Y^2$ over $\mathbb{K} = \mathbb{Q}$. We have seen that F has a system of rational Puiseux expansions over $\mathbb{Q}$ consisting of 4 expansions, each with coefficient field $\mathbb{Q}$. It follows that $\bar{\mathbb{Q}}(C)$ (*resp.* $\mathbb{Q}(C)$) has 4 places lying above $\bar{\mathfrak{p}}_0$ (*resp.* above $\mathfrak{p}_0$).

Now, let $F = (2X^2 + Y^2)^3 - 8X^2Y^2$ over $\mathbb{Q}$. It also has a system of 4 rational Puiseux expansions over $\mathbb{Q}$, namely

$$(\tilde{x}_1, \tilde{y}_1) = (T, T^2 + \ldots), (\tilde{x}_2, \tilde{y}_2) = (T, -T^2 + \ldots),$$

$$(\tilde{x}_3, \tilde{y}_3) = ((\sqrt{2}/4)T^2, T + \ldots), (\tilde{x}_4, \tilde{y}_4) = (-(\sqrt{2}/4)T^2, T + \ldots).$$

It follows that $\bar{\mathbb{Q}}(C)$ still has 4 places lying above $\mathfrak{p}_0$, while the field $\mathbb{Q}(C)$ has only 3 places lying above $\mathfrak{p}_0$: the two last expansions are conjugated over $\mathbb{Q}$ and thus they correspond to only one place of $\mathbb{Q}(C)$, with ramification index 2 and residual degree 2.

The two following examples, though very simple, point out the basic ideas of the algorithm:

Let $F = Y^2 + X$ over $\mathbb{Q}$. The classical Puiseux expansions of F are

$$\bar{y}_1 = iX^{1/2} \quad \text{and} \quad \bar{y}_2 = -iX^{1/2}$$

and it has a system of rational Puiseux expansions consisting of the unique pair

$$(\tilde{x}_1, \tilde{y}_1) = (-T^2, T).$$

The coefficient field is $\mathbb{Q}(i)$ in the classical case, and simply $\mathbb{Q}$ in the rational case, and thus the only branch of center (0, 0) of this parabola is real. In some sense, the coefficient (-1) of $\tilde{x}_1$ causes the disparition of the irrational coefficient i.

But it is not always so simple. An example of a more general situation is $F = Y^7 - 9X^5$ over $\mathbb{Q}$. The classical Puiseux expansions of F are the

$$v_1(\xi_7^i X^{1/7}) \quad \text{for } i = 0, 1, \ldots, 6,$$

where $v_1(T) = 9^{1/7}T^5$ and ζ_7 is a primitive root of unity of order 7 in $\bar{\mathbb{Q}}$. A system of rational Puiseux expansions of F is made of the unique expansion

$$(\tilde{x}_1, \tilde{y}_1) = (T^7/9^3, T^5/9^2)$$

which implies that C has only one branch centered at (0, 0) and that this branch is real. Actually in this example the exponent 1/7 of 9 in v_1 is "replaced" by -2, which is the inverse of 7 modulo 5, and this "mistake" is corrected by the coefficient 9^{-3} of $\tilde{x}_1$ (notice that $-2 \times 7 + 3 \times 5 = 1$).

It may be noticed that $\{(3T^7, 3T^5)\}$ is another system of rational Puiseux expansions of F over $\mathbb{Q}$. It is simpler, but cannot be obtained directly by the algorithm of Section 4.

4. Rational Newton algorithm

The aim of this section is to describe simultaneously the classical and rational Newton algorithms, as two different versions of a unique algorithm.

This algorithm consists in two parts, respectively called the singular and the regular part.

- The *singular part* is the one we are interested in: this part gives the integer $\bar{g}$, and for each k from 1 to $\bar{g}$, it gives $\tilde{x}_k$, e_k, f_k, $\mathbb{L}_k$, and R_k coefficients of the series $\tilde{y}_k$, for some positive integer R_k.
- The *regular part* is simpler and does not depend on the chosen version, but computations are performed in a smaller field in the rational case. This part gives as many terms as wanted for the $\tilde{y}_k$'s. If a large number of terms is required, the algorithm of Kung and Traub [K–T] is recommended in both versions.

4.1. Notations and formulae

A $\mathbb{K}$-*term* is defined as a list $\tau = (q, \mu, m, \beta)$ of four elements, where q and m are coprime integers, q is positive, and μ and β are non-zero elements of $\bar{\mathbb{K}}$.

A *finite* $\mathbb{K}$-*expansion* is a finite sequence $(\tau_1, \tau_2, \ldots, \tau_M)$ of $\mathbb{K}$-terms such that $m_h > 0$ for $h \geqslant 2$ (where $\tau_h = (q_h, \mu_h, m_h, \beta_h)$). A $\mathbb{K}$-*expansion* is then a sequence (usually infinite) $\pi = (\tau_1, \tau_2, \ldots, \tau_h, \ldots)$ of $\mathbb{K}$-terms, such that $m_h > 0$ for $h \geqslant 2$, and there exists an integer R such that $q_h = 1$, $\mu_h = 1$, and $\beta_h \in \mathbb{K}(\mu_1, \beta_1, \mu_2, \beta_2, \ldots, \mu_R, \beta_R)$ for every $h > R$.

To each $\mathbb{K}$-expansion π is associated a pair $P(\pi) = (\tilde{x}, \tilde{y})$ of elements of $\bar{\mathbb{K}}[[T]]$, where $\tilde{x}$ is a non-constant monomial, in the following way:

Let $\pi = (\tau_1, \tau_2, \ldots, \tau_h, \ldots)$ and $\tau_h = (q_h, \mu_h, m_h, \beta_h)$. Consider new symbols $X_0, X_1, \ldots, X_R$ and $Y_0, Y_1, \ldots, Y_h, \ldots$ and the relations

$$\begin{cases} X_{h-1} = \mu_h X_h^{q_h} & \text{for } 1 \leqslant h \leqslant R \\ Y_{h-1} = (\beta_h + Y_h) X_h^{m_h} & \text{for } 1 \leqslant h \leqslant M \\ Y_{h-1} = (\beta_h + Y_h) X_R^{m_h} & \text{for } h > R \end{cases}$$

The elimination of $X_1, X_2, \ldots, X_{R-1}$ and of $Y_1, Y_2, \ldots, Y_{M-1}$ for any $M \geqslant R$ gives two relations

$$\begin{cases} X_0 = \lambda X_R^e \\ Y_0 = \Sigma_{h=1}^{M} \alpha_h X_R^{n_h} + \tilde{\alpha}_M X_R^{n_M} Y_M \end{cases}$$

where α_h does not depend of M. The expression of λ, e, of the α_h's and the n_h's is easily obtained, but is not simple. It is given below for the sake of completeness, but it will note be used. Let

$$q_{h_1}^{h_2} = q_{h_1+1} q_{h_1+2} \ldots q_{h_2} = \prod_{l=h_1+1}^{h_2} q_l \quad \text{for } 0 \leqslant h_1 \leqslant h_2 \leqslant R,$$

so that $q_h^h = 1$ and $q_{h_1}^{h_2} q_{h_2}^{h_3} = q_{h_1}^{h_3}$. Then

$$X_h = \mu_{h+1}^{q_h^h} \mu_{h+2}^{q_h^{h+1}} \mu_{h+3}^{q_h^{h+2}} \ldots \mu_R^{q_h^R} X_R^{q_h^R}.$$

It follows that

$$(\mathbf{E_x}) \begin{cases} e = q_0^R = q_1 q_2 \ldots q_R \\ \lambda = \mu_1^{q_0^0} \mu_2^{q_0^1} \mu_3^{q_0^2} \ldots \mu_R^{q_0^{R-1}} \end{cases}$$

And from $Y_0 = \beta_1 X_1^{m_1} + X_1^{m_1} Y_1 = \beta_1 X_1^{m_1} + \beta_2 X_1^{m_1} X_2^{m_2} + X_1^{m_1} X_2^{m_2} Y_2 = \ldots = \beta_1 X_1^{m_1} + \beta_2 X_1^{m_1} X_2^{m_2} + \cdots + \beta_R X_1^{m_1} \ldots X_R^{m_R} + X_1^{m_1} \ldots X_R^{m_R} Y_R$ comes

$\alpha_h X_R^{n_h} = \beta_h X_1^{M_1} X_2^{m_2} \ldots X_h^{m_h}$ for $1 \leqslant h \leqslant R$, and thus:

$$(\mathbf{E_y^{(s)}}) \begin{cases} n_h = m_1 q_1^R + m_2 q_2^R + \cdots + m_h q_h^R \\ \alpha_h = \beta_h \tilde{\alpha}_h \\ \tilde{\alpha}_h = \mu_2^{m_1 q_1^1} \mu_3^{m_1 q_1^2 + m_2 q_2^2} \ldots \mu_{h+1}^{m_1 q_1^h + m_2 q_2^h + \cdots + m_h q_h^h} \\ \qquad \mu_{h+2}^{m_1 q_1^{h+1} + \cdots + m_h q_h^{h+1}} \ldots \mu_R^{m_1 q_1^{R-1} + \cdots + m_h q_h^{R-1}} \quad \text{for } h \leqslant R. \end{cases}$$

For $h > R$, from $X_1^{m_1} \ldots X_R^{m_R} Y_R = \tilde{\alpha}_R X_R^{n_R} Y_R$ and from $Y_R = \beta_{R+1} X_R^{m_{r+1}} + \beta_{R+2} X_R^{m_{R+1}+m_{R+2}} + \cdots + \beta_h X_R^{m_{R+1}+\cdots+m_h} + X_R^{m_{R+1}+\cdots+m_h} Y_h$ comes

$$\alpha_h X_R^{n_h} = \tilde{\alpha}_R X_R^{n_R} \beta_h X_R^{m_{h+1}+\cdots+m_h}, \text{ so that}$$

$$(\mathbf{E}_y^{(r)}) \begin{cases} n_h = n_R + m_{R+1} + \cdots + m_h \\ \alpha_h = \beta_h \tilde{\alpha}_R \qquad \text{for } h > R \end{cases}$$

Now, the pair $P(\pi) = (\tilde{x}, \tilde{y})$ is defined by

$$\left(\tilde{x} = \lambda X^e, \tilde{y} = \sum_{h=1}^{+\infty} \alpha_h X^{n_h} \right).$$

The result of Newton's algorithm (described below) defines a set of $\mathbb{K}$-expansions $\{\pi_k\}_k$. In the classical version of the algorithm, k varies from 1 to N and the $P(\pi_k)$'s are the parametrizations (u_k, v_k)'s of section 1, associated to the classical Puiseux series of F. In the rational case, we shall prove that k varies from 1 to $\bar{g}$ and that the $P(\pi_k)$'s form a system of rational Puiseux expansions of F over $\mathbb{K}$.

4.2. Description of the algorithm

In the description of the algorithm, finite ordered sets are represented by lists $(\ldots)$ – thus the empty set is $(\ )$ –, and $(a_1, a_2, \ldots, a_k) \cup (b_1, b_2, \ldots, b_l)$ represents $(a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l)$. Comments are in *italic*. And $\mathbb{L}$ stands for any finite extension of $\mathbb{K}$.

The *Newton polygon* of a polynomial $F(X, Y) = \Sigma_{i=0}^{N} \Sigma_{j=0}^{M} a_{i,j} X^j Y^i$ is defined as the lower part of the convex hull of the set of points (i, j) in the plane such that $a_{i,j}$ is non-zero [Wa, 4].

We shall use the following five "primitive" algorithms:

Algorithm COEFFICIENT (F, i, j).
In: $F \in \mathbb{L}[X, Y]$; i, j non-negative integers;
Out: the coefficient of $X^j Y^i$ in F.

Algorithm BEZOUT (q, m).
In: two coprime integers q and m, with $q > 0$;
Out: (u, v), where u and v are integers such that $uq + vm = 1$.

Algorithm SQUARE-FREE (Φ).
In: $\Phi \in \mathbb{L}[Z]$;
Out: A finite set of lists (Ψ, r) with $\Psi \in \mathbb{L}[Z]$ and r a positive integer, such that each Ψ is square-free and $\Phi = \Pi_{(\Psi,r)} \Psi^r$ and the Ψ's are pairwise coprime.

It is well known that such a decomposition can be obtained with derivations and gcd's computations, without any factorization algorithm [D–S–T].

Algorithm NEW-POLYNOMIAL (F, τ, l).
In: $F \in \mathbb{L}[X, Y]$; a $\mathbb{K}$-term $\tau = (q, \mu, m, \beta)$; an integer l;
Out: $X^{-1}F(\mu X^q, X^m(\beta + Y)) \in \mathbb{L}(\mu, \beta)(X)[Y]$.
This algorithm will always be used with values of the parameters such that the result is in $\mathbb{L}(\mu, \beta)[X, Y]$.

Algorithm POLYGON (F, I).
In: $F \in \mathbb{L}[X, Y]$; $I = 1$ or 2;
Out: A finite set of lists (q, m, l, Φ) with q, m, l integers, q and m coprime, $q > 0$, and $\Phi \in \mathbb{L}[Z]$.
Those lists are in one-to-one correspondence with the segments of the Newton polygon of F *if* $I = 1$, *and only with the segments with negative slope if* $I = 2$. *The correspondence is the following: The segment* Δ *corresponding to the list* (q, m, l, Φ) *is on the line* $qj + mi = l$ *in the* (i, j)*-plane, and* $\Phi = \Sigma_{(i,j)\in\Delta} a_{i,j} Z^{(i-i_0)/q}$ *where* i_0 *is the smallest value of* i *such that there is a point* (i, j) *on* Δ. *It is easily seen that* Φ *is in* $\mathbb{L}[Z]$ *and not only in* $\mathbb{L}(Z^{1/q})$.

Let us now come to the description of the algorithm NEWTON. The subalgorithm SINGULAR computes the singular part of the expansions, with the help of SINGULAR-TERM which computes a set of terms. The result of SINGULAR is then sent to the sub-algorithm REGULAR, which computes the regular part of the expansions, and is independent of the chosen version. The difference between both versions comes from the SINGULAR-TERM sub-algorithm.

Algorithm NEWTON (*version*, F, H).
In: *version* has one of the two values *classical* or *rational*; H is a positive integer; F is an absolutely irreducible polynomial of $\mathbb{K}[X, Y]$, monic and of positive degree in Y. In order to simplify the description of the algorithm, we assume in addition that F has no "finite" Puiseux expansion (*cf.* Section 2). If such is not the case, during the computation is met a Newton polynomial with no point on the j-axis, which means that the corresponding expansion is completely obtained.
See the conclusion of this paper for looser assumptions on F.
Out: a finite set of finite $\mathbb{K}$-expansions, each of them containing at least H terms.
Sub-algorithms: REGULAR, SINGULAR.
begin
  return REGULAR (SINGULAR (*version*, F, $\mathbb{K}$, ( )), H)
end.

Algorithm REGULAR (S, H).
In: S is a finite set of pairs $\{(\pi_k, F_k)\}_{1 \leqslant k \leqslant B}$ where for each k, π_k is a finite $\mathbb{K}$-expansion, $F_k \in \bar{\mathbb{K}}[X, Y]$, with $F_k(0, 0) = 0$, $(F_k)'_Y(0, 0) \neq 0$ and $F_k(X, 0) \neq 0$; H is a positive integer;
Out: A set $\{\pi'_k\}_{1 \leqslant k \leqslant B}$ of finite $\mathbb{K}$-expansions, such that each π'_k begins with π_k and contains at least H $\mathbb{K}$-terms.
Sub-algorithms: COEFFICIENT, NEW-POLYNOMIAL.
begin
  $R \leftarrow (\ )$; *results will be grouped in the set* R.
  for each (π, F) in S do
    while cardinal $(\pi) < H$ do
      $m \leftarrow$ Min $\{j/\text{COEFFICIENT}\ (F, 0, j) \neq 0\}$;
      $\beta \leftarrow -\text{COEFFICIENT}\ (F, 0, m)/\text{COEFFICIENT}\ (F, 1, 0)$
      $\tau \leftarrow (1, 1, m, \beta)$;
      $\pi \leftarrow \pi \cup (\tau)$;
      $F \leftarrow$ NEW-POLYNOMIAL (F, τ, m);
    $R \leftarrow R \cup (\pi)$;
  return R
end.

Algorithm SINGULAR (*version*, F, $\mathbb{L}$, π).
In: *version* as in NEWTON; $F \in \mathbb{L}[X, Y]$; π is a finite $\mathbb{K}$-expansion;
Out: a finite set of pairs $(\pi 1, F1)$ where $\pi 1$ is a finite $\mathbb{K}$-expansion beginning by π, and $F1 \in \mathbb{L}1[X, Y]$ for some extension $\mathbb{L}1$ of $\mathbb{L}$.
Sub-algorithms: SINGULAR-TERM, NEW-POLYNOMIAL, SINGULAR.
This algorithm is recursive.
begin
  $S \leftarrow (\ )$; *results of the algorithm will be grouped in the set* S.
  if $\pi = (\ )$ then $I \leftarrow 1$ else $I \leftarrow 2$;
  for each (τ, l, r) in SINGULAR-TERM (*version*, F, L, I) do
    $\pi 1 \leftarrow \pi \cup (\tau)$;
    $F1 \leftarrow$ NEW-POLYNOMIAL (F, τ, l);
    $\mathbb{L}1 \leftarrow$ the extension of $\mathbb{L}$ generated by the elements μ and β of τ;
    if $r = 1$ then $S \leftarrow S \cup ((\pi 1, F1))$
      else $S \leftarrow S \cup$ SINGULAR (*version*, $F1$, $\mathbb{L}1$, $\pi 1$);
  return S
end.

Algorithm SINGULAR-TERM (*version*, F, $\mathbb{L}$, I).
In: *version*, F and $\mathbb{L}$, as in SINGULAR; $I = 1$ or 2;
$I = 1$ *for the computation of the first term of each finite* $\mathbb{K}$*-expansion,* $I = 2$ *for the other terms.*

Out: a finite set of lists (τ, l, r), where τ is a $\mathbb{K}$-term, l and r are integers, and $r > 0$.
Sub-algorithms: POLYGON, BEZOUT, SQUARE-FREE.
begin
  $T \leftarrow (\ )$; *results will be grouped in the set* T.
  for each (q, m, l, Φ) in POLYGON (F, I) do
    if *version* = *rational* then $(u, v) \leftarrow$ BEZOUT (q, m);
    for each (Ψ, r) in SQUARE-FREE (Φ) do
      for each root ξ of ψ in $\bar{\mathbb{K}}$ do
        if *version* = *classical* then
          for each root β of $U^q - \xi$ in $\bar{\mathbb{K}}$ do
            $\tau \leftarrow (q, 1, m, \beta)$;
            $T \leftarrow T \cup ((\tau, l, r))$;
        if *version* = *rational* then
          $\mu \leftarrow \xi^{-v}$;
          $\beta \leftarrow \xi^{u}$;
          $\tau \leftarrow (q, \mu, m, \beta)$;
          $T \leftarrow T \cup ((\tau, l, r))$;
  return T
end

Remarks:

● The result of this algorithm, in its rational version, depends on the choice of the integers u and v returned by the sub-algorithm BEZOUT. We shall prove that the result always corresponds to a system of rational Puiseux expansions of F over $\mathbb{K}$. For example, if $F = Y^7 - 9X^5$ (*cf.* section 3), the unique expansion returned by the algorithm can be $(\tilde{x}_1, \tilde{y}_1) = (T^7/9^3, T^5/9^2)$, or $(\tilde{x}_1, \tilde{y}_1) = (9^4 T^7, 9^3 T^5)$. Of course, it is recommended to choose u and v "small", and particularly $u = 1$ and $v = 0$ as soon as $q = 1$.

● We have used in the sub-algorithm SINGULAR-TERM the "root extraction" instructions:

  for each root ξ of ψ in $\bar{\mathbb{K}}$ do
    if *version* = *classical* then
      for each root β of $U^q - \xi$ in $\bar{\mathbb{K}}$ do . . .

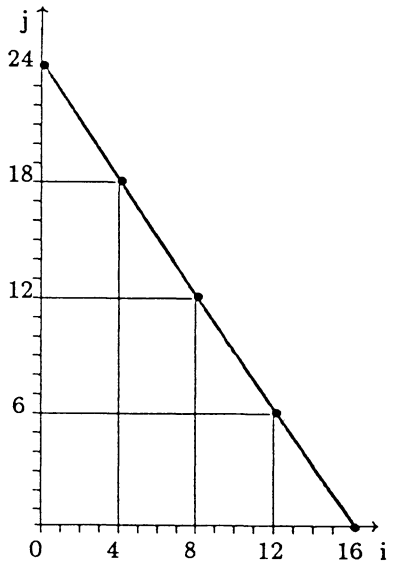
Those instructions can be executed by the D5 system (*cf.* [D–D]): The idea is to introduce a new symbol (say ξ) with the rule $\Psi(\xi) = 0$, and to consider different cases "in parallel" when the roots of Ψ do not all behave in the same way.

4.3. Examples: Before proving that the rational version of the algorithm above actually returns a system of rational Puiseux expansions of F over $\mathbb{K}$,

let us have it work on the example of

$$F = Y^{16} - 4Y^{12}X^6 - 4Y^{11}X^8 + Y^{10}X^{10} + 6Y^8X^{12} + 8Y^7X^{14} + 14Y^6X^{16} + 4Y^5X^{18} + Y^4(X^{20} - 4X^{18}) - 4Y^3X^{20} + Y^2X^{22} + X^{24} \text{ over } \mathbb{Q}.$$

● The classical version of the algorithm runs as follows: The Newton polygon of F has only one segment:



and POLYGON (F, 1) returns the list

$$((q_1, m_1, l_1, \Phi_1)) = ((2, 3, 48, Z^8 - 4Z^6 + 6Z^4 - 4Z^2 + 1)).$$

Here, $\Phi_1 = \Psi_1^4$ where $\Psi_1 = Z^2 - 1$ is squarefree. The result of SINGULAR-TERM (*classical*, F, $\mathbb{Q}$, 1) is made of 4 lists

$$(\tau_1, l_1, r_1) = ((2, 1, 3, \beta_1), 48, 4),$$

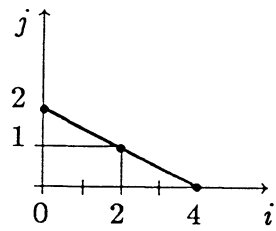
one for each β_1 in $\bar{\mathbb{Q}}$ such that $\psi_1(\beta_1^{q_1}) = 1$, i.e., such that $\beta_1^4 - 1 = 0$. They correspond (*cf.* 4.1.) to the relations

$$\begin{cases} X_0 = X_1^2 \\ Y_0 = (\beta_1 + Y_1)X_1^3 \end{cases}$$

The new polynomial now is, for each β_1:

$$\begin{aligned} F_1 &= X^{-48}F(X^2, (\beta_1 + Y)X^3) \\ &= (\textit{terms of degree} > 4 \textit{ in } Y) \\ &\quad + Y^4(X^4 + 20\beta_1 X^3 + 420\beta_1^2 X^2 - 1040\beta_1^3 X + 256) \\ &\quad + Y^3(4\beta_1 X^4 + 40\beta_1^2 X^3 + 400\beta_1^3 X^2 - 384X) \\ &\quad + Y^2(6\beta_1^2 X^4 + 40\beta_1^3 X^3 + 256X^2 - 64\beta_1 X) + Y(4\beta_1^3 X^4 \\ &\quad + 20X^3 + 96\beta_1 X^2) + (X^4 + 4\beta_1 X^3 + 16\beta_1^2 X^2). \end{aligned}$$

Newton polygon of F_1 is the same for each β_1, and it has only one segment with negative slope:



The result of POLYGON (F_1, 2) is

$$((q_2, m_2, l_2, \Phi_2)) = ((2, 1, 4, 16(16Z^2 - 4\beta_1 Z + \beta_1^2)))$$

and Φ_2 is squarefree. Thus $\Psi_2 = \Phi_2$, and the result of SINGULAR-TERM (*classical*, F_1, $\mathbb{Q}(\beta_1)$, 2) is made of 4 lists

$$(\tau_2, l_2, r_2) = ((2, 1, 1, \beta_2), 4, 1),$$

one for each β_2 in $\bar{\mathbb{Q}}$ such that $\psi_2(\beta_2^{q_2}) = 0$, i.e., such that $16\beta_2^4 - 4\beta_1\beta_2^2 + \beta_1^2 = 0$. They corespond to the relations

$$\begin{cases} X_1 = X_2^2 \\ Y_1 = (\beta_2 + Y_1)X_2 \end{cases}$$

Finally, NEWTON (*classical*, F, 1) returns sixteen $\mathbb{Q}$-expansions

$$\tau = (\tau_1, \tau_2) = ((2, 1, 3, \beta_1), (2, 1, 1, \beta_2)),$$

one for each choice of β_1 and β_2 in $\bar{\mathbb{Q}}$ such that $\beta_1^4 - 1 = 0$ and $16\beta_2^4 - 4\beta_1\beta_2^2 + \beta_1^2 = 0$.

The 16 classical Puiseux expansions of F are obtained:

$$\bar{y}_{\beta_1,\beta_2} = \beta_1 X^{3/2} + \beta_2 X^{7/4} + X^{7/4} z_{\beta_1,\beta_2}$$

with $z_{\beta_1,\beta_2} \in \mathbb{Q}(\beta_1, \beta_2)((X^{1/4}))$ of positive X-order.

● Now, the rational version of the algorithm works as follows: As above, POLYGON (F, 1) returns the list

$$((q, m, l, \Phi_1)) = ((2, 3, 48, Z^8 - 4Z^6 + 6Z^4 - 4Z^2 + 1))$$

where $\Phi_1 = \Psi_1^4$ and $\Psi_1 = Z^2 - 1$, squarefree. We can choose $u = -1$ and $v = 1$ in BEZOUT (2, 3). The result of SINGULAR-TERM (*rational*, F, $\mathbb{Q}$, 1) is thus made of two lists

$$(\tau_1, l_1, r_1) = ((2, \xi_1^{-1}, 3, \xi_1^{-1}), 48, 4),$$

one for each root ξ_1 of Ψ_1 in $\bar{\mathbb{Q}}$. They correspond to the relations

$$\begin{cases} X_0 = \xi_1^{-1} X_1^2 \\ Y_0 = (\xi_1^{-1} + Y_1) X_1^3 \end{cases}$$

The new polynomial is

$$\begin{aligned} F_1 &= X^{-48} F(\xi_1^{-1} X^2, (\xi_1^{-1} + Y) X^3) \\ &= (\textit{terms of degree} > 4 \text{ in } Y) \\ &\quad + Y^4(X^4 + 20\xi_1 X^3 + 420X^2 - 1040\xi_1 X + 256) + Y^3(4\xi_1 X^4 \\ &\quad + 40X^3 + 400\xi_1 X^2 - 384X) + Y^2(6X^4 + 40\xi_1 X^3 + 256X^2 \\ &\quad - 64\xi_1 X) + Y(\xi_1 X^4 + 20X^3 + 96\xi_1 X^2) + (X^4 + 4\xi_1 X^3 + 16X^2). \end{aligned}$$

The Newton polygon of F_1 is the same as in the classical case, and does not depend on ξ_1. The result of POLYGON (F_1, 2) is

$$((q_2, m_2, l_2, \Phi_2)) = ((2, 1, 4, 16(15Z^2 - 4\xi_1 Z + 1))).$$

We can choose $u = 0$ and $v = 1$ in BEZOUT(2,1). Since $\Phi_2 = \Psi_2$ is squarefree, SINGULAR-TERM(*rational*, F_1, $\mathbb{Q}(\xi_1)$, 2) returns two lists

$$(\tau_2, l_2, r_2) = ((2, \xi_2^{-1}, 1, 1), 4, 1),$$

one for each root ξ_2 of Ψ_2 in $\bar{\mathbb{Q}}$. They correspond to

$$\begin{cases} X_1 = \xi_2^{-1} X_2^2 \\ Y_1 = (1 + Y_2)X_2 \end{cases}.$$

Finally, NEWTON (*rational*, F, 1) returns four $\mathbb{Q}$-expansions

$$\pi = (\tau_1, \tau_2) = ((2, \xi_1^{-1}, 3, \xi_1^{-1}), (2, \xi_2^{-1}, 1, 1))$$

for ξ_1 and ξ_2 in $\bar{\mathbb{Q}}$ such that $\xi_1^2 - 1 = 0$ and $16\xi_2^2 - 4\xi_1\xi_2 + 1 = 0$.

And we get a system of 4 rational Puiseux expansions of F:

$$(\tilde{x}_{\xi_1,\xi_2} = -64\xi_2 T^4, \tilde{y}_{\xi_1,\xi_2} = -64T^6 - 64\xi_1 T^7 + T^7 z_{\xi_1,\xi_2})$$

with z_{ξ_1,ξ_2} in $\mathbb{Q}(\xi_1, \xi_2)((T))$ of positive T-order.

Either classical or rational expansions of F prove that the field $\bar{\mathbb{Q}}(C)$ has 4 places lying above $\bar{\mathfrak{p}}_0$, each with ramification index 4.

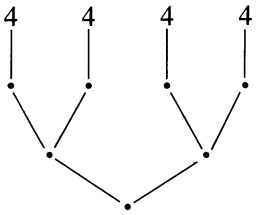
In order to conclude for the field $\mathbb{Q}(C)$, one must use the rational expansions, and also factorization features. Since the polynomial Ψ_1 is the product of two linear factors over $\mathbb{Q}$, and Ψ_2 is irreducible over $\mathbb{Q}(\xi_1)(=\mathbb{Q})$, the 4 expansions are pairwise conjugated over $\mathbb{Q}$. It follows that there are two places of $\mathbb{Q}(C)$ lying above $\mathfrak{p}_0$, each with ramification index 4 and residual degree 2.

Since $\mathbb{R}$ contains $\mathbb{Q}$, it is easy to see that the system of rational Puiseux expansions of F over $\mathbb{Q}$ is also rational over $\mathbb{R}$. It happens here that Ψ_2 has no real root. It follows that $\mathbb{R}(C)$ also has two places lying above $\mathfrak{p}_0$, with ramification index 4 and residual degree 2 (the residual fields are $\mathbb{C}$). And that the curve C has no real branch above 0, but two pairs of complex conjugate branches. Notice that the number of real roots of a real polynomial may be counted with Sturm sequences techniques [C–R], similar to Euclid's

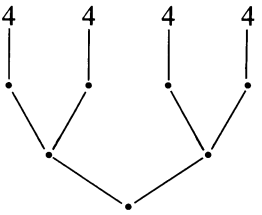
algorithm and much easier than the factorization techniques that are needed for $\mathbb{Q}(C)$.

In this example, the diagrams corresponding to $\mathbb{Q}(C)$ and to $\mathbb{R}(C)$ are similar:

$\mathbb{Q}(C)$:



$\mathbb{R}(C)$:



In general, the situation needs not be the same for $\mathbb{Q}(C)$ and $\mathbb{R}(C)$. Here are two more examples, where $\bar{\mathbb{Q}}(C)$ still has 4 places over $\bar{\mathfrak{p}}_0$, each with ramification index 4:

$$\begin{aligned}\text{For } G \;=\; & Y^{16} - 2Y^{13}X^5 - 4Y^{12}X^6 + Y^{10}X^{10} + 2Y^9X^{11} \\ & + Y^8(8X^{13} + 6X^{12}) - 2Y^6X^{16} + Y^5(-4X^{18} + 2X^{17}) \\ & + Y^4(-X^{20} + 8X^{19} - 4X^{18}) + Y^2X^{22} - 2YX^{23} + X^{24}\end{aligned}$$

the result of NEWTON (*rational*, G, 1) is

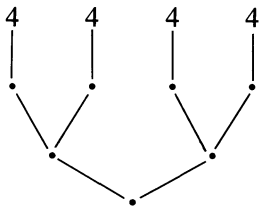
$$\tilde{x} \;=\; 16(-4\xi_1\xi_2 + \xi_1 - 1)T^4,$$

$$\begin{aligned}\tilde{y} \;=\; & (256\xi_2\xi_1 - 256\xi_2 - 128\xi_1 + 64)T^6 \\ & + (-256\xi_2\xi_1 + 256\xi_2 + 64\xi_1 - 128)T^7 + \ldots\end{aligned}$$

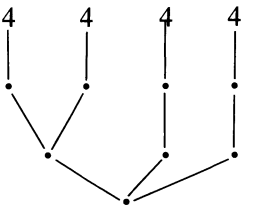
where $\xi_1^2 - 1 = 0$ and $16\xi_2^2 - 4\xi_2 + \xi_1 = 0$. As above, $Z^2 - 1 = (Z - 1)(Z + 1)$ over $\mathbb{Q}$ and $\mathbb{R}$, and $16Z^2 - 4Z + \xi_1$ is irreducible over $\mathbb{Q}$. It has no real root when $\xi_1 = 1$, but two real roots when $\xi_1 = -1$. It follows that the result for $\mathbb{Q}(C_G)$ is the same as for $\mathbb{Q}(C)$ above, but for $\mathbb{R}(C_G)$ there are 3 places above $\mathfrak{p}_0$, one with residual degree 2 (corresponding to a pair of complex conjugate branches) and two with residual degree 1 (corresponding to 2 real branches). The diagrams now

are:

$\mathbb{Q}(C_G)$:



$\mathbb{R}(C_G)$:



For $H = Y^{16} - 2Y^{13}X^5 - 8Y^{12}X^6 + Y^{10}X^{10} + 4Y^9X^{11}$

$+ Y^8(128X^{13} + 24X^{12}) - 4Y^6X^{16} + Y^5(-64X^{18} + 8X^{17})$

$+ Y^4(-128X^{20} + 256X^{19} - 32X^{18}) + 4Y^2X^{22} - 16YX^{23} + 16X^{24}$

the result of NEWTON(*rational*, H, 1) is

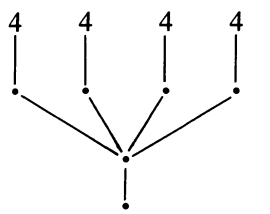
$\tilde{x} = (-16\xi_2\xi_1 + \xi_1 - 16)T^4,$

$\tilde{y} = (256\xi_2\xi_1 - 32\xi_2 - 32\xi_1 + 2)T^6$

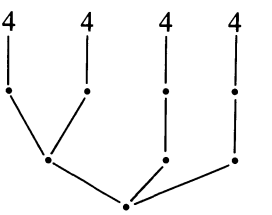
$+ (-32\xi_2\xi_1 + 512\xi_2 + 2\xi_1 - 64)T^7 + \ldots$

where $\xi_1^2 - 2 = 0$ and $32\xi_2^2 - 2\xi_2 + \xi_1 = 0$. Here, $Z^2 - 2$ is irreducible over $\mathbb{Q}$ and has two real roots. And $Z^2 - 2Z + \xi_1$ is irreducible over $\mathbb{Q}(\xi_1)$, it has no real root when $\xi_1 = \sqrt{2}$, but it has two real roots when $\xi_1 = -\sqrt{2}$. It follows that the conclusion for $\mathbb{R}(C_H)$ is the same as for $\mathbb{R}(C_G)$, but $\mathbb{Q}(C_H)$ has only one place above $\mathfrak{p}_0$, with residual degree 4. The corresponding diagrams are:

$\mathbb{Q}(C_H)$:



$\mathbb{R}(C_H)$:



4.4. Existence of rational Puiseux expansions

Let $\{\pi_k^{(H)}\}_{1 \leqslant k \leqslant \bar{g}^\circ}$ be the result of NEWTON(*rational*, F, H) for every $H > 0$, and $\pi_k^{(H)} = (\tau_{k,h})_{1 \leqslant h \leqslant M_k^{(H)}}$. It is clear from the algorithm that $\bar{g}^\circ$ and the $\tau_{k,h}$'s do not depend on H. But the number of $\mathbb{K}$-terms in each τ_k varies with H; if $R_k = M_k^{(1)}$ is the number of terms in $\pi_k^{(1)}$, then $M_k^{(H)} = \mathrm{Max}(R_k, H)$ for every H.

If $\pi_k = (\tau_{k,h})_{1 \leqslant h \leqslant +\infty}$ for $1 \leqslant h \leqslant \bar{g}^\circ$, it is clear from the algorithm that π_k is a $\mathbb{K}$-expansion, and that the set of the π_k's (for $1 \leqslant k \leqslant \bar{g}^\circ$) is invariant under the action of $\mathcal{G}$. Let g° be the number of orbits for this action, assume that the π_k's for $1 \leqslant k \leqslant g^\circ$ are in different orbits. It follows from the description of the algorithm that, for each k between 1 and g°, the integer R_k is the smallest positive integer such that the three following properties hold:

(R1.) $q_{k,h} = 1$ for every $h > R_k$;

(R2.) $\mu_{k,h}$ and $\beta_{k,h}$ are in $\mathbb{K}(\mu_{k,1}, \beta_{k,1}, \mu_{k,2}, \ldots, \beta_{k,R_k})$ for every $h > R_k$;

(R3.) If $\tau_{k,h} = \tau_{k',h}$ for some k' between 1 and g° and for every h from 1 to R_k, then $k = k'$.

In addition, $\mu_{k,h} = 1$ for $h > R_k$. This integer R_k is called the *regularity index* of the $\mathbb{K}$-expansion π_k, or of the corresponding pair of series $P(\pi_k)$ (*cf.* 4.1.).

THEOREM 4: *The set* $\{P(\pi_k)\}_{1 \leqslant k \leqslant \bar{g}^\circ}$ *obtained from the results of NEWTON* (*rational*, F, H) (*for every* H) *is a system of rational Puiseux expansions of* F.

Proof: By mimicking the proof that the classical Newton's algorithm terminates and gives classical Puiseux expansions of F [Wa, 4], we see that the rational Newton's algorithm terminates and gives irreducible parametrizations of branches of C lying above 0.

Let $\mathfrak{P}_k$ be the place of $\bar{\mathbb{K}}(C)$ corresponding to the parametrization $P(\pi_k) = (\tilde{x}_k^\circ = \lambda_k^\circ T^{e_k^\circ}, \tilde{y}_k^\circ)$. Then, as in the proof of theorem 1, for each k the

$$\tilde{y}_k^\circ(\zeta_k^i(\lambda_k^\circ)^{-1/e_k^\circ} X^{1/e_k^\circ})$$

for $1 \leqslant i \leqslant e_k^\circ$, where ζ_k is a primitive root of unity of order e_k° in $\bar{\mathbb{K}}$, are classical Puiseux expansions of F, and are pairwise distinct. It follows that e_k° is the ramification index e_k of $\mathfrak{P}_k$.

In addition, comparison of both versions of Newton's algorithm shows that every classical Puiseux expansion of F is of this form for some k. Thus,

if we can prove that $\Sigma_{k=1}^{\bar{g}^\circ} e_k^\circ \leqslant N$, then

$$\sum_{k=1}^{\bar{g}^\circ} e_k^\circ \;=\; N \;=\; \sum_{k=1}^{\bar{g}} e_k$$

and we shall be sure that the $P(\pi_k)$ are pairwise non-equivalent parametrizations.

But, if f_k° is the cardinal of the orbit of $P(\pi_k)$ under the action of $\mathscr{G}$ for $1 \leqslant k \leqslant g^\circ$, then $\Sigma_{k=1}^{\bar{g}^\circ} e_k^\circ = \Sigma_{k=1}^{g^\circ} e_k^\circ f_k^\circ$, and f_k° is the degree of the coefficient field $\mathbb{L}_k^\circ$ of $P(\pi_k)$. And, with obvious notations, $\mathbb{L}_k^\circ$ is contained in $\mathbb{K}(\mu_{k,1}, \beta_{k,1}, \mu_{k,2}, \ldots, \beta_{k,R_k})$, which is equal to $\mathbb{K}(\xi_{k,1}, \xi_{k,2}, \ldots, \xi_{k,R_k})$. From the description of rational Newton's algorithm comes

$$\sum_{k=1}^{g^\circ} e_k^\circ [\mathbb{K}(\xi_{k,1}, \ldots, \xi_{k,R_k}) : \mathbb{K}] \;=\; N$$

which proves that $\Sigma_{k=1}^{g^\circ} e_k^\circ f_k^\circ \leqslant N$, i.e. that $\Sigma_{k=1}^{\bar{g}^\circ} e_k^\circ \leqslant N$, as wanted.

Remarks:

- The proof above shows that the $\circ$'s are useless, i.e., that

$$e_k^\circ \;=\; e_k, f_k^\circ \;=\; f_k, \mathbb{L}_k^\circ \;=\; \mathbb{L}_k.$$

So that the coefficient field $\mathbb{K}(\lambda_k, \alpha_{k,1}, \ldots, \alpha_{k,R_k})$ is equal to $\mathbb{K}(\xi_{k,1}, \ldots, \xi_{k,R_k})$.

- The equality $\Sigma_{k=1}^{g} e_k [\mathbb{K}(\xi_{k,1}, \ldots, \xi_{k,R_k}) : \mathbb{K}] = N$ implies that

$$\sum_{k=1}^{g} [\mathbb{K}(\xi_{k,1}, \ldots, \xi_{k,R_k}) : \mathbb{K}] \leqslant N,$$

this result will be used in section 5.

- It will also be used in section 5 that the computation of the $\mathbb{K}$-expansion π_k is entirely done in this field $\mathbb{K}(\xi_{k,1}, \ldots, \xi_{k,R_k})$.

5. Complexity

In this section, assumptions on F are as in section 4: F is an absolutely irreducible polynomial of $\mathbb{K}[X, Y]$, monic and of positive degree in Y.

The two major problems for implementing Newton's algorithm are the intermediate growth of the polynomials, and the handling of algebraic numbers (*cf.* [Ma] and [Ba]).

For the first problem, a solution using "lazy evaluation" is presented in [H–M]. Let us now focus on the second problem, which is met in most computer algebra applications: how is it possible to compute exactly with algebraic numbers? More precisely, how is it possible to execute an instruction like:

"for each root ξ of Ψ in $\bar{\mathbb{K}}$ do . . ."?

Note that approximations are not allowed, since we must test equalities between numbers which depend on ξ, in order to build the Newton polygons.

By the lemma of section 3, and the description of the algorithm in section 4, we know that the rational Newton's algorithm restricts as much as possible the size of the algebraic extensions where computations are performed, but it does not suppress these extensions.

A solution to this problem is offered by the D5 system for algebraic computations with algebraic numbers [D–D]. This system does not use any factorization algorithm, which leads to improvements of the theoretical and practical complexity of the computations. The $\mathbb{K}$-expansions that are obtained with D5 are grouped in such a way that expansions which are conjugated over $\mathbb{K}$ are computed together, but in addition expansions may be computed together without being conjugated over $\mathbb{K}$.

For example, with the function G of 4.3., the result of the computation with the D5 system has the following form:

$$\tilde{x} = 16(-4\xi_1\xi_2 + \xi_1 - 1)T^4,$$

$$\tilde{y} = (256\xi_2\xi_1 - 256\xi_2 - 128\xi_1 + 64)T^6 + (-256\xi_2\xi_1 + 256\xi_2 + 64\xi_1 - 128)T^7 + \ldots$$

where $\xi_1^2 - 1 = 0$ and $16\xi_2^2 - 4\xi_2 + \xi_1 = 0$.

Now, the computation for H (in 4.3. too) returns

$$\tilde{x} = (-16\xi_1\xi_2 + \xi_1 - 16)T^4,$$

$$\tilde{y} = (256\xi_2\xi_1 - 32\xi_2 - 32\xi_1 + 2)T^6 + (-32\xi_2\xi_1 + 512\xi_2 + 2\xi_1 - 64)T^7 + \ldots$$

where $\xi_1^2 - 2 = 0$ and $32\xi_2^2 - 2\xi_2 + \xi_1 = 0$.

This is sufficient to conclude that, in both examples, the field $\bar{\mathbb{Q}}(C)$ has 4 places lying above $\bar{\mathfrak{p}}_0$, each with ramification index 4.

But, as explained in section 4.3., factorization algorithms are now needed to conclude over $\mathbb{Q}(C)$. And it is no more factorization algorithms, but rather Sturm sequences techniques, that are used to conclude over $\mathbb{R}$.

The.complexity computation below is made only for the results over $\bar{\mathbb{K}}$, not for the "rationality" results over $\mathbb{K}$, which (as we have just seen) are largely dependent on $\mathbb{K}$. In order to simplify the proofs, we assume that F has no finite Puiseux expansion.

It follows from [D-D] that the number C of elementary operations on $\mathbb{K}$ that are needed to compute NEWTON(*rational*, F, 1) – i.e. the singular part of the rational Puiseux expansions of F – with D5 is at most $O(C_a \times E(D))$, where

- C_a is an upper bound for the number of elementary operations on $\bar{\mathbb{K}}$ that are needed to compute *one* $\mathbb{K}$-expansion in NEWTON(*rational*, F, 1). In the evaluation of C_a, additions and subtractions may be forgotten, but not equality tests.
- D is the sum $\Sigma_{k=1}^{g} D_k$ where D_k is the degree of the biggest extension of $\mathbb{K}$ that is used to compute the k-st expansion.
- and $E(D)$ is the number of elementary operations over $\mathbb{K}$ that are necessary for computing the gcd of two polynomials of $\mathbb{K}[T]$ of degree less than D.

But we showed at the end of Section 4 that $D_k = f_k$ and that $\Sigma_{k=1}^{g} f_k = \bar{g} \leqslant N$, so that

$$D \leqslant N,$$

And it is known (cf. [D-S-T]) that a reasonable value for $E(D)$ is $E(D) = O(D^2)$, and thus

$$C = C_a \times O(N^2)$$

Our goal in this section is to prove that C is bounded by some polynomial expression in d, where $d = \text{Max}(M, N)$, but we do not look for an optimal bound, and do not evaluate, even when $\mathbb{K} = \mathbb{Q}$, the size of the integers that appear in the computations.

THEOREM 5: *The number C of elementary operations on $\mathbb{K}$ that are needed to compute the singular part of the rational Puiseux expansions of F is at most $O(d^8)$, where $d = \text{Max}(\deg_X(F), \deg_Y(F))$.*

Proof: Since the theorem is trivially satisfied when $N = 1$, we now assume $N \geqslant 2$. It remains to prove that C_a is bounded by $O(d^6)$. Let $\pi = (\tau_h)_{1 \leqslant h \leqslant +\infty}$ be one of the $\mathbb{K}$-expansions returned by NEWTON(*rational*, F, $*$), with $\tau_h = (q_h, \mu_h, m_h, \beta_h)$, and let R be the regularity index of π. Let

$$(\tilde{x}, \tilde{y}) = \left(\lambda T^e, \sum_{h=1}^{R} \alpha_h T^{m_h} + T^{m_h} z\right)$$

be the rational Puiseux expansion $P(\pi)$, of coefficient field $\mathbb{L} = \mathbb{K}(\lambda, \alpha_1, \ldots, \alpha_R)$, and $f = [L:K]$. Let $F = F_0, F_1, \ldots$ be the succesive values of the parameter F during the computation of π. In addition, ω_X denotes the X-order function in $\mathfrak{R}$, with values in $\mathbb{Q} \cup \{+\infty\}$.

The proof of the theorem begins with three lemmas:

LEMMA 1: *Let $\bar{y}$ be one of the classical Puiseux expansion of F corresponding to $(\tilde{x}, \tilde{y})$, as in theorem 1. Then there exists another classical Puieux expansion $\bar{y}'$ of F such that*

$$\omega_X(\bar{y} - \bar{y}') > \frac{R-2}{e}.$$

Proof: We have seen in section 4 that R is the smallest integer that satisfies properties (R1), (R2), and (R3). It follows that at least one of the following conditions hold:

(*i*) $q_R \neq 1$;

(*ii*) μ_R or β_R is not in $\mathbb{K}(\xi_1, \xi_2, \ldots, \xi_{R-1})$;

(*iii*) There exists a $\mathbb{K}$-expansion π' (not conjugated to π over $\mathbb{K}$) in the result of NEWTON(*rational*, F, $*$) such that $\tau_h = \tau'_h$ for $1 \leqslant h \leqslant R-1$ and $\tau_R \neq \tau'_R$.

In each case, it is possible to find a classical Puiseux expansion of F with the same $R-1$ terms as $\bar{y}$ but different R-th term: In case (*i*), $\bar{y}'$ can be chosen equivalent to $\bar{y}$; In case (*ii*), it is equivalent to some $\mathbb{K}$-conjugate of $\bar{y}$; and in case (*iii*), $\bar{y}'$ corresponds to π'. Anyway, $\bar{y}'$ is such that $\omega_X(\bar{y} - \bar{y}') > n_{R-1}/e$.

But the n_h's (for $h \geqslant 1$) form a sequence of non-negative strictly increasing integers, so that $n_h \geqslant h - 1$, and thus $\omega_X(\bar{y} - \bar{y}') > (R-2)/e$, as wanted.

LEMMA 2: $R \leqslant 2NM - 2M + 1$, *and thus* $R \leqslant 2NM$ *as soon as* $M \neq 0$.

Proof: (This proof is a refinement of Coates', *cf.* [Co]). Let $\mathrm{disc}_Y(F)$ be the discriminant of F in Y, i.e., the determinant of the Sylvester matrix of the Y-polynomials F and F'_Y. This matrix has dimension $2N - 1$, its coefficients are polynomials in X of degree at most M, and the coefficients of the first column are constants. Thus $\mathrm{disc}_Y(F)$ is a polynomial of $\mathbb{K}[X]$ of degree

$$\deg_X(D(X)) \leqslant (2N - 2)M.$$

On the other hand, $\mathrm{disc}_Y(F) = \Pi_{1 \leqslant k < k' \leqslant N}(\bar{y}_k - \bar{y}_{k'})^2$ where $\bar{y}_1$, $\bar{y}_2, \ldots, \bar{y}_N$ are the roots of F in $\bar{\mathbb{K}}$, i.e. the classical Puieux expansions of F. By lemma 1, for each $\bar{y}_k$ corresponding to π, there exists at least one k' such that $\omega_X(\bar{y}_k - \bar{y}_{k'}) > (R - 2)/e$. And we get the same result if $\bar{y}_k$ is associated with some $\mathbb{K}$-conjugate of π. Since $\bar{y}'$ can correspond to a $\mathbb{K}$-conjugate of π too, and since there are ef classical Puiseux expansions of F corresponding to some $\mathbb{K}$-conjugate of π, at least $(ef)/2$ among the factors $(\bar{y}_k - \bar{y}_{k'})$ of $\mathrm{disc}_Y(F)$ are such that $\omega_X(\bar{y}_k - \bar{y}_{k'}) > (R - 2)/e$.

On the other hand, since F is monic in Y, each $\bar{y}_k$ has non-negative X-order, and thus

$$\omega_X(D(X)) > 2\,\frac{ef}{2}\,\frac{R - 2}{e}.$$

But $D(X) \neq 0$ because F has simple roots in Y, and thus $v_X(D(X)) \leqslant \deg_X(D(X))$, i.e.,

$$R - 2 < 2(N - 1)M,$$

as wanted.

REMARK: From the proof of lemma 1, we see that $R - 2$ may be replaced by n_{R-1} in lemma 2, leading to

$$n_{R-1} < 2(N - 1)M.$$

LEMMA 3: *Let* M_h(resp. N_h) *be the degree of* F_h in X (resp. in Y), for $0 \leqslant h \leqslant R - 1$. *Then* $N_h = N$, $M_0 = M$ *and* $M_h \leqslant (2N - 1)NM$ *for* $h \geqslant 1$.

Proof: By definition, $N_0 = N$ and $M_0 = M$. For $h \geqslant 1$, the relations $F_h(X, Y) = X^{-l_h}F_{h-1}(\mu_h X^{q_h}, X^{m_h}(\beta_h + Y))$ lead to

$$F_h(X, Y) = X^{-1(l_1 + \cdots + l_h)}F(\lambda^{(h)}X^{e^{(h)}}, y^{(h)}(X) + \tilde{\alpha}^{(h)}X^{n^{(h)}}Y)$$

with $\lambda^{(h)}$ and $\tilde{\alpha}^{(h)}$ in L, $y^{(h)}(X)$ in $L[X]$ of degree $n^{(h)}$, and $e^{(h)} \leqslant e$, $n^{(h)} \leqslant n_h$. It follows that $N_h = N$, and $M_h \leqslant eM + n_{R-1}N$. But $e \leqslant N$ and $n_{R-1} < 2(N-1)M$ by the remark following lemma 2, proving that $M_h \leqslant NM + 2N(N-1)M = NM(2N-1)$.

End of proof of theorem 5:
In order to compute π, the sub-algorithms SINGULAR-TERM and NEW-POLYNOMIAL are used R times, with the successive values F_0, $F_1, \ldots, F_{R-1}$ of the parameter F.

The algorithm SINGULAR-TERM with parameter F_h tests the equality with 0 of at most $(N_h + 1) \times (M_h + 1)$ algebraic numbers (the coefficients of F_h). Other computations (squarefree decomposition of $\Phi(Z)$, computation of μ and β) can be neglected, so that, by lemma 3, the number of elementary operations on $\mathbb{K}$ needed by this algorithm is bounded by $O(N^3M)$.

The algorithm NEW-POLYNOMIAL essentially computes all the products $\mu_h^j \beta_h^k$ for $j \leqslant M_h$ and $k \leqslant N_h$, which amounts to $O(M_h N_h)$ multiplications, i.e., $O(N^3M)$ multiplications by lemma 3.

And thus C_α is bounded by $O(RN^3M)$, or by lemma 2

$$C_a \leqslant O(N^4M^2).$$

This concludes the proof of theorem 5.

Conclusion

Let us first notice that both versions of Newton's algorithm can be applied

- when F, as a Y-polynomial, is primitive and square-free,
- and when the characteristic of $\mathbb{K}$ is a prime number p greater than N.

Every result of the paper remains essentially true with these assumptions, but is more difficult to state: for example $\bar{\mathbb{K}}(C)$ is no more a field, but a product of fields, and so on. The algorithm of section 4 is valid under those assumptions.

Applications of the rational Puiseux expansions are, first, applications of classical Puiseux expansions. For example:

- Determination of Puiseux pairs, topological questions about plane curves [Ph, Ba].
- Dedekind-Weber algorithm to compute the space of functions associated to a divisor on a curve [B1]. This algorithm, in turn, can be used for algebraic integration [Da], absolute factorization of polynomials [Du], and

in finite characteristic for coding Goppa codes [Go]. However, in many cases a more "global" algorithm, due to Trager [Tr2], that does not use Puiseux expansions, can be used instead of Dedekind-Weber algorithm.

But rational Newton's algorithm has applications on its own, since it leads to a precise "arithmetical" study of the singularities of the curve over any base field $\mathbb{K}$ of characteristic 0, e.g., $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{R}$ (cf. section 4.3.).

It is also possible to define a "rational" version of the algorithm for computing formal solutions of linear differential equations (*cf.* [To] for the classical algorithm).

To conclude with, there are at least three reasons to prefer the rational Newton algorithm to the classical one:

- computations are performed in a smaller field,
- computations of equivalent expansions are performed together,
- and the coefficient field is interesting by itself.

References

[Ba] V. Baladi: *Calculs systématiques pour les singularités de courbes planes,* Mémoire de diplôme de mathématicien, Université de Genève, (1986).

[Bl] G.A. Bliss: *Algebraic Functions, Amer. Math. Soc. Colloq. Publ.* 16 (1933).

[Ch] C. Chevalley: *Introduction to the theory of algebraic functions of one variable, AMS Math. Surveys* 6 (1951).

[Co] J. Coates: *Construction of rational functions on a curve, Proc. Camb. Phil. Soc.* 68(1970) 105–123.

[C–R] M. Coste and M.-F. Roy: *Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets, Calsyf* 6 (1986).

[Da] J.H. Davenport: *On the integration of algebraic functions, Lecture Notes in Comput. Sci.*, Springer 102 (1981).

[D–S–T] J. Davenport, Y. Siret and E. Tournier: *Calcul formel,* Masson, (1987).

[D–D] C. Dicrescenzo and D. Duval: *Computations with algebraic numbers – the D5 system, submitted to publication,* 1987.

[Du] D. Duval: *Une approche géométrique de la factorisation absolue de polynômes,* Thèse d'Etat, Université de Grenoble 1, (1987), 71–104.

[Fu] W. Fulton: *Algebraic curves,* Benjamin (1969).

[Go] V.D. Goppa: *Codes and information, Uspekhi Mat. Nauk* 39.1 (1984) 77–120, = *Russian Math. Surveys* 39.1 (1984) 87–143.

[H–M] J.-P. Henry and M. Merle, *Paires de Puiseux, résolution de courbes et évaluation paresseuse,* Preprint, Ecole Polytechnique, Palaiseau, 1987.

[K–T] H.T. Kung, J.F. Traub: *All algebraic functions can be computed fast, Journal ACM* 25 (1978) 245–260.

[Ma] D. Maurer: *Der algorithmus von Coates,* Dipolomarbeit, Universität des Saarlandes (1981–1982).

[Ne] I. Newton: *La méthode des fluxions et des suites infinies,* traduit par M. de Buffon, Librairie Albert Blanchard, Paris (1966).

[Ph] F. Pham: *Singularités des courbes planes: une introduction à la géométrie analytique complexe,* Cours de 3e cycle, Paris (1969–70).

[Pu] V. Puiseux: *Recherches sur les fonctions algébriques*, *J. Math. Pures Appl.* 15 (1850) 365–480.

[To] E. Tournier: *Solutions formelles d'équations différentielles. Le logiciel de calcul formel DESIR. Etude théorique et réalisation*, Thèse d'Etat, Université de Grenoble 1 (1987).

[Tr1] B.M. Trager: *Algebraic factoring and rational function integration*, *SYMSAC'76*, *ACM Inc.* (1976) 219–226.

[Tr2] B.M. Trager: Integration of algebraic functions, Ph.D. Thesis, MIT, (1985).

[Wa] R.J. Walker: *Algebraic curves*, Dover Publ. (1950).