

Valuations in algebraic field extensions

F. J. Herrera Govantes^{a,1,2}, M. A. Olalla Acosta^{a,1,2},
M. Spivakovsky^{b,2}

^a*Departamento de Álgebra, Facultad de Matemáticas, Universidad de Sevilla,
Apartado 1160, 41080 Sevilla, Spain*

^b*Laboratoire de Mathématiques E. Picard, UMR 5580 du CNRS, Université Paul
Sabatier, 31062 Toulouse cedex 9, France*

Abstract

Let $K \rightarrow L$ be an algebraic field extension and ν a valuation of K . The purpose of this paper is to describe the totality of extensions $\{\nu'\}$ of ν to L using a refined version of MacLane's key polynomials. In the basic case when L is a finite separable extension and $rk \nu = 1$, we give an explicit description of the limit key polynomials (which can be viewed as a generalization of the Artin–Schreier polynomials). We also give a realistic upper bound on the order type of the set of key polynomials. Namely, we show that if $char K = 0$ then the set of key polynomials has order type at most \mathbb{N} , while in the case $char K = p > 0$ this order type is bounded above by $([\log_p n] + 1)\omega$, where $n = [L : K]$. Our results provide a new point of view of the well known formula $\sum_{j=1}^s e_j f_j d_j = n$ and the notion of defect.

Key words: valuation, algebraic extension, key polynomial, Newton polygon

1 Introduction

All the rings in this paper will be commutative with 1.

This paper grew out of the authors' joint work [3] with B. Teissier, which is devoted to classifying the extensions $\hat{\nu}$ of a given valuation ν , centered in a

Email addresses: jherrera@algebra.us.es (F. J. Herrera Govantes),
miguelolalla@algebra.us.es (M. A. Olalla Acosta),
spivakov@picard.ups-tlse.fr (M. Spivakovsky).

¹ Partially supported by MTM2004-07203-C02-01 and FEDER

² Partially supported by HF2004-0117.

local domain R , to rings of the form $\frac{\hat{R}}{P}$, where \hat{R} is the formal completion of R and P is a prime ideal of \hat{R} such that $P \cap R = (0)$. In particular, in [3] we are interested in characterizing situations in which the valuation $\hat{\nu}$ (or one of its composed valuations) is unique. This naturally led us to the following

Question. Given a field extension $K \hookrightarrow L$ and a finite rank valuation ν of K , when is the extension of ν to L unique?

An obvious necessary condition for uniqueness is that L be algebraic over K .

In the present paper, we give an algorithm for describing the totality of extensions ν' of ν to L in terms of (a refined version of) MacLane's key polynomials, assuming L is algebraic over K . The case of purely inseparable extensions being trivial, we will assume that L is separable over K . Since an arbitrary algebraic field extension is a direct limit of finite extensions, we may assume that L is finite over K . In particular, L is simple by the primitive element theorem; write $L = K[x]$.

It is sufficient to solve the problem in the case $rk \nu = 1$: the case of a valuation of an arbitrary finite rank will then follow by induction on $rk \nu$. Indeed, if ν is the composition of two lower rank valuations ν_1 and ν_2 , then ν' is the composition of ν'_1 and ν'_2 , where ν'_1 is an extension of ν_1 to L and ν'_2 is a valuation of the residue field $k_{\nu'_1}$ of the valuation ring $R_{\nu'_1}$, extending ν_2 . Since the field $k_{\nu'_1}$ is an algebraic extension of k_{ν_1} ([13], Chapter VI, §11), it is enough to describe the extensions ν'_1 of ν_1 to L and the extensions of ν_2 to $k_{\nu'_1}$.

Two main techniques used in this paper are higher Newton polygons and a version of MacLane's key polynomials, similar to those considered by M. Vaquié ([9], [10], [11], and [12]), and reminiscent of related objects studied by Abhyankar and Moh (approximate roots [1], [2]) and T.C. Kuo ([4], [5]). When $L = K[x]$ is a simple extension of K , our algorithm is phrased in terms of the slopes of higher Newton polygons of the minimal polynomial f of x , the first one being the usual Newton polygon of x ; the algorithm amounts to successively constructing key polynomials of ν' . At each step of the algorithm there are finitely many possibilities to choose from. Namely, at the i -th step we have to choose a non-vertical side L of the i -th Newton polygon, consider the polynomial g over the graded algebra of ν determined by L and choose an irreducible factor of g . The number of steps itself can be countable (in fact, the number of steps has order type at most ω in characteristic zero and is bounded above by the ordinal $(\lceil \log_p n \rceil + 1)\omega$ in characteristic $p > 0$, where n is the degree of x over K and ω stands for the first infinite ordinal). Thus our algorithm can be viewed as providing an answer to the above question about uniqueness: the extension ν' is unique if and only if the choice of both L and g is unique at every step of the algorithm. A simple sufficient condition for the extension ν' to be unique is that the image $\text{in}_{\nu'} x$ in the graded algebra $G_{\nu'}$

have the same degree n over the graded algebra G_ν of ν as x does over K ; this condition is valid whether or not ν has rank 1 and has a very explicit characterization in terms of the (first) Newton polygon of f (namely, it is equivalent to saying that the Newton polygon has only one non-vertical side L and the polynomial over the graded algebra of ν , determined by L , is irreducible).

This paper is organized as follows. In §2 we summarize some basic definitions and results about algebras without zero divisors, graded by ordered semi-groups. §3–§7 are devoted to the main construction of the paper — that of key polynomials. Namely, we suppose given an extension ν' of ν to L . We define a well ordered set $\mathbf{Q} = \{Q_i\}_{i \in \Lambda}$ of key polynomials of ν' , which may be finite or countable. If $\text{char } K = 0$, the set Λ has order type at most ω ; if $\text{char } K = p > 0$ then Λ has order type strictly less than $(\lceil \log_p n \rceil + 1)\omega$, where n is the degree of x over K .

Notation. \mathbb{N} will denote the set of non-negative integers. For an element $l \in \Lambda$, we will denote by $l+1$ the immediate successor of l in Λ . The immediate predecessor, when it exists, will be denoted by $l-1$. For a positive integer t , $l+t$ will denote the immediate successor of $l+(t-1)$. For an element $l \in \Lambda$, the initial segment $\{Q_i\}_{i < l}$ of the set of key polynomials will be denoted by \mathbf{Q}_l . Throughout this paper, we let

$$p = 1 \quad \text{if } \text{char } K = 0 \quad (1)$$

$$= \text{char } K \quad \text{if } \text{char } K > 0. \quad (2)$$

In §3, we will fix an ordinal l and assume that the key polynomials \mathbf{Q}_{l+1} are already defined. We will define the notion of the l -th Newton polygon and the l -standard expansion of an element of $K[X]$ with respect to \mathbf{Q}_{l+1} . We will then define the next key polynomial Q_{l+1} . Roughly speaking, Q_{l+1} will be defined to be the lifting to L of the monic minimal polynomial, satisfied by $\text{in}_{\nu'} Q_l$ over the graded algebra $G_\nu[\text{in}_{\nu'} \mathbf{Q}_l]$.

In §4 we study the situation when the above recursive algorithm does not stop after finitely many steps, that is, when it gives rise to an infinite sequence $\{Q_{l+t}\}_{t \in \mathbb{N}}$ of key polynomials. We define a pair $(\delta_i(f), \epsilon_i(f))$ of basic positive integer invariants of the Newton polygon $\Delta_i(f)$ (where i runs over the set of all ordinals for which Q_i is defined). We prove that the pair $(\delta_i(f), \epsilon_i(f))$ is non-increasing in the lexicographical ordering. We deduce that if $\text{char } K = 0$ and $\text{rk } \nu = 1$ then iterating this construction at most ω times, we obtain a sequence $\{Q_i\}$ of key polynomials such that

$$\lim_{i \rightarrow \infty} \nu'(Q_i) = \infty. \quad (3)$$

In §5 we study the effect of the differential operators $\frac{1}{p^{b!}} \frac{\partial^b}{\partial x^{p^b}}$ on key polynomials and on f in the case the above invariant $\delta_i(f)$ stabilizes.

In §6 we use the results of §5 to show that $\delta_i(f)$ can stabilize only if it is of the form $\delta_i(f) = p^e$ for some $e \in \mathbb{N}$.

In §7 we assume that $\text{char } K = p > 0$ and consider an ordinal l which does not have an immediate predecessor. We assume that the key polynomials Q_i are already defined and then define the next key polynomial Q_l . We show that this case can occur at most $\lceil \log_p n \rceil$ times. A set of key polynomials is said to be **complete** if every ν' -ideal of R_ν is generated by products of powers of the Q_i (in other words, the valuation ν' is completely determined by the data $\{Q_i, \nu'(Q_i)\}$). In §8 we prove the main property of key polynomials $\{Q_i\}$, constructed in §§3–7: they form a complete set of key polynomials.

An algorithm for describing the totality of extensions ν' can be read off from this data. This algorithm will be described in §9. As a corollary, we deduce the well known formula $\sum_{j=1}^s e_j f_j d_j = n$, where $\{\nu_1, \dots, \nu_s\}$ is the set of all the extensions of ν to L , f_i is the index of the value group of ν viewed as a subgroup of the value group of ν_i , e_i is the degree of the residue field extension $k_\nu \hookrightarrow k_{\nu_i}$ and d_i is the defect of ν_i (a much more complete and detailed treatment of this formula can be found in M. Vaquié’s paper [12]).

In case $\text{char } K = p > 0$ our algorithm is less satisfactory than in characteristic zero in that at certain junctures it depends on non-constructive considerations such as a given subset of Γ having a maximum or an upper bound.

The idea of using key polynomials and Newton polygons in this context is not new. What we believe to be new in this paper is the explicit description of the totality of key polynomials and the definition and an explicit construction of limit key polynomials, rather intricate in the case of positive characteristic. In particular, we believe that our bound on the order type of the set of key polynomials required is new and is the first realistic bound of its kind.

We want to acknowledge the fact that there is some intersection of our results with those obtained independently and simultaneously by Michel Vaquié [12]. We thank him for helpful conversations and, in particular, for sharing his insights into the notion of defect.

2 Algebras graded by ordered semigroups.

Graded algebras associated to valuations will play a crucial role in this paper. In this section, we give some basic definitions and prove several easy results about graded algebras. Throughout this paper, a “graded algebra” will mean “an algebra without zero divisors, graded by an ordered semigroup”. As usual, for a graded algebra G , ord will denote the natural valuation of G , given by

the grading.

Definition 1 Let G be a graded algebra without zero divisors. The **saturation** of G , denoted by G^* , is the graded algebra

$$G^* = \left\{ \frac{g}{h} \mid g, h \in G, h \text{ homogeneous, } h \neq 0 \right\}.$$

The algebra G is said to be **saturated** if $G = G^*$.

Of course, we have $G^* = (G^*)^*$ for any graded algebra G , so G^* is always saturated.

The main example of saturated graded algebras appearing in this paper is the following.

Example 2 Let $\nu : K^* \rightarrow \Gamma$ be a valuation. Let (R_ν, M_ν, k_ν) denote the valuation ring of ν . For $\beta \in \Gamma$, consider the following R_ν -submodules of K :

$$\begin{aligned} \mathbf{P}_\beta &= \{x \in K^* \mid \nu(x) \geq \beta\} \cup \{0\}, \\ \mathbf{P}_{\beta+} &= \{x \in K^* \mid \nu(x) > \beta\} \cup \{0\}. \end{aligned}$$

We define

$$G_\nu = \bigoplus_{\beta \in \Gamma} \frac{\mathbf{P}_\beta}{\mathbf{P}_{\beta+}}.$$

The k_ν -algebra G_ν is an integral domain. For any element $x \in K^*$ with $\nu(x) = \beta$, the natural image of x in $\frac{\mathbf{P}_\beta}{\mathbf{P}_{\beta+}} \subset G_\nu$ is a homogeneous element of G_ν of degree β , which we will denote by $\text{in}_\nu x$. The algebra G_ν is saturated.

Let ν' be an extension of ν to L . For an element $\beta \in \Gamma$, let

$$\mathbf{P}'_\beta = \{y \in L \mid \nu'(y) \geq \beta\} \cup \{0\} \tag{4}$$

$$\mathbf{P}'_{\beta+} = \{y \in L \mid \nu'(y) > \beta\} \cup \{0\}. \tag{5}$$

Put $G_{\nu'} = \bigoplus_{\beta \in \Gamma} \frac{\mathbf{P}'_\beta}{\mathbf{P}'_{\beta+}}$. The extension $G_\nu \rightarrow G_{\nu'}$ of graded algebras is finite of degree bounded by $[L : K]$ (cf. [13], Chapter VI, §11). In the present paper, we do not use this result of Zariski–Samuel but rather give another proof of it.

Remark 3 Let G, G' be two graded algebras without zero divisors, with $G \subset G'$. Let x be a homogeneous element of G' , satisfying an algebraic dependence relation

$$a_0 x^\alpha + a_1 x^{\alpha-1} + \cdots + a_\alpha = 0 \tag{6}$$

over G (here $a_j \in G$ for $0 \leq j \leq \alpha$). Without loss of generality, we may assume that (6) is homogeneous (that is, the quantity $j \text{ ord } x + \text{ord } a_j$ is constant for $0 \leq j \leq \alpha$; this is achieved by replacing (6) by the sum of those

terms $a_j x^j$ for which the quantity $j \text{ ord } x + \text{ord } a_j$ is minimal), and that the integer α is the smallest possible. Dividing (6) by a_0 , we see that x satisfies an integral homogeneous relation over G^* of degree α and no algebraic relation of degree less than α . In other words, x is algebraic over G if and only if it is integral over G^* ; the conditions of being “algebraic over G^* ” and “integral over G^* ” are one and the same thing.

Let $G \subset G'$, let x be as above and let $G[x]$ denote the graded subalgebra of G' , generated by x over G . By the above Remark, we may assume that x satisfies a homogeneous integral relation

$$x^\alpha + a_1 x^{\alpha-1} + \cdots + a_\alpha = 0 \quad (7)$$

over G^* and no algebraic relations over G^* of degree less than α .

Proposition 4 *Every element of $(G[x])^*$ can be written uniquely as a polynomial in x with coefficients in G^* , of degree strictly less than α .*

PROOF. Let y be a homogeneous element of $G[x]$. Since x is integral over G^* , so is y . Let

$$y^\gamma + b_1 y^{\gamma-1} + \cdots + b_\gamma = 0 \quad (8)$$

with $b_j \in G^*$, be a homogeneous integral dependence relation of y over G^* , with $b_\gamma \neq 0$. By (8),

$$\frac{1}{y} = -\frac{1}{b_\gamma}(y^{\gamma-1} + b_1 y^{\gamma-2} + \cdots + b_{\gamma-1}).$$

Thus, for any $z \in G[x]$, we have

$$\frac{z}{y} \in G^*[x]. \quad (9)$$

Since y was an arbitrary homogeneous element of $G[x]$, we have proved that

$$(G[x])^* = G^*[x].$$

Now, for every element $y \in G^*[x]$ we can add a multiple of (7) to y so as to express y as a polynomial in x of degree less than α . Moreover, this expression is unique because x does not satisfy any algebraic relation over G^* of degree less than α . \square

The following result is an immediate consequence of definitions:

Proposition 5 *Let G_ν be the graded algebra associated to a valuation $\nu : K \rightarrow \Gamma$, as above. Consider a sum of the form $y = \sum_{i=1}^s y_i$, with $y_i \in K$. Let*

$\beta = \min_{1 \leq i \leq s} \nu(y_i)$ and

$$S = \{i \in \{1, \dots, n\} \mid \nu(y_i) = \beta\}.$$

The following two conditions are equivalent:

(1) $\nu(y) = \beta$

(2) $\sum_{i \in S} \text{in}_\nu y_i \neq 0.$

3 Key polynomials and higher Newton polygons

Let $K \hookrightarrow L$ be a finite separable field extension and $\nu : K^* \rightarrow \Gamma$ a valuation of K of real rank 1, where Γ is a \mathbb{Q} -divisible group and $\nu(K^*)$ is a subgroup of Γ . The extension L is simple by the primitive element theorem. Pick and fix a generator x of L over K ; write $L = K[x]$.

In this section we begin the main construction of the paper — that of key polynomials. Namely, we suppose given an extension ν' of ν to L .

Definition 6 A *complete set of key polynomials* for ν' is a well ordered collection $\mathbf{Q} = \{Q_i\}_{i \in \Lambda}$ of elements of L such that for each $\beta \in \Gamma$ the R_ν -module \mathbf{P}'_β is generated by all the products of the form $\prod_{j=1}^s Q_{i_j}^{\gamma_j}$ such that

$$\sum_{j=1}^s \gamma_j \nu'(Q_{i_j}) \geq \beta.$$

Note, in particular, that if \mathbf{Q} is a complete set of key polynomials then their images $\text{in}_{\nu'} Q_i \in G_{\nu'}$ induce a set of generators of $G_{\nu'}$ over G_ν . Furthermore, we want to make the set Λ as small as possible, that is, to minimize the order type of Λ .

Our algorithm for constructing all the possible extensions ν' of ν to L amounts to successively constructing key polynomials until the resulting set of key polynomials becomes complete for ν' .

We will fix an ordinal l and assume that the key polynomials \mathbf{Q}_{l+1} are already defined (the notation \mathbf{Q}_{l+1} is defined in the Introduction). We will then define the next key polynomial Q_{l+1} . If $Q_{l+1} = 0$, the algorithm stops. In §4 we will study what happens when this algorithm does not stop after finitely many steps and will show that if $\text{char } K = 0$ then iterating this construction at most ω times, we obtain a sequence $\{Q_i\}_{i \in \mathbb{N}}$ of elements of L such that

$$\lim_{i \rightarrow \infty} \nu'(Q_i) = \infty. \tag{10}$$

This will end the construction of key polynomials in characteristic zero; in §8 we will show that the resulting set of key polynomials is complete.

For each $l \in \Lambda$, we will define the notion of the l -th Newton polygon and the l -standard expansion of an element of $K[x]$ with respect to \mathbf{Q}_{l+1} . Roughly speaking, Q_{l+1} will be defined to be the lifting to L of the monic minimal polynomial, satisfied by $\text{in}_{\nu'} Q_l$ over the graded algebra $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_l]$. An algorithm for describing the totality of extensions ν' can be read off from this data. This algorithm will be described in §9.

Put $Q_1 = x$ and $\alpha_1 = 1$.

Let X be an independent variable and let $f = \sum_{i=0}^n a_i X^i$ denote the minimal polynomial of x over K . Making a change of variables of the form $x \rightarrow ax$ with $a \in K$, if necessary, we may assume that

$$\nu(a_n) < \nu(a_i) \text{ for } 0 \leq i < n; \quad (11)$$

furthermore, dividing f by a_n we may assume f to be monic with $\nu(a_i) > 0$ for $0 \leq i < n$. The condition (11) is needed to ensure that

$$\nu'(x) > 0 \quad (12)$$

for any extension ν' of ν to L . Let Γ_+ (resp. \mathbb{Q}_+) denote the semigroup of non-negative elements of Γ (resp. \mathbb{Q}).

Take an element $h = \sum_{i=0}^s d_i X^i \in K[X]$.

Definition 7 *The first **Newton polygon** of h with respect to ν is the convex hull $\Delta_1(h)$ of the set $\bigcup_{i=0}^s ((\nu(d_i), i) + (\Gamma_+ \oplus \mathbb{Q}_+))$ in $\Gamma \oplus \mathbb{Q}$.*

To an element $\beta_1 \in \Gamma_+$, we associate the following valuation ν_1 of $K(X)$: for a polynomial $h = \sum_{i=0}^s d_i X^i$, we put

$$\nu_1(h) = \min \{ \nu(d_i) + i\beta_1 \mid 0 \leq i \leq s \}.$$

In what follows, for an element $y \in L$, we will write informally $\nu_1(y)$ for $\nu_1(y(X))$, where $y(X)$ is the unique representative of y in $K[X]$ of degree strictly less than n . Similarly, for a polynomial $h \in K[X]$ we will sometimes write $\nu'(h)$ to mean $\nu'(h \bmod (f))$.

Consider an element $\beta_1 \in \Gamma_+$.

Definition 8 *We say that β_1 **determines a side** of $\Delta_1(h)$ if the following*

condition holds. Let

$$S_1(h, \beta_1) = \{i \in \{0, \dots, s\} \mid i\beta_1 + \nu(d_i) = \nu_1(h)\}.$$

We require that $\#S_1(h, \beta_1) \geq 2$.

Let $\beta_1 = \nu'(x)$. Then for any $h \in K[X]$ we have $\nu_1(h) \leq \nu'(h)$; furthermore, $\nu_1(f) < \infty = \nu'(f)$.

Proposition 9 Take a polynomial $h = \sum_{i=0}^s d_i X^i \in K[X]$ such that

$$\nu_1(h) < \nu'(h) \quad (13)$$

(for example, we may take $h = f$). Then

$$\sum_{i \in S(h, \beta_1)} \text{in}_\nu d_i \text{in}_{\nu'} x^i = 0. \quad (14)$$

PROOF. We have

$$\sum_{i \in S(h, \beta_1)} d_i x^i = h(x) - \sum_{i \in \{0, \dots, s\} \setminus S(h, \beta_1)} d_i x^i,$$

hence

$$\nu' \left(\sum_{i \in S(h, \beta_1)} d_i x^i \right) > \nu_1(h).$$

Then $\sum_{i \in S_1(h, \beta_1)} \text{in}_\nu d_i \text{in}_{\nu'} x^i = 0$ in $\frac{\mathbf{P}'_{\nu_1(h)}}{\mathbf{P}'_{\nu_1(h)}^+} \subset G_{\nu'}$ by Proposition 5. \square

Corollary 10 Take a polynomial $h \in K[X]$ such that $\nu_1(h) < \nu'(h)$. Then β_1 determines a side of $\Delta_1(h)$.

PROOF. If $S_1(h, \beta_1)$ consisted of a single element i , we would have

$$\text{in}_\nu d_i \text{in}_{\nu'} x^i \neq 0,$$

contradicting Proposition 9. \square

Letting $h = f$, we see from (11) that $\beta_1 > 0$ (geometrically, this corresponds to the fact that the side of $\Delta_1(f)$ determined by β_1 has strictly negative slope).

Notation. Let \bar{X} be a new variable. Take a polynomial h as above. We denote

$$\text{in}_1 h := \sum_{i \in S_1(h, \beta_1)} \text{in}_\nu d_i \bar{X}^i.$$

The polynomial $\text{in}_1 h$ is quasi-homogeneous in $G_\nu[\bar{X}]$, where the weight assigned to \bar{X} is β_1 . Let

$$\text{in}_1 h = v \prod_{j=1}^t g_j^{\gamma_j} \quad (15)$$

be the factorization of $\text{in}_1 h$ into irreducible factors in $G_\nu[\bar{X}]$. Here $v \in G_\nu$ and the g_j are monic polynomials in $G_\nu[\bar{X}]$ (to be precise, we first factor $\text{in}_1 h$ over the field of fractions of G_ν and then observe that all the factors are quasi-homogeneous and therefore lie in $G_\nu[\bar{X}]$).

Proposition 11 (1) *The element $\text{in}_{\nu'} x$ is integral over G_ν .*

(2) *The minimal polynomial of $\text{in}_{\nu'} x$ over G_ν is one of the irreducible factors g_j of (15).*

PROOF. Both (1) and (2) of the Proposition follow from the fact that $\text{in}_{\nu'} x$ is a root of the polynomial $\text{in}_1 h$ (Proposition 9). \square

Now take $h = f$. Renumbering the factors in (15), if necessary, we may assume that g_1 is the minimal polynomial of $\text{in}_{\nu'} x$ over G_ν . Let $\alpha_2 = \deg_{\bar{X}} g_1$. Write $g_1 = \sum_{i=0}^{\alpha_2} \bar{b}_i \bar{X}^i$, where $\bar{b}_{\alpha_2} = 1$. For each i , $0 \leq i \leq \alpha_2$, choose a representative b_i of \bar{b}_i in R_ν (that is, an element of R_ν such that $\text{in}_\nu b_i = \bar{b}_i$; in particular, we take $b_{\alpha_2} = 1$). Put $Q_2 = \sum_{i=0}^{\alpha_2} b_i x^i$.

Definition 12 *The elements Q_1 and Q_2 are called, respectively, **the first and second key polynomials** of ν' .*

Now, every element y of L can be written uniquely as a finite sum of the form

$$y = \sum_{\substack{0 \leq \gamma_1 < \alpha_2 \\ \gamma_1 + \gamma_2 \alpha_2 < n}} b_{\gamma_1 \gamma_2} Q_1^{\gamma_1} Q_2^{\gamma_2} \quad (16)$$

where $b_{\gamma_1 \gamma_2} \in K$ (this is proved by Euclidean division by the monic polynomial Q_2). The expression (16) is called **the second standard expansion of y** .

Now, take an ordinal number $l \geq 2$ which has an immediate predecessor; denote this ordinal by $l + 1$. If $\text{char } K = 0$, assume that $l \in \mathbb{N}$. Assume, inductively, that key polynomials \mathbf{Q}_{l+1} , and positive integers $\boldsymbol{\alpha}_{l+1} = \{\alpha_i\}_{i \leq l}$ are already constructed, and that all but finitely many of the α_i are equal to 1. We want to define the key polynomial Q_{l+1} .

We will use the following multi-index notation: $\gamma_{l+1} = \{\gamma_i\}_{i \leq l}$, where all but finitely many γ_i are equal to 0, $\mathbf{Q}_{l+1}^{\gamma_{l+1}} = \prod_{i \leq l} Q_i^{\gamma_i}$. Let $\beta_i = \nu'(Q_i)$.

Definition 13 An index $i < l$ is said to be ***l-essential*** if there exists a positive integer t such that either $i + t = l$ or $i + t < l$ and $\alpha_{i+t} > 1$; otherwise i is called ***l-inessential***.

In other words, i is *l-inessential* if and only if $i + \omega \leq l$ and $\alpha_{i+t} = 1$ for all $t \in \mathbb{N}$.

Notation. For $i < l$, let

$$i+ = i + 1 \quad \text{if } i \text{ is } l\text{-essential} \quad (17)$$

$$= i + \omega \quad \text{otherwise.} \quad (18)$$

Definition 14 A multiindex γ_{l+1} is said to be ***standard with respect to*** α_{l+1} if

$$0 \leq \gamma_i < \alpha_{i+} \text{ for } i \leq l, \quad (19)$$

$$\sum_{i \leq l} \gamma_i \prod_{j \leq i} \alpha_j \leq n, \quad (20)$$

and if i is *l-inessential* then the set $\{j < i+ \mid j+ = i+ \text{ and } \gamma_j \neq 0\}$ has cardinality at most one. An ***l-standard monomial in*** \mathbf{Q}_{l+1} (resp. an ***l-standard monomial in*** $in_{\nu'}\mathbf{Q}_{l+1}$) is a product of the form $c_{\gamma_{l+1}} \mathbf{Q}_{l+1}^{\gamma_{l+1}}$, (resp. $c_{\gamma_{l+1}} in_{\nu'} \mathbf{Q}_{l+1}^{\gamma_{l+1}}$) where $c_{\gamma_{l+1}} \in K$ (resp. $c_{\gamma_{l+1}} \in G_{\nu}$) and the multiindex γ_{l+1} is standard with respect to α_{l+1} .

Remark 15 In the case when i admits an immediate predecessor, the condition (19) amounts to saying that $\gamma_{i-1} < \alpha_i$.

Definition 16 An ***l-standard expansion not involving*** Q_l is a finite sum S of *l-standard monomials*, not involving Q_l , having the following property. Write $S = \sum_{\beta} S_{\beta}$, where β ranges over a certain finite subset of Γ_+ and

$$S_{\beta} = \sum_j d_{\beta j} \quad (21)$$

is a sum of standard monomials $d_{\beta j}$ of value β . We require that

$$\sum_j in_{\nu'} d_{\beta j} \neq 0 \quad (22)$$

for each β appearing in (21).

In the special case when $l \in \mathbb{N}$, (22) holds automatically for any sum of l -standard monomials not involving Q_l (this follows from Proposition 36 below by induction on l).

Proposition 17 *Let l be an ordinal and t a positive integer. Assume that the key polynomials \mathbf{Q}_{l+t+1} are defined and that $\alpha_l = \cdots = \alpha_{l+t} = 1$. Then any $(l+t)$ -standard expansion does not involve any Q_i with $l \leq i < l+t$. In particular, an l -standard expansion not involving Q_l is the same thing as an $(l+t)$ -standard expansion, not involving Q_{l+t} .*

PROOF. (19) implies that for $l \leq i \leq l+t$, Q_i cannot appear in an $(l+t)$ -standard expansion with a positive exponent. \square

We will frequently use this fact in the sequel without mentioning it explicitly.

Definition 18 *For an element $g \in K[X]$, an expression of the form $g = \sum_{j=0}^s c_j Q_l^j$, where each c_j is an l -standard expansion not involving Q_l , will be called an **l -standard expansion of g** . For a non-zero element $y \in L$, an **l -standard expansion of y** is an l -standard expansion of the representative $y(X)$ of y in $K[X]$ of degree strictly less than n .*

In what follows, we will be mostly interested in standard expansions of non-zero elements of L and of the polynomial $f(X)$.

Definition 19 *Let $\sum_{\gamma} \bar{c}_{\gamma} \text{in}_{\nu'} \mathbf{Q}_{l+1}^{\gamma}$ be an l -standard expansion, where $\bar{c}_{\gamma} \in G_{\nu'}$. A **lifting** of $\sum_{\gamma} \bar{c}_{\gamma} \text{in}_{\nu'} \mathbf{Q}_{l+1}^{\gamma}$ to L is an l -standard expansion $\sum_{\gamma} c_{\gamma} \mathbf{Q}_{l+1}^{\gamma}$, where c_{γ} is a representative of \bar{c}_{γ} in K .*

Definition 20 *Assume that $\text{char } K = p > 0$. An l -standard expansion $\sum_j c_j Q_l^j$, where each c_j is an l -standard expansion not involving Q_l , is said to be **weakly affine** if $c_j = 0$ whenever $j > 0$ and j is not of the form p^e for some $e \in \mathbb{N}$.*

Assume, inductively, that for each ordinal $i \leq l$, every element h of L and the polynomial $f(X)$ admit an i -standard expansion. Furthermore, assume that for each $i \leq l$, the i -th key polynomial Q_i admits an i -standard expansion, having the following additional properties.

If i has an immediate predecessor $i-1$ in Λ (such is always the case in

characteristic 0), the i -th standard expansion of Q_i has the form

$$Q_i = Q_{i-1}^{\alpha_i} + \sum_{j=0}^{\alpha_i-1} \left(\sum_{\gamma_{i-1}} c_{ji} \gamma_{i-1} \mathbf{Q}_{i-1}^{\gamma_{i-1}} \right) Q_{i-1}^j, \quad (23)$$

where:

- (1) each $c_{ji} \gamma_{i-1} \mathbf{Q}_{i-1}^{\gamma_{i-1}}$ is an $(i-1)$ -standard monomial, not involving Q_{i-1}
- (2) the quantity $j\beta_{i-1} + \sum_{q < i-1} \gamma_q \beta_q$ is constant for all the monomials

$$\left(c_{ji} \gamma_{i-1} \mathbf{Q}_{i-1}^{\gamma_{i-1}} \right) Q_{i-1}^j$$

appearing on the right hand side of (23)

- (3) the equation

$$\text{in}_{\nu'} Q_{i-1}^{\alpha_i} + \sum_{j=0}^{\alpha_i-1} \left(\sum_{\gamma_{i-1}} \text{in}_{\nu'} c_{ji} \gamma_{i-1} \text{in}_{\nu'} \mathbf{Q}_{i-1}^{\gamma_{i-1}} \right) \text{in}_{\nu'} Q_{i-1}^j = 0 \quad (24)$$

is the minimal algebraic relation satisfied by $\text{in}_{\nu'} Q_{i-1}$ over the subalgebra $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_{i-1}]^* \subset G_{\nu'}$.

Finally, if $\text{char } K = p > 0$ and i does not have an immediate predecessor in Λ then there exist an i -inessential index i_0 and a strictly positive integer e_i such that $i = i_0 +$ and $Q_i = \sum_{j=0}^{e_i} c_{ji_0} Q_{i_0}^{p^j}$ is a weakly affine monic i_0 -standard expansion of degree $\alpha_i = p^{e_i}$ in Q_{i_0} , where each c_{ji_0} is an i_0 -standard expansion not involving Q_{i_0} . Moreover, there exists a positive element $\bar{\beta}_i \in \Gamma$ such that

$$\bar{\beta}_i > \beta_q \quad \text{for all } q < i, \quad (25)$$

$$\beta_i \geq p^{e_i} \bar{\beta}_i \quad \text{and} \quad (26)$$

$$p^j \bar{\beta}_i + \nu(c_{i_0 j}) = p^{e_i} \bar{\beta}_i \quad \text{for } 0 \leq j \leq e_i. \quad (27)$$

If $i \in \mathbb{N}$, we assume, inductively, that the i -standard expansion is unique. If $\text{char } K > 0$, and $h = \sum_{j=0}^{s_i} d_{ji} Q_i^j$ is an i -standard expansion of h (where h is either $f(X)$ or an element of L), we assume that the elements $d_{ji} \in L$ are uniquely determined by h (strictly speaking, this does not mean that the i -standard expansion is unique: for example, if i is a limit ordinal, d_{ji} admits an i_0 -standard expansion for each $i_0 < i$ such that $i = i_0 +$, but there may be countably many choices of i_0 for which such an i_0 -standard expansion is an i_0 -standard expansion, not involving Q_{i-1} in the sense of Definition 16).

Proposition 21 (1) *The polynomial Q_i is monic in x ; we have*

$$\deg_x Q_i = \prod_{j \leq i} \alpha_j. \quad (28)$$

(2) *Let z be an i -standard expansion, not involving Q_i . Then*

$$\deg_x z < \deg_x Q_i. \quad (29)$$

PROOF. (28) and (29) are proved simultaneously by transfinite induction on i , using (23) and (19) repeatedly to calculate and bound the degree in x of any standard monomial (recall that by assumption all but finitely many of the α_i are equal to 1). \square

The rest of this section is devoted to the definition of Q_{l+1} . In what follows, we will sometimes not distinguish between the elements Q_i and their representatives in $K[X]$ in order to simplify the notation. When we do wish to make such a distinction, we will denote the representative of Q_i in $K[X]$ by $Q_i(X)$.

Write

$$f = \sum_{i=0}^{n_l} a_{jl} Q_l^j, \quad (30)$$

where each a_{jl} is a homogeneous l -standard expansion not involving Q_l , such that

$$\deg_x a_{jl} + j \prod_{q=1}^l \alpha_q \leq n,$$

with strict inequality for $j < n_l$.

Take any element $h \in K[X]$ and let $h = \sum_{i=0}^s d_i Q_l^i$ be an l -standard expansion of h , where each d_i is an l -standard expansion, not involving Q_l .

Definition 22 *The l -th Newton polygon of h with respect to ν is the convex hull $\Delta_l(h)$ of the set $\bigcup_{i=0}^s ((\nu'(d_i), i) + (\Gamma_+ \oplus \mathbb{Q}_+))$ in $\Gamma \oplus \mathbb{Q}$.*

To an element $\beta_l \in \Gamma_+$, we associate a valuation ν_l of $K(X)$ as follows. Given an l -standard expansion $h = \sum_{i=0}^s d_i Q_l^i$ as above, put $\nu_l(h) = \min_{0 \leq i \leq s} \{i\beta_l + \nu'(d_i)\}$. Note that even though in the case of positive characteristic the standard expansions of the elements d_i are not, in general, unique, the elements $d_i \in L$ themselves are unique by Euclidean division, so ν_l is well defined. That ν_l is, in fact, a valuation, rather than a pseudo-valuation, follows from the definition of standard expansion, particularly, from (22). We always have $\nu_l(h) \leq \nu'(h)$ and $\nu_l(f) < \infty = \nu'(f)$.

Notation. Let \bar{Q}_l be a new variable and let h be as above. We denote

$$S_l(h, \beta_l) := \{j \in \{0, \dots, s\} \mid j\beta_l + \nu'(d_j) = \nu_l(h)\}. \quad (31)$$

$$\text{in}_l h := \sum_{j \in S_l(h, \beta_l)} \text{in}_{\nu'} d_j \bar{Q}_l^j; \quad (32)$$

The polynomial $\text{in}_l h$ is quasi-homogeneous in $G[\text{in}_{\nu'} \mathbf{Q}_l, \bar{Q}_l]$, where the weight assigned to \bar{Q}_l is β_l .

Take a polynomial h such that

$$\nu_l(h) < \nu'(h) \quad (33)$$

(for example, we may take $h = f$).

Proposition 23 *We have $\sum_{j \in S_l(h, \beta_l)} \text{in}_{\nu'}(d_j Q_l^j) = 0$ in $\frac{\mathbf{P}'_{\nu_l(h)}}{\mathbf{P}'_{\nu_l(h)+}} \subset G_{\nu'}$.*

PROOF. This follows immediately from (33), the fact that

$$\sum_{j \in S_l(h, \beta_l)} d_j Q_l^j = h - \sum_{j \in S_l(h, \beta_l) \setminus \{0, \dots, s\}} d_j Q_l^j$$

and Proposition 5. \square

Let β_l be a non-negative element of Γ .

Definition 24 *We say that β_l **determines a side** of $\Delta_l(h)$ if $\#S_l(h, \beta_l) \geq 2$.*

Corollary 25 *Let $\beta_l = \nu'(Q_l)$. Then:*

(1) β_l determines a side of $\Delta_l(h)$.

(2)

$$\beta_l > \alpha_l \beta_{l-1} \quad \text{if } (l-1) \text{ exists} \quad (34)$$

$$\beta_l \geq p^{e_l} \bar{\beta}_l \quad \text{otherwise.} \quad (35)$$

PROOF. (1) Suppose not. Then the sum $0 = \sum_{j \in S_l(h, \beta_l)} \text{in}_{\nu'}(d_j Q_l^j)$ consists of only one term and hence cannot be 0. This contradicts Proposition 23; (1) is proved.

(2) follows immediately from (24) and (26). This completes the proof of Corollary 25. \square

Let

$$\text{in}_l h = v_l \prod_{j=1}^t g_{jl}^{\gamma_{jl}} \quad (36)$$

be the factorization of $\text{in}_l h$ into (monic) irreducible factors in $G_\nu[\text{in}_{\nu'} \mathbf{Q}_l][\bar{Q}_l]$ (to be precise, we first factor $\text{in}_l h$ over the field of fractions of $G_\nu[\text{in}_{\nu'} \mathbf{Q}_l]$ and then observe that all the factors are quasi-homogeneous and therefore lie in $G_\nu[\text{in}_{\nu'} \mathbf{Q}_l][\bar{Q}_l]$).

Corollary 26 *The element $\text{in}_{\nu'} Q_l$ is integral over G_ν . Its minimal polynomial over G_ν is one of the irreducible factors g_{jl} of (36).*

Put $h = f$ in (36). Renumbering the factors in (36), if necessary, we may assume that g_{1l} is the minimal polynomial of $\text{in}_{\nu'} Q_l$ over $G_\nu[\text{in}_{\nu'} \mathbf{Q}_l]$. Let

$$\alpha_{l+1} = \deg_{\bar{Q}_l} g_{1l}. \quad (37)$$

Write

$$g_{1l} = \bar{Q}_l^{\alpha_{l+1}} + \sum_{j=0}^{\alpha_{l+1}-1} \left(\sum_{\gamma_l} \bar{c}_{l+1,j} \gamma_l \text{in}_{\nu'} \mathbf{Q}_l^{\gamma_l} \right) \bar{Q}_l^j, \quad (38)$$

Define **the $(l+1)$ -st key polynomial** of ν' to be a lifting

$$Q_{l+1} = Q_l^{\alpha_{l+1}} + \sum_{j=0}^{\alpha_{l+1}-1} \left(\sum_{\gamma_l} c_{l+1,j} \gamma_l \mathbf{Q}_l^{\gamma_l} \right) Q_l^j \quad (39)$$

(38) to L . In the special case when $t = \alpha_{l+1} = 1$ in (36) and (37), some additional (and rather intricate) conditions must be imposed on the lifting (39). In fact, in this case we will define several consecutive key polynomials at the same time. We will now explain what these additional conditions are, after making one general remark:

Remark 27 *Since g_{1l} is an irreducible polynomial in \bar{Q}_l by definition, the key polynomial $Q_{l+1}(X)$ is also irreducible (for a non-trivial factorization of $Q_{l+1}(X)$ would give rise to a non-trivial factorization of g_{1l}).*

To define Q_{l+1} in the case $t = \alpha_{l+1} = 1$, we first introduce two numerical characters of the situation which will play a crucial role in the rest of the paper. Let $\delta_l(h) = \deg_{\bar{Q}_l} \text{in}_l h$.

Definition 28 *The vertex $(\nu' (a_{\delta_l(h),l}), \delta_l(h))$ of the Newton polygon $\Delta(h)$ is called the **pivotal vertex** of $\Delta(h)$.*

Let

$$\nu_l^+(h) = \min \left\{ \nu' \left(d_j Q_l^j \right) \mid \delta_l(h) < j \leq s \right\} \quad (40)$$

and

$$S'_l(h) = \left\{ j \in \{ \delta_l(h) + 1, \dots, s \} \mid \nu' \left(d_j Q_l^j \right) = \nu_l^+(h) \right\}.$$

Let $\epsilon_l(h) = \max S'_l(h)$ (if the set on the right hand side of (40) is empty, we adopt the convention that $\nu_l^+(h) = \epsilon_l(h) = \infty$). The quantities $\delta_l(h)$ and $\epsilon_l(h)$ are strictly positive by definition. It follows from definitions that $\epsilon_l(h) > \delta_l(h)$. Below, we will see that the pair $(\delta_l(h), \epsilon_l(h))$ is non-increasing with l (in the lexicographical ordering), that the equality $\delta_{l+1}(h) = \delta_l(h)$ imposes strong restrictions on $\text{in}_l h$ and that decreasing $(\delta_l(f), \epsilon_l(h))$ strictly ensures that the algorithm stops after a finite number of steps.

Assume that $t = \alpha_{l+1} = 1$ in (36) and (37). Let $\delta = \delta_l(f)$. We have $v_l = \text{in}_{\nu'} a_{\delta l}$ and (36) rewrites as

$$\text{in}_l f = \text{in}_{\nu'} a_{\delta l} g_{1l}^\delta. \quad (41)$$

In what follows, we will consider l -standard expansions of the form

$$Q' = Q_l + z_l + \dots + z_i, \quad (42)$$

where each z_j is a homogeneous l -standard expansion, not involving Q_l , such that

$$\beta_l = \nu'(z_l) < \nu'(z_{l+1}) < \dots < \nu'(z_i). \quad (43)$$

Remark 29 Note that by (29), we have $\deg_x z_q < \deg_x Q_l$ for all q .

Definition 30 Let Q' be as above. A **standard expansion** of f with respect to Q' is an expression of the form $f = \sum_{j=0}^{n_l} a'_j Q'^j$, where each a'_j is an l -standard expansion, not involving Q_l . The **Newton polygon** $\Delta(f, Q')$ of f with respect to Q' is the convex hull in $\Gamma_+ \oplus \mathbb{Q}_+$ of the set $\bigcup_{i=0}^{n_l} ((\nu'(a'_i), i) + (\Gamma_+ \oplus \mathbb{Q}_+))$.

Substituting $Q' - z_l - \dots - z_i$ for Q_l in (30), writing

$$\sum_{i=0}^{n_l} a_{il} (Q' - z_l - \dots - z_i)^i = \sum_{j=0}^{n_l} a'_j Q'^j,$$

and using (43), we see that $\nu'(a'_\delta) = \nu'(a_{\delta l})$ and that $(\nu'(a_{\delta l}), \delta)$ is a vertex of $\Delta(f, Q')$ (though it might not be the pivotal one).

Definition 31 The **characteristic side** of $\Delta(f, Q')$ is the side $A(f, Q')$ whose upper endpoint is $(\nu'(a_{\delta l}), \delta)$.

Let $\beta(Q')$ denote the element of Γ_+ which determines the side $A(f, Q')$.

For $l \leq j \leq i$, put $Q'_j = Q_l + z_l + \cdots + z_{j-1}$, let $\Delta(f, Q'_j)$ be the corresponding Newton polygon and $A(f, Q'_j)$ the characteristic side of $\Delta(f, Q'_j)$.

Let T denote the set of all the l -standard expansions of the form (42), where each z_j is a homogeneous l -standard expansion, not involving Q_l , such that the inequalities (43) hold, $\nu'(z_i) < \beta(Q')$ and

$$\text{in}_{A(f, Q'_j)} f = \text{in}_{\nu'} a'_\delta \left(\bar{Q} + \text{in}_{\nu'} z_j \right)^\delta \quad (44)$$

whenever $l \leq j < i$.

We impose the following partial ordering on T . Given an element $Q' = Q_l + z_l + \cdots + z_i \in T$ with $i > l$, we declare its immediate predecessor in T to be the element $Q_l + z_l + \cdots + z_{i-1}$. By definition, our partial ordering is the coarsest one among those in which $Q_l + z_l + \cdots + z_{i-1}$ precedes $Q_l + z_l + \cdots + z_i$ for all the elements Q' as above.

Take an element $Q' := Q_l + z_l + \cdots + z_i \in T$. Let $A' = A(f, Q')$.

Remark 32 *Assume that*

$$\text{in}_{A'} f = \text{in}_{\nu'} a'_\delta (\bar{Q} + \text{in}_{\nu'} z')^\delta$$

for some l -standard expansion z' , not involving Q_l . Then

$$\text{in}_{\nu'}(Q') = -\text{in}_{\nu'} z'; \quad (45)$$

in particular, $\nu'(Q') = \nu'(z')$. In other words, $\nu'(Q')$, $\nu'(z')$ and the slope of the side A' are all equivalent sets of data. In the sequel, we prefer to talk about $\nu'(z')$ rather than $\nu'(Q')$ for the following reason. In §9, rather than working with a fixed valuation ν' , we will use the same algorithm to construct all the possible extensions ν' . Therefore it will be important to describe the next step in the algorithm using only the data known at this stage of the construction, rather than the entire data of ν' itself. Since we are assuming that the key polynomials \mathbf{Q}_l and their values are already known, we may consider $\nu'(z')$ as being known as well.

Notation. In what follows, for an element $b \in L$, $b(X)$ will denote the representative of b in $K[X]$ of degree less than n .

Proposition 33 *Consider an l -standard expansion w of the form $w_l + w_{l+1} + \cdots + w_i$, where w_l, \dots, w_i are homogeneous l -standard expansions and w_l is an l -standard expansions, not involving Q_l , such that $\beta_l = \nu'(w_l) < \cdots < \nu'(w_i)$. Fix an element $\beta \in \Gamma_+$,*

$$\beta > \beta_l. \quad (46)$$

Then $w(X)$ can be written in the form

$$w(X) = w_l(X) + \tilde{w}_{l+1}(X) + \cdots + \tilde{w}_j(X) + w^\dagger(X)((Q_l(X) + w(X))) + \psi_\beta(X), \quad (47)$$

where ψ_β is an l -standard expansion, $w_l, \tilde{w}_{l+1}, \dots, \tilde{w}_j$ are homogeneous l -standard expansions, not involving Q_l , such that

$$\beta_l = \nu'(w_l) < \nu'(\tilde{w}_{l+1}) < \cdots < \nu'(\tilde{w}_j), \quad (48)$$

$$\nu_l(\psi_\beta(X)) \geq \beta, \quad \text{and} \quad (49)$$

$$\nu_l(w^\dagger(X)) > 0 \quad (50)$$

PROOF. Let $\mu = \nu_l(w_{l+1})$. By definitions, the Proposition is true for $\beta = \mu$. Assume that the Proposition holds for a certain β . We will show that it holds for β replaced by $\beta + \mu$, and that will complete the proof. Consider an expression (47) satisfying (48)–(50). Write ψ_β in the form $\psi_\beta = \psi_{\beta+\mu} + \tilde{\psi}$, where $\nu_l(\psi_{\beta+\mu}(X)) \geq \beta + \mu$ and $\tilde{\psi}$ consists of monomials of value greater than or equal to β but strictly less than $\beta + \mu$. By assumptions and Remark 29, $\deg_X w_l(X) < \deg_X Q_l(X)$. Divide the polynomial $\tilde{\psi}(X)$ by $Q_l(X) + w_l(X)$:

$$\tilde{\psi}(X) = q(X)(Q_l(X) + w_l(X)) + r(X),$$

where $\deg_X r(X) < \deg_X Q_l(X)$. Then

$$\tilde{\psi}(X) = q(X)(Q_l(X) + w(X)) + r(X) + \tilde{\psi}_{\beta+\mu}(X),$$

where $\nu_l(\tilde{\psi}_{\beta+\mu}) \geq \beta + \mu$. Absorb the quotient $q(X)$ into $w^\dagger(X)$ and $\tilde{\psi}_{\beta+\mu}$ into $\psi_{\beta+\mu}$. Let

$$r(X) = \tilde{w}_{j+1}(X) + \cdots + \tilde{w}_j(X) \quad (51)$$

be the l -standard expansion of $r(X)$. Since the remainder $r(X)$ is of degree strictly less than $\deg_X Q_l(X)$, its standard expansion (51) does not involve any monomials divisible by $Q_l(X)$. We obtain the desired decomposition

$$\begin{aligned} w(X) &= w_l(X) + \tilde{w}_{l+1}(X) + \cdots + \tilde{w}_j(X) + \\ &\quad + (w^\dagger(X) + q(X))(Q_l(X) + w(X)) + \psi_{\beta+\mu}(X). \end{aligned}$$

Condition (46) implies that $\nu_l(w^\dagger(X) + q(X)) > 0$, as desired. \square

Proposition 34 Consider two elements $Q' := Q_l + z'_l + \cdots + z'_{i'}$, $Q'' := Q_l + z''_l + \cdots + z''_{i''} \in T$. Let $\Delta'(f)$ and $\Delta''(f)$ be the corresponding Newton polyhedra and A' (resp. A'') the characteristic side of $\Delta'(f)$ (resp. $\Delta''(f)$). Assume that

$$in_{A'} f = in_{\nu'} a_{\delta l} (\bar{Q} + in_{\nu'} w')^\delta \quad \text{and} \quad (52)$$

$$in_{A''} f = in_{\nu'} a_{\delta l} (\bar{Q} + in_{\nu'} w'')^\delta \quad (53)$$

for some l -standard expansions w' and w'' , not involving Q_l . Furthermore, assume that

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

Then there exists a third element

$$Q''' := Q_l + z_i''' + \cdots + z_{i'''}''' \in T, \quad Q''' > Q',$$

having the following property. Let $\Delta'''(f)$ denote the Newton polygon determined by Q''' and A''' the characteristic side of $\Delta'''(f)$. Then $A''' = A''$ and $\text{in}_{A'''} f = \text{in}_{A''} f$.

PROOF. Let $w = Q'' - Q'$ and fix an element $\beta \in \Gamma$, $\beta > \nu'(Q'')$. Apply Proposition 33 with Q_l replaced by Q' . The hypotheses of Proposition 33 are satisfied because

$$\nu'(w') = \nu'(Q') < \nu'(Q'') = \nu'(w'')$$

and $\text{in}_{\nu'} w' = -\text{in}_{\nu'} Q'$ by assumptions, hence $\text{in}_{\nu'} w = -\text{in}_{\nu'} Q' = \text{in}_{\nu'} w'$, in particular, $\text{in}_{\nu'} w$ does not involve $\text{in}_{\nu'} Q_l$. By Proposition 33 we can write

$$w = z_{i'+1} + \cdots + z_{i'''} + w^\dagger Q'' + \psi_\beta \quad (54)$$

such that

$$\nu_l(w^\dagger) > 0, \quad (55)$$

$$\nu_l(\psi_\beta) > \nu'(Q'') \quad (56)$$

and $z_{i'+1}, \dots, z_{i'''}'$ are l -standard expansions, not involving Q_l . Put

$$Q''' = Q_l + z_l' + \cdots + z_{i'}' + z_{i'+1} + \cdots + z_{i'''}.$$

Then (54), (55) and (56) show that

$$\nu'(Q''') = \nu'(Q'')$$

and

$$\text{in}_{\nu'} Q''' = \text{in}_{\nu'} Q'';$$

the Proposition follows immediately. \square

To define Q_{l+1} in the special case when

$$t = \alpha_{l+1} = 1 \quad (57)$$

in (36) and (37), first assume that $\text{char } K = 0$. Equations (41) and (57) imply that $a_{\delta-1,l} \neq 0$ and

$$g_{1l} = \bar{Q}_l + \text{in}_{\nu'} \frac{a_{\delta-1,l}}{\delta a_{\delta l}}. \quad (58)$$

Consider the l -standard expansion of $\frac{a_{\delta-1,l}}{\delta a_{\delta l}}$ and write it in the form

$$\frac{a_{\delta-1,l}}{\delta a_{\delta l}} = z_l + z_{l+1} + \cdots + z_{l_1-1} + \phi + w, \quad (59)$$

where l_1 is an integer strictly greater than l , each z_i is a homogeneous l -standard expansion, not involving Q_l , such that

$$\nu' \left(\frac{a_{\delta-1,l}}{\delta a_{\delta l}} \right) = \nu'(z_l) < \nu'(z_{l+1}) < \cdots < \nu'(z_{l_1-1}) < \nu_l^+(h) - \nu_l(h) + \beta_l, \quad (60)$$

ϕ is a sum of standard monomials of value greater than or equal to $\nu_l^+(h) - \nu_l(h) + \beta_l$ and w is divisible by $Q_l + \frac{a_{\delta-1,l}}{\delta a_{\delta l}}$ (such an expression (59) exists by Proposition 33). Let

$$s = \max\{i \mid l \leq i \leq l_1 \text{ and } Q_l + z_l + \cdots + z_{i-1} \in T\}. \quad (61)$$

For $l \leq i \leq s$, define $Q_i = Q_l + z_l + \cdots + z_{i-1}$.

Next, assume $\text{char } K = p > 0$. Two cases are possible:

Case 1. The set T contains a maximal element. Let $z = z_l + z_{l+1} + \cdots + z_{s-1}$ be this maximal element, where each z_i is a homogeneous l -standard expansion, not involving Q_l , and s is an ordinal of the form $s = l + t$, $t \in \mathbb{N}$. Define

$$Q_i = Q_l + z_l + \cdots + z_{i-1} \quad \text{for } l + 1 \leq i \leq s.$$

Case 2. The set T does not contain a maximal element. Let

$$\bar{\beta} = \sup\{\nu(Q') \mid Q' \in T\}$$

(here we allow the possibility $\bar{\beta} = \infty$). In this case, Proposition 34 (together with Remark 32) shows that there exists an infinite sequence z_l, z_{l+1}, \dots of homogeneous l -standard expansions, not involving Q_l , such that for each $t \in \mathbb{N}$ we have

$$Q_l + z_l + \cdots + z_{l+t} \in T \quad (62)$$

and $\lim_{t \rightarrow \infty} \nu(Q_l + z_l + \cdots + z_{l+t}) = \bar{\beta}$; pick and fix one such sequence. Define

$$Q_{l+t} = Q_l + z_l + z_{l+1} + \cdots + z_{l+t-1} \quad \text{for } t \in \mathbb{N}.$$

Note that (62), (44) and Remark 32 imply that the sequence $\{\nu(Q_l + z_l + \cdots + z_{l+t})\}_{t \in \mathbb{N}}$ is strictly increasing.

For future reference, it will be convenient to distinguish two subcases of Case 2:

Case 2a. $\bar{\beta} = \infty$, that is, the sequence $\{\beta_{l+t}\}_{t \in \mathbb{N}}$ is unbounded in Γ . In this case, the definition of the key polynomials Q_i is complete. In §4, we will use

differential operators to show that in this case δ is necessarily of the form p^e for some $e \in \mathbb{N}$.

Case 2b. The set $\{\nu(Q') \mid Q' \in T\}$ has a least upper bound $\bar{\beta} < \infty$ (but no maximum) in Γ . In this case, we must continue the construction and define $Q_{l+\omega}, Q_{l+\omega+1}$, etc. This will be accomplished in §7.

Remark 35 *Note that the definition of Q_{l+1} depends only on the key polynomials \mathbf{Q}_{l+1} defined so far, their values β_{l+1} and the resulting Newton polygons $\Delta_i(f)$, $i \leq l$. This will be important in §9 where we will use the Q_i to construct all the possible extensions ν' .*

Proposition 36 *Let y be an element of L , represented by a polynomial in $K[X]$ of degree strictly less than $\deg_x Q_{l+1} = \prod_{i=0}^{l+1} \alpha_i$. Then $\nu'(y) = \nu_l(y)$.*

PROOF. Let $y = \sum_{j=0}^s c_j Q_l^j$ be an l -standard expansion of y , where each c_j is an l -standard expansion not involving Q_l . Let

$$S = \left\{ j \in \{0, \dots, s\} \mid \nu'(c_j Q_l^j) = \nu_l(y) \right\}.$$

Let $\bar{c}_j := \text{in}_{\nu'} c_j$. Since the degree of $\text{in}_{\nu'} Q_l$ over $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_l]^*$ is α_{l+1} , we see, using the assumption on $\deg_x y$, that $\sum_{j=0}^s \bar{c}_j \text{in}_{\nu'} Q_l^j \neq 0$ in $G_{\nu'}$. The result now follows from Proposition 5. \square

Now, take any polynomial $h \in K[X]$. The $(l+1)$ -st standard expansion $h = \sum_{j=0}^s c_j Q_{l+1}^j$ is constructed from the l -th one by Euclidean division by the polynomial Q_{l+1} . Condition $\nu_l(c_j) = \nu'(c_j)$ required in the definition of standard expansion (cf. Definition 18 and (22)) follows immediately from the above Proposition and Proposition 21 (2).

By induction on t , this defines key polynomials Q_{l+t} for $t \in \mathbb{N}$. If for some $t \in \mathbb{N}$ we obtain $Q_{l+t} = 0$ in L , stop. In §8, we will show that \mathbf{Q}_{l+t} is a complete set of key polynomials for ν' , and, in particular, that the data \mathbf{Q}_{l+t} and β_{l+t} completely determines ν' .

If $Q_{l+t} \neq 0$ for all $t \in \mathbb{N}$, we obtain an infinite sequence $\{Q_{l+t}\}$ of key polynomials. If

$$\text{char } K = 0 \quad \text{or} \tag{63}$$

$$\lim_{t \rightarrow \infty} \beta_{l+t} = \infty, \tag{64}$$

stop (in fact, in the next section we will see that (63) implies (64) and also that in this case δ has the form p^e , $e \in \mathbb{N}$). In §8, we will show that the $\{Q_{l+t}\}$ is a complete set of key polynomials for ν' . If $\text{char} K = p > 0$ and $\lim_{t \rightarrow \infty} \beta_{l+t} < \infty$, the construction of the next key polynomial $Q_{l+\omega}$ will be described in §7.

In the next three sections, we analyze the case when infinitely many such iterations give rise to an infinite sequence $\{Q_{l+i}\}$ of key polynomials.

4 Infinite sequences of key polynomials.

Keep the assumption $rk \nu = 1$. In this section, we analyze the case when iterating the recursive construction of the previous section produces an infinite sequence $\{Q_{l+i}\}_{t \in \mathbb{N}}$. If $\text{char} K = 0$, we show that if the above algorithm produces an infinite sequence of key polynomials then

$$\lim_{i \rightarrow \infty} \beta_i = \infty. \quad (65)$$

In §8 we will show that (65) implies that the valuation ν' is completely determined by the resulting data $\{Q_i\}$ and $\{\beta_i\}$, that is, that the resulting set $\{Q_i\}$ is, indeed, a complete set of key polynomials. The case when $\text{char} K = p > 0$ and the values β_i are bounded above in Γ is studied in detail in §7.

Take an ordinal i such that Q_i and Q_{i+1} are defined. Take a polynomial h such that $\nu_i(h) < \nu'(h)$ (for example, we may take $h = f$). Consider the i -th Newton polygon of h . Let $S_i(h, \beta_i)$ be as in (31). Recall the definition of $\delta_i(h)$:

$$\delta_i(h) := \max\{S_i(h, \beta_i)\}. \quad (66)$$

Let $h = \sum_{j=0}^{s_i} d_{ji} Q_i^j$ denote the i -standard expansion of h , where each d_{ji} is an l -standard expansion, not involving Q_l . Recall the definition (40) of $\nu_i^+(h)$. The next Proposition shows that the pair $(\delta_i(h), \epsilon_i(h))$ is non-increasing with i (in the lexicographical ordering) and that the equality $\delta_{i+1}(h) = \delta_i(h)$ imposes strong restrictions on $\text{in}_i h$.

Proposition 37 (1) *We have*

$$\alpha_{i+1} \delta_{i+1}(h) \leq \delta_i(h). \quad (67)$$

(2) *If $\delta_{i+1}(h) = \delta_i(h)$ then*

$$\epsilon_{i+1}(h) \leq \epsilon_i(h), \quad (68)$$

$$\text{in}_i h = \text{in}_{\nu'} d_{\delta_i(h)i} \left(\bar{Q}_i + \text{in}_{\nu'} z_i \right)^{\delta_i(h)}, \quad (69)$$

where z_i is some i -standard expansion not involving Q_i , and $in_{i+1}h$ contains a monomial of the form $in_{\nu'}d_{\delta_i(h)i}\bar{Q}_{i+1}^{\delta_i(h)}$; in particular,

$$in_{\nu'}d_{\delta_i(h)i} = in_{\nu'}d_{\delta_i(h),i+1} \quad (70)$$

(3) If

$$(\delta_i(h), \epsilon_i(h)) = (\delta_{i+1}(h), \epsilon_{i+1}(h)) \quad (71)$$

then

$$in_{\nu'}d_{\epsilon_i(h)i} = in_{\nu'}d_{\epsilon_i(h),i+1}. \quad (72)$$

PROOF. We start with three Lemmas. First, consider the $(i+1)$ -standard expansion of h :

$$h = \sum_{j=0}^s d_{j,i+1}Q_{i+1}^j, \quad (73)$$

where the $d_{j,i+1}$ are $(i+1)$ -standard expansions, not involving Q_{i+1} .

Lemma 38 (1) *We have*

$$\nu_i(h) = \min_{0 \leq j \leq s} \nu_i(d_{j,i+1}Q_{i+1}^j) = \min_{0 \leq j \leq s} \{\nu'(d_{j,i+1}) + j\alpha_{i+1}\beta_i\}.$$

(2) *Let*

$$S_{i,i+1} = \{j \in \{0, \dots, s\} \mid \nu_i(d_{j,i+1}Q_{i+1}^j) = \nu_i(h)\}$$

and $j_0 = \max S_{i,i+1}$. Then $\delta_i(h) = \alpha_{i+1}j_0 + \deg_{Q_i} d_{j_0,i+1}$.

PROOF. (1) Provisionally, let

$$\mu = \min_{0 \leq j \leq s} \nu_i(d_{j,i+1}Q_{i+1}^j) = \min_{0 \leq j \leq s} \{\nu'(d_{j,i+1}) + j\alpha_{i+1}\beta_i\},$$

$$S'_{i,i+1} = \{j \in \{0, \dots, s\} \mid \nu_i(d_{j,i+1}Q_{i+1}^j) = \mu\},$$

$j' = \max S'_{i,i+1}$ and $\delta' = \alpha_{i+1}j' + \deg_{Q_i} d_{j',i+1}$. We want to show that $\mu = \nu_i(h)$, $S'_{i,i+1} = S_{i,i+1}$, $j' = j_0$ and $\delta_i(h) = \delta'$.

Let $\bar{h} = \sum_{j \in S'(i,i+1)} d_{j,i+1}Q_{i+1}^j$. Then $\nu_i(h - \bar{h}) > \mu$ by definition, so to prove that $\nu_i(h) = \mu$ it is sufficient to prove that $\nu_i(\bar{h}) = \mu$.

Now, $\deg_x \bar{h} = \deg_x d_{\delta',i+1}Q_i^{\delta'}$ by definition of δ' and Proposition 21 (2). Hence the i -standard expansion of \bar{h} contains the monomial $d_{\delta',i+1}Q_i^{\alpha_{i+1}\delta'}$ and all the other monomials have degree in x strictly smaller than $\deg_x d_{\delta',i+1}Q_i^{\alpha_{i+1}\delta'}$. Thus $\nu_i(\bar{h}) \leq \nu_i(d_{\delta',i+1}Q_i^{\alpha_{i+1}\delta'}) = \mu$, so $\nu_i(h) \leq \mu$. The opposite inequality is trivial and (1) is proved. (2) follows immediately from this. \square

Lemma 39 Consider two terms of the form dQ_{i+1}^j and $d'Q_{i+1}^{j'}$ (where $j, j' \in \mathbb{N}$ and d and d' are i -standard expansions not involving Q_i). Assume that

$$\nu_i(dQ_{i+1}^j) \leq \nu_i(d'Q_{i+1}^{j'}) \quad (74)$$

and

$$\nu'(dQ_{i+1}^j) \geq \nu'(d'Q_{i+1}^{j'}). \quad (75)$$

Then $j \geq j'$. If at least one of the inequalities (74),(75) is strict then $j > j'$.

PROOF. Subtract (74) from (75) and use the definition of ν_i and the facts that $\nu_i(Q_{i+1}) = \beta_i$ and $\alpha_{i+1}\beta_i < \beta_{i+1}$. \square

In the notation of Lemma 38, let $\theta_{i+1}(h) = \min S_{i,i+1}$.

Definition 40 The vertex $(\nu(d_{\theta_{i+1}(h),i+1}), \theta_{i+1}(h))$ is called the **characteristic vertex** of $\Delta_{i+1}(h)$. By convention, $\theta_1(f) = n$, so the characteristic vertex of $\Delta_1(f)$ is also defined.

The notion of characteristic vertex will be needed in §9 when we discuss the totality of the extensions ν' of ν and the formula $\sum_j f_j e_j d_j = n$. It is important that the characteristic vertex of $\Delta_{i+1}(f)$ is determined by \mathbf{Q}_{i+2} and β_{i+1} : it does not depend on β_{i+1} .

Let

$$\text{in}_i h = \text{in}_{\nu'} d_{\delta_i} \prod_{j=1}^t g_{j_i}^{\gamma_{j_i}} \quad (76)$$

be the factorization of $\text{in}_i h$ into (monic) irreducible factors in $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_i] [\bar{Q}_i]$, where g_{1_i} is the minimal polynomial of $\text{in}_{\nu'} Q_i$ over $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_i]$.

Lemma 41 We have

$$\gamma_{1_i} = \theta_{i+1}(h) \quad (77)$$

(in particular, $d_{\gamma_{1_i},i+1} \neq 0$) and

$$\text{in}_{\nu'} d_{\theta_{i+1}(h),i+1} = \text{in}_{\nu'} d_{\delta_i} \prod_{j=2}^t g_{j_i}^{\gamma_{j_i}} (\text{in}_{\nu'} Q_i). \quad (78)$$

PROOF. Write

$$h = \sum_{q \in S_{i,i+1}} d_{q,i+1} Q_{i+1}^q + \sum_{q \in \{0, \dots, n_{i+1}\} \setminus S_{i,i+1}} d_{q,i+1} Q_{i+1}^q.$$

By Lemma 38,

$$\text{in}_i h = \sum_{q \in \mathcal{S}_{i,i+1}} \text{in}_i d_{q,i+1} \text{in}_i Q_{i+1}^q. \quad (79)$$

By definition of $\theta_{i+1}(h)$, $\text{in}_i Q_{i+1}^{\theta_{i+1}(h)}$ is the highest power of $\text{in}_i Q_{i+1}$ dividing $\sum_{q \in \mathcal{S}_{i,i+1}} \text{in}_i d_{q,i+1} \text{in}_i Q_{i+1}^q$. Also by definition, we have

$$\text{in}_i Q_{i+1} = g_{1i}. \quad (80)$$

Now (77) follows from (79). Also from (79), we see that $\text{in}_{\nu'} d_{\theta_{i+1}(h),i+1}$ is obtained by substituting $\text{in}_{\nu'} Q_i$ in $\text{in}_i h$, and (78) follows. \square

Now, apply Lemma 39 to the monomials $d_{\theta_{i+1}(h),i+1} Q_{i+1}^{\theta_{i+1}(h)}$ and $d_{\delta_{i+1}(h),i+1} Q_{i+1}^{\delta_{i+1}(h)}$. We have

$$\nu' \left(d_{\delta_{i+1}(h),i+1} Q_{i+1}^{\delta_{i+1}(h)} \right) \leq \nu' \left(d_{\theta_{i+1}(h),i+1} Q_{i+1}^{\theta_{i+1}(h)} \right) \quad (81)$$

by definition of δ_{i+1} and

$$\nu_i \left(d_{\theta_{i+1}(h),i+1} Q_{i+1}^{\theta_{i+1}(h)} \right) = \nu_i(h) \leq \nu_i \left(d_{\delta_{i+1}(h),i+1} Q_{i+1}^{\delta_{i+1}(h)} \right) \quad (82)$$

by Lemma 38, so the hypotheses of Lemma 39 are satisfied. By Lemma 39,

$$\theta_{i+1}(h) \geq \delta_{i+1}(h). \quad (83)$$

Since

$$\alpha_{i+1} \gamma_{1i} = \alpha_{i+1} \theta_{i+1}(h) \leq \deg_{\bar{Q}_i} \text{in}_i h = \delta_i(h) \quad (84)$$

by (76), (1) of the Proposition follows.

(2) Assume that $\delta_{i+1}(h) = \delta_i(h)$. Then the above two monomials coincide and

$$\alpha_{i+1} = 1. \quad (85)$$

Furthermore, we have equality in (84), so $\text{in}_i h = \text{in}_{\nu'} d_{\delta_i(h),i} g_{1i}^{\delta_i(h)}$. Combined with (85), this proves (2) of the Proposition.

Finally, (68) (assuming (67)) is proved by exactly the same reasoning as (67). (72) (assuming (71)) is proved by the same reasoning as (70). This completes the proof of the Proposition. \square

Remark 42 *One way of interpreting Lemma 39, together with the inequalities (81), (82) and (83) is to say that the characteristic vertex $(\nu'(d_{\theta_{i+1}(h),i+1}), \theta_{i+1}(h))$ of $\Delta_{i+1}(h)$ always lies above its pivotal vertex $(\nu'(d_{\delta_{i+1}(h),i+1}), \delta_{i+1}(h))$. This fact will be important in §9.*

For the rest of this section, assume that Q_{l+1} is defined for a certain ordinal number l and that \mathbb{N} iterations of the algorithm of the previous section produce an infinite sequence $\{Q_{l+t}\}_{t \in \mathbb{N}}$.

Take an ordinal i of the form $l + t$, $t \in \mathbb{N}$.

Corollary 43 (of Proposition 37) *We have $\alpha_{l+i} = 1$ for $i \gg 0$.*

This fact can also be easily seen without using Proposition 37. Indeed, equations (28), (32) and (36) show that

$$\prod_{j \leq i} \alpha_j \leq n$$

for all i . The Corollary follows immediately. \square

Choose the ordinal l above so that $\alpha_{l+t} = 1$ for all (strictly) positive integers t . By definition, for $t \in \mathbb{N}$, we have

$$Q_{l+t+1} = Q_{l+t} + z_{l+t}, \quad (86)$$

where z_{l+t} is a homogeneous l -standard expansion of value β_{l+t} , not involving Q_l (cf. Proposition 17). By Proposition 21 (2), we have

$$\deg_x z_{l+t} < \deg_x Q_{l+t}. \quad (87)$$

Finally,

$$\text{in}_{\nu'} Q_{l+t} = -\text{in}_{\nu'} z_{l+t} \quad (88)$$

by (45).

As before, let $h = \sum_{j=0}^{s_i} d_{ji} Q_i^j$ be an i -standard expansion of h for $i \geq l$, where each d_{ji} is an l -standard expansion, not involving Q_l . Note that since $\alpha_{l+t} = 1$ for $t \in \mathbb{N}$, we have $\deg_x Q_i = \prod_{j=2}^{\alpha_i} \alpha_j = \prod_{j=2}^{\alpha_l} \alpha_j = \deg_x Q_l$ and so

$$s_i = \left\lfloor \frac{\deg_x h}{\deg_x Q_i} \right\rfloor = \left\lfloor \frac{\deg_x h}{\deg_x Q_l} \right\rfloor = s_l. \quad (89)$$

By Proposition 37 (1), $\delta_i(h)$ is constant for all $i \gg l$. Let $\delta = \delta_i(h)$ for $i \gg l$. Write $\delta = p^e u$, where if $p > 1$ then $p \nmid u$. Then, according to Proposition 37 (2) and using the notation of (32), we see that for $i \gg l$

$$\delta - p^e \in S_i(h, \beta_i) \quad (90)$$

(in particular, $d_{\delta-p^e, i} \neq 0$) and that

$$\text{in}_i z_i = \left(\frac{\text{in}_i d_{\delta-p^e, i}}{u \text{in}_i d_{\delta, i}} \right)^{\frac{1}{p^e}} \quad (91)$$

In what follows, the ordinal i will run over the sequence $\{l + t\}_{t \in \mathbb{N}}$.

Next, we prove a comparison result which expresses the coefficients d_{ji} in terms of d_{jl} for $\delta - p^e \leq j \leq \delta$, modulo terms of sufficiently high value.

Proposition 44 *Assume that*

$$\delta_{i+1}(h) = \delta_i(h) = \delta. \quad (92)$$

Take an integer $v \in \{\delta - p^e, \delta - p^e + 1, \dots, \delta\}$. We have

$$\begin{aligned} d_{vi} \equiv & \sum_{j=0}^{\delta-v} (-1)^j \binom{v+j}{j} d_{v+j,l} (z_l + \dots + z_{i-1})^j \\ & \text{mod } \mathbf{P}'_{(\nu_l(h)-v\beta_l)+\min\{\nu_l^+(h)-\nu_l(h), \beta_i-\beta_l\}}. \end{aligned} \quad (93)$$

In particular, letting $v = \delta - p^e$ and $v = \delta$ in (93) we obtain

$$\begin{aligned} d_{\delta-p^e,i} \equiv & \sum_{j=0}^{p^e} (-1)^j \binom{\delta-p^e+j}{j} d_{\delta-p^e+j,l} (z_l + \dots + z_{i-1})^j \\ & \text{mod } \mathbf{P}'_{\nu'(\delta-p^e,l)+\min\{\nu_l^+(h)-\nu_l(h), \beta_i-\beta_l\}}. \end{aligned} \quad (94)$$

and

$$d_{\delta i} \equiv d_{\delta l} \quad \text{mod } \mathbf{P}'_{\nu'(d_{\delta l})+\min\{\nu_l^+(h)-\nu_l(h), \beta_i-\beta_l\}}, \quad (95)$$

respectively. If $p^e = 1$ (in particular, whenever $\text{char } K = 0$), (94) reduces to

$$d_{\delta-1,i} \equiv d_{\delta-1,l} - \delta d_{\delta l} (z_l + \dots + z_{i-1}) \quad \text{mod } \mathbf{P}'_{\nu'(d_{\delta-1,l})+\min\{\nu_l^+(h)-\nu_l(h), \beta_i-\beta_l\}}. \quad (96)$$

PROOF. By definitions, we have $Q_i = Q_l + z_l + \dots + z_{i-1}$. First, we will compare the l -standard expansion of h with the i -standard one. To this end, we substitute $Q_l = Q_i - z_l - \dots - z_{i-1}$ into the l -standard expansion of h . We obtain

$$h = \sum_{j=0}^{s_l} d_{jl} (Q_i - z_l - \dots - z_{i-1})^j = \sum_{j=0}^{s_l} d_{ji} Q_i^j. \quad (97)$$

We want to derive information about $\text{in}_i h$ from (97). First note that for each $q \in \{0, \dots, s_l - 1\}$ we have $\deg_x \sum_{j=0}^q d_{jl} (Q_i - z_l - \dots - z_{i-1})^j < (q+1) \deg_x Q_i$. Hence $d_{q+1,i}$ is completely determined by $d_{q+1,l}, d_{q+2,l}, \dots, d_{s_l l}$. Next, for $\delta - v < j \leq s_l - v$ and $l \leq s \leq i - 1$, note that

$$\nu' \left(d_{v+j,l} z_s^j \right) \geq j\beta_l + \nu'(d_{v+j,l}) \geq \nu_l^+(h) - v\beta_l, \quad (98)$$

so for $\delta - v < j \leq s_l - v$ the terms $d_{v+j,l} Q_l^{v+j}$ in (97) contribute nothing to

$$d_{vi} \quad \text{mod } \mathbf{P}'_{(\nu_l(h)-v\beta_l)+\min\{\nu_l^+(h)-\nu_l(h), \beta_i-\beta_l\}}.$$

Now, the coefficients d_{vi} in (97) are obtained from $\sum_{j=0}^{s_l} d_{jl}(Q_i - z_l - \cdots - z_{i-1})^j$ by opening the parentheses and then applying Euclidean division by Q_i ; such a Euclidean division may change the coefficients d_{vi} by adding terms of value at least $\nu'(Q_i) - \nu_l(Q_i) = \beta_i - \alpha_{l+1}\beta_l = \beta_i - \beta_l$. Finally, using (69) (which holds thanks to the hypothesis (92)) we observe that for v and j as in (93) we have $\nu'(d_{v+j,l}) \geq \nu'(d_{\delta l}) + (\delta - v - j)\beta_l = \nu_l(h) - (v + j)\beta_l$. This completes the proof of (93).

(94) and (95) follow from (93), after observing that

$$\nu_l(h) = \nu'(d_{\delta l}) + \delta\beta_l = \nu'(d_{\delta-p^e,l}) + (\delta - p^e)\beta_l$$

by (69). (96) obtained from (94) by substituting $p^e = 1$. The Proposition is proved. \square

Now let $f = h$ and let $f = \sum_{j=0}^{n_i} a_{ji}Q_i^j$ be the i -standard expansion of f . We have $n_i = n_l$ (this is a special case of (89)).

Proposition 45 *Assume that the sequence $\{Q_i\}$ is infinite. There are two mutually exclusive possibilities: either*

$$\lim_{i \rightarrow \infty} \beta_i = \infty \tag{99}$$

or *char $K = p > 0$ and there exists $t_0 \in \mathbb{N}$ such that, letting $i_0 = l + t_0$, we have*

$$\lim_{i \rightarrow \infty} \beta_i < \beta_{i_0} + \frac{1}{p^e} \left(\nu_{i_0}^+(f) - \nu_{i_0}(f) \right) \tag{100}$$

(recall that we are assuming $\text{rk } \nu = 1$).

PROOF. We start with a few lemmas.

Lemma 46 *Assume that either $\text{char } K = 0$ and $s < l_1$ in (61) or the set T contains a maximal element $Q_s = Q_l + z_l + \cdots + z_{s-1}$. Then $\delta_{s+1}(f) < \delta$. In particular, this case can occur at most finitely many times.*

PROOF. We give a proof by contradiction. Suppose $\delta_{s+1}(f) = \delta$. By Proposition 37 (2),

$$\text{in}_s f = \text{in}_{\nu'} a_{\delta s} (\bar{Q}_s + \text{in}_{\nu'} w)^\delta, \tag{101}$$

for some l -standard expansion w , not involving Q_l . This shows that Q_s is not maximal in T : the element $Q_s + w$ is greater than Q_s . It remains to consider the case $\text{char } K = 0$ and $s < l_1$. In this case, (59), (95) and (96) imply that

$$\text{in}_{\nu'} a_{\delta s} = \text{in}_{\nu'} a_{\delta l} \quad \text{and} \quad (102)$$

$$\text{in}_{\nu'} a_{\delta-1, s} = \text{in}_{\nu'} (a_{\delta-1, l} - \delta a_{\delta l} (z_l + \cdots + z_{s-1})) = \text{in}_{\nu'} (\delta a_{\delta} z_s). \quad (103)$$

Combining this with (101), we see that $\text{in}_{\nu'} w = \text{in}_{\nu'} z_s$. Then $Q_{s+1} \in T$, which contradicts the maximality of s in (61) (since $s+1$ belongs to the set on the right hand side of (61)). This completes the proof of the Lemma. \square

If $\text{char } K = 0$ and $s = l_1$ then, by definition, $\beta_s = \beta_{l_1} \geq \beta_l + \nu_l^+(f) - \nu_l(f)$. Take $q \geq l$ such that $\delta_i = \delta$ for all $i \geq q$. Thus Lemma 46 implies that if $\text{char } K = 0$ and $i_0 \geq q$ then there exists $i > i_0$ with $\beta_i > \beta_{i_0} + \nu_{i_0}^+(f) - \nu_{i_0}(f)$. Thus to complete the proof of the Proposition, it remains to show (99) assuming that there is no i_0 satisfying (100).

To do that, we will define a sequence of integers l_0, l_1, \dots recursively as follows. Let $l_0 = l$, where we choose l sufficiently large so that $\delta_i(f)$ and $\epsilon_i(f)$ stabilize for all $i \geq l$. Let $\delta = \delta_i(f)$ and $\epsilon = \epsilon_i(f)$. By assumption, there exists l_1 of the form $l + t$, $t \in \mathbb{N}$, such that $\beta_{l_1} \geq \beta_l + \frac{1}{p^e}(\nu_l^+(f) - \nu_l(f))$. We iterate this procedure. In other words, assume that the ordinal l_q is already defined. Choose l_{q+1} of the form $l + t$, $t \in \mathbb{N}$, such that

$$\beta_{l_{q+1}} \geq \beta_{l_q} + \frac{1}{p^e} (\nu_{l_q}^+(f) - \nu_{l_q}(f)). \quad (104)$$

Lemma 47 *We have*

$$\nu_{l_1}^+(f) - \nu_{l_1}(f) \geq \nu_l^+(f) - \nu_l(f). \quad (105)$$

PROOF. By Proposition 37, $\nu'(a_{\delta l_1}) = \nu'(a_{\delta l_0})$ and $\nu'(a_{\epsilon l_1}) = \nu'(a_{\epsilon l_0})$. Hence

$$\begin{aligned} \nu_{l_1}^+(f) - \nu_{l_1}(f) &= \nu'(a_{\epsilon l_1}) - \nu'(a_{\delta l_1}) - (\epsilon - \delta)\beta_{l_1} \geq \\ &\geq \nu'(a_{\epsilon l}) - \nu'(a_{\delta l}) - (\epsilon - \delta)\beta_l \geq \nu_l^+(f) - \nu_l(f), \end{aligned}$$

and the Lemma is proved. \square

We are now in the position to finish the proof of Proposition 45. Lemma 47 shows that $\nu_{l_j}^+(f) - \nu_{l_j}(f)$ is an increasing function of j , so, by (104), $\beta_{l_{j+1}} - \beta_{l_j}$ is bounded below by an increasing function of j . This proves that $\lim_{q \rightarrow \infty} \beta_q = \infty$, as desired. \square

Two things remain to be accomplished in our study of infinite sequences $\{Q_{l+t}\}_{t \in \mathbb{N}}$ of key polynomials. First, we must show that if $\lim_{t \rightarrow \infty} \beta_{l+t} = \infty$ and

$\delta = \delta_{l+t}(f)$ for t sufficiently large then δ is of the form $\delta = p^e$ for some $e \in \mathbb{N}$. Secondly, we must investigate the case when the sequence β_{l+t} is bounded and define the next key polynomial $Q_{l+\omega}$. Our main technique for dealing with the first of these problems will be differential operators. As for the second problem, we will use Proposition 44 (particularly, equation (94)). There we will not use differential operators as such, however, we will apply to f what could intuitively be termed “differentiation of order p^e with respect to Q_i ”. We now make a digression devoted to differential operators and their effect on key polynomials.

5 Key polynomials and differential operators

As we saw in the previous section, the most difficult situation to handle is one in which $t = \alpha_{i+1} = 1$ in (36) and (37): it is the only one which can give rise to infinite sequences of key polynomials. Then $\text{in}_i h$ has the form

$$\text{in}_i h = \text{in}_{\nu'} d_{\delta_i}(\bar{Q} + \text{in}_{\nu'} z_i)^\delta = \text{in}_i Q_{i+1}^\delta. \quad (106)$$

This section is devoted to proving some basic results about the effect of differential operators on key polynomials, needed to study equations h of the above form. Here and below, for a non-negative integer b , ∂_b will denote the differential operator $\frac{1}{b!} \frac{\partial^b}{\partial x^b}$. We are interested in proving lower bounds on the quantity $\nu'(\partial_{p^b} h)$ and also in giving sufficient conditions under which $\partial_{p^b} h$ is not identically zero.

Fix an ordinal l and a natural number t such that

$$\delta_{l+1}(h) = \delta_{l+2}(h) = \cdots = \delta_{l+t}(h)$$

By Proposition 37, this implies that

$$\alpha_{l+2} = \cdots = \alpha_{l+t} = 1 \quad (107)$$

and that h satisfies (106) for $l+1 \leq i < l+t$. Let $\delta = \delta_{l+1}(h)$. Write $\delta = p^e u$, where if $\text{char } K > 0$ then $p \nmid u$. If $\text{char } K = 0$, let $e = 0$.

Take an ordinal i having an immediate predecessor and such that the key polynomials Q_{i+1} are defined. If $\text{char } K > 0$, let

$$e_i = \min \left\{ e' \mid \partial_{p^{e'}} Q_i \not\equiv 0 \right\}. \quad (108)$$

If $\text{char } K = 0$, let $e_i = 0$. Let

$$b = e + e_i. \quad (109)$$

In the next section we will use our results on differential operators to prove that if $\lim_{t \in \mathbb{N}} \beta_{l+t} = \infty$ then δ is of the form $\delta = p^e$, that is, $u > 1$. This will be proved by contradiction: we will assume that $u > 1$ and show that $\lim_{t \in \mathbb{N}} \nu'(\partial_{p^b} f) = \infty$ but $\partial_{p^b} f \neq 0$.

Let $\mathbf{Q}_{i+1}^{\gamma_{i+1}}$ be an i -standard monomial. One of our main tasks in this section is to study the quantity $\nu'(\partial_{p^b} \mathbf{Q}_{i+1}^{\gamma_{i+1}})$. Since an exact formula for $\nu'(\partial_{p^b} \mathbf{Q}_{i+1}^{\gamma_{i+1}})$ seems too complicated to compute, we are only able to give an approximate lower bound, except under the additional assumption that $\beta_i \gg \beta_l$ (a precise form of this inequality is (111) below).

Let b be any non-negative integer such that $b \geq e_i$.

Proposition 48 (1) *We have*

$$\nu'(\mathbf{Q}_{i+1}^{\gamma_{i+1}}) - \nu_i(\partial_{p^b} \mathbf{Q}_{i+1}^{\gamma_{i+1}}) \leq \max\{p^{b-e_i}(\beta_i - \nu_i(\partial_{p^{e_i}} Q_i)), p^b \beta_l\}. \quad (110)$$

(2) *Assume that*

$$p^{b-e_i}(\beta_i - \nu_i(\partial_{p^{e_i}} Q_i)) > p^b \beta_l. \quad (111)$$

Then equality holds in (110) if and only if

$$\binom{\gamma_i}{p^{b-e_i}} \neq 0. \quad (112)$$

In particular, $\partial_{p^b} \mathbf{Q}_{i+1}^{\gamma_{i+1}} \neq 0$.

(3) *Assume that both (111) and (112) hold. Then*

$$in_i \partial_{p^b} \mathbf{Q}_{i+1}^{\gamma_{i+1}} = in_i \frac{\mathbf{Q}_{i+1}^{\gamma_{i+1}} (\partial_{p^{e_i}} Q_i)^{p^{b-e_i}}}{Q_i^{p^{b-e_i}}}.$$

PROOF. Direct calculation, using induction on i and the fact that, by (107) and Proposition 17, the i -standard monomial $\mathbf{Q}_{i+1}^{\gamma_{i+1}}$ does not involve any of Q_{l+1}, \dots, Q_{i-1} . \square

Remark 49 *The following is a well known characterization of the inequation (112). Let $\gamma_i = k_0 + pk_1 + \dots + p^q k_q$, with $k_0, \dots, k_q \in \{0, 1, \dots, p-1\}$, denote the p -adic expansion of γ_i . Then (112) holds if and only if $k_{b-e_i} > 0$. In particular, (112) holds whenever γ_i is of the form $\gamma_i = p^{b-e_i} u$, with $p \nmid u$. This is the only situation in which Proposition 48 will be applied in this paper.*

Corollary 50 *Let h be any element of $K[X]$, not necessarily satisfying (106).*

(1) *We have*

$$\nu_i(\partial_{p^b} h) \geq \nu_i(h) - \max \left\{ p^{b-e_i} \left(\beta_i - \nu_i(\partial_{p^{b-e_i}} Q_i) \right), p^b \beta_l \right\}. \quad (113)$$

(2) *Write $in_i h = \sum_{j \in S_i} in_i(d_{ji} Q_i^j)$. Let $S_{bi} = \{j \in S_i \mid \binom{j}{p^{b-e_i}} \neq 0\}$. Assume that the inequality (111) holds and that $S_{bi} \neq \emptyset$. Then equality holds in (113) and $in_i \partial_{p^b} h = \sum_{j \in S_{bi}} in_i(d_{ji} Q_i^{j-p^{b-e_i}} (\partial_{p^{e_i}} Q_i)^{p^{b-e_i}})$. In particular, $\partial_{p^b} h \neq 0$.*

Corollary 51 *Assume that h satisfies (106). Let b be as in (109). Then $\partial_{p^b} h \neq 0$.*

PROOF. This is a special case of Corollary 50. \square

Corollary 52 *Assume that h and b satisfy the hypotheses of Corollary 50 (or, more specifically, those of Corollary 51). Then*

$$h \notin K[X^{p^{b+1}}]. \quad (114)$$

6 Sequences of key polynomials whose values tend to infinity

Let the notation be as above. Let l be an ordinal and assume that the above construction of key polynomials gives rise to a sequence $\{Q_{l+t}\}_{t \in \mathbb{N}}$ of key polynomials such that

$$\lim_{t \rightarrow \infty} \beta_{l+t} = \infty. \quad (115)$$

Let $\delta = \delta_{l+t}(f)$ for t sufficiently large. The purpose of this section is to prove

Theorem 53 *The integer δ is of the form $\delta = p^e$ for some $e \in \mathbb{N}$.*

PROOF. We give a proof by contradiction. Suppose that (115) holds but δ is of the form $\delta = p^e u$ with $u > 1$. Let b be as in (109) and let $g = \partial_{p^b} f$. The quantity $p^b \beta_l$ is independent of t , hence, by (115), the inequality (111) holds for t sufficiently large. By Proposition 37 (2), $in_{l+t} f$ has the form (106) for $i = l + t$, as t runs over \mathbb{N} . Hence $h = f$ satisfies the hypotheses of Corollary 51. By Corollary 51, $g \neq 0$. Moreover, by Corollary 50 (1), we have $\nu'(g) \geq \nu_{l+t}(g) \geq \delta \beta_{l+t} - p^e \beta_{l+t} = p^e (u - 1) \beta_{l+t}$. Since $u > 1$, this shows that $\nu'(g) = \infty$, which contradicts the fact that g is given by a polynomial in x of degree strictly less than n . \square

The following Proposition will come in useful in the remaining sections.

Proposition 54 *Take an element h of L and an ordinal i such that the key polynomials \mathbf{Q}_{i+1} are defined. Assume that*

$$\nu'(h) < \beta_i \quad (116)$$

and that h admits an i -standard expansion

$$h = \sum_{j=0}^s c_j Q_i^j, \quad (117)$$

such that $\nu'(c_j) \geq 0$ for all j . Then $\nu'(h) = \nu_i(h)$.

PROOF. By definition of standard expansion, each c_j in (117) is an i -standard expansion not involving Q_i . Then c_j is a sum of monomials in \mathbf{Q}_i , which does not vanish in $G_{\nu'}$ (22), hence all the monomials appearing in c_j have value at least $\nu'(c_j)$. By (116),

$$\nu'(c_j Q_i^j) = \nu_i(c_j Q_i^j) > \nu'(h) \quad \text{for } j > 0 \quad (118)$$

(117) and (118) imply that $\nu'(h) = \nu'(c_0)$. Thus h is a sum of monomials in \mathbf{Q}_i of value at least $\nu'(h)$, as desired. \square

7 Sequences of key polynomials with bounded values in fields of positive characteristic

In this section, we assume that $\text{char } K = p > 0$. Let l be an ordinal number and assume that the key polynomials $\mathbf{Q}_l \cup \{Q_{l+t}\}_{t \in \mathbb{N}}$ are already defined. Moreover, assume that we are in Case 2b of §3 (in particular, the sequence $\{\beta_{l+t}\}_{t \in \mathbb{N}}$ has an upper bound $\bar{\beta}$ but no maximum in Γ ; this is the only case which remains to be treated to complete the definition of the Q_i). By Proposition 43, there exists $t_0 \in \mathbb{N}$ such that

$$\alpha_{l+t} = 1 \quad \text{and} \quad \delta_{l+t} = \delta_{l+t_0} \quad \text{for all } t \geq t_0. \quad (119)$$

Replacing l by $l + s$ for a suitable positive integer s , we may assume that $\alpha_{l+t} = 1$ for all strictly positive t . In what follows, the index i will run over the set $\{l + t\}_{t \in \mathbb{N}}$. As usual, let δ denote the common value of all the $\delta_i(f)$.

Proposition 55 *Assume we are in Case 2b. There exist $i \in \{l + t\}_{t \in \mathbb{N}}$, a strictly positive integer $e_0 \leq e$ and a weakly affine i -standard expansion $Q_{l+\omega}$, monic of degree p^{e_0} in Q_i , such that*

$$\bar{\beta} \leq \frac{1}{p^{e_0}} \nu(Q_{l+\omega}). \quad (120)$$

Of course, the inequality (120) is equivalent to saying that

$$\nu'(Q_{l+\omega}) > p^{e_0} \nu(Q_l + z_l + \cdots + z_{l+t}) \quad (121)$$

for all $t \in \mathbb{N}$.

PROOF. The idea is to start with the inequality $\nu'(f) > \nu_{l+t}(f)$ for all $t \in \mathbb{N}$ and to gradually construct polynomials g of the smallest possible degree satisfying

$$\nu'(g) > \nu_i(g) \quad (122)$$

until we arrive at $g = Q_{l+\omega}$ satisfying the conclusion of the Proposition.

First, let a^* be an l -standard expansion, not involving Q_l , such that

$$\text{in}_{\nu'}(a^* a_{\delta l}) = 1 \quad (123)$$

and let $a^*(X)$ be the representative of a^* in $K[X]$ of degree less than n . Note that

$$\text{in}_{\nu'} a_{\delta l} = \text{in}_{\nu'} a_{\delta i} \quad \text{for all } i \geq l \quad (124)$$

by Proposition 37 (2).

Let $\tilde{f} = a^*(X)\bar{f}$. By Proposition 37 (2), for all $i \geq l$ we have

$$\text{in}_i \tilde{f} = \text{in}_i f = \text{in}_{\nu'} a_{\delta i} (\bar{Q}_i + \text{in}_{\nu'} z_i)^\delta,$$

hence in view of (124) we have $\text{in}_i \tilde{f} = (\bar{Q}_i + \text{in}_{\nu'} z_i)^\delta$. In particular,

$$\nu'(\tilde{f}) > \nu_i(\tilde{f}) \quad \text{for all } i. \quad (125)$$

Let $\tilde{f} = \sum_{j=0}^{\tilde{n}_l} \tilde{a}_{ji} Q_i^j$ be the i -standard expansion of \tilde{f} . We have $\text{in}_{\nu'} \tilde{a}_{\delta i} = 1$ for all i .

As noted in the previous section, since $\alpha_i = 1$ for all i , all the i -standard expansions of \tilde{f} have the same degree \tilde{n}_l in Q_i .

By Lemma 47 the quantity $\nu_i^+(\tilde{f}) - \nu_i(\tilde{f})$ is increasing with i . Taking into account the fact that $\bar{\beta} = \lim_{i \rightarrow \infty} \beta_i$, we have, for i sufficiently large,

$$\nu'(\tilde{a}_{i\delta}) + \delta \bar{\beta} - \nu_i(\tilde{f}) = \delta(\bar{\beta} - \beta_i) < \nu_i^+(\tilde{f}) - \nu_i(\tilde{f}). \quad (126)$$

By choosing l sufficiently large, we may assume that (126) holds for $i \geq l$.

Next, write $\tilde{a}_{\delta l} = 1 + \tilde{a}^\dagger$ with $\nu'(\tilde{a}^\dagger) > 0$. Let $\tilde{\tilde{f}} = (1 - \tilde{a}^\dagger(X))\tilde{f}$ and let $\tilde{\tilde{f}} = \sum_{j=0}^{\tilde{\tilde{n}}_l} \tilde{\tilde{a}}_{jl} Q_l^j$ be the l -standard expansion of $\tilde{\tilde{f}}$. By (126) terms of the form

$(1 - \tilde{a}^\dagger(X))\tilde{a}_{jl}$ with $j > \delta$ contribute terms of negligibly high value to $\tilde{a}_{\delta l}$. Terms $(1 - \tilde{a}^\dagger(X))\tilde{a}_{jl}$ with $j < \delta$ contribute terms of value at least $\nu'(\tilde{a}^\dagger) + (\beta_l - \alpha_l\beta_{l-1})$ to $\tilde{a}_{\delta l}$. Thus $\nu'(\tilde{a}^\dagger) \geq \nu'(\tilde{a}^\dagger) + \min\{\nu'(\tilde{a}^\dagger), \beta_l - \alpha_l\beta_{l-1}\}$, so multiplying \tilde{f} by $(1 - \tilde{a}^\dagger(X))$ increases $\nu'(\tilde{a}^\dagger)$ by a fixed amount. Iterating this procedure finitely many times, we may assume that $\nu'(\tilde{a}^\dagger) > \delta\bar{\beta} > \nu_i(\tilde{f})$ for all i . Then replacing $a_{\delta l}$ by 1 does not affect the inequality (125), hence we may assume that $\tilde{a}_{\delta l} = 1$.

Let

$$\bar{f} = \sum_{j=0}^{\delta} \tilde{a}_{jl} Q_l^j.$$

(126) implies that for all j , $\delta < j \leq \tilde{n}_l$,

$$\nu'(\tilde{a}_{jl} Q_l^j) \geq \nu_l^+(\tilde{f}) > \delta\bar{\beta} > \delta\beta_i = \nu_i(\tilde{f}).$$

Hence $\text{in}_i \tilde{f} = \text{in}_i \bar{f}$; in particular, $\nu(\bar{f}) > \nu_i(\bar{f})$ for all i .

The polynomial \bar{f} is monic of degree δ ; the expression $\bar{f} = \sum_{j=0}^{\delta} \tilde{a}_{ji} Q_i^j$ is the i -standard expansion of \bar{f} . None of the subsequent transformations $Q_i = Q_l + z_l + \cdots + z_{i-1}$ affect the coefficient $a_{\delta l} = 1$, so $a_{\delta i} = 1$ for all i .

Write $\delta = p^e u$, as in the previous section. Let $g = \sum_{j=0}^{p^e} \binom{\delta - p^e + j}{j} \tilde{a}_{\delta - p^e + j} Q_l^j$ (roughly speaking, the reader should think of the process of constructing g from \bar{f} as applying a differential operator of order $\delta - p^e$ with respect to Q_{i_0}). By construction,

$$\text{in}_i \bar{f} = (\bar{Q}_i + \text{in}_{\nu'} z_i)^\delta \quad \text{for } i \geq l. \quad (127)$$

On the other hand, let $w_{i-1} = z_l + \cdots + z_{i-1}$. Then

$$\bar{f} = \sum_{j=0}^{\delta} \tilde{a}_{jl} (Q_i - w_{i-1})^j. \quad (128)$$

The terms in (128) with $j < \delta - p^e$ give rise to polynomials of degree strictly less than $(\delta - p^e) \deg_x Q_l$. Thus (128) can be rewritten as

$$\bar{f} = \sum_{j=0}^{p^e} \tilde{a}_{\delta - p^e + j, l} (Q_i - w_{i-1})^{\delta - p^e + j} + \phi \quad (129)$$

$$= Q_i^{\delta - p^e} \sum_{j=0}^{p^e} \sum_{v=j}^{p^e} (-1)^{v-j} \binom{\delta - p^e + v}{\delta - p^e + j} \tilde{a}_{\delta - p^e + v, l} w_{i-1}^{v-j} Q_i^j + \psi \quad (130)$$

$$= Q_i^\delta + Q_i^{\delta - p^e} \sum_{j=0}^{p^e - 1} \sum_{v=j}^{p^e} (-1)^{v-j} \binom{\delta - p^e + v}{\delta - p^e + j} \tilde{a}_{\delta - p^e + v, l} w_{i-1}^{v-j} Q_i^j + \psi \quad (131)$$

where $\deg_x \phi, \deg_x \psi < (\delta - p^e) \deg_x Q_l$. On the other hand, we have

$$g = \sum_{j=0}^{p^e} \binom{\delta - p^e + j}{j} \tilde{a}_{\delta - p^e + j, l} Q_i^j \quad (132)$$

$$= \sum_{j=0}^{p^e} \binom{\delta - p^e + j}{j} \tilde{a}_{\delta - p^e + j, l} (Q_i - w_{i-1})^j \quad (133)$$

$$= \sum_{j=0}^{p^e} \sum_{v=j}^{p^e} (-1)^{v-j} \binom{\delta - p^e + v}{v} \binom{v}{j} \tilde{a}_{\delta - p^e + v, l} w_{i-1}^{v-j} Q_i^j \quad (134)$$

$$= u Q_i^{p^e} + \sum_{j=0}^{p^e-1} \sum_{v=j}^{p^e} (-1)^{v-j} \binom{\delta - p^e + v}{v} \binom{v}{j} \tilde{a}_{\delta - p^e + v, l} w_{i-1}^{v-j} Q_i^j. \quad (135)$$

Now, $\binom{\delta - p^e + v}{v} \binom{v}{j} = \binom{\delta - p^e + v}{\delta - p^e + j} \binom{\delta - p^e + j}{j}$ whenever $j \leq v$; moreover,

$$\binom{\delta - p^e + j}{j} = 1 \quad \text{if } 0 \leq j < p^e \quad (136)$$

$$= u \quad \text{if } j = p^e. \quad (137)$$

Thus the double sums in (131) and (135) are identical; note also that everything in these double sums has degree strictly less than $p^e \deg_x Q_l$. Thus rewriting the double sum as an i -standard expansion and comparing (135) with (127) shows that $\text{in}_i g = u \bar{Q}_i^{p^e} + u \text{in}_{\nu'} z_i^{p^e} = u (\bar{Q}_i + \text{in}_{\nu'} z_i)^{p^e}$; in particular, g satisfies (122). Dividing g by the non-zero integer u does not change the problem, so we may assume that g is a monic polynomial in Q_i of degree p^e . Write

$$g = \sum_{j=0}^{p^e} c_{ji} Q_i^j. \quad (138)$$

Choose $i_0 \geq l$ sufficiently large so that

$$\beta_{i_0} - \alpha_l \beta_{l-1} > p^e (\bar{\beta} - \beta_{i_0}). \quad (139)$$

Remark 56 *Assume that there exist $i \geq i_0$ and j , $1 \leq j < p^e$, such that $\nu'(c_{ji}) + j\bar{\beta} > 2p^e\bar{\beta} - p^e\beta_i$. Then for any $i' > i$ we have $\text{in}_{i'}(g - c_{ji}Q_i^j) = \text{in}_{i'}g$; in particular, $\nu_{i'}(g - c_{ji}Q_i^j) < \nu'(g - c_{ji}Q_i^j)$. Thus we are free to replace g by $g - c_{ji}Q_i^j$.*

Assume that there exist $j \in \{1, \dots, p^e - 1\}$ and $i_1 \geq i_0$ such that $c_{ji_1} \neq 0$ and

$$p^e\bar{\beta} < \nu(c_{ji_1}) + j\bar{\beta} < (p^e + 1)\beta_{i_1} - \alpha_l\beta_{l-1}. \quad (140)$$

Take the greatest such j .

Lemma 57 (1) We have $\nu'(c_{ji}) + j\bar{\beta} > p^e\bar{\beta}$ for all $i \geq i_1$.

(2) The element $in_{\nu'}c_{ji}$ is constant for all $i \geq i_1$.

(3) There exists $i_2 \geq i_1$ such that for all $i \geq i_2$ we have

$$\nu_i(g - c_{ji_2}Q_{i_2}^j) < \nu'(g - c_{ji_2}Q_{i_2}^j).$$

PROOF. (2) follows the maximality of j and the inequalities (139) and (140): $in_{\nu'}c_{ji_2}$ cannot be affected by any subsequent coordinate changes of the form $Q_i = Q_{i_1} + z_{i_1} + \dots + z_{i-1}$. (1) follows immediately from (2).

By (1) and (2), taking i_2 sufficiently large, we can ensure that

$$\nu'(c_{ji_2}Q_{i_2}^j) > p^e\bar{\beta}.$$

Since $p^e\bar{\beta} > p^e\beta_i = \nu_i(g)$, we have

$$\nu_i(g - c_{ji_2}Q_{i_2}^j) = \nu_i(g) < \min\{\nu'(g), \nu'(c_{ji_2}Q_{i_2}^j)\} \leq \nu'(g - c_{ji_2}Q_{i_2}^j)$$

for all $i \in i_2 + \mathbb{N}$, and (3) is proved. This completes the proof of Lemma 57. \square

If there exists $j \in \{1, \dots, p^e - 1\}$ satisfying the hypotheses of Lemma 57, replace g by $g - c_{ji_2}Q_{i_2}^j$; Lemma 57 (3) says that strict inequality (122) is satisfied with g replaced by $g - c_{i_2j}Q_{i_2}^j$. This procedure strictly decreases the integer j appearing in Lemma 57. Hence after finitely many repetitions of this procedure we obtain a polynomial g such that there do not exist j and i_1 satisfying (140). By the second inequality in (140), the non-existence of such j and i_1 is preserved as we pass from i to $i + 1$; hence, after finitely many steps we may assume that no j and i_1 satisfying (140) exist. We will make this assumption from now on.

Remark 58 Now, by the same reasoning as in Lemma 57, the sets

$$\mathcal{S} := \left\{ j \in \{1, \dots, p^e\} \mid c_{ji} \neq 0 \text{ and } \nu(c_{ji}) = (p^e - j)\bar{\beta} \right\}$$

and $\{in_{\nu'}c_{ji} \mid j \in \mathcal{S}\}$ are independent of i for $i \geq i_0$.

Lemma 59 Consider an index $j \in \{1, \dots, p^e - 1\}$ and an ordinal $i \geq i_0$ of the form $i = i_0 + t$, $t \in \mathbb{N}$, as above. Assume that $c_{ji} \neq 0$. We have

$$\nu'(c_{ji}) + j\bar{\beta} \geq p^e\bar{\beta} \tag{141}$$

and j is a power of p whenever equality holds in (141).

PROOF. We give a proof by contradiction. Assume that for a certain $i_1 \geq i_0$ there exists $j \in \{1, \dots, p^e - 1\}$ such that $c_{ji_1} \neq 0$, and either

$$\nu(c_{ji_1}) < (p^e - j)\bar{\beta} \quad (142)$$

or j is not a p -power (or both). Let $j(g)$ denote the greatest such j . Let $j = j(g)$. Then the element $\text{in}_{\nu'} c_{ji_1}$ is not affected by the subsequent coordinate changes $Q_{i_1} = Q_i - z_{i_1} - \dots - z_{i-1}$, so $\text{in}_{\nu'} c_{ji} = \text{in}_{\nu'} c_{ji_1}$ for all $i \geq i_1$.

First assume that (142) holds. (142) can be rewritten as $\nu(c_{ji}) + j\bar{\beta} < p^e\bar{\beta}$. Now, taking i sufficiently large, the difference $\bar{\beta} - \beta_i$ can be made arbitrarily small, so $\nu(c_{ji}) + j\beta_i < p^e\beta_i$. This inequality shows that

$$\nu(c_{ji}Q_i^j) < \nu(Q_i^{p^e}),$$

so $\text{in}_i g$ does not contain the monomial $Q_i^{p^e}$, which is a contradiction.

From now on assume that

$$\nu'(c_{ji}) + j\bar{\beta} = p^e\bar{\beta} \quad \text{for all } i \geq i_1. \quad (143)$$

Then, by definition of j , j is not a p -power. Write $j = p^{e'}u'$ and $Q_{i+1} = Q_i + z_i$. Then the $(i+1)$ -standard expansion of g contains a monomial of value $\nu'(c_{ji}z_i^{j-p^{e'}}Q_{i+1}^{p^{e'}})$. We have

$$\nu'(c_{ji}z_i^{j-p^{e'}}) + p^{e'}\bar{\beta} = \nu'(c_{ji}) + (j - p^{e'})\beta_i + p^{e'}\bar{\beta} < \nu'(c_{ji}) + j\bar{\beta} = p^e\bar{\beta}.$$

Thus the appearance of a monomial of value $\nu'(c_{ji}z_i^{j-p^{e'}}Q_{i+1}^{p^{e'}})$ in the standard expansion of g contradicts (143) with i replaced by $i+1$. This completes the proof of Lemma 59. \square

If $Q_{l+\omega} = g$ satisfies the conclusion of Proposition 55 there is nothing more to prove. Otherwise, by Lemma 59 and since no j and i_1 satisfy (140), there exist $j \in \{1, \dots, p^e - 1\}$ and $i_1 \geq i_0$ such that for all $i \geq i_1$ we have

$$\nu(c_{ji}) + j\bar{\beta} > (p^e + 1)\beta_i - \alpha_l\beta_{l-1} \geq (p^e + 1)\beta_{i_1} - \alpha_l\beta_{l-1} > p^e\bar{\beta}. \quad (144)$$

Let \mathcal{A} denote the set of all such j . Replace g by $g - \sum_{j \in \mathcal{A}} c_{ji_1}Q_{i_1}^j$. Remark 56 says that strict inequality (122) is satisfied for this new g . In this way, we obtain a polynomial g such that $Q_{l+\omega} = g$ satisfies the conclusion of Proposition 55. This completes the proof of Proposition 55. \square

Remark 60 *We are not claiming that the property that g is a weakly affine expansion in Q_{i_1} is preserved when we pass from i_1 to some other ordinal*

$i > i_1$. However, the above results show that for any $i \geq i_1$ of the form $i = l + t$, $t \in \mathbb{N}$, g is a sum of a weakly affine expansion in Q_i all of whose monomials $c_{ji}Q_i^j$ lie on the critical line $\nu'(c_{ji}) = (p^e - j)\bar{\beta}$ and another standard expansion of degree strictly less than p^e in Q_i , all of whose monomials have value greater than or equal to $(p^e + 1)\beta_{i_1} - \alpha_l\beta_{l-1} > p^e\bar{\beta}$.

We define $Q_{l+\omega}$ to be a weakly affine standard expansion satisfying the conclusion of Proposition 55, which minimizes the integer e_0 (so that $\alpha_{l+\omega} = p^{e_0}$). This completes the definition of the Q_i .

Let $\theta_{l+\omega}(f) = \frac{\delta}{\alpha_{l+\omega}}$. It is easy to see, by the same argument as in Lemma 38, that the Newton polygon $\Delta_{l+\omega}(f)$ contains a vertex $(\nu'(a_{\theta_{l+\omega}(f)}), \theta_{l+\omega}(f))$, and that this vertex lies above the pivotal vertex $(\nu'(a_{\delta_{l+\omega}(f)}), \delta_{l+\omega}(f))$. The vertex $(\nu'(a_{\theta_{l+\omega}(f)}), \theta_{l+\omega}(f))$ will be called the **characteristic vertex** of $\Delta_{l+\omega}(f)$. The notion of characteristic vertex will be used in §9 when we study the totality of extensions of ν to L . It is important that the characteristic vertex is determined by $\mathbf{Q}_{l+\omega+1}$ and $\beta_{l+\omega}$; it does not depend on $\beta_{l+\omega}$.

Remark 61 *By construction, we have $\alpha_{l+\omega} = p^{e_0} \geq p$. Then the fact that $\deg_x Q_{l+\omega} \leq n$ and Proposition 21 show that the situation considered in this section can arise at most $\lceil \log_p n \rceil$ times, so the set $\mathbf{Q} := \{Q_i\}$ thus defined has order type of at most $\lceil \log_p n \rceil \omega + t$, where $t \in \mathbb{N}$.*

8 Proof that $\{Q_i\}$ is a complete set of key polynomials

This section is devoted to proving

Theorem 62 *The well ordered set $\mathbf{Q} := \{Q_i\}$ defined in the previous sections is a complete set of key polynomials. In other words, for any element $\beta \in \Gamma_+$ the corresponding ν' -ideal \mathbf{P}'_β is generated by all the monomials in the Q_i of value β or higher. In particular, we have $G_{\nu'} = G_\nu[in_{\nu'}\mathbf{Q}]^*$.*

Corollary 63 *The valuation ν' is completely determined by the data $\mathbf{Q}, \{\beta_i\}$.*

PROOF. Let λ be the ordinal number which represents the order type of the set \mathbf{Q} , so that $\mathbf{Q} = \mathbf{Q}_\lambda$. Let l denote the smallest ordinal such that $0 \leq l < \lambda$ and $\alpha_i = 1$ whenever $l < i < \lambda$ (note, in particular, that if λ admits an immediate predecessor and $\alpha_{\lambda-1} > 1$ then $l = \lambda - 1$; at the other end of the spectrum is the possibility that $\alpha_i = 1$ for all $i < \lambda$ and $l = 0$). To prove the Theorem, it is sufficient to show that for every positive $\beta \in \Gamma$ and every $h \in L$ such that $\nu'(h) = \beta$, h belongs to the ideal generated by all the monomials $c\mathbf{Q}^\gamma$ such that $\nu'(c\mathbf{Q}^\gamma) \geq \beta$.

Take any element $h \in L$. Without loss of generality, we may assume that, writing $h = \sum_{j=0}^s d_j x^j$, we have $\nu(d_j) \geq 0$ for all j (otherwise, multiply h by a suitable element of K).

Claim 64 *There exists $i < \lambda$ of the form $i = l + t$, $t \in \mathbb{N}$, such that*

$$\beta_i > \nu'(h). \quad (145)$$

PROOF. There are two possibilities: either λ has an immediate predecessor or it does not. By construction, for any i such that $l < i < \lambda$ we have $i = l + t$ for some $t \in \mathbb{N}$. The ordinal λ admits an immediate predecessor if and only if $\lambda = l + t$ for some $t \in \mathbb{N}$ and does not admit an immediate predecessor if and only if $\lambda > l + t$ for all $t \in \mathbb{N}$. If λ has an immediate predecessor then $Q_{\lambda-1} = f(x) = 0$, so $\nu'(Q_{\lambda-1}) = \infty > \nu'(h)$. If λ does not have an immediate predecessor then by construction $\lim_{t \rightarrow \infty} \beta_{l+t} = \infty$, so there exists $i = l + t$, $t \in \mathbb{N}$ such that (145) holds. The Claim is proved. \square

Now, Lemma 54 says that $\nu_i(h) = \nu'(h)$. This means, by definition, that h can be written as a sum of monomials in \mathbf{Q}_{i+1} of value at least $\nu'(h)$, hence it belongs to the ideal generated by all such monomials. This completes the proof. \square

9 A description of the algorithm.

Let $K \hookrightarrow L$ be a finite separable field extension and $\nu : K^* \rightarrow \Gamma$ a valuation of K . In this section we describe an algorithm for constructing all the possible extensions ν' of ν to L . Pick and fix a generator x of L over K once and for all. Let $f = \sum_{i=0}^n a_i x^i$ denote the minimal polynomial of x over K .

First, we reduce the problem to the case $rk \nu = 1$. Let $r = rk \nu$. Write ν as a composition of r rank 1 valuations: $\nu = \nu_1 \circ \cdots \circ \nu_r$, where ν_1 is the valuation of K , centered at the smallest non-zero prime ideal of R_ν . Assume the problem is already solved for rank 1 valuations. Then any extension ν' of ν to L is of the form $\nu' = \nu'_1 \circ \cdots \circ \nu'_r$, where ν'_1 is an extension of ν_1 to L , ν'_2 is an extension of ν_2 to $k_{\nu'_1}$, and so on. The valuation ν'_i is an extension of the valuation ν_i of the field $k_{\nu_{i-1}}$ to its algebraic extension $k_{\nu'_{i-1}}$. Thus, it is sufficient to solve the problem in the case $rk \nu = 1$.

From now on, we assume that $rk \nu = 1$.

Step 1.1 of the algorithm. Choose an element $\beta_1 \in \Gamma_+$ which determines a side of $\Delta(f)$ and put $\nu'(x) = \beta_1$.

Step 1.2 of the algorithm. Let

$$\text{in}_1 f = v \prod_{j=1}^s g_j^{\gamma_j} \quad (146)$$

be the factorization of $\text{in}_1 f$ into (monic) irreducible factors in $G_\nu[\bar{x}]$. Since for any extension ν' of ν we have $\text{in}_1 f(\text{in}_{\nu'} x) = 0$, one of the irreducible factors in (146) is the minimal polynomial of $\text{in}_{\nu'} x$ over G_ν . Choose one of the irreducible factors in (146) (other than \bar{x}), say g_1 . Write

$$g_1 = \sum_{i=0}^{\alpha_1} \bar{b}_i \bar{x}^i,$$

where $\bar{b}_{\alpha_1} = 1$. For each i , $0 \leq i \leq \alpha_1$, let b_i be a representative of \bar{b}_i in R_ν (that is, an element of R_ν such that $\text{in}_\nu b_i = \bar{b}_i$). Put $Q_1 = x$ and $Q_2 = \sum_{i=1}^{\alpha_1} b_i x^i$.

Assume, inductively, that key polynomials Q_1, \dots, Q_l and positive integers $\alpha_1, \dots, \alpha_{l-1}$ are already constructed for a certain ordinal l , where $l < \omega$ if $\text{char } K = 0$ and $l < ([\log_p n] + 1)\omega$ if $\text{char } K = p > 0$.

Assume, inductively, that for each i , $1 \leq i < l$, the $(i+1)$ -st key polynomial Q_{i+1} admits an i -th standard expansion of the form

$$Q_{i+1} = Q_i^{\alpha_i} + \sum_{j=0}^{i-1} \left(\sum_{\gamma} c_{ji\gamma} \mathbf{Q}_j^\gamma \right) Q_i^j, \quad (147)$$

where each of $c_{ji\gamma} \mathbf{Q}_j^\gamma$ is an i -standard monomial. Assume that the standard expansions (147) satisfy all the conditions described in §3.

Write $f = \sum_{j=0}^{n_l} a_{jl} Q_l^j$, where each a_{jl} is a homogeneous l -standard expansion not involving Q_l . The next two steps of the algorithm are a generalization of the first two steps, with 1 replaced by l .

Step 1.1 of the algorithm. If l does not have an immediate predecessor (that is, l is of the form $l = l_0 + \omega$), let $\bar{\beta}_l = \sup\{\beta_{l_0+t}\}_{t \in \mathbb{N}}$. Choose an element β_l which determines a side A_l of $\Delta_l(f)$ and satisfies the following condition:

Condition (*). If l has an immediate predecessor then $\beta_l > \alpha_l \beta_{l-1}$; if l does not have an immediate predecessor then $\beta_l > \alpha_l \bar{\beta}_l$.

Put $\nu'(Q_l) = \beta_l$.

Remark 65 We know from §3 and §7 that Condition (*) must hold for any extension ν' of ν ; it is a consequence of the proof of Proposition 37 (see (83)) that the pivotal vertex of $\Delta_l(f)$ lies below its characteristic vertex. Conversely, if \mathbf{Q}_{l+1} and β_l are given, any side of $\Delta_l(f)$ lying below its characteristic vertex can be chosen to be the characteristic side; the choice of β_l which determines such a characteristic side will automatically satisfy Condition (*).

Step 1.2 of the algorithm. By Proposition 36 the value $\nu'(a_{jl})$, where $1 \leq i \leq n_l$, is completely determined by the l -standard expansion of a_{il} ; in particular, it is completely determined at this stage of the algorithm. Similarly, $\text{in}_l f := \sum_{(\nu'(a_{il}), i) \in A_l} \text{in}_{\nu'} a_{il} \bar{Q}_l^i$ is a well-defined element of $G_{\nu'}[\text{in}_{\nu'} Q_1, \dots, \text{in}_{\nu'} Q_{l-1}][\bar{Q}_l]$.

Let $\text{in}_l f = v_l \prod_{j=1}^{t_l} g_{jl}^{\gamma_{jl}}$ be the factorization of $\text{in}_l f$ into (monic) irreducible factors in $G_{\nu'}[\text{in}_{\nu'} Q_1, \dots, \text{in}_{\nu'} Q_{l-1}][\bar{Q}_l]$. Choose one of these factors (other than \bar{Q}_l), say g_{1l} (then g_{1l} will be the minimal polynomial of $\text{in}_{\nu'} Q_l$ over $G_{\nu'}[\text{in}_{\nu'} Q_1, \dots, \text{in}_{\nu'} Q_{l-1}]$ for the valuation ν' we are about to construct). Let $\alpha_{l+1} = \deg_{\bar{Q}_l} g_{1l}$. Write

$$g_{1l} = \bar{Q}_l^{\alpha_{l+1}} + \sum_{j=0}^{\alpha_{l+1}-1} \left(\sum_{\gamma_l} \bar{c}_{l+1,j} \gamma_l \text{in}_{\nu'} \mathbf{Q}_l^{\gamma_l} \right) \bar{Q}_l^j, \quad (148)$$

If $t_l > 1$ or $\alpha_{l+1} > 1$, define **the $(l+1)$ -st key polynomial** of ν' to be a lifting

$$Q_{l+1} = Q_l^{\alpha_{l+1}} + \sum_{j=0}^{\alpha_{l+1}-1} \left(\sum_{\gamma_l} c_{l+1,j} \gamma_l \mathbf{Q}_l^{\gamma_l} \right) Q_l^j$$

(148) to L . If $t_l = \alpha_{l+1} = 1$, the $(l+1)$ -st key polynomial Q_{l+1} will also be a lifting of (148) to L , but we require it to satisfy additional conditions, as in §3. Let $\delta_l(f)$ be defined as in (66). Define the next key polynomials Q_{l+1}, Q_{l+2}, \dots , as in §3. More precisely, we define finitely many polynomials Q_{l+1}, \dots, Q_s if either $\text{char } K = 0$ or $\text{char } K = p > 0$ and we are in Case 1 of §3.

In Case 2, there exists an infinite sequence z_l, z_{l+1}, \dots of homogeneous standard expansions in \mathbf{Q}_l , not involving Q_l , such that the sequence $\{\nu'(Q_l + z_l + \dots + z_{l+t})\}_{t \in \mathbb{N}}$ is strictly increasing; pick and fix one such sequence. Define $Q_{l+t} = Q_l + z_l + z_{l+1} + \dots + z_{l+t-1}$ for $t \in \mathbb{N}$. For each key polynomial Q_i , write $f = \sum_{j=0}^{n_i} a_{ji} Q_i^j$ and consider the corresponding Newton polygon $\Delta_i(f)$. By definition of $\delta_i(f)$, the Newton polygon $\Delta_i(f)$ contains a vertex $(\nu'(a_{\delta_i(f)i}), \delta_i(f))$. Since $\delta_i(f) = \delta_{i+1}(f)$, the characteristic side A_i of $\Delta_i(f)$ is uniquely determined, that is, there exists a unique element $\beta_i \in \Gamma \cup \{\infty\}$ such that $\beta_i \geq \beta_{i'}$ for all $i' < i$, β_i determines a side A_i of $\Delta_i(f)$ and $(\nu'(a_{\delta_i}), \delta_i(f))$ is the leftmost endpoint of A_i . This defines an infinite sequence $\{Q_{l+t}\}_{t \in \mathbb{N}}$ of key polynomials, such that for each $i = l + t$, $t \in \mathbb{N}$, we have $\text{in}_i f = \text{in}_{\nu'} a_{\delta_i} (\bar{Q}_i + \text{in}_{\nu'} z_i)^{\delta_i(f)}$.

Let $\bar{\beta} = \lim_{t \rightarrow \infty} \nu'(Q_l + z_l + \cdots + z_{l+t})$. By definition, we are in Case 2a if $\bar{\beta} = \infty$ and in Case 2b if $\bar{\beta} < \infty$.

In Case 2b, define the next key polynomial to be a polynomial $Q_{l+\omega}$ satisfying the conclusion of Proposition 55. Note that in all the cases both the slope of the characteristic side L_i and the irreducible factor of $\text{in}_i f$ which is the minimal polynomial of $\text{in}_{\nu'} Q_i$ over $G_{\nu'}[\text{in}_{\nu'} \mathbf{Q}_i]^*$ are uniquely determined.

The algorithm stops if one of the following occurs: either $Q_i = 0$ or

$$\sup_i \{\beta_i\} = \infty,$$

where β_i ranges over the values of key polynomials defined so far. In both cases, the valuation ν' is completely determined by the data $\{Q_i, \beta_i\}$.

This completes our construction of the extensions ν' . Note that **every** choice described in the algorithm above leads to an extension ν' . Indeed, such a choice defines, in particular, the well ordered set $\{\nu_i\}_{i \in \Lambda}$ of valuations of $K[X]$ and their graded algebras; whenever $i < i'$, we have a natural homomorphism of graded algebras $G_{\nu_i} \rightarrow G_{\nu_{i'}}$. The proof of Theorem 62 applies verbatim to show that for each $h \in L$, the value $\nu_i(h(X))$ stabilizes for i sufficiently large. Setting $\nu'(h)$ to be that stable value of $\nu_i(h(X))$ defines a valuation ν' of L .

Corollary 66 *The extension ν' is unique if and only if, for each i in the above algorithm, the following two conditions hold:*

- (1) *The i -th Newton polygon $\Delta_i(f)$ has only one face L_i (other than the two axes).*
- (2) *The corresponding initial form $\text{in}_i f$ does not have two distinct irreducible factors (in other words, $\text{in}_i f$ is a power of an irreducible polynomial).*

The next Corollary is valid for valuations of arbitrary rank (and not only for those of rank 1).

Corollary 67 *Assume that $\text{in}_{\nu'} x$ has degree n over $G_{\nu'}$. Then ν admits a unique extension ν' to L .*

PROOF. By writing ν as a composition of several rank 1 valuations, it is sufficient to prove the Corollary under the assumption $rk \nu = 1$. Now, the hypotheses imply that (1) and (2) of Corollary 66 hold for $i = 1$. Moreover, we may take $f = Q_2$, so the algorithm consists of only one step, and the Corollary follows. \square

We end this paper with a discussion of the well known formula

$$\sum_{j=1}^t f_j e_j d_j = n, \quad (149)$$

where $\{\nu'_1, \dots, \nu'_t\}$ is the set of all the extensions of ν to L , f_j is the index of the value group of ν inside the value group of ν'_j , e_j is the degree of the residue field extension $k_\nu \rightarrow k_{\nu'_j}$ and d_j is the defect of ν'_j . Of course, for each j we have $f_j e_j = [G_{\nu'_j} : G_\nu]$. We associate to the above algorithm the following finite, oriented, weighted tree U . The set of vertices of U is partially ordered. In each vertex, we have a key polynomial Q_l appearing at some step in one of the branches of the above algorithm. The important data associated to this vertex is the data $\delta_l(f)$, as well as the data \mathbf{Q}_l of all the key polynomials preceding Q_l in the given branch of the algorithm. The set of vertices has a unique minimal element and the key polynomial associated to this minimal vertex is $x = Q_1$. Each vertex is adjacent to exactly one vertex smaller than itself and, possibly, to finitely many vertices greater than itself. Let us denote each vertex by the key polynomial Q_l associated to it. Not every key polynomial will be associated to a vertex of U . If l admits an immediate predecessor then the unique vertex adjacent to Q_l , preceding Q_l , is Q_{l-1} . Consider a vertex Q_l . We will now describe all the vertices following Q_l . There are two possibilities:

- (a) There is a unique β_l satisfying Condition (*) and Case 2b of §3 holds in the definition of Q_l .
- (b) Condition (a) does not hold.

In case (a), the unique vertex following Q_l is $Q_{l+\omega}$. In case (b), Q_l is followed by all the possible key polynomials Q_{l+1} , appearing in the above algorithm.

This information determines the tree U completely. It is obvious that U is finite.

Proposition 68 *Fix a vertex Q_l of U . Assume that Case (b) holds for Q_l and let $Q_{l+1}^{(1)}, \dots, Q_{l+1}^{(s)}$ denote all the vertices of U , adjacent to Q_l and following it. Let $\theta_l(f), \theta_{l+1}^{(1)}(f), \dots, \theta_{l+1}^{(s)}(f)$, and $\alpha_{l+1}^{(1)}, \dots, \alpha_{l+1}^{(s)}$ denote the numerical characters corresponding to the s resulting branches of the above algorithm. Then*

$$\sum_{j=1}^s \alpha_{l+1}^{(j)} \theta_{l+1}^{(j)}(f) = \theta_l(f). \quad (150)$$

PROOF. Let $A_l^{(1)}, \dots, A_l^{(t)}$ denote the sides of $\Delta_l(f)$ lying below the characteristic vertex $(\nu'(a_{\theta_l(f)}), \theta_l(f))$. For $1 \leq j \leq t$, let $\beta_l^{(j)}$ denote the element of Γ_+ which determines the side $A_l^{(j)}$ and let $\text{in}_l^{(j)} f$ denote the corresponding

initial form of f . By construction, renumbering the vertices $Q_{l+1}^{(j)}$, if necessary, we can find indices $1 \leq s_1 < \dots < s_t = s$ such that the factorization of $\text{in}_l^{(j)} f$ into irreducible factors has the form $\text{in}_l^{(j)} f = \bar{Q}^{u_j} \prod_{q=s_{j-1}+1}^{s_j} \text{in}_l^{(j)} (Q_{l+1}^{(q)})^{\theta_{l+1}^{(q)}}$, where the exponent u_j may or may not be zero (cf. Lemma 41 and (80)). Since $\theta_l(f)$ equals the sum of the heights of sides of $\Delta_l(f)$ lying below the characteristic vertex, we have $\theta_l = \sum_{j=1}^t \deg_{\bar{Q}} \prod_{q=s_{j-1}+1}^{s_j} \text{in}_l^{(j)} (Q_{l+1}^{(q)})^{\theta_{l+1}^{(q)}}$. Recalling that $\deg_{\bar{Q}} \text{in}_l Q_{l+1}^{(q)} = \alpha_{l+1}^{(q)}$ completes the proof of the Proposition. \square

If Case (a) holds for Q_l then the pivotal vertex of Δ_l is uniquely determined and coincides with the characteristic vertex. There is only one choice for the key polynomial $Q_{l+\omega}$ and, by definition,

$$\theta_l = \alpha_{l+\omega} \theta_{l+\omega}. \quad (151)$$

Thus, the analogue of the formula (150) holds also in the Case (a).

For each vertex Q_l of U , let $\alpha_l(Q_l)$ denote the integer α_l corresponding to Q_l in the above algorithm, and similarly for $\theta_l(Q_l)$. Fix a vertex Q_l of U and consider a subtree $U' \subset U$, having the following properties:

- (1) Q_l is the unique minimal element of U' .
- (2) For each vertex Q_i of U' , if U' contains one vertex immediately following Q_i then it contains all of them.

Let $\{Q_{l_1}, \dots, Q_{l_t}\}$ be the set of maximal elements among the vertices of U' .

Corollary 69 *We have*

$$\theta_l = \sum_{j=1}^t \left(\prod_{Q_{l'} \leq Q_{l_j}} \alpha_{l'}(Q_{l'}) \right) \theta_{l_j}(Q_{l_j}). \quad (152)$$

PROOF. This follows immediately from Proposition 68 and equation (151) by induction on the size of U' . \square

Let $\{\nu'_1, \dots, \nu'_s\}$ be the set of all the extensions of ν to L and take $U' = U$ in the above Corollary. Let $\{Q_{l_1}, \dots, Q_{l_s}\}$ be the set of maximal elements among the vertices of U . For each $j \in \{1, \dots, s\}$, consider the following partition of the set of all vertices Q_l of U such that $Q_l \leq Q_{l_j}$. We will say that such a Q_l belongs to the set D_j if Case (a) holds for the vertex immediately preceding

Q_l , and belongs to the set E_j otherwise. Noting that $\theta_1 = n$, we can now rewrite (152) as $n = \sum_{j=1}^t \left(\prod_{Q_{l'} \in D_j} \alpha_{l'}(Q_{l'}) \right) \left(\prod_{Q_{l'} \in E_j} \alpha_{l'}(Q_{l'}) \right) \theta_{l_j}(Q_{l_j})$.

Now, if $Q_{l'} \in E_j$ then the graded algebra extension

$$G_\nu[\text{in}_{\nu'} Q_{l'}] \hookrightarrow G_\nu[\text{in}_{\nu'} Q_{l'}][\text{in}_{\nu'} Q_{l'}]$$

has degree $\alpha_{l'}(Q_{l'})$. We can now interpret the formula (149) by observing that $\left(\prod_{Q_{l'} \in E_j} \alpha_{l'}(Q_{l'}) \right)$ equals the degree of the graded algebra extension

$$[G_{\nu'_j} : G_\nu] = e_j f_j,$$

whereas the quantity $\left(\prod_{Q_{l'} \in D_j} \alpha_{l'}(Q_{l'}) \right) \theta_{l_j}(Q_{l_j})$ is nothing but the defect of the extension ν'_j .

We refer the reader to Michel Vaquié's paper [12] for a detailed treatment of defect.

References

- [1] S. Abhyankar and T.T. Moh, *Newton–Puiseux expansion and generalized Tschirnhausen transformation I*, Reine Agew. Math., vol. 260, 1973, pp. 47–83
- [2] S. Abhyankar and T.T. Moh, *Newton–Puiseux expansion and generalized Tschirnhausen transformation II*, Reine Agew. Math. vol 261, 1973, pp. 29–54
- [3] J. Herrera, M.A. Olalla, M. Spivakovsky, B. Teissier, *Extending a valuation centered in a local domain to the formal completion*, in preparation.
- [4] T.C. Kuo, *Generalized Newton–Puiseux theory and Hensel's lemma in $\mathbb{C}[[x, y]]$* , Canadian J. Math. (6) XLI, 1989, pp. 1101–1116.
- [5] T.C. Kuo *A simple algorithm for deciding primes in $\mathbb{C}[[x, y]]$* , Canadian J. Math. 47 (4), 1995, pp. 801–816
- [6] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. J., 12:492–510 (1936).
- [7] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the AMS, 40:363–395 (1936).
- [8] S. MacLane and O.F.G Schilling, *Zero-dimensional branches of rank one on algebraic varieties*, Ann. of Math., 140, 3 (1939).

- [9] M. Vaquié, *Famille admise associée à une valuation de $K[x]$* , Séminaires et Congrès 10, edited by Jean-Paul Brasselet and Tatsuo Suwa, 2005, pp. 391–428.
- [10] M. Vaquié, *Extension d'une valuation*, to appear in Transactions of the AMS.
- [11] M. Vaquié, *Algèbre gradée associée à une valuation de $K[x]$* , to appear in Advanced Studies in Pure Mathematics, Progress in Algebraic Combinatorics.
- [12] M. Vaquié, *Défaut*, preprint.
- [13] O. Zariski, P. Samuel *Commutative Algebra, Vol. II*, Springer-Verlag (1960).