Simultaneous Monomialization

Julie Decaup
Institute of Mathematics, National Autonomous University of Mexico, Unidad Cuernavaca, Mexico
Email: julie.decaup@im.unam.mx

Abstract: We give a proof of the simultaneous monomialization Theorem in zero characteristic for rings essentially of finite type over a field and for quasi-excellent rings. The methods develop the key elements theory that is a more subtle notion than the notion of key polynomials.
***Keywords*:** valuations, monomialization, key polynomials

1. Introduction

The resolution of singularities can be formulated in the following way.

Let V be a singular variety. The variety V admits a resolution of singularities if there exists a smooth variety W and a proper birational morphism $W \to V$.

This problem has been solved in many cases but remains an open problem in others. In characteristic zero Hironaka proved resolution of singularities in all dimensions ([33]) in 1964. Much work has been done since 1964 to simplify and better understand resolution of singularities in characteristic zero. We mention [7-10, 12-15,17-20, 26, 32, 44-46, 50], and [52].

The problem remains open in positive characteristic. The first proof for surfaces is due to *S*. Abhyankar in 1956[1] with subsequent strengthenings by *H*. Hironaka[34] and J. Lipman[37] to the case of more general 2-dimensional schemes, with Lipman giving necessary and sucient condition for a 2-dimensional scheme to admit a resolution of singularities. See also [25]. Still, Abhyankar's proof is extremely technical and dicult and comprises a total of 508 pages ([2-6]). For a more recent and more palatable proof we refer the reader to [27]. It was not until much later that *V*. Cossart and O. Piltant settled the problem of resolution of threefolds in complete generality (their theorem holds for arbitrary quasi-excellent noetherian schemes of dimension three, including the arithmetic case) in a series of three long papers spanning the years 2008 to 2019 [21], [22] and [23]. To try to solve the problem of resolution of singularities numerous methods were introduced, in particular Zariski and Abhyankar used the local uniformization. But it does not allow at the moment to solve completely the problem.

We are interested in a stronger problem than the local uniformization: the mono-mialization problem. In this work we solve the monomialization problem in characteristic zero. We hope that these methods, applicable in positive characteristic, may help to attack the global problem of resolution of singularities on a different point of view.

One of the essential tools to handle the monomialization or the local uniformiza-tion is a valuation. Let us look on an example how valuations naturally fit into the problem.

Let V be a singular variety and Z be an irreducible closed set of V.

If we knew how to resolve the singularities of V, we would have a smooth variety W and a proper birational morphism $W \to V$. In W, we can consider an irreducible set Z' whose image is Z. And so the regular local ring $\mathcal{O}_{W,Z'}$ dominates the non regular local ring $\mathcal{O}_{V,Z}$. It mems that we have an inclusion $\mathcal{O}_{V,Z} \subseteq \mathcal{O}_{W,Z'}$ and the maximal ideal of $\mathcal{O}_{V,Z}$ is the intersection of those of $\mathcal{O}_{W,Z'}$ with $\mathcal{O}_{V,Z}$. Up to a blow-up Z' is a hypersurface and so $\mathcal{O}_{W,Z'}$ is dominated by a discrete valuation ring. In this case the valuation is the order of vanishing along the hypersurface.

Before stating the local uniformization Theorem, we need a classical notion that will be very important: the center of a valuation. For details, we can read ([54]) or ([47, sections 2 and 3]).

Let K be a field and ν be a valuation defined over K. We set

$$R_\nu := \{x \in K \text{ such that } \nu(x) \geq 0\},$$

DOI: https://doi.org/10.37256/cm.152020329

the valuation ring of v, and $\mathfrak{m}_v$ its maximal ideal.

We consider a subring A of K such that $A \subset R_v$. Then the center of v in A is the ideal $\mathfrak{p}$ of A such that $\mathfrak{p} = A \cap \mathfrak{m}_v$.

Now we consider an algebraic variety V over a field k and K its fractions field. Assume V is an affine variety. Then V = Spec (A) where A is a finite type integral k-algebra with $A \subseteq K$. If $A \subseteq R_v$, then the center of v over V is the point ζ of V which corresponds to the prime ideal $A \cap \mathfrak{m}_v$ of A.

The irreducible closed sub-scheme Z of V defined by $A \cap \mathfrak{m}_v$ (it means the image of the morphism $\mathrm{Spec}(\frac{A}{A\cap \mathfrak{m}_v}) \to \mathrm{Spec}(A)$) has a generic point ξ. Equivalently ζ is the point associated to the zero ideal. We say that Z is the center of v over V. Now let us state the local uniformization Theorem. It has been proved in characteristic zero but it is always a conjecture in positive characteristic.

Theorem (Zariski[54]). Let X = Spec (A) be an affine variety of fractions field K over a field k.We consider v a valuation over K of valuation ring R_v.

Then A can be embedded in a regular local sub-ring A' essentially of finite type over k and dominated by R_v.

In this work we prove a stronger result: the simultaneous monomialization Theorem. We are going to explain what is the monomialization and what are the objects that we handle.

Let k be a field of characteristic zero and $f \in k[u_1,\ldots,u_n]$ be a polynomial in n variables, irreducible over k. We denote by $V(f)$ the hypersurface defined by f and we assume that it has a singularity at the origin. Then we set $R := k[u_1,\ldots,u_n]_{(u_1,\ldots,u_n)}$. This is a regular local ring that is essentially of finite type over the field k. The vector $u = (u_1, ..., u_n)$ is a regular system of parameters of R. We use the notation (R, u) to express the fact that u is a regular system of parameters of the regular local ring R.

Definition 4.9 The element f is monomializable if there exists a map

$$(R,u) \to (R', u' = (u'_1, \ldots u'_n))$$

that is a sequence of blow-ups such that the total transform of f is a monomial. It means that in R', the total transform of f is $v\prod_{i=1}^{n}(u'_i)^{\alpha_i}$, with v a unit of R'.

Now we can give a simplified version of one of the main theorems of this work.

Theorem 7.1 Let (R, u) be a regular local ring that is essentially of finite type over a field k of characteristic zero.

Then there exists a countable sequence of blow-ups

$$(R,u) \to \cdots \to (R_i, u^{(i)}) \to \cdots$$

that monomializes simultaneously all the elements of R.

Equivalently, it means that for each element f in R, there exists an index i such that in R_i, f is one monomial.

If f is an irreducible polynomial of k [u_1, ..., u_n], then $A := \frac{R}{(f)}$ is a local domain. We can find a valuation v over Frac (A) centered in R. One consequence of Theorem 7.1 is that the total transform of f in one of the R_i is $v\prod_{j=1}^{n}(u_j^{(i)})^{\alpha_j}$. By the irreducibility of f its strict transform is exactly $u_n^{(i)}$.

Hence there exists an embedding of A into the ring $A' = \frac{R_i}{(u_n^{(i)})}$ which is dominated by R_v. So a consequence of Theorem 7.1 is the Local Uniformization Theorem as announced.

And we obtain a stronger result here: the total transform is a normal crossing divisor. We call this result the embedded local uniformization. We will give a new proof of this theorem in this work.

Let us explain why simultaneous monomialization is a stronger result than the embedded local uniformization Theorem. First we monomialize all the elements of R with the same sequence of blow-ups. Secondly, this sequence is effective and at each step of the process we can express the $u^{(i+1)}$ in terms of the $u^{(i)}$. Indeed, we consider an essentially of finite type regular local ring R, and a valuation centered in R. Thanks to this valuation we construct an effective sequence of blow-ups that monomializes all the elements of R. One more advantage of the proof we give here is that in the essentially of finite type case, we prove the simultaneous embedded local uniformization whatever is the valuation. In particular we do not need any hypothesis on the rank of the valuation.

One of the most important ingredient in the proof of this theorem is the notion of key polynomial. We give here a new definition of key polynomial, introduced by Spivakovsky and appearing for the first time in ([28] and [41]). Let K

be a field, v be a valuation over K and we denote by $\partial_b := \frac{1}{b!}\frac{\partial^b}{\partial X^b}$ the formal derivative of the order b on $K[X]$. For every polynomial $P \in K[X]$, we set

$$\epsilon_v(P) := \max_{b \in \mathbb{N}^*}\left\{\frac{v(P) - v(\partial_b P)}{b}\right\}.$$

Definition 1.7 Let $Q \in K[X]$ be a monic polynomial. The polynomial Q is a key polynomial for v if for every polynomial $P \in K[X]$:

$$\epsilon_v(P) \geq \epsilon_v(Q) \Rightarrow \deg_X(P) \geq \deg_X(Q).$$

One of the interests of this new definition is the following notion:

Definition 2.1 Let Q_1 and Q_2 be two key polynomials. We say that Q_2 is an immediate successor of Q_1 if $\epsilon(Q_1) < \epsilon(Q_2)$ and if Q_2 is of minimal degree for this property. We denote this by $Q_1 < Q_2$.

We denote by M_{Q_1} the of immediate successors of Q_1. We assume that they all have the same degree as Q_1 and that $\epsilon(M_{Q_1})$ does not have any maximal element.

Definition 2.10 We assume that there exists a key polynomial Q' such that $\epsilon(Q') > \epsilon(M_{Q_1})$. We call immediate limit successor of Q_1 every polynomial Q_2 of minimal degree satisfying $\epsilon(Q_2) > \epsilon(M_{Q_1})$, and we denote this by $Q_1 <_{\lim} Q_2$.

Let Q_1 and Q_2 be two key polynomials. Let us write Q_2 according to the powers of Q_1, $Q_2 = \sum_{i=0}^{S} q_i Q_1^i$ where the q_i are polynomials of degree strictly less than Q_1.

We call this expression the Q_1-expansion of Q_2.

An important result in this work, and the only one for which we need the characteristic zero hypothesis, is the following Theorem.

Theorem 2.17 Let Q_2 be an immediate limit suecessor of Q_1. Then the terms of the Q_1-expansion of Q_2 that minimize the valuation are exactly those of degrees 0 and 1.

Then the hypothesis of characteristic zero is necessary also for the results that follow from this theorem.

Here we give an idea of our proof of Theorem 7.1. Let us consider a regular local ring R essentially of Hnite type over a field k of characteristic zero. We fix $u = (u_1, ..., u_n)$ a regular system of parameters of R.

The first ingredient in the proof is the notion of non degeneration.

Definition 3.1 We say that an element f of R is non degenerated with respect to u if there exists an ideal N of R, generated by monomials in u, such that $v(f) = \min_{x \in N}\{v(x)\}$.

The first step is to monomialize all the elements that are non degenerated with respect to a regular system of parameters of R. So let f be an element of R that is non degenerated with respect to u. We construct a sequence of blow-ups

$$(R, u) \to \cdots \to (R', u')$$

such that the strict transform of f in R' is a monomial in u'.

There exist elements f of R that are not non degenerated with respect to u. So we wonder if we could find a sequence of blow-ups

$$(R, u) \to \cdots \to (T, t)$$

such that f is non degenerated with respect to t. If we can, after a new sequence of blow-ups, we monomialize f. Doing this for all the elements of R would would be too complicated. So we would want to find a sequence of blow-ups $(R, u) \to \cdots \to (R', u')$ such that all the elements of R are non degenerated with respect to u'. It is a little optimistic and we need to do something more subtle. We will find an infinite sequence of blow-ups

$$(R, u)\ (R_1, u^{(1)}) \to \cdots \to (R_i, u^{(i)}) \to \cdots$$

such that for each element f of R, there exists i such that f is non degenerated with respect to $u^{(i)}$.

For this, we need the second main ingredient: the key polynomials.

We construct a sequence of key polynomials $(Q_i)_i$ such that each element f of R is non degenerated with respect to some Q_i. It means that:

$$\forall f \in R, \exists i \text{ such that } \nu(f) = \nu_{Q_i}(f).$$

We construct the sequence $(Q_i)_i$ step by step. We require the following properties for this sequence: for every index i, the polynomial Q_{i+1} is an (eventually limit) immediate successor of Q_i. Furthermore the sequence $(\epsilon(Q_i))_i$ is cofoial in $\epsilon(\Lambda)$ where Λ is the set of key polynomials of the extension $k(u_1,...,u_{n-1})(u_n)$.

Equivalently it means:

$$\begin{cases} \forall i, Q_i < Q_{i+1} \text{ or } Q_i <_{\lim} Q_{i+1}, \\ \forall Q \in \Lambda \ \exists i \text{ such that } \epsilon(Q_i) \geq \epsilon(Q). \end{cases}$$

Assume now that we can construct a sequence of blow-ups

$$(R, u) \to \cdots \to (R_j, u^{(j)}) \to \cdots$$

such that all the Q_i belong to a regular system of parameters. It means that

$$\forall i, \exists j, k \text{ such that } Q_i^{\text{strict},j} = u_k^{(j)},$$

where $Q_i^{\text{strict},j}$ is the strict transform of Q_i in R_j. Then every element f of R which is non degenerated with respect to Q_i is non degenerated with respect to $u^{(j)}$. Thus it is monomializable. So the next step is to monomialize all the Q_i.

In order to do this once again we have to be subtle. The notion of key polynomial is not stable by blow-up, so we need a better notion: the notion of key element. Let (Q_i, Q_{i+1}) a couple of (eventually limit) immediate successors of our sequence. We consider $Q_{i+1} = \sum_{j=0}^{s} q_j Q_i^j$ the Q_i-expansion of Q_{i+1}. Then we associate to Q_{i+1} a key element Q'_{i+1} defined as follows.

Definition 3.11 An element $Q'_{i+1} = \sum_{j=0}^{s} a_j q_j Q_i^j$ where the a_j are units is called a key element associated to Q_{i+1}.

In fact we also have a notion of (eventually limit) immediate successors in this case.

Definition 3.13 and 3.14 Let P'_1 and P'_2 be two key elements. We say that P'_1 and P'_2 are (eventually limit) immediate successors key elements if their respective associated key polynomials P_1 and P_2 are such that $P_1 < P_2$ (eventually $P_1 <_{\lim} P_2$).

After some blow ups we prove that (eventually limit) immediate successors become (eventually limit) immediate successors key elements. So we monomialize these key elements. For this we construct a sequence of blow-ups

$$(R, u) \to \cdots \to (R_s, u^{(s)}) \to \cdots$$

that monomializes all the key polynomials Q_i. More precisely, for every index i there exists an index S_i such that in R_{s_i}, Q_i is a monomial in $u^{(s_i)}$ up to a unit of R_{s_i}.

So in the case of essentially of finite type regular local rings, no matter the rank of the valuation is, we prove the embedded local uniformization Theorem. And we do this using only a sequence of blow-ups for all the elements of the ring, and in an effective way. It means that every blow-up is effective and we know how to express all the systems of coordinates.

Then we want to prove the same kind of result over more general rings, even if it means adding conditions on the valuation. We work with quasi excellent rings. Indeed, Grothendieck and Nagata showed that there is no resolution of singularities for rings that are not quasi excellent.

The second main result of this paper can be express in the following simplified form.

Theorem 12.3 Let R be a noetherian quasi excellent complete regular local ring and ν be a valuation centered in R.

Assume that v is of rank 1, or of rank 2 but composed with a discrete valuation, and that car $(k_v) = 0$.

There exists a countable sequence of blow-ups

$$(R, u) \to \cdots \to (R_l, u^{(l)}) \to \cdots$$

that monomializes all the element of R.

So let R be a quasi excellent local domain. This time R is not assume to be of finite type, so we cannot repeat what we did before. We need to introduce one more ingredient: the implicit prime ideal.

Let v be a valuation of the fractions field of R centered in R. We call implicit prime ideal of R asociated to v the ideal of the completion $\hat{R}$ of R defined by:

$$H := \bigcap_{\beta \in \nu(R \setminus \{0\})} P_\beta \hat{R}$$

where $P_\beta := \{f \in R \text{ such that } \nu(f) \geq \beta\}$.

One can show that in this case desingularizing R means desingularizing $\hat{R}$. In the last part of this work we also prove that to desingularize $\hat{R}$, we only need to desingularize $\hat{R}_H$ and (up to one more sequence of blow-ups) $\frac{\hat{R}}{H}$. We prove that the implicit prime ideal satisfies the property that $\hat{R}_H$ is regular. So we only have to desingularize $\frac{\hat{R}}{H}$ and this is done by Theorem 11.2.

2. Key polynomials

The notion of key polynomials was first introduced by Saunders Mac Lane in 1936, in the case of discrete valuations of rank 1. The first motivation to introduce this notion was to describe all the extensions of a valuation to a field extension. Let $K \to L$ be an extension of field and v a valuation on K. We consider a valuation μ that extends v to L. In the case where v is of rank 1 and where L is a simple algebraic extension of K, Mac Lane created the notion of key polynomial for μ. He also created the notion of augmented valuations. Given a valuation μ and Q a key polynomial of Mac Lane, we write $f = \sum_{i=0}^{r} f_j Q^j$ the Q-expansion of an element $f \in K[X]$. An augmented valuation μ' of μ is the on defined by $\mu'(f) = \min_{0 \leq j \leq r} \{\mu(f_j) + j\delta\}$ where $\delta > \mu(Q)$. He proved that μ is the limit of a family of augmented valuations over the ring $K[x]$. Michel Vaquié extended this definition to arbitrary valued field K, without assuming that v is discrete. The most important difierence between these notions is the fact that those of Vaquié involves limit key polynomials while those of Mac Lane not.

More recently, the notion of key polynomials has been used by Spivakovsky to study the local uniformization problem, and to do this he created a new notion of key polynomials. It is the one we use here.

2.1 Key polynomials of Spivakovsky et al

For some results of this part, we refer the reader to [28], but we recall the definitions and properties used in this work to have a selfcontained manuscript.

First, recall the definition of a valuation.

Definition 1.1 Let R be a commutative domain with a unit element, K be a commutative field and Γ be a totally ordered abelian group. We set $\Gamma_\infty := \Gamma \cup \{+\infty\}$.

A valuation of R is a map

$$\nu : R \to \Gamma_\infty$$

such that:

(1) $\forall x \in R, \nu(x) = +\infty \Leftrightarrow x = 0,$

(2) $\forall (x, y) \in R^2, \nu(xy) = \nu(x) + \nu(y),$

(3) $\forall (x, y) \in R^2, \nu(x + y) \geq \min\{\nu(x), \nu(y)\}.$

Example 1.2 The map $\nu_1 : \mathbb{C}[x] \to \mathbb{Z} \cup \{+\infty\}$ which sends a polynomial $P = \sum_{i=0}^{d} p_i x^i$ to $\min\{i \text{ such that } p_i \neq 0\}$ is a valuation.

Example 1.3 We want to define a valuation ν_2 on $\mathbb{C}(x, y, z)$. The value of a quotient $\frac{P}{Q}$ is $\nu_2(P) - \nu_2(Q)$.

And we define the value of a polynomial $P = \sum_i p_i x^{i_1} y^{i_2} z^{i_3}$ as the minimal of the values of $p_i x^{i_1} y^{i_2} z^{i_3}$.

Then we only have to define the values of the generators x, y and z.

Hence the map $\nu_2 : \mathbb{C}(x, y, z) \to \mathbb{R}_\infty$ which sends x to 1, y to 2π and z to $1 + \pi$ is a valuation.

Example 1.4 Let us set $Q = z^2 - x^2 y$. Every polynomial $P \in \mathbb{C}[x, y, z]$ can be written according to the powers of Q. We write $P = \sum_i p_i Q^i$ with the $p_i \in \mathbb{C}[x, y][z]$ of degree in z strictly less than $\deg_z(Q) = 2$. Assume that the first non zero p_i is P_n.

Then the map $\nu_3 : \mathbb{C}(x, y, z) \to (\mathbb{R}^2, \text{lex})$ which sends P to $(n, V_2(P_n))$ defines a valuation, with ν_2 the valuation defined in Example 1.3.

Let K be a field equipped with a valuation ν and consider a simple transcendental extension

$$K \to K(X)$$

with a valuation ν that extends μ to $K(X)$. We still denote by ν the restriction of ν to $K(X)$.

For every non zero integer b, we set $\partial_b := \frac{1}{b!}\frac{\partial^b}{\partial X^b}$. This is called the formal derivative of order b.

For every polynomial $P \in K[X]$, we set

$$\epsilon_\nu(P) := \max_{b \in \mathbb{N}^*} \left\{ \frac{\nu(P) - \nu(\partial_b P)}{b} \right\}.$$

Remark 1.5 Most of the time we will note $\epsilon(P) := \epsilon_\nu(P)$.

Example 1.6 We consider $\mathbb{C}(x, y)[z]$ and the valuation $\nu := V_3$ defined in Example 1.4.

We have $\nu(z) = (0, 1 + \pi)$ and $\nu(\partial z) = \nu(1) = (0, 0)$. So

$$\epsilon(z) = \max_{b \in \mathbb{N}^*} \left\{ \frac{\nu(z) - \nu(\partial_b z)}{b} \right\} = \frac{\nu(z) - \nu(\partial z)}{1} = \nu(z) = (0, 1 + \pi).$$

Also we have $\nu(x) = (0, 1)$ and $\nu(\partial x) = \nu(0) = (+\infty, +\infty)$ so $\epsilon(x) = (-\infty, -\infty)$. Furthermore $\epsilon(y) = (-\infty, -\infty)$.

Finally, let us compute $\epsilon(Q)$. Recall that $Q = z^2 - x^2 y$. We have $\nu(Q) = (1, 0)$, $\nu(\partial Q) = \nu(2z) = (0, 1 + \pi)$ and $\nu(\partial_2 Q) = \nu(2) = (0,0)$.

$$\text{So } \epsilon(Q) = \max \left\{ \frac{\nu(Q) - \nu(\partial Q)}{1}, \frac{\nu(Q) - \nu(\partial_2 Q)}{2} \right\} = \max \left\{ \frac{(1,0) - (0,1+\pi)}{1}, \frac{(1,0) - (0,0)}{2} \right\} = (1, -1 - \pi).$$

Definition 1.7 Let $Q \in K[X]$ be a monic polynomial. We say that Q is a key polynomial for ν if for every polynomial $P \in K[X]$, we have:

$$\epsilon_\nu(P) \geq \epsilon_\nu(Q) \Rightarrow \deg_X(P) \geq \deg_X(Q).$$

Example 1.8 We consider the same example as in example 1.6.

Let us show that z is a key polynomial. We do a proof by contrapositive. Let P be a polynomial of degree in z strictly less than $\deg_z(z) = 1$. So P does not depend on z. Then we saw that $\epsilon(P) = (-\infty, -\infty)$. So $\epsilon(P) < \epsilon(z)$ and z is a key polynomial.

Now, let us show that $Q = z^2 - x^2 z$ is a key polynomial. So we consider a polynomial P such that $\epsilon(P) \geq \epsilon(Q) = (1, -1 -\pi)$.

Then $\epsilon(P) = (n, *)$ where $n \geq 1$ and $*$ is a scalar. So $\nu(P) = (m, *)$ where $m \geq 1$. Hence $Q^m \mid P$ and so $\deg_z(P) \geq \deg_z(Q)$. We proved that Q is a key polynomial.

We have two key polynomials z and Q and we have $\epsilon(z) < \epsilon(Q)$. One can show that Q is of minimal degree for this property. In this situation we will say that Q is an immediate successor of z.

For every polynomial $P \in K[X]$, we set

$$b_v(P) := \min I(P)$$

where

$$I(P) := \left\{ b \in \mathbb{N}^* \text{ such that } \frac{\nu(P) - \nu(\partial_b P)}{b} = \epsilon_\nu(P) \right\}.$$

Again, if there is no confusion, we will omit the index v.

Let P and Q be two polynomials such that Q is monic. Then P can be written $\sum_{j=1}^{n} p_j Q^j$ with p_j polynomials of degree strictly less than the degree of Q. This expression is unique and is called the Q-expansion of P.

Definition 1.9 Let $(P,Q) \in K[X]^2$ such that Q is monic, and we consider $P = \sum_{j=1}^{n} p_j Q^j$ the Q-expansion of the polynomial P. Then we set $\nu_Q(P) := \min_{0 \le j \le n} \nu(p_j Q^j)$. The map ν_Q is called the Q-truncation of v.

Also we set

$$S_Q(P) := \left\{ j \in \{0, \ldots, n\} \text{ such that } \nu\left(p_j Q^j\right) = \nu_Q(P) \right\}$$

and

$$\delta_Q(P) := \max\left\{ S_Q(P) \right\}.$$

Now, we set

$$\tilde{P}_{\nu,Q} := \sum_{j \in S_Q(P)} p_j Q^j.$$

Remark 1.10 In the general case, ν_Q is not a valuation. But if Q is a key polynomial, we are going to show that ν_Q is a valuation.

In order to do that, we need the next result, which will also be needed for a proof of the fundamental theorem 2.17.

Lemma 1.11 Let $t \in \mathbb{N}_{>1}$ and Q be a key polynomial. We consider $P_1, \ldots, P_t$ some polynomials of $K[X]$ all of degree strictly less than deg (Q) and we set $\prod_{i=1}^{t} P_i := qQ + r$ the Euclidean division of $\prod_{i=1}^{t} P_i$ by Q in $K[X]$. Then:

$$\nu(r) = \nu\left(\prod_{i=1}^{t} P_i\right) < \nu(qQ).$$

Proof. We use induction on t.

Base of the induction: $t = 2$. So we want to show that $\nu(P_1 P_2) < \nu(qQ)$.

Indeed, if $\nu(P_1 P_2) < \nu(qQ)$, then

$$\begin{aligned} \nu(R) &= \nu(P_1 P_2 - qQ) \\ &= \nu(P_1 P_2) \\ &< \nu(qQ) \end{aligned}$$

and we have the result.

Assume, aiming for contradiction, that $v(P_1 P_2) > v(qQ)$ and so $v(R) \geq v(qQ)$. Since Q is a key polynomial, every polynomial P of degree strictly less than $\deg(Q)$ satisfies $\epsilon(P) < \epsilon(Q)$. In particular, for every non-zero integer j, we have $v(P) - v(\partial_j P) < j\epsilon(Q)$. So it is the case for P_1, P_2 and r. Since P_1 and P_2 are of degree strictly less than $\deg(Q)$, we have

$$\begin{aligned}\deg_X(P_1 P_2) &= \deg_X(P_1) + \deg_X(P_2) \\ &< 2\deg_X(Q).\end{aligned}$$

However, $\deg_X(P_1 P_2) = \deg_X(qQ) = \deg_X(q) + \deg_X(Q)$. So q is of degree strictly less than $\deg(Q)$ too, and then q satisfies, for every non-zero integer j: $v(q) - v(\partial_j q) < j\epsilon(Q)$. We are going to compute $v(\partial_{b(Q)}(qQ))$ in two different ways to get a contradiction.

First,

$$v\left(\partial_{b(Q)}(qQ)\right) = v\left(\sum_{j=0}^{b(Q)}\left(\partial_{b(Q)-j}(Q)\partial_j(q)\right)\right).$$

Look at the first term of the sum: $q\partial_{b(Q)}(Q)$, and compute its value $v(q\partial_{b(Q)}(Q))$. We are going to show that its value is the smallest of the sum.

We have

$$\begin{aligned}v(q\partial_{b(Q)}(Q)) &= v(q) + v(\partial_{b(Q)}(Q)) \\ &= v(q) + v(Q) - b(Q)\epsilon(Q)\end{aligned}$$

by definition of $b(Q)$. But we know that for every non-zero integer j, we have $v(q) < j\epsilon(Q) + v(\partial_j q)$, so

$$\begin{aligned}v(q\partial_{b(Q)}(Q)) &< (j - b(Q))\epsilon(Q) + v(Q) + v(\partial_j q) \\ &\leq v(\partial_j q) + v(\partial_{b(Q)-j} Q)\end{aligned}$$

Then $q\partial_{b(Q)}(Q)$ is the term of smallest value in the sum. In particular,

$$\begin{aligned}v(\partial_{b(Q)}(qQ)) &= v(q\partial_{b(Q)}(Q)) \\ &= v(q) + v(\partial_{b(Q)}(Q)) \\ &= v(qQ) - b(Q)\epsilon(Q). \qquad (1)\end{aligned}$$

Now we compute this value in a different way. We have:

$$\begin{aligned}v(\partial_{b(Q)}(qQ)) &= v(\partial_{b(Q)}(P_1 P_2 - r)) \\ &= v(\partial_{b(Q)}(P_1 P_2) - (\partial_{b(Q)}(r)) \\ &\geq \min\{v(\partial_{b(Q)}(P_1 P_2)), v(\partial_{b(Q)}(r))\}.\end{aligned}$$

But also:

$$\nu\left(\partial_{b(Q)}\left(P_1P_2\right)\right)=\nu\left(\sum_{j=0}^{b(Q)}\partial_j\left(P_1\right)\partial_{b(Q)-j}\left(P_2\right)\right)$$

$$\geq \min_{0\leq j\leq b(Q)}\left\{\nu\left(\partial_j P_1\right)+\nu\left(\partial_{b(Q)-j}\left(P_2\right)\right)\right\}.$$

If $j \neq 0$, we have $\nu(P_1) < j\epsilon(Q) + \nu(\partial_j(P_1))$ and so

$$\nu(\partial_j(P_1)) > \nu(P_1) - j\epsilon(Q)$$

since $\deg_X(P_1) < \deg_X(Q)$. If $0 \leq j < b(Q)$, we also have

$$\nu(\partial_{b(Q)-j}(P_2)) > \nu(P_2) - (b(Q) - j)\,\epsilon(Q).$$

So if $0 < j < b(Q)$, we have

$$\nu(\partial_j P_1) + \nu(\partial_{b(Q)-j}(P_2)) > \nu(P_1P_2) - b(Q)\,\epsilon(Q).$$

This inequality stays true if $j = 0$ and $j = b(Q)$, so:

$$\nu(\partial_{b(Q)}(P_1P_2)) > \nu(P_1P_2) - b(Q)\,\epsilon(Q).$$

By hypothesis, $\nu(P_1P_2) \geq \nu(qQ)$, so

$$\nu(\partial_{b(Q)}(P_1P_2)) > \nu(qQ) - b(Q)\,\epsilon(Q).$$

But since r is of degree strictly less than deg(Q), we know that $\nu(\partial_{b(Q)}(r)) > \nu(r) - b(Q)\,\epsilon(Q)$, and by hypothesis $\nu(r) \geq \nu(qQ)$. Then $\nu(\partial_{b(Q)}(r)) > \nu(qQ) - b(Q)\,\epsilon(Q)$.

So

$$\nu(\partial_{b(Q)}(qQ)) \geq \min\{\nu(\partial_{b(Q)}(P_1P_2)), \nu(\partial_{b(Q)}(r))\}$$

$$> \nu(qQ) - b(Q)\,\epsilon(Q)$$

which contradicts (1). So we do have $\nu(r) = \nu(P_1P_2) < \nu(qQ)$, and this completes the proof of the base of the induction.

We now assume the result true for $t - 1 \geq 2$ and we are going to show it for t.

We set $P := \prod_{i=1}^{t-1} P_i$.

Let

$$P = q_1Q + r_1$$

be the Euclidean division of P by Q and

$$r_1P_t = q_2Q + r_2$$

be that of r_1P_t by Q. Since $PP_t = qQ + r$, we have $r = r_2$ and $q = q_1P_t + q_2$.

By the induction hypothesis, $\nu(r_1) = \nu(P) < \nu(q_1Q)$. In particular,

$$\nu\left(r_1P_t\right)=\nu\left(\prod_{i=1}^{t}P_i\right)<\nu\left(q_1P_tQ\right).$$

Since the polynomials r_1 and P_t are both of degree strictly less than deg (Q), we can apply the base of the induction and so

$$v\,(r_1P_t) = v\,(r_2) < v\,(q_2Q).$$

So $v(r) = v(r_2) = v(r_1P_t) = v(\prod_{i=1}^{t} P_i)$ and furthermore this value is strictly less than both $v\,(q_1P_tQ)$ and than $v\,(q_2Q)$. So it is strictly less than the minimum, which is less then or equal to $v\,(q_1P_tQ + q_2Q)$ by definition of a valuation. So

$$v(r) = v\left(\prod_{i=1}^{t} P_i\right)$$

$$< v\,((q_1P_t + q_2)Q)$$

$$= v\,(qQ)$$

which completes the proof.

Theorem 1.12 Let Q be a key polynomial. The map v_Q is a valuation.

Proof. The only thing we have to prove is that for every $(P_1, P_2) \in K[X]^2$, and we have

$$v_Q\,(P_1P_2) = v_Q\,(P_1) + v_Q\,(P_2).$$

First case: P_1 and P_2 are both of degree strictly less than deg (Q). Then $v_Q\,(P_1) = v\,(P_1)$ and $v_Q\,(P_2) = v\,(P_2)$. Since v is a valuation, we have $v\,(P_1P_2) = v\,(P_1) + v\,(P_2)$.

Then, $v\,(P_1P_2) = v_Q\,(P_1) + v_Q\,(P_2)$. Sinee P_1 and P_2 are both of degree strictly less than deg(Q), by previous Lemma, we have $v_Q\,(P_1P_2) = v\,(P_1P_2)$ and we are done.

Second case: $P_1 = p_i^{(1)}Q^i$ and $P_2 = p_j^{(2)}Q^j$ with $p_i^{(1)}$ and $p_j^{(2)}$ both of degree strictly less than deg (Q).

Let $p_i^{(1)}p_j^{(2)} = qQ + r$ be the Euclidean division of $p_i^{(1)}p_j^{(2)}$ by Q. Sinee $\deg_X(p_i^{(1)}p_j^{(2)}) < 2\deg_X(Q)$, we know that $\deg_X(q) < \deg_X(Q)$, and by definition of the Euclidean division, we have $\deg_X(r) < \deg_X(Q)$. So $P_1P_2 = qQ^{i+j+1} + rQ^{i+j}$ is the Q-expansion of P_1P_2.

We are going to prove that in this case we still have

$$v_Q\,(P_1P_2) = v\,(P_1P_2),$$

and since v is a valuation, we will have the result. We have:

$$v_Q\,(P_1P_2) = v_Q\,(qQ^{i+j+1} + rQ^{i+j})$$

$$= \min\{v\,(qQ^{i+j+1}),\, v\,(rQ^{i+j})\}$$

$$= \min\{v\,(qQ) + v\,(Q^{i+j}),\, v\,(r) + v\,(Q^{i+j})\}.$$

However, we can apply thee previous Lemma to the product

$$p_i^{(1)}p_j^{(2)} = qQ + r$$

and conclude that $v\,(r) = v\,(p_i^{(1)}p_j^{(2)}) < v\,(qQ)$.

Then

$$vQ\,(P_1 P_2) = \nu\,(r) + \nu\,(Q^{i+j})$$

$$= \nu\,(p_i^{(1)} p_j^{(2)}) + \nu\,(Q^{i+j})$$

$$= \nu\,(P_1 P_2)$$

and we have the result.

Last case: general case. Since we only look at the terms of smallest value, we can replace P_1 by

$$\left(\tilde{P}_1\right)_{\nu,Q} = \sum_{j \in S_Q(P_1)} p_j^{(1)} Q^j$$

and P_2 by

$$\left(\tilde{P}_2\right)_{\nu,Q} = \sum_{i \in S_Q(P_2)} p_i^{(2)} Q^i.$$

We know that

$$\nu_Q\,(P_1 + P_2) \geq \min\{\, \nu_Q\,(P_1), \nu_Q\,(P_2)\}$$

and

$$\nu_Q\,(p_j^{(1)} Q^j p_i^{(2)} Q^i) = \nu_Q\,(p_j^{(1)} Q^j) + \nu_Q\,(p_i^{(2)} Q^i).$$

So

$$\nu_Q\left(P_1 P_2\right) = \nu_Q\left(\sum p_j^{(1)} p_i^{(2)} Q^{j+i}\right)$$

$$\geq \min\left\{\nu_Q\left(p_j^{(1)} Q^j\right) + \nu_Q\left(p_i^{(2)} Q^i\right)\right\}.$$

However

$$\nu_Q\left(p_j^{(1)} Q^j\right) = \nu\left(p_j^{(1)} Q^j\right) = \nu_Q\left(P_1\right)$$

and

$$\nu_Q\left(p_i^{(2)} Q^i\right) = \nu\left(p_i^{(2)} Q^i\right) = \nu_Q\left(P_2\right).$$

So $\nu_Q\,(P_1 P_2) \geq \nu_Q\,(P_1) + \nu_Q\,(P_2)$ and we only have to show that it is an equality. In order to do that, it is enough to find a term in the Q-expansion of $P_1 P_2$ whose value is exactly $\nu_Q\,(P_1) + \nu_Q\,(P_2)$ Let us consider the term of smallest value in each Q-expansion, so let us consider $p_{n_1}^{(1)} Q^{n_1}$ and $p_{m_2}^{(2)} Q^{m_2}$, where $n_1 = \min S_Q\,(P_1)$ and $m_2 = \min S_Q\,(P_2)$.

Let $p_{n_1}^{(1)} p_{m_2}^{(2)} = qQ + r$ be the Euclidean division of $p_{n_1}^{(1)} p_{m_2}^{(2)}$ by Q, which is its Q-expansion too.

By Lemmd 1.11, we have $\nu(r) = \nu(p_{n_1}^{(1)} p_{m_2}^{(2)})$. In fact, in the Q-expansion of $P_1 P_2$, there is the term $rQ^{n_1+m_2}$, and we have:

$$\nu_Q\left(rQ^{n_1+m_2}\right) = \nu\left(rQ^{n_1+m_2}\right)$$

$$= \nu\left(p^{(1)}_{n_1} p^{(2)}_{m_2} Q^{n_1+m_2}\right)$$

$$= \nu_Q(P_1) + \nu_Q(P_2).$$

This completes the proof.

Remark 1.13 For every polynomial $P \in K[X]$, we have

$$\nu_Q(P) \le \nu(P).$$

It will be very important to be able to determine when this inequality is an equality.

A key polynomial P which satisfies the strict inequality and which is of minimal degree for this property will be called an immediate successor of Q (Definition 2.1). We will study these polynomials in more details in this work. First, let us concentrate on the equality case.

Definition 1.14 Let Q be a key polynomial and P be a polynomial such that $\nu_Q(P) = \nu(P)$.We say that P is non-degenerate with respect to Q.

Another very important thing is to be able to compare the ϵ of key polynomials. Indeed, if I have two key polynomials Q_1 and Q_2, do I have $\epsilon(Q_1) < \epsilon(Q_2)$, or do I have $\epsilon(Q_1) = \epsilon(Q_2)$? Being able to answer will be crucial. The next four results can be found in [28] but we recall them for more clarity.

Lemma 1.15 For every polynomial $P \in K[X]$ and every stricly positive integer d, we have :

$$\nu_Q(\partial_d P) \ge \nu_Q(P) - d\epsilon(Q)$$

Proof. We consider the Q-expansion $P = \sum_{i=0}^{n} p_i Q^i$ of P.

Assume we have the result for $p_i Q^i$. It means that

$$\nu_Q(\partial_d(p_i Q^i)) \ge \nu_Q(p_i Q^i) - d\epsilon(Q)$$

for every index i. Then:

$$\begin{aligned}
\nu_Q(\partial_d P) &= \nu_Q\left(\partial_d\left(\sum_{i=0}^{n} p_i Q^i\right)\right)\\
&= \nu_Q\left(\sum_{i=0}^{n} \partial_d\left(p_i Q^i\right)\right)\\
&\ge \min_{0\le i\le n} \nu_Q\left(\partial_d\left(p_i Q^i\right)\right)\\
&\ge \min_{0\le i\le n}\left\{\nu_Q\left(p_i Q^i\right) - d\epsilon(Q)\right\}\\
&\ge \min_{0\le i\le n}\left\{\nu_Q\left(p_i Q^i\right)\right\} - d\epsilon(Q)\\
&\ge \nu_Q(P) - d\epsilon(Q)
\end{aligned}$$

and the proof is finished.

So we just have to prove the result for $P = p_i Q^i$.

First, we know that $\nu_Q(\partial_d(Q) \ge \nu_Q(Q) - d\epsilon(Q)$. Now we will prove that we have the result for $P = p_i$. Then we will conclude by showing that if we have the result for two polynomials, we have the result for the product.

So let us prove the result for $P = p_i$.

Since $\deg_X(p_i) < \deg_X(Q)$ and since Q is a key polynomial, we have $\epsilon(p_i) < \epsilon(Q)$. So, for every strictly positive integer d, we have:

$$
\begin{aligned}
v_Q(\partial_d p_i) &= v(\partial_d p_i)\\
&\geq v(p_i) - d\epsilon(p_i)\\
&= v_Q(p_i) - d\epsilon(p_i)\\
&> v_Q(p_i) - d\epsilon(Q).
\end{aligned}
$$

Now, it just remains to prove that if we have the result for two polynomials P and S, then we have it for PS. Assume the result proven for P and S. Then:

$$
\begin{aligned}
v_Q(\partial_d(PS)) &= v_Q\left(\sum_{r=0}^{d}\partial_r(P)\partial_{d-r}(S)\right)\\
&\geq \min_{0\leq r\leq d}\left\{v(\partial_r(P)) + v(\partial_{d-r}(S))\right\}\\
&\geq \min_{0\leq r\leq d}\left\{v_Q(P) - r\epsilon(Q) + v_Q(S) - (d-r)\epsilon(Q)\right\}\\
&\geq v_Q(PS) - d\epsilon(Q)
\end{aligned}
$$

This completes the proof.

Proposition 1.16 Let Q be a key polynomial and $P \in K[X]$ a polynomial such that $S_Q(P) \neq \{0\}$.
Then there exists a strictly positive integer b such that

$$
\frac{v_Q(P) - v_Q(\partial_b P)}{b} = \epsilon(Q).
$$

Proof. First, by Lemma 1.15, we can replace P by $\tilde{P}_{v,Q} = \sum_{i\in S_Q(P)} p_i Q^i$.

We want to show the existence of a strictly positive integer b such that $v_Q(P) - v_Q(\partial_b P) = b\epsilon(Q)$.

Since $S_Q(P) \neq \{0\}$, we can consider the smallest non-zero element l of $S_Q(P)$. We write $l = p^e u$, with $p \nmid u$.

We are going to prove that we have the desired equality for the integer $b := p^e b(Q) > 0$. To do this, we need to compute $\partial_b(P)$, it is the objective of the following technical lemma.

Lemma 1.17 We have $\partial_b(P) = urQ^{l-p^e} + Q^{l-p^e+1}R + S$, where:

(1)The polynomial r is the remainder of the Euclidean division of $p_l(\partial_{b(Q)}Q)^{p^e}$ by Q,

(2)The polynomials R and S satisfy

$$
v_Q(S) > v_Q(P) - b\epsilon(Q).
$$

Proof. First let us show that the Lemma is true for $P = p_l Q^l$ and that for every $j \in S_Q(P)\setminus\{l\}$, we have

$$
\partial_b(p_j Q^j) = Q^{l-p^e+1}R_j + S_j,
$$

where R_j and S_j are two polynomials, and where $v_Q(S_j) > v_Q(P) - b\epsilon(Q)$.

So we consider $j \in S_Q(P)$. We set

$$
M_j := \left\{B_s = (b_0,\ldots,b_s) \in \mathbb{N}^{s+1} \text{ such that } \sum_{i=0}^{s} b_i = b \text{ and } s \leq j\right\}.
$$

The generalized Leibniz rule tells us that:

$$
\partial_b\left(p_j Q^j\right) = \sum_{B_s\in M_j}\left(T(B_s)\right)
$$

where

$$\begin{aligned} T\left(B_s\right) &= T\left(\left(b_0,\ldots,b_s\right)\right) \\ &= C\left(B_s\right)\partial_{b_0}\left(p_j\right)\left(\prod_{i=1}^{s}\partial_{b_i}\left(Q\right)\right)Q^{j-s} \end{aligned}$$

with $C(B_s)$ some elements of K whose exact value can be found in [35]. We set

$$\alpha := \left(0, b(Q), \ldots, b(Q)\right) \in \mathbb{N}^{p^e+1}.$$

Recall that $I(Q) = \{d \in \mathbb{N}^* \text{ such that } \frac{\nu(Q)-\nu(\partial_d Q)}{d} = \epsilon(Q)\}$. We set

$$N_j := \left\{B_s = \left(b_0,\ldots,b_s\right) \in M_j \text{ such that } b_0 > 0 \text{ or } \left\{b_1,\ldots,b_s\right\} \not\subseteq I(Q)\right\},$$

$$S_j := \sum_{B_s \in N_j} T\left(B_s\right)$$

and finally we set

$$Q^{l-p^e+1}R_j := \begin{cases} \sum_{B_s \in M_j \setminus N_j} T\left(B_s\right) & \text{if } j \neq l \\ \sum_{B_s \in M_j \setminus \left(N_j \cup \{\alpha\}\right)} T\left(B_s\right) & \text{if } j = l \end{cases}.$$

If $j = l$, the term $T(\alpha)$ appears $\binom{l}{p^e} = u$ times in $\partial_b\left(p_l Q^l\right)$. Equivalently, $C(\alpha) = u$ and so

$$\begin{aligned} T(\alpha) &= u p_l \left(\partial_{b(Q)} Q\right)^{p^e} Q^{l-p^e} \\ &= u\left(qQ + r\right)Q^{l-p^e} \end{aligned}$$

where $qQ + r$ is the Euclidean division of $p_l(\partial_{b(Q)}Q)^{p^e}$ by Q.

In other words

$$T(\alpha) = \underbrace{uq}_{:=R_0} Q^{l-p^e+1} + urQ^{l-p^e}.$$

So if $j \neq l$, then $\partial_b(p_j Q^j) = Q^{l-p^e+1}R_j + S_j$. It remains to prove that $\nu_Q(S_j) > \nu_Q(p_j Q^j) - b\epsilon(Q)$. But:

$$\begin{aligned} \nu_Q\left(S_j\right) &= \nu_Q\left(\sum_{B_s \in N_j} T\left(B_s\right)\right) \\ &= \nu_Q\left(\sum_{B_s \in N_j} C\left(B_s\right)\partial_{b_0}\left(p_j\right)\left(\prod_{i=1}^{s}\partial_{b_i}\left(Q\right)\right)Q^{j-s}\right) \\ &\geq \min_{B_s \in N_j}\left\{\nu\left(\partial_{b_0}\left(p_j\right)\right) + \sum_{i=1}^{s}\nu\left(\partial_{b_i}\left(Q\right)\right) + \left(j-s\right)\nu\left(Q\right)\right\}. \end{aligned}$$

Since $B_s \in N_j$, we have two options. The first is $b_0 = 0$ and $\{b_1,\dots,b_s\} \not\subseteq I(Q)$. In other words for every $i \in \{1,\dots,s\}$ we have $\nu(\partial_{b_i}(Q)) \geq \nu(Q) - b_i\epsilon(Q)$. And then the inequality is strict for at least one index $i \in \{1,\dots,s\}$. The second option is $b_0 > 0$ and then

$$\frac{\nu\left(p_j\right)-\nu\left(\partial_{b_0}\left(p_j\right)\right)}{b_0} \leq \epsilon\left(p_j\right) < \epsilon(Q)$$

because $\deg_X(p_j) < \deg_X(Q)$ and Q is a key polynomial. Equivalently,

$$\nu\left(\partial_{b_0}\left(p_j\right)\right) > \nu\left(p_j\right) - b_0\epsilon(Q).$$

So if $b_0 = 0$ and $\{b_1,\dots,b_s\} \not\subseteq I(Q)$. we have

$$\underbrace{\nu\left(\partial_{b_0}\left(p_j\right)\right)+\sum_{i=1}^{s}\nu\left(\partial_{b_i}(Q)\right)+(j-s)\nu(Q) > \nu\left(p_j\right)+s\nu(Q)-b\epsilon(Q)+(j-s)\nu(Q).}_{\nu\left(p_jQ^j\right)-b\epsilon(Q)}$$

And if $b_0 > 0$, then

$$\underbrace{\nu\left(\partial_{b_0}\left(p_j\right)\right)+\sum_{i=1}^{s}\nu\left(\partial_{b_i}(Q)\right)+(j-s)\nu(Q) > \nu\left(p_j\right)-b_0\epsilon(Q)+s\nu(Q)-\sum_{i=1}^{s}b_i\epsilon(Q)+(j-s)\nu(Q).}_{\nu\left(p_jQ^j\right)-b\epsilon(Q)}$$

So:

$$\begin{aligned}\nu_Q\left(S_j\right) &> \min_{B_s\in N_j}\left\{\nu\left(p_jQ^j\right)-b\epsilon(Q)\right\}\\ &> \nu_Q(P)-b\epsilon(Q)\end{aligned}$$

If $j = l$, then

$$\partial_b\left(p_lQ^l\right) = \left(R_0+R_l\right)Q^{l-p^e+1}+S_l+urQ^{l-p^e}$$

hand using the same argument as before, $\nu_Q(S_l) > \nu_Q(P) - b\epsilon(Q)$. It remains to prove the general case. We have:

$$\begin{aligned}\partial_b(P) &= \partial_b\left(\sum_{i\in S_Q(P)} p_iQ^i\right)\\ &= \partial_b\left(p_lQ^l\right)+\sum_{j\in S_Q(P)\setminus\{l\}}\partial_b\left(p_jQ^j\right).\end{aligned}$$

Then:

$$\begin{aligned}\partial_b(P) &= \left(R_0+R_l\right)Q^{l-p^e+1}+S_l+urQ^{l-p^e}+\sum_{j\in S_Q(P)\setminus\{l\}}\left(Q^{l-p^e+1}R_j+S_j\right)\\ &= urQ^{l-p^e}+Q^{l-p^e+1}R+S\end{aligned}$$

where

$$R := R_0 + \sum_{j \in S_Q(P)} R_j$$

and

$$S := \sum_{j \in S_Q(P)} S_j.$$

We have

$$\nu_Q(S) \geq \min_{j \in S_Q(P)} \{\nu_Q(S_j)\} > \nu_Q(P) - b\epsilon(Q).$$

This completes the proof of the Lemma.
Recall that we want to prove that

$$\nu_Q(\partial_b P) = \nu_Q(P) - b\epsilon(Q).$$

We just saw that the Q-expansion of $\partial_b P$ contains the term urQ^{l-p^e}, some terms divisible by Q^{l-p^e+1} and others of value strictly higher than $\nu_Q(P) - b\epsilon(Q)$. It is sufficient now to show that

$$\nu_Q(\partial_b P) \geq \nu_Q(P) - b\epsilon(Q).$$

and that

$$\nu_Q\left(urQ^{l-p^e}\right) = \nu_Q(P) - b\epsilon(Q).$$

Let us compute $\nu_Q(urQ^{l-p^e})$.

Recall that $p_l(\partial_{b(Q)}Q)^{p^e} = qQ + r$. By Lemma 1.11, we have $\nu(r) = \nu(p_l(\partial_{b(Q)}Q)^{p^e})$.
So:

$$\begin{aligned}
\nu_Q\left(urQ^{l-p^e}\right) &= \nu_Q\left(rQ^{l-p^e}\right) \\
&= \nu\left(rQ^{l-p^e}\right) \\
&= \nu\left(p_l\left(\partial_{b(Q)}Q\right)^{p^e}\right) + \nu\left(Q^{l-p^e}\right) \\
&= \nu\left(p_l Q^l\right) + p^e \nu\left(\partial_{b(Q)}Q\right) - p^e \nu(Q) \\
&= \nu_Q(P) + p^e\left(\nu\left(\partial_{b(Q)}Q\right) - \nu(Q)\right) \\
&= \nu_Q(P) + p^e\left(-b(Q)\epsilon(Q)\right) \\
&= \nu_Q(P) - b\epsilon(Q).
\end{aligned}$$

The result now follows from Lemma 1.15.

Remark 1.18 One can show that the implication of the proposition is, in fact, an equivalence.

Proposition 1.19 Let Q be a key polynomial and P a polynomial such that there exists a strictly positive integer b such that

$$\nu_Q(P) = \nu_Q(\partial_b P) - b\epsilon(Q).$$

and

$$\nu_Q(\partial_b P) = \nu(\partial_b P).$$

Then $\epsilon(P) \geq \epsilon(Q)$.

If, in addition, $\nu(P) > \nu_Q(P)$ then $\epsilon(P) > \epsilon(Q)$.

Proof. We have

$$\begin{aligned}
\epsilon(P) &\geq \frac{\nu(P)-\nu(\partial_b P)}{b} \\
&= \frac{\nu(P)-\nu_Q(\partial_b P)}{b} \\
&= \frac{\nu(P)+b\epsilon(Q)-\nu_Q(P)}{b} \\
&= \epsilon(Q)+\frac{\nu(P)-\nu_Q(P)}{b}.
\end{aligned}$$

We know that for every polynomial P, we have $\nu(P) \geq \nu_Q(P)$, so $\epsilon(P) \geq \epsilon(Q)$. And if $\nu(P) > \nu_Q(P)$, we have the strict inequality $\epsilon(P) > \epsilon(Q)$.

Proposition 1.20 Let Q_1 and Q_2 be two key polynomials such that

$$\epsilon(Q_1) \leq \epsilon(Q_2)$$

and let $P \in K[X]$ be a polynomial.

Then $\nu_{Q_1}(P) \leq \nu_{Q_2}(P)$.

Furthermore, if $\nu_{Q_1}(P) = \nu(P)$, then $\nu_{Q_2}(P) = \nu(P)$.

Proof. First, we show that $\nu_{Q_2}(Q_1) = \nu(Q_1)$. If $\deg_X(Q_1) < \deg_X(Q_2)$, we do have this equality. Otherwise we have $\deg_X(Q_1) = \deg_X(Q_2)$ since $\epsilon(Q_1) \leq \epsilon(Q_2)$ and since Q_1 is a key polynomial.

Assume, aiming for contradiction, that $\nu_{Q_2}(Q_1) < \nu(Q_1)$.

So $S_{Q_2}(Q_1) \neq \{0\}$ and by Proposition 1.16, there exists a non-zero integer b such that $\nu_{Q_2}(Q_1) - \nu_{Q_2}(\partial_b Q_1) = b\epsilon(Q_2)$. However $\deg_X(\partial_b Q_1) < \deg_X(Q_2)$, so $\nu_{Q_2}(\partial_b Q_1) = \nu(\partial_b Q_1)$ and by Proposition 1.19, we have $\epsilon(Q_1) > \epsilon(Q_2)$. This is a contradiction. So we do have $\nu_{Q_2}(Q_1) = \nu(Q_1)$.

Let $P = \sum\limits_{i=0}^{n} p_i Q_1^i$ be the Q_1-expansion of P.

For every $i \in \{0,\ldots,n\}$, we have:

$$\nu_{Q_2}\left(p_i Q_1^i\right) = \nu_{Q_2}(p_i) + i\nu_{Q_2}(Q_1) = \nu_{Q_2}(p_i) + i\nu(Q_1).$$

But $\deg_X(p_i) < \deg_X(Q_1) \leq \deg_X(Q_2)$, so $\nu_{Q_2}(p_i) = \nu(p_i)$ and $\nu_{Q_2}(p_i Q_1^i) = \nu(p_i Q_1^i)$.

Then

$$\begin{aligned}
\nu_{Q_2}(P) &\geq \min_{0 \leq i \leq n}\left\{\nu_{Q_2}\left(p_i Q_1^i\right)\right\} \\
&= \min_{0 \leq i \leq n}\left\{\nu\left(p_i Q_1^i\right)\right\} \\
&= \nu_{Q_1}(P).
\end{aligned}$$

Assume that, in addition, $\nu_{Q_1}(P) = \nu(P)$. Then $\nu(P) \leq \nu_{Q_2}(P)$. By definition of ν_{Q_2}, we have $\nu_{Q_2}(P) \leq \nu(P)$, and hence the equality.

Proposition 1.21 Let $P_1,\dots,P_n \in K[X]$ be pelynemials and set $d := \max_{1\le i\le n}\{\deg_X(P_i)\}$.

There exists a key polynomial Q of degree less than or equal to d such that all the P_i are non-degenerate with respect to Q. In other words, there exists a key polynomial Q such that for every i, we have $\nu_Q(P_i) = \nu(P_i)$.

Proof. Assume the result for only one polynomial and let $n > 1$.

So we have $Q_1, ..., Q_n$ some key polynomials of degrees less than or equal to d such that for every $i \in \{0,\dots,n\}$, the polynomial P_i is non-degenerate with respect to Q_i. In other words $\nu_{Q_i}(P_i) = \nu(P_i)$.

We can assume

$$\epsilon(Q_n) = \max_{1\le i\le n}\{\epsilon(Q_i)\}.$$

By Proposition 1.20, for every $i \in \{1,\dots,n\}$, we have $\nu_{Q_i}(P_i) = \nu(P_i) = \nu_{Q_n}(P_i)$. So all the P_i are non-degenerate with respect to Q_n. This completes the proof.

It remains to show the result for $n = 1$. We give a proof by contradiction. Assume the existence of a polynomial P such that for every key polynomial Q of degree less than or equal to d, we have $\nu_Q(P) < \nu(P)$. We choose P of minimal degree for this property.

Let us show that there exists a key polynomial Q, of degree less than or equal to $d = \deg_X(P)$ such that for every $b > 0$, we have $\nu_Q(\partial_b P) = \nu(\partial_b P)$.

First, for every $b > d$, we have $\partial_b P = 0$. Then, by minimality of the degree of P, for every $b \in \{1,\dots,d\}$, there exists a key polynomial Q_b such that $\nu_{Q_b}(\partial_b P) = \nu(\partial_b P)$.

Take an element $Q \in \{Q_1,\dots,Q_d\}$ such that $\epsilon(Q) = \max_{1\le b\le d}\{\epsilon(Q_b)\}$. By Proposition 1.20, we have $\nu_Q(\partial_b P) = \nu(\partial_b P)$, for every $b > 0$.

So we have $\nu_Q(P) < \nu(P)$. In particular, $S_Q(P) \neq \{0\}$ and $\nu_Q(\partial_b P) = \nu(\partial_b P)$ for every $b > 0$. By Proposition 1.16 and Corollary 1.19, we conclude that $\epsilon(P) > \epsilon(Q)$.

Let us show that this last inequality is true for every key polynomial of degree less than or equal than deg(P). Let Q_0 be such a key polynomial.

First case: $\epsilon(Q_0) \le \epsilon(Q)$. Then $\epsilon(Q_0) < \epsilon(P)$ since $\epsilon(Q) < \epsilon(P)$.

Last case: $\epsilon(Q_0) > \epsilon(Q)$. By Proposition 1.20, we have $\nu(\partial_b P) = \nu_Q(\partial_b P) = \nu_{Q_0}(\partial_b P)$ for every $b > 0$. By hypothesis we know that $\nu_{Q_0}(P) < \nu(P)$. So by Proposition 1.16 and Corollary 1.19, we have $\epsilon(P) > \epsilon(Q_0)$ as desired.

So we know that for every key polynomial of degree less than or equan than those of P, we have $\epsilon(P) < \epsilon(Q)$. But by definition of key polynomials, there exists a key polynomial $\tilde{Q}$ of degree less than or equal than those of P and such that $\epsilon(P) \le \epsilon(\tilde{Q})$Contradiction. This completes the proof.

2.2 Immediate successors

Definition 2.1 Let Q_1 and Q_2 be two key polynomials. We say that Q_2 is an immediate successor of Q_1 and we write $Q_1 < Q_2$ if $\epsilon(Q_1) < \epsilon(Q_2)$ and if Q_2 is of minimal degree for this property.

Remark 2.2 We keep the hypotheses of Example 1.8. Then we have $z < z^2 - x^2y$.

Definition 2.3 It will be useful to have simpler ways to check if a key polynomial is an immediate successor of another key polynomial. This is why we give these two results.

Proposition 2.4 Let Q_1 and Q_2 be two key polynomials. The following are equivalent.

(1) The polynomials Q_1 and Q_2 satisfy $Q_1 < Q_2$.

(2) We have $\nu_{Q_1}(Q_2) < \nu(Q_2)$ and Q_2 is of minimal degree for this property.

Proof. First let us show that

$$\epsilon(Q_1) < \epsilon(Q_2) \Rightarrow \nu_{Q_1}(Q_2) < \nu(Q_2).$$

We set $b := b(Q_2) = \min\{b \in \mathbb{N}^* \text{ such that } \frac{\nu(Q_2)-\nu(\partial_b Q_2)}{b} = \epsilon(Q_2)\}$.

We have

$$\begin{aligned}\epsilon(Q_1) < \epsilon(Q_2) \quad &\Leftrightarrow \quad b\epsilon(Q_1) < \nu(Q_2) - \nu(\partial_b Q_2)\\ &\Rightarrow \quad b\epsilon(Q_1) < \nu(Q_2) - \nu_{Q_1}(\partial_b Q_2)\end{aligned}$$

because for every polynomial g, we have $v_{Q_1}(g) \leq v(g)$.

But by Lemma 1.15, $v_{Q_1}(Q_2) - v_{Q_1}(\partial_b Q_2) \leq b\epsilon(Q_1)$, so

$$v_{Q_1}(Q_2) - v_{Q_1}(\partial_b Q_2) < v(Q_2) - v_{Q_1}(\partial_b Q_2).$$

Then $v_{Q_1}(Q_2) < v(Q_2)$.

Now let us show that $v_{Q_1}(Q_2) < v(Q_2) \Rightarrow \epsilon(Q_1) < \epsilon(Q_2)$. Assume, aiming for contradiction, that $\epsilon(Q_1) \geq \epsilon(Q_2)$. Then $\deg(Q_1) \geq \deg(Q_2)$.

If we have $\deg(Q_1) > \deg(Q_2)$, then $v_{Q_1}(Q_2) = v(Q_2)$ and this is a contradiction. Hence we assume that Q_1 and Q_2 have same degree.

Let $Q_2 = Q_1 + (Q_2 - Q_1)$ be the Q_1-expansion of Q_2.

If $v(Q_1) \neq v(Q_2 - Q_1)$, then

$$v(Q_2) = \min\{(v(Q_1), v(Q_2 - Q_1)\} = v_{Q_1}(Q_2)\}$$

and again we have a contradiction.

So $v(Q_1) = v(Q_2 - Q_1) = v_{Q_1}(Q_2) < v(Q_2)$.

But $v(Q_2) = v_{Q_2}(Q_2) \leq v_{Q_1}(Q_2)$ by Proposition 1.20. Again, this is a contradiction.

So we showed that $\epsilon(Q_1) < \epsilon(Q_2) \Leftrightarrow v_{Q_1}(Q_2) < v(Q_2)$.

Let Q_2 be of minimal degree for the first property.

Assume the existence of Q_3 of degg strictly less than Q_2 such that $v_{Q_1}(Q_3) < v(Q_3)$. So $\epsilon(Q_1) < \epsilon(Q_3)$, which is in contradiction with the minimality of the degree of Q_2 for this property.

So we have $Q_1 < Q_2 \Rightarrow v_{Q_1}(Q_2) < v(Q_2)$ and Q_2 is of minimal degree for this property.

Take Q_2 such that $v_{Q_1}(Q_2) < v(Q_2)$ and Q_2 is of minimal degree for this property. Assume the existence of Q_3 of degree strictly less than $\deg(Q_2)$ and such that $\epsilon(Q_1) < \epsilon(Q_3)$). By this last property, we have $v_{Q_1}(Q_3) < v(Q_3)$, which is in contradiction with the minimality of the degree of Q_2 for this property.

This completes the proof.

Proposition 2.5 Let Q_1 and Q_2 be two key polynomials, and let

$$Q_2 = \sum_{j \in \Theta} q_j Q_1^j$$

be the Q_1-expansion of Q_2.

The following are equivalent:

(1) The polynomials Q_1 and Q_2 satisfy $Q_1 < Q_2$.

(2) We have $\sum_{j \in S_{Q_1}(Q_2)} \mathrm{in}_\nu(q_j Q_1^j) = 0$ with Q_2 of minimal degree for this property.

Proof. First, let us show that

$$Q_1 < Q_2 \Rightarrow \sum_{j \in S_{Q_1}(Q_2)} \mathrm{in}_\nu\left(q_j Q_1^j\right) = 0.$$

Assume $Q_1 < Q_2$. By Proposition 2.4, we know that $v_{Q_1}(Q_2) < v(Q_2)$. So by definition

$$\sum_{j \in S_{Q_1}(Q_2)} \mathrm{in}_\nu\left(q_j Q_1^j\right) = 0.$$

Furthermore, if $Q_1 < Q_2$, we have that Q_2 is of minimal degree for this property by definition of immediate successor.

Now let us show that if $\sum_{j \in S_{Q_1}(Q_2)} \mathrm{in}_\nu(q_j Q_1^j) = 0$ with Q_2 of minimal degree for this property, then $Q_1 < Q_2$.

Assume $\sum_{j \in S_{Q_1}(Q_2)} \mathrm{in}_\nu(q_j Q_1^j) = 0$. Then

$$\nu(Q_2) > \min_{j\in\Theta} \nu(q_j Q_1^j) = \nu_{Q_1}(Q_2),$$

and so $Q_2 > Q_1$ by Proposition 2.4.

Remark 2.6 Let Q_1 and Q_2 be key polynomials such that Q_2 is an immediate successor of Q_1 and let $Q_2 = \sum_{j\in\Theta} q_j Q_1^j$ be the Q_1-expansion of Q_2. We set

$$\tilde{Q}_2 = \sum_{j\in S_{Q_1}(Q_2)} q_j Q_1^j.$$

We will show that $\tilde{Q}_2$ is an immediate successor of Q_1. Then we will always consider "optimal" immediate successor key polynomials. This means, by definition, that all the terms in their expansion in the powers of the previous key polynomial are of same value.

Proposition 2.7 Let Q_1 and Q_2 be keg polgnomieds such that Q_2 is an immediate successor of Q_1 and let $Q_2 = \sum_{j\in\Theta} q_j Q_1^j$ be the Q_1-expansion of Q_2. We set

$$\tilde{Q}_2 = \sum_{j\in S_{Q_1}(Q_2)} q_j Q_1^j$$

Then $\tilde{Q}_2$ is an immediate successor of Q_1.

Proof. First, by definition of $\tilde{Q}_2$, we have deg $(\tilde{Q}_2)$ < deg (Q_2). We are going to show that this inequality is, in fact, an equality.

We have $\sum_{j\in S_{Q_1}(Q_2)} \mathrm{in}_\nu\ (q_j Q_1^j) = \sum_{j\in S_{Q_1}(\tilde{Q}_2)} \mathrm{in}_\nu\ (q_j Q_1^j) = 0$. Since Q_2 is of minimal degree for this property, we know that its term of greatest degree appears in this sum. So $\deg_X(\tilde{Q}_2) = \deg_X(Q_2)$.

Now let us show that $\epsilon(\tilde{Q}_2) > \epsilon(Q_1)$.

Since $\sum_{j\in S_{Q_1}(\tilde{Q}_2)} \mathrm{in}_\nu (q_j Q_1^j) = 0$, we have $\nu_{Q_1}(\tilde{Q}_2) < \nu(\tilde{Q}_2)$, and $\tilde{Q}_2$ is still of minimal degree for this property. Then $S_{Q_1}(\tilde{Q}_2) \neq \{0\}$ and for every non-zero integer b, we have $\nu_{Q_1}(\partial_b \tilde{Q}_2) = \nu(\partial_b \tilde{Q}_2)$. By Proposition 1.16, there exists a strictly positive integer b such that $\nu_Q(P) - \nu_Q(\partial_b P) = b\epsilon(Q)$. So we can use Corollary 1.19 to conclude that

$$\epsilon\left(\tilde{Q}_2\right) > \epsilon\left(Q_1\right).$$

Assume that we already know that $\tilde{Q}_2$ is a key polynomial. Since deg $(\tilde{Q}_2)$ = deg $(\tilde{Q}_2)$, we have that $\tilde{Q}_2$ is of minimal degree for the property $\epsilon(\tilde{Q}_2) > \epsilon(Q_1)$, and so $Q_1 < \tilde{Q}_2$.

It remains to prove that $\tilde{Q}_2$ is a key polynomial.

Assume, aiming for contradiction, that $\tilde{Q}_2$ is not a key polynomial. Then there exists a polynomial $P \in K[X]$ such that

$$\epsilon\left(P\right) \geq \epsilon\left(\tilde{Q}_2\right)$$

and

$$\deg_X\left(P\right) < \deg_X\left(\tilde{Q}_2\right).$$

We take P of minimal degree for this property. We can also assume that P is monic. Let us show that P is a key polynomial.

Let $S \in K[X]$ be a polynomial such that $\epsilon(S) \geq \epsilon(P)$. Then $\epsilon(S) \geq \epsilon(\tilde{Q}_2)$. If $\deg_X(S) \geq \deg_X(\tilde{Q}_2)$, then $\deg_X(S) > \deg_X(P)$ and the proof is finished. So let us assume that $\deg_X(S) < \deg_X(\tilde{Q}_2)$.

We have $\epsilon(S) \geq \epsilon(\tilde{Q}_2)$ and $\deg_X(S) < \deg_X(\tilde{Q}_2)$. By minimality of the degree of P for this property, we have $\deg_X(S) \geq \deg_X(P)$, and hence P is a key polynomial.

So there exists a key polynomial P such that

$$\epsilon(P) \geq \epsilon(\tilde{Q}_2)$$

and

$$\deg_X(P) < \deg_X(\tilde{Q}_2).$$

Since $\epsilon(\tilde{Q}_2) > \epsilon(Q_1)$, we also have $\epsilon(P) > \epsilon(Q_1)$. By minimality of the degree of Q_2 among the key polynomials satisfying this inequality, we have $\deg_X(Q_2) \leq \deg_X(P) < \deg_X(\tilde{Q}_2)$ which is a contradiction by the equality of the degrees of Q_2 and $\tilde{Q}_2$. Hence the polynomial $\tilde{Q}_2$ is a key polynomial.

Definition 2.8 Let Q_1 and Q_2 be two key polynomials such that $Q_1 < Q_2$. We say that Q_2 is an optimal immediate suecessor of Q_1 if all the terms of its Q_1-expansion have same value.

Remark 2.9 Proposition 2.7 shows how to associate to every immediate successor Q_2 of Q_1 an optimal immediate successor $\tilde{Q}_2$.

Hence, if Q_1 is not maximal in the set of the key polynomials Λ, it admits an optimal immediate successor.

Let $Q \in \Lambda$ be a key polynomial. We note

$$M_Q := \{P \in \Lambda \text{ such that } Q < P\}.$$

Definition 2.10 We assume that M_Q does not have a maximal element and that for every element $P \in M_Q$ we have $\deg_X(P) = \deg_X(Q)$.

We also assume that there exists a key polynomial $Q' \in \Lambda$ such that $\epsilon(Q') > \epsilon(M_Q)$.

We call a limit immediat successor of Q every polynomial Q' of minimal degree which has this property, and we write $Q <_{\lim} Q'$.

Proposition 2.11 Let Q and Q' be two key polgncmidls such that $\epsilon(Q) < \epsilon(Q')$. Then there exists a sequence $Q_1 = Q, ..., Q_h = Q'$ where for emry index i, the polynomial Q_{i+1} is either an immediate successor of Q_i or a limit immediate successor of Q_i.

Proof. If Q' is an immediate successor of Q, we are done, so we assume that Q' is not an immediate successor of Q, and we write this $Q \not< Q'$.

Let us first look at $M_Q = M_{Q_1}$. If this set has a maximum, we denote this maximum by Q_2. We have:

$$\begin{cases} Q < Q_2 \\ \epsilon(Q) < \epsilon(Q') \\ Q \not< Q' \end{cases}$$

and by minimality of the degree of Q_2 we know that $\deg_X(Q_2) < \deg_X(Q')$. But Q' is a key polynomial, so $\epsilon(Q_2) < \epsilon(Q')$.

Then we have

$$\begin{cases} Q = Q_1 < Q_2 \\ \epsilon(Q) < \epsilon(Q_2) < \epsilon(Q') \end{cases}$$

and since $Q < Q_2$, we know that $\deg_X(Q) \leq \deg_Q(Q_2)$.

We iterate the process as long as M_{Q_i} has a maximum.

Assume that there exists an index i such that M_{Q_i} does not have a maximum.

Assume that $\epsilon(M_{Q_i}) \not< \epsilon(Q')$. So there exists $g_i \in M_{Q_i}$ such that $\epsilon(g_i) \geq \epsilon(Q')$. Since Q' is a key polynomial, we know that $\deg_X(g_i) \geq \deg_X(Q')$.

We have:

$$\begin{cases} \epsilon(Q_i) < \epsilon(Q') \\ Q_i < g_i \\ \deg_X(Q') \leq \deg_X(g_i) \end{cases}$$

By definition of immediate successors, we have $Q_i < Q'$ and we set $Q_{i+1} = Q'$. This completes the proof.

Now assume that $\epsilon(Q') > \epsilon(M_{Q_i})$.

Since $\deg_X(Q) \le \deg_X(Q_i) < \deg_Q(Q')$ for every index i, there exists a natural number N such that for every index $j \ge N$ we have

$$\deg_X(Q_j) = \deg_X(Q_{j+1}) < \deg_X(Q').$$

Let $P \in M_{Q_N}$. By constmction, $\epsilon(P) \le \epsilon(Q_{N+1}) < \epsilon(Q')$. If Q' is not of minimal degree for this property, then there exists a key polynomial P' limit immediate successor of Q_N, of degree strictly less than the degree of Q'. So

$$\deg_X(Q_{N+1}) < \deg_X(P') < \deg_X(Q').$$

Then we replace Q_{N+1} by P' and iterate the process, which ends because the sequence of the degrees increase strictly.

Otherwise, Q' is of minimal degree among all the key polynomials such that $\epsilon(M_{Q_N}) < \epsilon(Q')$, so Q' is a limit immediate successor of Q_N and the process ends at $Q_{N+1} = Q'$.

In each case, we construct a family of key polynomials which begins at Q, ends at Q' and such that for every index i, the polynomial Q_{i+1} is either an immediate successor of Q_i, or a limit immediate successor of Q_i. This completes the proof.

Proposition 2.12 Let Q and Q' be two key polgncmidls such that $\epsilon(Q) < \epsilon(Q')$. Then there exists a sequence $Q_1 = Q$, ..., $Q_h = Q'$ where for every index i, the polynomial Q_{i+1} is either an optimal immediate successor of Q_i or a limit immediate successor of Q_i.

Proof. Let Q_2 be an optimal immediate successor of Q. We look at $M_Q = M_{Q_1}$. If this set has a maximum, we denote this maximum by P.

If $\epsilon(Q_2) = \epsilon(P)$, we set $P = Q_2$. Otherwise, $\epsilon(Q_2) < \epsilon(P)$. Since P and Q_2 are both immediate successors of Q, they have same degree.

Hence P is an immediate successor of Q_2, of the degree as Q_2. The polynomial P is then an optimal immediate successor of Q_2.

So we set $Q_3 = P$.

In fact, we have a finite sequence of optimal immediate successors which begins at Q and ends at $P = \max\{M_Q\}$.

We iterate the process as long as M_{Q_i} has a maximum. Assume that there exists an index i such that M_{Q_i}. does not have a maximum.

Then we do exactly the same thing that we did in the proof ofcProposition 2.11 and this completes the proof.

Lemma 2.13 Let Q and Q' be two key polynomials such that $Q < Q'$ and we denote by $Q' = \sum_{j=0}^{m} q_j Q^j$ the Q-expansion of Q'. Then $q_m = 1$.

Proof. Since $\epsilon(Q) < \epsilon(Q')$ we know by Proposition 2.5 that $\sum_{j=0}^{m} \mathrm{in}_\nu\left(q_j Q^j\right) = 0$.

In fact we have

$$\mathrm{in}_\nu(q_m)\mathrm{in}_\nu(Q)^m + \ldots + \mathrm{in}_\nu(q_1)\mathrm{in}_\nu(Q) + \mathrm{in}_\nu(q_0) = 0.$$

Then, since $\mathrm{in}_\nu(q_m) \ne 0$, we have

$$\mathrm{in}_\nu(Q)^m + \ldots + \frac{\mathrm{in}_\nu(q_1)}{\mathrm{in}_\nu(q_m)}\mathrm{in}_\nu(Q) + \frac{\mathrm{in}_\nu(q_0)}{\mathrm{in}_\nu(q_m)} = 0. \qquad (2)$$

We set $a := \deg_X(Q)$ and we consider $G_{<a}$ subalgebra of $gr_\nu(K[X])$ generated by the initial forms of all the polynomials of degree strictly less than a.

Hence $G_{<a}$ is a saturated algebra, and all the coefficients of the form $\frac{\mathrm{in}_\nu(q_i)}{\mathrm{in}_\nu(q_m)}$ of the equation (2) can be represented by polynomials. We denote by h_i some liftings, of degrees strictly less than a.

The element $\mathrm{in}_\nu(Q)$ is hence a solution of a homogeneous monic equation with coefficients in $G_{<a}$ and whose leading coefficient is 1.

We consider the polynomial $\tilde{Q} = Q^m + \sum_{j=0}^{m-1} h_j Q^j$, with, by hypothesis, $\deg_X(\tilde{Q}) \le \deg_X(Q')$. By construction we have

$$\mathrm{in}_\nu(Q)^m + \sum_{j=0}^{m-1} \mathrm{in}_\nu(h_j)\,\mathrm{in}_\nu(Q)^j = 0$$

and by the proof of the proposition 2.5, we have $\epsilon(\tilde{Q}) > \epsilon(Q)$.

By minimality of the degree of Q' for this property, if we can show that $\tilde{Q}$ is a key polynomial, then we would have $\deg_X(Q') = \deg_X(\tilde{Q})$and so $q_m = 1$.

Let us show that $\tilde{Q}$ is a key polynomial.

Assume, aiming for contradiction, that it is not. Then there exists a polynomial P such that $\epsilon(P) \geq \epsilon(\tilde{Q})$and $\deg_X(P) < \deg_X(\tilde{Q})$. We choose P monic and of minimal degree for this property. Let us show that P is a key polynomial.

Let S be a polynomial such that $\epsilon(S) \geq \epsilon(P)$. Then $\epsilon(S) \geq \epsilon(\tilde{Q})$.

If $\deg_X(S) \geq \deg_X(\tilde{Q})$, then, since $\deg_X(P) < \deg_X(\tilde{Q})$, the proof is finished.

So let us assume that $\deg_X(S) < \deg_X(\tilde{Q})$. Then $\epsilon(S) \geq \epsilon(\tilde{Q})$and $\deg_X(S) < \deg_X(\tilde{Q})$. By minimality of the degree of P for that property, $\deg_X(S) \geq \deg_X(P)$ and the proof is finished.

So there exists a key polynomial P such that $\epsilon(P) \geq \epsilon(\tilde{Q})$ and $\deg_X(P) < \deg_X(\tilde{Q})$.

Since $\epsilon(\tilde{Q}) > \epsilon(Q)$, we have $\epsilon(P) > \epsilon(Q)$.

So we have a key polynomial P such that $\epsilon(P) > \epsilon(Q)$. By minimality the degree of Q' for this property, we know that $\deg_X(Q') \leq \deg_X(P)$. But $\deg_X(P) < \deg_X(\tilde{Q})$, and this implies that $\deg_X(Q') < \deg_X(\tilde{Q})$, which is a contradiction.

Thus $\tilde{Q}$ is a key polynomial.

Proposition 2.14 Let Q and Q' be two key polynomials such that:

$$\epsilon(Q) < \epsilon(Q').$$

Let c and c' be two polgnomials of degrees strictly less than $\deg_X Q'$ and let j and j' be two integers such that:

$$\begin{cases} \nu_Q(c) = \nu(c) \\ \nu_Q(c') = \nu(c') \\ j \leq j' \\ \nu_Q\left(c(Q')^j\right) \leq \nu_Q\left(c'(Q')^{j'}\right). \end{cases}$$

Then:

$$\nu\left(c(Q')^j\right) \leq \nu\left(c'(Q')^{j'}\right).$$

If, in addition, either $j < j'$ or $\nu_Q(c(Q')^j) < \nu_Q(c'(Q')^{j'})$, then

$$\nu\left(c(Q')^j\right) < \nu\left(c'(Q')^{j'}\right).$$

Proof. We know that $\nu_Q(Q') \leq \nu(Q')$, hence

$$\nu(Q') - \nu_Q(Q') \geq 0.$$

Since we assumed that $j \leq j'$, we have

$$j\left(\nu(Q') - \nu_Q(Q')\right) \leq j'\left(\nu(Q') - \nu_Q(Q')\right).$$

Furthermore, we know that $\nu_Q(c(Q')^j) \leq \nu_Q(c'(Q')^{j'})$, hence

$$\nu_Q\left(c(Q')^j\right) + j\left(\nu(Q') - \nu_Q(Q')\right) \leq \nu_Q\left(c'(Q')^{j'}\right) + j'\left(\nu(Q') - \nu_Q(Q')\right).$$

So we have the inequality

$$\nu_Q(c)+j\nu_Q(Q')+j\nu(Q')-j\nu_Q(Q')\le \nu_Q(c')+j'\nu_Q(Q')+j'\nu(Q')-j'\nu_Q(Q').$$

Equivalently, $\nu_Q(c)+j\nu(Q')\le \nu_Q(c')+j'\nu(Q')$.

But $\nu_Q(c)=\nu(c)$ and $\nu_Q(c')=\nu(c')$, so $\nu(c(Q')^j)\le \nu(c'(Q')^{j'})$.

If, in addition, either $j<j'$ or $\nu_Q(c(Q')^j)<\nu_Q(c'(Q')^{j'})$, then we have $\nu(c(Q')^j)<\nu(c'(Q')^{j'})$.

Lemma 2.15 Let Q and Q' be two polynomials such that

$$\epsilon(Q)<\epsilon(Q')$$

and let $f\in K[X]$ be a polynomial whose Q'-expansion is $Q\ f=\sum_{j=0}^{r} f_j(Q')^j$. Then

$$\nu_Q(f)=\min_{0\le j\le r}\left\{\nu_Q\left(f_j(Q')^j\right)\right\}.$$

If we set

$$T_{Q,Q'}(f):=\left\{j\in\{0,\dots,r\}\text{ such that }\nu_Q\left(f_j(Q')^j\right)=\nu_Q(f)\right\},$$

then we have

$$\mathrm{in}_{\nu_Q}(f)=\sum_{j\in T_{Q,Q'}(f)}\mathrm{in}_{\nu_Q}\left(f_j(Q')^j\right).$$

Proof. Only for the purposes of this proof, we will write

$$\nu'(f):=\min_{0\le j\le r}\left\{\nu_Q\left(f_j(Q')^j\right)\right\}$$

and

$$T'(f):=\left\{j\in\{0,\dots,r\}\text{ such that }\nu_Q\left(f_j(Q')^j\right)=\nu'(f)\right\}.$$

Let us show that $\nu_Q(f)=\nu'(f)$.

First, we have

$$\begin{aligned}\nu_Q\left(\sum_{j\in T'(f)} f_j(Q')^j\right) &\ge \min_{j\in T'(f)}\nu_Q\left(f_j(Q')^j\right)\\ &= \min_{j\in T'(f)}\nu'(f)\\ &= \nu'(f).\end{aligned}$$

Set $b'=\max \mathrm{T}'(f)$ and $b=\delta_Q(f_{b'})$. In other words

$$b=\max\left\{j\in\{0,\dots,n\}\text{ such that }\nu\left(a_jQ^j\right)=\nu_Q\left(f_{b'}\right)\right\}$$

where $f_{b'}=\sum_{j=0}^{n} a_jQ^j$. Hence, the expression $\sum_{j\in T'(f)} f_j(Q')^j$ contains the term

$$a_b c_{\deg_Q Q'} Q^{b+b'\deg_Q Q'}.$$

Then for every $j \in \{0,\ldots,r\}$ such that $f_j \neq 0$, we have:

$$\begin{aligned} \nu_Q\left(f_j (Q')^j\right) &\geq \min_{0\leq j\leq r}\left\{\nu_Q\left(f_j (Q')^j\right)\right\} \\ &= \nu'(f) \\ &= \nu_Q\left(f_i (Q')^i\right) \end{aligned}$$

for every index $i \in T'(f)$. So in particular,

$$\begin{aligned} \nu_Q\left(f_j (Q')^j\right) &\geq \nu_Q\left(f_{b'} (Q')^{b'}\right) \\ &= \nu_Q(f_{b'}) + \nu_Q\left((Q')^{b'}\right) \\ &= \nu\left(a_b Q^b\right) + \nu_Q\left((Q')^{b'}\right) \\ &= \nu\left(a_b Q^b\right) + \nu\left(c_{\deg_Q Q'} Q^{b'\deg_Q Q'}\right) \\ &= \nu\left(a_b c_{\deg_Q Q'} Q^{b+b'\deg_Q Q'}\right) \end{aligned}$$

with strict inequality if $j \notin T'(f)$.

So

$$\nu\left(a_b c_{\deg_Q Q'} Q^{b+b'\deg_Q Q'}\right) = \nu'(f)$$

and

$$\nu_Q\left(\sum_{j\notin T'(f)} f_j (Q')^j\right) > \nu'(f).$$

By maximality of b and b', the term $a_b c_{\deg_Q Q'} Q^{b+b'\deg_Q Q'}$ cannot be cancelled and so $\nu_Q(f) = \nu(a_b c_{\deg_Q Q'} Q^{b+b'\deg_Q Q'}) = \nu'(f)$. In other words $\nu_Q(f) = \min_{0\leq j\leq r}\{\nu_Q(f_j (Q')^j)\}$. So we also have

$$T'(f) = T_{Q,Q'}(f).$$

Then $\sum_{j\in T'(f)} \mathrm{in}_{\nu_Q}(f_j (Q')^j)$ is a non-zero element of G_{ν_Q}, equal to $\mathrm{in}_{\nu_Q}(f)$. This completes the proof.

Corollary 2.16 Let Q and Q' be two key polynomials such that

$$\epsilon(Q) < \epsilon(Q')$$

and let

$$f = \sum_{j=0}^{r} f_j (Q')^j = \sum_{j=0}^{n} a_j Q^j$$

be the Q' and Q-ewpansions of an element $f \in K[X]$. We set

$$\theta := \min T_{Q,Q'}(f) = \min\left\{ j \in \{0,\ldots,r\} \text{ such that } \nu_Q\left(f_j (Q')^j\right) = \nu_Q(f)\right\}$$

and we assume that $\nu_Q(f_{\delta_{Q'}(f)}) = \nu(f_{\delta_{Q'}(f)})$ and that $\nu_Q(f_\theta) = \nu(f_\theta)$.

Then:

(1) $\Delta_{Q'}(f) \deg_{Q'} Q' \le \Delta_Q(f)$, and so $\Delta_{Q'}(f) \le \Delta_Q(f)$.

(2) If $\Delta_Q(f) = \Delta_{Q'}(f)$, we set $\Delta := \Delta_Q(f)$ and then

$$\deg_Q Q' = 1,$$

$$T_{Q,Q'}(f) = \{\delta\}$$

and

$$\mathrm{in}_{\nu_Q}(f) = \left(\mathrm{in}_{\nu_Q} a_\delta\right)\left(\mathrm{in}_{\nu_Q} Q'\right)^{\delta}.$$

Proof. First let us show the point 1.

By the proof of the previous Lemma, we know that

$$\theta \deg_Q Q' \le \delta_Q(f).$$

Furthermore,

$$\nu_Q\left(f_{\delta_{Q'}(f)}\right) = \nu\left(f_{\delta_{Q'}(f)}\right),$$

$$\nu_Q(f_\theta) = \nu(f_\theta).$$

By definition of $\delta = \delta_{Q'}(f)$, we have $\nu(f_\delta(Q')^\delta) \le \nu(f_\theta(Q')^\theta)$. We know by Lemma 2.15 that $\nu_Q(f) = \nu_Q(f) = \min\limits_{0\le j\le r}\{\nu_Q(f_j(Q')^j)\}$. Since $\theta = \min T_{Q,Q'}(f)$, we have

$$\nu_Q\left(f_\theta (Q')^\theta\right) = \nu_Q(f) = \min_{0\le j\le r}\left\{\nu_Q\left(f_j(Q')^j\right)\right\}.$$

Hence $\nu_Q(f_\theta(Q')^\theta) \le \nu_Q(f_\delta(Q')^\delta)$.

Then, since $\nu_Q(f_\theta) = \nu(f_\theta)$ and $\nu_Q(f_\delta) = \nu(f_\delta)$:

$$\begin{aligned} &\nu_Q\left(f_\theta(Q')^\theta\right) \le \nu_Q\left(f_\delta(Q')^\delta\right)\\ \Leftrightarrow\ &\nu_Q(f_\theta) + \theta\nu_Q(Q') \le \nu_Q(f_\delta) + \delta\nu_Q(Q')\\ \Leftrightarrow\ &\nu(f_\theta) + \theta\nu_Q(Q') \le \nu(f_\delta) + \delta\nu_Q(Q'). \end{aligned}$$

Assume we have equality on ν, it means that $\nu(f_\theta(Q')^\theta) = \nu(f_\delta(Q')^\delta)$. So $\nu(f_\theta) = \nu(f_\delta) + \delta\nu(Q') - \theta\nu(Q')$ and

$$\begin{aligned} &\nu_Q\left(f_\theta(Q')^\theta\right) \le \nu_Q\left(f_\delta(Q')^\delta\right)\\ \Leftrightarrow\ &\nu(f_\delta) + \delta\nu(Q') - \theta\nu(Q') + \theta\nu_Q(Q') \le \nu(f_\delta) + \delta\nu_Q(Q')\\ \Leftrightarrow\ &(\delta-\theta)\nu(Q') \le (\delta-\theta)\nu_Q(Q'). \end{aligned}$$

Since we know that $\epsilon(Q) < \epsilon(Q')$, by the proof of Proposition 2.4, we know that $\nu_Q(Q') < \nu(Q')$ and then $\delta - \theta \le 0$, that is $\delta \le \theta$.

Otherwise we have $\nu(f_\delta(Q')^\delta) < \nu(f_\theta(Q')^\theta)$.

Then the following four conditions hold:

$$\begin{cases} \nu_Q(f_\theta) = \nu(f_\theta) \\ \nu_Q(f_\delta) = \nu(f_\delta) \\ \nu_Q\left(f_\theta (Q')^\theta\right) \leq \nu_Q\left(f_\delta (Q')^\delta\right) \\ \nu\left(f_\delta (Q')^\delta\right) < \nu\left(f_\theta (Q')^\theta\right). \end{cases}$$

By the contrapositive of Proposition 2.14, we deduce that $\delta < \theta$.

In each case, we have $\delta \leq \theta$. Then since $\theta \deg_Q Q' \leq \delta_Q(f)$, we know that $\Delta \deg_Q Q' \leq \delta_Q(f)$. So in particular $\delta_{Q'}(f) \leq \delta_Q(f)$.

Now let us show the point 2.

Assume $\delta_{Q'}(f) = \delta_Q(f) = \delta$. We just saw that $\delta_{Q'}(f) \deg_Q Q' \leq \Delta_Q(f)$, so we have $\deg_Q Q' = 1$. Then $Q' = Q + b$ with b a polynomial of degree strictly less than the degree of Q.

We know by the proof of point 1 that $\delta \leq \theta$. Furthermore, we know that $\theta \deg_Q Q' \leq \delta_Q(f) = \delta$, in other words $\theta \leq \delta$ since $\deg_Q Q' = 1$.

Hence $\delta \leq \theta \leq \delta$, hence $\theta = \delta = \min T_Q Q'(f)$. We now have to prove that for every index $j > \delta$, we have $j \notin T_{Q,Q'}(f)$. Equivalently, that:

$$\nu_Q\left(f_j (Q')^j\right) > \nu_Q(f) = \min_{0 \leq i \leq r}\left\{\nu_Q\left(f_i (Q')^i\right)\right\}.$$

And then we will have $T_{Q\ Q'}(f) = \{\delta\}$.

So let $j > \delta$. By definition of $\delta_Q(f)$ and $\delta_{Q'}(f)$, we know that $\nu(f_j (Q')^j) > \nu_{Q'}(f)$ and $\nu(a_j Q^j) > \nu_Q(f)$.

Furthermore, since $\delta \in T_{Q,Q'}(f)$, we have $\nu_Q(f_\delta (Q')^\delta) = \nu_Q(f)$. We want to prove that $\nu_Q(f_j (Q')^j) > \nu_Q(f_\delta (Q')^\delta)$ for every index $j \in \{\delta+1, \ldots, r\}$.

We know that:

$$\begin{cases} \nu\left(f_\delta (Q')^\delta\right) = \nu_{Q'}(f) < \nu\left(f_j (Q')^j\right) & \\ \nu_Q(f_\delta) = \nu(f_\delta) & \text{because } \deg_X(f_\delta) < \deg_X(Q') = \deg_X(Q) \\ \nu_Q(f_j) = \nu(f_j) & \text{because } \deg_X(f_j) < \deg_X(Q') = \deg_X(Q) \\ \delta < j & \end{cases}$$

By the contrapositive of Proposition 2.14, we have

$$\nu_Q\left(f_\delta (Q')^\delta\right) < \nu_Q\left(f_j (Q')^j\right).$$

By Lemma 2.15, we have

$$\begin{aligned} \mathrm{in}_{\nu_Q}(f) &= \sum_{j \in T_{Q,Q'}(f)} \mathrm{in}_{\nu_Q}\left(f_j (Q')^j\right) \\ &= \mathrm{in}_{\nu_Q}\left(f_\delta (Q')^\delta\right) \\ &= \mathrm{in}_{\nu_Q}(f_\delta)\left(\mathrm{in}_{\nu_Q}(Q')\right)^\delta. \end{aligned}$$

Theorem 2.17 Let Q and Q' be two key polynomials such that

$\epsilon(Q) < \epsilon(Q')$.

We recall that char $(k_v) = 0$ If Q' is a limit immediate successor of Q, then $\delta_Q(Q') = 1$.

Proof. We give a proof by contradiction. Assume that $\delta_Q(Q') > 1$. Among all the couples (Q, Q') such that Q' is a limit immediat successor of Q and such that $\delta_Q(Q') > 1$, we choose Q and Q' such that $\deg(Q') - \deg(Q)$ is minimal.

By definition of a limit immediate successor, for every sequence of immediate successors $(Q_i)_{i\in\mathbb{N}^*}$ with $Q_1 = Q$, we have $Q_i \neq Q'$ for every non-zero index i. By definition of limit key polynomials and by hypothesis, we know that $\deg(Q') - \deg(Q)$ is minimal for this property.

If we find a polynomial $\tilde{Q}$ such that

$$\epsilon(Q) < \epsilon(\tilde{Q}) < \epsilon(Q')$$

and $\deg(Q) < \deg(\tilde{Q}) < \deg(Q')$ then by minimality of $\deg(Q') - \deg(Q)$, we know that there exists a finite sequence of immediate successors between Q and $\tilde{Q}$ and that there exists a finite sequence of immediate successors between $\tilde{Q}$ and Q'. Then we have a finite sequence of immediate successors between Q and Q', which is a contradiction.

Hence there exists a key polynomial $\tilde{Q}$ such that

$$\epsilon(Q) < \epsilon(\tilde{Q}) < \epsilon(Q')$$

and $\deg(\tilde{Q}) < \deg(Q')$ and so $\deg(Q) = \deg(\tilde{Q})$.

Let $\tilde{Q}$ be a such key polynomial. We have $\tilde{Q} := Q - a$ where a is a polynomial of degree strictly kss than the degree of Q.

Since $\epsilon(Q) < \epsilon(\tilde{Q})$, by Proposition 2.5 ,we know that $\mathrm{in}_v(Q) = \mathrm{in}_v(a)$.

Consider the Q-expansion $\sum_{j=0}^{n} a_j Q^j$ of Q'. We may assume that $\delta_Q(Q') = \delta_{\tilde{Q}}(Q')$ and we set $\delta := \delta_Q(Q')$.

By Corollary 2.16, we know that $\mathrm{in}_{v_Q}(Q') = \mathrm{in}_{v_Q}(a_\delta)\mathrm{in}_{v_Q}(\tilde{Q})^\delta$. In other words $\mathrm{in}_{v_Q}(Q') = \mathrm{in}_{v_Q}(a_\delta)\mathrm{in}_{v_Q}(Q-a)^\delta$.

Furthermore, $\partial Q' = \sum_{j=0}^{n}[\partial(a_j)Q^j + a_j jQ^{j-1}\partial Q]$.

We first show that the terms $\partial(a_j)Q^j$ do not appear in $\mathrm{in}_v(\partial Q')$. So let $j \in \{0,\ldots,n\}$.

We have

$$v_Q(\partial a_j) = v(\partial a_j)$$

$$\geq v(a_j) - \epsilon(a_j).$$

But Q is a key polynomial and a_j is of degree strictly less than the degree of Q since it is a coefficient of a Q-expansion. Then $\epsilon(a_j) < \epsilon(Q)$.

So

$$v_Q(\partial a_j) > v(a_j) - \epsilon(Q) = v_Q(a_j) - \epsilon(Q).$$

By the proof of Proposition 1.16, we know that, since we are in characteristic zero,

$$v_Q(Q) - v_Q(\partial Q) = \epsilon(Q).$$

Then $v_Q(\partial a_j) > v_Q(a_j) - v_Q(Q) + v_Q(\partial Q)$. In fact,

$$v_Q(\partial a_j) + v_Q(Q) > v_Q(a_j) + v_Q(\partial Q).$$

It means that $v_Q(Q\partial a_j) > v_Q(a_j\partial Q)$, and adding $v_Q(Q^{j-1})$ to each side, we obtain:

$$v_Q(Q^j\partial a_j) > v_Q(a_jQ^{j-1}\partial Q) = v_Q(ja_jQ^{j-1}\partial Q).$$

So

$$\mathrm{in}_{v_Q}\left(\partial Q'\right)=\mathrm{in}_{v_Q}\left(\sum_{j=1}^{n}\left[ja_jQ^{j-1}\partial Q\right]\right).$$

Even though the expression $\sum_{j=1}^{n}[ja_jQ^{j-1}\partial Q]$ need not be a Q-expansion, since a_j and ∂Q are of degrees strictly less than the degree of Q in characteristic zero, by Lemma 1.11, the v_Q-initial form of $a_j\partial Q$ is equal to the initial form of its remainder after the Euclidean division by Q. So we conserve this expression and consider it a substitute of a Q-expansion.

Now let us prove that $\delta_Q(\partial Q') = \delta - 1$.

Replacing Q by $\tilde{Q}$ in the computation of the initial form of Q' with respect to Q (respectively $\tilde{Q}$) does not change the problem, and we assume that δ stabilizes starting with Q. Then, if $\delta_Q(\partial Q') = \delta - 1$, we would also have $\delta_{\tilde{Q}}(\partial Q') = \delta - 1$.

Let $j > \delta$. Let us first show that

$$v_Q\left(ja_jQ^{j-1}\partial Q\right)>v_Q\left(\delta a_\delta Q^{\delta-1}\partial Q\right).$$

It is enough to show that

$$v_Q\left(ja_jQ^{j-1}\right)>v_Q\left(\delta a_\delta Q^{\delta-1}\right).$$

But by definition of δ. we have $v_Q(a_jQ^j) > v_Q(a_\delta Q^\delta)$. So

$$v_Q(a_jQ^{j-1}) > v_Q(a_\delta Q^{\delta-1})$$

hence $v_Q(ja_jQ^{j-1}) > v_Q(\delta a_\delta Q^{\delta-1})$.

We now have to prove that the value of the term $\delta - 1$ is minimal.

Let $j < \delta$. We know that $v_Q(a_jQ^j) = v_Q(a_\delta Q^\delta)$, and hence

$$v_Q(a_jQ^{j-1}\partial Q) = v_Q(a_\delta Q^{\delta-1}\partial Q).$$

So $v_Q(ja_jQ^{j-1}\partial Q) = v_Q(\delta a_\delta Q^{\delta-1}\partial Q)$ since we are in characteristic zero.

So we do have $\delta_Q(\partial Q') = \delta_{\tilde{Q}}(\partial Q') = \delta - 1$. By Corollary 2.16, we have:

$$\mathrm{in}_{v_Q}\left(\partial Q'\right)=\mathrm{in}_{v_Q}\left(\delta a_\delta\partial Q\right)\mathrm{in}_{v_Q}\left(\tilde{Q}\right)^{\delta-1}.$$

In other words

$$\mathrm{in}_{v_Q}\left(\partial Q'\right)=\delta\,\mathrm{in}_{v_Q}\left(a_\delta\partial Q\right)\mathrm{in}_{v_Q}\left(Q-a\right)^{\delta-1}.$$

We know that $v_Q(Q - a) < v(Q - a)$. Then, since $\delta > 1$,

$$v_Q\left(\delta a_\delta\partial Q\left(Q-a\right)^{\delta-1}\right)<v\left(\delta a_\delta\partial Q\left(Q-a\right)^{\delta-1}\right).$$

It means that the image by $\varphi: gr_{v_Q}K[x] \to gr_v K[x]$ of

$$\mathrm{in}_{v_Q}\left(\delta a_\delta\partial Q\left(Q-a\right)^{\delta-1}\right)$$

is zero. Then, the image by φ of $\mathrm{in}_{v_Q}(\partial Q')$ is zero, and so

$$v_Q(\partial Q') < v(\partial Q').$$

By the proof of Proposition 2.4, we have $\epsilon(Q) < \epsilon(\partial Q')$. But we know that $\deg(\partial Q') < \deg(Q')$, and since Q' is a key polynomial, we have $\epsilon(\partial Q') < \epsilon(Q')$.

More generally, the above argument holds if we replace Q by any key polynomial $\tilde{Q}$ of the same degree as Q.

So for every key polynomial $\tilde{Q}$ of the same degree as deg (Q), we have $\epsilon(\tilde{Q}) < \epsilon(\partial Q')$.

In fact, $\epsilon(Q) < \epsilon(\partial Q') < \epsilon(Q')$ and $\deg(\partial Q') < \deg(Q')$. So if we show that $\partial Q'$ is a key polynomial, we will have

$$\deg(Q) = \deg(\partial Q').$$

Let us show that $\partial Q'$ is a key polynomial. We assume, aiming for contradiction, that it is not. There exists a polynomial P such that $\epsilon(P) \geq \epsilon(\partial Q')$ and $\deg(P) < \deg(\partial Q')$. We choose P of minimal degree for this property. Using the same idea as before, we can show that P is a key polynomial.

We have $\deg(P) < \deg(\partial Q')$, hence $\deg(P) < \deg(Q')$ and since Q' is a key polynomial, we have $\epsilon(P) < \epsilon(Q')$.

Since $\epsilon(P) \geq \epsilon(\partial Q')$, we have $\epsilon(P) > \epsilon(Q)$.

Thus we have another key polynomial P such that $\epsilon(Q) < \epsilon(P) < \epsilon(Q')$ and deg (P) < $\deg(Q')$. Then $\deg(P) = \deg(Q)$. Hence the polynomial P is a key polynomial of same degree as Q, and so $\epsilon(P) < \epsilon(\partial Q')$, which is a contradiction.

We have proved that $\partial Q'$ is a key polynomial. Then $\deg(Q) = \deg(\partial Q')$. But then $\epsilon(\partial Q') < \epsilon(\partial Q')$ and this in a contradiction. This completes the proof.

3. Simultaneous local uniformization in the case of rings essentially of finite type over a field

The objective of this part is to give a proof of the local uniformization in the case of rings essentially of finite type over a field of zero characteristic without any restriction on the rank of the valuation. The proof of the local uniformization is well known in characteristic zero. It has been proved for the first time by Zariski in 1940 ([54]) in every dimension. The benefit of our proof is to present a universal construction which works for all the elements of the regular ring we start with, and in which the strict transforms of key polynomials become coordinates after blowing up. Thus we will have an infinite sequence of blow-ups given explicitly, together with regular systems of parameters of the local rings appearing in the sequence, and which eventually monomializes every element of our algebra essentially of finite type.

To do this, we will proceed in several steps. Let us give the idea.

Let k be a field of characteristic zero, R a regular local k-algebra essentially of finite type, with residual field k. Let $u = (u_1, ..., u_n)$ be a regular system of parameters of R, v a valuation centered in R, Γ the value group of v and $K = k(u_1, ..., u_{n-1})$. We assume that $k = k_v$. This property is preserved under blowings-up. Thus every ring that will appear in our local blowing-up sequence along the valuation v will have the same residue field: k.

We will construct a single sequence of blowings-up which monomializes every element of R provided we look far enough in the sequence. To do this, we will construct a particular sequence of (possibly limit) immediate successors. We will show that every element f of R will be non-degenerate with respect to a key polynomial Q of this sequence, in other words, that we will have $\nu_Q(f) = \nu(f)$. Furthermore, all the polynomials of this sequence will be monomializable. At this point we will have proved that every element of R is non-degenerate with respect to a regular system of parameters of a suitable regular local ring R_i. Then we will just have to see that every element non-degenerate with respect to a regular system of parameters is monomializable by our sequence of blow-ups.

We will begin this part by some preliminaries, where we define non-degeneracy and framed and monomial blowing-up.

Then, we will see that every element non-degenerate with respect to a regular system of paramaters is monomializable. And then it will be sufficient to prove that it is the case of all the elements of R.

So, after that, we construct sequence of (possibly limit) immediate successors such that every element f of R is non-degenerate with respect to one of these key polynomials.

In sections 6 and 7 we prove that all the key polynomials of this sequence are monomializable, and that we have proven the simultaneous local uniformization. To do this we will need a new notion: the one of key element. Indeed, modified by the blow-ups, the key polynomials of the above mentioned sequence have no reason to still be polynomials. So we will give a new definition, this one of key element. This notion has the benefit to be conserved by blow-ups. We will monomialize the key elements and not the key polynomials, and the proof will be complete by induction.

3.1 Preliminaries

Let k be a field of characteristic zero and R a regular local k-algebra which is essentially of finite type over k. We consider $u = (u_1, ..., u_n)$ a regular system of parameters of R and v a valuation centered on R whose group of values is denoted by Γ.We write $\beta_i = v(u_i)$ for every integer $i \in \{1,\dots,n\}$, and $K = k(u_1, ..., u_{n-1})$.

3.1.1 Non-degenerate elements

Definition 3.1 Let $f \in R$. We say that f is non-degenerate with respect to v and u if we have $v_u(f) = v(f)$, where v_u is the monomial valuation with respect to u.

We need a more convenient way of knowing whether an element is non-degenerate with respect to a regular system of parameters. It is the objective of the following Proposition.

Proposition 3.2 Let $f \in R$. The element f is non-degenerate with respect to v and u if and only if there exists an ideal N of R which contains f, monomial with respect to u and such that

$$\nu(f) = \nu(N) = \min_{x \in N}\{\nu(x)\}.$$

Proof. Let us show that if there exists an ideal N of R which contains f, monomial with respect to u and such that

$$\nu(f) = \nu(N) = \min_{x \in N}\{\nu(x)\},$$

then $v_u(f) = v(f)$. Let N be such an ideal. As N is monomial with respect to u, we have $v_u(N) = v(N)$ and $v_u(N) \leq v_u(f)$ since $f \in N$.

So $v(f) = v(N) < v_u(f)$, which give us the equality.

Now let us show that if $v_u(f) = v(f)$, then there exists an ideal N of R which contains f, monomial with respect to u and such that $\nu(f) = \nu(N) = \min_{x \in N}\{\nu(x)\}$.

Let us assume that $v_u(f) = v(f)$. Let N be the smallest ideal of R generated by monomials in u containing f. So $v(N) = v_u(N) = v_u(f)$ and since $v_u(f) = v(f)$, we have $v(N) = v(f)$.

3.1.2 Framed and monomial blow-up

Let $J_1 \subset \{1,\dots,n\}$, $A_1 = \{1,\dots,n\} \setminus J_1$ and $j_1 \in J_1$.

We write

$$u'_q = \begin{cases} \dfrac{u_q}{u_{j_1}} & \text{if } q \in J_1 \setminus \{j_1\} \\ u_q & \text{otherwise} \end{cases}$$

and we let R_1 be a localisation of $R' = R[u'_{J_1 \setminus \{j_1\}}]$ by a prime ideal, say $R_1 = R'_{m'}$ of maximal ideal $\mathfrak{m}_1 = \mathfrak{m}'R_1$. Since R is regular, R' and R_1 are regular. Let $u^{(1)} = (u_1^{(1)},\dots,u_{n_1}^{(1)})$ be a regular system of parameters of $\mathfrak{m}_1$.

We write

$$B_1 := \{q \in J_1 \setminus \{j_1\} \text{ such that } u'_q \notin R_1^{\times}\}$$

and

$$C_1 := J_1 \setminus (B_1 \cup \{j_1\}).$$

Since u is a regular system of parameters of R, we have the disjoint union

$$u' = u'_{A_1} \sqcup u'_{B_1} \sqcup u'_{C_1} \sqcup \{u'_{j_1}\}.$$

Let $\pi: R \to R_1$ be the natural map. Without loss of generality, we may assume that

$J_1 = \{1, ..., h\}$.

Definition 3.3 We say that π: $(R, u) \to (R_1, u^{(1)})$ is a framed blow-up of (R, u) along (u_{J_1}) with respect to v if there exists $D_1 \subset \{1,\dots,n_1\}$ such that

$$u'_{A_1\cup B_1\cup\{j_1\}} = u^{(1)}_{D_1}$$

and if $\mathfrak{m}' = \{x \in R' \text{ such that } \nu(x) > 0\}$.

Remark 3.4 A blow-up π is framed if among the given generators of the maximal ideal $\mathfrak{m}_1$ of R_1, we have all the elements of u', except, possibly, those that are in u'_{C_1}. In other words, except, possibly, those that are invertibles in R_1.

It is framed with respect to v if we localized in the center of v.

Let π be such a blow-up.

Definition 3.5 We say that π is monomial if $B_1 = J_1 \setminus \{j_1\}$.

Remark 3.6 Let π be a monomial blow-up.

Then $n_1 = n$ and $D_1 = \{1, ..., n\}$.

Definition 3.7 Let π: $(R, u) \to (R_1, u^{(1)})$ be a framed blow-up and $T \subset \{1,\dots,n\}$.

We say that π is independent of u_T if $T \cap J_1 = \emptyset$, in other words if $T \subset A_1$.

Remark 3.8 Since we look at blow-ups with respect to a valuation v, we have blow-ups such that $v(R_1) \geq 0$. Since $u'_q \in R_1$ for every $q \in J_1$, we want $\nu(\frac{u_q}{u_{j_1}}) \geq 0$, so $\nu(u_q) \geq \nu(u_{j_1})$ for every $q \in J_1 \setminus \{j_1\}$. So we can set j_1 to be an element of J_1 such that $\beta_{j_1} = \min_{q\in J_1}\{\beta_q\}$.

We have :

$$\begin{aligned} B_1 &:= \left\{q \in J_1 \setminus \{j_1\} \text{ such that } u'_q \notin R_1^{\times}\right\} \\ &= \left\{q \in J_1 \setminus \{j_1\} \text{such that } \nu\left(u'_q = \frac{u_q}{u_{j_1}}\right) > 0\right\} \\ &= \left\{q \in J_1 \setminus \{j_1\} \text{ such that } \beta_q > \beta_{j_1}\right\}. \end{aligned}$$

And $C_1 = \{q \in J_1 \setminus \{j_1\} \text{ such that } \beta_q = \beta_{j_1}\}$.

Let k_1 be the residue field of R_1 and t_{k_1} the transcendence degree of $k \to k_1$. Let us show that $t_{k_1} \leq \sharp C$.

We write $\overline{R} = \frac{R'}{\mathfrak{m}R'}$. We denote by $\overline{u}_q$ the image of u'_q in $\overline{R}$ for every $q \in J_1 \setminus \{j_1\}$. So $\overline{R} = k[\overline{u}_{B_1}, \overline{u}_{C_1}^{\pm 1}]$. We have $R \to R' \to R_1 \to k_1$, which induces homomorphisms $k \to \overline{R} \to \frac{R_1}{\mathfrak{m}R_1} \to k_1$.

We have $\mathfrak{m} = \mathfrak{m}_1 \cap R = \mathfrak{m}'R_1 \cap R = \mathfrak{m}' \cap R$. Let $\overline{\mathfrak{m}} = \frac{\mathfrak{m}'}{\mathfrak{m}R'}$. We have

$$\begin{aligned} \frac{R_1}{\mathfrak{m}R_1} &= \frac{R'_{\mathfrak{m}'}}{\mathfrak{m}R'_{\mathfrak{m}'}} \\ &= \left(\frac{R'_{\mathfrak{m}'}}{\mathfrak{m}R'_{\mathfrak{m}'}}\right)_{\frac{\mathfrak{m}'}{\mathfrak{m}R'}} \\ &= \overline{R}_{\overline{\mathfrak{m}}} \end{aligned}$$

in other words

$$k \to \overline{R} \to \overline{R}_{\overline{\mathfrak{m}}} \to k_1. \qquad (3)$$

Since $u'_{A_1\cup B_1\cup\{j_1\}} \subset \mathfrak{m}'$, for every $q \in A_1 \cup B_1 \cup \{j_1\}$, the image of u'_q in k_1 is zero. So k_1 is generated over k by the images of the u'_q with $q \in C_1$. Hence $t_{k_1} \leq \sharp C_1$.

But we have $C_1 := J_1 \setminus (B_1 \cup \{j_1\})$. So $\sharp C_1 + \sharp B_1 + 1 = \sharp J_1 = h$, and:

$$\sharp B_1 + 1 \leq t_{k_1} + \sharp B_1 + 1 \leq \sharp C_1 + \sharp B_1 + 1 = h \leq n. \qquad (4)$$

We will often set $J_1 \subset \{1,\ldots,r,n\}$ where r is the dimension of $\sum_{i=1}^{n} \mathbb{Q}\nu(u_i)$ in $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. If $J_1 \subset \{1,\ldots,r\}$, the family β_{J_1} is a family of $\mathbb{Q}$-linearly independent elements, and so $B_1 = J_1 \setminus \{j_1\}$.

Otherwise $n \in J_1$. Then we have $B_1 = J_1 \setminus \{j_1\}$ or $B_1 = J_1 \setminus \{j_1, q_1\}$ where $q_1 \in J_1 \setminus \{j_1\}$. The interesting cases are those where $h - 2 \leq \sharp B_1$, in other words, those where $h - 1 \leq \sharp B_1 + 1$.

Since (4), we have $h - 1 + t_{k_1} \leq \sharp B_1 + 1 + t_{k_1} \leq h$.

Then we have three cases.

The first one, $\sharp B_1 + 1 = h$ and $t_{k_1} = 0$, it occurs when the blow-up is monomial.

The second one, $\sharp B_1 + 1 = h - 1$ and $t_{k_1} = 1$.

The last one, $\sharp B_1 + 1 = h - 1$ and $t_{k_1} = 0$.

Fact 3.9 In the cases 1 and 3, we have $n_1 = n$ and in the case 2 we have $n_1 = n - 1$.

Remark 3.10 In the rest of the chapter, we will assume that the valuation ring has k as residue field. So $k_1 = k$ and $t_{k_1} = 0$. Hence we will have $n_1 = n$.

Since $k_1 \simeq \frac{k[Z]}{(\lambda(Z))}$, we know that $\lambda(Z)$ is a polynomial of degree 1 over k.

3.1.3 Key elements

We need a more general notion than the one of key polynomials. Indeed, after several blow-ups, a key polynomial might not be a polynomial anymore.

For example, we can have $\frac{1}{u_n+1}u_{n-1}$, which is not a polynomial.

Definition 3.11 Let P_1, P_2 be two key polynomials for the field extension $k(u_1^{(l)},\ldots,u_{n-1}^{(l)})(u_n^{(l)})$ with P_2 and immediate successor of P_1. Let $P_2 = \sum_{j \in S_{P_1}(P_2)} a_j P_1^j$ be the P_1-expansion of P_2.

We call key element every element P'_2 of the form

$$P'_2 = \sum_{j \in S_{P_1}(P_2)} a_j b_j P_1^j$$

where b_j are units of $R_l = k(u_1^{(l)},\ldots,u_n^{(l)})_{(u_1^{(l)},\ldots,u_n^{(l)})}$. The polynomial P_2 is the key polynomial associated to the key element P'_2.

Remark 3.12 A key element is not necessarily a polynomial. Indeed, for example, $\frac{1}{1+u_{nl}^{(l)}}$ is a unit of R_l.

Definition 3.13 Let P'_1 and P'_2 be two key elements. We say that P'_2 is an immediate successor of P'_1, and we write, $P'_1 \ll P'_2$, if their associated key polynomials are immediate successors of each other.

Now we define limit immediate successors key elements.

Definition 3.14 Let P'_1 and P'_2 be two key elements. We say that P'_2 is a limit immediate successor of P'_1, and we write $P'_1 \ll_{\lim} P'_2$, if their associated key polynomials P_1 and P_2 are such that P_2 is a limit immediate successor of P_1.

3.2 Monomialization in the non-degenerate case

In this section, we will monomialize all the elements which are non-degenerate with respect to a system of parameters.

Let α and γ be two elenients of $\mathbb{Z}^n$, and let $\delta = (\min\{\alpha_j, \gamma_j\})_{1 \leq j \leq n}$. We say that $u^\alpha \mid u^\gamma$ if for every integer i, α_i is less than or equal to γ_i , in other words if α is componentwise less than or equal to β.

Let us set

$$\tilde{\alpha} = \alpha - \delta = \left(\tilde{\alpha}_1,\ldots,\tilde{\alpha}_a,0,\ldots,0\right) \in \mathbb{N}^n.$$

The objective is to build a sequence of blow-ups $(R, u) \to \cdots \to (R', u')$ such that in R', we have $u^\alpha \mid u^\gamma$.

Definition 4.1 We say that $\alpha \preceq \gamma$ if for every index i, we have $\alpha_i \leq \gamma_i$.

We assume that $\gamma \npreceq \alpha$ and that $\alpha \npreceq \gamma$. So we may assume that $\mid \tilde{\alpha} \mid \neq 0$, and $\tilde{\alpha}_i > 0$ for every integer $i \in \{1,\ldots,a\}$.

Similarly, we set

$$\tilde{\gamma} = \gamma - \delta = \left(0,\ldots,0,\tilde{\gamma}_{a+1},\ldots,\tilde{\gamma}_n\right) \in \mathbb{N}^n.$$

Interchanging α and γ, if necessary, we may assume that $0 < \mid \tilde{\alpha} \mid \leq \mid \tilde{\gamma} \mid$.

3.2.1 Construction of a stricly decreasing numerical character

Definition 4.2 Let $\tau : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{N}^2$ be the map such that

$$\tau(\alpha, \gamma) = (|\tilde{\alpha}|, |\tilde{\gamma}|).$$

Let J be a minimal subset of $\{1, ..., n\}$ such that $\{1, \ldots, a\} \subset J$ and $\sum_{q \in J} \tilde{\gamma}_q \geq |\tilde{\alpha}|$.
Let π: $(R, u) \to (R_1, u^{(1)})$ be a framed blow-up along (u_J). Let $j \in J$ be such that R_1 is a localization of $R[\frac{u_J}{u_j}]$.
If $q \in J \setminus \{j\}$, we recall that $u'_q = \frac{u_q}{u_j}$, and $u'_q = u_q$ otherwise.

We now define $\tilde{\alpha}'_q = \tilde{\alpha}_q$ for $q \neq j$, and $\tilde{\alpha}'_q = 0$ otherwise. We set $\tilde{\gamma}'_q = \tilde{\gamma}_q$ if $q \neq j$, $\tilde{\gamma}'_q = \sum_{q \in J} \tilde{\gamma}_q - |\tilde{\alpha}|$ otherwise.
And finally we define

$$\delta' = (\delta_1, \ldots, \delta_{j-1}, \sum_{q \in J} \delta_q + |\tilde{\alpha}|, \delta_{j+1}, \ldots, \delta_n).$$

So we have:

$$\begin{aligned} u^\alpha &= \prod_{l=1}^{n} u_l^{\alpha_l} \\ &= \prod_{\substack{l=1 \\ l \in J \setminus \{j\}}}^{n} u_l^{\alpha_l} \times \prod_{\substack{l=1 \\ l \notin J \setminus \{j\}}}^{n} u_l^{\alpha_l}. \end{aligned}$$

But for every $l \in J \setminus \{j\}$, we have $u_l = u'_l \times u_j$ and for $l \notin J \setminus \{j\}$, we have $u_l = u'_l$. Hence

$$u^\alpha = \prod_{\substack{l=1 \\ l \in J \setminus \{j\}}}^{n} \left(u'_l \times u_j\right)^{\alpha_l} \times \prod_{\substack{l=1 \\ l \notin J \setminus \{j\}}}^{n} \left(u'_l\right)^{\alpha_l}.$$

Let us isolate the term u_j. We obtain:

$$u^\alpha = u_j^{\sum_{l \in J \setminus \{j\}} \alpha_l} \times \prod_{l=1}^{n} \left(u'_l\right)^{\alpha_l}$$

and since $\tilde{\alpha} = \alpha - \delta$, we have $\alpha = \tilde{\alpha} + \delta$ and then

$$u^\alpha = u_j^{\sum_{l \in J \setminus \{j\}} \alpha_l} \times \prod_{l=1}^{n} \left(u'_l\right)^{\alpha_l + \delta_l} = u_j^{\sum_{l \in J \setminus \{j\}} \alpha_l} \times \prod_{\substack{l=1 \\ l \neq j}}^{n} \left(u'_l\right)^{\alpha_l + \delta_l} \times \left(u'_j\right)^{\alpha_j + \delta_j}.$$

But $\tilde{\alpha}'_q = \tilde{\alpha}_q$ for $q \neq j$ and $\delta' = (\delta_1, \ldots, \delta_{j-1}, \sum_{q \in J} \delta_q + |\tilde{\alpha}|, \delta_{j+1}, \ldots, \delta_n)$, so

$$\begin{aligned} u^\alpha &= u_j^{\sum_{l \in J \setminus \{j\}} \alpha_l} \times \prod_{\substack{l=1 \\ l \neq j}}^{n} \left(u'_l\right)^{\tilde{\alpha}'_l + \delta'_l} \times \left(u'_j\right)^{\tilde{\alpha}_j + \delta_j} \\ &= u_j^{\sum_{l \in J \setminus \{j\}} \alpha_l + \tilde{\alpha}_j + \delta_j} \times \prod_{\substack{l=1 \\ l \neq j}}^{n} \left(u'_l\right)^{\tilde{\alpha}'_l + \delta'_l}. \end{aligned}$$

We include another time the term $l = j$ in the product, and then:

$$
\begin{aligned}
u^{\alpha} &= u_j^{\sum_{l\in J\setminus\{j\}}\alpha_l+\tilde{\alpha}_j+\delta_j-\tilde{\alpha}'_j-\delta'_j} \times \prod_{l=1}^{n}\left(u'_l\right)^{\tilde{\alpha}'_l+\delta'_l} \\
&= u_j^{\sum_{l\in J\setminus\{j\}}\alpha_l+\tilde{\alpha}_j+\delta_j-\tilde{\alpha}'_j-\delta'_j} \times \left(u'\right)^{\tilde{\alpha}'+\delta'}.
\end{aligned}
$$

But we have

$$
\begin{aligned}
\sum_{l\in J\setminus\{j\}}\alpha_l+\tilde{\alpha}_j+\delta_j-\tilde{\alpha}'_j-\delta'_j &= \sum_{l\in J\setminus\{j\}}\alpha_l+\tilde{\alpha}_j+\delta_j-\delta'_j \\
&= \sum_{l\in J\setminus\{j\}}\alpha_l+\tilde{\alpha}_j+\delta_j-\sum_{q\in J}\delta_q-|\tilde{\alpha}| \\
&= \sum_{l\in J\setminus\{j\}}\left(\tilde{\alpha}_l+\delta_l\right)+\tilde{\alpha}_j-\sum_{q\in J\setminus\{j\}}\delta_q-|\tilde{\alpha}| \\
&= \sum_{l\in J}\tilde{\alpha}_l-|\tilde{\alpha}| \\
&= 0.
\end{aligned}
$$

So $u^{\alpha}=(u')^{\tilde{\alpha}'+\delta'}$, and similarly $u^{\gamma}=(u')^{\tilde{\gamma}'+\delta'}$.
We set $\alpha'=\delta'+\tilde{\alpha}'$ and $\gamma'=\delta'+\tilde{\gamma}'$.
Proposition 4.3 We have $\tau(\alpha', \gamma') < \tau(\alpha, \gamma)$.
Proof. First case: $j\in\{1,\dots,a\}$. Then

$$|\tilde{\alpha}'|=|\tilde{\alpha}|-\tilde{\alpha}_j<|\tilde{\alpha}|.$$

Second case: $j\in\{a+1,\dots,n\}$. Then $|\tilde{\alpha}'|=|\tilde{\alpha}|$. Let us show that $|\tilde{\gamma}'|<|\tilde{\gamma}|$. We have

$$|\tilde{\gamma}'|=\sum_{\substack{q=a+1\\ q\neq j}}^{n}\tilde{\gamma}_q+\sum_{q\in J}\tilde{\gamma}_q-|\tilde{\alpha}|=\sum_{q=a+1}^{n}\tilde{\gamma}_q+\sum_{q\in J\setminus\{j\}}\tilde{\gamma}_q-|\tilde{\alpha}|.$$

By the minimality of J, we have $\sum_{q\in J\setminus\{j\}}\tilde{\gamma}_q-|\tilde{\alpha}|<0$, and so

$$|\tilde{\gamma}'|<\sum_{q=a+1}^{n}\tilde{\gamma}_q=|\tilde{\gamma}|.$$

In every case, we have $\left(|\tilde{\alpha}'|,|\tilde{\gamma}'|\right)<\left(|\tilde{\alpha}|,|\tilde{\gamma}|\right)=\tau(\alpha,\gamma)$.

If $|\tilde{\alpha}'|\le|\tilde{\gamma}'|$, then $\tau(\alpha',\gamma')=(|\tilde{\alpha}'|,|\tilde{\gamma}'|)$ and this completes the proof.
Otherwise, $|\tilde{\alpha}'|>|\tilde{\gamma}'|$, so

$$\tau(\alpha',\gamma')=\left(|\tilde{\gamma}'|,|\tilde{\alpha}'|\right)<\left(|\tilde{\alpha}'|,|\tilde{\gamma}'|\right),$$

and the proof is complete.

Renumbering the u'_q, if necessary, we may assume that $u'_q\notin R_1^{\times}$ for every $q\in\{1,\dots,s\}$ and $u'_q\in R_1^{\times}$ otherwise. Since π is a framed blow-up, we have $\{u'_1,\dots,u'_s\}\subset u^{(1)}$, so renumbering again, if necessary, we may assume that $u'_q=u_q^{(1)}$ for every $q\in\{1,\dots,s\}$. We set

$$\alpha^{(1)}=\left(\alpha'_1,\dots,\alpha'_s,0,\dots 0\right)\in\mathbb{Z}^{n_1}$$

and

$\gamma^{(1)} = (\gamma'_1,\dots,\gamma'_s,0,\dots 0) \in \mathbb{Z}^{n_1}$.

We have $\tau(\alpha^{(1)},\gamma^{(1)}) \leq \tau(\alpha',\gamma')$. By Proposition 4.3, we have

$\tau(\alpha^{(1)},\gamma^{(1)}) < \tau(\alpha,\gamma)$.

3.2.2 Divisibility and change of variables

Let $s \in \{1,\dots,n\}$. We write $u = (w, v)$ where
$w = (w_1, ..., w_s) = (u_1, ..., u_s)$

and

$v = (v_1, ..., v_{n-s})$.

Let α and γ be two elements of $\mathbb{Z}^s$.

Proposition 4.4 There exists a framed local sequence

$(R, u) \to (R_l, u^{(l)})$,

with respect to v independent of v, such that in R_l , we have $w^\alpha \mid w^\gamma$ or $w^\gamma \mid w^\alpha$.

Proof. Unless $\gamma \preceq \alpha$, or $\alpha \preceq \gamma$, we can iterate the above construction, choosing blow-up with respect to v and independent of v. Since τ is a vector in $\mathbb{N}^2$ and is stricly decreasing, after a finite number of steps, the process stops. After these steps, we have $w^\alpha = U \times (u^{(l)})^{\alpha^{(l)}}$, $w^\gamma = U \times (u^{(l)})^{\gamma^{(l)}}$, with $U \in R_l^\times$ and with $\gamma^{(l)} \preceq \alpha^{(l)}$, or $\alpha^{(l)} \preceq \gamma^{(l)}$. So we do have $w^\alpha \mid w^\gamma$ or $w^\gamma \mid w^\alpha$ in R_l ,

Let us now study the change of variables we do at each blow-up. We consider i and i' some indexes of the framed local sequence

$$(R,u) \to \dots \to (R_i,u^{(i)}) \to \dots \to (R_{i'},u^{(i')}) \to \dots \to (R_l,u^{(l)}). \tag{5}$$

Proposition 4.5 Let us consider $0 \leq i < i' \leq l$. We let m be an element of $\{1, ..., n_i\}$ and m' one of $\{1, ..., n_{i'}\}$. Then:

(1) There exists a vector $\delta_m^{(i',i)} \in \mathbb{N}^{\sharp D_i}$ such that

$$u_m^{(i)} \in \left(u_{D_{i'}}^{(i')}\right)^{\delta_m^{(i',i)}} R_{i'}^\times.$$

(2) If, in addition, the local sequence (5) is independent of u_T, with $T \subset \{1,\dots,n\}$; and if we assume that $u_m^{(i)} \notin u_T$, then $(u_{D_{i'}}^{(i')})^{\delta_m^{(i',i)}}$ is monomial in $u_{D_{i'}}^{(i')} \setminus u_T$.

(3) We assume that $i'' > 0$ such that $i \leq i'' < i'$. We have $D_{i''} = \{1, ..., n_{i''}\}$, and we assume that $m' \in D_{i'}$. Then exists a vector $\gamma_{m'}^{(i,i')}$ of $\mathbb{Z}^{n_i}$ such that

$$u_{m'}^{(i')} = \left(u^{(i)}\right)^{\gamma_{m'}^{(i,i')}}.$$

(4) If, in addition, the local sequence (4.1) is independent of u_T and if we assume that $u_{m'}^{(i')} \notin u_T$, then $u_{m'}^{(i')}$ is monomial in $u^{(i)} \setminus u_T$.

Proof. We only consider the case $i' - i + 1$, the general case can be proved by induction on $i - i'$. We can also assume that $i = 0$.

Let us show (1). By DeHnition 3.3, we have $u'_{A_1 \cup B_1 \cup \{j_1\}} = u_{D_1}^{(1)}$.

We denote by $D_1 = D_1^{A_1} \cup D_1^{B_1}$ where

$$u'_{A_1} = u_{D_1^{A_1}}^{(1)}$$

and

$$u'_{B_1\cup\{j_1\}} = u^{(1)}_{D_1^{B_1}}.$$

If $m \in A_1 \cup \{j_1\}$, so $u_m = u'_m$ and the proof is finished. If $m \in B_1$ then $u_m = u_{j_1} u'_m = u'_{j_1} u'_m$ and the proof is finished.

If $m \in C_1$, so $u_m = u'_{j_1} u'_m$ and by ddinition, $u'_m \in R_1^{\times}$, which gives us the result.

Let us show (3). We have $m' \in D_1 = D_1^{A_1} \cup D_1^{B_1}$ and $u'_{A_1\cup B_1\cup\{j_1\}} = u^{(1)}_{D_1}$. If $m' \in D_1^{A_1}$ then by definition $u^{(1)}_{m'} \in u'_{A_1} = u_{A_1}$ and we have the result. Otherwise $m' \in D_1^{B_1}$. So

$$u^{(1)}_{m'} \in u'_{B_1\cup\{j_1\}} = \left\{ u_{j_1}, \frac{u_q}{u_{j_1}} \; q \in B_1 \right\}.$$

This completes the proof of (3).

Now let us assume that the sequence is independent of u_T. By definition we have $u_{J_1} \cap u_T = \emptyset$ and also

$$u^{(1)}_{D_1^{B_1}} \cap u_T = \emptyset.$$

Let us show (2). Assume that $u_m \notin u_T$.

If $m \in A_1$, then $u_m = u'_m \in u^{(1)}_{D_1^{A_1}}$ and $u_m \notin u_T$ and the proof is finished. Otherwise $m \in J_1$. We saw in the proof of (1) that m was monomial in $u^{(1)}_{D_1^{B_1}}$, and since $u^{(1)}_{D_1^{B_1}} \cap u_T = \emptyset$, this completes the proof of (2).

It remains to prove (4). We assume that $u^{(1)}_{m'} \notin u_T$, with $m' \in D_1 = D_1^{A_1} \cup D_1^{B_1}$.

If $m' \in D_1^{A_1}$, then $u^{(1)}_{m'} \in u'_{A_1} = u_{A_1}$. Since $u^{(1)}_{m'} \notin u_T$, we have $u^{(1)}_{m'} \in u \setminus u_T$.

Otherwise $m' \in D_1^{B_1}$ and we saw that $u^{(1)}_{m'}$ is monomial in $u_{B_1\cup[j_1\}} \subset u_J$. Since $u_J \cap u_T = \emptyset$, we are done.

Remark 4.6 Let $T \subset A$, be a set of cardinality t, and $s := n - t$. We set

$$v = (v_1, \ldots, v_t) = u_T$$

and

$$w = (w_1, \ldots, w_s) = u_{\{1,\ldots,n\}\setminus T}.$$

In this Remark, we only consider monomial blow-ups.

We have $u' = (v, w')$ where $w' = (w'_1, \ldots, w'_s) = (w^{\gamma(1)}, \ldots, w^{\gamma(s)})$ with $\gamma(i) \in \mathbb{Z}^s$, by Proposition 4.5. By the proof of this Proposition, the matrix $F_s = [\gamma(1) \ldots \gamma(s)]$ is a unimodular matrix. For every $\delta \in \mathbb{Z}^s$, we have $w'^{\delta} = w^{\delta F_s}$. In the same vein $w_i = w'^{\delta(i)}$ and the s-vectors $\delta(1), \ldots, \delta(s)$ form a unimodular matrix equal to the inverse of F_s. Then we have $w'^{\gamma} = w^{\gamma F_s^{-1}}$, for every $\gamma \in \mathbb{Z}^s$.

Proposition 4.7 We have:

$$w^{\alpha} \mid w^{\gamma} \text{ in } R_l \Leftrightarrow \nu(w^{\alpha}) \leq \nu(w^{\gamma}).$$

Proof. We have $u^{(l)} = (w_1^{(l)}, \ldots, w_{r_l}^{(l)}, v)$.

By Proposition 4.5, there exists $\alpha^{(l)}, \gamma^{(l)} \in \mathbb{N}^{r_l}$ and $y, z \in R_l^{\times}$ such that $w^{\alpha} = y(w^{(l)})^{\alpha^{(l)}}$ and $w^{\gamma} = z(w^{(l)})^{\gamma^{(l)}}$.

For every $i \in \{1, \ldots, r_l\}$, we have $\nu(w_i^{(l)}) \geq 0$ since the blow-up is with respect to ν, so centered in R_l, By constniction of R_l, we have that $\gamma^{(l)} \preceq \alpha^{(l)}$ or $\alpha^{(l)} \preceq \gamma^{(l)}$.

So

$$\left(w^{(l)}\right)^{\alpha^{(l)}} | \left(w^{(l)}\right)^{\gamma^{(l)}} \Leftrightarrow \nu\left(\left(w^{(l)}\right)^{\alpha^{(l)}}\right) \leq \nu\left(\left(w^{(l)}\right)^{\gamma^{(l)}}\right),$$

hence

$$w^{\alpha} | \ w^{\gamma} \Leftrightarrow \nu(w^{\alpha}) \leq \nu(w^{\gamma}).$$

3.2.3 Monomialization of non-degenerate elements

Let N be an ideal of R generated by monomials in w. We choose $w^{\epsilon_0}, \ldots, w^{\epsilon_b}$ to be a minimal set of generators of N, with $\nu(w^{\epsilon_0}) \leq \nu(w^{\epsilon_i})$ for every i.

Proposition 3.2.8 There exists a local framed sequence

$$\phi : (R, u) \to \left(R_l, u^{(l)}\right)$$

with respect to ν, independent of v and such that $NR_l = (w^{\epsilon_0})R_l$.

Proof. Let

$$\tau(N, w) := \begin{cases} \left(b, \min\limits_{0 \leq i < j \leq b} \tau\left(w^{\epsilon_i}, w^{\epsilon_j}\right)\right) & \text{if } b \neq 0 \\ (0,1) & \text{otherwise.} \end{cases}$$

Assume $b \neq 0$.

We let $\left(w^{\epsilon_{i_0}}, w^{\epsilon_{j_0}}\right)$ be a pair for which the minimum

$$\min_{0 \leq i < j \leq b} \tau\left(w^{\epsilon_i}, w^{\epsilon_j}\right)$$

is attained. By Proposition 3.2.3, $\tau(N, w)$ is strictly decreasing at each blow-up.

Since the process stops, NR_l is generated by a unique element as an ideal of R_l. By Proposition 3.2.7, this element is w^{ϵ_0} (which has the minimal value), which divides the others. Then $NR_l = (w^{\epsilon_0})R_l$.

Definition 3.2.9 An element f of R is monomializable if there exists a sequence of blow-ups

$$(R, u) \to (R', u')$$

such that the total transformed of f is a monomial. It means that in R', the total transform of f is $v\prod_{i=1}^{n}(u_i')^{\alpha_i}$, with v a unit of R'.

Theorem 3.2.10 Let f be a non-degenerate element with respect to $u = (w, \nu)$, and let N be the ideal which satisfies the conclusion of the Proposition 3.1.2, generated by monomials in w.

Then there exists a local framed sequence, independent of ν,

$$(R, u) \to (R', u')$$

such that f is a monomial in u' multiplied by a unit of R'. Equivalently, f is monomializable.

Proof. Let $(R, u) \to (R', u')$ be the local framed sequence of the Proposition 3.2.8. We have $NR' = w^{\epsilon_0}R'$. Since $f \in N$, by the proof of the Proposition 3.1.2, there exists an element $z \in R'$ such that $f = w^{\epsilon_0}z$. Since ν is centered in R', to show that z is a unit of R', we will show that $\nu(z) = 0$.

But $\nu(z) = \nu(f) - \nu(w^{\epsilon_0}) = \nu(N) - \nu(w^{\epsilon_0})$ by Proposition 3.1.2.

Since $NR' = w^{\epsilon_0}R'$, we have $\nu(N) = \nu(w^{\epsilon_0})$, and so $\nu(z) = 0$, and this completes the proof.

3.3 Non-degeneracy and key polynomials

Now that we monomialized every non-degenerate element with respect to the generators of the maximal ideal of our local ring, we are going to show that every element is non-degenerate with respect to a particular sequence of immediate successors. We denote by Λ the set of key polynomials and

$$M_\alpha := \{Q \in \Lambda \text{ such that deg } (Q)=\alpha\}.$$

Proposition 3.3.1 We consider ν an archimedean valuation centered in a noetherian local domain $(R, \mathfrak{m}, k)$. We denote by Γ the value group of ν and we set $\Phi := \nu(R \setminus (0))$.

The set Φ does not contain an infinite bounded strictly increasing sequence.

Proof. Assume, aiming for contradiction, that we have an infinite sequence

$$\alpha_1 < \alpha_2 < \dots$$

of elements of Φ bounded by an element $\beta \in \Phi$.

Then we have an infinite decreasing sequence $\dots \subseteq P_{\alpha_2} \subseteq P_{\alpha_1}$ such that for every index i, we have $P_\beta \subseteq P_{\alpha_i}$. And so we have an infinite decreasing sequen of ideals of $\frac{R}{P_\beta}$.

We set

$$\delta = \nu(\mathfrak{m}) = \min_{x \in \Phi \setminus \{0\}} \{\nu(x)\}.$$

Since ν is archimedean, we know that there exists a non-zero integer n such that $\beta \leq n\delta$, and so such that $\mathfrak{m}^n \subseteq P_\beta$. This way, we construct an epimorphism of rings $\frac{R}{\mathfrak{m}^n} \twoheadrightarrow \frac{R}{P_\beta}$. Since the ring R is noetherian, $\frac{R}{\mathfrak{m}^n}$ is artinian, and so is $\frac{R}{P_\beta}$. This contradicts the existence of the infinite decreasing sequence of ideals of $\frac{R}{P_\beta}$.

Definition 3.3.2 Assume that the set M_α is non-empty and does not have an maximal element. Assume also that there exists a key polynomial $Q \in \Lambda$ such that $\epsilon(Q) > \epsilon(M_\alpha)$. We call a limit key polynomial every polynomial of minimal degree which has this property.

Definition 3.3.3 Let $(Q_i)_{i\in\mathbb{N}}$ be a sequence of key polynomials. We say that it is a sequence of immediate successors if for every integer i, we have $Q_i < Q_{i+1}$.

Proposition 3.3.4 If there are no limit key polynomials then there exists a finite or infinite sequence of immediate successors $Q_1 < \dots < Q_i < \dots$ such that the sequence $\{\epsilon(Q_i)\}$ is cofinal in $\epsilon(\Lambda)$. Equivalently, such that

$$\forall Q \in \Lambda \ \exists i \text{ such that } \epsilon(Q_i) \geq \epsilon(Q).$$

Proof. We do the proof by contrapositive.

Assume that for every finite or infinite sequence of immediate successors key polynomials Q_i, the sequence $\{\epsilon(Q_i)\}$ is not cofinal in $\epsilon(\Lambda)$. Let us show that there exists a limit key polynomial.

First let assume that for every $\alpha \in \Omega = \{\beta \text{ such that } M_\beta \neq \phi\}$, M_α has a maximal element. It means that

$$\forall \alpha \in \Omega \ \exists R_\alpha \in M_\alpha \text{ such that } \forall Q \in M_\alpha, \epsilon(R_\alpha) \geq \epsilon(Q).$$

We set $M := \{R_\alpha\}_{\alpha\in\Omega}$. All elements in M are of distinct degree, so they are strictly ordered by their degrees. So if $\alpha < \alpha'$, then $\deg(R_\alpha) < \deg(R_{\alpha'})$. Since $R_{\alpha'}$ is a key polynomial, by definition, we have $\epsilon(R_\alpha) < \epsilon(R_{\alpha'})$ as soon as $\alpha < \alpha'$. Then in M the elements are strictly ordered by their values of ϵ.

Let us show that they are immediate successors. Let R_α and $R_{\alpha'}$ be two consecutive elements of M. We know that

$$\alpha = \deg(R_\alpha) < \deg(R_{\alpha'}) = \alpha'$$

and $\epsilon(R_\alpha) < \epsilon(R_{\alpha'})$. We want to show that $R_{\alpha'}$ is of minimal degree for the property. So let us set $R \in \Lambda$ such that $\epsilon(R_\alpha) < \epsilon(R)$ and $\deg(R) \leq \deg(R_{\alpha'})$. Let us show that $\deg(R) = \deg(R_{\alpha'}) = \alpha'$. Since $\epsilon(R_\alpha) < \epsilon(R)$ and since R_α is a key polynomial, by definition,

$$\deg(R_\alpha) = \alpha \le \deg(R) \le \alpha'.$$

Since R is a key polynomial, if we had $\deg(R) = \deg(R_\alpha)$, then we should have $\epsilon(R_\alpha) \ge \epsilon(R)$, which is a contradiction. Let us set $\lambda := \deg(R)$, so we have $\alpha < \lambda \le \alpha'$, $R \in M_\lambda$ and $R_\lambda \in M$. Since the polynomials in M are strictly ordered by their degrees and that R_α and $R_{\alpha'}$ are consecutive, then we have $\lambda = \alpha'$, and so $R\alpha < R_{\alpha'}$.

So the set M is a sequence of immediate successors. By hypothesis, the sequence $\epsilon(M)$ is not cofinal, so there exists $R \in \Lambda$ such that $\epsilon(R) > \epsilon(M)$. But then there exists α such that $R \in M_\alpha$ and then $\epsilon(R_\alpha) \ge \epsilon(R) > \epsilon(R_\alpha)$. It is a contradiction.

So there exists $\alpha \in \Omega$ such that M_α does not have any maximal ideal. Then we have a sequence:

$$\epsilon(Q_1) < \epsilon(Q_2) < \ldots < \epsilon(Q_i) < \ldots$$

where Q_i is an element of M_α for every integer i.

Let us show that the Q_i are immediate successors. Let $R \in \Lambda$ such that $\epsilon(Q_i) < \epsilon(R)$ and $\deg(R) \le \deg(Q_{i+1}) = \alpha$. Since Q_i is a key polynomial, by definition, $\deg(R) \ge \deg(Q_i) = \alpha$. So $\deg(R) = \deg(Q_{i+1}) = \alpha$, and Q_{i+1} is of minimal degree for the property. Then for every integer i, we have $Q_i < Q_{i+1}$.

By hypothesis, the sequence of the Q_i is a sequence of immediate successors, so the sequence $(\epsilon(Q_i))_i$ is not cofinal. So there exists a key polynomial $Q \in \Lambda$ such that $\epsilon(Q) > \epsilon(Q_i)$ for every integer i. Let $R \in M_\alpha$, since M_α does not have a maximal element, there exists i such that $\epsilon(R) < \epsilon(Q_i) < \epsilon(Q)$. So there exists a key polynomial $Q \in \Lambda$ such that $\epsilon(Q) > \epsilon(M_\alpha)$. Then the polynomial Q is a limit key polynomial.

Theorem 3.3.5 There exists a finite or infinite sequence $(Q_i)_{i \ge 1}$ of key polynomials such that for each i the polynomial Q_{i+1} is either an optimal or a limit immediate successor of Q_i and such that the sequence $\{\epsilon(Q_i)\}$ is cofinal in $\epsilon(\Lambda)$ where Λ is the set of key polynomials.

Proof. We know that x is a key polynomial. If for every key polynomial $Q \in \Lambda$, we have $\epsilon(x) \ge \epsilon(Q)$, then the sequence $\{\epsilon(x)\}$ is cofinal in $\epsilon(\Lambda)$ and it is done. Otherwise, it exists a key polynomial $Q \in \Lambda$ such that $\epsilon(x) < \epsilon(Q)$. If it exists a maximal element among the key polynomials of same degree than Q, then we exchange Q by this element. By Proposition 2.12, it exists a finite sequence $Q_1 = x < \cdots < Q_p = Q$ of optimal (possibly limit) immediate successors which begins at x and ends at Q.

If for every key polynomial $Q' \in \Lambda$, there exists a key polynomial of this sequence Q_i such that $\epsilon(Q_i) \ge \epsilon(Q')$, then the sequence $\{\epsilon(Q_i)\}$ is cofinal in $\epsilon(\Lambda)$ and it is over.

Otherwise there exists a polynomial $Q' \in \Lambda$ such that for every integer $i \in \{1,..., p\}$, we have $\epsilon(Q_i) < \epsilon(Q')$. So $\epsilon(Q_p) < \epsilon(Q')$ and we use Proposition 2.12 again to construct a sequence of optimal (possibly limit) immediate successors which begins at Q_p and ends at Q'. So we have a sequence $Q_1 = x,..., Q_r = Q'$ of optimal (possibly limit) immediate successors which begins at x and ends at Q'.

We iterate the process until the sequence $\{\epsilon(Q_i)\}$ is cofinal in $\epsilon(\Lambda)$. If Q_i is maximal among the set of key polynomials of degree $\deg_X(Q_i)$, then $\deg_X(Q_i) < \deg_X(Q_{i+1})$. If $Q_i <_{\lim} Q_{i+1}$, we have again $\deg_X(Q_i) < \deg_X(Q_{i+1})$. In fact, the degree of the polynomials of the sequence stricly increase at least each two steps, so the process stops.

Proposition 3.3.6 Assume that $k = k_\nu$. There exists a finite or infinite sequence $(Q_i)_{i \ge 1}$ of key polynomials such that for each i the polynomial Q_{i+1} is either an optimal or a limit immediate successor of Q_i and such that the sequence $\{\epsilon(Q_i)\}$ is cofinal in $\epsilon(\Lambda)$ where Λ is the set of key polynomials.

And this sequence is such that: if $Q_i < Q_{i+1}$, then the Q_i-expansion of Q_{i+1} has exactly two terms.

Proof. We have $Q_1 = x$, and we assume that $Q_1, Q_2,..., Q_i$ have been constructed. We note $a := \deg_x(Q_i)$ and recall that

$$G_{<a} = \sum_{\deg_x(P)<a} \mathrm{in}_{\nu_{Q_i}}(P) G_\nu .$$

If Q_i is maximal in Λ, we stop. Otherwise, Q_i is not maximal and so it has an immediate successor.

We set $\alpha := \min\{h \in \mathbb{N}^* \text{ such that } h\nu(Q_i) \in \Delta_{<a}\}$ where $\Delta_{<a}$ is the subgroup of Γ generated by the values of the elements of $G_{<a}$

In fact, there exists a polynomial f of degree strictly less than a such that $\alpha\nu(Q_i) = \nu(Q_i^\alpha) = \nu(f) \neq 0$.

Then, since $k_\nu = k$, there exists $c \in k^*$ such that $\text{in}_\nu(Q_i^\alpha) = \text{in}_\nu(cf)$.

We set $Q = Q_i^\alpha - cf$. By the proof of Proposition 2.5, we have $\epsilon(Q_i) < \epsilon(Q)$.

Let us show that $Q_i < Q$. We only have to show that Q is of minimal degree.

So let us set P a key polynomial such that $\epsilon(Q_i) < \epsilon(P)$.

Assume by contradiction that $\deg(P) < a\alpha$. We set $P = \sum_{j=0}^{\alpha-1} p_j Q_i^j$ the Q_i-expansion of P. Then by the proof of Proposition 2.5, we have $\sum_{j=0}^{\alpha-1} \text{in}_\nu(p_j)\,\text{in}_\nu(Q_i)^j = 0$, which contradicts the minimality of α.

Then Q is of minimal degree and $Q_i < Q$. Since it has just two terms in his Q_i-expansion, it is an optimal immediate successor of Q_i.

First case: $\alpha > 1$. Then we set $Q_{i+1} := Q$ and we iterate.

Second case: $\alpha = 1$. Then all the elements of M_{Q_i} have same degree than Q_i. If M_{Q_i} does not have a maximal element, then we do the same thing than in the proof of Proposition 2.12 and we set Q_{i+1} a limit immediate successor of Q_i.

Otherwise, M_{Q_i} has a maximal element Q_{i+1}. This element has same degree as Q_i, so we have $Q_{i+1} = Q_i - h$ with h of degree strictly less than the degree of Q_i. Then it is an immediate successor of Q_i which Q_i-expansion admits uniquely two terms. So it is optimal, and this completes the proof.

We now assume $k = k_\nu$ and consider $\mathcal{Q} := (Q_i)_i$ a sequence of optimal (possibly limit) immediate successors such that $(\epsilon(Q_i))_i$ is cofinal in $\epsilon(\Lambda)$ and such that if $Q_i < Q_{i+1}$, then the Q_i-expansion of Q_{i+1} admits exactly two terms.

Remark 3.3.7 We keep the same hypothesis as in Example 1.8. Then $\mathcal{Q} = \{z, Q\}$.

Corollary 3.3.8 For every polynomial f, there exists an index i such that $\nu_{Q_i}(f) = \nu(f)$.

Proof. By Proposition 1.21, there exists a key polynomial Q such that $\nu_Q(f) = \nu(f)$.

The sequence $\{\epsilon(Q_i)\}$ being cofinal, there exists an index i such that

$$\epsilon(Q_i) \geq \epsilon(Q).$$

By Proposition 1.20, $\nu_Q(f) \leq \nu_{Q_i}(f)$ and since $\nu_Q(f) = \nu(f)$, we have $\nu_{Q_i}(f) = \nu(f)$.

Remark 3.3.9 So, for every polynomial f, there exists a key polynomial Q_i of the sequence $\mathcal{Q}$ such that f is non-degenerate with respect to Q_i.

Remark 3.3.10 Let $Q_i \in \mathcal{Q}$. We don't assume here $k = k_\nu$.

We set $a_i := \deg_x(Q_i)$ and $\Gamma_{<a_i}$ the group $\nu(G_{<a_i} \setminus \{0\})$.

If $\nu(Q_i) \notin \Gamma_{<a_i} \otimes_{\mathbb{Z}} \mathbb{Q}$, then $\epsilon(Q_i)$ is maximal in $\epsilon(\Lambda)$ and the sequence $\mathcal{Q}$ stops at Q_i.

3.4 Monomialization of the key polynomials

We set $K := k(u_1, ..., u_{n-1})$ and we consider the extension $K(u_n)$. We consider also a sequence of key polynomials $\mathcal{Q}$ as in the section 3.3.

In other words, $\mathcal{Q} = (Q_i)_i$ is a sequence of optimal (possibly limit) immediate successors such that $(\epsilon(Q_i))_i$ is cofinal in $\epsilon(\Lambda)$.

Let f be an element of R. We know that this element is non-degenerate with respect to a key polynomial of the sequence $\mathcal{Q}$. We also know that every element non-degenerate with respect to a regular system of parameters is monomializable.

Then, to monomialize f, it is enough to monomialize the set of key polynomials of this sequence. We assume in this part that the residue field is k.

3.4.1 Generalities

Let $r := r(R, u, \nu)$ be the dimension of

$$\sum_{i=1}^{n} \nu(u_i)\mathbb{Q}$$

in $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. Renumbering, if necessary, we can assume that $\nu(u_1),\ldots, \nu(u_r)$ are rationally independent and we consider Δ the subgroup of Γ generated by $\nu(u_1),\ldots, \nu(u_r)$.

Remark 3.4.1 Let $(R, u) \to (R_1, u^{(1)})$ be a framed blow-up. Then $r \leq r_1 := r\left(R_1, u^{(1)}, \nu\right)$.

Remark 3.4.2 We will consider the framed local blow-ups

$$\left(R, u\right) \to \ldots \to \left(R_i, u^{(i)}\right) \to \ldots$$

Then we write $r_i := r\left(R_i, u^{(i)}, \nu\right)$.

We set $E := \{1,..., r, n\}$ and $\overline{\alpha^{(0)}} := \min_{h \in \mathbb{N}^*} \{h \text{ such that } h\nu(u_n) \in \Delta\}$.

So $\overline{\alpha^{(0)}}\nu(u_n) = \sum_{j=1}^{r} \alpha_j^{(0)} \nu(u_j)$ with, renumbering the $\alpha_i^{(0)}$ if necessary,

$$\alpha_1^{(0)}, \ldots, \alpha_s^{(0)} \geq 0$$

and

$$\alpha_{s+1}^{(0)}, \ldots, \alpha_r^{(0)} < 0$$

We set

$$w = (w_1, \ldots, w_r, w_n) = (u_1, \ldots, u_r, u_n)$$

and

$$v = (v_1, \ldots, v_t) = (u_{r+1}, \ldots, u_{n-1}),$$

with $t = n - r - 1$.

We set $x_i = \mathrm{in}_\nu u_i$, and we have that $x_1,..., x_r$ are algebraically independent over k in G_ν. Let λ_0 be the minimal polynomial of x_n over $k(x_1,..., x_r)$, of degree α.

We set:

$$y = \prod_{j=1}^{r} x_j^{\alpha_j^{(0)}},$$

$$\overline{y} = \prod_{j=1}^{r} w_j^{\alpha_j^{(0)}},$$

$$z = \frac{x_n^{\overline{\alpha^{(0)}}}}{y}$$

and

$$\overline{z} = \frac{w_n^{\overline{\alpha^{(0)}}}}{\overline{y}}.$$

We have

$$\lambda_0 = X^{\alpha} + c_0 y$$

where $c_0 \in k$, and $Z + c_0$ is the minimal polynomial λ_z of z over $\mathrm{gr}_\nu k(x_1, \ldots, x_r)$.

Indeed, $k_\nu \simeq k \simeq \frac{k[Z]}{(\lambda_z)}$ so λ_z is of degree 1 in Z. Then λ_0 is of degree $\alpha^{(0)}$, and so $\alpha = \overline{\alpha^{(0)}}$.

Definition 3.4.3 We say that Q_i is monomializable if there exists a sequence of blow-ups $(R, u) \to (R_l, u^{(l)})$ such that in R_l, Q_i can be written as $u_n^{(l)}$ multiplied by a monomial in $\left(u_1^{(l)}, \ldots, u_{r_l}^{(l)}\right)$ up to a unit of R_l, where $r_l := r\left(R_l, u^{(l)}, \nu\right)$.

We are going to show that there exists a local framed sequence that monomializes all the Q_i.

We have $Q_1 = u_n$, it is a monomial. By the blow-ups, Q_1 stays a monomial. So we have to begin monomializing Q_2.

Since we want to monomialize the key polynomials Q_i of the sequence $\mathcal{Q}$ constructed earlier by induction on i, we are going to do something more general here: we consider an immediate successors (possibly limit) key element Q_2 of Q_1 instead of immediate successor (possibly limit) key polynomial of Q_1.

First, let us consider

$$Q = w_n^{\alpha} + a_0 b_0 \overline{y}$$

where $b_0 \in R$ such that $b_0 \equiv c_0$ modulo $\mathfrak{m}$ and $a_0 \in R^{\times}$.

A priori, Q is not a key polynomial but we are going to prove that we can reduce this case to the case $Q_2 = Q$ by a local framed sequence independent of u_n.

3.4.2 Puiseux packages

Let

$$\gamma = (\gamma_1, \ldots, \gamma_r, \gamma_n) = (\alpha_1^{(0)}, \ldots, \alpha_s^{(0)}, 0, \ldots, 0)$$

and

$$\delta = (\delta_1, \ldots, \delta_r, \delta_n) = (0, \ldots, 0, -\alpha_{s+1}^{(0)}, \ldots, -\alpha_r^{(0)}, \alpha).$$

We have

$$w^{\delta} = w_n^{\delta_n} \prod_{j=1}^{r} w_j^{\delta_j} = \frac{w_n^{\alpha}}{\prod_{j=s+1}^{r} w_j^{\alpha_j^{(0)}}}$$

and

$$w^{\gamma} = \prod_{j=1}^{s} w_j^{\alpha_j^{(0)}}.$$

So $\dfrac{w^{\delta}}{w^{\gamma}} = \dfrac{w_n^{\alpha}}{\prod_{j=1}^{r} w_j^{\alpha_j^{(0)}}} = \overline{z}$.

Let us compute the value of w^{δ}.

$$\begin{aligned}
\nu(w^{\delta}) &= \alpha\nu(w_n) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(w_j) \\
&= \alpha\nu(u_n) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(u_j) \\
&= \sum_{j=1}^{r}\alpha_j^{(0)}\nu(u_j) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(u_j) \\
&= \sum_{j=1}^{s}\alpha_j^{(0)}\nu(w_j) \\
&= \nu(\prod_{j=1}^{s} w_j^{\alpha_j^{(0)}}) \\
&= \nu(w^{\gamma}).
\end{aligned}$$

Theorem 3.4.4 There exists a local framed sequence

$$\left(R,u\right) \xrightarrow{\pi_0} \left(R_1,u^{(1)}\right) \xrightarrow{\pi_1} \cdots \xrightarrow{\pi_{l-1}} \left(R_l,u^{(l)}\right) \qquad (6)$$

with respect to ν, independent of v, and that has the next properties:

For every integer $i \in \{1,..., l\}$, we write $u^{(i)} := \left(u_1^{(i)},\dots,u_n^{(i)}\right)$ and we recall that k is the residue field of R_i .

(1) The blow-ups $\pi_0,..., \pi_{l-2}$ are monomials.

(2) We have $\overline{z} \in R_l^{\times}$.

(3) We set $u^{(l)} := \left(w_1^{(l)},\dots,w_r^{(l)},v,w_n^{(l)}\right)$. So for every integer $j \in \{1,..., r, n\}$, w_j is a monomial in $w_1^{(l)},\dots,w_r^{(l)}$ multiplied by an element of $R_l^{\times}$. And for every integer $j \in \{1,\dots,r\}$, $w_j^{(l)} = w^{\eta}$ where $\eta \in \mathbb{Z}^{r+1}$.

(4) We have $Q = w_n^{(l)} \times \overline{y}$.

Proof. We apply Proposition 3.2.4 to (w^{δ}, w^{γ}) and so we obtain a local framed sequence for ν, independent of v and such that $w^{\gamma} \mid w^{\delta}$ in R_l.

By Proposition 3.2.7 and the fact that w^{δ} and w^{γ} have same value, we have that $w^{\delta} \mid w^{\gamma}$ in R_l. In fact $\overline{z}, \overline{z}^{-1} \in R_l^{\times}$. So we have (2).

We choose the local sequence to be minimal, in other words the sequence made by $\pi_0,..., \pi_{l-2}$ does not satisfy the conclusion of the Proposition 3.2.4 for (w^{δ}, w^{γ}). Now we are going to prove that this sequence satisfies the five properties of Theorem 3.4.4. Let $i \in \{0,..., l\}$. We write $w^{(i)} = \left(w_1^{(i)},\dots,w_r^{(i)},w_n^{(i)}\right)$, with $r = n - t - 1$ and define J_i, A_i, B_i, j_i and D_i similarly that we defined J, A, B, j and D_1, considering the i-th blow-up.

Since $D_i \subset \{1,\dots,n\}$, we have $\sharp D_i \leq n$. Hence $\sharp(A_i \cup (B_i \cup \{j_i\})) \leq n$, so $\sharp A_i + \sharp B_i + 1 \leq n$. As the sequence is independent of v, this implies that $T \subset A_i$, and so $\sharp T \leq \sharp A_i$. Then $\sharp T + 1 + \sharp B_i \leq n$, so $t + 1 \leq n$, and so $r \geq 0$. By the minimality of the sequence, we know that if $i < l$, $w^{\delta} \nmid w^{\gamma}$ in R_i, and so $\sharp B_i \neq 0$, hence $r > 0$.

For every integers $i \in \{1,..., l\}$ and $j \in \{1,..., n\}$, we set $\beta_j^{(i)} = \nu\left(u_j^{(i)}\right)$. For each $i < l$, π_i is a blow-up along an ideal of the form $\left(u_{J_i}^{(i)}\right)$. Renumbering if necessary, we may assume that $1 \in J_i$ and that R_{i+1} is a localisation of $R_i\left[\dfrac{u_{J_i}^{(i)}}{u_1^{(i)}}\right]$ So we have $\beta_1^{(i)} = \min_{j \in J_i}\left\{\beta_j^{(i)}\right\}$.

Fact 3.4.5 Let $X = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ be a vector whose elements are relatively prime. Then there exists a matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ of determinant 1 such that X is the first line of A.

Proof. This proof is made by induction on n and using Bezout theorem.

Lemma 3.4.6 Let $i \in \{0, \ldots, l-1\}$. We assume that the sequence $\pi_0, \ldots, \pi_{i-1}$ of 3.4.1 is monomial.

We set $w^{\gamma} = \left(w^{(i)}\right)^{\gamma^{(i)}}$ and $w^{\delta} = \left(w^{(i)}\right)^{\delta^{(i)}}$. Then

(1)

$$\sum_{q \in E} \left(\gamma_q^{(i)} - \delta_q^{(i)}\right)\beta_q^{(i)} = 0, \tag{7}$$

(2) pgcd $\left(\gamma_1^{(i)} - \delta_1^{(i)}, \ldots, \gamma_r^{(i)} - \delta_r^{(i)}, \gamma_n^{(i)} - \delta_n^{(i)}\right) = 1$,

(3) Every $\mathbb{Z}$-linear dependence relation between $\beta_1^{(i)}, \ldots, \beta_r^{(i)}, \beta_n^{(i)}$ is an integer multiple of (7).

Proof.

(1) We have $\nu\left(w^{\gamma}\right) = \nu\left(w^{\delta}\right)$, hence $\nu\left(\left(w^{(i)}\right)^{\gamma^{(i)}}\right) = \nu\left(\left(w^{(i)}\right)^{\delta^{(i)}}\right)$. So, since $w^{(i)} = \left(w_1^{(i)}, \ldots, w_r^{(i)}, w_n^{(i)}\right)$:

$$\nu\left(\prod_{j=1}^{r}\left(w_j^{(i)}\right)^{\gamma_j^{(i)}} \times \left(w_n^{(i)}\right)^{\gamma_n^{(i)}}\right) = \nu\left(\prod_{j=1}^{r}\left(w_j^{(i)}\right)^{\delta_j^{(i)}} \times \left(w_n^{(i)}\right)^{\delta_n^{(i)}}\right)$$

in other words

$$\sum_{j=1}^{r} \gamma_j^{(i)} \nu\left(w_j^{(i)}\right) + \gamma_n^{(i)} \nu\left(w_n^{(i)}\right) = \sum_{j=1}^{r} \delta_j^{(i)} \nu\left(w_j^{(i)}\right) + \delta_n^{(i)} \nu\left(w_n^{(i)}\right).$$

By definition of $w^{(i)}$, for every integer $j \in \{1, \ldots, r, n\}$, we have $w_j^{(i)} = u_j^{(i)}$, so $\nu(w_j^{(i)}) = \beta_j^{(i)}$. Then:

$$\sum_{j=1}^{r} \gamma_j^{(i)} \beta_j^{(i)} + \gamma_n^{(i)} \beta_n^{(i)} = \sum_{j=1}^{r} \delta_j^{(i)} \beta_j^{(i)} + \delta_n^{(i)} \beta_n^{(i)}.$$

Then $\sum_{j \in \{1, \ldots, r, n\}} \left(\gamma_j^{(i)} - \delta_j^{(i)}\right)\beta_j^{(i)} = 0$.

(2) We do an induction. Case $i = 0$.

We have

$$\begin{aligned}
&\text{pgcd}\left(\gamma_1^{(i)} - \delta_1^{(i)}, \ldots, \gamma_r^{(i)} - \delta_r^{(i)}, \gamma_n^{(i)} - \delta_n^{(i)}\right) \\
&= \text{pgcd}\left(\gamma_1^{(0)} - \delta_1^{(0)}, \ldots, \gamma_r^{(0)} - \delta_r^{(0)}, \gamma_n^{(0)} - \delta_n^{(0)}\right) \\
&= \text{pgcd}\left(\alpha_1^{(0)}, \ldots, \alpha_s^{(0)}, \alpha_{s+1}^{(0)}, \ldots, \alpha_r^{(0)}, -\overline{\alpha^{(0)}}\right).
\end{aligned}$$

By definition

$$\alpha = \overline{\alpha^{(0)}} = \min_{h \in \mathbb{N}^*} \left\{h \text{ such that } h\beta_n \in \Delta\right\}$$

and

$$\alpha\beta_n = \sum_{j=1}^{r} \alpha_j^{(0)} \beta_j.$$

So pgcd $\left(\alpha_1^{(0)}, \ldots, \alpha_s^{(0)}, \alpha_{s+1}^{(0)}, \ldots, \alpha_r^{(0)}, -\alpha\right) = 1$.

Case $i > 0$. We assume the result shown at the previous rank. We have $\gamma^{(i)} = \gamma^{(i-1)}G^{(i)}$, $\delta^{(i)} = \delta^{(i-1)}G^{(i)}$ and $\beta^{(i)} = \beta^{(i-1)}F^{(i)}$ where $F^{(i)} = \left(G^{(i)}\right)^{-1}$ and $G^{(i)} \in \mathrm{SL}_{r+1}(\mathbb{Z})$ such that

$$G_{sq}^{(i)} = \begin{cases} 1 & \text{if } s = q \\ 1 & \text{if } q = j \text{ and } s \in J \\ 0 & \text{otherwise.} \end{cases}$$

So $(\gamma^{(i)} - \delta^{(i)}) = (\gamma^{(i-1)} - \delta^{(i-1)})G^{(i)} = (\gamma - \delta)G$ where G is a product of unimodular matrixes, and so G is unimodular.

By the case $i = 0$, $(\gamma - \delta)$ is a vector whose elements are relatively prime.

By (10) this vecteur can be complete as a base of $\mathbb{Z}^{r+1}$, which, by a unimodular matrix, stay a base of $\mathbb{Z}^{r+1}$. The vector $(\gamma^{(i)} - \delta^{(i)})$ is then a vector of this base, so its elements are relatively prime.

(3) Case $i = 0$ is the fact that $\beta_1, \ldots, \beta_r, \beta_n$ generate a vector space of dimension r.

Let

$$Z := \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{Z}^{r+1} \text{ such that } \sum_{j=1}^{r} x_j \beta_j + x_{r+1}\beta_n = 0 \right\}.$$

But $\alpha\beta_n = \sum_{j=1}^{r} \alpha_j^{(0)} \beta_j$, so:

$$Z = \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{Z}^{r+1} \text{ such that } \sum_{j=1}^{r} \left(\alpha x_j + x_{r+1}\alpha_j^{(0)}\right) \beta_j = 0 \right\}.$$

Since $\beta_1, \ldots, \beta_r$ are $\mathbb{Q}$-linearly independent elements, we have that Z is a free $\mathbb{Z}$-module of rank 1, so it is generated by a unique vector. By point (1), the vector $(\gamma - \delta)$ is in Z, and by point (2), it is composed of relatively prime elements. This vector generates the free $\mathbb{Z}$-module of rank 1.

Let $i > 0$. We already know that $\beta^{(i)} = \beta^{(i-1)}F^{(i)} = \beta F$ where F is a unimodular matrix, so an automorphism of $\mathbb{Z}^r$.

Let

$$Z^{(i)} := \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{Z}^{r+1} \text{ such that } \sum_{j=1}^{r} x_j \beta_j^{(i)} + x_{r+1}\beta_n^{(i)} = 0 \right\}.$$

So

$$Z^{(i)} = \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{Z}^{r+1} \text{ such that } \sum_{j=1}^{r} x_j \beta_j F + x_{r+1}\beta_n F = 0 \right\},$$

then

$$Z^{(i)} = \left\{ (x_1, \ldots, x_{r+1}) \in \mathbb{Z}^{r+1} \text{ such that } \sum_{j=1}^{r} x_j \beta_j + x_{r+1}\beta_n = 0 \right\}.$$

Then the set $Z^{(i)}$ is a free $\mathbb{Z}$-module of rank 1 by the case $i = 0$. And we know by (3) that the vector $(\gamma^{(i)} - \delta^{(i)})$ is a vector of $Z^{(i)}$ composed of relatively prime elements, so it generates $Z^{(i)}$. This completes the proof.

Lemma 3.4.7 The sequence (6) is not monomial.

Proof. Assume, aiming for contradiction, that it is. By induction on i, we have $r_i = r$ for every $i \in \{0, \ldots, l\}$. We know that $w^{(l)}$ is a regular system of parameters of R_l and that w^{δ} and w^{γ} divide each other in R_l.

We saw that

$$\begin{aligned} \gamma^{(l)} &= \gamma^{(l-1)} G^{(l)} \\ &= \gamma \prod_{j \in \{1, \ldots, l\}} G^{(j)} \end{aligned}$$

and

$$\begin{aligned} \delta^{(l)} &= \delta^{(l-1)} G^{(l)} \\ &= \delta \prod_{j \in \{1, \ldots, l\}} G^{(j)}. \end{aligned}$$

So $\delta^{(l)} = \gamma^{(l)}$.

But $(\gamma^{(l)} - \delta^{(l)}) = (\gamma - \delta)G$ where G is a unimodular matrix, hence $\gamma = \delta$, which is a contradiction.

Lemma 3.4.8 Let $i \in \{0, \ldots, l-1\}$ and assume $\pi_0, \ldots, \pi_{i-1}$ are all monomials. Then the following assertions are equivalent:

(1) The blow-up π_i is not monomial.

(2) There exists a unique index $q \in J_i \setminus \{1\}$ such that $\beta_q^{(i)} = \beta_1^{(i)}$.

(3) We have $i = l - 1$.

Proof. (3) $\Rightarrow$ (1) by Lemma 3.4.7.

(1) $\Rightarrow$ (2) First, we prove the existence. We have $\beta_1^{(i)} = \min_{j \in J_i} \{\beta_j^{(i)}\}$. So π_i monomial $\Leftrightarrow B_i = J_i \setminus \{1\} \Leftrightarrow \beta_q^{(i)} > \beta_1^{(i)}$ for every $q \in J_i \setminus \{1\}$.

Since the blow-up is not monomial by hypothesis, there exists $q \in J_i \setminus \{1\}$ such that $\beta_q^{(i)} = \beta_1^{(i)}$.

Now let us show the unicity. Assume, aiming for contradiction, that there exist two difierent indexes q and q' in $J_i \setminus \{1\}$ such that $\beta_q^{(i)} - \beta_1^{(i)} = 0$ and $\beta_{q'}^{(i)} - \beta_1^{(i)} = 0$.

Then we have two linear dependence relations between $\beta_1^{(i)}, \ldots, \beta_r^{(i)}$ and the element $\beta_n^{(i)}$, which are not linearly dependent. It is a contradiction by point (3.2) of Lemma 3.4.6.

(2) $\Rightarrow$ (3)

By Remark 3.2.6, we write $w_1^{(i)} = w^{\epsilon}$ and $w_q^{(i)} = w^{\mu}$ where ϵ and μ are two colons of an unimodular matrix. Then $\epsilon - \mu$ is unimodular, so its total pgcd is one.

So

$$\nu(w^{\mu}) = \sum_{s \in E} \mu_s \beta_s = \nu(w_q^{(i)}) = \beta_q^{(i)}$$

and

$$\nu(w^{\epsilon}) = \sum_{s \in E} \epsilon_s \beta_s = \nu(w_1^{(i)}) = \beta_1^{(i)}.$$

By hypothesis, $\beta_q^{(i)} = \beta_1^{(i)}$ Then $\sum_{s\in E}(\mu_s - \epsilon_s)\beta_s = 0$ and by points (3.1) and (3.2) of Lemma 3.4.6, and the fact that the total pgcd of $\mu - \epsilon$ is one, we have $\mu - \epsilon = \pm(\gamma - \delta)$.

So $\frac{w_q^{(i)}}{w_1^{(i)}} = w^{\epsilon-\mu} = w^{\pm(\gamma-\delta)} = \overline{z}^{\pm 1}$, then either $\overline{z} \in R_{i+1}$ or $\overline{z}^{-1} \in R_{i+1}$.

To show that $i = l - 1$, we are going to show that $i + 1 = l$. And to do this, we are going to use the fact that l has been chosen minimal such that $\overline{z} \in R_l^{\times}$. So let us show that $\overline{z} \in R_{i+1}^{\times}$.

Since $\overline{z} \in R_{i+1}$ or $\overline{z}^{-1} \in R_{i+1}$, we know that $w^{\delta} \mid w^{\gamma}$ in R_{i+1} or the converse. By Proposition 3.2.7 and the fact that w^{δ} and w^{γ} have same value, we have $w^{\delta} \mid w^{\gamma}$ in R_{i+1} if and only if the converse is true. So $\overline{z} \in R_{i+1}^{\times}$, and the proof is complete.

Doing an induction on i and using Lemma 3.4.8, we conclude that $\pi_0,..., \pi_{l-2}$ are monomials. So we have the first point of Theorem 3.4.4.

It remains to show the points (3.1) and (3.2).

By Lemma 3.4.8 there exists a unique element $q \in J_{l-1} \setminus \{j_{l-1}\}$ such that $\beta_q^{(l-1)} = \beta_1^{(l-1)}$, so we are in the case $\sharp B_{l-1} + 1 = \sharp J_{l-1} - 1$. Now we have to see if we are in the case $t_{k_{l-1}} = 0$ or in the case $t_{k_{l-1}} = 1$.

We recall that $w_1^{(l-1)} = w^{\epsilon}$ and $w_q^{(l-1)} = w^{\mu}$ where ϵ and μ are two colons of a unimodular matrix such that $\mu - \epsilon = \pm(\gamma - \delta)$. So we have $x_1^{(l-1)} = x^{\epsilon}$ and $x_q^{(l-1)} = x^{\mu}$, then

$$\frac{x_q^{(l-1)}}{x_1^{(l-1)}} = x^{\mu-\epsilon} = x^{\pm(\gamma-\delta)} = x^{\pm\left(\alpha_1^{(0)},\ldots,\alpha_r^{(0)},-\alpha\right)}.$$

In other words

$$\frac{x_q^{(l-1)}}{x_1^{(l-1)}} = \left(\frac{\prod_{j=1}^{r} x_j^{\alpha_j^{(0)}}}{x_n^{\alpha}}\right)^{\pm 1} = \left(z^{-1}\right)^{\pm 1} = z^{\pm 1}.$$

Replacing $x_1^{(l-1)}$ and $x_q^{(l-1)}$ if necessary, we may assume $\frac{x_q^{(l-1)}}{x_1^{(l-1)}} = z$.

Since $\beta_1^{(l-1)},\ldots,\beta_r^{(l-1)}$ are linearly independent, we have $q = n$.

We recall that $\lambda_0 = X^{\alpha} + c_0 y$ where $c_0 \in k$, and $Z + c_0$ is the minimal polynomial λ_z of z on $\operatorname{gr}_v k\left(x_1,\ldots,x_r\right)$. By 3.1.9, we have

$$w_n^{(l)} = u_n^{(l)} = \overline{\lambda_0}(u_n') = \overline{\lambda_0}\left(\frac{u_n^{(l-1)}}{u_1^{(l-1)}}\right) = \overline{\lambda_0}\left(\frac{w_n^{(l-1)}}{w_1^{(l-1)}}\right) = \overline{\lambda_0}\left(\overline{z}\right) = \overline{z} + a_0 b_0.$$

Remark 3.4.9 We know that $\overline{\lambda_0}\left(\overline{z}\right) = \overline{z} + b_0 g_0$ where g_0 is a unit and $b_0 \in R$ such that $b_0 \equiv c_0$ modulo $\mathfrak{m}$. Then we choose $g_0 = a_0$.

But $\overline{z} = \frac{w_n^{\alpha}}{\overline{y}}$, so

$$w_n^{(l)} = \frac{w_n^{\alpha}}{\overline{y}} + a_0 b_0 = \frac{w_n^{\alpha} + a_0 b_0 \overline{y}}{\overline{y}} = \frac{Q}{\overline{y}}$$

as desired in point (3.2).

Let us show the point (3.1). We apply Proposition 3.2.5 at $i = 0$ and $i' = 1$. By the monomiality of $\pi_0,..., \pi_{l-2}$, we know that $D_i = \{1,..., n\}$ for each $i \in \{1,..., l-1\}$, and we know that $D_l = \{1,..., n\}$. We set $u_T = v$.

For every $j \in \{1,\ldots, r, n\}$, the fact that $w_j = u_j$ is a monomial in $w_1^{(l)},\ldots,w_r^{(l)}$, in other words in $u_1^{(l)},\ldots,u_r^{(l)}$ multiplied by an element of $R_l^{\times}$ is a consequence of Proposition 3.2.5.

The fact that for every integer $j \in \{1,\ldots, r\}$, we have $w_j^{(l)} = w^{\eta}$ is a consequence of the same Proposition. This completes the proof.

Remark 3.4.10 In the case $Q_2 = Q$, we monomialized Q_2 as desired.

Definition 3.4.11 [24] A local framed sequence that satisfies Theorem 3.4.4 is called a n-Puiseux package.

Let $j \in \{r+1,\ldots, n\}$. A j-Puiseux package is a n-Puiseux package replacing n by j in Theorem 3.4.4.

Lemma 3.4.12 Let $P = u_n^{\alpha} + c_0$ be the u_n-expansion of an immediate successor key element of u_n.

There exists a local framed sequence $(R, u) \to (R_l, u^{(l)})$, independant of u_n, that transforms c_0 in a monomial in $\left(u_1^{(l)},\ldots,u_r^{(l)}\right)$, multiplied by a unit of R_l.

In particular, after this local framed sequence, the element P is of the form $w_n^{\alpha} + a_0 b_0 \overline{y}$.

Proof. We will prove this Lemma in a more general version in Lemma 3.4.16.

Corollary 3.4.13 Let P be an immediate successor key element of u_n. Then P is monomializable.

Proof. If $u_n \ll P$, we use Lemma 3.4.12 to reduce to the case $P = w_n^{\alpha} + a_0 b_0 \overline{y}$. By Theorem 3.4.4, we can monomialize P.

Let G be a local ring essentially of finite type over k of dimension strictly less than n that is equipped with a valuation centered on G.

Theorem 3.4.14 Assume that for every ring G as above, every element of G is monomializable.

We recall that $\operatorname{car}(k_{\nu}) = 0$. If $u_n \ll_{\lim} P$, then P is monomializable.

Proof. We write $P = \sum_{j=0}^{N} b_j a_j u_n^j$ the u_n-expansion of P, with $a_j \in R^{\times}$ and $Q = \sum_{j=0}^{N} b_j u_n^j$ a limite immediate successor of u_n.

By Theorem 2.17, we have $\delta_{u_n}(Q) = 1$. Then:

$$\nu(b_0) = \nu(b_1 u_n) < \nu\left(b_j u_n^j\right),$$

for every $j > 1$.

The elements a_i are units of R, so for every $j > 1$ we have:

$$\nu(a_0 b_0) = \nu(a_1 b_1 u_n) < \nu\left(a_j b_j u_n^j\right).$$

In fact, $\nu(a_1 b_1) < \nu(a_0 b_0)$ and by hypothesis, after a sequence of blow-ups independent of u_n, we can monomialize $a_j b_j$ for every index j, and assume that $a_1 b_1 \mid a_0 b_0$ by Proposition 3.2.7.

Then

$$\nu(b_0) = \nu(b_1 u_n) < \nu(b_j) + j\nu(u_n) = \nu(b_j) + j\left(\nu(b_0) - \nu(b_1)\right).$$

So $\nu(b_0) < (b_j) + j\left(\nu(b_0) - \nu(b_1)\right)$.

In fact, $\nu\left(b_1^j\right) < \nu\left(b_j b_0^{j-1}\right)$. So after a sequence of blow-ups independent of u_n, we have $b_1^j \mid b_j b_0^{j-1}$. After a n-Puiseux package $(*)$ $(R, u) \to \cdots \to (R', u')$ in the special case $\alpha = 1$, we obtain $P = \sum_{j=0}^{N} b_j' \left(u_n'\right)^j$ with $b_1' \mid b_j'$ for every index j with $u_n' = \frac{b_1 u_n}{b_0} + 1$.

In fact, $\frac{P}{b_1'} = u_n' + \varphi$ with $\varphi \in \left(u_1',\ldots,u_{n-1}'\right)$. So $u'' := \left(u_1',\ldots,u_{n-1}', \frac{P}{b_1'}\right)$ is a regular system of parameters of R'. Then, the sequence $(R, u) \to \cdots \to (R', u'')$ given by $(*)$ changing uniquely the last parameter u_n' after the last blow-up is still a local framed sequence. So P is monomializable.

Remark 3.4.15 Since Q_2 is an immediate successor (possibly limit) of u_n, this is in particular an immediate successor (possibly limit) key element of u_n. By Corollary 3.4.13, or Theorem 3.4.14, it is monomializable modulo Lemma 3.4.12.

3.4.3 Generalization

Now we monomialized Q_2, but we want to monomialize every key polynomial of the sequence $\mathcal{Q}$. Here the key elements will be useful. Indeed, modified by the blow-ups which monomialized Q_2, we cannot know if Q_3 is still a key polynomial.

To be more general, we will show that if $Q_i \in \mathcal{Q}$ is monomializable, then Q_{i+1} is monomializable.

Assume that the polynomial Q_i is monomializable after a sequence of blow-ups $(R, u) \to (R_l, u^{(l)})$.

Let Δ_l be the group $\nu\left(k\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)\setminus\{0\}\right)$. We set

$$\alpha_l := \min\left\{h \text{ such that } h\beta_n^{(l)} \in \Delta_l\right\}.$$

We set $X_j = \mathrm{in}_\nu\left(u_j^{(l)}\right)$, $W_j = w_j^{(l)}$ and λ_l the minimal polynomial of X_n over $\mathrm{gr}_\nu k\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)$ of degree α_l.

Since $k = k_\nu$ there exists $c_0 \in \mathrm{gr}_\nu k\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)$ such that

$$\lambda_l(X) = X^{\alpha_l} + c_0.$$

Furthermore, we have $Q_i = \bar{\omega} w_n^{(l)}$ with $\bar{\omega}$ a monomial in $W_1, \ldots, W_{r_l}$ multiplied by a unit. We set $\omega := \mathrm{in}_\nu(\bar{\omega})$.

We know that Q_{i+1} is an optimal immediate successor of Q_i so we denote by

$$Q_{i+1} = Q_i^{\alpha_l} + b_0$$

the Q_i-expansion of Q_{i+1} in $k(u_1, \ldots, u_{n-1})[u_n]$ by Proposition 5.6 with $c_0 = \mathrm{in}_\nu(b_0)$.

Since $Q_i = \bar{\omega} W_n$ and $Q_{i+1} = Q_i^{\alpha_l} + b_0$, we have

$$\frac{Q_{i+1}}{\bar{\omega}^{\alpha_l}} = \left(u_n^{(l)}\right)^{\alpha_l} + \frac{b_0}{\bar{\omega}^{\alpha_l}}.$$

We know that both terms of the Q_i-expansion of Q_{i+1} have same value. So these two terms are divisible by the same power of $\bar{\omega}$ after a suitable sequence of blow-ups $(*_i)$ independent of $u_n^{(l)}$.

We denote by $\widetilde{Q}_{i+1}$ the strict transform of Q_{i+1} by the composition of $(*_i)$ with the sequence of blow-ups $(*'_i)$ that monomialize Q_i. We denote this composition by (c_i). We write $(R,u) \xrightarrow{(c_i)} \left(R_l, u^{(l)}\right)$.

We know that $\widetilde{Q}_i$, the strict transform of Q_i by (c_i), is a regular parameter of R_l. Indeed, by Proposition 3.2.5, we know that every u_j of R can be written as a monomial in $w_1^{(l)}, \ldots, w_{r_l}^{(l)}$. In fact, the reduced exceptional divisor of this sequence of blow-ups is exactly $V(\bar{\omega})_{\mathrm{red}}$. Then, since $Q_i = W_n \bar{\omega}$, we have that the strict transform of Q_i is $\widetilde{Q}_i = W_n = w_n^{(l)} = u_n^{(l)}$. So it is a key polynomial in the extension $k\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)\left(u_n^{(l)}\right)$.

Let us show that $\widetilde{Q}_{i+1} = \dfrac{Q_{i+1}}{\bar{\omega}^{\alpha_l}}$.

We have

$$Q_i^{\alpha_l} = \bar{\omega}^{\alpha_l}\left(u_n^{(l)}\right)^{\alpha_l}$$

and also $u_n^{(l)} \nmid \bar{\omega}$. Thus $\bar{\omega}^{\alpha_l}$ divides $Q_i^{\alpha_l}$ and all the non-zero terms of the Q_i-expansion of Q_{i+1}. Furthermore, it is the greatest power of $\bar{\omega}$ that divides all the terms, so $\dfrac{Q_{i+1}}{\bar{\omega}^{\alpha_l}}$ is $\widetilde{Q}_{i+1}$, the strict transform of Q_{i+1} by the sequence of blow-ups.

Let G be a local ring essentially of finite type over k of dimension strictly less than n equipped with a valuation centered in G whose residue field is k.

Lemma 3.4.16 Assume that for every ring G as above, every element of G is monomializable.

Assume that $Q_i < Q_{i+1}$ in $\mathcal{Q}$.

There exists a local framed sequence $(R_l, u^{(l)}) \to (R_e, u^{(e)})$ such that in R_e, the strict transform of Q_{i+1} is of the form $\left(u_n^{(e)}\right)^{\alpha_l} + \tau_0\eta$, where $\tau_0 \in R_e^{\times}$ and η is a monomial in $u_1^{(e)}, \ldots, u_{r_e}^{(e)}$.

Proof. By hypothesis, after a sequence of blow-ups independent of $u_n^{(l)}$, we can monomialize b_0 and assume that it is a monomial in $\left(u_1^{(l)}, \ldots, u_{n-1}^{(l)}\right)$ multiplied by a unit of R_l.

For every $g \in \{r_l + 1, \ldots, n-1\}$ we do a g-Puiseux package, and then we have a sequence

$$\left(R_l, u^{(l)}\right) \to \left(R_t, u^{(t)}\right)$$

such that every $u_g^{(l)}$ is a monomial in $\left(u_1^{(t)}, \ldots, u_{r_t}^{(t)}\right)$.

In fact, we can assume that b_0 is a monomial in $\left(u_1^{(l)}, \ldots, u_{r_l}^{(l)}\right)$ multiplied by a unit of R_l.

Since the strict transform $\widetilde{Q}_{i+1} = \left(u_n^{(l)}\right)^{\alpha_l} + \frac{b_0}{\varpi^{\alpha_l}}$ is an immediate successor key element of $\widetilde{Q}_i$. This completes the proof.

Remark 3.4.17 Lemma 3.4.12 is a special case of Lemma 3.4.16.

Let G be a local ring essentially of finite type over k of dimension strictly less than n equipped with a valuation centered in G whose residue field is k.

Theorem 3.4.18 Assume that for every ring G as above, every element of G is monomializable.

We recall that car $(k_\nu) = 0$. If Q_i is monomializable, there exists a local framed sequence

$$\left(R, u\right) \xrightarrow{\pi_0} \left(R_1, u^{(1)}\right) \xrightarrow{\pi_1} \cdots \xrightarrow{\pi_{l-1}} \left(R_l, u^{(l)}\right) \xrightarrow{\pi_l} \cdots \xrightarrow{\pi_{m-1}} \left(R_m, u^{(m)}\right) \quad (8)$$

that monomializes Q_{i+1}.

Proof. There are two cases.

First: $Q_i < Q_{i+1}$. Then we just saw that the strict transform $\widetilde{Q}_{i+1}$ of Q_{i+1} by the sequence $(R, u) \to (R_l, u^{(l)})$ that monomializes Q_i is an immediate successor key element of $\widetilde{Q}_i = u_n^{(l)}$, and that we can reduce the problem to the hypotheses of Theorem 3.4.4 by Lemma 3.4.16. So we use Theorem 3.4.4 replacing Q_1 by $\widetilde{Q}_i$ and Q_2 by $\widetilde{Q}_{i+1}$.

Then we have constructed a local framed sequence (8) that monomializes $\widetilde{Q}_{i+1}$.

Second case: $Q_i <_{\lim} Q_{i+1}$.

Then we saw that the strict transform $\widetilde{Q}_{i+1}$ of Q_{i+1} by the sequence $(R, u) \to (R_l, u^{(l)})$ that monomialize $\widetilde{Q}_i = u_n^{(l)}$. Then we apply Theorem 3.4.14 replacing Q_1 by $\widetilde{Q}_i$ and Q_2 by $\widetilde{Q}_{i+1}$.

We have constructed a local framed sequence (8) that monomializes $\widetilde{Q}_{i+1}$.

Theorem 3.4.19 There exists a local sequence

$$\left(R, u\right) \xrightarrow{\pi_0} \cdots \xrightarrow{\pi_{s-1}} \left(R_s, u^{(s)}\right) \xrightarrow{\pi_s} \cdots \quad (9)$$

that monomializes all the key polynomials of $\mathcal{Q}$.

More precisely, for every index i, there exists an index s_i such that in R_{s_i}, Q_i is a monomial in $u^{(s_i)}$ multiplied by a unit of R_{s_i}.

Proof. Induction on the dimension n and on the index i and we iterate the previous process.

3.4.4 Divisibility

We consider, for every integer j, the countable sets

$$\mathscr{S}_j := \left\{ \prod_{i=1}^{n} \left(u_i^{(j)}\right)^{\alpha_i^{(j)}}, \text{ with } \alpha_i^{(j)} \in \mathbb{Z} \right\}$$

and

$$\widetilde{\mathscr{T}_j} := \left\{ \left(s_1, s_2 \right) \in \mathscr{S}_j \times \mathscr{S}_j, \text{ with } \nu\left(s_1\right) \leq \nu\left(s_2\right) \right\}$$

with the convention that for every $i \in \{1, \ldots, n\}$, $u_i^{(0)} = u_i$.

The set $\widetilde{\mathscr{T}_j}$ being countable for every integer j, we can number its elements, and then we write $\widetilde{\mathscr{T}_j} := \left\{ s_m^{(j)} \right\}_{m \in \mathbb{N}}$. We consider now the finite set

$$\mathscr{S}_j' := \left\{ s_m^{(j)},\ m \leq j \right\} \cup \left\{ s_j^{(m)},\ m \leq j \right\}.$$

Then $\bigcup_{j \in \mathbb{N}} \left(\mathscr{S}_j \times \mathscr{S}_j \right) = \bigcup_{j \in \mathbb{N}} \widetilde{\mathscr{T}_j} = \bigcup_{j \in \mathbb{N}} \mathscr{S}_j'$ is a countable union of finite sets.

Now we fix a local framed sequence

$$\left(R, u\right) \to \cdots \to \left(R_i, u^{(i)}\right).$$

Theorem 3.4.20 There exists a finite local framed sequence

$$p_i : \left(R_i, u^{(i)}\right) \to \cdots \to \left(R_{i+q_i}, u^{(i+q_i)}\right)$$

such that for every integer $j \leq i$ and for every element s of $\mathscr{S}_j'$, the first coordinate of s divides its second coordinate in R_{i+q_i}.

Proof. Consider an integer $j \leq i$ and an element $s = \left(s_1, s_2\right) \in \mathscr{S}_j'$. We want to construct a sequence of blow-ups such that at the end we have $s_1 \mid s_2$.

We know that $s \in \widetilde{\mathscr{T}_m}$ with $m \leq j$. All cases being similar, we may assume $s \in \widetilde{\mathscr{T}_j}$ and then we have

$$s_1 = \prod_{i=1}^{n} \left(u_i^{(j)}\right)^{\alpha_{i,1}^{(j)}}$$

and

$$s_2 = \prod_{i=1}^{n} \left(u_i^{(j)}\right)^{\alpha_{i,2}^{(j)}}.$$

By Proposition 3.2.4 applied to R_i instead of R, there exists a sequence $(R_i, u^{(i)}) \to \cdots \to (R_{i+l}, u^{(i+l)})$ such that in R_{i+l}, $s_1 \mid s_2$ or $s_2 \mid s_1$. By definition $\nu(s_1) \leq \nu(s_2)$, so we have $s_1 \mid s_2$ by Proposition 3.2.7.

By point 4 of Theorem 3.4.4, we know that $\mathscr{S}_j \subseteq R_{i+l}^{\times} \mathscr{S}_{i+l}$. In other words every element of $\mathscr{S}_j$ can be written $z_{i+l}s_{i+l}$ with $z_{i+l} \in R_{i+l}^{\times}$ and $s_{i+l} \in \mathscr{S}_{i+l}$.

Let $\left(s_3, s_4\right) \in \mathscr{S}_j'$, be another pair of $\mathscr{S}_j'$, let us say that it is still in $\widetilde{\mathscr{T}_j}$. We just saw that $s_3, s_4 \in R_{i+l}^{\times} \mathscr{S}_{i+l}$. Units don't have an effect on divisibility, so we can only consider the part of s_3 and s_4 which is in $\mathscr{S}_{i+l}$. Hence we can iterate the Proposition 3.2.4 applying it to $(R_{i+l}, u^{(i+l)})$. So we constructed an other sequence of blow-ups

$$\left(R_{i+l}, u^{(i+l)}\right) \to \cdots \to \left(R_{i+h}, u^{(i+h)}\right)$$

such that R_{i+h} we have $s_3 \mid s_4$ or $s_4 \mid s_3$. Since $\nu(s_3) \leq \nu(s_4)$, we know that s_3 divides s_4.

We iterate the process for all the pairs of $\mathscr{S}_j'$, and for every $j \leq i$. This is a finite number of times since $\mathscr{S}_j'$ has a finite number of elements for every j and since we consider a finite number of such sets. Then we obtain a finite sequence of blow-ups

$$\left(R_i, u^{(i)}\right) \to \cdots \to \left(R_{i+q_i}, u^{(i+q_i)}\right)$$

such that for every integer $j \leq i$ and every s in $\mathscr{S}_j'$, the first coordinate of s divides the second coordinate in R_{i+q_i}.

The goal of the next theorem is to construct an infinite local framed sequence

$$(R, u) \to \ldots \to \left(R_i, u^{(i)}\right) \ldots \tag{10}$$

that monomializes all the key elements, as well as other elements specified below, and to ensure countably many divisibility conditions, also specified below. We will use the notation

$$B_i := k\left[u_1^{(i)}, \ldots, u_{n-1}^{(i)}\right].$$

Theorem 3.4.21 We recall that $\operatorname{car}(k_\nu) = 0$. There exists an infinite sequence of blow-ups

$$\left(R, u\right) \to \cdots \to \left(R_m, u^{(m)}\right) \to \cdots \tag{11}$$

that monomializes all the key polynomials, all the elements of B_i for every index i and that has the following property:

$$\forall j \in \mathbb{N}\ \forall s = \left(s_1, s_2\right) \in \mathscr{S}_j'\ \exists i \in \mathbb{N}_{\geq j} \text{ such that in } R_i \text{ we have } s_1 \mid s_2.$$

Proof. The first key polynomial is a monomial, so for it we do not need to do anything. For $j = 0$, the elements of $\mathscr{S}_j' = \mathscr{S}_0'$ are just pairs of monomials in u. Let us consider $s = (s_1, s_2) \in \mathscr{S}_0'$ and apply Proposition 3.2.4. We construct a sequence $p_0 : R \to R_{q_0}$ such that in R_{q_0}, we have $s_1 \mid s_2$ or $s_2 \mid s_1$. Since $\nu(s_1) \leq \nu(s_2)$, we have $s_1 \mid s_2$. We do the same for all the elements of $\mathscr{S}_0'$ (recall that the set $\mathscr{S}_0'$ is finite), and by abuse of notation we still denote by $p_0 : R \to R_{q_0}$ the sequence obtained at the end. Now we have a sequence of blow-ups $p_0 : R \to R_{q_0}$ such that the first key polynomial is a monomial and such that for every $s = (s_1, s_2) \in \mathscr{S}_0'$, we have $s_1 \mid s_2$ in R_{q_0}.

We denote by $\left(P_j^{(i)}\right)_{j \in \mathbb{N}}$ the sequence of the generators of the ν-ideals of the B_i. For the moment we only monomialize $P_0^{(0)}$ and still denote by $p_0 : R \to R_{q_0}$ the sequence of blow-ups that monomializes the first key polynomial $P_0^{(0)}$ and such that for every $s = (s_1, s_2) \in \mathscr{S}_0'$, we have $s_1 \mid s_2$ in R_{q_0}.

Arguing exactly as in the proof of Theorem 3.4.19, we show that there exists a sequence $\pi^{(2)} : R_{q_0} \to \ldots \to R_1$ that monomializes the second key polynomial.

We have a sequence $\pi^{(2)} \circ p_0 : R \to R_{q_0} \to R_1$ that monomializes the first two key polynomials, the element $P_0^{(0)}$, and such that for every $s = (s_1, s_2) \in \mathscr{S}_0'$, we have $s_1 \mid s_2$ in R_{q_0}. Now, again by Proposition 3.2.4, we construct a sequence $p_1 : R_1 \to R_{q_1}$ such that for every $s = (s_1, s_2) \in \mathscr{S}_1'$, we have $s_1 \mid s_2$ in R_{q_1}.

Now we monomialize all the $P_j^{(i)}$ for $i, j \leq 1$ and still denote, by abuse of notation, by $p_1 : R_1 \to R_{q_1}$ the sequence of blow-ups that monomializes these $P_j^{(i)}$ and such that for every $s = (s_1, s_2) \in \mathscr{S}_1'$, we have $s_1 \mid s_2$ in R_{q_1}.

Arguing exactly as in the proof of Theorem 3.4.19, we show that there exists a sequence of blow-ups $\pi^{(3)} : R_{q_1} \to \ldots \to R_2$ that monomializes the third key polynomial.

So we have a sequence $\pi^{(3)} \circ p_1 \circ \pi^{(2)} \circ p_0 : R \to R_{q_0} \to R_{q_1} \to R_2$ that monomializes the first three key polynomials, the elements $P_j^{(i)}$ for $i, j \leq 1$, and such that for every $s = (s_1, s_2) \in \mathscr{S}_0'$ or $\mathscr{S}_1'$, we have $s_1 \mid s_2$ in R_{q_0} or in R_{q_1}. Now, again by Proposition 3.2.4, we construct a sequence $p_2 : R_2 \to R_{q_2}$ such that for every $s = (s_1, s_2) \in \mathscr{S}_2'$, we have $s_1 \mid s_2$ in R_{q_2}.

Now we monomialize all the $P_j^{(i)}$ for $i, j \leq 2$ and still denote, by abuse of notation, by $p_2 : R_2 \to R_{q_2}$ the sequence of blow-ups that monomializes these $P_j^{(i)}$ and such that for every $s = (s_1, s_2) \in \mathscr{S}_2'$, we have $s_1 \mid s_2$ in R_{q_2}.

Then we have a sequence $p_2 \circ \pi^{(3)} \circ p_1 \circ \pi^{(2)} \circ p_0$ that monomializes the first three key polynomials, the elements $P_j^{(i)}$ for $i, j \leq 2$, and such that for every $s = (s_1, s_2) \in \mathscr{S}_i'$ for $i \in \{0, 1, 2\}$ we have $s_1 \mid s_2$ in R_{q_i}. We iterate this process an infinite number of times. Hence we construct a sequence of blow-ups $(R, u) \to \cdots \to (R_m, u^{(m)}) \to \cdots$ that monomializes all the key polynomials, all the generators $P_j^{(i)}$ (and so all the elements of the B_i) and that has the last property of the statement of the Theorem.

3.5 Conclusion

Now we can prove the main result of this chapter, namely, simultaneaous embedded local uniformization for the local rings essentially of finite type over a field of characteristic zero.

A local algebra K essentially of field type over a field k that has k as residue field is an étale extension of

$$K' = k\left[u_1, \ldots, u_n\right]_{(u_1, \ldots, u_n)}.$$

Let $f \in K$ be an irreducible element over k and

$$I := (f) \bigcap k\left[u_1, \ldots, u_n\right].$$

The ideal I is a prime ideal of height 1, so I principal. We consider a generator $\tilde{f}$ of I. Then $\frac{K'}{(\tilde{f})} \hookrightarrow \frac{K}{(f)}$ and each local sequence in $\frac{K'}{(\tilde{f})}$ induced a local sequence in $\frac{K}{(f)}$.

So it is enough to prove local uniformization in the case of the rings $k[u_1,..., u_n]_{(u_1,..., u_n)}$ to prove it in the general case of algebras essentially of finite type over a field k.

Theorem 3.5.1 Let us consider the sequence

$$(R, u) \to \cdots \to \left(R_m, u^{(m)}\right) \to \cdots$$

of Theorem 3.4.21.

Then for every element f of R, there exists i such that in R_i, f is a monomial multiplied by a unit.

Proof. Let $f \in R$. By Theorem 3.3.5, there exists a finite or infinite sequence $(Q_i)_i$ of key polynomials of the extension $K(u_n)$, optimal (possibly limit) immediate successors, such that $(\epsilon(Q_i))_i$ is cofinal in $\epsilon(\Lambda)$ where Λ is the set of key polynomials.

Then by Remark 3.3.9, f is non-degenerate with respect to one of these polynomials Q_i. But we saw in Theorem 3.4.21 that there exists an index l such that in R_l, all the Q_j with $j \leq i$ are monomials, hence f is non-degenerate with respect to a regular system of parameters of R_l.

Let $N = (w_1,..., w_s)$ be a monomial ideal in $u^{(l)}$ such that $\nu(N) = \nu(f)$ with w j monomials in $u^{(l)}$ such that $\nu(w_1) = \min\{\nu(w_j)\}$. By construction of the local framed sequence, there exists $l' \geq l$ such that in $R_{l'}$, $w_1 \mid w_j$ for all j. So in $R_{l'}$, f is equal to w_1 multiplied by a unit of $R_{l'}$.

Theorem 3.5.2 (Embedded local uniformization). Let k be a zero characteristic field and $f = (f_1,..., f_l) \in k[u_1,..., u_n]^l$ be a set of l polynomials in n variables, that are irreducible over k. We set $R := k[u_1,..., u_n]_{(u_1,..., u_n)}$ and ν a valuation centered in R such that $k = k_\nu$.

We consider the sequence $(R, u) \to \cdots \to (R_m, u^{(m)}) \to \cdots$ of Theorem 3.4.21.

Then there exists an index j such that the subscheme of Spec(R_j) defined by the ideal $(f_1,..., f_l)$ is a normal crossing divisor.

Proof. Renumbering, if necessary, we may assume

$$\nu\left(f_1\right) = \min\left\{\nu\left(f_j\right)\right\}.$$

By Theorem 3.4.21 there exists an index j_1 such that in R_{j_1}, the total transform of f_1 is a monomial in $u^{(j_1)}$, and so defines a normal crossing divisor.

Now we look at the equation f_2 in R_{j_1}. By Theorem 3.4.21, there exists an index j_2 such that in R_{j_2}, the total transform of f_2 defines a normal crossing divisor.

In R_2, the total transforms of f_1 and f_2 define normal crossing divisors.

We iterate the process until the total transforms of $f_1, ..., f_l$ define normal crossing divisors in R_{j_l}.

By construction of the local framed sequence $(R, u) \to \cdots \to (R_m, u^{(m)}) \to \cdots$, there exists $j \geq j_l$ such that in R_j, we have $f_1 \mid f_i$ for every index i.

Corollary 3.5.3 We keep the same notation and hypotheses as in the previous Theorem.

Then $R_\nu = \lim\limits_{\rightarrow} R_i$.

4. Simultaneous local uniformization in the case of quasi-excellent rings for valuations of rank less than or equal to 2

4.1 Preliminaries

Let R be a local noetherian domain of equicharacteristic zero and ν a valuation of Frac(R) of rank 1, centered in R and of value group Γ_1. We are going to define the implicit prime ideal H of R for the valuation ν, which is a key object in local uniformization. Indeed, this ideal will be the ideal we have to desingularize. We are going to prove in this part that to regularize R, hence to construct a local uniformization, we only have to regularize $\widehat{R}_H$ and $\frac{\widehat{R}}{H}$. At this point, the hypothesis of quasi excellence is very important: if R is quasi excellent, the ring $\widehat{R}_H$ is regular. So we will only have to monomialize the elements of $\frac{\widehat{R}}{H}$.

4.1.1 Quasi-excellent rings and the implicit prime ideal

Definition 4.1.1 Let R be a domain. We say that R is a G-ring if for every prime ideal $\mathfrak{p}$ of R, the completion morphism $R_\mathfrak{p} \to \widehat{R}_\mathfrak{p}$ is a regular homomorphism.

Definition 4.1.2 Let R be a local ring. Then R is quasi-excellent if R is a G-ring. More generally, if A is a ring, then A is quasi-excellent if A is a local G-ring whose regular locus is open for all A-algebra of finite type.

Proposition 4.1.3 [38] A local noetherian ring R is quasi-excellent if the completion morphism $R \to \widehat{R}$ is regular.

Remark 4.1.4 Let R be a local ring. If R is a G-ring, then its regular locus is open. Since the class of G-rings is stable under passing to algebras of finite type, for every R-algebra A of finite type, the set Reg(A) is open.

Definition 4.1.5 We call the implicit prime ideal H of R the ideal $H = \bigcap\limits_{\beta \in \nu(R \setminus \{0\})} P_\beta \widehat{R}$. The ideal H is composed of the elements of $\widehat{R}$ whose value is greater than every element of Γ_1.

Furthermore, the valuation ν extends uniquely to a valuation $\tilde{\nu}$ centered in $\frac{\widehat{R}}{H}$ [47].

Proposition 4.1.6 Let R be a quasi-excellent local ring. Then $\widehat{R}_H$ is regular.

Proof. The ring R is a G-ring. Then for every prime ideal $\mathfrak{p}$ of R, we have the injective map $\kappa(\mathfrak{p}) \hookrightarrow \kappa(\mathfrak{p}) \otimes_R \widehat{R}$ such that the fiber $\kappa(\mathfrak{p}) \otimes_R \widehat{R}$ is geometrically regular over $\kappa(\mathfrak{p})$, where $\kappa(\mathfrak{p}) := \frac{R_\mathfrak{p}}{\mathfrak{p} R_\mathfrak{p}}$. Since R is a domain, (0) is a prime ideal of R.

We write $K :=$ Frac(R), then we have the injective map $K \hookrightarrow K \otimes_R \widehat{R}$ such that the fiber $K \otimes_R \widehat{R}$ is geometrically regular over K. In other words the morphism $K \hookrightarrow K \otimes_R \widehat{R}$ is regular.

But $R \setminus \{0\}$ and $\widehat{R} \setminus H$ are two multiplicative subsets of $\widehat{R}$ such that $R \setminus \{0\} \subseteq \widehat{R} \setminus H$, since $R \cap H = \{0\}$. Then, $\widehat{R}_H$ is a localisation of $\widehat{R}_{R \setminus \{0\}}$. If we show that $\widehat{R}_{R \setminus \{0\}}$ is regular, then $\widehat{R}_H$ will be also regular as a localization of a regular ring. By the universal property of tensor product, the ring $\widehat{R}_{R \setminus \{0\}}$ is isomorphic to $K \otimes_R \widehat{R}$, which is regular by hypothesis. This completes the proof.

4.1.2 Numerical characters associated to a singular local noetherian ring

Let $(S, \mathfrak{q}, L)$ be a local noetherian ring and μ a valuation centered in S. We write $\mu = \mu_2 \circ \mu_1$ with μ_1 of rank 1. The valuation μ_2 is trivial if and only if μ is also of rank 1. We denote by G the value group of μ and by G_1 the value group of μ_1. In fact G_1 is the smallest isolated subgroup non-trivial of G. We set $I := \{x \in S \text{ such that } \mu(x) \notin G_1\}$, and then μ_1 induces a valuation of rank 1 over $\frac{S}{I}$. Let $\overline{J}$ be the implicit prime ideal of $\frac{\hat{S}}{I\hat{S}}$ for the valuation μ_1 and J its preimage in $\hat{S}$.

Definition 4.1.7 We set

$$e(S,\mu) := \text{emb.dim}\left(\frac{\hat{S}}{J}\right).$$

We assume that $I \subseteq \mathfrak{q}^2$. Let $v = (v_1, \ldots, v_n)$ be a minimal set of generators of $\mathfrak{q}$. We have $\mu(v_j) \in G_1$ for every index j.

Definition 4.1.8 We have $\sum_{j=1}^{n} \mathbb{Q}\mu(v_j) \subseteq G_1 \otimes \mathbb{Q}$ and we set

$$r(S,v,\mu) := \dim_{\mathbb{Q}}\left(\sum_{j=1}^{n} \mathbb{Q}\mu(v_j)\right).$$

Remark 4.1.9 We have $r(S, v, \mu) \leq e(S, \mu)$.

Now we consider $M \subset \{1, ..., n\}$ and

$$(S,v) \to \left(S_1, v^{(1)} = \left(v_1^{(1)}, \ldots, v_{n_1}^{(1)}\right)\right)$$

a framed blow-up along (v_M). We set $C' = \{1, ..., n_1\} \setminus D_1$, where D_1 is as in 3.1.3.

If the elements of v_M are L-linearly independent in $\frac{\mathfrak{q}\hat{S}}{J+\mathfrak{q}^2\hat{S}}$, then there exists a partition of A that we denote by $A' \sqcup A''$. This partition is such that $v_M \cup v_{A'}$ are L-linearly independent modulo $J+\mathfrak{q}^2\hat{S}$ and $v_{A''}$ is in the space generated by $v_J \cup v_{A'}$ over L modulo $J+\mathfrak{q}^2\hat{S}$. As we know that $v'_{A\cup B\cup\{j\}} = v_{D_1}^{(1)}$, we can identify $A' \cup B \cup \{j\}$ with a subset of D_1.

Now we set $I_1 := \{x \in S_1 \text{ such that } \mu(x) \notin G_1\}$ and we consider $\overline{J}_1$ the implicit prime ideal of $\frac{\hat{S}_1}{I_1\hat{S}_1}$ with respect to μ_1 and J_1 its preimage in $\hat{S}_1$. We call $\mathfrak{q}_1$ the maximal ideal of S_1 and L_1 its residue field.

Remark 4.1.10 We have $e(S, \mu) = n$ if and only if the elements of v are L-linarly independent in $\frac{\mathfrak{q}\hat{S}}{J+\mathfrak{q}^2\hat{S}}$.

Theorem 4.1.11 If $e(S, \mu) = n$, then:

$$e(S_1,\mu) \leq e(S,\mu).$$

This inequality is strict once the elements of $v^{(1)}_{A'\cup B\cup\{j\}\cup C'}$ are L_1-linearly dependent in $\frac{\mathfrak{q}_1\hat{S}_1}{J_1+\mathfrak{q}_1^2\hat{S}_1}$.

Proof. By definition, $v^{(1)}$ generates the maximal ideal $\mathfrak{q}_1$ of S_1, and so induces a set of generators of $\mathfrak{q}_1\frac{\widehat{S_1}}{J_1}$. Since $n_1 \leq n$, by definition of a framed blow-up, we know that $\sharp C' \leq \sharp C$.

Furthermore, we have $e(S, \mu) = \sharp M + \sharp A'$. We also know that $v^{(1)}_{D_1\setminus(A'\cup B\cup\{j\})}$ is in the L-vector space of $v^{(1)}_{A'\cup B\cup\{j\}\cup C'}$ modulo $J_1+\mathfrak{q}_1^2\hat{S}_1$.

So:

$$\begin{aligned} e(S_1,\mu) &\leq \sharp A' + \sharp B + \sharp\{j\} + \sharp C' \\ &\leq \sharp A' + \sharp B + 1 + \sharp C \\ &= \sharp A' + \sharp M \\ &= e(S,\mu). \end{aligned}$$

If in addition the elements of $v^{(1)}_{A'\cup B\cup\{j\}\cup C'}$ are L_1-linearly dependents in $\frac{\mathfrak{q}_1\hat{S}_1}{J_1+\mathfrak{q}_1^2\hat{S}_1}$ then we have $e(S_1, \mu) < \sharp A' + \sharp B + \sharp\{j\} + \sharp C'$ and so $e(S_1, \mu) < e(S, \mu)$.

Theorem 4.1.12 We have $r(S_1, v^{(1)}, \mu) \geq r(S, v, \mu)$.

Proof. This is induced by the two last points of Proposition 3.2.5.

Corollary 4.1.13 Once $e(S, \mu) = n$, we have

$$\left(e\left(S_1, \mu\right), e\left(S_1, \mu\right) - r\left(S_1, v^{(1)}, \mu\right)\right) \leq \left(e\left(S, \mu\right), e\left(S, \mu\right) - r\left(S, v, \mu\right)\right).$$

The inequality is strict if $e(S_1, \mu) < n$.

Remark 4.1.14 We are doing an induction on the dimension n. We saw that this dimension decreases by the sequence of blow-ups.

If it decreases strictly, then it will happen a finite number of time and the proof is finished.

Then, after now, we assume this dimension to be constant by blow-up. In other words for all framed sequence $S \to S_1$, we assume that $e(S, \mu) = e(S_1, \mu) = n$.

Similarly, we may assume that $r(S, v, \mu) = r(S_1, v^{(1)}, \mu)$.

4.2 Implicit ideal

Let $(R, \mathfrak{m}, k)$ be a local quasi excellent ring equicharacteristic and let ν be a valuation of rank 1 of its field of fractions, centered in R and of value group Γ_1. We denote by H the implicit prime ideal of R for the valuation ν.

By the Cohen structure Theorem, there exists an epimorphism Φ from a complete regular local ring $A \simeq k[[u_1,...,u_n]]$ of field of fractions K into $\frac{\hat{R}}{H}$. Its kernel I is a prime ideal of A.

We consider μ a monomial valuation with respect to a regular system of parameters of A_I. It is a valuation on A centered in I such that $k_\mu = \kappa(I)$ where $\kappa(I)$ is the residue field of I. Then we set $\widehat{\nu} := \widetilde{\nu} \circ \mu$, hence we define a valuation on A. Let Γ be the group of $\widehat{\nu}$.

Then, Γ_1 is the smallest non-trivial isolated subgroup of Γ and we have:

$$I = \left\{ f \in A \text{ such that } \widehat{\nu}\left(f\right) \notin \Gamma_1 \right\}.$$

Definition 4.2.1 Let $\pi : (A, u) \to (A', u')$ be a framed blow-up and $\sigma : A' \to \widehat{A'}$ be the formal completion of A'. The composition $\sigma \circ \pi$ is called formal framed blow-up.

A composition of such blow-ups is called a formal framed sequence.

Let $(A, u) \to (A_1, u^{(1)}) \to \cdots \to (A_l, u^{(l)})$ a formal sequence, that we denote by $(*)$.

Definition 4.2.2 The formal sequence$(A, u) \to (A_1, u^{(1)}) \to \cdots \to (A_l, u^{(l)})$ is said defined on Γ_1 if for every integers $i \in \{0,..., l - 1\}$ and $q \in J_i$, we have $\nu\left(u_q^{(i)}\right) \in \Gamma_1$.

Now we consider $A_i \simeq k_i\left[\left[u_1^{(i)},\ldots,u_n^{(i)}\right]\right]$ and we denote by I_i^{strict} the strict transform of I in A_i.

Definition 4.2.3 We call formal transformed of I in A_i, and we denote it by I_i, the preimage in A_i of the implicit ideal of $\frac{A_i}{I_i^{\text{strict}}}$.

Let v_i be the greatest integer of $\{r,..., n\}$ such that

$$I_i \cap k_i\left[\left[u_1^{(i)},\ldots,u_{v_i}^{(i)}\right]\right] = (0)$$

and we set

$$B_i := k_i\left[\left[u_1^{(i)},\ldots,u_{v_i}^{(i)}\right]\right].$$

Definition 4.2.4 Let P be a prime ideal of A. We call ℓ-th symbolic power of P the ideal $P^{(\ell)} := \left(P^\ell A_P\right) \cap A$.

Equivalently, we have $P^{(\ell)} = \left\{x \in A \text{ such that } \exists y \in A \setminus P \text{ such that } xy \in P^\ell\right\}$.

It is the set composed by the elements that vanish with order at least ℓ in the generic point of $V(P)$.

Let G be a complete ring of dimension strictly less than n and let θ be a valuation centered in G, of value group $\widetilde{\Gamma}$.

We consider $\widetilde{\Gamma}_1$ the first non trivial isolated subgroup of $\widetilde{\Gamma}$ and $\mathfrak{g} := \left\{g \in G \text{ such that } \theta(g) \notin \widetilde{\Gamma}_1\right\}$.

The next result will help us to prove the simultaneous local uniformization by induction.

Proposition 4.2.5 Assume that:

(1) In the formal sequence $(A, u) \to (A_1, u^{(1)}) \to \cdots \to (A_l, u^{(l)})$, there exists a formal framed subsequence

$$\pi : (A, u) \to (A_i, u^{(i)})$$

such that $v_i < n - 1$.

(2) For every ring G as above, every element in $G \setminus \mathfrak{g}^{(2)}$ is monomializable by a formal framed sequence defined on $\widetilde{\Gamma}_1$.

Then for every element f of $A \setminus I^{(2)}$, there exists a formal sequence

$$(A, u) \to \cdots \to (A_l, u^{(l)})$$

defined over Γ_1 such that f can be written as a monomial in $u_1^{(l)}, \ldots, u_n^{(l)}$ multiplied by an element of $A_l^{\times}$.

Proof. We assume that there exists a formal framed sequence

$$\pi : (A, u) \to (A_i, u^{(i)})$$

such that $v_i < n - 1$. It means that $v_i + 1 < n$. By definition of v_i, we know that $\mathfrak{g}_i := I_i \cap k_i\left[\left[u_1^{(i)}, \ldots, u_{v_i+1}^{(i)}\right]\right] \neq (0)$. So we consider an element g in $\mathfrak{g}_i \setminus \mathfrak{g}_i^{(2)} \subseteq C_i \setminus \mathfrak{g}_i^{(2)}$, where $C_i := k_i\left[\left[u_1^{(i)}, \ldots, u_{v_i+1}^{(i)}\right]\right]$. Since $v_i + 1 < n$, the ring C_i is of dimension strictly less than n. So we can use the second hypothesis on the element g in the ring C_i.

Hence there exists a formal sequence defined over Γ_1

$$\left(C_i, \left(u_1^{(i)}, \ldots, u_{v_i+1}^{(i)}\right)\right) \to \cdots \to \left(S', \left(u_1', \ldots, u_{v'}'\right)\right)$$

where $v' \leq v_i + 1$, and such that g can be written as a monomial in $u_1', \ldots, u_{v'}'$ multiplied by an element of $S'^{\times}$.

Since $g \in \mathfrak{g}_i$, there exists a regular parameter of S', say $u_{v'}'$, such that $\nu\left(u_{v'}'\right) \notin \Gamma_1$. Indeed, $g \in \mathfrak{g}_i = I_i \cap C_i$, so $g \in I_i$ hence it belongs to I. Equivalently, itsatisfies $\widehat{\nu}(g)$ / $\notin$ Γ_1. Since g can be written as a monomial in the generators of the maximal ideal of S', one of these generator which appears in the factorization of g must be in I. Hence $e\left(S', \widehat{\nu}_{|S'}\right) < v_i + 1$.

Replacing every ring O which appears in

$$\left(C_i, \left(u_1^{(i)}, \ldots, u_{v_i+1}^{(i)}\right)\right) \to \cdots \to \left(S', \left(u_1', \ldots, u_{v'}'\right)\right)$$

by $O\left[\left[u_{v_i+2}^{(i)}, \ldots, u_n^{(i)}\right]\right]$, we obtain a formal sequence

$$\pi' : \left(A_i, u^{(i)}\right) \to \cdots \to \left(A_l, u^{(l)}\right)$$

independent of $u_{v_i+2}^{(i)}, \ldots, u_n^{(i)}$, with $A_l = S'\left[\left[u_{v_i+2}^{(i)}, \ldots, u_n^{(i)}\right]\right]$. But we know that $e\left(S', \widehat{\nu}_{|S'}\right) < v_i + 1$, and so $e\left(A_l, \widehat{\nu}\right) < n$.

Let f be an element of $A \setminus I^{(2)}$. Its image under $\pi' \circ \pi$ is an element of A_l, whose dimension is strictly less than n. Since all the A_i are quasi-excellent, we have $f \notin A_i \setminus I_i^{(2)}$ and we can use again the second hypothesis. Hence we constructed a formal sequence $\pi' \circ \pi$ such that f can be written as a monomial in the generators of the maximal ideal of A_l multiplied by a unit of A_l. This completes the proof.

Now, we assume that for every formal sequence $(A, u) \to (A_1, u^{(1)}) \to \cdots \to (A_l, u^{(l)})$ and for every integer i, we have $v_i \in \{n - 1, n\}$.

So for every integer i, we have $I_i \cap k_i\left[\left[u_1^{(i)},\ldots,u_{n-1}^{(i)}\right]\right]=(0)$.

We consider a complete local ring G of dimension strictly less than n and a valuation θ of rank 1 centered in G.

Lemma 4.2.6 Assume that for every ring G as above, there exists a formal framed sequence that monomializes every element of G.

Then I is of height at most 1.

Proof. If $I = (0)$, the proof is finished. So we assume $I \neq (0)$ and we consider $f \in I \setminus \{0\}$. We write

$$f=\sum_{j=0}^{\infty} a_j u_n^j$$

with $a_j \in k[[u_1,\ldots, u_{n-1}]]$. We consider an integer N big enough such that every a_j with $j > N$ is in the ideal generated by $(a_0,\ldots, a_N)$. Now let us consider

$$\delta:=\min\left\{j\in\{0,\ldots,N\} \text{ such that } \nu\left(a_j\right)=\min_{0\le s\le N}\left\{\nu\left(a_s\right)\right\}\right\}.$$

We set $\overline{u}:=\left(u_1,\ldots,u_{n-1}\right)$ and $B:=k\left[\left[\overline{u}\right]\right]$. Since B is a complete local ring of dimension strictly less than n, by hypothesis we can construct a formal sequence $\left(B,\overline{u}\right)\to\left(B',\overline{u}'\right)$ such that for every $j \in \{0,\ldots, N\}$, the element a_j is a monomial in $\overline{u}'$. By Propositions 3.2.4 and 3.2.7, we can construct a local framed sequence $\left(B',\overline{u}'\right)\to\left(B'',\overline{u}''\right)$ such that $a_\delta \mid a_j$ for every $j \in \{0,\ldots, N\}$ in B'', since a_δ has minimal value. So we have a sequence

$$\left(B,\overline{u}\right)\to\left(B',\overline{u}'\right)\to\left(B'',\overline{u}''\right).$$

We compose with the formal completion and obtain

$$\left(B,\overline{u}\right)\to\left(\widehat{B''},\overline{u}''\right)$$

in which we still have $a_\delta \mid a_j$ for every $j \in \{0,\ldots, N\}$.

We replace again all the rings O of the sequence $\left(B,\overline{u}\right)\to\left(\widehat{B''},\overline{u}''\right)$ by $O[[u_n]]$, and obtain a sequence $(A, u) \to (A', u')$ independent of u_n and in which we still have $a_\delta \mid a_j$ for every $j \in \{0,\ldots, N\}$.

We recall that for every index i, we have

$$I_i\cap k_i\left[\left[u_1^{(i)},\ldots,u_{n-1}^{(i)}\right]\right]=(0).$$

If we denote by I' the formal transform of I in A', we obtain $I'\cap\widehat{B''}=(0)$. We know that $\frac{f}{a_\delta}\in I'$, and by Weierstrass preparation Theorem, $\frac{f}{a_\delta}=xy$ where x is a unit of A', and y is a monic polynomial in u_n of degree δ. Then the morphism $\widehat{B''}\to\frac{A'}{I'}$ is injective and finite.

Hence $\dim\left(\frac{A'}{I'}\right)=\dim\left(\widehat{B''}\right)=n-1$. Since $\dim\left(A'\right)=n$, we have $\operatorname{ht}\left(I\right)\le\operatorname{ht}\left(I'\right)=\dim\left(A'\right)-\dim\left(\frac{A'}{I'}\right)=n-(n-1)=1$. This completes the proof.

Corollary 4.2.7 (of Lemma 4.2.6). We keep the same hypothesis as in Lemma 4.2.6. Let $I = (h)$.

There exists a formal framed sequence $(A, u) \to (A', u')$ such that in A', the strict transform of h is a monic polynomial of degree δ.

From now on, we assume that h is a monic polynomial of degree δ.

Proposition 4.2.8 We keep the same hypothesis as in Lemma 4.2.6. Let $I = (h)$. The polynomial h is a key polynomial.

Proof. By definition, $I = \{f \in A \text{ such that } \widehat{\nu}(f) \notin \Gamma_1\}$, so $\widehat{\nu}(h) \notin \Gamma_1$. Further-more, for every non-zero integer b, we have $\widehat{\nu}(\partial_b h) \in \Gamma_1$ since h is a generator of I, hence has the smallest degree among all the elements of I and so $\partial_b h \notin I$.

Then $\epsilon(h) \notin \Gamma_1$.

Let P be a polynomial such that $\deg(P) < \deg(h)$. To show that h is a key polynomial, it remains to prove that $\epsilon(P) < \epsilon(h)$.

By the minimality of $\deg(h)$, we still have $P \notin I$ and so $\widehat{\nu}(P) \in \Gamma_1$. So for every non-zero integer b, we also have $\widehat{\nu}(\partial_b P) \in \Gamma_1$. Then $\epsilon(P) \in \Gamma_1$.

Assume, aiming for contradiction, that $\epsilon(P) \geq \epsilon(h)$.

Then $-\epsilon(P) \leq \epsilon(h) \leq \epsilon(P)$ and since Γ_1 is an isolated subgroup, Γ_1 is a segment and so $\epsilon(h) \in \Gamma_1$. Contradiction.

Hence, $\epsilon(P) < \epsilon(h)$ and h is a key polynomial.

Now we are going to monomialize the key polynomial h.

As in the previous part, we construct a sequence $(Q_i)_{i \geq 1}$ of key polynomials such that for each i the polynomial Q_{i+1} is either an optimal or a limit immediate successor of Q_i that begins with x and ends with h. So since $\epsilon(h)$ is maximal in $\epsilon(\Lambda)$, we stop. Then we have a finite sequence $(Q_i)_{i \geq 1}$ of key polynomials such that for each i the polynomial Q_{i+1} is either an optimal or a limit immediate successor of Q_i that begins with x and ends with h.

In the case $I = (0)$, we construct again a sequence $(Q_i)_{i \geq 1}$ of key polynomials such that for each i the polynomial Q_{i+1} is either an optimal or a limit immediate successor of Q_i such that $\epsilon(\mathcal{Q})$ is cofinal in $\epsilon(\Lambda)$.

Since we don't assume $k = k_\nu$ in this part, we need a generalization of the monomialization Theorems of the Part 3, paragraph 7.

4.3 Monomialization of key polynomials

Here we consider the ring $A \simeq k[[u_1,...,u_n]]$ and a valuation ν centered in A of value group Γ. For more clarity, we recall some previous notation.

Let r be the dimension of $\sum_{i=1}^{n} \mathbb{Q}\nu(u_i)$ in $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. Renumbering if necessary, we may assume that $\nu(u_1),..., \nu(u_r)$ are rationaly independent and we consider Δ the subgroup of Γ generated by $\nu(u_1),..., \nu(u_r)$.

We set $E := \{1,..., r, n\}$ and

$$\overline{\alpha^{(0)}} := \min_{\alpha \in \mathbb{N}^*} \{\alpha \text{ such that } \alpha\nu(u_n) \in \Delta\}.$$

So $\overline{\alpha^{(0)}}\nu(u_n) = \sum_{j=1}^{r} \alpha_j^{(0)}\nu(u_j)$ with

$$\alpha_1^{(0)},\ldots,\alpha_s^{(0)} \geq 0$$

and

$$\alpha_{s+1}^{(0)},\ldots,\alpha_r^{(0)} < 0.$$

We set

$$w = (w_1,\ldots,w_r,w_n) = (u_1,\ldots,u_r,u_n)$$

and

$$v = (v_1,\ldots,v_t) = (u_{r+1},\ldots,u_{n-1}),$$

with $t = n - r - 1$.

We write $x_i = \mathrm{in}_\nu u_i$, and so $x_1,..., x_r$ are algebraically independent over k in G_ν. Let λ_0 be the minimal polynomial of x_n over $k[x_1,..., x_r]$, of degree α. If x_n is transcental, we set $\lambda_0 := 0$.

We consider

$$y = \prod_{j=1}^{r} x_j^{\alpha_j^{(0)}},$$

$$\overline{y} = \prod_{j=1}^{r} w_j^{\alpha_j^{(0)}},$$

$$z = \frac{x_n^{\overline{\alpha^{(0)}}}}{y}$$

and

$$\overline{z} = \frac{w_n^{\overline{\alpha^{(0)}}}}{\overline{y}}.$$

Let $d_0 := \frac{\alpha}{\overline{\alpha^{(0)}}} \in \mathbb{N}$.

If $\lambda_0 \neq 0$, we have

$$\lambda_0 = \sum_{q=0}^{d_0} c_q y^{d_0 - q} X^{q\overline{\alpha^{(0)}}}$$

where $c_q \in k$, $c_d = 1$ and $\sum_{q=0}^{d_0} c_q Z^q$ is the minimal polynomial of z over G_ν.

We are going to show that there exists a formal framed sequence that monomializes all the Q_i. We have $Q_1 = u_n$ so we have to begin by monomializing Q_2.

First, let us consider

$$Q = \sum_{q=0}^{d_0} a_q b_q \overline{y}^{d_0 - q} w_n^{q\overline{\alpha^{(0)}}}$$

where $b_q \in R$ such that $b_q \equiv c_q$ modulo $\mathfrak{m}$ and $a_q \in A^\times$.

Then we will show that we can reduce the problem to this special case.

Let

$$\gamma = (\gamma_1, \ldots, \gamma_r, \gamma_n) = (\alpha_1^{(0)}, \ldots, \alpha_s^{(0)}, 0, \ldots, 0)$$

and

$$\delta = (\delta_1, \ldots, \delta_r, \delta_n) = (0, \ldots, 0, -\alpha_{s+1}^{(0)}, \ldots, -\alpha_r^{(0)}, \overline{\alpha^{(0)}}).$$

We have

$$w^{\delta} = w_n^{\delta_n} \prod_{j=1}^{r} w_j^{\delta_j} = \frac{w_n^{\overline{\alpha^{(0)}}}}{\prod_{j=s+1}^{r} w_j^{\alpha_j^{(0)}}}$$

and

$$w^{\gamma} = \prod_{j=1}^{s} w_j^{\alpha_j^{(0)}}.$$

So $\frac{w^{\delta}}{w^{\gamma}} = \frac{w_n^{\overline{\alpha^{(0)}}}}{\prod_{j=1}^{r} w_j^{\alpha_j^{(0)}}} = \overline{z}$.

Let us compute the value of w^{δ}.

$$\begin{aligned}
\nu(w^{\delta}) &= \overline{\alpha^{(0)}}\nu(w_n) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(w_j) \\
&= \overline{\alpha^{(0)}}\nu(u_n) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(u_j) \\
&= \sum_{j=1}^{r} \alpha_j^{(0)}\nu(u_j) - \sum_{j=s+1}^{r} \alpha_j^{(0)}\nu(u_j) \\
&= \sum_{j=1}^{s} \alpha_j^{(0)}\nu(u_j) \\
&= \sum_{j=1}^{s} \alpha_j^{(0)}\nu(w_j) \\
&= \nu(w^{\gamma}).
\end{aligned}$$

Theorem 4.3.1 There exists a local framed sequence

$$\left(A,u\right)\xrightarrow{\pi_0}\left(A_1,u^{(1)}\right)\xrightarrow{\pi_1}\cdots\xrightarrow{\pi_{l-1}}\left(A_l,u^{(l)}\right) \tag{12}$$

with respect to ν, independent of v, that has the following properties:

For every integer $i \in \{1,..., l\}$, we write $u^{(i)} = \left(u_1^{(i)},\ldots,u_{n_i}^{(i)}\right)$ and denote by k_i the residue field of A_i.

(1) The blow-ups $\pi_0,..., \pi_{l-2}$ are monomial.

(2) We have $\overline{z} \in A_l^{\times}$.

(3) We have

$$n_l = \begin{cases} n & \text{if } \lambda_0 \neq 0 \\ n-1 & \text{otherwise.} \end{cases}$$

(4) We set

$$u^{(l)} = \begin{cases} \left(w_1^{(l)}, \dots, w_r^{(l)}, v, w_n^{(l)}\right) & \text{if } \lambda_0 \neq 0 \\ \left(w_1^{(l)}, \dots, w_r^{(l)}, v\right) & \text{otherwise.} \end{cases}$$

For every integer $j \in \{1,..., r, n\}$, w_j is a monomial in $w_1^{(l)}, \dots, w_r^{(l)}$ multiplied by an element of $A_l^\times$. And for every integer $j \in \{1,..., r\}$, $w_j^{(l)} = w^\eta$ where $\eta \in \mathbb{Z}^{r+1}$.

(5) If $\lambda_0 \neq 0$, then $Q = w_n^{(l)} \times \overline{y}^{d_0}$.

Proof. We apply Proposition 3.2.4 to (w^δ, w^γ) and obtain a local framed sequence for ν, independent of v, such that $w^\gamma \mid w^\delta$ in A_l.

By Proposition 3.2.7 and the fact that w^δ and w^γ have same value, we have $w^\delta \mid w^\gamma$ in R_l. In fact $\overline{z}, \overline{z}^{-1} \in A_l^\times$. So we have the point (2).

We choose the sequence to be minimal, it means that the sequence composed by $\pi_0,..., \pi_{l-2}$ does not satisfy the conclusion of Proposition 3.2.4 for (w^δ, w^γ). We are now going to show that this sequence satisfies the conclusion of Theorem 4.3.1. Let $i \in \{0,..., l\}$. We write $w^{(i)} = \left(w_1^{(i)}, \dots, w_{r_i}^{(i)}, w_{n_i}^{(i)}\right)$, with $r_i = n_i - t - 1 > 0$. For every integers $i \in \{0,..., l\}$ and $j \in \{1, \dots, n_i\}$, we write $\beta_j^{(i)} = \nu\left(u_j^{(i)}\right)$. For all $i < l$, π_i is a blow-up along an ideal of the form $\left(u_{J_i}^{(i)}\right)$. Renumbering if necessary, we may assume that $1 \in J_i$ and that A_{i+1} is a localization of $A_i\left[\frac{u_{J_i}^{(i)}}{u_1^{(i)}}\right]$. Hence, $\beta_1^{(i)} = \min_{j \in J_i}\left\{\beta_j^{(i)}\right\}$.

Lemma 4.3.2 Let $i \in \{0,..., l-1\}$. We assume that the sequence $\pi_0,..., \pi_{i-1}$ of (12) is monomial.

We write $w^\gamma = \left(w^{(i)}\right)^{\gamma^{(i)}}$ and $w^\delta = \left(w^{(i)}\right)^{\delta^{(i)}}$. Then:

(1) $r_i = r$,

(2)

$$\sum_{q \in E}\left(\gamma_q^{(i)} - \delta_q^{(i)}\right)\beta_q^{(i)} = 0, \tag{13}$$

(3) gcd $\left(\gamma_1^{(i)} - \delta_1^{(i)}, \dots, \gamma_r^{(i)} - \delta_r^{(i)}, \gamma_n^{(i)} - \delta_n^{(i)}\right) = 1$,

(4) Every $\mathbb{Z}$-linear dependence relation between $\beta_1^{(i)}, \dots, \beta_r^{(i)}, \beta_n^{(i)}$ is an integer multiple of (13).

Proof.

(1) It is enough to do an induction on i and use Remark 3.1.6.

(2) We have $\nu\left(w^\gamma\right) = \nu\left(w^\delta\right)$, in other words $\nu\left(\left(w^{(i)}\right)^{\gamma^{(i)}}\right) = \nu\left(\left(w^{(i)}\right)^{\delta^{(i)}}\right)$. Since $w^{(i)} = \left(w_1^{(i)}, \dots, w_{r_i}^{(i)}, w_{n_i}^{(i)}\right)$, we have:

$$\nu\left(\prod_{j=1}^{r_i}\left(w_j^{(i)}\right)^{\gamma_j^{(i)}} \times \left(w_{n_i}^{(i)}\right)^{\gamma_{n_i}^{(i)}}\right) = \nu\left(\prod_{j=1}^{r_i}\left(w_j^{(i)}\right)^{\delta_j^{(i)}} \times \left(w_{n_i}^{(i)}\right)^{\delta_{n_i}^{(i)}}\right).$$

So we have

$$\sum_{j=1}^{r_i}\gamma_j^{(i)}\nu\left(w_j^{(i)}\right) + \gamma_{n_i}^{(i)}\nu\left(w_{n_i}^{(i)}\right) = \sum_{j=1}^{r_i}\delta_j^{(i)}\nu\left(w_j^{(i)}\right) + \delta_{n_i}^{(i)}\nu\left(w_{n_i}^{(i)}\right).$$

By definition of $w^{(i)}$, for every integer $j \in \{1, \dots, r_i, n_i\}$, we have $w_j^{(i)} = u_j^{(i)}$. So $\nu\left(w_j^{(i)}\right) = \beta_j^{(i)}$. Then:

$$\sum_{j=1}^{r_i}\gamma_j^{(i)}\beta_j^{(i)} + \gamma_{n_i}^{(i)}\beta_{n_i}^{(i)} = \sum_{j=1}^{r_i}\delta_j^{(i)}\beta_j^{(i)} + \delta_{n_i}^{(i)}\beta_{n_i}^{(i)}.$$

Hence $\sum_{j\in\{1,\ldots,r_i,n_i\}}\left(\gamma_j^{(i)}-\delta_j^{(i)}\right)\beta_j^{(i)}=0.$

But $r_i = n_i - t - 1 = $ r, so $n_i = r + t + 1 = n$, and:

$$\begin{aligned}\sum_{j\in\{1,\ldots,r_i,n_i\}}\left(\gamma_j^{(i)}-\delta_j^{(i)}\right)\beta_j^{(i)} &= \sum_{j\in\{1,\ldots,r,n\}}\left(\gamma_j^{(i)}-\delta_j^{(i)}\right)\beta_j^{(i)}\\ &= \sum_{j\in E}\left(\gamma_j^{(i)}-\delta_j^{(i)}\right)\beta_j^{(i)}\\ &= 0.\end{aligned}$$

(3) Same proof as in Theorem 3.4.4.

Lemma 4.3.3 The sequence $(A,u)\xrightarrow{\pi_0}\left(A_1,u^{(1)}\right)\xrightarrow{\pi_1}\cdots\xrightarrow{\pi_{l-1}}\left(A_l,u^{(l)}\right)$ of Theorem 4.3.1 is not monomial.

Proof. Same proof as Lemma 3.4.7.

Lemma 4.3.4 Let $i \in \{0,\ldots, l-1\}$ and we assume that $\pi_0,\ldots,\pi_{i-1}$ are all monomial. Then following properties are equivalent:

(1) The blow-up π_i is not monomial.

(2) There exists a unique index $q\in J_i\setminus\{1\}$ such that $\beta_q^{(i)}=\beta_1^{(i)}$.

(3) We have $i = l - 1$.

Proof. Same proof as Lemma 3.4.8.

Using induction on i and Lemma 4.3.4, we conclude that $\pi_0,\ldots,\pi_{l-2}$ are monomial. This proves the first point of the Theorem.

It remains to prove the last three points.

By Lemma 4.3.4 we know that there exists a unique element $q\in J_{l-1}\setminus\{j_{l-1}\}$ such that $\beta_q^{(l-1)}=\beta_1^{(l-1)}$, hence we are in the case $\sharp B_{l-1} + 1 = \sharp J_{l-1} - 1$. We now have to see if $t_{k_{l-1}}=0$ or 1.

We recall that $w_1^{(l-1)}=w^{\epsilon}$ and $w_q^{(l-1)}=w^{\mu}$ where ϵ and μ are two columns of a unimodular matrix such that $\mu-\epsilon=\pm(\gamma-\delta)$. So $x_1^{(l-1)}=x^{\epsilon}$ and $x_q^{(l-1)}=x^{\mu}$, then

$$\frac{x_q^{(l-1)}}{x_1^{(l-1)}}=x^{\mu-\epsilon}=x^{\pm(\gamma-\delta)}=x^{\pm\left(\alpha_1^{(0)},\ldots,\alpha_r^{(0)},-\overline{\alpha^{(0)}}\right)}.$$

In other words

$$\frac{x_q^{(l-1)}}{x_1^{(l-1)}}=\left(\frac{\prod_{j=1}^{r}x_j^{\alpha_j^{(0)}}}{x_n^{\overline{\alpha^{(0)}}}}\right)^{\pm1}=\left(z^{-1}\right)^{\pm1}=z^{\pm1}.$$

So we can assume $\frac{x_q^{(l-1)}}{x_1^{(l-1)}}=z$.

The case $t_{k_{l-1}}$ = 1 corresponds to the fact that z is transcendantal over k, in other words $\lambda_0 = 0$. The case $t_{k_{l-1}}$ = 0 corresponds to the fact that z is algebraic over k, in other words $\lambda_0 \neq 0$. The third point of the Theorem is then a consequence of 3.1.9.

Since $\beta_1^{(l-1)},\ldots,\beta_r^{(l-1)}$ are linearly independent, we have $q = n$. By 3.1.9, if $\lambda_0 \neq 0$, we have

$$w_n^{(l)} = u_n^{(l)} = \overline{\lambda_0}(u_n') = \overline{\lambda_0}\left(\frac{u_n^{(l-1)}}{u_1^{(l-1)}}\right) = \overline{\lambda_0}\left(\frac{w_n^{(l-1)}}{w_1^{(l-1)}}\right) = \overline{\lambda_0}\left(\overline{z}\right) = \sum_{i=0}^{d} a_i b_i \overline{z}^i .$$

Remark 4.3.5 We have $\overline{\lambda_0}\left(\overline{z}\right) = \sum_{i=0}^{d} c_i b_i \overline{z}^i$ where c_i are units. Then we choose to set $c_i = a_i$ for every index i. But since $\overline{z} = \frac{\overline{w_n^{\alpha(0)}}}{\overline{y}}$, we have

$$w_n^{(l)} = \sum_{i=0}^{d_0} a_i b_i \left(\frac{\overline{w_n^{\alpha(0)}}}{\overline{y}}\right)^i = \frac{\sum_{i=0}^{d_0} a_i b_i \overline{y}^{d_0-i}\left(\overline{w_n^{\alpha(0)}}\right)^i}{\overline{y}^{d_0}} = \frac{Q}{\overline{y}^{d_0}}$$

and the point (3.3) is proven.

So it remains to prove the point (3.2).

We apply Proposition 3.2.5 to $i = 0$ and $i' = l$. By the monomiality of $\pi_0,..., \pi_{l-2}$, we know that $D_i = \{1,..., n\}$ for every $i \in \{1,..., l-1\}$.

We know that $D_l = \{1,..., n\}$ if $\lambda \neq 0$ and $D_l = \{1,..., n-1\}$ otherwise. Here we set again $u_T = v$.

By Proposition 3.2.5, for every $j \in \{1,..., r, n\}$, $w_j = u_j$ is a monomial in $w_1^{(l)},\ldots,w_r^{(l)}$ (or equivalently in $u_1^{(l)},\ldots,u_r^{(l)}$) multiplied by an element of $A_l^{\times}$.

Same thing for the fact that for every integer $j \in \{1,..., r\}$, we have $w_j^{(l)} = w^{\eta}$. This completes the proof.

Remark 4.3.6 In the case $Q_2 = Q$, we constructed a local framed sequence such that the total transform of Q_2 is a monomial. We will bring us to this case.

Definition 4.3.7 [24] A local framed sequence that satisfies Theorem 4.3.1 is called a n-generalized Puiseux package.

Let $j \in \{r+1,..., n\}$. A j-generalized Puiseux package is a n-generalized Puiseux package replacing n by j in Theorem 4.2.1.

Remark 4.3.8 We consider $(A, u) \to \cdots \to (A_i, u^{(i)}) \to ...$ a j-generalized Puiseux package, with $j \in \{r+1,..., n\}$. We replace each ring of this sequence by its formal completion, hence we obtain o formal framed sequence that we call a formal j-Puiseux package. So Theorem 4.3.1 induces a formal n-Puiseux package that satisfies the same conclusion as in Theorem 4.3.1.

Since we want to do an induction, now we will assume until the end of Theorem 4.3.14, that we know how to monomialize every complete local equicharacteristic quasi excellent ring G of dimension strictly less than n equipped with a valuation of rank 1 centered in G by a formal framed sequence. This hypothesis is called H_n.

Lemma 4.3.9 Let $P = \sum_{j \in S_{u_n}(P)} c_j u_n^j$ the u_n-expansion of an optimal immediat successor key element of u_n.

There exists a formal framed sequence $(A, u) \to (A_l, u^{(l)})$ that transforms each coeficient c_j in a monomial in $\left(u_1^{(l)},\ldots,u_r^{(l)}\right)$, multiplied by a unit of A_l.

Hence, after this sequence, P can be written like $\sum_{i=0}^{d_0} a_i b_i \overline{y}^{d_0-i}\left(\overline{w_n^{\alpha(0)}}\right)^i$.

Proof. We will prove a more general result in 4.3.12.

Theorem 4.3.10 If $u_n \ll_{\lim} P$, then P is monomializable.

Proof. Same proof as Theorem 3.4.14.

Lemma 4.3.11 There exists a formal framed sequence

$$\left(A,u\right) \to \left(A_l,u^{(l)}\right)$$

such that in A_l, the strict transform of the polynomial Q_2 is a monomial.

Proof. If $u_n < Q_2$, we use Lemma 4.3.9 and Theorem 4.3.1 to conclude. Otherwise, $u_n <_{\lim} Q_2$ and so we use Theorem 3.4.14.

We constructed a formal framed sequence that monomializes Q_2. But we want one that monomializes all the key polynomials of $\mathcal{Q}$.

Now we are going to show that if we constructed a formal framed sequence $(A, u) \to (A_l, u^{(l)})$ that monomializes Q_i, then we can associate another $(A_l, u^{(l)}) \to (A_s, u^{(s)})$ such that in A_s, the strict transform of Q_{i+1} is also a monomial.

Let Δ_l be the group $\nu\left(k_l\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)\setminus\{0\}\right)$ and

$$\alpha_l := \min\ h \text{ such that } h\beta_n^{(l)} \in \Delta_l\}.$$

We set $X_j = \mathrm{in}_\nu\left(u_j^{(l)}\right)$, $W_j = w_j^{(l)}$ and λ_l the minimal polynomial of X_n over $\mathrm{gr}_\nu k_l\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)$ of degree α_l.

We know that $Q_i = \varpi w_n^{(l)}$ with ϖ a monomial in $W_1,\ldots, W_r$ multiplied by a unit. We set $\omega := \mathrm{in}_\nu(\varpi)$.

If $Q_i <_{\lim} Q_{i+1}$, we use Theorem 4.3.10 and the proof is finished. So we assume that Q_{i+1} is an optimal immediate successor of Q_i.

We write $Q_{i+1} = \sum_{j\in S_{Q_i}(Q_{i+1})} a_j Q_i^j = \sum_{j=0}^{s} a_j Q_i^j$ the Q_i-expansion of Q_{i+1} in $k_l\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)\left(u_n^{(l)}\right)$.

We have $Q_{i+1} = Q_i^s + a_{s-1}Q_i^{s-1} + \cdots + a_0$ and since $Q_i = \varpi w_n^{(l)}$, we have

$$\frac{Q_{i+1}}{\varpi^s} = \left(u_n^{(l)}\right)^s + \frac{a_{s-1}}{\varpi}\left(u_n^{(l)}\right)^{s-1} + \cdots + \frac{a_0}{\varpi^s}.$$

We know that for every index j such that $a_j \neq 0$, we have

$$\nu\left(a_j Q_i^j\right) = \nu_{Q_i}\left(Q_{i+1}\right).$$

So all non-zero terms of the Q_i-expansion of Q_{i+1} have same value. Then, by hypothesis H_n, all these terms are divisible by the same power of ϖ after an appropriate sequence of blow-ups $(*_i)$ independent of $u_n^{(l)}$.

We denote by $\widetilde{Q}_{i+1}$ the strict transform of Q_{i+1} by the composition of $(*_i)$ with the sequence $(*_i')$ that monomializes Q_i. We denote this composition by (c_i).

We know that $\widetilde{Q}_i$, the strict transform of Q_i by (c_i), is a regular parameter of the maximal ideal of A_l. Indeed, by Proposition 3.2.5, we know that each u_j of A can be written as a monomial on $w_1^{(l)},\ldots,w_r^{(l)}$. In fact, the reduced exceptional divisor of this sequence is exactly $\mathrm{V}(\varpi)_{\mathrm{red}}$. Hence, as we know that $Q_i = w_n^{(l)}\varpi$, we do have that the strict transform of Q_i is $\widetilde{Q}_i = w_n^{(l)} = u_n^{(l)}$. So it is a key polynomial in the extension $k_l\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)\left(u_n^{(l)}\right)$.

Let us show that $\widetilde{Q}_{i+1} = \frac{Q_{i+1}}{\varpi^s}$.

We have $a_s = 1$ and $Q_i^s = \varpi^s\left(u_n^{(l)}\right)^s$ and also $u_n^{(l)} \nmid \varpi$, so ϖ^s divides the term $a_s Q_i^s$ and so all the non-zero terms of Q_i-expansion of Q_{i+1}. Furthermore, it is the biggest power of ϖ that divides each term, hence $\frac{Q_{i+1}}{\varpi^s}\left(u_n^{(l)}\right)^s + \frac{a_{s-1}}{\varpi}\left(u_n^{(l)}\right)^{s-1} + \cdots + \frac{a_0}{\varpi^s}$ is $\widetilde{Q}_{i+1}$ the strict transform of Q_{i+1} by the sequence of blow-ups, that satisfies $\widetilde{Q}_i \ll \widetilde{Q}_{i+1}$ by hypothesis.

Let G be a complete local equicharaceristic ring of dimension strictly less than n equipped with a valuation centered in G.

Lemma 4.3.12 We assume that for every ring G as above, every element of G is monomializable.

Assume that $Q_i < Q_{i+1}$ in $\mathcal{Q}$.

Then there exists a local framed sequence $(A_l, u^{(l)}) \to (A_e, u^{(e)})$ such that in A_e, he strict transform of Q_{i+1} is of the form $\sum_{q=0}^{s} \tau_q \eta_q X_n^q$, where $\tau_q \in R_e^\times$ and η_q are monomials in $u_1^{(e)},\ldots,u_r^{(e)}$.

Proof. By hypothesis, after a sequence of blow-ups independent of $u_n^{(l)}$, we can monomialize the a_j and assume that they are monomials in $\left(u_1^{(l)},\ldots,u_{n-1}^{(l)}\right)$ multiplied by units of A_l.

For every $g \in \{r + 1,..., n - 1\}$, we do a generalized g-Puiseux package as in Theorem 4.3.1, hence we have a sequence

$$\left(A_l, u^{(l)}\right) \to \left(A_t, u^{(t)}\right)$$

such that each $u_g^{(l)}$ is amonomial in $\left(u_1^{(t)}, \ldots, u_r^{(t)}\right)$.

In fact we can assume that the a_j are monomials in $\left(u_1^{(l)}, \ldots, u_r^{(l)}\right)$ multiplied by units of A_l.

Since the strict transform

$$\widetilde{Q}_{i+1} = \frac{Q_{i+1}}{\overline{\omega}^s} = \left(u_n^{(l)}\right)^s + \frac{a_{s-1}}{\overline{\omega}}\left(u_n^{(l)}\right)^{s-1} + \cdots + \frac{a_0}{\overline{\omega}^s}$$

is an immediate successor key element of $\widetilde{Q}_i$, this completes the proof.

Remark 4.3.13 Lemma 4.3.9 is a particular case of Lemma 4.3.12.

Theorem 4.3.14 We still assume H_n.

We recall that car $\left(k_\nu\right) = 0$ If Q_i is monomializable, then there exists a formal framed sequence

$$\left(A, u\right) \overset{\pi_0}{\to} \left(A_1, u^{(1)}\right) \overset{\pi_1}{\to} \cdots \overset{\pi_{l-1}}{\to} \left(A_l, u^{(l)}\right) \overset{\pi_l}{\to} \cdots \overset{\pi_{m-1}}{\to} \left(A_m, u^{(m)}\right) \tag{14}$$

that monomializes Q_{i+1}.

Proof. There are two cases.

The first one: $Q_i < Q_{i+1}$.

Then the strict transform $\widetilde{Q}_{i+1}$ of Q_{i+1} by the sequence $(A, u) \to (A_l, u^{(l)})$ that monomializes Q_i is an immediate successor key element of $\widetilde{Q}_i = u_{n_l}^{(l)}$, and by Lemma 4.3.12 we just saw that we can bring us to the hypothesis of Theorem 4.3.1. So we use Theorem 4.3.1 replacing Q_1 by $\widetilde{Q}_i$ and Q_2 by $\widetilde{Q}_{i+1}$.

The last one: $Q_i <_{\lim} Q_{i+1}$.

We apply Theorem 4.3.10 replacing u_n by $\widetilde{Q}_i$ and P by $\widetilde{Q}_{i+1}$.

As in the previous part, we consider, for every integer j, the countable sets

$$\mathscr{S}_j := \left\{ \prod_{i=1}^{n} \left(u_i^{(j)}\right)^{\alpha_i^{(j)}}, \text{ with } \alpha_i^{(j)} \in \mathbb{Z} \right\}$$

and

$$\widetilde{\mathscr{S}_j} := \left\{ \left(s_1, s_2\right) \in \mathscr{S}_j \times \mathscr{S}_j, \text{ with } \nu\left(s_1\right) \le \nu\left(s_2\right) \right\}$$

assuming that for every $i \in \{1, \ldots, n\}$, $u_i^{(0)} = u_i$.

The set $\widetilde{\mathscr{S}_j}$ is countable for every j, so we can number its elements, and set $\widetilde{\mathscr{S}_j} := \left\{s_m^{(j)}\right\}_{m \in \mathbb{N}}$. Now we consider the finite set

$$\mathscr{S}_j' := \left\{s_m^{(j)}, \ m \le j\right\} \cup \left\{s_j^{(m)}, \ m \le j\right\}.$$

Hence $\bigcup_{j \in \mathbb{N}} \left(\mathscr{S}_j \times \mathscr{S}_j\right) = \bigcup_{j \in \mathbb{N}} \widetilde{\mathscr{S}_j} = \bigcup_{j \in \mathbb{N}} \mathscr{S}_j'$ is a countable union of finite sets.

Since we consider all the elements according uniquely to the variable u_n, and more generally according to $u_n^{(i)}$, and since we do an induction on the dimension, we have to know how to monomialize the elements of $B_i := k\left[u_1^{(i)}, \ldots, u_{n-1}^{(i)}\right]$.

Theorem 4.3.15 Let $A \simeq k[[u_1,...,u_n]]$ equipped with a valuation ν centered in A.

We recall that car $\left(k_\nu\right) = 0$. There exists a formal sequence

$$\left(A,u\right)\xrightarrow{\pi_0}\cdots\xrightarrow{\pi_{s-1}}\left(A_s,u^{(s)}\right)\xrightarrow{\pi_s}\cdots \tag{15}$$

that monomializes all the key polynomials of $\mathcal{Q}$ and all the elements of the B_i for all i. Furthermore, the sequence has the property:

$$\forall j\in\mathbb{N}\ \forall s=\left(s_1,s_2\right)\in\mathscr{S}_j'\ \exists i\in\mathbb{N}_{\geq j}\ \text{such that}\ s_1|\ s_2\ \text{in}\ A_i.$$

In other words for every index l, there exists an index p_l such that in A_{p_l}, Q_l is a monomial in $u^{(p_l)}$ multiplied by a unit of A_{p_l}.

Proof. To show that we can choose the sequence (15) such that

$$\forall j\in\mathbb{N}\ \forall s=\left(s_1,s_2\right)\in\mathscr{S}_j'\ \exists i\in\mathbb{N}_{\geq j}\ \text{such that}\ s_1|\ s_2\ \text{in}\ A_i,$$

and that all the elements of the B_i are monomialized, we do the same thing than in Theorem 3.4.21.

Then we do an induction on the dimension n and on the index i and we iterate the above process.

Corollary 4.3.16 Let $A\simeq k[[u_1,\ldots,u_n]]$ equipped with a valuation $\widehat{\nu}$ centered in A, of value group Γ. We assume

$$I=\left\{a\in A\ \text{such that}\ \widehat{\nu}\left(a\right)\notin\Gamma_1\right\}=\left(h\right)\neq\left(0\right),$$

where Γ_1 is the smallest isolated subgroup of Γ. We recall that car $\left(k_\nu\right)=0$.

There exists a formal framed sequence

$$\left(A,u\right)\to\ldots\to\left(A_l,u^{(l)}\right)\to\ldots$$

such that in A_l, the polynomial h can be written as a monomial multiplied by a unit.

Proof. The sequence $\mathcal{Q}$ has been constructed to contain h, so we just have to use Theorem 4.3.15.

4.4 Reduction

Let $(R, \mathfrak{m}, k)$ be a local quasi excellent equicharacteristic ring and let ν be a valuation of its field of fractions, of rank 1, centered in R and of value group Γ_1.

We denote by $\overline{H}$ the implicit ideal of R.

We are going to see that in this case, we just have to regularise $\frac{\widehat{R}}{\overline{H}}$.

We consider $\mathcal{F}:=\{f_1,\ldots,f_s\}\subseteq\mathfrak{m}$, and assume that f_1 has minimal value.

Remark 4.4.1 We consider $R\to\widehat{R}\to R_1\to\widehat{R}_1$ a formal framed blow-up and we denote by H' the strict transformed of $\overline{H}$ in R_1.

Then we define $\overline{H_1}$ as the preimage in $\widehat{R}_1$ of the implicit ideal of $\frac{\widehat{R}_1}{H'\widehat{R}_1}$.

We iterate this contruction for every formal framed sequence.

Theorem 4.4.2 We recall that car $\left(k_\nu\right)=0$. There exists a formal framed sequence

$$\left(R,u,k\right)=\left(R_0,u^{(0)},k_0\right)\to\cdots\to\left(R_i,u^{(i)}=\left(u_1^{(i)},\ldots,u_n^{(i)}\right),k_i\right)$$

such that:

(1) The ring $\frac{\widehat{R}_i}{\overline{H}_i}$ is regular,

(2) For every index j, we have that f_j mod $\left(\overline{H_i}\right)$ is a monomial in $u^{(i)}$ multiplied by a unit of $\frac{\widehat{R}_i}{\overline{H}_i}$,

(3) For every index j, we have f_1 mod $\left(\overline{H_i}\right)$ | f_j mod $\left(\overline{H_i}\right)$ in $\frac{\widehat{R}_i}{\overline{H}_i}$.

Proof. Set $n := e(R, \nu)$ and $u := (y, x)$ with

$$y := \left(y_1, \ldots, y_{\tilde{n}-n}\right)$$

and

$$x := \left(x_1, \ldots, x_n\right)$$

such that the images of the x_j in $\frac{\widehat{R}}{\overline{H}}$ induce a minimal set of generators of $\frac{\mathfrak{m}}{\overline{H}}$ and such that y generates $\overline{H}$.

We do an induction on $(n_i, n_i - r_i, v_i)$.

We saw the existence of the surjection Φ from $A \simeq k[[u_1,...,u_n]]$ to $\frac{\widehat{R}}{\overline{H}}$, of kernel $I = \{f \in A \text{ such that } \widehat{\nu}(f) \notin \Gamma_1\} \in \operatorname{Spec}(A)$ where $\widehat{\nu}$ is defined as in section 4.2. We denote by L the field of fractions of A.

If $v_0 < n-1$, then we do the same thing as in Proposition 4.2.5 and we strictly decrease $e(A, \widehat{\nu})$.

The we can assume $v_0 \in \{n-1, n\}$.

Assume $v_0 = n-1$.

Then we know that $I = (h)$ and that there exists a formal framed sequence $(A, x) \to \left(A_\ell, x^{(\ell)}\right)$ that monomializes h by Corollary 4.3.16. So one of the generators that appears in its decomposition must be in I_ℓ. Hence there exists $x_p^{(\ell)}$ such that $\widehat{\nu}\left(x_p^{(\ell)}\right) \notin \Gamma_1$. So by Theorems 4.2.5 and 4.1.11, there exists a local framed sequence that decreases strictly $e(A, \widehat{\nu})$, so this case can happen a finite number of time, and we bring us at the case $I = (0)$. It means the case where $\frac{A}{I}$ is regular.

Case $I = (0)$. For every f_j, we have $\widehat{\nu}(f_j) \in \Gamma_1$. So the element f_j is a non-zero formal series and by Weierstrass preparation Theorem, we know that we can see it like a polynomial in x_l with coeffcients in $k[[x_1,..., x_{n-1}]]$. We construct a sequence of key polynomials in the extension $k((x_1,..., x_{n-1}))(x_n)$ as in previous section. In other words this sequence is a sequence of optimal (possibly limit) immediate successors which is cofinal in $\epsilon(\Lambda)$, where Λ is the set of key polynomials. So the element f_j is non-degenerate with respect of one of these polynomials that all are monomializable by the above part. Hence there exists a local framed sequence $(A, x) \to (A_i, x^{(i)})$ such that in A_i, the strict transform of f_j is a monomial in $x^{(i)}$ multiplied by a unit of A_i.

If there exists a formal framed sequence such that $v_i < n-1$, then by Proposition 4.2.5, we can conclude by induction.

Iterating the case $I = (0)$, we assure the existence of a local framed sequence such that all the strict transforms of the f_j are monomials multiplied by units. Doing another blow-up if necessary, we assume that there exists of a local framed sequence $(A, x) \to (A', x')$ such that all the strict transforms of the f_j are monomials only in $x'_1, \ldots, x'_r$.

By Proposition 3.2.4, we can assume that for every j and every p, we have either $f_j \mid f_p$ or $f_p \mid f_j$.

So we have a local framed sequence

$$\left(A, x, k\right) \overset{\rho_0}{\to} \left(A_1, x^{(1)}, k_1\right) \overset{\rho_1}{\to} \cdots \overset{\rho_i}{\to} \left(A_i, x^{(i)}, k_i\right)$$

that monomializes the f_j and such that for all j and q, we have $f_j \mid f_q$ or the converse.

By the minimality of $\nu(f_1)$, in A_i, we have $f_1 \mid f_j$ for every j.

We have also two maps

$$\left(R, u, k\right) \to \left(\frac{\widehat{R}}{\overline{H}}, x, k\right) \leftarrow \left(A, x, k\right),$$

and we know that $\frac{A}{I} \simeq \frac{\widehat{R}}{\overline{H}}$ since $I = \operatorname{Ker}(\Phi)$. Hence, looking at the strict transform of $\frac{A}{I}$ at each step of the sequence $\{\rho_j\}_{0 \le j \le i}$, we obtain a local framed sequence

$$\left(\frac{\widehat{R}}{\overline{H}}, x, k\right) \xrightarrow{\widetilde{\rho_0}} \left(\tilde{R}_1, x^{(1)}, k_1\right) \xrightarrow{\widetilde{\rho_1}} \cdots \xrightarrow{\widetilde{\rho_i}} \left(\tilde{R}_i, x^{(i)}, k_i\right).$$

So we have the diagram:

$$\begin{array}{ccccccc} \left(\frac{\widehat{R}}{\overline{H}}, x, k\right) & \xrightarrow{\widetilde{\rho_0}} & \left(\tilde{R}_1, x^{(1)}, k_1\right) & \xrightarrow{\widetilde{\rho_1}} & \cdots & \xrightarrow{\widetilde{\rho_i}} & \left(\tilde{R}_i, x^{(i)}, k_i\right). \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \left(A, x, k\right) & \xrightarrow{\rho_0} & \left(A_1, x^{(1)}, k_1\right) & \xrightarrow{\rho_1} & \cdots & \xrightarrow{\rho_i} & \left(A_i, x^{(i)}, k_i\right) \end{array}$$

Similarly, either $\frac{A}{I}$ is regular, or the sequence $\{\rho_j\}$ can be chosen such that $e(R, \mu)$ strictly decreases.

So after a finite sequence of blow-ups, we bring us to the case where $\frac{\widehat{R_i}}{\overline{H_i}}$ is regular. Hence we can assume $\frac{\widehat{R_i}}{\overline{H_i}}$ regular and consider $f_1,..., f_s$ elements of $R \setminus \{0\}$ such that $\nu\left(f_1\right) = \min_{1 \le j \le s}\left\{\nu\left(f_j\right)\right\}$. We know that the f_j are all monomials in the $u^{(i)}$ and that $f_1 \bmod \left(\overline{H_i}\right) \mid f_j \bmod \left(\overline{H_i}\right)$. This completes the proof.

Theorem 4.4.3 Let R be a local quasi excellent domain and H be his implicit prime ideal. We assume that $\frac{\widehat{R}}{H}$ is regular.

We recall that car $\left(k_\nu\right) = 0$. There exists a sequence of blow-ups defined over R that resolves the singularities of R.

Proof. The ring $\widehat{R}_H$ is regular by Proposition 4.1.6. So we know that there exist elements $\left(\tilde{y}_1, \ldots, \tilde{y}_g\right)$ of $H\widehat{R}_H$ that form a regular system of parameters of $\widehat{R}_H$.

By definition of $H\widehat{R}_H$, it means that there exist $y_1,..., y_g$ elements of H and $b_1,..., b_g$ elements of $\widehat{R} \setminus H$ such that for every index i, we have $\tilde{y}_i = \frac{y_i}{b_i}$.

The b_i are elements of $R_H^{\times}$, so

$$\left(\tilde{y}_1, \ldots, \tilde{y}_g\right)\widehat{R}_H = \left(\frac{y_1}{b_1}, \ldots, \frac{y_g}{b_g}\right)\widehat{R}_H = \left(y_1, \ldots, y_g\right)\widehat{R}_H.$$

Then we have some elements $(y_1,..., y_g)$ of H that form a regular system of parameters of $\widehat{R}_H$.

Now we consider $(x_1,..., x_t)$ some elements of $\widehat{R} \setminus H$ whose images $\left(\overline{x}_1, \ldots, \overline{x}_t\right)$ modulo H form a regular system of parameters of $\frac{\widehat{R}}{H}$.

If $(y_1,..., y_g)$ generate H, then $\widehat{R}$ is regular. Indeed, in this case, $(y_1,..., y_g, x_1,..., x_t)$ generate $\widehat{\mathfrak{m}} = \mathfrak{m} \otimes_R \widehat{R}$, which is the maximal ideal of $\widehat{R}$.

So

$$\dim\left(\widehat{R}\right) \le g + t.$$

We know that

$$g = \dim\left(\widehat{R}_H\right) = \mathrm{ht}\left(H\right)$$

and

$$t = \dim\left(\frac{\widehat{R}}{H}\right) = \mathrm{ht}\left(\frac{\widehat{\mathfrak{m}}}{H}\right).$$

Then

$$\begin{aligned}
\dim\left(\widehat{R}\right) &= \mathrm{ht}\left(\widehat{\mathfrak{m}}\right) \\
&\geq \mathrm{ht}(H) + \mathrm{ht}\left(\frac{\widehat{\mathfrak{m}}}{H}\right) \\
&= g + t \\
&\geq \dim\left(\widehat{R}\right).
\end{aligned}$$

Then $\dim(\widehat{R}) = g + t$ and $(y_1,..., y_g, x_1,..., x_t)$ is a minimal set of generators of $\widehat{\mathfrak{m}}$, and so $\widehat{R}$ is regular.

Now we assume that $(y_1,..., y_g)$ do not generate H in $\widehat{R}$. So let us set $(y_1,..., y_g, y_{g+1},..., y_{g+s})$ some elements that generate H in $\widehat{R}$.

We consider $V := \frac{H\widehat{R}_H}{H^2\widehat{R}_H}$ that is a vector space of dimension $g = ht(H)$ over the residue field of H since $\widehat{R}_H$ is regular.

We know that $y_1,..., y_{g+s}$ generate V and that

$$g + s > \dim(V) = g,$$

so there exist elements $a_1,..., a_{g+s}$ of $\widehat{R}$ such that

$$a_1 y_1 + \ldots + a_{g+s} y_{g+s} \in H^2 \widehat{R}_H.$$

In other words there exist $a_1,..., a_{g+s}$ in $\widehat{R}$ and $\left(b_{i,j}\right)_{1\leq i,j\leq g+s}$ in $\widehat{R}_H$ such that

$$a_1 y_1 + \ldots + a_{g+s} y_{g+s} = \sum_{1\leq i,j\leq g+s} b_{i,j} y_i y_j.$$

We may assume

$$\nu(a_1) = \min_{1\leq i\leq s}\{\nu(a_i)\}$$

and also that for every i, the element a_i is not in H or is zero.

Since the a_i are in $\widehat{R}$, we look at them modulo H. By Theorem 3.4.21, we know that the classes $\overline{a_i}$ of a_i modulo H are monomialisable in $\frac{\widehat{R}}{H}$ and that for every i, we have $\overline{a_1} \mid \overline{a_i}$.

Hence after a sequence of blow-ups, we have that $\overline{a_1}$ is a monomial $w = \prod_{i=1}^{t} x_i^{c_i}$ in x multiplied by a unit.

If we can show that a_1 divides all the $b_{i,j}$, then we could generate H in $\widehat{R}$ by $(y_2,..., y_{g+s})$.

Iterating, we could generate H in $\widehat{R}$ by g elements, and it would be over.

So let us show that we can do a sequence of blow-ups such that at the end a_1 divides all the $b_{i,j}$.

For every index $i \in \{1,\dots,g+s\}$, there exists $n_i \in \mathbb{N}_{>1}$ such that $y_i \in \widehat{\mathfrak{m}}^{n_{i-1}} \setminus \widehat{\mathfrak{m}}^{n_i}$ We set $N := \max_{i\in\{1,\dots,g+s\}} \{n_i\}$, and then for every $i \in \{1,\dots,g+s\}$, $y_i \notin \widehat{\mathfrak{m}}^N$.

We have a map $R \to \widehat{R}$ and we know that for every integer c, we have $\widehat{\mathfrak{m}}^c \cap R = \mathfrak{m}^c$. Hence we have an isomorphism $\frac{R}{\mathfrak{m}^c} \to \frac{\widehat{R}}{\widehat{\mathfrak{m}}^c}$.

So for all $i \in \{1,\dots,g+s\}$, there exists $z_i \in R$ whose class modulo $\mathfrak{m}^{N+2}$ is sent on y_i by this map. Hence z_i mod ($\mathfrak{m}^{N+2}$) = y_i. Increasing N if necessary, we may assume $\nu\left(\widehat{\mathfrak{m}}^N\right) > \nu(a_1)$.

More precisely $y_i = z_i + h_i + \zeta_i$ where $h_i \in (z_1,\dots,z_{g+s})^2$ and $\zeta_i \in (x_1,\dots,x_t)^N$.

After a sequence of blow-ups independent of $(z_1,\dots, z_{g+s})$, we may assume that w, and so a_1, divides all the ζ_i.

We do c_1 blow-ups of $(z_1,\dots, z_{g+s}, x_1)$. Each z_1 is transformed in a z_i' which is of the form $\frac{z_i}{x_1^{c_1}}$.

We do c_2 blow-ups of $(z_1',\dots, z_{g+s}', x_2)$. Each z_i' is transformed in a z_i'' which is of the form $\frac{z_i}{x_2^{c_2}} = \frac{z_i}{x_1^{c_1}x_2^{c_2}}$.

We iterate until doing c t blow-ups of

$$\left(z_1^{(t-1)},\dots,z_{g+s}^{(t-1)},x_t\right).$$

So we transformed z_i in $z_i^{(t)}$ which is of the form $\frac{z_i}{a_1}$.

Then a_1 divides all the $z_i^{(t)}$, and so all the $h_i^{(t)}$ and the $y_i^{(t)}$. The $b_{i,j}$ are elements of $\widehat{R}_H$, so after this sequence of blow-ups, since the strict transform of H is generated by the $y_i^{(t)}$, we have that a_1 divides all the $b_{i,j}$, and the proof is finished.

4.5 Conclusion

We know are going to give the principal results of this part. First we recall a fundamental result of Novacoski and Spivakovsky [42].

Theorem 4.5.1 Let S be a noetherian local ring. If the local uniformization Theorem is true for every valuation of rank 1 centered in S, then it is true for any valuation centered in S.

So we just have to consider valuations of rank 1.

Theorem 4.5.2 Let S be a noetherian equicharacteristic quasi excellent singular local ring of characteristic zero. We consider μ a valuation of rank 1 centered in S.

There exists a formal framed sequence

$$(S,u) \to \dots \to \left(S_i,u^{(i)}\right) \to \dots$$

such that for j big enough, S_j is regular and for every element s of S, there exists i such that in S_i, s is a monomial.

Proof. We consider $\widehat{S}$ the formal completion of S and H its implicit prime ideal. By Cohen structure Theorem, there exists an epimorphism Φ from a complete regular local ring R in $\widehat{S}$. We consider $\overline{H}$ the preimage of H in R. We extend now μ to a valuation ν centered in R by composition with a valuation centered in $\overline{H}$.

By Proposition 4.1.6 we know that $\widehat{S}_H$ is regular, and by Theorem 4.4.3 it is enough to show that $\frac{\widehat{S}}{H}$ is also regular.

We know that $\frac{\widehat{S}}{H} \simeq \frac{R}{\overline{H}}$, so we just have to regularize $\frac{R}{\overline{H}}$. We conclude withTheorem 4.3.15.

Now we prove the principal result of this part: the simultaneous embedded local uniformization for local noetherian quasi excellent equicharacteristic rings.

Theorem 4.5.3 Let R be a local noetherian quasi excellent complete regular ring and ν be a valuation centered in R.

Assume that ν is of rank 1 or 2 but composed of a valuation (f)-adic where f is an irreducible element of R. We assume car $(k_\nu) = 0$.

There exists a formal framed sequence

$$(R,u) \to \dots \to \left(R_l,u^{(l)}\right) \to \dots$$

such that for every element g of R, there exists i such that in R_i, g is a monomial.

Proof. We consider the ring $A=\frac{R}{(f)}$. The valuation ν is of rank 2 composed of valuation (f)-adic, so ν can be written $\mu \circ \theta$ where θ is the valuation (f)-adic.

So we have a valuation μ centered in A of rank 1. By Theorem 4.5.2, we can regularize A, and so there exists a local framed sequence $(R,u)\to\ldots\to(R_i,u^{(i)})$ such that in R_i, f is a monomial. In R_i, we also have that every element g of R can be written $g=\left(u_n^{(i)}\right)^a h$ where $u_n^{(i)}$ is the strict transform of f and h is not divisible by $u_n^{(i)}$. We apply another time Theorem 4.5.2 to construct a local framed sequence which monomialize h. This completes the proof.

Corollary 4.5.4 We keep the same notations and hypothesis as in the previous Theorem.

Then $\lim\limits_{\to} R_i$ is a valuation ring.

Remark 4.5.5 The restriction on the rank of the valuation was setted to give an autosuffcient proof. Otherwise, there exists a countable sequence of polynomials χ_i such that every ν-ideal P_β is generated by a subset of the χ_i. Assume the embedded local uniformization Theorem.

Then there exists a local (respectively formal) framed sequence $(R, u) \to \cdots \to (R_i, u^{(i)}) \to \ldots$ that has following properties:

(1) For i big enough, R_i is regular.

(2) For every finite set $\{f_1,\ldots,f_s\}\subseteq \mathfrak{m}$ there exists i such that in R_i, every f_j is a monomial and $f_1 \mid f_j$.

Then for every element g in R, there exists i such that in R_i, g is a monomial.

5. Index

Acknowledgments

The author is really grateful to her PHD advisor Mark Spivakovsky for all the helpful discussions.

References

[1] Shreeram Abhyankar. Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$. *Annals of Mathematics, Second Series*. 1956; 63(3): 491-526.

[2] Shreeram Abhyankar. *Resolution of Singularities of Embedded Algebraic Surfaces*. New York and London: Academic Press; 1966.

[3] S. Abhyankar. Reduction to multiplicity less than p in a p-cyclic extension of a two dimensional regular local ring (p = characteristic of the reside field). *Math. Annalen*. 1964; 154: 28-55.

[4] S. Abhyankar. An algorithm on polynomials in one indeterminate with coeffcients in a two dimensional regular local domain. *Annali di Matematica Pura ed Applicata*. 1966; 71: 25-60.

[5] S. Abhyankar. *Uniformization in a p-cyclic extension of a two dimensional regular local domain of residue field of characteristic p*. Festschrift zur Gedächtnisfeier für Karl Weierstrass 1815-1965. Köln und Opladen: Wissenschaftliche Abhandlungen des Landes Nordrhein-Westfalen 33 Westdeutscher Verlag; 1966. p.243-317.

[6] S. Abhyankar. Nonsplitting of valuations in extensions of two dimensional regular local domains. *Math. Annalen*. 1967; 170: 87-144.

[7] A. Benito, S. Encinas, O. Villamayor. Some natural properties of constructive resolution of singularities. *Asian J. Math*. 2011; 15(2): 141-192.

[8] B. Bennett. On the characteristic functions of a local ring. *Ann. of Math*. 1970; 91: 25-87.

[9] E. Bierstone, S. Da Silva, P. Milman F. Vera Pacheco. Desingularization by blowings-up avoiding simple normal crossings. *Proc. Amer. Math. Soc*. 2014; 142(12): 4099-4111.

[10] E. Bierstone, D. Grigoriev, P. Milman, J. Wlodarczyk. Effective hironaka resolution and its complexity. *Asian J. Math*. 2011; 15(2): 193-228.

[11] Edward Bierstone et Pierre D. Milman. Local resolution of singularities. *In real analytic and algebraic geometry* (Trento, 1988), volume 1420 of lecture notes in math. Berlin: Springer; 1990. p.42-64.

[12] E. Bierstone, P. Milman. A simple constructive proof of canonical resolution of singularities. *Effective Methods in Algebraic Geometry, Progress in Math*. 1991; 94: 11-30.

[13] E. Bierstone, P. Milman. Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant. *Invent. Math*. 1997; 28(2): 207-302.

[14] E. Bierstone, P. Milman. Resolution except for minimal singularities I. *Adv. Math*. 2012; 231(5): 3022-3053.

[15] E. Bierstone, P. Milman, M. Temkin. $\mathbb{Q}$-universal desingularization. *Asian J. Math*. 2011; 15(2): 229-249.

[16] Nicolas Bourbaki. Eléments de mathématiques : Algèbre commutative. *Masson*. 1985.

[17] A. Bravo, O.E. Villamayor. Strengthening the theorem of embedded desingularization. *Math. Res*. 2001; 8: 79-90 .

[18] A. Bravo, O. Villamayor. A strengthening of resolution of singularities in characteristic zero. *Proc. London. Math. Soc*. (3). 2003; 86(2): 327-357.

[19] E. Bierstone, F. Vera Pacheco. Resolution of singularities of pairs preserving semi-simple normal crossings. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM 107*. 2013; 1: 159-188.

[20] E. Bierstone, F. Vera Pacheco. Desingularization preserving stable simple normal crossings. *Israel J. Math*. 2015; 206(1): 233-280.

[21] Vincent Cossart et Olivier Piltant. Resolution of singularities of threefolds in positive characteristic. I. Reduction to local uniformization on Artin-Schreier and purely inseparable coverings. *Journal of Algebra*. 2008; 320(3): 1051-1082.

[22] Vincent Cossart et Olivier Piltant. Resolution of singularities of threefolds in positive characteristic. *II Journal of Algebra*. 2009; 321(7): 1836-1976

[23] Vincent Cossart et Olivier Piltant. Resolution of singularities of arithmetical threefolds II. Available from: arXiv: 1412.0868.

[24] Felipe Cano, Claude Roche et Mark Spivakovsky. Reduction of singularities of three-dimensional line foliations. R*evista de la Real Academia de Ciencias Ex-actas, Fisicas y Naturales. Serie A. Matematicas108*. 2014; 1: 221-258.

[25] V. Cossart, B. Schober. A strictly decreasing invariant for resolution of singularities in dimension two. 2014. Available from: arXiv: 1411.4452v2.

[26] S. D. Cutkosky. Resolution of singularities. *AMS, Providence, RI, Graduate Studies in Mathematics*. 2004; 63.

[27] S. D. Cutkosky. Resolution of singularities for 3-folds in positive characteristic. *American Journal of Mathematics*. 2009; 131(1): 59-127.

[28] Julie Decaup, Wael Mahboub et Mark Spivakovsky. Abstract key polynomials and comparison theorems with the key polynomials of mac lane-vaquié. Available from: arXiv: 611.06392.

[29] Santiago Encinas et Herwig Hauser. Strong resolution of singularities in characteristic zero. *Comment. Math. Helv*. 2002; 77(4): 821-845.

[30] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer; 1995.
[31] Santiago Encinas et Orlando Villamayor. A new proof of desingularization over fields of characteristic zero. *In Proceedings of the International Conference on Algebraic Geometry and Singularities (Sevilla, 2001)*. 2003; 19: 339-353.
[32] S. Encinas, O. Villamayor. Good points and constructive resolution of singularities. *Acta Mathematica*. 1998; 181: 109-158.
[33] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *I, II. Ann. of Math*. 1964; 79(2): 109-326.
[34] Hironaka, H. Desingularization of excellent surfaces. Notes by B. Bennett at the Conference on Algebraic Geometry, Bowdoin 1967. Reprinted in: Cossart, V., Giraud, J., Orbanz, U.: Resolution of surface singularities. *Lecture Notes in Math*. Springer; 1984. p.1101.
[35] Herrera Govantes, Mahboub, Olalla Acosta et Spivakovsky. Key polynomials for simple extensions of valued fields. Available from: arXiv: 1406.0657v3.
[36] Herrera Govantes, Olalla Acosta, Spivakovsky et Teissier. Extending a valuation centered in a local domain to the formal completion. *Proc. LMS105*. 2012; 3: 571-621.
[37] J. Lipman. Desingularization of two-dimensional schemes. *Ann. Math*. 1978; 107: 151-207.
[38] Matsumura. *Commutative Algebra*. Benjamin / Cummings Publishing Co. Reading, Mass; 1970.
[39] Saunders Mac Lane. A construction for absolute values in polynomial rings. *Transactions of the AMS*. 1936; 40: 363-395.
[40] Wael Mahboub. *Une construction explicite de polynômes-clefs pour des valuations de rang fini*. Thèse, Université Toulouse; 2013. p.3.
[41] Novacoski et Spivakovsky. Key polynomials and pseudo-convergent sequences. *Journal of Algebra*. 2018; 495: 199-219.
[42] Novacoski et Spivakovsky. Reduction of local uniformization to the case of rank one valuations for rings with zero divisors. *Valuation Theory in Interaction, EMS Series of Congress Reports.* European Mathematical Society. 2014. p.404-431.
[43] Teissier. Valuations, deformations and toric geometry. *Proceedings ofthe Saskatoon Conference and Workshop on valuation theory, Vol II, F-V*. Kuhlmann, S. Kuhlmann, M. Marshall, editors, Fields Institute Communi-cations. 2003; 33: 361-459.
[44] M. Temkin. Desingularization of quasi-excellent schemes of characteristic zero. *Adv. Math*. 2008; 219: 488-522.
[45] M. Temkin. Absolute desingularization in characteristic zero. Motivic integration and its interactions with model theory and non-archimedean geometry. *Volume II London Math. Soc. Lecture Note Ser*. 2011; 384: 213-250.
[46] M. Temkin. Functorial desingularization of quasi-excellent schemes in characteristic zero: the non-embedded case. *Duke Journal of Mathematics*. 2012; 161: 2208-2254.
[47] Michel Vaquié. Valuations and local uniformization. Singularity theory and its applications. *Advanced Studies in Pure Mathematics*. 2006; 43: 477-527.
[48] Michel Vaquié. Extension d'une valuation. *Trans. Amer. Math. Soc*. 2007; 359(7): 3439-3481.
[49] Michel Vaquié. Valuations, dans resolution of singularities. *Progr. in math*. 2000; 181. MR1748635 (2001i: 13005).
[50] Orlando Villamayor. Constructiveness of Hironaka's resolution. *Ann. Sci. École Norm. Sup.* (4). 1989; 22(1): 1-32.
[51] Robert J. Walker. Reduction of the singularities of an algebraic surface. *Annals of Mathematics, Second Series*. 1935; 36 (2): 336-365.
[52] Jaroslaw Wlodarczyk. Simple hironaka resolution in characteristic zero. *J. Amer. Math. Soc.* 2005; 18(4): 779-822.