RESIDUAL IDEALS OF MACLANE VALUATIONS

JULIO FERNÁNDEZ, JORDI GUÀRDIA, JESÚS MONTES, AND ENRIC NART

Abstract. Let K be a field equipped with a discrete valuation v. In a pioneering work, MacLane determined all valuations on $K(x)$ extending v. His work was recently reviewed and generalized by Vaquié, by using the graded algebra of a valuation. We extend Vaquié's approach by studying residual ideals of the graded algebra as an abstract counterpart of certain residual polynomials which play a key role in the computational applications of the theory. As a consequence, we determine the structure of the graded algebra of the discrete valuations on $K(x)$ and we show how these valuations may be used to parameterize irreducible polynomials over local fields up to Okutsu equivalence.

Introduction

In a pioneering work, MacLane linked in 1936 the theory of discrete valuations on a field of rational functions in one variable with the study of irreducible polynomials over local fields. Several authors have proposed since then different approaches to either of these questions. In this paper, we show that MacLane's original approach, combined with some ideas of Montes and Vaquié, provides a unified insight for the main developments of these topics. Before describing the contents of the paper in more detail, let us briefly recall some milestones in these developments.

MacLane's solution to a problem raised by Ore. In the 1920's, Ore developed a method to construct the prime ideals of a number field, dividing a given prime number p, in terms of a defining polynomial $f \in \mathbb{Z}[x]$ satisfying a certain *p-regularity* condition [15, 16]. The idea was to detect a p-adic factorization of f according to the different irreducible factors of certain residual polynomials over finite fields, attached to the sides of a Newton polygon of f. He raised then the question of the existence of a procedure to compute the prime ideals in the p-irregular case, based on the consideration of similar Newton polygons and residual polynomials of *higher order*.

MacLane solved this problem in 1936 in a more general context [10, 11]. For an arbitrary discrete valued field (K, v), he described the valuations extending v to the rational function field $K(x)$. Then, given an irreducible polynomial $f \in K[x]$, he characterized all extensions of v to the field $L = K[x]/(f)$ as limits of infinite families of valuations on $K(x)$ whose value at f grows to infinity. Finally, he gave a criterion to decide when a valuation on $K(x)$ is sufficiently close to a valuation on L to uniquely represent it.

There is a natural extension μ_0 of v to $K(x)$ satisfying $\mu_0(x) = 0$. Starting from μ_0, MacLane constructed *inductive* valuations μ on $K(x)$ extending v, by the concatenation of augmentation steps

$$\mu_0 \xrightarrow{(\phi_1,\nu_1)} \mu_1 \xrightarrow{(\phi_2,\nu_2)} \cdots \xrightarrow{(\phi_{r-1},\nu_{r-1})} \mu_{r-1} \xrightarrow{(\phi_r,\nu_r)} \mu_r = \mu,$$

2010 *Mathematics Subject Classification.* Primary 13A18; Secondary 13J10, 12J10, 11S05.

Key words and phrases. key polynomial, MacLane chain, MacLane invariants, Newton polygon, Okutsu invariants, residual ideal, residual polynomial, valuation.

Partially supported by MTM2012-34611 and MTM2009-10359 from the Spanish MEC.

based on the choice of certain *key polynomials* $\phi_i \in K[x]$ and arbitrary positive rational numbers ν_i. In the case $K = \mathbb{Q}$, Ore's p-regularity condition is satisfied when all valuations on L extending the p-adic valuation v are sufficiently close to valuations on $K(x)$ that may be obtained from μ_0 by a single augmentation step.

After MacLane's work, inductive valuations were rediscovered and extensively studied as *residually transcendental extensions* of v to $K(x)$ [1, 17, 19]. In this approach, the valuations are first analyzed for algebraically closed fields, where they may be constructed as an augmentation of μ_0 with respect to a key polynomial of degree one. The general case is then deduced by descent.

Okutsu equivalence of prime polynomials. Let K_v be the completion of the field K at the discrete valuation v and let $\mathcal{O}_v$ be the valuation ring of K_v. We refer to monic irreducible polynomials in $\mathcal{O}_v[x]$ as *prime polynomials* (with respect to v).

For a global field K and a prime polynomial F, Okutsu constructed in 1982 an explicit integral basis of the local field $K_F = K_v[x]/(F)$, in terms of a finite sequence of prime polynomials $[\phi_1, \dots, \phi_r]$ which are a kind of optimal approximations to F with respect to their degree [14]. Such a family is called an *Okutsu frame* of F. The polynomials ϕ_i support certain numerical data, the so-called *Okutsu invariants* of F, containing considerable information about F and the field K_F.

An equivalence relation $\approx$ on the set $\mathbb{P}$ of prime polynomials can be defined as follows: given $F \in \mathbb{P}$ with Okutsu frame $[\phi_1, \dots, \phi_r]$, a polynomial $G \in \mathbb{P}$ of the same degree as F is said to be *Okutsu equivalent* to F if their resultant satisfies

$$v(\operatorname{Res}(G, F))/\deg G > v(\operatorname{Res}(\phi_r, F))/\deg \phi_r.$$

In this case, F and G have the same Okutsu invariants, and the fields K_F, K_G have isomorphic maximal tamely ramified subextensions [3].

In 1999, Montes carried out Ore's program in its original formulation [12, 5]. Given a finite extension L/K of number fields defined by an irreducible polynomial $f \in K[x]$, and given a prime ideal $\mathfrak{p}$ of K, Montes constructed the prime ideals of L lying over $\mathfrak{p}$ by finding polynomials in $K[x]$ which are Okutsu equivalent to the irreducible factors of f in $K_v[x]$, where v is the $\mathfrak{p}$-adic valuation. The method computes as well Okutsu frames and the Okutsu invariants of each prime factor. In this setting, the use of MacLane's valuations μ_i and Newton polygon operators is complemented with the introduction of residual polynomial operators $R_i \colon K[x] \longrightarrow \mathbb{F}_i[y]$, where $\mathbb{F}_i$ is a certain finite field, making the whole theory constructive and well suited to computational applications. These ideas led to the design of several fast algorithms to perform arithmetic tasks in global fields [2, 4, 6, 7, 9, 13].

Contents of this paper. In 2007, Vaquié reviewed and generalized MacLane's work [20, 21]. For an arbitrary valued field (K, v), not necessarily discrete, he determined all valuations μ on $K(x)$ extending v. The use of the graded algebras $\mathcal{G}r(\mu)$ attached to these valuations led Vaquié to a more elegant presentation of the theory.

In this paper, which only deals with discrete valuations, we carry out a double purpose. First, we extend Vaquié's approach by including a treatment of the residual polynomial operators attached to an inductive valuation μ on $K(x)$. The residual polynomials are then interpreted as generators of *residual ideals* in the degree-zero subring $\Delta(\mu)$ of the graded algebra $\mathcal{G}r(\mu)$. The residual ideal of a polynomial $g \in K[x]$ is defined as $\mathcal{R}_\mu(g) = H_\mu(g)\mathcal{G}r(\mu) \cap \Delta(\mu)$, where $H_\mu(g)$ is the image of g in the piece of degree $\mu(g)$ of the algebra. In sections 1 to 5, we review the properties of MacLane's inductive valuations, while making apparent the key role of the residual ideals in the whole theory. As an application of this point of view, in Theorem 4.7 we determine the structure of $\mathcal{G}r(\mu)$ as a graded algebra.

Our second aim is to show that this approach leads to a natural generalization of the results of Okutsu and Montes to arbitrary discrete valued fields. A prime polynomial F with respect to v induces a pseudo-valuation

$$\mu_{\infty,F}\colon K[x] \hookrightarrow K_v[x] \longrightarrow K_F \xrightarrow{v} \mathbb{Q}\cup\{\infty\},$$

by composition of the quotient map defined by F with the unique extension of v to the field K_F. According to MacLane's insight, approximating F by polynomials in $K[x]$ is equivalent to approximating $\mu_{\infty,F}$ by valuations on $K(x)$. In section 6 we introduce a canonical inductive valuation μ_F which is a threshold valuation in this approximation process, and we generalize most of the fundamental results of [3, 5, 12, 14, 18] with much shorter proofs. An Okutsu frame of F is seen to be just a family of key polynomials of an *optimal* chain of inductive valuations linking μ_0 with μ_F, and the Okutsu invariants of F are essentially the MacLane invariants of these valuations, introduced in section 3.

Finally, in section 7 we briefly recall MacLane's results on limits of inductive valuations and analyze in detail the interval $[\mu_0, \mu_{\infty,F})$ of all valuations μ on $K(x)$ such that $\mu_0(g) \le \mu(g) \le \mu_{\infty,F}(g)$ for all $g \in K[x]$. We prove that this interval is totally ordered and give an explicit description of the valuations therein.

The main result of the paper is Theorem 6.13, which establishes a canonical bijection between the set $\mathbb{P}/\approx$ of Okutsu equivalence classes of prime polynomials and the *MacLane space* $\mathbb{M}$ of the valued field (K, v), defined as the set of all pairs $(\mu, \mathcal{L})$, where μ is an inductive valuation on $K(x)$ and $\mathcal{L}$ is a *strong* maximal ideal of $\Delta(\mu)$. The bijection sends the class of F to the pair $(\mu_F, \mathcal{R}_{\mu_F}(F))$. This result reveals that MacLane's original approach is best suited for computational applications, because the elements in the set $\mathbb{M}$ may be described in terms of discrete parameters which are easily handled by a computer. As a consequence, all computational developments based on the Montes algorithm [4, 6, 7, 9, 13] admit a more elegant description and a natural extension to arbitrary discrete valued fields. The paper [8] is devoted to the discussion of these computational applications.

1. Augmentation of valuations

Let K be a field equipped with a discrete valuation $v\colon K^* \longrightarrow \mathbb{Z}$, normalized so that $v(K^*) = \mathbb{Z}$. Let $\mathcal{O}$ be the valuation ring of K, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ the residue class field.

Let K_v be the completion of K and let $v\colon \overline{K}_v \to \mathbb{Q}\cup\{\infty\}$ still denote the canonical extension of the valuation to a fixed algebraic closure of K_v. Let $\mathcal{O}_v$ be the valuation ring of K_v, $\mathfrak{m}_v$ its maximal ideal and $\mathbb{F}_v = \mathcal{O}_v/\mathfrak{m}_v$ the residue class field. The canonical inclusion $K \subset K_v$ restricts to inclusions $\mathcal{O} \subset \mathcal{O}_v$, $\mathfrak{m} \subset \mathfrak{m}_v$, which determine a canonical isomorphism $\mathbb{F} \simeq \mathbb{F}_v$. We consider this isomorphism as an identity, $\mathbb{F} = \mathbb{F}_v$, and indicate simply with a bar, $\overline{}\colon \mathcal{O}_v[x] \longrightarrow \mathbb{F}[x]$, the canonical homomorphism of reduction of polynomials modulo $\mathfrak{m}_v$.

Our aim is to describe all extensions of v to discrete valuations on the field $K(x)$, where x is an indeterminate.

Definition 1.1. *Let $\mathbb{V}$ be the set of discrete valuations, $\mu\colon K(x)^* \longrightarrow \mathbb{Q}$, such that $\mu_{|K} = v$ and $\mu(x) \ge 0$. For any $\mu \in \mathbb{V}$, we use the following notation:*

- *$\Gamma(\mu) = \mu\left(K(x)^*\right) \subset \mathbb{Q}$ for the cyclic group of finite values of μ. The* ramification index *of μ is the positive integer $e(\mu)$ such that $e(\mu)\Gamma(\mu) = \mathbb{Z}$.*
- *$\kappa(\mu)$ for the residue class field of μ.*

From now on, the elements of $\mathbb{V}$ will be called simply valuations.

Since we are only interested in (rank one) discrete valuations, we can assume that all valuations are $\mathbb{Q}$-valued. Furthermore, the assumption $\mu(x) \ge 0$ is not essential; it gives a more compact form to the presentation of the results. For the determination of the discrete valuations μ with $\mu(x) < 0$ one may simply replace x with $1/x$ as a generator of the field $K(x)$ over K.

In the set $\mathbb{V}$ there is a natural partial ordering:

$$\mu \le \mu' \quad \text{if} \quad \mu(g) \le \mu'(g), \ \forall\, g \in K[x].$$

Consider the valuation $\mu_0 \in \mathbb{V}$ acting on polynomials as follows:

$$\mu_0\left(\sum\nolimits_{0\le s} a_s x^s\right) = \min_{0\le s}\left\{v(a_s)\right\}.$$

Clearly, $\mu_0 \le \mu$ for all $\mu \in \mathbb{V}$; in other words, μ_0 is the minimum element in $\mathbb{V}$.

1.1. **Graded algebra of a valuation.** Let $\mu \in \mathbb{V}$ be a valuation. For any $\alpha \in \Gamma(\mu)$ we consider the following $\mathcal{O}$-submodules in $K[x]$:

$$\mathcal{P}_\alpha = \mathcal{P}_\alpha(\mu) = \{g \in K[x] \mid \mu(g) \ge \alpha\} \supset \mathcal{P}_\alpha^+ = \mathcal{P}_\alpha^+(\mu) = \{g \in K[x] \mid \mu(g) > \alpha\}.$$

Clearly, $\mathcal{P}_0$ is a subring of $K[x]$, and $\mathcal{P}_\alpha$, $\mathcal{P}_\alpha^+$ are $\mathcal{P}_0$-submodules of $K[x]$ for all α.

The *graded algebra of* μ is the integral domain:

$$\mathcal{G}r(\mu) := \bigoplus\nolimits_{\alpha\in\Gamma(\mu)} \mathcal{P}_\alpha/\mathcal{P}_\alpha^+.$$

Let $\Delta(\mu) = \mathcal{P}_0/\mathcal{P}_0^+$ be the subring determined by the piece of degree zero of this algebra. Clearly, $\mathcal{O} \subset \mathcal{P}_0$ and $\mathfrak{m} = \mathcal{P}_0^+ \cap \mathcal{O}$; thus, there is a canonical homomorphism $\mathbb{F} \to \Delta(\mu)$, equipping $\Delta(\mu)$ (and $\mathcal{G}r(\mu)$) with a canonical structure of $\mathbb{F}$-algebra.

Let $\mathcal{O}_\mu \subset K(x)$ be the valuation ring of μ and let $\mathfrak{m}_\mu$ be its maximal ideal. Since $\mathcal{P}_0 = K[x] \cap \mathcal{O}_\mu$ and $\mathcal{P}_0^+ = K[x] \cap \mathfrak{m}_\mu$, we have an embedding $\Delta(\mu) \hookrightarrow \kappa(\mu)$. As we see in section 3, this embedding identifies $\kappa(\mu)$ with the field of fractions of $\Delta(\mu)$.

There is a natural map $H_\mu\colon K[x] \longrightarrow \mathcal{G}r(\mu)$, given by $H_\mu(0) = 0$, and

$$H_\mu(g) = g + \mathcal{P}_{\mu(g)}^+ \in \mathcal{P}_{\mu(g)}/\mathcal{P}_{\mu(g)}^+,$$

for $g \ne 0$. Note that $H_\mu(g) = 0$ if and only if $g = 0$. For all $g, h \in K[x]$ we have:

$$\begin{aligned} &H_\mu(gh) = H_\mu(g)H_\mu(h),\\ &H_\mu(g+h) = H_\mu(g) + H_\mu(h), \text{ if } \mu(g) = \mu(h) = \mu(g+h). \end{aligned} \tag{1}$$

For a valuation μ' with $\mu \le \mu'$, a canonical homomorphism of graded algebras $\mathcal{G}r(\mu) \to \mathcal{G}r(\mu')$ is determined by $g + \mathcal{P}_\alpha^+(\mu) \mapsto g + \mathcal{P}_\alpha^+(\mu')$ for all g, α with $\mu(g) \ge \alpha$. The image of $H_\mu(g)$ is $H_{\mu'}(g)$ if $\mu(g) = \mu'(g)$, and zero otherwise.

Definition 1.2.

We say that $g, h \in K[x]$ are μ-equivalent, *and we write $g \sim_\mu h$, if $H_\mu(g) = H_\mu(h)$. Thus, $g \sim_\mu h$ if and only if $\mu(g-h) > \mu(g) = \mu(h)$ or $g = h = 0$.*

We say that g is μ-divisible *by h, and we write $h \mid_\mu g$, if $H_\mu(g)$ is divisible by $H_\mu(h)$ in $\mathcal{G}r(\mu)$. Thus, $h \mid_\mu g$ if and only if $g \sim_\mu hf$ for some $f \in K[x]$.*

We say that $\phi \in K[x]$ is μ-irreducible if $H_\mu(\phi)\mathcal{G}r(\mu)$ is a non-zero prime ideal.

We say that $\phi \in K[x]$ is μ-minimal if $\phi \nmid_\mu g$ for any non-zero $g \in K[x]$ with $\deg g < \deg \phi$.

Lemma 1.3. *Let $\phi \in K[x]$ be a non-constant polynomial and let $g = \sum_{0\le s} a_s\phi^s$, $\deg a_s < \deg \phi$, be the canonical ϕ-expansion of $g \in K[x]$. The following conditions are equivalent:*

(1) *ϕ is μ-minimal*
(2) *For any $g \in K[x]$, $\mu(g) = \min\{\mu(a_0), \mu(g - a_0)\}$.*
(3) *For any $g \in K[x]$, $\mu(g) = \min_{0\le s}\{\mu(a_s\phi^s)\}$.*
(4) *For any non-zero $g \in K[x]$, $\phi \nmid_\mu g$ if and only if $\mu(g) = \mu(a_0)$.*

Proof. Write $g-a_0=\phi q$ with $q\in K[x]$. If $\mu(g)>\mu(a_0)$, which is equivalent to $\mu(g)>\mu(\phi q)$, then $a_0\sim_\mu -\phi q$ and $\phi\mid_\mu a_0$. Hence, (1) implies (2).

An inductive argument shows that (2) implies (3). Let us now deduce (4) from (3). For any non-zero $g\in K[x]$, (3) implies $\mu(g)\le\mu(a_0)$. If $\mu(g)<\mu(a_0)$, then $g\sim_\mu \sum_{0<s}a_s\phi^s$, so $\phi\mid_\mu g$. Conversely, if $g\sim_\mu \phi q$ for some $q\in K[x]$, then $\mu(g)<\mu(g-\phi q)\le\mu(a_0)$ again by (3), since a_0 is still the 0-th coefficient of the ϕ-expansion of $g-\phi q$. Finally, (4) implies (1) because $g=a_0$ if $\deg g<\deg\phi$. □

The property of μ-minimality is not stable under μ-equivalence. For instance, if g is μ-minimal and $\mu(g)>0$, then $g+g^2\sim_\mu g$ and $g+g^2$ is not μ-minimal. However, for μ-equivalent polynomials of the same degree, μ-minimality is clearly preserved.

For the minimal valuation μ_0 there is a canonical isomorphism $\Delta(\mu_0)\to\mathbb{F}[x]$ sending $H_{\mu_0}(g)$ to $\overline{g}$; thus, $\mathcal{G}r(\mu_0)\simeq\bigoplus_{\alpha\in\mathbb{Z}}H_{\mu_0}(\pi)^\alpha\mathbb{F}[x]$. Also, $g\in K[x]$ is μ_0-minimal if and only if $\mu_0(g)$ is the value of v at the leading coefficient of g. Thus, in the set of monic polynomials of $K[x]$, the μ_0-minimal ones are those lying in $\mathcal{O}[x]$.

1.2. **Key polynomials and augmented valuations.** A *key polynomial* for the valuation μ is a monic polynomial in $K[x]$ which is μ-minimal and μ-irreducible.

Let $\mathrm{KP}(\mu)$ be the set of key polynomials for μ. For instance, $\mathrm{KP}(\mu_0)$ is the set of all monic polynomials $g\in\mathcal{O}[x]$ such that $\overline{g}$ is irreducible in $\mathbb{F}[x]$.

Since μ-minimality is not stable under μ-equivalence, the property of being a key polynomial is not stable under μ-equivalence. However, for polynomials of the same degree this stability is clear.

Lemma 1.4. *Let ϕ be a key polynomial for μ, and $g\in K[x]$ a monic polynomial such that $\phi\mid_\mu g$ and $\deg g=\deg\phi$. Then, $\phi\sim_\mu g$ and g is a key polynomial for μ.*

Proof. The ϕ-expansion of g is of the form $g=a_0+\phi$, with $\deg a_0<\deg\phi$. By item (4) of Lemma 1.3, we have $\mu(g)<\mu(a_0)$, so that $H_\mu(g)=H_\mu(\phi)$. In particular, g is μ-irreducible and, since $\deg g=\deg\phi$, it is μ-minimal too. □

Definition 1.5. *For $\phi\in\mathrm{KP}(\mu)$ and a non-zero $g\in K[x]$, we let $\operatorname{ord}_{\mu,\phi}(g)$ denote the largest integer s such that $\phi^s\mid_\mu g$, namely the order with which the prime $H_\mu(\phi)$ divides $H_\mu(g)$ in $\mathcal{G}r(\mu)$. Accordingly, we set $\operatorname{ord}_{\mu,\phi}(0):=\infty$, and we have*

$$\operatorname{ord}_{\mu,\phi}(gh)=\operatorname{ord}_{\mu,\phi}(g)+\operatorname{ord}_{\mu,\phi}(h),\quad \textit{for all } g,h\in K[x]. \tag{2}$$

The map $\operatorname{ord}_{\mu,\phi}$ induces a group homomorphism $K(x)^*\to\mathbb{Z}$, but it is not a valuation. For instance, if $n>\mu(\phi)$, then $\operatorname{ord}_{\mu,\phi}(\phi)=1=\operatorname{ord}_{\mu,\phi}(\phi+\pi^n)$ but $\operatorname{ord}_{\mu,\phi}(\pi^n)=0$. However, as a consequence of (1),

$$\operatorname{ord}_{\mu,\phi}(g+h)\ge\min\{\operatorname{ord}_{\mu,\phi}(g),\operatorname{ord}_{\mu,\phi}(h)\} \tag{3}$$

whenever $\mu(g)=\mu(h)=\mu(g+h)$, and equality holds if $\operatorname{ord}_{\mu,\phi}(g)\ne\operatorname{ord}_{\mu,\phi}(h)$.

Definition 1.6. *Take $\phi\in\mathrm{KP}(\mu)$ and $\nu\in\mathbb{Q}_{>0}$. The augmented valuation of μ with respect to these data is the valuation μ' determined by the following action on $K[x]$:*

- *$\mu'(a)=\mu(a)$, if $\deg a<\deg\phi$.*
- *$\mu'(\phi)=\mu(\phi)+\nu$.*
- *If $g=\sum_{0\le s}a_s\phi^s$ is the ϕ-expansion of g, then $\mu'(g)=\min_{0\le s}\{\mu'(a_s\phi^s)\}$.*

Equivalently, $\mu'(g)=\min_{0\le s}\{\mu(a_s\phi^s)+s\nu\}$. We use the notation $\mu'=[\mu;(\phi,\nu)]$.

Proposition 1.7. [10, Thms. 4.2,5.1], [11, Lem. 4.3], [20, Thm. 1.2, Props. 1.3,1.5]

1. *The natural extension of μ' to $K(x)$ is a valuation on this field and $\mu\le\mu'$.*
2. *For a non-zero $g\in K[x]$, $\mu(g)=\mu'(g)$ if and only if $\phi\nmid_\mu g$. That is, the kernel of the canonical map $\mathcal{G}r(\mu)\to\mathcal{G}r(\mu')$ is the principal prime ideal $H_\mu(\phi)\,\mathcal{G}r(\mu)$.*

(3) *The value group* $\Gamma(\mu')$ *is the subgroup of* $\mathbb{Q}$ *generated by* $\mu'(\phi)$ *and the subset* $\Gamma_\phi(\mu) := \{\mu(a) \mid a \in K[x],\ a \neq 0,\ \deg a < \deg \phi\} \subset \Gamma(\mu)$.

(4) *The polynomial* ϕ *is a key polynomial for* μ'. $\square$

The group $\Gamma(\mu')$ does not necessarily contain $\Gamma(\mu)$. For instance, for the valuations

$$\mu = [\mu_0; (x, 1/2)], \qquad \mu' = [\mu; (x, 1/2)] = [\mu_0; (x, 1)],$$

we have $\Gamma(\mu) = (1/2)\mathbb{Z}$, which is larger than $\Gamma(\mu') = \mathbb{Z}$.

Lemma 1.8. *Every* $\phi \in \mathrm{KP}(\mu)$ *is irreducible in* $K_v[x]$.

Proof. Suppose $\phi = gh$ for two monic polynomials $g, h \in K_v[x]$. Then, for any positive integer n, there exist polynomials $g_n, h_n \in K[x]$ such that $\phi \equiv g_n h_n \pmod{\mathfrak{m}^n}$ and $\deg g_n = \deg g$, $\deg h_n = \deg h$. By taking n large enough, we get $\phi \sim_\mu g_n h_n$ and, by the μ-irreducibility of ϕ, then $\phi \mid_\mu g_n$ or $\phi \mid_\mu h_n$. By the μ-minimality of ϕ, this implies $\deg \phi \leq \deg g_n$ or $\deg \phi \leq \deg h_n$. Thus, necessarily $\phi = g$ or $\phi = h$. $\square$

Let ϕ be a key polynomial for μ. Choose a root $\theta \in \overline{K}_v$ of ϕ and let $K_\phi = K_v(\theta)$ stand for the finite extension of K_v generated by θ. Also, let $\mathcal{O}_\phi \subset K_\phi$ be the valuation ring of K_ϕ, $\mathfrak{m}_\phi$ its maximal ideal and $\mathbb{F}_\phi = \mathcal{O}_\phi/\mathfrak{m}_\phi$ the residue class field.

The ramification index $e(\phi)$ and the residual degree $f(\phi)$ of the extension K_ϕ/K_v do not depend on the choice of θ and satisfy $\deg \phi = [K_\phi\colon K_v] = e(\phi)f(\phi)$.

Let $\mu_{\infty,\phi}$ be the pseudo-valuation on $K[x]$ obtained as the composition:

$$\mu_{\infty,\phi}\colon K[x] \hookrightarrow K_v[x] \longrightarrow K_\phi \xrightarrow{v} \mathbb{Q} \cup \{\infty\},$$

the second mapping being determined by $x \mapsto \theta$. This pseudo-valuation does not depend on the choice of θ as a root of ϕ.

We recall that a pseudo-valuation has the same properties than a valuation, except for the fact that the pre-image of ∞ is a prime ideal which is not necessarily zero. For $\mu_{\infty,\phi}$ this prime ideal is the principal ideal $\phi K[x]$.

Consider now the pseudo-valuation $\mu^*\colon K[x] \longrightarrow \mathbb{Q}\cup\{\infty\}$, where $\mu^* = [\mu; (\phi, \infty)]$ is given as in Definition 1.6 but taking $\nu = \infty$. The preimage of ∞ under μ^* is also the maximal ideal $\phi K[x]$.

Both $\mu_{\infty,\phi}$ and μ^* induce a valuation on the quotient field $K[x]/\phi K[x]$. These two induced valuations coincide because the valuation v on K admits a unique extension to that field, by Lemma 1.8. This implies $\mu_{\infty,\phi} = \mu^*$, and we have the following analogue of Proposition 1.7.

Proposition 1.9. *If* ϕ *is a key polynomial for* μ, *then*

(1) $\mu \leq \mu_{\infty,\phi}$ *and, for a non-zero* $g \in K[x]$, $\mu(g) = \mu_{\infty,\phi}(g)$ *if and only if* $\phi \nmid_\mu g$.

(2) $v(K_\phi^*) = \Gamma_\phi(\mu) = \{\mu(a) \mid a \in K[x],\ a \neq 0,\ \deg a < \deg \phi\} \subset \Gamma(\mu)$. $\square$

Every element in K_ϕ^* can be expressed as $h(\theta)$ for some non-zero $h \in K_v[x]$ with $\deg h < \deg \phi$. Then, if $g \in K[x]$ has $\deg g = \deg h$ and is sufficiently close to h in the v-adic topology, we have $v(h(\theta)) = v(g(\theta)) = \mu(g) \in \Gamma_\phi(\mu)$. This justifies the second item of Proposition 1.9.

Corollary 1.10. $\mathrm{KP}(\mu) \subset \mathcal{O}[x]$.

Proof. Take $\phi \in \mathrm{KP}(\mu)$ and a root $\theta \in \overline{K}_v$ of ϕ. Since $0 \leq \mu(x) \leq \mu_{\infty,\phi}(x) = v(\theta)$, the root θ belongs to $\mathcal{O}_\phi$ and its minimal polynomial ϕ over K_v must have coefficients in $\mathcal{O}_v \cap K = \mathcal{O}$. $\square$

The next result is a kind of partial converse to Propositions 1.7 and 1.9.

Lemma 1.11. [20, Thm. 1.15] *Let μ be a valuation and let μ^* be a pseudo-valuation on $K[x]$ extending v such that $\mu < \mu^*$. Let $\phi \in K[x]$ be a monic polynomial with minimal degree satisfying $\mu(\phi) < \mu^*(\phi)$. Then, ϕ is a key polynomial for μ and, for any non-zero $g \in K[x]$, the equality $\mu(g) = \mu^*(g)$ is equivalent to $\phi \nmid_\mu g$. Moreover, for $\nu = \mu^*(\phi) - \mu(\phi) \in \mathbb{Q}_{>0} \cup \{\infty\}$, we have $\mu < [\mu; (\phi, \nu)] \leq \mu^*$.* □

1.3. **Residual ideals of polynomials.** Let μ be a valuation. Put $\Delta = \Delta(\mu)$, and let $I(\Delta)$ be the set of ideals in Δ. Consider the *residual ideal operator*:

$$\mathcal{R} = \mathcal{R}_\mu \colon K[x] \longrightarrow I(\Delta), \qquad g \mapsto \Delta \cap H_\mu(g)\mathcal{G}r(\mu).$$

In sections 4 and 5 we shall study in more detail this operator $\mathcal{R}$, which translates questions about $K[x]$ and μ into ideal-theoretic considerations in the ring Δ. Let us now see that $\mathcal{R}$ attaches a maximal ideal of Δ to any key polynomial for μ.

Proposition 1.12. *If ϕ is a key polynomial for μ, then*

1. *$\mathcal{R}(\phi)$ is the kernel of the onto ring homomorphism $\Delta \twoheadrightarrow \mathbb{F}_\phi$ determined by $g(x) + \mathcal{P}_0^+ \mapsto g(\theta) + \mathfrak{m}_\phi$. In particular, $\mathcal{R}(\phi)$ is a maximal ideal of Δ.*
2. *$\mathcal{R}(\phi)$ is the kernel of the homomorphism $\Delta \to \Delta(\mu')$ attached to any augmented valuation $\mu' = [\mu; (\phi, \nu)]$. In particular, the image of $\Delta \to \Delta(\mu')$ is a field, canonically isomorphic to $\mathbb{F}_\phi$.*

Proof. If $g \in \mathcal{P}_0$, we have $v(g(\theta)) \geq \mu(g) \geq 0$, and $g(\theta) \in \mathcal{O}_\phi$. Thus, we get a well-defined ring homomorphism $\mathcal{P}_0 \to \mathbb{F}_\phi$. This map is onto, because every element in $\mathbb{F}_\phi$ can be represented as $h(\theta) + \mathfrak{m}_\phi$ for some $h \in K[x]$, with $\deg h < \deg \phi$ and $v(h(\theta)) \geq 0$. Proposition 1.9 shows that $\mu(h) = v(h(\theta)) \geq 0$, so that h belongs to $\mathcal{P}_0$. Finally, if $g \in \mathcal{P}_0^+$, then $v(g(\theta)) \geq \mu(g) > 0$; thus, the above homomorphism vanishes on $\mathcal{P}_0^+$ and it induces an onto map $\Delta \twoheadrightarrow \mathbb{F}_\phi$, whose kernel is $\mathcal{R}(\phi)$ by Proposition 1.9. Item (2) is a consequence of Proposition 1.7 and item (1). □

2. Newton polygons

The choice of a key polynomial ϕ for a valuation μ determines a *Newton polygon operator*

$$N_{\mu,\phi} \colon K[x] \longrightarrow 2^{\mathbb{R}^2},$$

where $2^{\mathbb{R}^2}$ is the set of subsets of the euclidean plane $\mathbb{R}^2$. The Newton polygon of the zero polynomial is the empty set. If $g = \sum_{0 \leq s} a_s \phi^s$ is the canonical ϕ-expansion of a non-zero $g \in K[x]$, then $N_{\mu,\phi}(g)$ is the lower convex hull of the cloud of points $(s, \mu(a_s\phi^s))$ for all $0 \leq s$ (see Fig.1). Note that the rational number $\mu(g)$ is the lowest ordinate of all points in the polygon, by Lemma 1.3.

The *length* $\ell(N)$ of a Newton polygon N is the abscissa of its right end point. If N is not a single point, we formally write $N = S_1 \vdash \cdots \vdash S_k$, where S_i are the sides of N ordered by their (different) increasing slopes. The left and right end points of N and the points joining two sides are the *vertices* of N.

We are mostly interested in the *principal Newton polygon* $N^-_{\mu,\phi}(g)$ formed by the sides of $N_{\mu,\phi}(g)$ with negative slope. If there are no sides of negative slope, then $N^-_{\mu,\phi}(g)$ is the left end point of $N_{\mu,\phi}(g)$. The length of $N^-_{\mu,\phi}(g)$ codifies the power of the prime $H_\mu(\phi)$ dividing $H_\mu(g)$ in the graded algebra $\mathcal{G}r(\mu)$.

Lemma 2.1. *For every non-zero polynomial $g \in K[x]$, $\ell(N^-_{\mu,\phi}(g)) = \operatorname{ord}_{\mu,\phi}(g)$.*

Proof. If $\operatorname{ord}_{\mu,\phi}(g) = 0$, then the equality holds by item (4) of Lemma 1.3. Otherwise, take $h \in K[x]$ with $g \sim_\mu \phi h$. Since $\ell(N^-_{\mu,\phi}(g)) = \ell(N^-_{\mu,\phi}(\phi h)) = \ell(N^-_{\mu,\phi}(h)) + 1$ and $\operatorname{ord}_{\mu,\phi}(g) = \operatorname{ord}_{\mu,\phi}(\phi h) = \operatorname{ord}_{\mu,\phi}(h) + 1$, the result follows by induction. □

FIGURE 1. Newton polygon of $g \in K[x]$

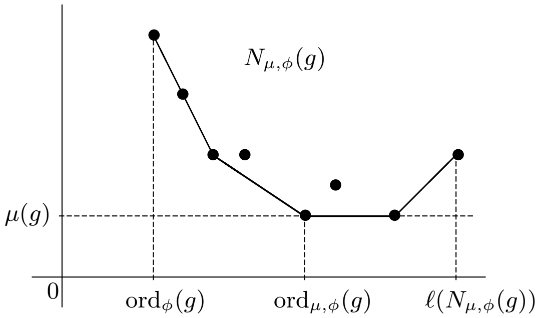
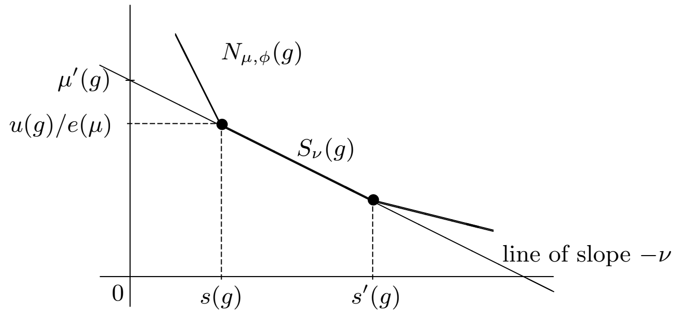


FIGURE 2. ν-component of $N_{\mu,\phi}(g)$ for a polynomial $g \in K[x]$.



For the rest of the section we fix an augmented valuation $\mu' = [\mu; (\phi, \nu)]$ with respect to the key polynomial ϕ and a positive rational number ν. By Proposition 1.7, ϕ is a key polynomial for μ'. So it makes sense to consider the Newton polygon $N_{\mu',\phi}(g)$, which is related to $N_{\mu,\phi}(g)$ as follows, due to the formula $\mu'(a_s\phi^s) = \mu(a_s\phi^s) + s\nu$.

Lemma 2.2. *Let $\mathcal{H}\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the affine transformation $\mathcal{H}(x, y) = (x, y + \nu x)$. Then, $N_{\mu',\phi}(g) = \mathcal{H}(N_{\mu,\phi}(g))$.* □

The affinity $\mathcal{H}$ acts as a translation on every vertical line, so a side S of $N_{\mu,\phi}(g)$ is mapped to a side of $N_{\mu',\phi}(g)$ whose end points have the same abscissas as those of S. Moreover, $\mathcal{H}$ maps a line of slope ρ to a line of slope $\rho+\nu$ and keeps the vertical axis pointwise invariant. This leads to the next result, which allows to read the value $\mu'(g)$ on the Newton polygon $N_{\mu,\phi}(g)$ (see Fig.2).

Corollary 2.3. *For any non-zero $g \in K[x]$, the line of slope $-\nu$ which first touches the polygon $N_{\mu,\phi}(g)$ from below has ordinate $\mu'(g)$ at the vertical axis.*

Proof. The statement follows from Lemma 2.2 taking into account that $\mu'(g)$ is the ordinate of the intersection point of the vertical axis with the line of slope zero which first touches the polygon $N_{\mu',\phi}(g)$ from below (see Fig.1). □

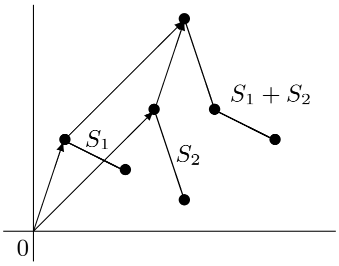
Definition 2.4. *For a non-zero $g \in K[x]$, the ν-*component *of $N_{\mu,\phi}(g)$ is the intersection of this polygon with the line of slope $-\nu$ which first touches it from below:*

$$S_\nu(g) := S_{\mu'}(g) := \{(x, y) \in N_{\mu,\phi}(g) \mid y + \nu x \text{ is minimal}\}. \qquad \text{(see Fig.2)}$$

Let $s(g) = s_{\mu'}(g) \le s'(g) = s'_{\mu'}(g)$ be the abscissas of the end points of $S_\nu(g)$, and $u(g) = u_{\mu'}(g)$ be the integer such that $(s(g), u(g)/e(\mu))$ is the left end point of $S_\nu(g)$.

According to MacLane's terminology, $s'(g)$ is the *effective degree* of g and $s'(g) - s(g)$ is the *projection* of g, with respect to the augmented valuation μ' [11, Secs. 3,4].

FIGURE 3. Addition of two plane segments



If $N_{\mu,\phi}(g)$ has a side S of slope $-\nu$, then $S_\nu(g)=S$. Otherwise, $S_\nu(g)$ is a vertex and $s(g)=s'(g)$. Since the affinity $\mathcal{H}$ in Lemma 2.2 maps $S_\nu(g)$ to the side of slope zero of $N_{\mu',\phi}(g)$, the ν-component is an invariant of the μ'-equivalence class of g:

Lemma 2.5. *For non-zero $g,h\in K[x]$, we have $S_\nu(g)=S_\nu(h)$ whenever $g\sim_{\mu'}h$.* $\square$

The vertex abscissas $s(g)$ and $s'(g)$ have also an algebraic meaning, in an analogous way to the length of the principal polygon $N^-_{\mu,\phi}(g)$.

Lemma 2.6. *For a non-zero $g\in K[x]$, the following holds:*
(1) *$s(g)=\operatorname{ord}_{\mu',\phi}(g)$.*
(2) *$s'(g)=\operatorname{ord}_{\mu'',\phi}(g)$, where $\mu''=[\mu;(\phi,\nu-\epsilon)]$ for a sufficiently small $\epsilon\in\mathbb{Q}_{>0}$.*

Proof. The first item is obtained from Lemma 2.1, since $s(g)=\ell(N^-_{\mu',\phi}(g))$ by the above remark on $\mathcal{H}(S_\nu(g))$. Now, the right end point of $S_\nu(g)$ equals the left end point of $S_{\nu-\epsilon}(g)$ if $\epsilon\in\mathbb{Q}_{>0}$ is small enough, so the second item comes from the first. $\square$

There is a natural addition of segments in the plane. We admit that a point is a segment whose right and left end points coincide. The sum S_1+S_2 of two plane segments is the ordinary vector sum if at least one of the segments is a single point. Otherwise, S_1+S_2 is the Newton polygon whose left end point is the vector sum of the two left end points of S_1,S_2 and whose sides are the join of S_1 and S_2 considered with increasing slopes from left to right (see Fig.3).

Corollary 2.7. *For non-zero $g,h\in K[x]$, we have $S_\nu(gh)=S_\nu(g)+S_\nu(h)$.*

Proof. Since the involved segments have either the same slope or length zero, the statement is equivalent to the equalities

$$s(gh)=s(g)+s(h),\quad s'(gh)=s'(g)+s'(h)\quad\text{and}\quad u(gh)=u(g)+u(h).$$

The first two equalities follow from equation (2) and Lemma 2.6. In order to prove the third, let $g=\sum_{0\le s}a_s\phi^s$, $h=\sum_{0\le t}b_t\phi^t$ be the ϕ-expansions of g,h and set $s_0=s(g)$, $t_0=s(h)$, $g^*=\sum_{s_0\le s}a_s\phi^s$, $h^*=\sum_{t_0\le t}b_t\phi^t$. Since $g^*\sim_{\mu'}g$, $h^*\sim_{\mu'}h$, we may suppose $g=g^*$, $h=h^*$. The left end point of $S_\nu(gh)$ has abscissa $s(gh)=s_0+t_0$ and the (s_0+t_0)-th term of the ϕ-expansion of gh is the remainder c of the division $a_{s_0}b_{t_0}=\phi q+c$. Since $\phi\nmid_\mu a_{s_0}b_{t_0}$, Lemma 1.3 shows that $\mu(a_{s_0}b_{t_0})=\mu(c)$. Thus, $\mu(c\,\phi^{s_0+t_0})=\mu(a_{s_0}\phi^{s_0})+\mu(b_{t_0}\phi^{t_0})$, which amounts to $u(gh)=u(g)+u(h)$. $\square$

The addition of segments may be extended to an addition law for Newton polygons. Given two polygons $N=S_1\vdash\cdots\vdash S_k$, $N'=S'_1\vdash\cdots\vdash S'_{k'}$, the left end point of the sum $N+N'$ is the vector sum of the left end points of N and N', whereas the sides of $N+N'$ are obtained by joining all sides in the multiset $\left\{S_1,\dots,S_k,S'_1,\dots,S'_{k'}\right\}$ ordered by increasing slopes [5, Sec. 1]. As an immediate consequence of Corollary 2.7, we get the *theorem of the product* for Newton polygons.

Theorem 2.8. *Let ϕ be a key polynomial for the valuation μ. Then, for any non-zero $g,h\in K[x]$ we have $N^-_{\mu,\phi}(gh)=N^-_{\mu,\phi}(g)+N^-_{\mu,\phi}(h)$.* ☐

The analogous statement for entire Newton polygons is false. For instance, consider $g,h\in K[x]$ such that $\deg g$, $\deg h<\deg\phi$ and $\deg gh\ge\deg\phi$; then, both $N_{\mu,\phi}(g)$ and $N_{\mu,\phi}(h)$ are a single point, while $N_{\mu,\phi}(gh)$ has a side of length one.

We now apply these Newton polygon techniques to obtain a characterization of the units in $\mathcal{G}r(\mu')$ and a criterion for μ'-minimality in terms of ϕ-expansions.

Lemma 2.9. *For any non-zero $g\in K[x]$, the following conditions are equivalent:*

1. *$H_{\mu'}(g)$ is a unit in $\mathcal{G}r(\mu')$.*
2. *$S_\nu(g)$ is a single point of abscissa zero, that is, $s(g)=s'(g)=0$.*
3. *$g\sim_{\mu'}a$ for some $a\in K[x]$ with $\deg a<\deg\phi$.*

These conditions hold if $\phi\nmid_\mu g$, namely if $\mu(g)=\mu'(g)$.

Proof. Item (2) can be deduced from (1) by using Lemma 2.5 and Corollary 2.7. Indeed, if $gh\sim_{\mu'}1$ for some $h\in K[x]$, then $S_\nu(g)+S_\nu(h)=S_\nu(gh)=S_\nu(1)=\{(0,0)\}$, so $S_\nu(g)$ must be a single point of abscissa zero.

Clearly, (2) implies (3). Lastly, let us deduce (1) from (3). Suppose $g\sim_{\mu'}a$ for some $a\in K[x]$ with $\deg a<\deg\phi$. By Lemma 1.8, a is coprime to ϕ, so we have a Bézout identity $ab=1+\phi q$, with $b,q\in K[x]$ and $\deg b<\deg\phi$. Hence,

$$\mu'(ab-1)=\mu'(\phi q)>\mu(\phi q)\ge\mu(ab)=\mu'(ab),$$

by the definition of μ'. Therefore, $ab\sim_{\mu'}1$ and $H_{\mu'}(g)=H_{\mu'}(a)$ is a unit in $\mathcal{G}r(\mu')$.

As for the condition $\phi\nmid_\mu g$, it amounts to saying, by Lemma 2.1, that $N_{\mu,\phi}(g)$ touches the vertical axis and has no sides of negative slope, which implies (2). ☐

Lemma 2.10. *For any $g\in K[x]$ with ϕ-expansion $g=\sum_{s=0}^{\ell}a_s\phi^s$, $a_\ell\ne0$, the following conditions are equivalent:*

1. *g is μ'-minimal.*
2. *$\deg a_\ell=0$ and $\mu'(g)=\mu'\left(a_\ell\phi^\ell\right)$.*
3. *$\deg g=s'(g)\deg\phi$.*

Proof. Since $\deg g=\deg a_\ell+\ell\deg\phi$, item (3) turns into $\deg a_\ell=0$ and $s'(g)=\ell$. By Corollary 2.3 applied to both g and $a_\ell\phi^\ell$, the last equality amounts to $\mu'(g)=\mu'\left(a_\ell\phi^\ell\right)$. Thus, (2) and (3) are equivalent.

Let us now deduce (2) from (1). If g is μ'-minimal, then $g-a_\ell\phi^\ell$ cannot be μ'-equivalent to g, so the equality $\mu'(g)=\mu'\left(a_\ell\phi^\ell\right)$ must hold. Moreover, Lemma 2.9 applied to a_ℓ yields $c\,a_\ell\sim_{\mu'}1$ for some $c\in K[x]$. Then, for each $0\le s<\ell$ such that $a_s\ne0$, Lemma 2.9 applied to the unit $H_{\mu'}(c\,a_s)$ shows that $ca_s\sim_{\mu'}c_s$ for some $c_s\in K[x]$ with $\deg c_s<\deg\phi$. Thus, $c\,g\sim_{\mu'}\phi^\ell+\sum_{s=0}^{\ell-1}c_s\phi^s$ and this implies $\deg g\le\ell\deg\phi$ by the μ'-minimality of g. Hence, $\deg a_\ell=0$.

Conversely, suppose that (3) holds and consider $f\in K[x]$ such that $f\sim_{\mu'}gh$ for a non-zero $h\in K[x]$. By Lemma 2.5 and Corollary 2.7, $s'(f)=s'(gh)=s'(g)+s'(h)$, so that $\deg g=s'(g)\deg\phi\le s'(f)\deg\phi\le\deg f$. Thus, g is μ'-minimal. ☐

As a consequence of the criterion for μ'-minimality given in Lemma 2.10, we may introduce an important numerical invariant of an augmented valuation.

Lemma 2.11. *Let $g\in K[x]$ be a monic non-constant μ'-minimal polynomial. Then, the rational number $C(\mu'):=\mu'(g)/\deg g$ is positive and does not depend on g.*

Proof. Lemma 2.10 shows that the ϕ-expansion of g is of the form

$$g = \phi^\ell + \sum\nolimits_{0\le s<\ell} a_s\phi^s, \quad \text{with} \quad \mu'(g) = \mu'(\phi^\ell).$$

Since $\deg g = \ell\deg\phi$, we get $\mu'(g)/\deg g = \mu'(\phi)/\deg\phi$. This value is positive due to Corollary 1.10 and the inequality $\mu'(\phi) > \mu_0(\phi)$. □

Lemma 2.11 holds for the minimal valuation μ_0 too, though the corresponding constant is no longer positive. Indeed, a monic non-constant μ_0-minimal polynomial g has coefficients in $\mathcal{O}$, and then $C(\mu_0) := \mu_0(g)/\deg g = 0$ is independent of g.

3. MacLane's inductive valuations

A valuation $\mu \in \mathbb{V}$ is called *inductive* if it is attained after a finite number of augmentation steps starting with μ_0. For such a chain of augmented valuations $\mu_i = [\mu_{i-1}; (\phi_i,\nu_i)]$, $1 \le i \le r$, we write

$$\mu_0 \xrightarrow{(\phi_1,\nu_1)} \mu_1 \xrightarrow{(\phi_2,\nu_2)} \cdots \xrightarrow{(\phi_{r-1},\nu_{r-1})} \mu_{r-1} \xrightarrow{(\phi_r,\nu_r)} \mu_r = \mu. \tag{4}$$

Let $\mathbb{V}^{\mathrm{ind}} := \mathbb{V}^{\mathrm{ind}}(K) \subset \mathbb{V}$ denote the subset of all inductive valuations. We agree that $\mu_0 \in \mathbb{V}^{\mathrm{ind}}$ by admitting empty chains of augmentations of length $r = 0$.

By Lemma 2.10, in every chain of augmented valuations as in (4) we have

$$\deg\phi_1 \mid \deg\phi_2 \mid \cdots \mid \deg\phi_{r-1} \mid \deg\phi_r.$$

Moreover, the constants $C(\mu_i)$ introduced in Lemma 2.11 grow strictly:

$$0 = C(\mu_0) < C(\mu_1) < \cdots < C(\mu_r) = C(\mu).$$

In fact, $\phi_{i+1} \in \mathrm{KP}(\mu_i) \cap \mathrm{KP}(\mu_{i+1})$ for any $0 \le i < r$, by Proposition 1.7. Hence,

$$C(\mu_{i+1}) = \frac{\mu_{i+1}(\phi_{i+1})}{\deg\phi_{i+1}} = \frac{\mu_i(\phi_{i+1}) + \nu_{i+1}}{\deg\phi_{i+1}} = C(\mu_i) + \frac{\nu_{i+1}}{\deg\phi_{i+1}}.$$

Lemma 3.1. *For a chain of augmented valuations as in* (4)*, consider* $g \in K[x]$ *such that* $\phi_i \nmid_{\mu_{i-1}} g$ *for some* $1 \le i < r$*. Then,* $\mu_{i-1}(g) = \mu_i(g) = \cdots = \mu_r(g)$*.*

Proof. By Proposition 1.7, $\mu_{i-1}(g) = \mu_i(g)$. By Lemma 2.9, $H_{\mu_i}(g)$ is a unit, so it is not divisible by the prime $H_{\mu_i}(\phi_{i+1})$ and the argument can be iterated. □

3.1. **MacLane chains of valuations.** A chain of augmented valuations as in (4) is called a *MacLane chain (of length r)* if $\phi_{i+1} \not\sim_{\mu_i} \phi_i$ for all $1 \le i < r$. We say that it is an *optimal MacLane chain* if $\deg\phi_1 < \cdots < \deg\phi_r$.

The condition $\phi_{i+1} \not\sim_{\mu_i} \phi_i$ in a MacLane chain amounts to the apparently stronger condition $\phi_{i+1} \nmid_{\mu_i} \phi_i$. Indeed, $\phi_{i+1} \mid_{\mu_i} \phi_i$ implies $\deg\phi_{i+1} = \deg\phi_i$ by the μ_i-minimality of ϕ_{i+1}; thus, $\phi_{i+1} \sim_{\mu_i} \phi_i$ by Lemma 1.4. This shows, in particular, that an optimal MacLane chain is certainly a MacLane chain.

Lemma 3.2. *In a MacLane chain as in* (4)*, the value group* $\Gamma(\mu_i)$*, for* $1 \le i \le r$*, is the subgroup of* $\mathbb{Q}$ *generated by* $\Gamma(\mu_{i-1})$ *and* ν_i*. In particular,*

$$\mathbb{Z} = \Gamma(\mu_0) \subset \Gamma(\mu_1) \subset \cdots \subset \Gamma(\mu_{r-1}) \subset \Gamma(\mu_r) = \Gamma(\mu).$$

Moreover, $\Gamma(\mu_{i-1}) = \Gamma_{\phi_i}(\mu_{i-1}) = \{\mu_{i-1}(a) \mid a \in K[x],\ a \ne 0,\ \deg a < \deg\phi_i\}$*.*

Proof. By Propositions 1.7 and 1.9, the group $\Gamma(\mu_i)$ is generated by $\mu_{i-1}(\phi_i) + \nu_i$ and the subgroup $\Gamma_{\phi_i} := \Gamma_{\phi_i}(\mu_{i-1})$. Thus, it suffices to show that $\Gamma(\mu_{i-1}) \subset \Gamma_{\phi_i}$. Since $\Gamma(\mu_0) = \mathbb{Z} \subset \Gamma_{\phi_1}$, we can assume $i > 1$. Let $g = \sum_{0\le s} a_s(\phi_{i-1})^s$ be the ϕ_{i-1}-expansion of a non-zero polynomial. By definition, there exists $s \ge 0$ such that

$$\mu_{i-1}(g) = \mu_{i-1}(a_s(\phi_{i-1})^s) = \mu_{i-1}(a_s) + s\,\mu_{i-1}(\phi_{i-1}).$$

We have $\mu_{i-1}(a_s)\in\Gamma_{\phi_i}$ because $\deg a_s<\deg\phi_{i-1}\le\deg\phi_i$. Since $\phi_i\nmid_{\mu_{i-1}}\phi_{i-1}$, Lemma 2.9 shows the existence of $a\in K[x]$ with $\deg a<\deg\phi_i$ such that $\phi_{i-1}\sim_{\mu_i}a$. Hence, $\mu_{i-1}(\phi_{i-1})=\mu_i(\phi_{i-1})=\mu_i(a)=\mu_{i-1}(a)\in\Gamma_{\phi_i}$, so that $\mu_{i-1}(g)\in\Gamma_{\phi_i}$. $\square$

In the next three auxiliary results, μ stands for an arbitrary valuation in $\mathbb{V}$. The first one comes right away from item (3) of Lemma 2.10.

Lemma 3.3. *For an augmented valuation $\mu'=[\mu;(\phi,\nu)]$, any monic μ'-minimal polynomial $g\in K[x]$ with $\deg g=\deg\phi$ satisfies $g\sim_\mu\phi$.* $\square$

Lemma 3.4. *Consider a chain of two augmented valuations*

$$\mu\ \xrightarrow{(\phi,\nu)}\ \mu'\ \xrightarrow{(\phi',\nu')}\ \mu''$$

with $\deg\phi'=\deg\phi$. Then, ϕ' is a key polynomial for μ, and $\mu''=[\mu;(\phi',\nu+\nu')]$.

Proof. By Lemmas 3.3 and 1.4, ϕ' is a key polynomial for μ. It is clear from the definitions that μ'' and $[\mu;(\phi',\nu+\nu')]$ coincide with μ on all polynomials of degree less than $\deg\phi$. It suffices to check that they also coincide on ϕ'. Indeed, we have

$$\mu''(\phi')=\mu'(\phi')+\nu'=\mu'(\phi)+\nu'=\mu(\phi)+\nu+\nu'=\mu(\phi')+\nu+\nu',$$

where the equality $\mu'(\phi')=\mu'(\phi)$ is deduced from item (4) of Proposition 1.7 and Lemma 2.11, while the equality $\mu(\phi')=\mu(\phi)$ is a consequence of Lemma 3.3. $\square$

Lemma 3.4 shows that every inductive valuation admits an optimal MacLane chain. Let us now discuss the unicity of such a chain.

Lemma 3.5. *Let $\eta=[\mu;(\phi,\nu)]$ and $\eta_*=[\mu;(\phi_*,\nu_*)]$ be two augmented valuations. Then, $\eta_*=\eta$ if and only if $\deg\phi_*=\deg\phi$, $\eta(\phi_*)=\eta(\phi)$ and $\nu_*=\nu$. In this case, we also have $\phi_*\sim_\mu\phi$.*

Proof. Suppose $\eta_*=\eta$. By the definition of an augmented valuation,

$$\deg\phi=\min\{\deg g\mid g\in K[x],\ \mu(g)<\eta(g)\}\tag{5}$$

and analogously for ϕ_* (and η_*), so that $\deg\phi_*=\deg\phi$. By Proposition 1.7, ϕ and ϕ_* are η-minimal; hence, $\phi_*\sim_\mu\phi$ by Lemma 3.3, and $\eta(\phi_*)=\eta(\phi)$ by Lemma 2.11. This implies $\mu(\phi_*)=\mu(\phi)$ and $\nu_*=\nu$.

Conversely, suppose $\deg\phi_*=\deg\phi$, $\eta(\phi_*)=\eta(\phi)$ and $\nu_*=\nu$. The first two assumptions imply the η-minimality of ϕ_* by item (2) of Lemma 2.10, and then

$$\eta_*(\phi_*)\ =\ \mu(\phi_*)+\nu_*\ =\ \mu(\phi)+\nu\ =\ \eta(\phi)\ =\ \eta(\phi_*)$$

is a consequence of Lemma 3.3. Now, since ϕ_* is η-minimal and η_*-minimal, item (3) of Lemma 1.3 shows that $\eta=\eta_*$. $\square$

Proposition 3.6. *Consider an optimal MacLane chain as in* (4) *and any other optimal MacLane chain*

$$\mu_0=\mu_0^*\ \xrightarrow{(\phi_1^*,\nu_1^*)}\ \mu_1^*\ \xrightarrow{(\phi_2^*,\nu_2^*)}\ \cdots\ \longrightarrow\ \mu_{t-1}^*\ \xrightarrow{(\phi_t^*,\nu_t^*)}\ \mu_t^*=\mu^*.$$

Then, $\mu=\mu^*$ if and only if $r=t$ and

$$\deg\phi_i=\deg\phi_i^*,\quad \mu_i(\phi_i)=\mu_i(\phi_i^*),\quad \nu_i=\nu_i^*\ \ \textit{for all}\ \ 1\le i\le r.$$

In this case, we also have $\mu_i=\mu_i^*$ and $\phi_i\sim_{\mu_{i-1}}\phi_i^*$ for all $1\le i\le r$.

Proof. The sufficiency of the conditions is a consequence of Lemma 3.5. Conversely, suppose $\mu=\mu^*$ and, for instance, $r\le t$. Let us prove the following for any $1\le i\le r$:

$$\mu_{i-1}=\mu_{i-1}^* \implies \deg\phi_i=\deg\phi_i^*,\quad \mu_i(\phi_i)=\mu_i(\phi_i^*),\quad \nu_i=\nu_i^*,\quad \mu_i=\mu_i^*.$$

Indeed, the degree equality comes from

$$\deg\phi_i=\min\{\deg g\mid g\in K[x],\ \mu_{i-1}(g)<\mu(g)\},$$

which is deduced from (5) and Lemma 3.1. The optimality of both chains and the minimality of the key polynomials imply $\phi_{i+1}\nmid_{\mu_i}\phi_i^*$ and $\phi_{i+1}^*\nmid_{\mu_i^*}\phi_i$. Hence,

$$\mu_i^*(\phi_i)=\mu(\phi_i)=\mu_i(\phi_i) \qquad\text{and}\qquad \mu_i(\phi_i^*)=\mu(\phi_i^*)=\mu_i^*(\phi_i^*),$$

again by Lemma 3.1. Now, $\mu_i(\phi_i^*)\le\mu_i(\phi_i)$ and $\mu_i^*(\phi_i)\le\mu_i^*(\phi_i^*)$, by the very definition of the valuations μ_i, μ_i^* on monic polynomials with the same degree as ϕ_i, ϕ_i^*. Therefore, $\mu_i(\phi_i)=\mu_i(\phi_i^*)$ and the equality $\nu_i=\nu_i^*$ follows straightforwardly. Lemma 3.5 asserts then $\mu_i=\mu_i^*$ and $\phi_i\sim_{\mu_{i-1}}\phi_i^*$. This leads by induction to $\mu_r=\mu_r^*$. The inequality $r<t$ would imply $\mu<\mu^*$, against our assumption. Thus, $r=t$. □

Hence, in an optimal MacLane chain for μ, the intermediate valuations $\mu_1,\dots,\mu_{r-1}$, the positive rational numbers $\nu_1,\dots,\nu_r$ and the integers $\deg\phi_1,\dots,\deg\phi_r$ are intrinsic data of μ, whereas the key polynomials $\phi_1,\dots,\phi_r$ admit different choices.

Definition 3.7. *The* MacLane depth *of an inductive valuation μ is the length r of any optimal MacLane chain for μ.*

We end this section with several applications of the existence of MacLane chains.

Proposition 3.8. *Let μ be an inductive valuation on $K_v(x)$. The restriction of μ to $K(x)$ is an inductive valuation with graded algebra isomorphic to $\mathcal{G}r(\mu)$. The mapping $\mathbb{V}^{\mathrm{ind}}(K_v)\to\mathbb{V}^{\mathrm{ind}}(K)$ obtained in this way is bijective.*

Proof. Proposition 3.6 shows that every $\mu\in\mathbb{V}^{\mathrm{ind}}(K_v)$ admits an optimal MacLane chain whose key polynomials have coefficients in K; clearly, the inductive valuation on $K(x)$ determined by this optimal MacLane chain is the restriction of μ to $K(x)$. Thus, the restriction of valuations induces a well-defined map $\mathbb{V}^{\mathrm{ind}}(K_v)\to\mathbb{V}^{\mathrm{ind}}(K)$. The statement about the graded algebras is obvious.

Conversely, an optimal MacLane chain of any $\mu\in\mathbb{V}^{\mathrm{ind}}(K)$ may be considered as an optimal MacLane chain of an inductive valuation $\mu\otimes_K K_v$ on $K_v(x)$, obtained by extending to polynomials in $K_v[x]$ the definition of the successive augmentations. This valuation does not depend on the chosen optimal MacLane chain, by Proposition 3.6 applied to both valuations μ and $\mu\otimes_K K_v$. Hence, we get a map $\mathbb{V}^{\mathrm{ind}}(K)\to\mathbb{V}^{\mathrm{ind}}(K_v)$ which is the inverse of the restriction map. □

Proposition 3.9. *For any inductive valuation μ, the canonical embedding $\Delta(\mu)\hookrightarrow\kappa(\mu)$ induces an isomorphism between the field of fractions of $\Delta(\mu)$ and $\kappa(\mu)$.*

Proof. We must show that the induced morphism $\operatorname{Frac}(\Delta(\mu))\to\kappa(\mu)$ is onto. An element in $\kappa(\mu)^*$ is the class modulo $\mathfrak{m}_\mu$ of a fraction g/h of polynomials with $\mu(g/h)=0$. Set $\alpha=\mu(g)=\mu(h)\in\Gamma(\mu)$. If there exists $f\in K[x]$ with $\mu(f)=-\alpha$, then $H_\mu(fg),H_\mu(fh)$ belong to $\Delta(\mu)$ and the fraction $H_\mu(fg)/H_\mu(fh)$ is sent to the class of g/h by the above morphism.

If $\mu=\mu_0$, then $\alpha\in\mathbb{Z}$ and we can take $f=\pi^{-\alpha}$. Otherwise, consider a MacLane chain for μ as in (4). By Lemma 3.2, $-\alpha=\beta+s\,\nu_r$ for some $\beta\in\Gamma(\mu_{r-1})$ and some integer s which can be assumed non-negative by taking, if necessary, the remainder of its euclidean division by $(\Gamma(\mu)\colon\Gamma(\mu_{r-1}))$. Also, Lemma 3.2 shows the existence of $a\in K[x]$ with $\deg a<\deg\phi_r$

such that $\mu_{r-1}(a)=\beta-s\mu_{r-1}(\phi_r)\in\Gamma(\mu_{r-1})$. Thus, $\mu_{r-1}(a\phi_r^s)=\beta$, and so we can take $f=a\phi_r^s$. □

Theorem 3.10. *For an inductive valuation μ, every monic non-constant $g\in K[x]$ satisfies $\mu(g)/\deg g\le C(\mu)$. Equality holds if and only if g is μ-minimal.*

Proof. By induction on the length r of a MacLane chain of μ. For $r=0$, a monic $g\in K[x]$ satisfies $\mu_0(g)\le 0=C(\mu_0)$, with equality if and only if it has coefficients in $\mathcal{O}$, which is equivalent to g being μ_0-minimal.

Take a MacLane chain of μ of length $r>0$ as in (4) and let $g=\sum_{s=0}^{\ell}a_s\phi_r^s$ be the ϕ_r-expansion of a monic non-constant polynomial in $K[x]$. Denote $m_r:=\deg\phi_r$.

If $a_\ell=1$, then $\mu(g)\le\mu(\phi_r^\ell)=\ell\, m_r\, C(\mu)=C(\mu)\deg g$, and equality holds if and only if g is μ-minimal, by Lemma 2.10. Otherwise, a_ℓ is monic and g is not μ-minimal, again by Lemma 2.10. Moreover,

$$\mu(g)\le\mu(a_\ell\phi_r^\ell)=\mu_{r-1}(a_\ell)+\ell\, m_r\, C(\mu)<C(\mu)\,(\deg a_\ell+\ell\, m_r)=C(\mu)\deg g,$$

since $C(\mu_{r-1})<C(\mu)$ and $\mu_{r-1}(a_\ell)\le\deg a_\ell\, C(\mu_{r-1})$ by the induction hypothesis. □

3.2. **Discrete data attached to a MacLane chain.** Let us fix an inductive valuation μ equipped with a Maclane chain of length r as in (4). In this and the next two sections, we attach to this chain several data and operators.

From now on we use the following notation:

$$\begin{array}{lll}\Gamma_i:=\Gamma(\mu_i)=e(\mu_i)^{-1}\mathbb{Z}, & \Delta_i:=\Delta(\mu_i), & 0\le i\le r,\\ \mathbb{F}_0:=\operatorname{Im}(\mathbb{F}\to\Delta_0), & \mathbb{F}_i:=\operatorname{Im}(\Delta_{i-1}\to\Delta_i), & 1\le i\le r.\end{array}$$

By Proposition 1.12, $\mathbb{F}_i$ is a field isomorphic to the residue class field $\mathbb{F}_{\phi_i}$ of the extension of K_v determined by ϕ_i; thus, $\mathbb{F}_i$ is a finite extension of $\mathbb{F}$. We abuse of language and identify $\mathbb{F}$ with $\mathbb{F}_0$ and each field $\mathbb{F}_i\subset\Delta_i$ with its image under the canonical map $\Delta_i\to\Delta_j$ for $j\ge i$. In other words, we consider as inclusions the canonical embeddings: $\mathbb{F}=\mathbb{F}_0\subset\mathbb{F}_1\subset\cdots\subset\mathbb{F}_r$.

To these objects we attach several numerical data. Set $\phi_0=x$, $\nu_0=0$, $\mu_{-1}=\mu_0$ and $\mathbb{F}_{-1}=\mathbb{F}_0$. For all $0\le i\le r$, we define:

$$\begin{array}{ll}e_i:=e(\mu_i)/e(\mu_{i-1}), & m_i:=\deg\phi_i,\\ f_{i-1}:=[\mathbb{F}_i\colon\mathbb{F}_{i-1}], & w_i:=\mu_{i-1}(\phi_i),\ V_i:=e(\mu_{i-1})w_i,\\ h_i:=e(\mu_i)\nu_i, & C_i:=C(\mu_i)=\mu_i(\phi_i)/\deg\phi_i,\end{array}$$

Note that $e_0=1$, $f_0=m_1$, $h_0=0$. Also, the relation $\Gamma_i=\Gamma_{i-1}+\nu_i\mathbb{Z}$ proved in Lemma 3.2 implies $\gcd(e_i,h_i)=1$. All these data may be derived from the integers

$$e_0,\dots,e_r,\ f_0,\dots,f_{r-1},\ h_1,\dots,h_r. \tag{6}$$

In fact, the following relations can be easily checked to hold for $1\le i\le r$:

$$\begin{array}{l}e(\phi_i)=e(\mu_{i-1})=e_0\cdots e_{i-1},\\ f(\phi_i)=[\mathbb{F}_i\colon\mathbb{F}_0]=f_0\cdots f_{i-1},\\ m_i=e_{i-1}f_{i-1}m_{i-1}=(e_0\cdots e_{i-1})(f_0\cdots f_{i-1}),\\ w_i=e_{i-1}f_{i-1}(w_{i-1}+\nu_{i-1})=\sum_{1\le j<i}(e_jf_j\cdots e_{i-1}f_{i-1})\nu_j,\\ C_i=(w_i+\nu_i)/m_i.\end{array} \tag{7}$$

The first equality comes from the last assertion of Lemma 3.2 and Proposition 1.9. The recurrence on w_i is deduced from Lemma 2.11 applied to ϕ_{i-1} and ϕ_i as key polynomials for μ_{i-1}. Note that $w_0=w_1=0$.

If the MacLane chain is optimal, Proposition 3.6 shows that all these rational numbers are intrinsic data of μ. In this case, we refer to them as $e_i(\mu)$, $f_i(\mu)$, $h_i(\mu)$, $\nu_i(\mu)$, $m_i(\mu)$, $w_i(\mu)$, $V_i(\mu)$, $C_i(\mu)$, respectively. The positive integers in (6) are then called the *basic MacLane invariants* of μ.

3.3. **Rational functions attached to a MacLane chain.** For every $0 \le i \le r$, we consider integers ℓ_i, ℓ'_i uniquely determined by

$$\ell_i h_i + \ell'_i e_i = 1, \qquad 0 \le \ell_i < e_i.$$

We consider several rational functions in $K(x)$ defined in a recursive way. We take $\pi_0 = \pi_1 = \pi$, $\Phi_0 = \phi_0 = \gamma_0 = x$, and

$$\Phi_i = \phi_i\, \pi_i^{-V_i}, \quad \gamma_i = \Phi_i^{e_i}\pi_i^{-h_i}, \quad \pi_{i+1} = \Phi_i^{\ell_i}\pi_i^{\ell'_i}, \quad 1 \le i \le r.$$

For $i \ge 1$, it is easy to deduce from the definition that:

$$\Phi_i = \pi^{n_0}(\phi_1)^{n_1}\cdots(\phi_{i-1})^{n_{i-1}}\phi_i, \quad \pi_i = \pi^{n'_0}(\phi_1)^{n'_1}\cdots(\phi_{i-2})^{n'_{i-2}}(\phi_{i-1})^{\ell_{i-1}}. \tag{8}$$

for certain integer exponents. By Lemma 3.1, $\mu_j(\phi_i) = \mu(\phi_i)$ for all $i \le j$; hence,

$$\mu_j(\Phi_i) = \mu(\Phi_i), \quad \mu_j(\gamma_i) = \mu(\gamma_i), \quad \mu_j(\pi_{i+1}) = \mu(\pi_{i+1}), \quad 1 \le i \le j \le r. \tag{9}$$

Let us compute these stable values.

Lemma 3.11. *For every index $0 \le i \le r$, we have*

(1) $\mu_i(\pi_i) = 1/e(\mu_{i-1})$, $\mu_i(\pi_{i+1}) = 1/e(\mu_i)$.
(2) $\mu_{i-1}(\Phi_i) = 0$, $\mu_i(\Phi_i) = \nu_i$.
(3) $\mu_i(\gamma_i) = 0$.

Proof. We prove (1) and (2) by induction on i. For $i = 0$ the statements are obvious. Suppose $i > 0$ and (1), (2) hold for a lower index. The identity $\mu_i(\pi_i) = \mu_{i-1}(\pi_i) = 1/e(\mu_{i-1})$ is a consequence of (9). We have then,

$$\begin{aligned}
&\mu_{i-1}(\Phi_i) = \mu_{i-1}(\phi_i) - V_i/e(\mu_{i-1}) = w_i - w_i = 0.\\
&\mu_i(\Phi_i) = \mu_i(\phi_i) - V_i/e(\mu_{i-1}) = w_i + \nu_i - w_i = \nu_i.\\
&\mu_i(\pi_{i+1}) = \ell_i\nu_i + \ell'_i/e(\mu_{i-1}) = 1/e(\mu_i).
\end{aligned}$$

The third item follows from the first two items. □

By Lemma 2.9, the element $H_{\mu_i}(\phi_j)$ is a unit in $\mathcal{G}r(\mu_i)$ for all $j < i \le r$. Hence, by using (8), it makes sense to define for all $0 \le i \le r$:

$$\begin{aligned}
&x_i := H_{\mu_i}(\Phi_i) := H_{\mu_i}(\pi)^{n_0} H_{\mu_i}(\phi_1)^{n_1}\cdots H_{\mu_i}(\phi_{i-1})^{n_{i-1}} H_{\mu_i}(\phi_i) \in \mathcal{G}r(\mu_i),\\
&p_i := H_{\mu_i}(\pi_i) := H_{\mu_i}(\pi)^{n'_0} H_{\mu_i}(\phi_1)^{n'_1}\cdots H_{\mu_i}(\phi_{i-2})^{n'_{i-2}} H_{\mu_i}(\phi_{i-1})^{\ell_{i-1}} \in \mathcal{G}r(\mu_i)^*,\\
&y_i := H_{\mu_i}(\gamma_i) := (x_i)^{e_i}(p_i)^{-h_i} \in \Delta_i.
\end{aligned}$$

Clearly, x_i is associate to the prime $H_{\mu_i}(\phi_i)$ in $\mathcal{G}r(\mu_i)$. For $i > 0$, $\phi_{i+1} \nmid_{\mu_i} \phi_i$ implies that $H_{\mu_i}(\phi_i)$ has a non-zero image in $\mathcal{G}r(\mu_{i+1})$, by Proposition 1.7. Thus, x_i, and hence y_i, have non-zero images in $\mathcal{G}r(\mu_{i+1})$ too. For $0 \le i < r$ we may define:

$$\begin{aligned}
&z_i \in \mathbb{F}_{i+1}, \quad \text{the image of } y_i \text{ under } \Delta_i \longrightarrow \Delta_{i+1},\\
&\psi_i \in \mathbb{F}_i[y], \quad \text{the minimal polynomial of } z_i \text{ over } \mathbb{F}_i.
\end{aligned}$$

As remarked above, $z_i \ne 0$ (and $\psi_i \ne y$) for $i > 0$. We have $z_0 = 0$ (and $\psi_0 = y$) if and only if $\phi_1 \sim_{\mu_0} x$, or equivalently, $\overline{\phi}_1 = \overline{x}$ in $\mathbb{F}[x]$.

We shall see in Corollary 4.4 that $\mathbb{F}_{i+1} = \mathbb{F}_i[z_i] = \mathbb{F}_0[z_0, \dots, z_i]$, so that $\deg \psi_i = f_i$.

In optimal MacLane chains, the elements $x_i, p_i, y_i, z_i \in \mathcal{G}r(\mu)$ are "almost" independent of the chain. Their precise variation is analyzed in Lemma 4.13.

3.4. **Operators attached to a MacLane chain.** We consider Newton polygon operators

$$N_i := N_{\mu_{i-1},\phi_i}\colon\ K[x] \longrightarrow 2^{\mathbb{R}^2}, \quad 0 \le i \le r,$$

and residual polynomial operators:

$$\begin{array}{rlll} R_{i,\alpha}\colon & \mathcal{P}_\alpha(\mu_i) \longrightarrow \mathbb{F}_i[y], & 0 \le i \le r, & \alpha \in \Gamma_i, \\ R_i\colon & K[x] \longrightarrow \mathbb{F}_i[y], & 0 \le i \le r. & \end{array}$$

The operators $R_{i,\alpha}$, R_i are attached to the MacLane chain of μ_i obtained by truncation of the given MacLane chain of μ. Thus, it suffices to describe $R_{r,\alpha}$ and R_r.

Let us first define certain constants involved in the recursive definition of $R_{r,\alpha}$.

Definition 3.12. *For $0 \le i \le r$ and $\alpha \in \Gamma_i$, let $s_i(\alpha)$, $u_i(\alpha)$ be the unique integers satisfying $u_i(\alpha)e_i + s_i(\alpha)h_i = e(\mu_i)\alpha$ and $0 \le s_i(\alpha) < e_i$. For $0 \le i < r$, define*

$$\epsilon_i(\alpha) = (z_i)^{\ell'_i s_i(\alpha) - \ell_i u_i(\alpha)} \in \mathbb{F}^*_{i+1}.$$

We agree that $\epsilon_0(\alpha) = (z_0)^0 = 1$ for all $\alpha \in \Gamma_0 = \mathbb{Z}$, even in the case $z_0 = 0$.

Definition 3.13. *For $\alpha \in \Gamma(\mu)$ and $g = \sum_{0 \le s} a_s \phi_r^s$ the ϕ_r-expansion of $g \in \mathcal{P}_\alpha(\mu)$, we define:*

$$R_{r,\alpha}(g) = \begin{cases} \overline{g(y)/\pi^\alpha}, & \text{if } r = 0, \\ \sum_{0 \le j} \epsilon_{r-1}(\alpha_j)\, R_{r-1,\alpha_j}(a_{s_j})(z_{r-1})\, y^j, & \text{if } r > 0, \end{cases}$$

where $s_j := s_r(\alpha) + je_i$ and $\alpha_j := \alpha - s_j\mu(\phi_r) \in \Gamma_{r-1}$.

Let us explain the meaning of the data s_j, α_j involved in the computation of the j-th coefficient of $R_{r,\alpha}(g)$ for $r > 0$ (see Fig.4).

Let $\mathcal{C} = (\mathbb{Z}_{\ge 0}) \times \Gamma_{r-1} \subset \mathbb{R}^2$ be the set of points of the plane that may be vertices of $N_r(g)$. Let L_α be the line of slope $-\nu_r$ cutting the vertical axis at the point $(0, \alpha)$. The monomials of $R_{r,\alpha}(g)$ are in 1-1 correspondence with the points of $\mathcal{C} \cap L_\alpha$. In fact, the points on $\mathcal{C} \cap L_\alpha$ may be parameterized as:

$$P_j = (s_r(\alpha) + je_r, (u_r(\alpha) - jh_r)/e(\mu_{r-1})), \quad j \in \mathbb{Z}_{\ge 0}.$$

We may write $P_j = (s_j, u_j/e(\mu_{r-1}))$, with $s_j = s_r(\alpha) + je_r$, $u_j = u_r(\alpha) - jh_r \in \mathbb{Z}$. Also, since $u_j/e(\mu_{r-1})$ and w_r (by definition) belong to Γ_{r-1}, we may consider

$$\alpha_j = \alpha - s_j\mu(\phi_r) = \alpha - s_j(w_r + \nu_r) = u_j/e(\mu_{r-1}) - s_j w_r \in \Gamma_{r-1}.$$

Denote $Q_s := (s, \mu_{r-1}(a_s\phi_r^s)) \in \mathcal{C}$, so that $\{Q_s \mid 0 \le s\}$ is the cloud of points whose lower convex hull is $N_r(g)$. By Corollary 2.3, all Q_s lie on or above the line L_α, and Q_s lies on L_α if and only if $\mu(a_s\phi_r^s) = \alpha$. Hence,

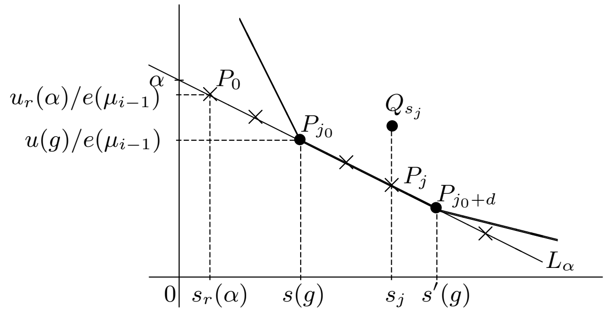
$$Q_s = P_j \in L_\alpha \iff s = s_j \ \text{ and } \ \mu_{r-1}(a_{s_j}) = \alpha_j. \tag{10}$$

We shall see in Corollary 4.9 that the j-th coefficient of $R_{r,\alpha}(g)$ is non-zero if and only if $Q_{s_j} = P_j$. Let us now check that this coefficient vanishes if Q_{s_j} lies above L_α.

Lemma 3.14. *For all $\alpha \in \Gamma(\mu)$ the operator $R_{r,\alpha}$ vanishes on $\mathcal{P}^+_\alpha(\mu)$.*

Proof. We proceed by induction on r. For $r = 0$ the statement is clear. Assume $r > 0$ and consider the ϕ_r-expansion $g = \sum_{0 \le s} a_s\phi_r^s$ of a polynomial g with $\mu(g) > \alpha$. By (10), $\mu_{r-1}(a_{s_j}) > \alpha_j$ for all $j \ge 0$. By the induction hypothesis, all $R_{r-1,\alpha_j}(a_{s_j})$ vanish (as polynomials in $\mathbb{F}_{r-1}[y]$) and all coefficients of $R_{r,\alpha}(g)$ vanish too. $\square$

FIGURE 4. Newton polygon $N_r(g)$ for $g \in K[x]$ with $\mu(g) = \alpha$



We may now describe the residual polynomial operator $R_r\colon K[x] \longrightarrow \mathbb{F}_r[y]$.

Take g as above with $\mu(g) = \alpha$, and let $s(g) = s_\mu(g) \le s'(g) = s'_\mu(g)$ be the abscissas of the end points of the ν_r-component of $N_r(g)$ (Definition 2.4). These end points belong to $\mathcal{C} \cap L_\alpha$, so that $s(g) = s_{j_0}$ for $j_0 = (s(g) - s_r(\alpha))/e_r = \lfloor s(g)/e_r \rfloor$, and $s'(g) = s_{j_0+d}$, where $d = (s'(g) - s(g))/e_r$ is the *degree* of the segment $S_{\nu_r}(g)$.

By Lemma 3.14, the non-zero coefficients of $R_{r,\alpha}(g)$ correspond to abscissas s_j with $j_0 \le j \le j_0 + d$ (see Fig.4).

Definition 3.15. *For a nonzero $g \in K[x]$, let $\alpha = \mu(g)$. We define*

$$R_0(g) := R_{0,\alpha}(g) = \overline{g(y)/\pi^\alpha},$$

$$R_r(g) := R_{r,\alpha}(g)/y^{j_0} = \sum\nolimits_{0 \le k \le d} \epsilon_{r-1}(\alpha_{j_0+k})\, R_{r-1,\alpha_{j_0+k}}(a_{s_{j_0+k}})(z_{r-1})\, y^k,$$

if $r > 0$, where $j_0 = \lfloor s(g)/e_r \rfloor$. We take $R_r(0) = 0$ for all r.

For $r > 0$ and any integer $s \ge 0$, the Newton polygon $N_r(\phi_r^s)$ is the single point (s, sw_r). Take $\alpha := \mu(\phi_r^s) = s(w_r + \nu_r)$ and let $j = \lfloor s/e_r \rfloor = (s - s_r(\alpha))/e_r$. With the above notation, $s = s_j$ and $\alpha_j = 0$. Since $\epsilon_{r-1}(0) = 1 = R_{r-1,0}(1)$, we have

$$R_{r,\alpha}(\phi_r^s) = y^{\lfloor s/e_r \rfloor}, \qquad R_r(\phi_r^s) = 1. \tag{11}$$

Corollary 4.9 below shows that $R_r(g)$ has always degree d and $R_r(g)(0) \ne 0$.

4. STRUCTURE OF THE GRADED ALGEBRA OF AN INDUCTIVE VALUATION

In this section, we fix an inductive valuation μ equipped with a MacLane chain of length r, and we denote $\Delta = \Delta(\mu)$. We shall freely use all data and operators of the MacLane chain described in section 3.

The essential property of the residual polynomials is revealed in Theorem 4.1. We shall derive from this result the structure of the graded algebra of μ and some more properties of the residual polynomials, including their link with the residual ideals. Also, at the end of the section we use Theorem 4.1 to find the precise relationship between the data and operators attached to two optimal MacLane chains of μ.

For $0 \le i \le r$ and $\alpha \in \Gamma_i$, consider the integers $s_i(\alpha)$, $u_i(\alpha)$ given in Definition 3.12. By Lemma 3.11, the following homogeneous element of $\mathcal{G}r(\mu)$ has degree α:

$$\varphi_i(\alpha) := x_i^{s_i(\alpha)} p_i^{u_i(\alpha)} \in \mathcal{P}_\alpha(\mu).$$

For a non-zero $g \in K[x]$, we recall that $(s(g), u(g)/e(\mu_{r-1}))$ is the left end point of $S_{\nu_r}(g)$, if $r > 0$ (see Fig.4). We agree that $s(g) := 0$, $u(g) := \mu_0(g)$ if $r = 0$.

Theorem 4.1. *Let $g \in K[x]$ be a non-zero polynomial and let $\alpha = \mu(g)$. Then,*

$$H_\mu(g) = \varphi_r(\alpha) R_{r,\alpha}(g)(y_r) = x_r^{s(g)} p_r^{u(g)} R_r(g)(y_r).$$

In particular, $\mathcal{P}_\alpha(\mu)/\mathcal{P}_\alpha^+(\mu) = \varphi_r(\alpha)\Delta$ is a free Δ-module of rank one.

Proof. Let $g = \sum_{0\le s} a_s \phi_r^s$ be the ϕ_r-expansion of g. Let $I = \{s \ge 0 \mid \mu(a_s\phi_r^s) = \alpha\}$. Since $g \sim_\mu \sum_{s\in I} a_s\phi_r^s$, we have $H_\mu(g) = \sum_{s\in I} H_\mu(a_s\phi_r^s)$ by equation (1).

If $r = 0$, we have $\phi_0 = x$, $s(\alpha) = 0$ and $\varphi_0(\alpha) = H_{\mu_0}(\pi)^\alpha = p_0^\alpha$. For all $s \in I$, we have $\mu_0(a_s) = \mu_0(a_s x^s) = \alpha$; thus, $b_s := a_s\pi^{-\alpha}$ has $\mu_0(b_s) = 0$, and

$$H_{\mu_0}(a_s x^s) = \varphi_0(\alpha) H_{\mu_0}(b_s)\, y_0^s = \varphi_0(\alpha)\bar{b}_s\, y_0^s,$$

by the identification of $\mathbb{F}$ with $\mathbb{F}_0 \subset \Delta_0$. This proves the theorem in this case.

For $r > 0$ let us prove by induction on r the identity

$$H_\mu(g) = \varphi_r(\alpha) R_{r,\alpha}(g)(y_r),$$

which, after (10), is equivalent to

$$H_\mu(a_{s_j}\phi_r^{s_j}) = \varphi_r(\alpha)\epsilon_{r-1}(\alpha_j) R_{r-1,\alpha_j}(a_{s_j})(z_{r-1})\, y_r^j,$$

for all $j \ge 0$ such that $\mu_{r-1}(a_{s_j}) = \alpha_j$. Since

$$\varphi_r(\alpha)\, y_r^j = x_r^{s_r(\alpha)} p_r^{u_r(\alpha)}\, y_r^j = x_r^{s_r(\alpha)+je_i} p_r^{u_r(\alpha)-jh_i} = x_r^{s_j} p_r^{u_j}, \tag{12}$$

our aim is equivalent to showing that $\mu_{r-1}(a_{s_j}) = \alpha_j$ implies:

$$H_\mu(a_{s_j}\phi_r^{s_j}) = x_r^{s_j} p_r^{u_j} \epsilon_{r-1}(\alpha_j) R_{r-1,\alpha_j}(a_{s_j})(z_{r-1}). \tag{13}$$

By the induction hypothesis, if $\mu_{r-1}(a_{s_j}) = \alpha_j$ we have

$$H_{\mu_{r-1}}(a_{s_j}) = \varphi_{r-1}(\alpha_j) R_{r-1,\alpha_j}(a_{s_j})(y_{r-1}). \tag{14}$$

Since $\deg a_{s_j} < \deg \phi_r$, we have $\mu(a_{s_j}) = \mu_{r-1}(a_{s_j})$. Also, (9) implies that $\mu(\Phi_{r-1}) = \mu_{r-1}(\Phi_{r-1})$, $\mu(\pi_{r-1}) = \mu_{r-1}(\pi_{r-1})$. Hence, if we apply the canonical homomorphism $\mathcal{G}r(\mu_{r-1}) \to \mathcal{G}r(\mu)$ to the identity (14), we get

$$H_\mu(a_{s_j}) = H_\mu(\Phi_{r-1})^{s_{r-1}(\alpha_j)} H_\mu(\pi_{r-1})^{u_{r-1}(\alpha_j)} R_{r-1,\alpha_j}(a_{s_j})(z_{r-1}). \tag{15}$$

Therefore, (13) is equivalent to

$$H_\mu\left((\Phi_{r-1})^{s_{r-1}(\alpha_j)}(\pi_{r-1})^{u_{r-1}(\alpha_j)}\phi_r^{s_j}\right) = H_\mu\left(\Phi_r^{s_j}\pi_r^{u_j}\right)\epsilon_{r-1}(\alpha_j),$$

and this is a consequence of an identity between the involved rational functions which is proved in Lemma 4.2 below.

Finally, equality (12) applied to $j = j_0 = \lfloor s(g)/e_r \rfloor$ yields $\varphi_r(\alpha)\, y_r^{j_0} = x_r^{s(g)} p_r^{u(g)}$. Hence, $\varphi_r(\alpha) R_{r,\alpha}(g)(y_r) = x_r^{s(g)} p_r^{u(g)} R_r(g)(y_r)$. $\square$

Lemma 4.2. *With the above notation, for any $j \ge 0$ we have*

$$(\Phi_{r-1})^{s_{r-1}(\alpha_j)}(\pi_{r-1})^{u_{r-1}(\alpha_j)}\,\phi_r^{s_j} = \Phi_r^{s_j}\pi_r^{u_j}(\gamma_{r-1})^{\ell'_{r-1}s_{r-1}(\alpha_j)-\ell_{r-1}u_{r-1}(\alpha_j)}.$$

Proof. Denote for simplicity $s = s_j$, $u = u_j$, $\bar{s} = s_{r-1}(\alpha_j)$, $\bar{u} = u_{r-1}(\alpha_j)$, $\ell = \ell_{r-1}$, $\ell' = \ell'_{r-1}$, $e = e_{r-1}$, $f = f_{r-1}$. The following identities are derived from the definitions of γ_{r-1}, π_r, Φ_r and the Bézout identity $\ell h + \ell' e = 1$.

$$\begin{aligned}(\Phi_{r-1})^{\bar{s}}(\pi_{r-1})^{\bar{u}}\ (\gamma_{r-1})^{\ell\bar{u}-\ell'\bar{s}} &= (\Phi_{r-1})^{\bar{s}+e(\ell\bar{u}-\ell'\bar{s})}(\pi_{r-1})^{\bar{u}-h(\ell\bar{u}-\ell'\bar{s})}\\ &= (\Phi_{r-1})^{\ell(h\bar{s}+e\bar{u})}(\pi_{r-1})^{\ell'(h\bar{s}+e\bar{u})} = \pi_r^{h\bar{s}+e\bar{u}} = \pi_r^{u-sV_r} = (\Phi_r/\phi_r)^s\pi_r^u.\end{aligned}$$

In the last but one equality we used the identity $u - sV_r = \bar{u}e + \bar{s}h$, which is derived from $u/e(\mu_{r-1}) - sw_r = \alpha_j = \bar{u}/e(\mu_{r-2}) + \bar{s}\nu_{r-1}$ by multiplying by $e(\mu_{r-1})$. $\square$

Theorem 4.3. *The map $\mathbb{F}_r[y]\to\Delta$ determined by $y\mapsto y_r$ is an isomorphism of $\mathbb{F}_r$-algebras.*

Proof. A non-zero element in Δ is of the form $H_\mu(g)$ for some $g\in K[x]$ with $\mu(g)=0$. Since $\varphi_r(0)=1$, Theorem 4.1 shows that $H_\mu(g)=R_{r,0}(g)(y_r)$ is a polynomial in y_r, so that the map $\mathbb{F}_r[y]\to\Delta$ is onto. On the other hand, Δ is a domain which is not a field, because $y_r\in\Delta$ is not a unit. Thus, the map is 1-1 because the kernel vanishes, being a prime ideal of $\mathbb{F}_r[y]$ which is not maximal. □

Corollary 4.4. *For all $0\le i<r$, $\mathbb{F}_{i+1}=\mathbb{F}_i[z_i]=\mathbb{F}_0[z_0,\dots,z_i]$ and $\deg\psi_i=f_i$.* □

By Proposition 3.9 and Theorem 4.3, we get an isomorphism $\kappa(\mu)\simeq\mathbb{F}_r(y)$. In particular, $\kappa(\mu)^{alg}\simeq\mathbb{F}_r$, where $\kappa(\mu)^{alg}$ is the algebraic closure of $\mathbb{F}$ in $\kappa(\mu)$.

Corollary 4.5. *For an inductive valuation μ, the subfield $\kappa(\mu)^{alg}\subset\kappa(\mu)$ is a finite extension of $\mathbb{F}$ and $\kappa(\mu)\simeq\kappa(\mu)^{alg}(y)$, where y is an indeterminate.* □

Corollary 4.6. *The operator $R_{r,\alpha}$ induces a bijective map $\overline{R}_{r,\alpha}\colon\mathcal{P}_\alpha/\mathcal{P}_\alpha^+\to\mathbb{F}_r[y]$.*

Proof. By Lemma 3.14, $\overline{R}_{r,\alpha}$ is well defined. Consider the map

$$\mathbb{F}_r[y]\longrightarrow\mathcal{P}_\alpha/\mathcal{P}_\alpha^+,\quad \psi(y)\mapsto\varphi_r(\alpha)\psi(y_r).$$

Theorems 4.1 and 4.3 show that these maps are one inverse to each other. □

Note that $\overline{R}_{r,0}$ is the inverse of the isomorphism $\mathbb{F}_r[y]\to\Delta$ of Theorem 4.3.

Theorem 4.7. *The graded algebra of μ admits the following description:*

$$\mathcal{G}r(\mu)=\bigoplus\nolimits_{\alpha\in\Gamma(\mu)}\varphi_r(\alpha)\Delta=\mathbb{F}_r[y_r,p_r,p_r^{-1}][x_r]=\Delta[p_r,p_r^{-1}][x_r].$$

The elements y_r,p_r are algebraically independent over $\mathbb{F}_r$ and x_r is algebraic over $\Delta[p_r,p_r^{-1}]$ with minimal equation $x_r^{e_r}=p_r^{h_r}y_r$.

Proof. Theorem 4.1 shows that x_r,y_r,p_r,p_r^{-1} generate $\mathcal{G}r(\mu)$ as an $\mathbb{F}_r$-algebra. The algebraic independence of y_r, p_r translates into the $\mathbb{F}_r$-linear independence of the family $\Sigma=\{y_r^mp_r^n\mid m\in\mathbb{Z}_{\ge0},\ n\in\mathbb{Z}\}$. We may group these elements by its degree:

$$\Sigma=\bigcup\nolimits_{\alpha\in\Gamma(\mu)}\Sigma_\alpha,\qquad \Sigma_\alpha=\{y_r^mp_r^{e(\mu_{r-1})\alpha}\mid m\in\mathbb{Z}_{\ge0}\}.$$

Each family Σ_α is $\mathbb{F}_r$-linearly independent because y_r is transcendental over $\mathbb{F}_r$. Therefore, Σ is $\mathbb{F}_r$-linearly independent because a linear combination of its elements vanishes if and only if each homogeneous component vanishes.

The minimality of the equation $x_r^{e_r}=p_r^{h_r}y_r$ is a consequence of $\gcd(h_r,e_r)=1$. □

Corollary 4.8. *Consider a polynomial $\psi\in\mathbb{F}_r[y]$ with $\psi(0)\ne0$. Then, $\psi(y_r)\in\Delta$ is a prime element in $\mathcal{G}r(\mu)$ if and only if ψ is irreducible in $\mathbb{F}_r[y]$.*

Proof. If $\psi(y_r)$ is a prime element in $\mathcal{G}r(\mu)$, then it is a prime element in Δ and Theorem 4.3 shows that ψ is irreducible.

Conversely, if ψ is irreducible, consider $\mathbb{F}'=\mathbb{F}_r[y]/(\psi)$ and denote by $z\in\mathbb{F}'$ the class of y. By Theorem 4.7, $\mathcal{G}r(\mu)/\psi(y_r)\mathcal{G}r(\mu)\simeq\mathbb{F}'[p,p^{-1}][x]$, where p is an indeterminate and x satisfies $x^{e_r}=p^{h_r}z$. Since $\psi(0)\ne0$, we have $z\ne0$ and $\mathbb{F}'[p,p^{-1}][x]$ is an integral domain. Hence, $\psi(y_r)\mathcal{G}r(\mu)$ is a prime ideal. □

We may now use Theorems 4.1 and 4.3 to derive some more properties of the residual polynomials.

Corollary 4.9. *Let $r>0$ and consider a nonzero $g\in\mathcal{P}_\alpha(\mu)$.*

(1) *The j-th coefficient of $R_{r,\alpha}(g)$ is non-zero if and only if $\mu_{r-1}(a_{s_j})=\alpha_j$.*

(2) $\deg R_{r,\alpha}(g) = \lfloor s'(g)/e_r \rfloor$ *and* $\operatorname{ord}_y(R_{r,\alpha}(g)) = \lfloor s(g)/e_r \rfloor$.
(3) $\deg R_r(g) = (s'(g) - s(g))/e_r$ *and* $R_r(g)(0) \neq 0$.

Proof. By Lemma 3.14, the j-th coefficient of $R_{r,\alpha}(g)$ vanishes if $\mu_{r-1}(a_{s_j}) > \alpha_j$. Otherwise, $R_{r-1,\alpha_j}(a_{s_j})(z_{r-1}) \neq 0$ by equation (15). This proves (1), and the other two items are an easy consequence. $\square$

The next result is an immediate consequence of Theorem 4.1 and Corollary 4.9.

Corollary 4.10. *For non-zero $g, h \in K[x]$, the following conditions are equivalent:*
(1) $g \sim_\mu h$.
(2) $\mu(g) = \mu(h)$ *and* $R_{r,\alpha}(g) = R_{r,\alpha}(h)$ *for* $\alpha = \mu(g)$.
(3) $S_{\nu_r}(g) = S_{\nu_r}(h)$ *and* $R_r(g) = R_r(h)$. $\square$

Corollary 4.11. *For any non-zero $g \in K[x]$, let $\alpha = \mu(g)$. Then,*

$$\mathcal{R}(g) = y_r^{\lceil s_r(\alpha)/e_r \rceil} R_{r,\alpha}(g)(y_r)\Delta = y_r^{\lceil s(g)/e_r \rceil} R_r(g)(y_r)\Delta.$$

Proof. By Theorem 4.1, $H_\mu(g) = x_r^{s_r(\alpha)} p_r^{u_r(\alpha)} R_{r,\alpha}(g)(y_r)$. If $s_r(\alpha) = 0$, then $\mathcal{R}(g) = H_\mu(g)\mathcal{G}r(\mu) \cap \Delta = R_{r,\alpha}(g)(y_r)\Delta$, because p_r is a unit. If $s_r(\alpha) > 0$, then $\lceil s_r(\alpha)/e_r \rceil = 1$, and the defining equation of $s_r(\alpha)$ given in Definition 3.12 shows that

$$s_r(-\alpha) = e_r - s_r(\alpha), \qquad u_r(-\alpha) = -h_r - u_r(\alpha).$$

A polynomial $h \in K[x]$ satisfies $H_\mu(gh) \in \Delta$ if and only if $\mu(h) = -\alpha$; in this case, $H_\mu(h) = x_r^{e_r - s_r(\alpha)} p_r^{-h_r - u_r(\alpha)} R_{r,-\alpha}(h)(y_r)$, by Theorem 4.1. Hence,

$$\mathcal{R}(g) = \{y_r R_{r,\alpha}(g)(y_r) R_{r,-\alpha}(h)(y_r) \mid \mu(h) = -\alpha\} \subset y_r R_{r,\alpha}(g)(y_r)\Delta.$$

Since $y_r R_{r,\alpha}(g)(y_r) = H_\mu(g) x_r^{e_r - s_r(\alpha)} p_r^{-h_r} \in \mathcal{R}(g)$, we have $\mathcal{R}(g) = y_r R_{r,\alpha}(g)(y_r)\Delta$.

Finally, $y_r^{\lceil s_r(\alpha)/e_r \rceil} R_{r,\alpha}(g)(y_r) = y_r^{\lceil s(g)/e_r \rceil} R_r(g)(y_r)$, by (2) of Corollary 4.9. $\square$

Corollary 4.12. *Let $\alpha \in \Gamma(\mu)$.*
(1) $R_{r,\alpha}(g + h) = R_{r,\alpha}(g) + R_{r,\alpha}(h)$ *for all* $g, h \in \mathcal{P}_\alpha(\mu)$.
(2) *If* $\beta \in \Gamma_{r-1}$, *then* $R_{r,\alpha+\beta}(gh) = R_{r,\alpha}(g) R_{r,\beta}(h)$ *for all* $g \in \mathcal{P}_\alpha(\mu)$, $h \in \mathcal{P}_\beta(\mu)$.
(3) $R_r(gh) = R_r(g) R_r(h)$ *for all* $g, h \in K[x]$.

Proof. For $r = 0$ the identities are easy to check. If $r > 0$, then equation (1) and Theorems 4.1, 4.3 show that:

$$\begin{array}{ll} \varphi_r(\alpha) R_{r,\alpha}(g+h) = \varphi_r(\alpha) R_{r,\alpha}(g) + \varphi_r(\alpha) R_{r,\alpha}(h), & \text{for } g, h \in \mathcal{P}_\alpha(\mu) \\ \varphi_r(\alpha+\beta) R_{r,\alpha+\beta}(gh) = \varphi_r(\alpha) R_{r,\alpha}(g) \varphi_r(\beta) R_{r,\beta}(h), & \text{for } g \in \mathcal{P}_\alpha(\mu),\ h \in \mathcal{P}_\beta(\mu) \\ x_r^{s(gh)} p_r^{u(gh)} R_r(gh) = x_r^{s(g)+s(h)} p_r^{u(g)+u(h)} R_r(g) R_r(h), & \text{for } g, h \in K[x] \end{array}$$

The first equality proves (1). The second equality proves (2) because $s_r(\beta) = 0$, and this leads to $s_r(\alpha + \beta) = s_r(\alpha)$, $u_r(\alpha + \beta) = u_r(\alpha) + u_r(\beta)$. The third equality proves (3) by Corollary 2.7. $\square$

Data comparison of optimal MacLane chains. Suppose that the given MacLane chain of μ as in (4) is optimal. By Proposition 3.6, any other optimal MacLane chain of μ is obtained by replacing the key polynomials $\phi_1, \dots, \phi_r$ with another family $\phi_1^*, \dots, \phi_r^*$ such that

$$\phi_i^* = \phi_i + a_i, \quad \deg a_i < m_i, \quad \mu_i(a_i) \geq \mu_i(\phi_i).$$

Take $\eta_0 := 0 \in \mathbb{F}$. For every $1 \leq i \leq r$ consider the following element $\eta_i \in \mathbb{F}_i$:

$$\eta_i := \begin{cases} 0, & \text{if } \mu_i(a_i) > \mu_i(\phi_i) \quad (\text{i.e. } \phi_i^* \sim_{\mu_i} \phi_i), \\ R_i(a_i) \in \mathbb{F}_i^*, & \text{if } \mu_i(a_i) = \mu_i(\phi_i) \quad (\text{i.e. } \phi_i^* \not\sim_{\mu_i} \phi_i). \end{cases} \tag{16}$$

Since $\deg a_i < \deg \phi_i$, we have $\mu_i(a_i) = \mu_{i-1}(a_i) \in \Gamma_{i-1}$. If $e_i > 1$, then $\mu_i(\phi_i) = \mu_{i-1}(\phi_i) + \nu_i \notin \Gamma_{i-1}$, so that $\mu_i(a_i)$ cannot be equal to $\mu_i(\phi_i)$. In other words,

$$e_i > 1 \implies \phi_i^* \sim_{\mu_i} \phi_i \implies \eta_i = 0. \tag{17}$$

By Proposition 3.6, the data $m_i, h_i, e_i, f_i, V_i, \ell_i, \ell_i'$ coincide for both MacLane chains. The next result describes the relationship between the data $x_i, p_i, y_i, z_i, \psi_i$ and the operators $R_{i,\alpha}$ attached to the optimal MacLane chain (4) with the analogous data $x_i^*, p_i^*, y_i^*, z_i^*, \psi_i^*$ and operators $R_{i,\alpha}^*$ attached to the optimal MacLane chain determined by the choice of $\phi_1^*, \dots, \phi_r^*$ as key polynomials.

Lemma 4.13. *With the above notation,*

$$\begin{array}{ll} p_i^* = p_i, \quad x_i^* = x_i + p_i^{h_i}\eta_i, \quad y_i^* = y_i + \eta_i, & 0 \le i \le r, \\ z_i^* = z_i + \eta_i, \quad \psi_i^*(y) = \psi_i(y - \eta_i), & 0 \le i < r, \\ R_{i,\alpha}^*(g)(y) = R_{i,\alpha}(g)(y - \eta_i), & 0 \le i \le r, \ g \in \mathcal{P}_\alpha(\mu_i). \end{array}$$

Proof. Let us first prove that $p_i^* = p_i$ and $x_i^* = x_i + p_i^{h_i}\eta_i$ by induction on i. Clearly, $p_0^* = \mathrm{H}_{\mu_0}(\pi) = p_0$ and $x_0^* = \mathrm{H}_{\mu_0}(x) = x_0$. Suppose that the two identities hold for an index $i < r$, and let us deduce them for the index $i+1$. If $e_i = 1$, then $\ell_i = 0$, $\ell_i' = 1$, and $\pi_{i+1} = \pi_i$, $\pi_{i+1}^* = \pi_i^*$; thus, $p_{i+1}^* = p_i^* = p_i = p_{i+1}$. If $e_i > 1$, then $\eta_i = 0$ and $p_{i+1}^* = (x_i^*)^{\ell_i}(p_i^*)^{\ell_i'} = (x_i)^{\ell_i}(p_i)^{\ell_i'} = p_{i+1}$.

If $\phi_i^* \sim_{\mu_i} \phi_i$, we have $\Phi_{i+1}^* = \phi_i^*(\pi_i^*)^{-V_i} \sim_{\mu_i} \phi_i\pi_i^{-V_i} = \Phi_{i+1}$, so that $x_{i+1}^* = x_{i+1}$. If $\phi_i^* \not\sim_{\mu_i} \phi_i$, we have necessarily $e_i = 1$ by (17), and

$$\mu_{i-1}(a_i) = \mu_i(a_i) = \mu_i(\phi_i) = \mu_{i-1}(\phi_i) + \nu_i = w_i + \frac{h_i}{e(\mu_i)} = w_i + \frac{h_i}{e(\mu_{i-1})}.$$

Hence, $N_i(a_i)$ is the point $(0, (V_i + h_i)/e(\mu_{i-1}))$ and $R_i(a_i) = \eta_i \in \mathbb{F}_i^*$ is a constant polynomial. By Theorem 4.1, $\mathrm{H}_{\mu_i}(a_i) = p_i^{V_i+h_i}R_i(a_i) = p_i^{V_i+h_i}\eta_i$. Therefore,

$$x_{i+1}^* = \mathrm{H}_{\mu_i}(\Phi_{i+1}^*) = \mathrm{H}_{\mu_i}(\phi_i^*(\pi_i^*)^{-V_i}) = \mathrm{H}_{\mu_i}(\phi_i + a_i)(p_i^*)^{-V_i} = x_{i+1} + p_i^{h_i}\eta_i.$$

The identity $y_i^* = y_i + \eta_i$ follows immediately from the two previous identities, and it trivially implies $z_i^* = z_i + \eta_i$ for all $i < r$. Since $\psi_i, \psi_i^* \in \mathbb{F}_i[y]$ are the minimal polynomials over $\mathbb{F}_i$ of $z_i, z_i^* \in \mathbb{F}_{i+1}$, respectively, we deduce that $\psi_i^*(y) = \psi_i(y - \eta_i)$.

Finally, for any nonzero $g \in \mathcal{P}_\alpha(\mu_i)$, Theorem 4.1 shows that

$$(x_i)^{s_i(\alpha)}(p_i)^{u_i(\alpha)}R_{i,\alpha}(g)(y_i) = \mathrm{H}_{\mu_i}(\phi_i) = (x_i^*)^{s_i(\alpha)}(p_i^*)^{u_i(\alpha)}R_{i,\alpha}^*(g)(y_i^*).$$

We have seen that $p_i = p_i^*$. If $e_i > 1$, then $x_i = x_i^*$, and if $e_i = 1$ we have $s_i(\alpha) = 0$. In both cases we get $R_{i,\alpha}(g)(y_i) = R_{i,\alpha}^*(g)(y_i^*) = R_{i,\alpha}^*(g)(y_i + \eta_i)$, which implies $R_{i,\alpha}(g)(y) = R_{i,\alpha}^*(g)(y + \eta_i)$ by Theorem 4.3. □

5. Canonical decomposition of the set of key polynomials

Let μ be an inductive valuation and denote $\Delta = \Delta(\mu)$. In this section we want to study the fiber of any $\mathcal{L} \in \operatorname{Max}(\Delta)$ under the mapping:

$$\mathcal{R}\colon \operatorname{KP}(\mu) \longrightarrow \operatorname{Max}(\Delta), \qquad \phi \mapsto \mathcal{R}(\phi) = \operatorname{Ker}(\Delta \to \mathbb{F}_\phi).$$

It is hard to analyze these subsets from a purely abstract perspective. Thus, we suppose that μ is equipped with a fixed MacLane chain of length r. We shall freely use all data and operators of the MacLane chain described in section 3.

For a non-zero $g \in K[x]$ we recall that $s(g) \le s'(g)$ are the abscissas of the end points of the ν_r-component of $N_r(g)$, if $r > 0$. We agree that $s(g) = 0$ if $r = 0$.

5.1. **Further properties of key polynomials.** Let us first obtain a criterion for a polynomial $g \in K[x]$ to be a key polynomial for μ in terms of ϕ_r-expansions.

Lemma 5.1. *A polynomial $g \in K[x]$ is μ-irreducible if and only if either:*
- *$s(g) = s'(g) = 1$, or*
- *$s(g) = 0$ and $R_r(g)$ is irreducible in $\mathbb{F}_r[y]$.*

Proof. By Theorem 4.1, $H_\mu(g) = x_r^{s(g)} p_r^{u(g)} R_r(g)(y_r)$. Since p_r is a unit and x_r is a prime (section 3.3), $H_\mu(g)$ is a prime if and only if either:
(i) $s(g) = 1$ and $R_r(g)(y_r)$ is a unit, or
(ii) $s(g) = 0$ and $R_r(g)(y_r)$ is a prime in $\mathcal{G}r(\mu)$.
By Theorem 4.3, (i) is equivalent to $s(g) = 1$ and $\deg R_r(g) = 0$, which is equivalent to $s(g) = s'(g) = 1$ by Corollary 4.9. By Corollary 4.8, (ii) is equivalent to $s(g) = 0$ and $R_r(g)$ irreducible in $\mathbb{F}_r[y]$. □

Lemma 5.2. *If $r > 0$, a monic $\phi \in K[x]$ is a key polynomial for μ if and only if one of the two following conditions is satisfied:*
(1) *$\deg \phi = m_r$ and $\phi \sim_\mu \phi_r$.*
(2) *$s(\phi) = 0$, $\deg \phi = s'(\phi) m_r$ and $R_r(\phi)$ is irreducible in $\mathbb{F}_r[y]$.*
In case (2), $\deg \phi = e_r(\deg R_r(\phi)) m_r$, $N_r(\phi) = S_{\nu_r}(\phi)$ and $R_r(\phi) \in \mathbb{F}_r[y]$ is monic.

Proof. The characterization of key polynomials follows immediately from Lemma 1.4 and the criteria of Lemmas 2.10 and 5.1.

In case (2), clearly $N_r(\phi) = S_{\nu_r}(\phi)$. By Corollary 4.9, $s'(\phi) = e_r \deg R_r(\phi)$, and the polynomial $R_r(\phi)$ is monic by equation (11) and item (1) of Corollary 4.12. □

The next result is a consequence of Theorem 4.1, Corollary 4.11 and Lemma 5.2.

Corollary 5.3. *For any $\phi \in \mathrm{KP}(\mu)$, we have:*

$$\begin{array}{lll} H_\mu(\phi) = H_\mu(\phi_r) = x_r p_r^{V_r}, & \mathcal{R}(\phi) = y_r \Delta, & \text{if } \phi \sim_\mu \phi_r, \\ H_\mu(\phi) = p_r^{(e_r V_r + h_r)\deg R_r(\phi)} R_r(\phi)(y_r), & \mathcal{R}(\phi) = R_r(\phi)(y_r)\Delta, & \text{if } \phi \not\sim_\mu \phi_r. \end{array} \quad \square$$

Definition 5.4. *For a non-zero $g \in K[x]$, we say that $N_{\mu,\phi}(g)$ is* one-sided of slope $-\nu$ *if $N_{\mu,\phi}(g) = S_\nu(g)$, $s(g) = 0$ and $s'(g) > 0$.*

Corollary 5.5.
(1) *$N_i(\phi_{i+1})$ is one-sided of slope $-\nu_i$, for all $1 \le i < r$.*
(2) *$R_i(\phi_{i+1}) = \psi_i$, the minimal polynomial of z_i over $\mathbb{F}_i$, for all $0 \le i < r$.*

Proof. The polynomial ϕ_{i+1} is a key polynomial for μ_i and $\phi_{i+1} \not\sim_{\mu_i} \phi_i$. Hence, it satifies (2) of Lemma 5.2. This proves (1).

By Corollary 5.3, $H_{\mu_i}(\phi_{i+1})$ is associate to $R_i(\phi_{i+1})(y_i)$ in $\mathcal{G}r(\mu_i)$. By Proposition 1.7, these elements belong to the kernel of $\mathcal{G}r(\mu_i) \to \mathcal{G}r(\mu_{i+1})$. Thus, $R_i(\phi_{i+1})(z_i) = 0$, and since $R_i(\phi_{i+1})$ is monic and irreducible, we have $R_i(\phi_{i+1}) = \psi_i$. □

5.2. **Analysis of the map** $\mathrm{KP}(\mu) \to \mathrm{Max}(\Delta)$**.**

Proposition 5.6. *Let $\phi, \phi' \in \mathrm{KP}(\mu)$. The following conditions are equivalent:*
(1) *$\mathcal{R}(\phi) = \mathcal{R}(\phi')$.*
(2) *$R_r(\phi) = R_r(\phi')$.*
(3) *$\phi \sim_\mu \phi'$.*
(4) *$H_\mu(\phi)$ and $H_\mu(\phi')$ are associate in $\mathcal{G}r(\mu)$.*
(5) *$\phi \mid_\mu \phi'$.*

Proof. If $\phi \sim_\mu \phi_r$, then $R_r(\phi)=y$ (for $r=0$) and $R_r(\phi)=1$ (for $r>0$), by equation (11). Otherwise, Lemma 5.2 shows that $R_r(\phi)$ is monic, irreducible and different from y, because $R_r(\phi)(0)\neq 0$. Therefore, Corollary 5.3 and Theorem 4.3 show that (1), (2) and (3) are equivalent. Clearly, (3) implies (4), and (4) implies (5). Finally, (5) implies $\mathcal{R}(\phi')\subset\mathcal{R}(\phi)$, and this implies (1), because $\mathcal{R}(\phi')$ is a maximal ideal. □

The analysis of the key polynomials provided by the use of a MacLane chain yields an intrinsic description of the mapping $\mathcal{R}\colon \operatorname{KP}(\mu)\to\operatorname{Max}(\Delta)$.

Theorem 5.7. *Let μ be an inductive valuation. The map $\mathcal{R}\colon \operatorname{KP}(\mu)\to\operatorname{Max}(\Delta)$ induces a bijection between $\operatorname{KP}(\mu)/\!\sim_\mu$ and $\operatorname{Max}(\Delta)$.*

Proof. By Proposition 5.6, $\mathcal{R}$ induces an injective mapping $\operatorname{KP}(\mu)/\!\sim_\mu\to\operatorname{Max}(\Delta)$.

Let us show that $\mathcal{R}$ is onto. A maximal ideal $\mathcal{L}$ in Δ corresponds to a monic irreducible polynomial $\psi\in\mathbb{F}_r[y]$, under the isomorphism $\Delta\simeq\mathbb{F}_r[y]$ of Theorem 4.3. If $\psi=y$, then $\mathcal{L}=\mathcal{R}(\phi_r)$, by Corollary 5.3. If $\psi\neq y$, then it suffices to show the existence of a key polynomial ϕ such that $R_r(\phi)=\psi$, again by Corollary 5.3.

If $r=0$, then any monic lifting $\phi\in\mathcal{O}[x]$ of ψ is a key polynomial with $R_0(\phi)=\psi$. Assume $r>0$ and take $f=\deg\psi$ and $\alpha=e_rf(w_r+\nu_r)\in\Gamma(\mu)$. By Corollary 4.6, there exists $g\in K[x]$ with $\mu(g)=\alpha$ and $R_{r,\alpha}(g)=\psi-y^f$. By dropping all terms with abscissa $s\geq e_rf$ from the ϕ_r-expansion of g, we may assume that $\deg g<e_rfm_r$. Then, $\phi:=\phi_r^{e_rf}+g$ is monic of degree e_rfm_r, and $R_{r,\alpha}(\phi)=R_{r,\alpha}(\phi_r^{e_rf})+R_{r,\alpha}(g)=\psi$, by the first item of Corollary 4.12 and equation (11). Since $R_{r,\alpha}(\phi)(0)=\psi(0)\neq 0$, we have $R_r(\phi)=R_{r,\alpha}(\phi)=\psi$. By Corollary 4.9, $s'(\phi)-s(\phi)=e_rf$; thus:

$$\deg\phi\geq s'(\phi)m_r\geq (s'(\phi)-s(\phi))m_r=e_rfm_r=\deg\phi.$$

Hence, $s(\phi)=0$ and $\deg\phi=s'(\phi)m_r$. Therefore, ϕ satisfies condition (2) of Lemma 5.2 and it is a key polynomial for μ. □

Corollary 5.8. *Let $\mathcal{P}\subset\operatorname{KP}(\mu)$ be a set of representatives of key polynomials under μ-equivalence. Then, the set $H\mathcal{P}=\{H_\mu(\phi)\mid\phi\in\mathcal{P}\}$ is a system of representatives of homogeneous prime elements of $\mathcal{G}r(\mu)$ up to associates in the algebra. Moreover, up to units in $\mathcal{G}r(\mu)$, for any non-zero $g\in K[x]$, there is a unique factorization:*

$$g\sim_\mu\prod\nolimits_{\phi\in\mathcal{P}}\phi^{a_\phi},\quad a_\phi=\operatorname{ord}_{\mu,\phi}(g).\tag{18}$$

Proof. By the definition of μ-irreducibility, all elements in $H\mathcal{P}$ are homogeneous prime elements, and they are pairwise non-associate by Proposition 5.6. As we saw in the proof of Lemma 5.1, every homogeneous prime element is associate either to $H_\mu(\phi_r)$ or to $\psi(y_r)$ for some irreducible polynomial $\psi\in\mathbb{F}_r[y]$. Corollary 5.3 and the proof of Theorem 5.7 show that $\psi(y_r)$ is associate to an element in $H\mathcal{P}$. Finally, every homogeneous element in $\mathcal{G}r(\mu)$ is a product of homogeneous prime elements, by Theorem 4.1 and Corollary 4.8. This implies the unique factorization (18). □

5.3. **Proper and strong key polynomials.** In this section, we assume that the given MacLane chain of μ is optimal. Thus, all numerical data e_r, m_r, etc. attached to the chain in section 3.2 are intrinsic. We may formulate two intrinsic distinctions between key polynomials, according to their degree.

Definition 5.9. *Let μ be an inductive valuation of depth r, and let $\phi\in\operatorname{KP}(\mu)$.*

We say that ϕ is a strong key polynomial *for μ if $r=0$ or $\deg\phi>m_r$.*

We say that ϕ is a proper key polynomial *for μ if $\deg\phi$ is a multiple of e_rm_r.*

*We say that $g\in K[x]$ is μ-*proper *if $\phi\nmid_\mu g$ for all improper key polynomials ϕ.*

In any MacLane chain, each ϕ_i is a proper key polynomial for μ_{i-1} by Lemma 5.2.

Let $\mathrm{KP}(\mu)^{\mathrm{str}}$, $\mathrm{KP}(\mu)^{\mathrm{pr}}$ denote the sets of strong and proper key polynomials for μ, respectively. Clearly, $\mathrm{KP}(\mu_0)^{\mathrm{str}} = \mathrm{KP}(\mu_0)^{\mathrm{pr}} = \mathrm{KP}(\mu_0)$, wheras for $r > 0$ Lemma 5.2 shows that

$$\begin{array}{ll} \mathrm{KP}(\mu)^{\mathrm{str}} \subsetneq \mathrm{KP}(\mu)^{\mathrm{pr}} = \mathrm{KP}(\mu), & \text{if } e_r = 1, \\ \mathrm{KP}(\mu)^{\mathrm{str}} = \mathrm{KP}(\mu)^{\mathrm{pr}} \subsetneq \mathrm{KP}(\mu), & \text{if } e_r > 1. \end{array}$$

Theorems 5.7 and 4.3 yield bijections

$$\mathrm{KP}(\mu)/\!\sim_\mu \longrightarrow \mathrm{Max}(\Delta) \longrightarrow \mathbb{P}(\mathbb{F}_r),$$

where $\mathbb{P}(\mathbb{F}_r)$ is the set of monic irreducible polynomials with coefficients in $\mathbb{F}_r$. The first bijection is canonical but the second one may depend on the choice of the optimal MacLane chain of μ.

Let $[\phi]$ denote the μ-equivalence class of the key polynomial ϕ. By Corollary 5.3, the composition of the above bijections maps:

$$[\phi] \mapsto \begin{cases} y, & \text{if } [\phi] = [\phi_r], \\ R_r(\phi)(y), & \text{if } [\phi] \neq [\phi_r]. \end{cases} \tag{19}$$

If $e_r > 1$, Theorem 4.3, Lemma 4.13, and equation (17) show that this map does not depend on the choice of the optimal MacLane chain. The distinguished "bad" class $[\phi_r]$ is intrinsic and it has special properties reflecting the fact that the prime ideal $x_r\mathcal{G}r(\mu)$ is ramified over the subalgebra $\Delta[p_r, p_r^{-1}]$ (Theorem 4.7). It is the only improper class; in other words, $\mathrm{KP}(\mu) = \mathrm{KP}(\mu)^{\mathrm{pr}} \cup [\phi_r]$.

If $e_r = 1$, Lemma 4.13 shows that for different choices of the optimal MacLane chains, the images of the map (19) replace y by $y + \eta$ for certain $\eta \in \mathbb{F}_r^*$. Thus, the class $[\phi_r]$ is not intrinsic. Actually, for any given $\phi \in \mathrm{KP}(\mu)$, we may find an optimal MacLane chain for μ such that $\phi \not\sim_\mu \phi_r$.

Corollary 5.10. *A key polynomial ϕ for μ is proper if and only if there exists a MacLane chain of μ such that $\phi \not\sim_\mu \phi_r$, where r is the length of the chain.* □

Lemma 5.11. *For non-zero $g, h \in K[x]$ with g μ-proper, we have $\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h)$.*

Proof. By Corollary 4.11 and Theorem 4.3, $\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h)$ is equivalent to the following equality, up to factors in $\mathbb{F}_r^*$:

$$y^{\lceil s(gh)/e_r \rceil} R_r(gh) = y^{\lceil s(g)/e_r \rceil} R_r(g) y^{\lceil s(h)/e_r \rceil} R_r(h).$$

By Lemma 2.6, $s(gh) = s(g) + s(h)$, and by Corollary 4.12, $R_r(gh) = R_r(g)R_r(h)$. Thus, we want to show that

$$\lceil (s(g) + s(h))/e_r \rceil = \lceil s(g)/e_r \rceil + \lceil s(h)/e_r \rceil. \tag{20}$$

If $e_r = 1$ this equality is obvious. If $e_r > 1$, we have $x_r \nmid H_\mu(g)$, because g is μ-proper and x_r is associate to $H_\mu(\phi_r)$. By Theorem 4.1, $x_r^{s(g)} \mid H_\mu(g)$, so that $s(g) = 0$ and (20) is obvious too. □

Proposition 5.12. *Let $\phi \in \mathrm{KP}(\mu)$ and $\mathcal{L} = \mathcal{R}(\phi)$. For any non-zero $g \in K[x]$:*

$$\mathrm{ord}_{\mathcal{L}}(\mathcal{R}(g)) = \begin{cases} \mathrm{ord}_{\mu,\phi}(g), & \textit{if } \phi \textit{ is proper}, \\ \lceil \mathrm{ord}_{\mu,\phi}(g)/e_r \rceil, & \textit{if } \phi \textit{ is improper}. \end{cases}$$

where $\mathrm{ord}_{\mathcal{L}}(\mathcal{R}(g))$ is the largest non-negative integer n such that $\mathcal{L}^n \mid \mathcal{R}(g)$.

Proof. Denote $a_\phi = \operatorname{ord}_{\mu,\phi}(g)$. If we apply $\mathcal{R}$ to both terms of the factorization (18), Lemma 5.11 shows that:

$$\mathcal{R}(g) = \mathcal{R}\left(\prod\nolimits_{\phi\in\mathcal{P}} \phi^{a_\phi}\right) = \prod\nolimits_{\phi\in\mathcal{P}} \mathcal{R}(\phi^{a_\phi}).$$

For all proper $\phi \in \mathcal{P}$ we have $\mathcal{R}(\phi^{a_\phi}) = \mathcal{R}(\phi)^{a_\phi}$ by Lemma 5.11. For the unique improper $\phi \in \mathcal{P}$ (if $e_r > 1$), we have $\mathcal{R}(\phi^{a_\phi}) = \mathcal{R}(\phi)^{\lceil a_\phi/e_r\rceil}$ by Corollary 4.11, equation (11) and Corollary 5.3. ☐

The next result follows from Proposition 5.12 and Corollary 5.3.

Corollary 5.13. *Let ϕ be a proper key polynomial for μ and denote $\psi = R_r(\phi)$. Then,* $\operatorname{ord}_\psi(R_r(g)) = \operatorname{ord}_{\mu,\phi}(g)$ *for any non-zero $g \in K[x]$.* ☐

6. MacLane-Okutsu invariants of prime polynomials

Let $\mathbb{P} = \mathbb{P}(\mathcal{O}_v) \subset \mathcal{O}_v[x]$ be the set of all monic irreducible polynomials in $\mathcal{O}_v[x]$. We say that an element in $\mathbb{P}$ is a *prime polynomial* with respect to v.

Let $F \in \mathbb{P}$ be a prime polynomial and fix $\theta \in \overline{K}_v$ a root of F. Let $K_F = K_v(\theta)$ be the finite extension of K_v generated by θ, $\mathcal{O}_F$ the ring of integers of K_F, $\mathfrak{m}_F$ the maximal ideal and $\mathbb{F}_F$ the residue class field. We have $\deg F = e(F)f(F)$, where $e(F)$, $f(F)$ are the ramification index and residual degree of K_F/K_v, respectively.

Lemma 6.1. *Let $F, F' \in \mathbb{P}$ be two prime polynomials, and let $\theta, \theta' \in \overline{K}_v$ be roots of F, F', respectively. Then, $v(F(\theta'))/\deg(F) = v(F'(\theta))/\deg(F')$.*

Proof. The value $v(F(\theta'))$ does not depend on the choice of the root θ'; hence,

$$\deg(F')v(F(\theta')) = v(\operatorname{Res}(F, F')) = \deg(F)v(F'(\theta)),$$

because $\operatorname{Res}(F, F') = \prod_{\theta\in Z(F)} F'(\theta) = \pm\prod_{\theta'\in Z(F')} F(\theta')$, where $Z(F)$ is the multiset of roots of F in $\overline{K}_v$, with due count of multiplicities if F is inseparable. ☐

In this section we look for properties of prime polynomials leading to a certain comprehension of the structure of the set $\mathbb{P}$. An inductive valuation μ admitting a key polynomial ϕ such that $\phi \mid_\mu F$ reveals many properties of F.

6.1. **Prime polynomials and inductive valuations.**

We apply inductive valuations μ on $K(x)$ to polynomials in $K_v[x]$, without any explicit mention to the natural extension of μ to $K_v(x)$ described in Proposition 3.8.

Theorem 6.2. *Let $F \in \mathbb{P}$ be a prime polynomial and $\theta \in \overline{K}_v$ a root of F. Let ϕ be a key polynomial for the inductive valuation μ. Then, $\phi \mid_\mu F$ if and only if $v(\phi(\theta)) > \mu(\phi)$. Moreover, if this condition holds, then:*

1. *Either $F = \phi$, or the Newton polygon $N_{\mu,\phi}(F)$ is one-sided of slope $-\nu$, where $\nu = v(\phi(\theta)) - \mu(\phi) \in \mathbb{Q}_{>0}$.*
2. *Let $\ell = \ell(N_{\mu,\phi}(F))$. Then, $F \sim_\mu \phi^\ell$ and* $\deg F = \deg \phi^\ell$. *In particular, $\mathcal{R}(F)$ is a power of the maximal ideal $\mathcal{R}(\phi)$.*

Proof. If $F = \phi$ the theorem is trivial. Assume $F \neq \phi$ and let $\theta_\phi \in \overline{K}_v$ be a root of ϕ.

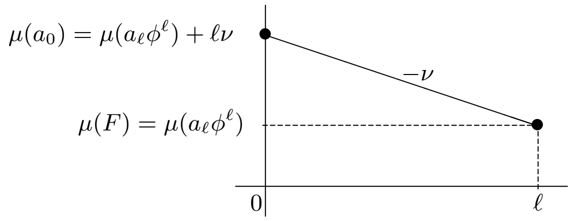
If $\phi \nmid_\mu F$, then $\mu(F) = v(F(\theta_\phi))$ by Proposition 1.9. Thus, Theorem 3.10 and Lemma 6.1 show that

$$\mu(\phi) \geq \mu(F)\deg\phi/\deg F = v(F(\theta_\phi))\deg\phi/\deg F = v(\phi(\theta)).$$

If $\phi \mid_\mu F$, let $g(x) = \sum_{j=0}^{k} b_j x^j \in \mathcal{O}_v[x]$ be the minimal polynomial of $\phi(\theta)$ over K_v. All roots of $g(x)$ in $\overline{K}_v$ have v-value equal to $\delta := v(\phi(\theta)) \geq 0$; hence,

$$v(b_0) = k\delta, \quad v(b_j) \geq (k-j)\delta,\ 1 \leq j < k, \quad v(b_k) = 0. \tag{21}$$

FIGURE 5. Newton polygon $N_{\mu,\phi}(F)$



Consider $G = \sum_{j=0}^{k} b_j\phi^j$ and denote $N := N_{\mu,\phi}$. The conditions in (21) imply that $N(G)$ is one-sided of slope $\mu(\phi)-\delta = -\nu$. Since $G(\theta) = 0$, the polynomial F divides G and Theorem 2.8 shows that

$$N^-(G) = N^-(F) + N^-(G/F). \tag{22}$$

By Lemma 2.1, $\ell(N^-(F)) = \operatorname{ord}_{\mu,\phi}(F) > 0$; hence, $N^-(G)$ has positive length too and ν must be positive. Since $N^-(G)$ is one-sided of slope $-\nu$, (22) shows that $N(F)$ is one-sided of slope $-\nu$ too.

This proves that $\phi \mid_\mu F$ if and only if $\nu > 0$, and also that (1) holds in this case.

Take $F = \sum_{s=0}^{\ell} a_s\phi^s$ the ϕ-expansion of F. By Lemma 6.1, $v(a_0(\theta_\phi)) = v(F(\theta_\phi)) = v(\phi(\theta))\deg F/\deg\phi$. On the other hand, since $\deg a_0 < \deg\phi$, Proposition 1.9 shows that $\mu(a_0) = v(a_0(\theta_\phi))$. Therefore, a look at Fig.5 shows that

$$\begin{aligned}\mu(a_\ell) + \ell(\mu(\phi)+\nu) = \mu(a_0) = v(a_0(\theta_\phi)) &= \frac{\deg F}{\deg\phi} v(\phi(\theta)) = \frac{\deg F}{\deg\phi}(\mu(\phi)+\nu) \\ &= \frac{\deg a_\ell + \ell\deg\phi}{\deg\phi}(\mu(\phi)+\nu) = \left(\frac{\deg a_\ell}{\deg\phi} + \ell\right)(\mu(\phi)+\nu).\end{aligned}$$

If $\deg a_\ell > 0$, then a_ℓ would be a monic polynomial contradicting Theorem 3.10:

$$\mu(a_\ell)/\deg a_\ell = (\mu(\phi)+\nu)/\deg\phi > \mu(\phi)/\deg\phi.$$

Hence, $a_\ell = 1$ and $\deg F = \ell\deg\phi$. By (1), $\mu(F) = \mu(\phi^\ell) < \mu(a_s\phi^s)$ for all $s < \ell$, so that $F \sim_\mu \phi^\ell$. The statement about $\mathcal{R}(F)$ follows from Proposition 5.12. ☐

Actually, if ϕ is proper the condition $\phi \mid_\mu F$ implies analogous properties of F with respect to the intermediate valuations of μ.

Corollary 6.3. *With the above notation, suppose that $\phi \mid_\mu F$ and μ admits a MacLane chain of length r as in (4) such that $\phi \not\sim_\mu \phi_r$. Then, for any $1 \le i \le r$, the Newton polygon $N_i(F)$ is one-sided of slope $-\nu_i$, we have $v(\phi_i(\theta)) = \mu(\phi_i)$ and*

$$F \sim_{\mu_{i-1}} \phi_i^{\ell_i}, \qquad \deg F = \deg\phi_i^{\ell_i}, \qquad R_{i-1}(F) = (\psi_{i-1})^{\ell_i}, \tag{23}$$

where $\ell_i := \ell(N_i(F))$. In particular, $\ell_i = e_i f_i \ell_{i+1}$ for all $1 \le i < r$.

Proof. Since $F \sim_\mu \phi^\ell$, we have $R_r(F) = R_r(\phi)^\ell$ by Corollaries 4.10 and 4.12. Hence, $\ell(N_r^-(F)) \ge \ell(S_{\nu_r}(F)) = e_r \deg R_r(F) > 0$, because $\deg R_r(\phi) > 0$ by Lemma 5.2. This implies that $\phi_r \mid_{\mu_{r-1}} F$ by Lemma 2.1. Therefore, $\phi_i \mid_{\mu_{i-1}} F$ for all $1 \le i \le r$, and (23) is a consequence of Theorem 6.2 and Corollaries 4.10, 4.12 and 5.5.

We have $F \ne \phi_i$ and $N_i(F)$ one-sided of slope $-\nu_i$ because otherwise $R_i(F)$ would be a constant, contradicting (23). Finally, $\mu_i(\phi_i) - \mu_{i-1}(\phi_i) = \nu_i = v(\phi_i(\theta)) - \mu_{i-1}(\phi_i)$ by Theorem 6.2. By Lemma 3.1, $\mu(\phi_i) = \mu_i(\phi_i) = v(\phi_i(\theta))$. ☐

If $F\neq\phi$, we may extend the given MacLane chain to a MacLane chain of length $r+1$ of the valuation $\mu'=[\mu;(\phi,\nu)]$ just by taking $\phi_{r+1}=\phi$, $\nu_{r+1}=\nu$.

$$\mu_0\ \stackrel{(\phi_1,\nu_1)}{\longrightarrow}\ \mu_1\ \stackrel{(\phi_2,\nu_2)}{\longrightarrow}\ \cdots\ \stackrel{(\phi_r,\nu_r)}{\longrightarrow}\ \mu_r=\mu\ \stackrel{(\phi_{r+1},\nu_{r+1})}{\longrightarrow}\ \mu_{r+1}=\mu'.$$

Since $s_{\mu'}(F)=0$ and $s'_{\mu'}(F)=\ell$, Corollary 4.9 shows that $\deg R_{r+1}(F)=\ell/e_{r+1}>0$. Let ψ be a monic irreducible factor of $R_{r+1}(F)$ in $\mathbb{F}_{r+1}[y]$. By Theorem 5.7, there exists $\phi'\in\operatorname{KP}(\mu')$ such that $\deg\phi'=e_{r+1}\deg\psi\deg\phi$ and $R_{r+1}(\phi')=\psi$. Since $R_{r+1}(\phi)=1$, Corollaries 4.10 and 5.10 show that $\phi'\not\sim_{\mu'}\phi$ and ϕ' is proper. By Corollary 5.13, $\phi'\mid_{\mu'}F$; hence, Theorem 6.2 yields

$$F\sim_{\mu'}(\phi')^{\ell'},\quad \deg F=\deg(\phi')^{\ell'},\quad R_{r+1}(F)=(\psi')^{\ell'},$$

for $\ell'=\deg F/\deg\phi'=\ell\deg\phi/\deg\phi'=\ell/(e_{r+1}\deg\psi)$.

The iteration of this procedure leads to a sequence of key polynomials with limit F in the v-adic topology.

We now deduce from Theorem 6.2 the fundamental result concerning factorization of polynomials over K_v. It has to be considered as a generalization of Hensel's lemma.

The *degree* of a maximal ideal $\mathcal{L}\in\operatorname{Max}(\Delta)$ is defined as $\deg\mathcal{L}:=\dim_{\mathbb{F}_r}(\Delta/\mathcal{L})$. If a MacLane chain of μ is given, then $\deg\mathcal{L}=\deg\psi$ for the unique monic irreducible polynomial $\psi\in\mathbb{F}_r[y]$ such that $\mathcal{L}=\psi(y_r)\Delta$, where r is the length of the chain.

Theorem 6.4. *Let ϕ be a proper key polynomial for the inductive valuation μ. Then, every monic $g\in\mathcal{O}_v[x]$ factorizes into a product of monic polynomials in $\mathcal{O}_v[x]$:*

$$g=g_0\,\phi^{\operatorname{ord}_\phi(g)}\prod\nolimits_{(\nu,\mathcal{L})}g_{\nu,\mathcal{L}},$$

where $-\nu$ runs on the slopes of $N^-_{\mu,\phi}(g)$. For each ν, let $\mu_\nu:=[\mu;(\phi,\nu)]$; then, $\mathcal{L}$ runs on the maximal ideals of $\Delta(\mu_\nu)$ dividing $\mathcal{R}_{\mu_\nu}(g)$. If e_ν is the least denominator of $e(\mu)\nu$, then

$$\deg g_0=\deg g-\ell(N^-_{\mu,\phi}(g))\deg\phi,\quad \deg g_{\nu,\mathcal{L}}=e_\nu\operatorname{ord}_{\mathcal{L}}(\mathcal{R}_{\mu_\nu}(g))\deg\mathcal{L}\deg\phi.$$

Moreover, if $\operatorname{ord}_{\mathcal{L}}(\mathcal{R}_{\mu_\nu}(g))=1$, then $g_{\nu,\mathcal{L}}$ is irreducible in $\mathcal{O}_v[x]$.

Proof. Let $g=F_1\cdots F_t$ be the factorization of g into a product of prime polynomials in $\mathcal{O}_v[x]$. Denote $\ell_j:=\ell\left(N^-_{\mu,\phi}(F_j)\right)=\operatorname{ord}_{\mu,\phi}(F_j)$ (Lemma 2.1). The factor g_0 is the product of all F_j satisfying $\phi\nmid_\mu F_j$. The factors F_j with $\phi\mid_\mu F_j$ have $\deg F_j=\ell_j\deg\phi$, by Theorem 6.2. By Theorem 2.8, $N^-_{\mu,\phi}(g)=\sum_j N^-_{\mu,\phi}(F_j)$; hence,

$$\deg g-\deg g_0=\sum_{\phi\mid_\mu F_j}\deg F_j=\sum_{\phi\mid_\mu F_j}\ell_j\deg\phi=\sum_j\ell_j\deg\phi=\ell\left(N^-_{\mu,\phi}(g)\right)\deg\phi.$$

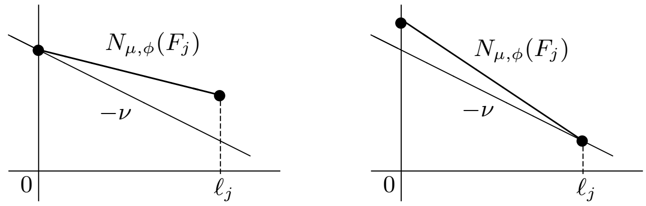
The factor $\phi^{\operatorname{ord}_\phi(g)}$ is the product of all F_j equal to ϕ. By Theorem 6.2, for the factors $F_j\neq\phi$ such that $\phi\mid_\mu F_j$, the Newton polygon $N_{\mu,\phi}(F_j)$ is one-sided of slope $-\nu$, where $-\nu$ is one of the slopes of $N^-_{\mu,\phi}(g)$, by Theorem 2.8. Along the discussion following Corollary 6.3, we saw that these F_j are μ_ν-proper and

$$\mathcal{R}_{\mu_\nu}(F_j)=\mathcal{L}^{\ell'_j},\quad \deg F_j=\ell'_je_\nu\deg\mathcal{L}\deg\phi$$

for a certain maximal ideal $\mathcal{L}$ in $\Delta(\mu_\nu)$. Since $s_{\mu_\nu}(F_j)=0$, Lemma 2.6 shows that $\phi\nmid_{\mu_\nu}F_j$, so that $\mathcal{L}\neq\mathcal{R}_{\mu_\nu}(\phi)$. Now, for a given pair $(\nu,\mathcal{L})$ we take $g_{\nu,\mathcal{L}}$ to be the product of all F_j such that $N_{\mu,\phi}(F_j)$ is one-sided of slope $-\nu$ and $\mathcal{R}_{\mu_\nu}(F_j)$ is a power of $\mathcal{L}$. Let $J_{\nu,\mathcal{L}}$ be the set of all indices j of the irreducible factors F_j of $g_{\nu,\mathcal{L}}$.

We claim that $\mathcal{L}\nmid\mathcal{R}_{\mu_\nu}(F_j)$ for all $j\notin J_{\nu,\mathcal{L}}$. In fact, if $\phi\nmid_\mu F_j$ or $N_{\mu,\phi}(F_j)$ is one-sided of a slope larger than $-\nu$, then $S_\nu(F_j)$ is a single point of abscissa zero (see Fig.6); by Lemma 2.9, $H_{\mu_\nu}(F_j)$ is a unit and $\mathcal{R}_{\mu_\nu}(F_j)=1$. If $F_j=\phi$ or $N_{\mu,\phi}(F_j)$ is one-sided of a slope

FIGURE 6. ν-component of $N_{\mu,\phi}(F_j)$ if $\phi \mid_\mu F_j$ and $j \notin J_{\nu,\mathcal{L}}$.



lower than $-\nu$, then $F_j \sim_{\mu_\nu} \phi^{\ell_j}$ (see Fig.6); by Proposition 5.12, $\mathcal{R}_{\mu_\nu}(F_j) = \mathcal{R}_{\mu_\nu}(\phi)^{\ell_j}$ is not divided by $\mathcal{L}$, because $\mathcal{L} \neq \mathcal{R}_{\mu_\nu}(\phi)$.

Therefore, from the equality $\mathcal{R}_{\mu_\nu}(g) = \prod_j \mathcal{R}_{\mu_\nu}(F_j)$ of Lemma 5.11, we deduce

$$\begin{aligned}\operatorname{ord}_{\mathcal{L}} \mathcal{R}_{\mu_\nu}(g) &= \sum\nolimits_j \operatorname{ord}_{\mathcal{L}} \mathcal{R}_{\mu_\nu}(F_j) = \sum\nolimits_{j \in J_{\nu,\mathcal{L}}} \operatorname{ord}_{\mathcal{L}} \mathcal{R}_{\mu_\nu}(F_j) \\ &= \sum\nolimits_{j \in J_{\nu,\mathcal{L}}} \deg F_j/(e_\nu \deg \mathcal{L} \deg \phi) = \deg g_{\nu,\mathcal{L}}/(e_\nu \deg \mathcal{L} \deg \phi).\end{aligned}$$

Finally, if $\operatorname{ord}_{\mathcal{L}} \mathcal{R}_{\mu_\nu}(g) = 1$, there is only one irreducible factor F_j dividing $g_{\nu,\mathcal{L}}$. $\square$

Theorem 6.5. *Let $F \in \mathbb{P}$ be a prime polynomial and let $\mu_{\infty,F}$ be the pseudo-valuation on $K[x]$ defined by $\mu_{\infty,F}(g) = v(g(\theta))$ for all $g \in K[x]$. An inductive valuation μ satisfies $\mu \le \mu_{\infty,F}$ if and only if there exists $\phi \in \operatorname{KP}(\mu)$ such that $\phi \mid_\mu F$. In this case, for a non-zero polynomial $g \in K[x]$, we have*

$$\mu(g) = \mu_{\infty,F}(g) \quad \textit{if and only if} \quad \phi \nmid_\mu g. \tag{24}$$

Proof. If $\mu \le \mu_{\infty,F}$, we may consider $\phi \in K[x]$ monic with minimal degree among all polynomials satisfying $\mu(\phi) < \mu_{\infty,F}(\phi)$. By Lemma 1.11, ϕ is a key polynomial for μ, and condition (24) is satisfied. In particular, $\phi \mid_\mu F$.

Conversely, suppose that $\phi \mid_\mu F$ for some $\phi \in \operatorname{KP}(\mu)$. Let us prove the inequality $\mu \le \mu_{\infty,F}$ and (24) by induction on the depth r of μ. The case $r = 0$ being trivial, suppose $r > 0$ and the statement holds for all valuations with lower depth.

Take a MacLane chain of μ. If $\phi \sim_\mu \phi_r$, then $\phi_r \mid_\mu F$ and $v(\phi_r(\theta)) > \mu(\phi_r)$ by Theorem 6.2. If $\phi \not\sim_\mu \phi_r$, then $v(\phi_r(\theta)) = \mu(\phi_r)$ by Corollary 6.3. In any case, $\mu(\phi_r) \le \mu_{\infty,F}(\phi_r)$. Now, for any $g \in K[x]$ with ϕ_r-expansion $g = \sum_{0 \le s} a_s \phi_r^s$, we have $\mu(a_s) = \mu_{r-1}(a_s) = \mu_{\infty,F}(a_s)$ by the induction hypothesis, since $\phi_r \nmid_{\mu_{r-1}} a_s$. Thus,

$$\mu_{\infty,F}(g) \ge \min_{0 \le s} \{\mu_{\infty,F}(a_s \phi_r^s)\} \ge \min_{0 \le s} \{\mu(a_s \phi_r^s)\} = \mu(g).$$

The initial argument shows then the existence of $\phi' \in \operatorname{KP}(\mu)$ such that $\phi' \mid_\mu F$ and (24) holds for ϕ'. By Theorem 6.2, $F \sim_\mu \phi^\ell$ for some $\ell > 0$, so that $\phi' \mid_\mu \phi$ and this implies $\phi \sim_\mu \phi'$ by Proposition 5.6. Hence, ϕ satisfies (24) as well. $\square$

Theorem 6.5 provides a device for the computation of $\mu_{\infty,F}$. Given $g \in K[x]$, one finds a pair (μ, ϕ) such that $\phi \mid_\mu F$ and $\phi \nmid_\mu g$, leading to $v(g(\theta)) = \mu(g)$. This yields a very efficient routine for the computation of the $\mathfrak{p}$-adic valuations attached to prime ideals $\mathfrak{p}$ in number fields [6, 8].

Corollary 6.6. *With the above notation, let $\theta_\phi \in \overline{K}_v$ be a root of ϕ.*

(1) *For any polynomial $g \in K[x]$ with $\deg g < \deg \phi$, we have $v(g(\theta_\phi)) = v(g(\theta))$. In particular, $e(\phi) \mid e(F)$.*
(2) *There is a canonical embedding $\mathbb{F}_\phi \to \mathbb{F}_F$, given by $g(\theta_\phi) + \mathfrak{m}_\phi \mapsto g(\theta) + \mathfrak{m}_F$ for any $g \in K[x]$ with $\deg g < \deg \phi$ such that $v(g(\theta_\phi)) \ge 0$.*

Proof. If a polynomial $g \in K[x]$ has $\deg g < \deg \phi$, then $\phi \nmid_\mu g$ and $v(g(\theta_\phi)) = \mu(g) = v(g(\theta))$, by Proposition 1.9 and Theorem 6.5, respectively. This proves (1).

Let us prove (2). Let $\mathcal{L}_F$ be the kernel of the canonical ring homomorphism

$$\Delta(\mu) \longrightarrow \mathbb{F}_F, \qquad g + \mathcal{P}_0^+(\mu) \mapsto g(\theta) + \mathfrak{m}_F.$$

Since $\mathcal{L}_F$ is a non-zero prime ideal of the PID $\Delta(\mu)$, it is a maximal ideal. By Theorem 6.2, $\mathcal{R}(\phi)^a = \mathcal{R}(F) \subset \mathcal{L}_F$ for a certain positive integer a. Since $\mathcal{R}(\phi)$ and $\mathcal{L}_F$ are maximal ideals, they coincide. By Proposition 1.12, the homomorphism $\Delta(\mu) \to \mathbb{F}_\phi$ given by $g + \mathcal{P}_0^+(\mu) \mapsto g(\theta) + \mathfrak{m}_\phi$ is onto and it has the same kernel. □

6.2. **Okutsu invariants of prime polynomials.** We keep dealing with a prime polynomial $F \in \mathbb{P}$ and a fixed root $\theta \in \overline{K}_v$ of F. Let $F_1, \dots, F_r \in \mathcal{O}[x]$ be monic polynomials such that $0 < \deg F_1 < \cdots < \deg F_r < \deg F$.

Denote $F_{r+1} := F$ and consider the following sequence of constants:

$$C_0 := 0; \quad C_i := v(F_i(\theta))/\deg F_i, \; 1 \le i \le r+1.$$

Note that $C_{r+1} = \infty$. We say that $[F_1, \dots, F_r]$ is an *Okutsu frame* of F if

$$\deg g < \deg F_{i+1} \implies v(g(\theta))/\deg g \le C_i < C_{i+1}, \tag{25}$$

for any monic polynomial $g(x) \in \mathcal{O}[x]$ and any $0 \le i \le r$.

Since v is discrete, every prime polynomial admits a finite Okutsu frame. The length r of the frame is called the *Okutsu depth* of F. Clearly, the depth r, the degrees $\deg F_i$ and the constants C_i attached to any Okutsu frame are intrinsic data of F and we may denote $C_i(F) := C_i$ for all $0 \le i \le r+1$. It is easy to deduce from (25) that $F_1, \dots, F_r$ are prime polynomials.

Theorem 6.7. *Consider an optimal MacLane chain of an inductive valuation μ as in (4). Then, $[\phi_1, \dots, \phi_r]$ is an Okutsu frame of every strong key polynomial ϕ for μ, and $C_i(\phi) = C_i(\mu)$ for all $1 \le i \le r$.*

Proof. Let $\phi \in \mathrm{KP}(\mu)^{\mathrm{str}}$, and let $\theta_\phi \in \overline{K}_v$ be a root of ϕ. By the optimality of the MacLane chain, $m_1 < \cdots < m_r < m_{r+1} := \deg \phi$. For any $0 \le i \le r$ and every monic polynomial g with $\deg g < m_{i+1}$, Proposition 1.9 and Lemma 3.1 show that

$$\mu_i(g) = \mu_{i+1}(g) = \cdots = \mu(g) = \mu_{\infty,\phi}(g).$$

These equalities hold in particular for ϕ_i. Hence, by Theorem 3.10:

$$v(g(\theta_\phi))/\deg g = \mu_i(g)/\deg g \le C(\mu_i) = \mu_i(\phi_i)/m_i = v(\phi_i(\theta_\phi))/m_i.$$

The inequality $C_i(\mu) < C_{i+1}(\mu)$ was proved at the beginning of section 3.1. □

Definition 6.8. *The* Okutsu bound *of $F \in \mathbb{P}$ is defined as $\delta_0(F) := \deg(F) C_r(F)$, where r is the Okutsu depth of F.*

We may attach to F a valuation $\mu_F \colon K(x)^* \to \mathbb{Q}$, determined by the following action on polynomials $g = \sum_{0 \le s} a_s F^s$ in terms of their F-expansion:

$$\mu_F(g) := \min_{0 \le s}\{\mu_{\infty,F}(a_s) + s\delta_0(F)\} = \min_{0 \le s}\{\mu_F(a_s F^s)\}.$$

The next result (a converse of Theorem 6.7) shows that μ_F is indeed a valuation.

Theorem 6.9. *Let $[F_1, \dots, F_r]$ be an Okutsu frame of a prime polynomial $F \in \mathbb{P}$. Then, μ_F is an inductive valuation admitting an optimal MacLane chain*

$$\mu_0 = \mu_{F_1} \xrightarrow{(F_1,\nu_1)} \mu_1 = \mu_{F_2} \xrightarrow{(F_2,\nu_2)} \cdots \longrightarrow \mu_{r-1} = \mu_{F_r} \xrightarrow{(F_r,\nu_r)} \mu_F,$$

with $\nu_i = v(F_i(\theta)) - \delta_0(F_i)$ for $1 \le i \le r$, being $\theta \in \overline{K}_v$ a root of F.

Moreover, F is a strong key polynomial for μ_F as a valuation on $K_v(x)$.

Proof. Denote $F_{r+1} := F$. Since F_1 is a monic polynomial with minimal degree among all polynomials g satisfying $\mu_0(g) < \mu_{\infty,F}(g)$, Lemma 1.11 shows that F_1 is a (strong) key polynomial for μ_0 and $F_1 \mid_{\mu_0} F$. As a key polynomial for μ_0, $\overline{F}_1 \in \mathbb{F}[y]$ is irreducible. This implies that F_1 has Okutsu depth zero, so that $\delta_0(F_1) = \deg(F_1)C_0(F_1) = 0$ and $\mu_{F_1} = \mu_0$. This proves the theorem in the case $r = 0$.

If $r > 0$, we have proved the following conditions for the index $i = 1$:

(a) μ_{F_i} is a valuation admitting an optimal MacLane chain

$$\mu_0 = \mu_{F_1} \xrightarrow{(F_1,\nu_1)} \mu_1 = \mu_{F_2} \xrightarrow{(F_2,\nu_2)} \cdots \longrightarrow \mu_{i-1} = \mu_{F_i},$$

with $\nu_j = v(F_j(\theta)) - \delta_0(F_j)$ for $1 \le j < i$.

(b) F_i is a strong key polynomial for μ_{F_i} and $F_i \mid_{\mu_{F_i}} F$.

We want to see that (a) and (b) hold for $i = r + 1$. It suffices to show that if these conditions hold for an index $1 \le i \le r$, then they hold for the index $i + 1$.

Since $F_i \mid_{\mu_{F_i}} F$, Theorem 6.2 shows that $\delta_0(F_i) = \mu_{F_i}(F_i) < v(F_i(\theta))$, and Corollary 6.6 shows that $\mu_{F_i}(a) = \mu_{\infty,F_i}(a) = \mu_{\infty,F}(a)$ for all $a \in K[x]$ with $\deg a < \deg F_i$. This implies $\mu := [\mu_{F_i}; (F_i, \nu_i)] \le \mu_{\infty,F}$, where $\nu_i = v(F_i(\theta)) - \delta_0(F_i)$.

Let ϕ be a monic polynomial with minimal degree among all polynomials g satisfying $\mu(g) < \mu_{\infty,F}(g)$. By Lemma 1.11, ϕ is a key polynomial for μ and $\phi \mid_\mu F$. By Proposition 1.7, F_i is a key polynomial for μ; hence, Lemma 2.11 shows that

$$\frac{v(\phi(\theta))}{\deg \phi} > \frac{\mu(\phi)}{\deg \phi} = C(\mu) = \frac{\mu(F_i)}{\deg F_i} = \frac{\mu_{F_i}(F_i) + \nu_i}{\deg F_i} = \frac{v(F_i(\theta))}{\deg F_i} = C_i(F). \tag{26}$$

By (25), we have necessarily $\deg \phi \ge \deg F_{i+1}$. On the other hand, by (25), (26) and Theorem 3.10, we have

$$v(F_{i+1}(\theta))/\deg F_{i+1} > C_i(F) = C(\mu) \ge \mu(F_{i+1})/\deg F_{i+1}.$$

Hence, $v(F_{i+1}(\theta)) > \mu(F_{i+1})$ and the minimality of $\deg \phi$ implies $\deg \phi = \deg F_{i+1}$. By Lemma 1.11, F_{i+1} is a key polynomial for μ and $F_{i+1} \mid_\mu F$. The inequality $\deg F_{i+1} > \deg F_i$ shows that F_{i+1} is a strong key polynomial for μ.

Let $\theta_{i+1} \in \overline{K}_v$ be a root of F_{i+1}. Since $F_{i+1} \mid_\mu F$, Corollary 6.6 shows that $v(a(\theta_{i+1})) = v(a(\theta))$ for any $a \in K[x]$ with $\deg a < \deg F_{i+1}$. In particular, $C_j(F_{i+1}) = C_j(F)$ for all $j \le i$, and $[F_1, \dots, F_i]$ is an Okutsu frame of F_{i+1}. By (26) we have:

$$\delta_0(F_{i+1}) = \deg F_{i+1}\, C_i(F_{i+1}) = \deg F_{i+1}\, C_i(F) = \deg F_{i+1} C(\mu). \tag{27}$$

Finally, let us show that $\mu = \mu_{F_{i+1}}$. Let $g = \sum_{0 \le s} a_s (F_{i+1})^s$ be the F_{i+1}-expansion of a polynomial $g \in K[x]$. Since $F_{i+1} \in \mathrm{KP}(\mu)$, we have:

- $\mu(a_s) = \mu_{\infty,F_{i+1}}(a_s) = \mu_{F_{i+1}}(a_s)$, by Proposition 1.9.
- $\mu(F_{i+1}) = \deg F_{i+1} C(\mu) = \delta_0(F_{i+1}) = \mu_{F_{i+1}}(F_{i+1})$, by Lemma 2.11 and (27).
- $\mu(g) = \min_{0 \le s}\{\mu(a_s (F_{i+1})^s)\} = \min_{0 \le s}\{\mu_{F_{i+1}}(a_s (F_{i+1})^s)\} = \mu_{F_{i+1}}(g)$. ☐

Corollary 6.10. *The MacLane depth of an inductive valuation μ is equal to the Okutsu depth of any strong key polynomial for μ. The Okutsu depth of a prime polynomial F is equal to the MacLane depth of the canonical valuation μ_F.* ☐

Corollary 6.11. *Let μ be an inductive valuation and F a prime polynomial. Then, $\mu = \mu_F$ if and only if F is a strong key polynomial for $\mu \otimes_K K_v$.*

Proof. If $\mu = \mu_F$, then $F \in \mathrm{KP}(\mu)^{\mathrm{str}}$ by Theorem 6.9. Conversely, suppose that $F \in \mathrm{KP}(\mu)^{\mathrm{str}}$ and consider an optimal MacLane chain of μ as in (4).

By Corollary 6.3, $\nu_i = v(\phi_i(\theta)) - \mu_{i-1}(\phi_i)$ for all $1 \le i \le r$. By Theorem 6.7, $[\phi_1, \dots, \phi_r]$ is an Okutsu frame of F. By Theorem 6.9, we get recursively $\mu_{i-1} = \mu_{\phi_i}$ for all $1 \le i \le r$, and $\mu = \mu_F$. $\square$

Let F be a prime polynomial of Okutsu depth r, and let $f_r := \deg \mathcal{R}_{\mu_F}(F) = \deg R_r(F)$ with respect to any optimal MacLane chain of μ_F. An *Okutsu invariant* of F is a rational number that depends only on the basic MacLane invariants of μ_F and the number f_r. That is, on $e_0, \dots, e_r, f_0, \dots, f_r, h_1, \dots, h_r$.

As shown in (7), the ramification index, residual degree, and Okutsu bound of F are Okutsu invariants:

$$e(F) = e_0 \cdots e_r, \qquad f(F) = f_0 \cdots f_r, \qquad \delta_0(F) = e_r f_r (w_r + \nu_r),$$

The *index*, the *exponent* and the *conductor* of a prime polynomial are also Okutsu invariants admitting explicit formulas in terms of the basic invariants e_i, f_i, h_i [13].

Proposition 6.12. *Let $F, G \in \mathbb{P}$ be two prime polynomials of the same degree. The following conditions are equivalent:*

(1) *$v(G(\theta)) > \delta_0(F)$, where $\theta \in \overline{K}_v$ is a root of F.*
(2) *$F \sim_{\mu_F} G$.*
(3) *$\mu_F = \mu_G$ and $\mathcal{R}(F) = \mathcal{R}(G)$, where $\mathcal{R} := \mathcal{R}_{\mu_F} = \mathcal{R}_{\mu_G}$.*

If they hold we say that F and G are Okutsu equivalent *and we write $F \approx G$.*

Proof. Since $\deg(F - G) < \deg F$, we have $\mu_F(F - G) = v((F - G)(\theta)) = v(G(\theta))$, by the definition of μ_F. Since $\delta_0(F) = \mu_F(F)$, (1) and (2) are equivalent.

Also, (2) and (3) are equivalent by Proposition 5.6 and Corollary 6.11. $\square$

The symmetry of condition (3) shows that $\approx$ is an equivalence relation on the set $\mathbb{P}$ of prime polynomials. Also, conditions (1) and (3) show that two polynomials in the same class are close enough to share the same Okutsu invariants.

Let us obtain a parameterization of the quotient set $\mathbb{P}/\!\approx$ by an adequate space. The *MacLane space* of the valued field (K, v) is defined to be the set

$$\mathbb{M} = \left\{ (\mu, \mathcal{L}) \mid \mu \in \mathbb{V}^{\mathrm{ind}},\ \mathcal{L} \in \operatorname{Max}(\Delta(\mu)),\ \mathcal{L} \text{ strong} \right\},$$

where $\mathcal{L}$ *strong* means that $\mathcal{L} = \mathcal{R}_\mu(\phi)$ for a strong key polynomial ϕ.

The next result is a consequence of Corollary 6.11 and Proposition 6.12.

Theorem 6.13. *The following mapping is bijective:*

$$\mathbb{M} \longrightarrow \mathbb{P}/\!\approx, \qquad (\mu, \mathcal{L}) \mapsto \{\phi \in \mathrm{KP}(\mu \otimes_K K_v) \mid \mathcal{R}_\mu(\phi) = \mathcal{L}\}.$$

The inverse map is determined by $F \mapsto (\mu_F, \mathcal{R}_{\mu_F}(F))$. $\square$

In this result we must consider $\mu \otimes_K K_v$ because the set $\mathrm{KP}(\mu) = \mathrm{KP}(\mu \otimes_K K_v) \cap \mathcal{O}[x]$ is too small to give the whole Okutsu class attached to $(\mu, \mathcal{L})$. On the other hand, the canonical map $\Delta(\mu) \to \Delta(\mu \otimes_K K_v)$ is an isomorphism and we do not need to distinguish between maximal ideals of the two algebras.

The bijection $\mathbb{M} \to \mathbb{P}/\!\approx$ has applications to the computational representation of prime polynomials, because the elements in the MacLane space may be described by discrete parameters which are easily handled by a computer. This provides an efficient manipulation of approximations to the irreducible factors in $K_v[x]$ of a polynomial with coefficients in K [8].

7. Limits of inductive valuations

MacLane showed that there are two kinds of valuations that may be obtained as limits of inductive valuations: those of finite and infinite depth. In this section we briefly review them. Let us first describe a canonical tree structure on $\mathbb{V}^{\mathrm{ind}}$.

Definition 7.1. *For $\mu,\mu'\in\mathbb{V}^{\mathrm{ind}}$, we say that μ is the previous node of μ', and we write $\mu\prec\mu'$, if $\mu'=[\mu;(\phi,\nu)]$ for some strong key polynomial ϕ for μ and some positive rational number ν.*

We denote by $(\mathbb{V}^{\mathrm{ind}},\prec)$ the oriented graph whose set of vertices is $\mathbb{V}^{\mathrm{ind}}$, and there is an edge from μ to μ' if and only if $\mu\prec\mu'$

Proposition 3.6 shows that $(\mathbb{V}^{\mathrm{ind}},\prec)$ is a connected tree with root node μ_0, and any optimal MacLane chain for $\mu\in\mathbb{V}^{\mathrm{ind}}$ yields the unique path joining μ with the root node. In particular, the length of this path is the MacLane depth of μ.

Since the tree structure is determined by the optimal MacLane chains, the bijective mapping $\mathbb{V}^{\mathrm{ind}}(K)\to\mathbb{V}^{\mathrm{ind}}(K_v)$ established in Proposition 3.8 is a tree isomorphism.

7.1. Limit valuations with infinite depth.

A *leaf* of $(\mathbb{V}^{\mathrm{ind}},\prec)$ is an infinite path

$$\mu_0\prec\mu_1\prec\cdots\prec\mu_n\prec\cdots$$

A leaf has attached an infinite number of MacLane invariants e_i,f_i,h_i,m_i, which do not depend on the choice of the strong key polynomials ϕ_i used to construct μ_i from μ_{i-1}. Since the degrees m_i of these polynomials grow strictly, for any $g\in K[x]$ we have $\deg g<m_{i+1}$ for a sufficiently advanced index i. Hence, by Lemma 3.1:

$$\mu_i(g)=\mu_j(g),\quad \text{for all } j\ge i.$$

Thus, any leaf determines a limit valuation $\mu_\infty=\lim\mu_n$, defined by $\mu_\infty(g)=\mu_i(g)$ for a sufficiently advanced index i such that the value $\mu_i(g)$ stabilizes.

Since $m_{i+1}=e_if_im_i$, we have $e_if_i>1$ for all $i\ge1$. Therefore, either $\lim e(\mu_n)=\infty$, or $\lim f(\mu_n)=\infty$ (not exclusively). If $\lim e(\mu_n)=\infty$, then the group of values of μ_∞ has accumulation points and the valuation is not discrete. If $\lim e(\mu_n)<\infty$, there exists an index n_0 such that $e_n=1$ for all $n>n_0$, or equivalently, $\Gamma(\mu_n)=\Gamma(\mu_{n_0})$ for all $n\ge n_0$; thus, $\Gamma(\mu_\infty)=\Gamma(\mu_{n_0})$ and the valuation μ_∞ is discrete.

In the discrete case, we must have $\lim f(\mu_n)=\infty$, so that the inductive limit $\mathbb{F}_\infty=\bigcup_n\mathbb{F}_n$ is an infinite algebraic extension of $\mathbb{F}$. It is easy to check that

$$\mathrm{KP}(\mu_\infty)=\emptyset,\qquad \kappa(\mu_\infty)\simeq\Delta(\mu_\infty)=\mathbb{F}_\infty,\qquad \mathcal{G}r(\mu_\infty)\simeq\mathbb{F}_\infty[p,p^{-1}],$$

where p is an indeterminate.

Since the tree isomorphism $(\mathbb{V}^{\mathrm{ind}}(K),\prec)\simeq(\mathbb{V}^{\mathrm{ind}}(K_v),\prec)$ preserves the MacLane invariants e_i,f_i,m_i attached to each node, it induces a 1-1 correspondence between the valuations with infinite depth on $K(x)$ and the valuations with infinite depth on $K_v(x)$.

7.2. Limit valuations with finite depth.

An *infinite MacLane chain* is an infinite sequence of augmented valuations:

$$\mu_0\ \xrightarrow{(\phi_1,\nu_1)}\ \cdots\ \longrightarrow\ \mu_{n-1}\ \xrightarrow{(\phi_n,\nu_n)}\ \mu_n\ \xrightarrow{(\phi_{n+1},\nu_{n+1})}\ \cdots$$

such that $\phi_{n+1}\nmid_{\mu_n}\phi_n$ for all n. By Lemmas 2.10 and 3.2, $m_n\mid m_{n+1}$ and $\Gamma(\mu_n)\subset\Gamma(\mu_{n+1})$ for all n.

If the degrees m_n of the key polynomials ϕ_n are not bounded, there exists a limit valuation of this sequence, which is one of the valuations with infinite depth already described in the previous section.

If the degrees m_n are bounded, there exists an index t such that $m_n = m_t$ for all $n \ge t$. Hence, $e_n = 1 = f_n$ for all $n \ge t$, and this implies

$$\Gamma(\mu_n) = \Gamma(\mu_{t-1}), \qquad \mathbb{F}_n = \mathbb{F}_t, \quad \text{for all } n \ge t.$$

Theorem 7.2. [10, Thm 7.1] *Every infinite MacLane chain with stable degrees determines a limit pseudo-valuation on $K[x]$, given by $g \mapsto \lim_n \mu_n(g)$. This pseudo-valuation is equal to $\mu_{\infty,F}$ for some prime polynomial $F \in \mathbb{P}$. Let $\theta \in \overline{K}_v$ be a root of F. If θ is algebraic over K, then $\mu_{\infty,F}$ is infinite on the ideal of $K[x]$ generated by the minimal polynomial of θ over K. If θ is transcendental over K, then $\mu_{\infty,F}$ determines a valuation on $K(x)$ with:*

$$e(F) = e(\mu_{\infty,F}) = e(\mu_{t-1}), \quad \mathbb{F}_F = \kappa(\mu_{\infty,F}) \simeq \Delta(\mu_{\infty,F}) = \mathbb{F}_t,$$

where $m_n = m_t$ for all $n \ge t$. Also, $\mathrm{KP}(\mu_{\infty,F}) = \emptyset$ *and $\mathcal{G}r(\mu_{\infty,F}) \simeq \mathbb{F}_F[p, p^{-1}]$, where p is an indeterminate.* □

Let us see that μ_F is a threshold valuation in the process of approximating $\mu_{\infty,F}$ by inductive valuations.

Proposition 7.3. *Consider an infinite MacLane chain with limit $\mu_{\infty,F}$ and let t be the first index such that* $\deg \phi_n = \deg \phi_t$ *for all $n \ge t$. Then, $\mu_{t-1} = \mu_F$.* □

Proof. Clearly, $\deg F = e(F)f(F) = e(\phi_t)f(\phi_t) = \deg \phi_t$. By Lemma 1.11, F is a key polynomial for μ_{t-1}. Since $\deg \phi_{t-1} < \deg F$, F is a strong key polynomial for μ_{t-1}. Corollary 6.11 shows that $\mu_{t-1} = \mu_F$. □

By Lemma 3.4, all valuations μ_n with $n \ge t$ have the same depth, and by Theorem 6.7, this depth coincides with the Okutsu depth of F. Thus, it makes sense to say that these pseudo-valuations are limits with *finite depth.*

Theorem 7.4. [10, Thm. 8.1] *The set $\mathbb{V}$ is the union of $\mathbb{V}^{\mathrm{ind}}$, the limit valuations given by the discrete leaves of $(\mathbb{V}^{\mathrm{ind}}, \prec)$, and the valuations $\mu_{\infty,F}$ determined by all prime polynomials in $\mathbb{P}$ which do not divide any polynomial in $\mathcal{O}[x]$.* □

Note that limit valuations $\mu_{\infty,F} \in \mathbb{V}$ of finite depth do not occur if $K = K_v$. A posteriori, it is easy to distinguish the inductive valuations among all valuations.

Corollary 7.5. *For any $\mu \in \mathbb{V}$, the following conditions are equivalent:*

(1) *μ is an inductive valuation.*
(2) *μ is residually transcendental; that is, $\kappa(\mu)/\kappa(v)$ is a transcendental extension.*
(3) $\mathrm{KP}(\mu) \ne \emptyset$.
(4) *$\mu(g)/\deg g$ is bounded on all monic non-constant polynomials $g \in K[x]$.*
(5) *there exists a pseudo-valuation μ' on $K[x]$ such that $\mu < \mu'$.* □

7.3. **Intervals of valuations.** For $\mu, \mu' \in \mathbb{V}$, the interval $[\mu, \mu']$ is defined as:

$$[\mu, \mu'] = \{\eta \in \mathbb{V} \mid \mu \le \eta \le \mu'\}.$$

Theorem 7.6. *For any pseudo-valuation μ on $K[x]$, the interval $[\mu_0, \mu) \subset \mathbb{V}^{\mathrm{ind}}$ is totally ordered.*

Proof. Consider two valuations $\eta, \eta' < \mu$. Take a monic $\phi \in K[x]$ of minimal degree satisfying $\eta(\phi) < \mu(\phi)$; by Lemma 1.11, $\phi \in \mathrm{KP}(\eta)$ and for any non-zero $g \in K[x]$ the equality $\eta(g) = \mu(g)$ is equivalent to $\phi \nmid_\eta g$. Let $\phi' \in K[x]$ be a monic polynomial with analogous properties with respect to η'. Suppose $\deg \phi \le \deg \phi'$.

By the minimality of $\deg \phi$ and $\deg \phi'$, for all $a \in K[x]$ with $\deg a < \deg \phi$, we have $\eta(a) = \mu(a) = \eta'(a)$. If $\deg \phi < \deg \phi'$, then $\eta'(\phi) = \mu(\phi) > \eta(\phi)$. Hence, $\eta' \ge \eta$, because for any non-zero $g \in K[x]$ with ϕ-expansion $g = \sum_{0 \le s} a_s \phi^s$, we have:

$$\eta'(g) \ge \min_{0 \le s}\{\eta'(a_s \phi^s)\} \ge \min_{0 \le s}\{\eta(a_s \phi^s)\} = \eta(g). \tag{28}$$

If $\deg\phi = \deg\phi'$, then $\phi' = \phi + a$ for some $a \in K[x]$ with $\deg a < \deg\phi$. Suppose $\eta(\phi) \le \eta'(\phi')$. Then, by the η-minimality of ϕ and the η'-minimality of ϕ', we have

$$\eta(\phi') = \min\{\eta(\phi), \eta(a)\} \le \eta'(\phi) = \min\{\eta'(\phi'), \eta(a)\} \le \eta'(\phi') < \mu(\phi').$$

Hence, $\phi \mid_\eta \phi'$. By Lemma 1.4, $\phi \sim_\eta \phi'$, so that $\eta(\phi) = \eta(\phi') \le \eta'(\phi)$. Therefore, (28) holds and $\eta' \ge \eta$. $\square$

Our aim is to find an explicit description of the valuations in such a totally ordered interval. Let us start with the interval determined by an augmented valuation.

For any key polynomial ϕ for μ, the pseudo-valuation $\mu_{\infty,\phi}$ can be regarded as $\mu_{\infty,\phi} = [\mu; (\phi, \infty)]$ (cf. section 1.3). Also, it makes sense to regard μ as a trivial augmentation of itself, namely $\mu = [\mu; (\phi, 0)]$.

Lemma 7.7. *Let ϕ be a key polynomial for an inductive valuation μ, and consider the augmented valuation $\mu' = [\mu; (\phi, \nu)]$ for some $\nu \in \mathbb{Q}_{>0} \cup \{\infty\}$. Then,*

$$[\mu, \mu') = \{[\mu; (\phi, \rho)] \mid \rho \in \mathbb{Q},\ 0 \le \rho < \nu\}.$$

Proof. For every $\rho \in \mathbb{Q} \cap [0, \nu]$, denote $\mu_\rho := [\mu; (\phi, \rho)]$. Consider a valuation $\eta \in \mathbb{V}$ such that $\mu \le \eta < \mu'$. For all $a \in K[x]$ with $\deg a < \deg\phi$, we have $\mu(a) \le \eta(a) \le \mu'(a) = \mu(a)$, leading to $\eta(a) = \mu'(a) = \mu(a)$. Take $\rho = \eta(\phi) - \mu(\phi) \in \mathbb{Q} \cap [0, \nu]$. For any $g \in K[x]$, with ϕ-expansion $g = \sum_{0\le s} a_s\phi^s$, we have

$$\eta(g) \ge \min_{0\le s}\{\eta(a_s\phi^s)\} = \min_{0\le s}\{\mu(a_s\phi^s) + s\rho\} = \mu_\rho(g), \tag{29}$$

so that $\mu_\rho \le \eta$. If $\rho = \nu$, then $\mu' = \mu_\rho \le \eta$, against our assumption. Thus, $\rho < \nu$, or equivalently $\eta(\phi) < \mu'(\phi)$. By Lemma 1.11, ϕ is a key polynomial for η, so that the inequality in (29) is an equality. $\square$

Let $F \in \mathbb{P}$ be a prime polynomial with respect to v. By Theorem 6.9, F is a key polynomial for the inductive valuation $\mu_F \in \mathbb{V}^{\mathrm{ind}}(K_v)$. Consider an optimal MacLane chain of its restriction $\mu_F \in \mathbb{V}^{\mathrm{ind}}(K)$:

$$\mu_0 \ \xrightarrow{(\phi_1,\nu_1)}\ \mu_1 \ \xrightarrow{(\phi_2,\nu_2)}\ \cdots \ \longrightarrow\ \mu_{r-1} \ \xrightarrow{(\phi_r,\nu_r)}\ \mu_r = \mu_F.$$

By Theorem 7.6,

$$[\mu_0, \mu_{\infty,F}) = [\mu_0, \mu_1) \cup [\mu_1, \mu_2) \cup \cdots \cup [\mu_{r-1}, \mu_F) \cup [\mu_F, \mu_{\infty,F}),$$

and Lemma 7.7 gives an explicit description of each of these subintervals. If we consider valuations on $K_v(x)$, then:

$$[\mu_F, \mu_{\infty,F}) = \{[\mu_F; (F, \nu)] \mid \nu \in \mathbb{Q}_{\ge 0}\} \subset \mathbb{V}^{\mathrm{ind}}(K_v).$$

By Proposition 3.8, the interval $[\mu_F, \mu_{\infty,F}) \subset \mathbb{V}^{\mathrm{ind}}(K)$ consists of the restrictions of these valuations to $K(x)$. By Lemma 3.5, the restriction of $[\mu_F; (F, \nu)]$ to $K(x)$ is equal to $[\mu_F; (\phi, \nu)]$ for any $\phi \in K[x]$ such that $\deg\phi = \deg F$ and $\mu_F(F - \phi) \ge \mu_F(F) + \nu$.

References

[1] V. Alexandru, N. Popescu, A. Zaharescu, *All valuations on $K(x)$*, Journal of Mathematics of Kyoto University **30** (1990), 281–296.

[2] J.-D. Bauch, *Genus computation of global function fields*, arXiv: 1209.0309v3 [math.NT]

[3] J. Guàrdia, J. Montes, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arithmetica **145** (2010), 83–108.

[4] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux **23** (2011), no. 3, 667–696.

[5] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Transactions of the American Mathematical Society **364** (2012), no. 1, 361–416.

[6] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Foundations of Computational Mathematics **13** (2013), 729–762.
[7] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, arXiv: 0902.3428v2 [math.NT].
[8] J. Guàrdia, E. Nart, *Genetics of polynomials over local fields*, arXiv:1309.4340 [math.NT].
[9] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lifting and factorization of polynomials over local fields*, Journal of Symbolic Computation **47** (2012), 1318–1346.
[10] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society, **40** (1936), pp. 363–395.
[11] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2** (1936), pp. 492–510.
[12] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.
[13] E. Nart, *Local computation of differents and discriminants*, arXiv: 1205.1340v1 [math.NT], to appear in Mathematics of Computation.
[14] K. Okutsu, *Construction of integral basis, I, II*, Proceedings of the Japan Academy, Ser. A **58** (1982), 47–49, 87–89.
[15] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica **44** (1923), pp. 219–314.
[16] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen **99** (1928), pp. 84–117.
[17] L. Popescu, N. Popescu, *On the residual transcendental extensions of a valuation. Key polynomials and augmented valuation*, Tsukuba Journal of Mathematics **15** (1991), 57–78.
[18] N. Popescu, A. Zaharescu, *On the structure of the irreducible polynomials over local fields*, Journal of Number Theory **52** (1995), 98–118.
[19] N. Popescu, C. Vraciu, *On the extension of valuations on a field K to $K(x)$, I, II*, Rendiconti del Seminario Matematico della Università di Padova **87** (1992), 151–168, **96** (1996), 1–14.
[20] M. Vaquié, *Extension d'une valuation*, Transactions of the American Mathematical Society **359** (2007), no. 7, 3439–3481.
[21] M. Vaquié, *Extensions de valuation et polygone de Newton*, Annales de l'Institute Fourier (Grenoble) **58** (2008), no. 7, 2503–2541.

Departament de Matemàtica Aplicada IV, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú, Catalonia, Spain

E-mail address: julio@ma4.upc.edu, guardia@ma4.upc.edu

Departament de Ciències Econòmiques i Empresarials, Facultat de Ciències Socials, Universitat Abat Oliba CEU, Bellesguard 30, E-08022 Barcelona, Catalonia, Spain, Departament de Matemàtica Econòmica, Financera i Actuarial, Facultat d'Economia i Empresa, Universitat de Barcelona, Av. Diagonal 690, E-08034 Barcelona, Catalonia, Spain

E-mail address: montes3@uao.es, jesus.montes@ub.edu

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia, Spain

E-mail address: nart@mat.uab.cat