Inductive valuations and defectless polynomials over henselian elds

Nathália Moraes de Oliveira

Universitat Autònoma
de Barcelona

DEPARTAMENT DE MATEMÀTIQUES

Doctorat en Matemàtiques

Curs Acadèmic 2018–2019

TESI DOCTORAL

Inductive valuations and defectless polynomials over henselian fields

Director de la Tesi:
Prof. Enric Nart Viñals

Candidata:
Nathália Moraes de Oliveira

Inductive valuations and defectless polynomials over henselian fields

Thesis submitted by **Nathália Moraes de Oliveira** for the degree of Philosophiae Doctor by the Universitat Autònoma de Barcelona, under the supervision of Prof. Dr. Enric Nart Viñals, in the Department of Mathematics.

Barcelona, November 2018

Autor

Nathália Moraes de Oliveira

Supervisor

Prof. Dr. Enric Nart Viñals

ABSTRACT

Let (K, v) be a discrete rank-one valued field. In a pioneering work, S. MacLane studied and characterized the extensions of the valuation v to the rational function field $K(x)$. M. Vaquié generalized his work for an arbitrary valued field (K, v), not necessarily rank-one nor discrete. A more constructive contribution for the theory was given in the case where v is discrete of rank-one, where J. Fernández, J. Guàrdia, J. Montes and E. Nart provided a computation of generators of the graded algebras and introduced some residual polynomial operators. In this memoir we extend these results to a valued field (K, v), not necessarily rank-one nor discrete. We also establish a connection between inductive valuations and irreducible polynomials with coefficients in K^h, precisely, we construct a bijective mapping $\mathbb{M} \longrightarrow \mathbb{P}_0/\approx$ between the MacLane space of (K, v) (considered as the set of *strong* types) and a certain quotient of the subset $\mathbb{P}_0 \subset \mathbb{P}$ of defectless polynomials with coefficients in the henselian field K. Finally, as an application of the techniques presented in this work we reobtain some results on the computation of invariants of tame algebraic elements over henselian fields.

I dedicate this work to my grandmothers Enilda (in memoriam) and Lasara.

Acknowledgements

First, I must thank my supervisor Enric Nart. I would like to say thank you in the first place for accepting me as a Ph.D. student and also for guiding me during these four years. I wouldn't be here without his support, patience and assistance.

I also would like to acknowledge Programa Ciência sem Fronteiras from CNPq/Brasil for financially supporting my doctoral studies.

I am thankful to all the members of the Department of Mathematics for their help and kindness during the four years of my studies.

I would like to express my special thanks and gratitude to all teachers that contribute to my mathematical development and for their wise advices. Especially, Célio Ignácio, Cleida de Assis Coutinho, Cícero Fernandes de Carvalho, Victor Gonzalo Lopez Neumann and Geraldo Márcio de Azevedo Botelho.

Also, I am grateful to the friends that I made during this fours years, especially, Bruna, Gustavo, Azin, Petr, Josué, and Lea.

I would like to thank my family, that despite the distance they always have been present during my whole life. They supported me and help me through all the difficulties of my life. Especially, I would like to thank my father Anilton, who always have a word to encourage me; my mother Nara, for always be with me; my sister Jainny, for be my best friend, and finally my grandmother Lasara for her assistance in all my life and no less important all grandmother's pampering.

I have left the most important person to last. To Murilo, who encourage me to do a Ph.D. here. He has been my partner, my friend, my support and without his love and support in all aspects of my life, I would not have made it here. I dont have enough words to say how important you are to me.

Contents

List of Figures

Introduction

Let (K, v) be a discrete rank-one valued field. In a pioneering work, S. MacLane studied and characterized the extensions of the valuation v to the rational function field $K(x)$ [17, 18].

For simplicity, let us focus our attention on those extensions μ of v for which $\mu(x) \geq 0$. Then, starting from Gauss' valuation μ_0 (which is the minimal extension of v to $K(x)$ satisfying $\mu(x) = 0$), and choosing certain *key polynomials* $\phi_i \in K[x]$ and positive rational numbers γ_i, MacLane constructed certain *inductive valuations* on $K(x)$,

$$\mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu, \tag{1}$$

where, for $1 \leq i \leq r$, each valuation μ_i is an *augmentation* of the valuation μ_{i-1}, determined by the condition $\gamma_i = \mu_i(\phi_i)$.

MacLane proved that all extensions of v to $K(x)$ can be obtained as a certain *limit* of inductive valuations [17]. Also, he showed that these ideas lead to a concrete algorithm to find all extensions of v to a finite extension of the base field K [18].

In [30, 31, 32], M. Vaquié generalized MacLane's theory to the case of an arbitrary valued field (K, v), not necessarily rank-one nor discrete. The graded algebra $\mathcal{G}_\mu$ attached to a valuation μ, and certain residual ideals in the degree-zero subring Δ_μ of $\mathcal{G}_\mu$ are crucial in the development of the theory.

The residual ideal of a non-zero polynomial $g \in K[x]$ is defined as

$$\mathcal{R}_\mu(g) = H_\mu(g)\mathcal{G}_\mu \cap \Delta_\mu,$$

where $H_\mu(g)$ is the image of g in the piece of degree $\mu(g)$ of the algebra.

J. Fernández, J. Guàrdia, J. Montes and E. Nart gave a constructive touch to Vaquié's approach [6]. Restricted to the case v discrete of rank-one, they provided a computation of generators of the graded algebras. Also, for an inductive valuation as in (1), they introduced some *residual polynomial operators*,

$$R_i \colon K[x] \longrightarrow k_i[y], \qquad 1 \leq i \leq r, \tag{2}$$

where y is an indeterminate, and $k_i \subset \Delta_{\mu_i}$ is a field which is a finite extension of the residue class field k of the initial valuation v. The structure of Δ_{μ_i} as a k-algebra is completely determined by the subfield k_i, since there are elements $y_i \in \Delta_{\mu_i}$ which are transcendental over k_i and satisfy $\Delta_{\mu_i} = k_i[y_i]$.

The operator R_r is a kind of algorithmic representation of the residual ideal operator $\mathcal{R}_\mu$. More precisely, for any polynomial $g \in K[x]$, the element

$$R_r(g)(y_r) \in \Delta_\mu$$

is, up to a power of y_r, a generator of the residual ideal $\mathcal{R}_\mu(g)$.

Let K_v be the completion of K with respect to the v-adic topology. This constructive approach leads to a fast algorithm for polynomial factorization in $K_v[x]$, inspired in a similar algorithm developed by J. Montes for p-adic fields [20]. This algorithm is a kind of efficient version of the original algorithm by MacLane in [18].

These polynomial factorization algorithms based on inductive valuations have many applications to the resolution of arithmetic tasks in number fields and function fields [8, 9, 10].

On the other hand, in [6] the authors found a tight link between the set of inductive valuations and the set $\mathbb{P}$ of monic and irreducible polynomials with coefficients in K_v. More precisely, they established a canonical bijection

$$\mathbb{M} \longrightarrow \mathbb{P}/\!\approx \tag{3}$$

between the *MacLane space* $\mathbb{M}$ and the quotient set of $\mathbb{P}$ under a certain equivalence relation $\approx$. The MacLane space is defined as the set of pairs $(\mu, \mathcal{L})$, where μ is an inductive valuation on $K(x)$ extending v, and $\mathcal{L}$ is a *strong* maximal ideal of Δ_μ.

In this memoir, we extend the results of [6] to an arbitrary valued field (K, v), not necessarily rank-one nor discrete.

In this general situation, the completion K_v looses the nice properties it had in the classical rank-one, discrete case. Its role is undertaken by any *henselization* (K^h, v^h) of the original valued field.

Also, the experts will not be surprised by the fact that inductive valuations may provide a bijection like (3) only for the subset $\mathbb{P}_0 \subset \mathbb{P}$ of *defectless* polynomials with coefficients in K^h.

A monic irreducible polynomial in $K^h[x]$ is defectless if by adjoining a root of it to K^h we get a valued field (K', v') such that

$$[K'\colon K] = e(v'/v^h)f(v'/v^h).$$

The memoir is distributed into three parts.

Part I: Background on valuations

This part, of a preliminary nature, contains two chapters.

In **Chapter 1**, we include basic facts about valued fields and semivaluations on the polynomial ring $K[x]$ in one indeterminate.

The graded algebra of a valuation on $K[x]$ is described, and the basic properties of key polynomials are reviewed, mainly taken from [23].

In **Chapter 2**, we review MacLane's construction of *augmented valuations* [17, 30]. If a given valuation μ on $K[x]$ admits key polynomials, it is possible to *augment* μ to a larger valuation with a prefixed value on a given key polynomial.

Most of the content of this chapter is extracted from Vaquié's paper [30]. Some results not contained in [30] are an easy transcription to the general case of results that were obtained in [6] for rank-one discrete valuations.

Finally, some basic results which we could not find in the literature are probably well known.

In any case, we provide proofs of all results in order to help the reader to get some familiarity with the main features of this construction.

Part II: Inductive valuations on polynomial rings

This part contains five chapters.

In **Chapter 3**, we review some basic facts about the Newton polygon operator attached to a pair μ, ϕ, where μ is a commensurable extension of v to $K[x]$ and ϕ is an arbitrary key polynomial for μ.

Tipically, when μ is a rank-one valuation, the Newton polygon of a polynomial in $K[x]$ lies in the euclidean plane. For higher rank valuations, Newton polygons of polynomials lie in the rational vector space $\mathbb{Q} \times \mathbb{Q}\Gamma$, where Γ is the value group of v.

Apart from this change of ambient space, all results of this chapter are an easy transcription of the results of [6, Sec.2], up to a different normalization of the Newton polygons.

Chapter 4 is devoted to *valuations of depth zero*, which are in a certain sense "very small" commensurable extensions of v to $K[x]$.

These valuations are constructed as an augmentation of an incommensurable valuation $\mu_{-\infty}$, which is a kind of absolute minimal extension of v to $K[x]$.

We analyze the structure of the graded algebra of the valuation $\mu_{-\infty}$ and describe its set of key polynomials.

Also, we determine the structure of the graded algebra of the depth-zero valuations. Their set of key polynomials is described in Chapter 6, where this is done for all valuations μ of *finite depth*.

In **Chapter 5**, we discuss inductive (finite depth) valuations and their MacLane chains as in (1). Optimal MacLane chains are analyzed and a certain unicity property is proved for them.

A MacLane chain of an inductive valuation μ supports many discrete data and operators which are described in this chapter.

As mentioned above, inductive valuations are useful to detect information about the irreducible factors over $K^h[x]$ of any given polynomial $f \in K[x]$.

Since we are interested in the design of algorithms which capture this information, we need algorithms able to compute all data and operators supported by a MacLane chain. To this end, we are led to fix an auxiliary finitely generated group $\Gamma^{\rm fg}$ of the value group Γ.

Finally, certain rational functions in $K(x)$ are construced, leading to special elements with prescribed degree in the graded algebra $\mathcal{G}_\mu$, which play an important role in the description of the structure of $\mathcal{G}_\mu$ as a $\mathcal{G}_v$-algebra, where $\mathcal{G}_v$ is the graded algebra of the initial valuation v.

Chapter 6 is devoted to the construction of *residual polynomial operators* as in (2), which play a key role in the whole theory.

There is a general residual polynomial operator R_μ introduced in [23] (cf. section 1.7 of this memoir). Its construction depends on the choice of rational functions in $K(x)$ with a prescribed μ-value.

From an algorithmic perspective, we need to choose these rational functions in a coherent way for the different levels of the MacLane chains, thus allowing a recursive (hence constructive) computation of the residual polynomial operators.

To this end, the results of Chapter 5 depending on the choice of an auxiliary finitely generated group $\Gamma^{\rm fg}$ of the value group Γ are crucial.

The chapter concludes with an analysis of the dependence of the residual polynomial operators on the choice of the finitely generated subgroup $\Gamma^{\rm fg}$ and the choice of an optimal MacLane chain for μ.

Chapter 7 contains a description of $\mathcal{G}_\mu$ as a $\mathcal{G}_v$-algebra. A complete description of $\mathcal{G}_\mu$ as a k-algebra is obtained only when the value group Γ of the initial valuation v is finitely generated.

Part III: Defectles polynomials over henselian fields

This part contains four chapters.

In **Chapter 8**, we review the basic properties of the henselization of a valued field. We show that an inductive valuation μ on $K[x]$ admits a unique extension to $K^h[x]$. This extension is still inductive, because every optimal MacLane chain of μ lifts in a natural way to a MacLane chain of the extension.

As a consequence of this result, all key polynomials of inductive valuations are defectless polynomials in $K^h[x]$.

The chapter ends with an example of a non-inductive valuation, admitting key polynomials which are not irreducible in $K^h[x]$.

Probably, all results of this chapter are well-known to the experts in the field.

In **Chapter 9**, inspired in [6] and [22], we formulate the concept of *proper* key polynomials and we introduce *types*.

A type is a pair $\mathbf{t} = (\mu, \mathcal{L})$ where μ is an inductive valuation on $K[x]$ and $\mathcal{L}$ is a *proper* maximal ideal of the subring Δ_μ of $\mathcal{G}_\mu$. In this context, $\mathcal{L}$ proper ideal means that $\mathcal{L} = \mathcal{R}_\mu(\phi)$ for some proper key polynomial ϕ for μ.

A proper key polynomial ϕ satisfying $\mathcal{L} = \mathcal{R}_\mu(\phi)$ is called a *representative* of the type $\mathbf{t}$. The main result of the chaper shows that two types coincide if and only if they have the same sets of representatives.

In **Chapter 10**, we assume that (K, v) is a henselian field, and we still denote by v the unique extension of v to a fixed algebraic closure $\overline{K}$.

As a general aim, we would like to study how far can we approximate a given prime polynomial $F \in K[x]$, by key polynomials of valuations on $K[x]$.

This problem distinguishes two phases. In section 10.1, we show that for any key polynomial ϕ of an inductive valuation μ on $K[x]$, the condition

$$\phi \mid_\mu F, \tag{4}$$

(meaning that $H_\mu(\phi)$ divides $H_\mu(F)$ in the graded algebra), implies that $\mathcal{R}_\mu(F)$ is a power of the maximal ideal $\mathcal{R}_\mu(\phi)$ in Δ_μ.

This fact leads to a vast generalization of Hensel's lemma (Theorem 10.7).

In this way, by constructing (via the augmentation process) larger valuations admitting key polynomials for which (4) holds, we discover several invariants of F, related to the discrete data supported by any optimal MacLane chain of μ.

Simultaneously, the key polynomials satisfying (4) are better approximations to F, in the sense that the resultant $\mathrm{Res}(F, \phi)$ has a larger v-value.

In a second phase, developed in section 10.4, we must determine under what conditions this approximation process is able to reach a valuation μ admitting F as a key polynomial.

Both phases are inspired in a pioneer work by Okutsu [24], who showed how to control the quality of the approximations when K is the completion of a rank-one discrete valuation v. In this classical case, this process converges for any prime polynomial, and all involved valuations are inductive.

The connection of Okutsu's approach with inductive valuations was found in [7]. Finally, still restricted to rank-one discrete valuations, the main result of Okutsu was reinterpreted in [6] as the existence of the canonical bijection (3).

For both phases, we follow closely the approach of [6]. The generalization of these ideas to the case of a general valuation v is easy, but it has a crucial limitation. The second phase is only possible for *defectless* polynomials.

The main result of the memoir is the construction of a bijective mapping

$$\mathbb{M} \longrightarrow \mathbb{P}_0/\approx$$

between the MacLane space of (K, v) (considered as the set of *strong* types) and a certain quotient of the subset $\mathbb{P}_0 \subset \mathbb{P}$ of defectles polynomials with coefficients in the henselian field K.

The extension of these ideas to arbitrary prime polynomials would require the use of *continuous MacLane chains* and their *limit augmentations* considered by Vaquié in [30]. We hope to be able to deal with the general case in a future work.

Finally, in **Chapter 11**, we apply the techniques of Chapter 10 to reobtain some results on the computation of invariants of tame algebraic elements over henselian fields.

These results may be found in the literature as the combined contribution of several papers of different authors [1, 2, 3, 4, 15, 16, 29].

Our aim is to give a unified presentation of these computations, with simplified proofs, derived in a natural way from the results of Chapter 10.

PART I

Background on valuations

Chapter 1

Valuations on polynomial rings

Throughout this memoir we fix a valuation on a field K,

$$v\colon K \longrightarrow \Gamma \cup \{\infty\}.$$

We suppose that $\Gamma = \Gamma_v$ is its value group, and we denote by

$$\mathcal{O} = \mathcal{O}_v, \qquad \mathfrak{m} = \mathfrak{m}_v, \qquad k = k_v$$

its valuation ring, maximal ideal and residue class field, respectively.

For any $a \in \mathcal{O}$, we denote by $\overline{a} \in k$ its class modulo $\mathfrak{m}$. Given a polynomial $g \in \mathcal{O}[x]$, we denote by $\overline{g} \in k[x]$ the polynomial which is obtained by taking classes modulo $\mathfrak{m}$ of all coefficients of g.

The aim of this memoir is to study *inductive* valuations over (K, v), and use them to parameterize defectless polynomials over henselian fields.

These valuations are certain commensurable extensions of the valuation v to the field $K(x)$ of rational functions in one indeterminate.

In this preliminary chapter, we recall some background on valued fields and rings.

1.1 Ordered abelian groups

An *ordered abelian group* is an abelian group $(\Gamma, +)$ equipped with a total order $\leq$, which is compatible with the group structure:

$$\alpha \leq \beta \quad \Longrightarrow \quad \alpha + \gamma \leq \beta + \gamma, \qquad \forall\, \alpha,\, \beta,\, \gamma \in \Gamma.$$

A subgroup $\Lambda \subset \Gamma$ is *convex* if

$$\alpha, \beta \in \Lambda \quad \Longrightarrow \quad [\alpha, \beta] \subset \Lambda.$$

The following properties of convex subgroups of ordered abelian groups are well known.

- The quotient Γ/Λ inherits a natural structure of ordered abelian group.

- The kernel of an order-preserving group homomorphism between two ordered abelian groups is a convex subgroup.
- The convex subgroups of Γ are totally ordered by inclusion.

Definition 1.1. *The* rank *of* Γ *is the cardinality of the set of proper convex subgroups of* Γ. *It is denoted as* $\mathrm{rk}(\Gamma)$.

For instance, let $\mathbb{R}^n_{\mathrm{lex}}$ be the additive group $(\mathbb{R}^n, +)$ equipped with the lexicographical order. This ordered abelian group has rank n, and any ordered abelian group of finite rank n can be embedded into $\mathbb{R}^n_{\mathrm{lex}}$ via an order-preserving homomorphism.

Definition 1.2. *We say that* $\mathbb{Q}\Gamma := \Gamma \otimes \mathbb{Q}$ *is the* divisible hull *of* Γ.
The dimension of $\mathbb{Q}\Gamma$ *as a* $\mathbb{Q}$*-vector space is called the* rational rank *of* Γ.
It is denoted as $\mathrm{rr}(\Gamma) = \dim_{\mathbb{Q}} \mathbb{Q}\Gamma$.

Thus, the rational rank of Γ is the cardinality of a maximal linearly independent subset of Γ, as a $\mathbb{Z}$-module.

For any subgroup $\Lambda \subset \Gamma$, we have

$$\mathrm{rk}(\Gamma) \leq \mathrm{rk}(\Lambda) + \mathrm{rr}(\Gamma/\Lambda). \tag{1.1}$$

In particular, $\mathrm{rk}(\Gamma) \leq \mathrm{rr}(\Gamma)$, but equality does not necessarily hold. For instance,

$$\mathrm{rk}(\mathbb{Q}) = 1 = \mathrm{rr}(\mathbb{Q}), \qquad \mathrm{rk}(\mathbb{R}) = 1 < \mathrm{rr}(\mathbb{R}) = \infty.$$

Ordered abelian groups are torsion free. In fact, suppose that $0 \neq \alpha \in \Gamma$ has finite order $n > 0$. By eventually replacing α with $-\alpha$, we may assume that $\alpha > 0$, and this leads to a contradiction:

$$0 < \alpha \quad \Longrightarrow \quad \alpha < 2\alpha < \cdots < n\alpha = 0.$$

Since Γ is torsion free, the natural group homomorphism

$$\Gamma \longrightarrow \mathbb{Q}\Gamma, \qquad \alpha \mapsto \alpha \otimes 1 \tag{1.2}$$

is an embedding. Every element in $\mathbb{Q}\Gamma$ can be written as $\alpha \otimes \frac{1}{e}$ for $\alpha \in \Gamma$ and some positive integer e. This expression is unique up to the following identification:

$$\alpha \otimes \frac{1}{e} = \beta \otimes \frac{1}{d} \quad \Longleftrightarrow \quad d\alpha = e\beta.$$

Notation. In the sequel we shall write α/e instead of $\alpha \otimes \frac{1}{e}$.

We can consider a total order in $\mathbb{Q}\Gamma$:

$$\alpha/e \leq \beta/d \quad \Longleftrightarrow \quad d\alpha \leq e\beta.$$

It is easy to check that $\mathbb{Q}\Gamma$ is an ordered abelian group and the embedding (1.2) preserves the order. Clearly,

$$\mathrm{rk}(\Gamma) = \mathrm{rk}(\mathbb{Q}\Gamma), \qquad \mathrm{rr}(\Gamma) = \mathrm{rr}(\mathbb{Q}\Gamma).$$

1.2 Valued fields

In this section, we collect several basic results on valuations on fields. Most of them have been extracted from [5].

Let K be a field and Γ an ordered abelian group. A mapping

$$v\colon K \longrightarrow \Gamma \cup \{\infty\}$$

is said to be a *valuation* on K if it satisfies the following properties for all $a, b \in K$:

(0) $v(a) = \infty$ if and only if $a = 0$,

(1) $v(ab) = v(a) + v(b)$,

(2) $v(a + b) \geq \mathrm{Min}\,\{v(a), v(b)\}$.

The *group of values* of v is the image of the group homomorphism $K^* \xrightarrow{v} \Gamma$ induced by v. We denote it by

$$\Gamma_v = v(K^*).$$

The subring $\mathcal{O}_v = \{a \in K \mid v(a) \geq 0\}$ is called the *valuation ring* of v.
The following properties of valuation rings are well-know:

- $\mathcal{O}_v$ is a local ring with maximal ideal $\mathfrak{m}_v = \{a \in K \mid v(a) > 0\}$.
  The quotient $k_v = \mathcal{O}_v/\mathfrak{m}_v$ is called the *residue class field* of v.
- For any $a \in K^*$, we have either $a \in \mathcal{O}$, or $1/a \in \mathfrak{m}$.
- $\mathcal{O}_v$ is integrally closed, and its ideals are totally ordered by inclusion.

Definition 1.3. *Two valuations $v_i\colon K \to \Gamma_i \cup \{\infty\}$ $(i = 1, 2)$ are equivalent if they have the same valuation ring: $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.*

This happens if and only if there exists an order-preserving group isomorphism

$$\iota : \Gamma_{v_1} \longrightarrow \Gamma_{v_2}$$

such that $\iota \circ v_1 = v_2$.

Definition 1.4. *Let $v\colon K \to \Gamma \cup \{\infty\}$ be a valuation.*
Let L/K be an extension of fields. A valuation on L,

$$w\colon L \longrightarrow \Gamma' \cup \{\infty\},$$

is said to be an extension *of v if $\mathcal{O}_w \cap K = \mathcal{O}_v$.*

Equivalently, there exists an order-preserving embedding $\Gamma_v \hookrightarrow \Gamma_w$ such that the following diagram commutes.

$$\begin{array}{ccc} L^* & \xrightarrow{w} & \Gamma_w \\ \uparrow & & \uparrow \\ K^* & \xrightarrow{v} & \Gamma_v \end{array}$$

We define the *index of ramification* of an extension w/v of valuations as:

$$e(w/v) = (\Gamma_w \colon \Gamma_v)\,,$$

having in mind that it can be infinite.

Also, an extension w/v of valuations determines an embedding $k_v \hookrightarrow k_w$ between the residue class fields.

We denote the *residual degree* of the extension w/v as

$$f(w/v) = [k_w \colon k_v]\,.$$

This number may be infinite as well.

Definition 1.5. *An extension w/v is said to be* immediate *if $e(w/v) = f(w/v) = 1$.*

Commensurable extensions

Definition 1.6. *An extension w/v of valuations is said to be* commensurable *if Γ_w/Γ_v is a torsion group. This is equivalent to $\mathrm{rr}(\Gamma_w/\Gamma_v) = 0$.*

In particular, (1.1) shows that

$$\mathrm{rk}(\Gamma_v) = \mathrm{rk}(\Gamma_w), \qquad \mathrm{rr}(\Gamma_v) = \mathrm{rr}(\Gamma_w).$$

Suppose v is the trivial valuation on K; that is, $\Gamma_v = \{0\}$. Then, for any field extension L/K, the trivial valuation on L is the only commensurable extension of v.

If the extension w/v is commensurable, there is a natural order-preserving embedding of Γ_w into the divisible hull of Γ_v:

$$i \colon \Gamma_w \hookrightarrow \mathbb{Q}\Gamma_v, \qquad \gamma \longmapsto (e\gamma)/e,$$

where $e \in \mathbb{Z}$, which depends on γ, satisfies $e\gamma \in \Gamma_v$.

The valuation on L given by

$$\widetilde{w} \colon L^* \xrightarrow{w} \Gamma_w \xhookrightarrow{i} \mathbb{Q}\Gamma_v$$

is another extension of v, and it is equivalent to w. In fact, $\widetilde{w} = i \circ w$ by construction; and i is an order-preserving group isomorphism between Γ_w and $\Gamma_{\widetilde{w}} = i\,(\Gamma_w)$.

Lemma 1.7. *Let w_1, w_2 be two commensurable extensions of v to L.*
Let $\widetilde{w}_1$, $\widetilde{w}_2$ be their $\mathbb{Q}\Gamma_v$-valued versions.
Then, w_1, w_2 are equivalent if and only if $\widetilde{w}_1 = \widetilde{w}_2$.

Proof. If $\widetilde{w}_1 = \widetilde{w}_2$, then w_1 and w_2 are equivalent, because each w_i is equivalent to $\widetilde{w}_i$ for $i = 1, 2$.

Conversely, suppose that w_1 and w_2 are equivalent. Let $\iota : \Gamma_{w_1} \to \Gamma_{w_2}$ be an order-preserving group isomorphism such that $\iota \circ w_1 = w_2$. This isomorphism extends in a unique way to an order-preserving automorphism $\tilde{\iota}$ of $\mathbb{Q}\Gamma_v$ such that

$$\tilde{\iota} \circ \widetilde{w}_1 = \widetilde{w}_2.$$

This leads to the following commutative diagram:

$$\begin{array}{ccccc} \Gamma_v & \hookrightarrow & \Gamma_{w_2} & \xhookrightarrow{i_2} & \mathbb{Q}\Gamma_v \\ \| & & \iota\uparrow & & \uparrow\tilde{\iota} \\ \Gamma_v & \hookrightarrow & \Gamma_{w_1} & \xhookrightarrow{i_1} & \mathbb{Q}\Gamma_v \end{array}$$

Since $\tilde{\iota}$ restricted to Γ_v is the identity, it must be the identity on $\mathbb{Q}\Gamma_v$ as well, so that $i_2 \circ \iota = i_1$. Hence, $\widetilde{w}_1 = \widetilde{w}_2$. □

Finally, let us mention another fundamental inequality.

Theorem 1.8. *For an arbitrary extension w/v of valuations, it follows that*

$$\text{tr. deg}(k_w/k_v) + \text{rr}(\Gamma_w/\Gamma_v) \leq \text{tr. deg}(L/K).$$

In particular, if L/K is algebraic, then k_w/k_v is algebraic and w/v is commensurable.

1.3 Graded algebra of a valuation

To any valuation v on K we may associate a graded algebra as follows.

For any $\alpha \in \Gamma_v$, consider the $\mathcal{O}_v$-submodules:

$$\mathcal{P}_\alpha = \{a \in K \mid v(a) \geq \alpha\} \supset \mathcal{P}_\alpha^+ = \{a \in K \mid v(a) > \alpha\},$$

leading to the graded algebra

$$\mathcal{G}_v := \text{gr}_v(K) = \bigoplus\nolimits_{\alpha\in\Gamma_v} \mathcal{P}_\alpha/\mathcal{P}_\alpha^+.$$

The product of homogeneous elements is defined in an obvious way:

$$\left(a + \mathcal{P}_\alpha^+\right)\left(b + \mathcal{P}_\beta^+\right) = ab + \mathcal{P}_{\alpha+\beta}^+.$$

If the class of $a + \mathcal{P}_\alpha^+$ and $b + \mathcal{P}_\beta^+$ are different from zero, then $v(a) = \alpha$, $v(b) = \beta$. Hence, $v(ab) = \alpha + \beta$, so that $ab + \mathcal{P}_{\alpha+\beta}^+$ is different from zero too.

This means that $\mathcal{G}_v$ is an integral domain.

The subring of homogeneous elements of degree zero is k_v, so that $\mathcal{G}_v$ has a natural structure of k_v-algebra.

Definition 1.9. *There is a natural mapping $H_v\colon K \to \mathcal{G}_v$, given by*

$$H_v(0) = 0, \qquad H_v(a) = a + \mathcal{P}_{v(a)}^+, \quad \textit{for } a \neq 0.$$

Two elements $a, b \in K$ are said to be v-equivalent if $H_v(a) = H_v(b)$. In this case, we write $a \sim_v b$.

This is equivalent to $v(a - b) > v(b)$, and it implies $v(a) = v(b)$.

An extension w/v of valuations determines an embedding of graded algebras

$$\mathcal{G}_v \hookrightarrow \mathcal{G}_w := \text{gr}_w(L), \qquad a + \mathcal{P}_\alpha^+(v) \mapsto a + \mathcal{P}_\alpha^+(w), \quad \forall \alpha \in \Gamma_v,\ \forall a \in \mathcal{P}_\alpha(v).$$

Lemma 1.10. *Let w/v be an extension of valuations. The following conditions are equivalent.*

(1) w/v is immediate.

(2) The natural embedding $\mathcal{G}_v \hookrightarrow \mathcal{G}_w$ is an isomorphism.

(3) For every $\xi \in L$, there exists $a \in K$ such that $\xi \sim_w a$.

Proof. Let us see that (1) implies (2). Since $f(w/v) = 1$, the canonical mapping $k_v \to k_w$ is an isomorphism. Thus, the embedding $\mathcal{G}_v \hookrightarrow \mathcal{G}_w$ restricts to an isomorphism between the homogeneous parts of degree zero.

On the other hand, since $e(w/v) = 1$, for every $\alpha \in \Gamma_w$ there exists $a \in K$ with $w(a) = \alpha$. Hence, the mapping $\mathcal{G}_v \to \mathcal{G}_w$ is an isomorphism on the homogeneous parts of degree α too:

$$\mathcal{P}_\alpha(v)/\mathcal{P}^+_\alpha(v) = H_v(a)k_v \quad \xrightarrow{\sim} \quad H_w(a)k_w = \mathcal{P}_\alpha(w)/\mathcal{P}^+_\alpha(w).$$

Conditions (2) and (3) are both equivalent to the fact that the mapping $\mathcal{G}_v \to \mathcal{G}_w$ is onto. Finally, (2) clearly implies (1). □

1.4 Semivaluations on $K[x]$

An extension of v to the field $K(x)$ is completely determined by its action on the polynomial ring $K[x]$. Thus, we may restrict our attention to mappings

$$\mu\colon K[x] \longrightarrow \Gamma' \cup \{\infty\},$$

satisfying conditions (0), (1), (2) of a valuation (cf. section 1.2), and such that

$$\mu_{|K} = \iota \circ v,$$

for some order-preserving embedding $\iota\colon \Gamma \hookrightarrow \Gamma'$.

It is convenient to enlarge a little bit the notion of valuation on a polynomial ring, and deal with *semivaluations*.

The definitions that follow can be extended to arbitrary commutative rings, but we keep dealing with our ring $K[x]$ for the reader's convenience.

Definition 1.11. *Let K be a field and Γ' an ordered abelian group.*

A semivaluation *on $K[x]$ is a mapping*

$$\mu\colon K[x] \longrightarrow \Gamma' \cup \{\infty\}$$

satisfying the following properties for all $f, g \in K[x]$:

(1) $\mu(fg) = \mu(f) + \mu(g)$,

(2) $\mu(f+g) \geq \operatorname{Min}\{\mu(f), \mu(g)\}$.

As usual, such a mapping satisfies

$$\mu(f) < \mu(g) \implies \mu(f+g) = \mu(f).$$

In fact, $\mu(f+g) > \mu(f)$ would lead to a contradiction:

$$\mu(f) \geq \operatorname{Min}\{\mu(-g), \mu(f+g)\} > \mu(f).$$

The *support* of μ is the ideal

$$\mathfrak{p} := \mathfrak{p}_\mu = \mu^{-1}(\infty).$$

Condition (1) shows that $\mathfrak{p}$ is a prime ideal of $K[x]$.

Definition 1.12. *We say that μ is a* valuation *on $K[x]$ if $\mathfrak{p} = 0$.*
Only in this case μ extends to a valuation on the field of fractions $K(x)$.

In any case, μ induces a valuation

$$\overline{\mu}\colon \kappa(\mathfrak{p})^* \longrightarrow \Gamma',$$

on the residue field $\kappa(\mathfrak{p})$, which is isomorphic to the field of fractions of $K[x]/\mathfrak{p}$.

Let us denote the corresponding maximal ideal and valuation ring by

$$\mathfrak{m}_\mu := \mathfrak{m}_{\overline{\mu}} \subset \mathcal{O}_\mu := \mathcal{O}_{\overline{\mu}} \subset \kappa(\mathfrak{p}).$$

The residue class field of μ is defined to be

$$k_\mu = \mathcal{O}_\mu/\mathfrak{m}_\mu = k_{\overline{\mu}}.$$

Also, we denote the group of values by

$$\Gamma_\mu := \Gamma_{\overline{\mu}} = \overline{\mu}\left(\kappa(\mathfrak{p})^*\right),$$

which coincides with the subgroup of Γ' generated by $\mu(K[x] \setminus \mathfrak{p})$.

Conversely, for any $\mathfrak{p} \in \operatorname{Spec}(K[x])$ and any valuation

$$\kappa(\mathfrak{p}) \longrightarrow \Gamma' \cup \{\infty\},$$

we obtain a semivaluation on $K[x]$ with support $\mathfrak{p}$, just by taking the composition

$$K[x] \longrightarrow K[x]/\mathfrak{p} \hookrightarrow \kappa(\mathfrak{p}) \longrightarrow \Gamma' \cup \{\infty\}.$$

Definition 1.13. *Two semivaluations ν, μ on $K[x]$ are said to be* equivalent *if the following equivalent conditions are satisfied.*

(1) There exists a (necessarily unique) order-preserving isomorphism $\iota\colon \Gamma_\nu \xrightarrow{\sim} \Gamma_\mu$ such that $\mu = \iota \circ \nu$.

(2) For all $f, g \in K[x]$, the condition $\mu(f) \geq \mu(g)$ is equivalent to $\nu(f) \geq \nu(g)$.

(3) $\mathfrak{p}_\nu = \mathfrak{p}_\mu$ and $\mathcal{O}_\nu = \mathcal{O}_\mu$.

Let us show that these conditions are equivalent. It is clear that (1) implies (2).

Condition (2) obviously implies $\mathfrak{p}_\nu = \mathfrak{p}_\mu$. Also, $\mathcal{O}_\nu = \mathcal{O}_\mu$ because $f \in \mathcal{O}_\nu$ is equivalent to $\mu(f) \geq \mu(1)$.

Finally, (3) implies that $\overline{\nu}$ and $\overline{\mu}$ are equivalent valuations on the same field. Hence, there exists an order-preserving isomorphism $\iota\colon \Gamma_\nu \xrightarrow{\sim} \Gamma_\mu$ such that $\overline{\mu} = \iota \circ \overline{\nu}$. By composing with the mapping $K[x] \to K[x]/\mathfrak{p}_\nu \hookrightarrow \kappa(\mathfrak{p})$, we get $\mu = \iota \circ \nu$.

Semivaluations on $K[x]$ extending a given valuation on K

We are interested in equivalence classes of semivaluations μ on $K[x]$ extending our given valuation v on K, with group of values Γ.

Equivalently, we are interested in pairs $(\mathfrak{p}, \overline{\mu})$, where $\mathfrak{p} \in \mathrm{Spec}(K[x])$ and $\overline{\mu}$ is a valuation on $\kappa(\mathfrak{p})$ extending v.

We say that the extension μ/v is commensurable if $\overline{\mu}/v$ is commensurable; that is, $\mathrm{rr}(\Gamma_\mu/\Gamma) = 0$. As mentioned in Chapter 0, to any such commensurable extension we may attach a $\mathbb{Q}\Gamma$-valued extension

$$K[x] \longrightarrow \mathbb{Q}\Gamma \cup \{\infty\}.$$

By Lemma 1.7, equivalence of commensurable extensions of v is translated into equality of $\mathbb{Q}\Gamma$-valued extensions of v.

Since we are only interested in commensurable extensions of v, we may focus our attention on the set of semivaluations with values in $\mathbb{Q}\Gamma$,

$$\mathbb{V} := \mathbb{V}(K, v) = \{\mu \colon K[x] \longrightarrow \mathbb{Q}\Gamma \cup \{\infty\} \mid \mu_{|K} = v\}.$$

If v is the trivial valuation on K, then $\mathbb{V}$ consists of the one-element set containing the trivial valuation on $K(x)$. Hence, we may exclude this case from our analysis.

Hypothesis. *From now on, we assume that v is not the trivial valuation.*

Since all our semivaluations take values in the same ordered group, there is a natural partial ordering in the set $\mathbb{V}$:

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

There is a special element in this set, which is called *Gauss' valuation*:

$$\mu_{\mathrm{Gauss}}\left(\sum\nolimits_{0\leq s} a_s x^s\right) = \min_{0\leq s}\left\{v(a_s)\right\}.$$

Clearly, μ_{Gauss} has trivial support, so that it is a valuation indeed.

Gauss' valuation is the least element in the subset of semivaluations satisfying $\mu(x) \geq 0$:

$$\mu \in \mathbb{V}, \quad \mu(x) \geq 0 \implies \mu_{\mathrm{Gauss}} \leq \mu.$$

We may classify the elements in $\mathbb{V}$ according to its support:

$$\mathbb{V} = \bigcup_{\mathfrak{p}\in\mathrm{Spec}(K[x])} \mathbb{V}_\mathfrak{p}, \qquad \mathbb{V}_\mathfrak{p} = \{\mu \in \mathbb{V} \mid \mathfrak{p}_\mu = \mathfrak{p}\}.$$

For $\mathfrak{p} = 0$, note that $\mathbb{V}_0 \subset \mathbb{V}$ is precisely the subset of all valuations in $\mathbb{V}$.

For $\mathfrak{p} \neq 0$, we have $\mathfrak{p} = \phi K[x]$ for some monic irreducible $\phi \in K[x]$. The field

$$L = \kappa(\mathfrak{p}) = K[x]/\mathfrak{p}$$

is a finite extension of K. Thus, $\mathbb{V}_\mathfrak{p}$ may be identified to the set of all equivalence classes of valuations μ on L extending v.

1.5 Graded algebra of a valuation on $K[x]$

Let μ be any valuation on $K[x]$ extending v. Recall that μ extends to a valuation $\bar{\mu}$ on the field $K(x)$.

For any $\alpha \in \Gamma_\mu$, consider the following $\mathcal{O}$-submodules in $K[x]$:

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

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

$$\mathcal{G}_\mu := \mathrm{gr}_\mu(K[x]) = \bigoplus\nolimits_{\alpha\in\Gamma_\mu} \mathcal{P}_\alpha/\mathcal{P}^+_\alpha.$$

Clearly,

$$\mathcal{O} \subset \mathcal{P}_0 = K[x] \cap \mathcal{O}_\mu, \qquad \mathfrak{m} = \mathcal{P}^+_0 \cap \mathcal{O} \subset \mathcal{P}^+_0 = K[x] \cap \mathfrak{m}_\mu.$$

Let $\Delta := \Delta_\mu = \mathcal{P}_0/\mathcal{P}^+_0$ be the subring determined by the piece of degree zero of this algebra. There are canonical injective ring homomorphisms:

$$k \hookrightarrow \Delta \hookrightarrow k_\mu.$$

In particular, Δ and $\mathcal{G}_\mu$ are equipped with a canonical structure of k-algebra.

We have natural embeddings of graded k-algebras

$$\mathcal{G}_v = \mathrm{gr}_v(K) \hookrightarrow \mathcal{G}_\mu = \mathrm{gr}_\mu(K[x]) \hookrightarrow \mathrm{gr}_{\overline{\mu}}(K(x)).$$

none of which is necessarily onto.

The graded algebras $\mathrm{gr}_v(K)$, $\mathrm{gr}_{\overline{\mu}}(K(x))$ are the ordinary graded algebras introduced in section 1.3, attached to the valued fields (K, v), $(K(x), \overline{\mu})$, respectively.

There is a natural map $H_\mu\colon K[x] \to \mathcal{G}_\mu$, given by

$$H_\mu(g) = \begin{cases} g + \mathcal{P}^+_{\mu(g)} \in \mathcal{P}_{\mu(g)}/\mathcal{P}^+_{\mu(g)}, & \text{if } g \neq 0, \\ 0, & \text{if } g = 0. \end{cases}$$

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

$$\begin{aligned} &H_\mu(gh) = H_\mu(g)H_\mu(h), \\ &H_\mu(g+h) = H_\mu(g) + H_\mu(h), \quad \text{if } \mu(g) = \mu(h) = \mu(g+h). \end{aligned} \tag{1.3}$$

For a valuation $\mu' \in \mathbb{V}$ with $\mu \leq \mu'$, there is a canonical homomorphism of graded algebras:

$$\mathcal{G}_\mu \longrightarrow \mathcal{G}_{\mu'}, \qquad g + \mathcal{P}^+_{\mu(g)}(\mu) \longmapsto g + \mathcal{P}^+_{\mu(g)}(\mu').$$

Clearly,

$$H_\mu(g) \mapsto \begin{cases} H_{\mu'}(g), & \text{if } \mu(g) = \mu'(g), \\ 0, & \text{if } \mu(g) < \mu'(g). \end{cases}$$

Definition 1.14. *Let $I(\Delta)$ be the set of ideals in Δ, and consider the* residual ideal operator*:*

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

This operator $\mathcal{R}$ translates questions about the action of μ on $K[x]$ into ideal-theoretic considerations in the ring Δ.

To this end, the next definitions are crucial to translate properties of the action of μ on $K[x]$ into algebraic relationships in the graded algebra $\mathcal{G}_\mu$.

Definition 1.15. *Let $g,\, h \in K[x]$.*

We say that g, h are μ-equivalent*, and we write $g \sim_\mu h$, if $H_\mu(g) = H_\mu(h)$.*

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 $\mathcal{G}_\mu$.*

We say that g is μ-irreducible if $H_\mu(g)\mathcal{G}_\mu$ is a non-zero prime ideal.

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

In other words, for $f, g, h \in K[x] \setminus \mathfrak{p}$:

- $g \sim_\mu h \iff \mu(g-h) > \mu(g)$.
- $h \mid_\mu g \iff g \sim_\mu hf$, for some $f \in K[x]$.
- g is μ-irreducible $\iff$ [$g \mid_\mu fh \implies g \mid_\mu f$ or $g \mid_\mu h$].

The property of g being μ-minimal admits a relevant characterization.

Lemma 1.16. *Let $\phi \in K[x]$ be a non-constant polynomial. Let*

$$f = \sum\nolimits_{0 \le s} a_s \phi^s, \qquad a_s \in K[x],\ \deg(a_s) < \deg(\phi)$$

be the canonical ϕ-expansion of $f \in K[x]$. The following conditions are equivalent:

(1) ϕ is μ-minimal

(2) For any $f \in K[x]$, $\mu(f) = \mathrm{Min}\{\mu(a_0), \mu(f - a_0)\}$.

(3) For any $f \in K[x]$, $\mu(f) = \underset{0 \le s}{\mathrm{Min}}\{\mu(a_s\phi^s)\}$.

(4) For any non-zero $f \in K[x]$, $\phi \nmid_\mu f$ if and only if $\mu(f) = \mu(a_0)$.

Proof. Write $f - a_0 = \phi q$ with $q \in K[x]$. Then, $\mu(f) \ge \mathrm{Min}\{\mu(a_0), \mu(\phi q)\}$.

An strict inequality implies $a_0 \sim_\mu -\phi q$. In particular, ϕ is not μ-minimal, because $\phi \mid_\mu a_0$ with $\deg(a_0) < \deg(\phi)$. Hence, (1) implies (2).

An inductive argument shows that (2) implies (3).

Let us now deduce (4) from (3). For any non-zero $f \in K[x]$ we have $\mu(f) \le \mu(a_0)$, by item (3). If $\mu(f) < \mu(a_0)$, then $f \sim_\mu \phi q$, so $\phi \mid_\mu f$.

Conversely, if $f \sim_\mu \phi g$ for some $g \in K[x]$, then $\mu(f - \phi g) > \mu(f)$. Since the ϕ-expansion of $f - \phi g$ has the same coefficient a_0, we have $\mu(f - \phi g) \le \mu(a_0)$, by condition (3). Hence, $\mu(f) < \mu(a_0)$.

Finally, (4) implies (1). If $\deg(f) < \deg(\phi)$, the ϕ-expansion of f is $f = a_0$. By item (4), $\phi \nmid_\mu f$. □

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

1.6 Key polynomials

We keep dealing with an arbitrary valuation μ on $K[x]$, extending v.

Definition 1.17. *A* key polynomial *for μ is a monic polynomial in $K[x]$ which is simultaneously μ-minimal and μ-irreducible.*

The set of key polynomials for μ will be denoted by $\mathrm{KP}(\mu)$.

Key polynomials for valuations on $K[x]$ were introduced in the seminal paper of S. MacLane [17]. Since then, these objects have been extensively studied, mainly for its connection with the study of the defect of a valuation in a finite extension, and the local uniformization problem [6, 13, 19, 23, 28, 31].

In this section, we collect several basic facts about key polynomials, most of them extracted from [23].

Lemma 1.18. *Let $\chi \in \mathrm{KP}(\mu)$, and let $f \in K[x]$ a monic polynomial such that $\chi \mid_\mu f$ and $\deg(f) = \deg(\chi)$. Then, $\chi \sim_\mu f$ and f is a key polynomial for μ too.*

Let us introduce some notation, to be used throughout the memoir.

Notation. For any positive integer m we denote:

$$K[x]_m = \{a \in K[x] \mid \deg(a) < m\},$$
$$\Gamma_m = \Gamma_{\mu,m} = \{\mu(a) \in \Gamma_\mu \mid a \in K[x]_m,\ a \neq 0\}.$$

Lemma 1.19. *Let $\chi \in \mathrm{KP}(\mu)$. Then,*

1. *The polynomial χ is irreducible in $K[x]$.*
2. *For $a, b \in K[x]_{\deg(\chi)}$, let $ab = c + d\chi$ be its χ-expansion. Then,*

$$\mu(ab) = \mu(c) \leq \mu(d\chi).$$

Proof. Take $a, b \in K[x]_{\deg(\chi)}$. Since χ is μ-minimal, we have $\chi \nmid_\mu a$ and $\chi \nmid_\mu b$. Hence, $\chi \nmid_\mu ab$, because χ is μ-irreducible too. In particular, we can't have $\chi = ab$.

Also, $\mu(ab) = \mu(c) \leq \mu(d\chi)$ follows from Lemma 1.16. This proves (1) and (2). □

Semivaluation attached to a key polynomial

Let $\chi \in \mathrm{KP}(\mu)$. Consider the prime ideal $\mathfrak{p} = \chi\, K[x]$ and the field $K_\chi = K[x]/\mathfrak{p}$.

Lemma 1.20. *The set $\Gamma_{\deg(\chi)}$ is a subgroup of Γ_μ, and $\langle\, \Gamma_{\deg(\chi)}, \mu(\chi)\,\rangle = \Gamma_\mu$.*

By the definition of $\Gamma_{\deg(\chi)}$, we get a well-defined onto mapping:

$$v_\chi \colon K_\chi^* \longrightarrow\!\!\!\!\!\rightarrow \Gamma_{\deg(\chi)}, \qquad v_\chi(f + \mathfrak{p}) = \mu(f_0), \quad \forall f \in K[x] \setminus \mathfrak{p},$$

where $f_0 \in K[x]$ is the common 0-th coefficient of the χ-expansion of all polynomials in the class $f + \mathfrak{p}$.

Proposition 1.21. *The mapping v_χ is a valuation on K_χ extending v, with group of values $\Gamma_{\deg(\chi)}$.*

Moreover, $\mu(f) \leq v_\chi(f)$ for all $f \in K[x]$, and equality holds if and only if $\chi \nmid_\mu f$.

Denote the maximal ideal, the valuation ring and the residue class field of v_χ by:

$$\mathfrak{m}_\chi \subset \mathcal{O}_\chi \subset K_\chi, \qquad k_\chi = \mathcal{O}_\chi/\mathfrak{m}_\chi.$$

Let $\theta \in K_\chi = K[x]/(\chi)$ be the root of χ determined by the class of x.
With this notation, we have $K_\chi = K(\theta)$, and

$$v_\chi(f(\theta)) = \mu(f_0) = v_\chi(f_0(\theta)), \qquad \forall f \in K[x].$$

We abuse of language and denote still by v_χ the corresponding semivaluation

$$K[x] \longrightarrow\!\!\!\!\!\rightarrow K_\chi \xrightarrow{v_\chi} \Gamma_{\deg(\chi)} \cup \{\infty\}$$

with support $\mathfrak{p} = \chi K[x] = v_\chi^{-1}(\infty)$.

Proposition 1.22. *The residual ideal $\mathcal{R}(\chi)$ is the kernel of the onto homomorphism*

$$\Delta \longrightarrow\!\!\!\!\!\rightarrow k_\chi, \qquad g + \mathcal{P}_0^+ \;\mapsto\; g(\theta) + \mathfrak{m}_\chi.$$

In particular, $\mathcal{R}(\chi)$ is a maximal ideal in Δ.

Minimal expression of $H_\mu(f)$ in terms of χ-expansions

Let $\chi \in \mathrm{KP}(\mu)$. For any non-zero $f \in K[x]$ with canonical χ-expansion

$$f = \sum_{0 \leq s} f_s \chi^s, \qquad f_s \in K[x]_{\deg(\chi)},$$

we denote $I_\chi(f) = \{s \in \mathbb{Z}_{\geq 0} \mid \mu(f_s\chi^s) = \mu(f)\}$, and

$$s_{\mu,\chi}(f) = \mathrm{Min}(I_\chi(f)), \qquad s'_{\mu,\chi}(f) = \mathrm{Max}(I_\chi(f)). \tag{1.4}$$

Lemma 1.23. *Let $f, g \in K[x]$ be non-zero polynomials. Then,*

(1) $f \sim_\mu \sum_{s \in I_\chi(f)} f_s \chi^s$.

(2) If $f \sim_\mu g$, then $I_\chi(f) = I_\chi(g)$, and $f_s \sim_\mu g_s$ for all $s \in I_\chi(f)$.

(3) The integer $s = s_{\mu,\chi}(f)$ is maximal with the property $\chi^s \mid_\mu f$. Namely, $s_{\mu,\chi}(f)$ is the order with which the prime $H_\mu(\chi)$ divides $H_\mu(f)$ in $\mathcal{G}_\mu$. In particular,

$$s_{\mu,\chi}(fg) = s_{\mu,\chi}(f) + s_{\mu,\chi}(g). \tag{1.5}$$

Key polynomials of minimal degree

Suppose that $\phi \in \mathrm{KP}(\mu)$ has minimal degree among all key polynomials for μ.

Proposition 1.24. *For any non-zero $g \in K[x]$, with ϕ-expansion $g = \sum_{0\le s} g_s\phi^s$, the following conditions are equivalent.*

(1) $g \sim_\mu a$, *for some* $a \in K[x]_{\deg(\phi)}$.

(2) $H_\mu(g)$ *is algebraic over* $\mathcal{G}_v$.

(3) $H_\mu(g)$ *is a unit in* $\mathcal{G}_\mu$.

(4) $s_{\mu,\phi}(g) = s'_{\mu,\phi}(g) = 0$.

(5) $g \sim_\mu g_0$.

Proposition 1.25. *Let $\kappa \subset \Delta$ be the algebraic closure of k in Δ. Then, κ is the maximal subfield of Δ and the mapping $\kappa \hookrightarrow \Delta \twoheadrightarrow k_\phi$ is an isomorphism.*

Let us characterize μ-minimality of any $f \in K[x]$ in terms of its ϕ-expansion.

Proposition 1.26. *For any $f \in K[x]$ with ϕ-expansion $f = \sum_{s=0}^{\ell} f_s\phi^s$, $f_\ell \neq 0$, the following conditions are equivalent:*

(1) f *is μ-minimal.*

(2) $\deg(f) = s'_{\mu,\phi}(f)\deg(\phi)$.

(3) $\deg(f_\ell) = 0$ *and* $\mu(f) = \mu\left(f_\ell\phi^\ell\right)$.

Let us introduce an important numerical invariant of a valuation on $K[x]$ admitting key polynomials.

Theorem 1.27. *For any monic non-constant $f \in K[x]$ we have*

$$\mu(f)/\deg(f) \le C(\mu) := \mu(\phi)/\deg(\phi),$$

and equality holds if and only if f is μ-minimal.

Structure of Δ as a k-algebra

Theorem 1.28.

- *If μ/v is incommensurable, then $\kappa = \Delta = k_\mu$ is a finite extension of k.*
- *If $\mathrm{KP}(\mu) = \emptyset$, then $\kappa = \Delta = k_\mu$ is an algebraic extension of k.*
- *If μ/v is commensurable and $\mathrm{KP}(\mu) \neq \emptyset$, then there exists $\xi \in \Delta$ transcendental over κ such that*

  $$\Delta = \kappa[\xi], \qquad \mathrm{Frac}(\Delta) = \kappa(\xi) \simeq k_\mu,$$

  the last isomorphism being induced by the canonical embedding $\Delta \hookrightarrow k_\mu$.

  We may take $\xi = H_\mu(\phi^e)H_\mu(u)^{-1}$, where $\phi \in \mathrm{KP}(\mu)$ is a key polynomial of minimal degree n, e is a minimal positive integer such that $e\mu(\phi) \in \Gamma_{\deg(\phi)}$, and $u \in K[x]_{\deg(\phi)}$ satisfies $\mu(u) = e\mu(\phi)$.

1.7 Residual polynomial operator

Let $\mu \in \mathbb{V}$ be a valuation with $\mathrm{KP}(\mu) \neq \emptyset$.

The choice of the pair ϕ, u as above, determines a transcendental generator ξ of Δ as a κ-algebra, and a *residual polynomial operator*:

$$R := R_\mu \colon K[x] \longrightarrow \kappa[y]$$

which is a kind of computational representation of the residual ideal operator $\mathcal{R}$.

We agree that $R(0) = 0$. For the definition of $R(f)$ for a non-zero $f \in K[x]$, let us consider its canonical ϕ-expansion $f = \sum_{0 \leq s} a_s \phi^s$.

Let us simplify the notation of some data we attached to this expansion in the last section:

$$I(f) := I_\phi(f) = \{s \in \mathbb{Z}_{\geq 0} \mid \mu(a_s\phi^s) = \mu(f)\},$$
$$s(f) := s_{\mu,\phi}(f) = \mathrm{Min}(I(f)), \qquad s'(f) := s'_{\mu,\phi}(f) = \mathrm{Max}(I(f)).$$

For $s \in I(f)$, the condition $\mu(a_s\phi^s) = \mu(f)$ implies that s belongs to a fixed class modulo e. In fact, for any pair $s, t \in I(f)$,

$$\mu(a_s\phi^s) = \mu(a_t\phi^t) \implies (t-s)\mu(\phi) = \mu(a_s) - \mu(a_t) \in \Gamma_{\deg(\phi)} \implies t \equiv s \pmod{e}.$$

Hence, $I(f) \subset \{s_0, s_1, \ldots, s_d\}$, where $d = (s'(f) - s(f))/e$, and

$$s_0 = s(f), \quad s_j = s_0 + je, \ 0 \leq j \leq d, \quad s_d = s'(f).$$

By Lemma 1.23, we may write

$$f \sim_\mu \sum_{s \in I(f)} a_s\phi^s \sim_\mu \phi^{s_0}\left(a_{s_0} + \cdots + a_{s_j}\phi^{je} + \cdots + a_{s_d}\phi^{de}\right), \tag{1.6}$$

having into account only the monomials for which $s_j \in I(f)$. We define

$$R(f) = c_0 + c_1 y + \cdots + c_{d-1}y^{d-1} + y^d \in \kappa[y],$$

where the coefficients $c_j \in \kappa$ are defined by:

$$\zeta_j = \begin{cases} H_\mu(a_{s_d})^{-1} H_\mu(u)^{j-d} H_\mu(a_{s_j}), & \text{if } s_j \in I(f), \\ 0, & \text{if } s_j \notin I(f). \end{cases} \tag{1.7}$$

We define the *normalized leading coefficient* of f as:

$$\mathrm{nlc}(f) = H_\mu(a_{s_d})H_\mu(u)^d.$$

It is a homogeneous unit in $\mathcal{G}_\mu$ of degree $\mu(f) - s(f)\mu(\phi)$.

Let us mention some of the basic properties of the operator R.

Lemma 1.29. *Let $f, g \in K[x]$ be non-zero polynomials. Then,*

- $\deg(R(f)) = d = (s'(f) - s(f))/e$.

- $R(f)(0) \neq 0$.
- $f \sim_\mu g \implies R(f) = R(g)$.
- $H_\mu(f) = \operatorname{nlc}(f)\, H_\mu(\phi)^{s(f)} R(f)(\xi)$.
- $R(fg) = R(f)R(g)$.
- $\mathcal{R}(f) = \xi^{\lceil s(f)/e \rceil} R(f)(\xi)\Delta$.

Another application of the residual polynomial operator is the characterization of all key polynomials for μ.

Proposition 1.30. *Let ϕ be a key polynomial for μ, of minimal degree.*

A monic $\chi \in K[x]$ is a key polynomial for μ if and only if one of the two following conditions is satisfied:

(a) $\deg(\chi) = \deg(\phi)$ *and* $\chi \sim_\mu \phi$.

(b) $s(\chi) = 0$, $\deg(\chi) = e \deg(\phi) \deg(R(\chi))$ *and* $R(\chi)$ *is irreducible in* $\kappa[y]$.

In the first case, $\mathcal{R}(\chi) = \xi\Delta$. In the second case, $\mathcal{R}(\chi) = R(\chi)(\xi)\Delta$.

Finally, a last relevant application of the operator R is its contribution to the study of the fibers of the mapping

$$\mathcal{R}\colon \operatorname{KP}(\mu) \to \operatorname{Max}(\Delta),$$

leading to a unique factorization theorem in $\mathcal{G}_\mu$.

Proposition 1.31. *Let $\phi, \phi' \in \operatorname{KP}(\mu)$. The following conditions are equivalent:*

1. $\phi \sim_\mu \phi'$.
2. $H_\mu(\phi)$ *and* $H_\mu(\phi')$ *are associate in* $\mathcal{G}_\mu$.
3. $\phi \mid_\mu \phi'$.
4. $\mathcal{R}(\phi) = \mathcal{R}(\phi')$.
5. $R(\phi) = R(\phi')$.

Moreover, these conditions imply $\deg(\phi) = \deg(\phi')$.

Theorem 1.32. *Let μ be a valuation with* $\operatorname{KP}(\mu) \neq \emptyset$. *The residual ideal mapping*

$$\mathcal{R}\colon \operatorname{KP}(\mu) \longrightarrow \operatorname{Max}(\Delta)$$

induces a bijection between $\operatorname{KP}(\mu)/\!\sim_\mu$ *and* $\operatorname{Max}(\Delta)$.

Theorem 1.33. *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 $\mathcal{G}_\mu$ up to associates.*

Also, up to units in $\mathcal{G}_\mu$, for any non-zero $f \in K[x]$, there is a unique factorization:

$$f \sim_\mu \prod\nolimits_{\phi \in \mathcal{P}} \phi^{a_\phi}, \quad a_\phi = s_{\mu,\phi}(f), \tag{1.8}$$

where $s_{\mu,\phi}(f)$ is the order with which the prime element $H_\mu(\phi)$ divides $H_\mu(f)$ in $\mathcal{G}_\mu$.

1.8 Valuations admitting key polynomials

Theorem 1.34. *Let μ be a valuation on $K[x]$ extending v.*
The following conditions are equivalent.

1. $\mathrm{KP}(\mu) = \emptyset$.
2. *$\mathcal{G}_\mu$ is algebraic over $\mathcal{G}_v$.*
3. *Every non-zero homogeneous element in $\mathcal{G}_\mu$ is a unit.*
4. *μ/v is commensurable and k_μ/k is algebraic.*
5. *The set of weighted values*

$$W = \{\mu(f)/\deg(f) \mid f \in K[x] \setminus K \text{ monic}\}$$

does not contain a maximal element.

Chapter 2

Augmentation of valuations

In this chapter, we review a relevant construction due to MacLane [17]. If a given valuation μ on $K[x]$ admits key polynomials, it is possible to *augment* μ to a larger valuation with a prefixed value on a given key polynomial.

MacLane dealt only with discrete rank one valuations. In 2007, Vaquié generalised MacLane's theory to arbitrary valuations [30].

Most of the content of this chapter is extracted from that paper by Vaquié. There are some results not contained in [30], which are an easy transcription to the general case of results that were obtained in [6] for discrete rank one valuations. Finally, some basic results which we could not find in the literature are probably well known.

In any case, we provide proofs of all results in order to help the reader to get some familiarity with the main features of this construction.

2.1 Basic properties of augmentation

Let us fix an arbitrary valuation μ on $K[x]$, extending v.

Definition 2.1. *Let $\iota\colon \Gamma_\mu \hookrightarrow \Gamma'$ be an order-preserving embedding of Γ_μ into another abelian ordered group. Take $\phi \in \mathrm{KP}(\mu)$ and $\gamma \in \Gamma'$ any element such that $\mu(\phi) < \gamma$.*

The augmented valuation *of μ with respect to these data is the mapping*

$$\mu'\colon K[x] \to \Gamma' \cup \{\infty\}$$

determined by:

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

$$\mu'(f) = \mathrm{Min}\left\{\mu'(a_s\phi^s) \mid 0 \le s\right\} = \mathrm{Min}\left\{\mu(a_s) + s\gamma \mid 0 \le s\right\}.$$

We use the notation $\mu' = [\mu; \phi, \gamma]$.

We emphasize that ϕ is an arbitrary key polynomial for μ, not necessarily of minimal degree. However, it becomes a key polynomial of minimal degree for the augmented valuation μ'.

Proposition 2.2. *Let $\mu' = [\mu; \phi, \gamma]$.*

(a) This mapping μ' is a valuation extending v, and satisfies

$$\mu(f) \leq \mu'(f), \qquad \forall\, f \in K[x].$$

Moreover, equality holds if and only if $\phi \nmid_\mu f$.

(b) For all $a \in K[x]_{\deg(\phi)}$, $a \neq 0$, the element $H_{\mu'}(a) \in \mathcal{G}_{\mu'}$ is a unit.

(c) The kernel of the homomorphism $\mathcal{G}_\mu \to \mathcal{G}_{\mu'}$ is the prime ideal $H_\mu(\phi)\,\mathcal{G}_\mu$.

(d) The polynomial ϕ is a key polynomial for μ' of minimal degree.

(e) The value group $\Gamma_{\mu'}$ is the subgroup $\Gamma_{\mu'} = \left\langle\, \Gamma_{\mu,\deg(\phi)}, \gamma \,\right\rangle \subset \Gamma'$.

Proof. Let us prove (a). For any non-zero $f = \sum_{0\leq s} a_s\phi^s$ it is clear that

$$\mu(f) = \operatorname{Min}\{\mu(a_s\phi^s) \mid 0 \leq s\} \leq \operatorname{Min}\{\mu(a_s) + s\gamma \mid 0 \leq s\} = \mu'(f).$$

Equality holds if and only if $\mu(f) = \mu(a_0)$, which is equivalent to $\phi \nmid_\mu f$ by Lemma 1.16.

Clearly, $(\mu')^{-1}(\infty) = \{0\}$ and $\mu'_{|K} = \mu_{|K} = v$. Thus, in order to end the proof of (a) we need only to check that μ' satisfies conditions (1) and (2) of a valuation.

Let $g = \sum_{0\leq r} b_r\phi^r$ be the ϕ-expansion of another non-zero $g \in K[x]$. Clearly, $f + g = \sum_{0\leq s}(a_s + b_s)\phi^s$ is the canonical ϕ-expansion of $f + g$. Hence,

$$\begin{aligned}\mu'(f+g) &= \operatorname{Min}\{\mu(a_s + b_s) + s\gamma \mid 0 \leq s\} \\ &\geq \operatorname{Min}\{\operatorname{Min}\{\mu(a_s) + s\gamma, \mu(b_s) + s\gamma\} \mid 0 \leq s\} = \operatorname{Min}\{\mu'(f), \mu'(g)\}.\end{aligned}$$

Finally, let us check that $\mu'(fg) = \mu'(f) + \mu'(g)$. We claim that

$$\mu'\left(a_s b_r \phi^{r+s}\right) = \mu'\left(a_s\phi^s\right) + \mu'\left(b_r\phi^r\right), \qquad \forall\, r, s \geq 0. \tag{2.1}$$

In fact, let $a_s b_r = c + d\phi$, be the ϕ-expansion of $a_s b_r$. By Lemma 1.19,

$$\mu(a_s b_r) = \mu(c) \leq \mu(d\phi) = \mu(d) + \mu(\phi) < \mu(d) + \gamma.$$

The proof of (2.1) follows from this inequality, because

$$\begin{aligned}\mu'\left(a_s b_r \phi^{r+s}\right) &= \operatorname{Min}\{\mu\left(c\right) + (r+s)\gamma,\ \mu\left(d\right) + (r+s+1)\gamma\} \\ &= \mu\left(c\right) + (r+s)\gamma = \mu\left(a_s b_r\right) + (r+s)\gamma = \mu'\left(a_s\phi^s\right) + \mu'\left(b_r\phi^r\right).\end{aligned}$$

Consider the sets

$$I = \{0 \leq s \mid \mu'(a_s\phi^s) = \mu'(f)\}, \qquad J = \{0 \leq r \mid \mu'(b_r\phi^r) = \mu'(g)\},$$

and denote $i_0 = \mathrm{Min}(I)$, $j_0 = \mathrm{Min}(J)$. Write $f = F + F'$, $g = G + G'$, where

$$F = \sum_{s \geq i_0} a_s \phi^s, \qquad F' = \sum_{s < i_0} a_s \phi^s, \qquad G = \sum_{s \geq j_0} b_r \phi^r, \qquad G' = \sum_{s < j_0} b_r \phi^r.$$

If $s \notin I$ or $r \notin J$, then $\mu'(a_s b_r \phi^{r+s}) > \mu'(f) + \mu'(g)$. Hence,

$$\mu'(F'G' + F'G + G'F) > \mu'(f) + \mu'(g).$$

We need only to show that $\mu'(FG) = \mu'(f) + \mu'(g)$. Indeed, by (2.1),

$$\mu'(FG) \geq \mu'(f) + \mu'(g).$$

On the other hand, let $a_{i_0} b_{j_0} = c + d\phi$ be the ϕ-expansion of $a_{i_0} b_{j_0}$. Then, c is the canonical coefficient of degree $i_0 + j_0$ of the ϕ-expansion of FG, and Lemma 1.19 shows that $\mu(a_{i_0} b_{j_0}) = \mu(c)$. Therefore, by (2.1),

$$\mu'(FG) \leq \mu'(c\phi^{i_0+j_0}) = \mu'(a_{i_0} b_{j_0} \phi^{i_0+j_0}) = \mu'(a_{i_0}\phi^{i_0}) + \mu'(b_{j_0}\phi^{j_0}) = \mu'(f) + \mu'(g).$$

This ends the proof of (a).

By Lemma 1.19, ϕ is irreducible in $K[x]$. Hence, any non-zero $a \in K[x]_{\deg(\phi)}$ is coprime to ϕ, and we have a Bézout identity in $K[x]$,

$$ab = 1 + \phi\, q, \qquad \deg(b),\, \deg(q) < \deg(\phi).$$

On the other hand, (a) shows that $\mu(ab) = \mu'(ab)$, because $\phi \nmid_\mu ab$. Thus,

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

so that $ab \sim_{\mu'} 1$ and $H_{\mu'}(a)$ is a unit in $\mathcal{G}_{\mu'}$. This proves (b).

The canonical mapping $\mathcal{G}_\mu \to \mathcal{G}_{\mu'}$ sends

$$H_\mu(g) \mapsto \begin{cases} H_{\mu'}(g), & \text{if } \mu(g) = \mu'(g), \\ 0, & \text{if } \mu(g) < \mu'(g). \end{cases}$$

By (a), $H_\mu(g) \in \mathrm{Ker}\,(\mathcal{G}_\mu \to \mathcal{G}_{\mu'})$ if and only if $\phi \mid_\mu g$. This proves (c)

Lemma 1.16, shows that ϕ is μ'-minimal. Let us prove that ϕ is μ'-irreducible.

Suppose $\phi \nmid_{\mu'} f$, $\phi \nmid_{\mu'} g$ for some $f, g \in K[x]$. Let a_0, b_0 be the coefficients of 0-th degree of the ϕ-expansions of f and g, respectively. Let $a_0 b_0 = c + d\phi$ be the ϕ-expansion of $a_0 b_0$, so that c is the coefficient of 0-th degree of the ϕ-expansion of fg. By Lemma 1.19, $\mu(a_0 b_0) = \mu(c)$.

By Lemma 1.16, $\mu'(f) = \mu'(a_0) = \mu(a_0)$, $\mu'(g) = \mu'(b_0) = \mu(b_0)$. Hence,

$$\mu'(fg) = \mu(a_0 b_0) = \mu(c) = \mu'(c).$$

Hence, $\phi \nmid_{\mu'} fg$, by Lemma 1.16. This shows that ϕ is a key polynomial for μ'.

By (b), ϕ has minimal degree among all key polynomials for μ'. In fact, any $a \in K[x]_{\deg(\phi)}$ is not μ'-irreducible, because $H_{\mu'}(a)$ is a unit in $\mathcal{G}_{\mu'}$. This ends the proof of (d).

Finally, statement (e) follows immediately from the definition of μ'. □

Let us analyze when different building data ϕ, γ may determine the same augmented valuation of a given μ.

Lemma 2.3. *Let $\phi, \phi_* \in \mathrm{KP}(\mu)$, $\gamma, \gamma_* \in \Gamma'$ such that $\gamma > \mu(\phi)$, $\gamma_* > \mu(\phi_*)$. Then,*

$$[\mu; \phi, \gamma] = [\mu; \phi_*, \gamma_*] \iff \deg(\phi) = \deg(\phi_*), \quad \mu(\phi - \phi_*) \geq \gamma = \gamma^*.$$

In this case, $\phi \sim_\mu \phi_*$.

Proof. Denote $\eta = [\mu; \phi, \gamma]$, $\eta_* = [\mu; \phi_*, \gamma_*]$. The right-hand condition yields $\mu(\phi - \phi_*) \geq \gamma > \mu(\phi)$, so that $\phi \sim_\mu \phi_*$.

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

$$\deg(\phi) = \mathrm{Min}\{\deg(g) \mid g \in K[x],\ \mu(g) < \eta(g)\} = \deg(\phi_*).$$

Write $\phi = \phi_* + a$, with $\deg(a) < \deg(\phi) = \deg(\phi_*)$. By the definition of the augmented valuations,

$$\gamma = \eta(\phi) = \eta_*(\phi) = \mathrm{Min}\{\mu(a), \gamma_*\}, \qquad \gamma_* = \eta_*(\phi_*) = \eta(\phi_*) = \mathrm{Min}\{\mu(a), \gamma\}.$$

This implies $\gamma_* = \gamma \leq \mu(a)$.

Conversely, suppose $\gamma = \gamma_*$, $\deg(\phi) = \deg(\phi_*)$ and $\mu(\phi - \phi_*) \geq \gamma$.

Consider the ϕ_*-expansion $\phi = \phi_* + a$, with $a = \phi - \phi_* \in K[x]_{\deg(\phi)}$. By the definition of η_*,

$$\eta_*(\phi) = \mathrm{Min}\{\mu(a), \gamma_*\} = \gamma_* = \gamma.$$

Hence, for any non-zero $f \in K[x]$ with ϕ-expansion $f = \sum_{0 \leq s} a_s \phi^s$, we have

$$\eta_*(f) \geq \mathrm{Min}\,\{\eta_*(a_s\phi^s) \mid 0 \leq s\} = \mathrm{Min}\,\{\mu(a_s) + s\gamma \mid 0 \leq s\} = \eta(f).$$

The symmetry of the argument shows that $\eta_* = \eta$. □

Let us quote an auxiliary result about μ'-minimal polynomials.

Lemma 2.4. *Let $\mu' = [\mu; \phi, \gamma]$ and $f \in K[x]$ a monic μ'-minimal polynomial with $\deg(f) = \deg(\phi)$. Then, $f \sim_\mu \phi$.*

Proof. Since $\deg(f) = \deg(\phi)$ and both polynomials are monic, the canonical ϕ-expansion of f is

$$f = a + \phi, \qquad a \in K[x]_{\deg(\phi)}.$$

By Proposition 2.2, ϕ is a key polynomial for μ' of minimal degree. Therefore, the criterion of μ'-minimality given in Proposition 1.26 shows that $\mu'(f) = \mu'(\phi)$. Hence,

$$\mu(f - \phi) = \mu(a) = \mu'(a) \geq \mu'(f) = \mu'(\phi) > \mu(\phi),$$

so that $f \sim_\mu \phi$. □

2.2 Image of the homomorphism $\mathcal{G}_\mu \to \mathcal{G}_{\mu'}$

The next result will be used very often along the rest of the memoir.

Lemma 2.5. *Let $\mu' = [\mu; \phi, \gamma]$ and $f \in K[x]$ a non-zero polynomial.*
If $\phi \nmid_\mu f$, then $H_\mu(f)$ is a unit in $\mathcal{G}_{\mu'}$.

Proof. Write $f = a + q\phi$ with a, $q \in K[x]$ and $\deg(a) < \deg(\phi)$.

By Lemma 1.16, $\mu(f) = \mu(a) \leq \mu(q\phi)$, and Proposition 2.2 shows that $\mu(f) = \mu'(f)$. Putting both results together, we get

$$\mu'(f) = \mu(f) = \mu(a) \leq \mu(q\phi) < \mu'(q\phi) = \mu'(f - a),$$

so that $f \sim_{\mu'} a$. By item (b) of Proposition 2.2, $H_{\mu'}(f) = H_{\mu'}(a)$ is a unit in $\mathcal{G}_{\mu'}$. □

By Proposition 2.2, all homogeneous elements in the image of the canonical homomorphism $\mathcal{G}_\mu \to \mathcal{G}_{\mu'}$ are those of the form $H_{\mu'}(f)$ with $\phi \nmid_\mu f$.

By Lemma 2.5, all these homogeneous elements in $\mathrm{Im}(\mathcal{G}_\mu \to \mathcal{G}_{\mu'})$ are units.

Let us give a more precise description of the image of the homogeneous elements of degree zero.

Lemma 2.6. *Let $\mu' = [\mu; \phi, \gamma]$. Then,*

$$\mathrm{Ker}(\Delta_\mu \to \Delta_{\mu'}) = \mathcal{R}_\mu(\phi), \qquad \mathrm{Im}(\Delta_\mu \to \Delta_{\mu'}) = \kappa_{\mu'} \hookrightarrow k_{\mu'},$$

where $\kappa_{\mu'}$ is the algebraic closure of k simultaneously in $\Delta_{\mu'}$ and in $k_{\mu'}$.

Also, $\kappa^*_{\mu'} = \Delta^*_{\mu'}$, and $\kappa_{\mu'}$ is k-isomorphic to the residue class feld k_ϕ of the semivaluation v_ϕ.

Proof. The statement about the kernel follows from the definition of $\mathcal{R}_\mu(\phi)$, and the description of $\mathrm{Ker}(\mathcal{G}_\mu \to \mathcal{G}_{\mu'})$ in Proposition 2.2.

The statement about the image follows from Propositions 1.22 and 1.25. □

2.3 Generically, $\Gamma_{\mu'}$ contains Γ_μ

The group $\Gamma_{\mu'}$ does not necessarily contain Γ_μ.

For instance, for the valuations

$$\mu = [\mu_{\mathrm{Gauss}}; x, 1/2], \qquad \mu' = [\mu; x, 1] = [\mu_{\mathrm{Gauss}}; x, 1],$$

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

This anomalous behaviour may occur only when all key polynomials for μ of minimal degree are μ-equivalent.

Lemma 2.7. *Let ϕ_0 be a key polynomial for μ of minimal degree, and let ϕ be a key polynomial for μ such that $\phi \nmid_\mu \phi_0$. Then,*

(1) $\Gamma_{\mu,\deg(\phi)} = \Gamma_\mu$.

(2) The semivaluation v_ϕ on K_ϕ defined in section 1.6 has group of values $\Gamma_{v_\phi} = \Gamma_\mu$.

(3) All augmentations $\mu' = [\mu; \phi, \gamma]$ have $\Gamma_{\mu'} = \left\langle \Gamma_\mu, \gamma \right\rangle \supset \Gamma_\mu$.

Proof. For any augmentation $\mu' = [\mu; \phi, \gamma]$, Propositions 1.21 and 2.2 show that

$$\Gamma_{v_\phi} = \Gamma_{\mu,\deg(\phi)}, \qquad \Gamma_{\mu'} = \left\langle \Gamma_{\mu,\deg(\phi)}, \gamma \right\rangle.$$

Hence, the two last statements of the lemma follow from (1), which is proved in [23, Cor. 6.4]. □

2.4 Maximal semivaluations in $\mathbb{V}$

Let us go back to our space $\mathbb{V}$ of semivaluations on $K[x]$ extending v, with values in $\mathbb{Q}\Gamma$, introduced in section 1.4.

All semivaluations in $\mathbb{V}$ which are not valuations are maximal.

Lemma 2.8. *Let $\nu \in \mathbb{V}$ be a semivaluation with support $\mathfrak{p} \neq 0$.*
Then, ν is maximal in $\mathbb{V}$ with respect to the partial ordering $\leq$.

Proof. Suppose $\nu \leq \mu$ for some $\mu \in \mathbb{V}$. Then, $\mathfrak{p} \subset \mathfrak{p}_\mu$, and this implies $\mathfrak{p} = \mathfrak{p}_\mu$, because $\mathfrak{p}$ and $\mathfrak{p}_\mu$ are maximal ideals.

Hence, $\overline{\nu}$, $\overline{\mu}$ are two valuations on the same finite extension $L = \kappa(\mathfrak{p})$ of K, and they satisfy $\overline{\nu}(\xi) \leq \overline{\mu}(\xi)$ for all $\xi \in L$. In particular, $\mathcal{O}_{\overline{\nu}} \subset \mathcal{O}_{\overline{\mu}}$, and this implies $\overline{\nu} = \overline{\mu}$ [5, Lem. 3.2.8]. Hence, $\nu = \mu$. □

Let $\mu \in \mathbb{V}$ be a valuation. If $\mathrm{KP}(\mu) \neq \emptyset$, then Proposition 2.2 shows that μ is not maximal with respect to the partial ordering in $\mathbb{V}$.

The converse implication holds too: if μ is not maximal in $\mathbb{V}$, then $\mathrm{KP}(\mu) \neq \emptyset$.

Proposition 2.9. *[30, Thm. 1.15] Let $\mu, \mu^* \in \mathbb{V}$ such that $\mu < \mu^*$. Let $\phi \in K[x]$ be a monic polynomial with minimal degree satisfying $\mu(\phi) < \mu^*(\phi)$. Then, μ is a valuation satisfying*

(1) *$\mu(g) = \mu^*(g)$ if and only if $\phi \nmid_\mu g$.*

(2) *ϕ is a key polynomial for μ.*

(3) *$\mu < [\mu; \phi, \gamma] \leq \mu^*$, for $\gamma = \mu^*(\phi)$.*

Proof. By Lemma 2.8, μ is a valuation.

Let us prove (1). If $\phi \mid_\mu g$, we have $g \sim_\mu \phi\, q$ for some $q \in K[x]$. Hence,

$$\mu^*(g - \phi q) \geq \mu(g - \phi q) > \mu(g) = \mu(\phi q).$$

Since $\mu^*(\phi q) > \mu(\phi q) = \mu(g)$, we deduce

$$\mu^*(g) \geq \mathrm{Min}\{\mu^*(\phi q), \mu^*(g - \phi q)\} > \mu(g).$$

Conversely, suppose that $\mu(g) < \mu^*(g)$. Let $g = q\phi + a$, with $\deg(a) < \deg(\phi)$. By the minimality of $\deg(\phi)$, we have $q \neq 0$ and $\mu^*(a) = \mu(a)$.

Therefore, $g \sim_\mu q\phi$, because

$$\mu(g - \phi q) = \mu^*(g - \phi q) \geq \mathrm{Min}\{\mu^*(g), \mu^*(q\phi)\} > \mathrm{Min}\{\mu(g), \mu(q\phi)\} = \mu(g),$$

the last equality by Lemma 1.16.

Let us prove (2). If $g \in K[x]$ has $\deg(g) < \deg(\phi)$, we have $\mu(g) = \mu^*(g)$. Hence, $\phi \nmid_\mu g$ by item (1). This shows that ϕ is μ-minimal.

Now, suppose $\phi \nmid_\mu f$, $\phi \nmid_\mu g$. By item (1), $\mu^*(f) = \mu(f)$ and $\mu^*(g) = \mu(g)$. Hence, $\mu^*(fg) = \mu(fg)$, leading to $\phi \nmid_\mu fg$ by item (1). This implies that ϕ is μ-irreducible.

Finally, (3) is obvious. For any $g = \sum_{0 \leq s} a_s \phi^s \in K[x]$, we have

$$\mu^*(g) \geq \mathrm{Min}\{\mu^*(a_s\phi^s) \mid 0 \leq s\} = \mathrm{Min}\{\mu'(a_s\phi^s) \mid 0 \leq s\} = \mu'(g),$$

where we denoted $\mu' = [\mu; \phi, \gamma]$. □

Corollary 2.10. *Let μ be a valuation in $\mathbb{V}$. Then, μ is maximal in $\mathbb{V}$ with respect to the partial ordering $\leq$ if and only if $\mathrm{KP}(\mu)$ is empty.*

Notation. *Let us denote by $[\phi]_\mu$, or simply $[\phi]$ if μ is clear fom the context, the μ-equivalence class of a key polynomial ϕ.*

Corollary 2.11. *Let $\mu, \mu^* \in \mathbb{V}$ such that $\mu < \mu^*$. Let Φ_{μ,μ^*} be the set of all monic polynomials $\phi \in K[x]$ of minimal degree satisfying $\mu(\phi) < \mu^*(\phi)$. Then, μ is a valuation and Φ_{μ,μ^*} is one of the equivalence classes in the quotient set $\mathrm{KP}(\mu)/\sim_\mu$.*

Proof. By Lemma 2.8, μ is a valuation. Take any $\phi \in \Phi_{\mu,\mu^*}$. By Proposition 2.9, ϕ is a key polynomial for μ, and for all non-zero $g \in K[x]$:

$$\phi \mid_\mu g \iff \mu(g) < \mu^*(g).$$

In particular, all $\chi \in \Phi_{\mu,\mu^*}$ are key polynomials for μ satisfying $\phi \mid_\mu \chi$. Since $\deg(\chi) = \deg(\phi)$, Lemma 1.18 shows that all $\chi \in \Phi_{\mu,\mu^*}$ belong to the equivalence class $[\phi]$.

Conversely, any $\chi \in [\phi]$ has degree $\deg(\phi)$ by Proposition 1.31. Since $\phi \mid_\mu \chi$, we have $\mu(\chi) < \mu^*(\chi)$, so that $\chi \in \Phi_{\mu,\mu^*}$. This proves that $\Phi_{\mu,\mu^*} = [\phi]$. □

We end the chapter with another important application of Proposition 2.9.

Theorem 2.12. *For any $\mu, \mu^* \in \mathbb{V}$ such that $\mu < \mu^*$, the interval $[\mu, \mu^*] \subset \mathbb{V}$ is totally ordered.*

Actually, we may formulate this result in an apparently stronger form.

Theorem 2.13. *Let $\eta, \eta', \mu^* \in \mathbb{V}$ such that $\eta, \eta' < \mu^*$. Then either $\eta \leq \eta'$ or $\eta' \leq \eta$.*

Proof. Take monic polynomials $\phi, \phi' \in K[x]$ of minimal degree satisfying

$$\eta(\phi) < \mu^*(\phi), \qquad \eta'(\phi') < \mu^*(\phi'),$$

respectively. By Proposition 2.9, η, η' are valuations and $\phi \in \mathrm{KP}(\eta)$, $\phi' \in \mathrm{KP}(\eta')$.

Suppose $\deg(\phi) < \deg(\phi')$. By the minimality of $\deg(\phi)$ and $\deg(\phi')$,

$$\eta'(\phi) = \mu^*(\phi) > \eta(\phi), \qquad \eta'(a) = \mu^*(a) = \eta(a), \quad \forall\, a \in K[x]_{\deg(\phi)}.$$

Hence, for any non-zero $g \in K[x]$ with ϕ-expansion $g = \sum_{0\le s} a_s\phi^s$, we have:

$$\eta'(g) \ge \mathrm{Min}_{0\le s}\{\eta'(a_s\phi^s)\} \ge \mathrm{Min}_{0\le s}\{\eta(a_s\phi^s)\} = \eta(g),$$

so that $\eta' \ge \eta$.

Now, suppose $\deg(\phi) = \deg(\phi')$. Then, $\phi = \phi' + a$ for some $a \in K[x]_{\deg(\phi)}$. By the η'-minimality of ϕ' we have $\eta'(\phi) \le \eta'(\phi')$.

After eventually exchanging η and η', we may assume that $\eta'(\phi') \le \eta(\phi)$. Then,

$$\eta'(\phi) \le \eta'(\phi') \le \eta(\phi) < \mu^*(\phi).$$

By Proposition 2.9, this implies $\phi' \mid_{\eta'} \phi$. By Lemma 1.18, $\phi' \sim_{\eta'} \phi$, and ϕ is a key polynomial for η'. In particular, $\eta'(\phi) = \eta'(\phi') \le \eta(\phi)$. Therefore,

$$\eta(g) = \mathrm{Min}_{0\le s}\{\eta(a_s\phi^s)\} \ge \mathrm{Min}_{0\le s}\{\eta'(a_s\phi^s)\} = \eta'(g),$$

so that $\eta' \le \eta$. □

PART II

Inductive valuations on polynomial rings

Chapter 3

Newton polygons

In this chapter, we review some basic facts about the Newton polygon operator attached to a pair μ, ϕ, where μ is a valuation on $K[x]$ and ϕ is an arbitrary key polynomial for μ.

Tipically, when μ is a rank one valuation, the Newton polygon of a polynomial in $K[x]$ lies in the euclidean plane. For higher rank valuations, Newton polygons of polynomials lie in the rational vector space $\mathbb{Q} \times \mathbb{Q}\Gamma$.

Apart from this change of ambient space, all results of this chapter are an easy transcription of the results of [6, Sec.2], up to a different normalization of the Newton polygons.

3.1 The rational space $\mathbb{Q} \times \mathbb{Q}\Gamma$

Given any two points in the $\mathbb{Q}$-vector space $\mathbb{Q} \times \mathbb{Q}\Gamma$

$$P = (s, \alpha),\ Q = (t, \beta)\ \in\ \mathbb{Q} \times \mathbb{Q}\Gamma,$$

we may define the segment joining them, as the subset

$$S = \{(s, \alpha) + \epsilon\,(t - s, \beta - \alpha)\ |\ \ \epsilon \in \mathbb{Q},\ 0 \leq \epsilon \leq 1\} \subset \mathbb{Q} \times \mathbb{Q}\Gamma.$$

If $P = Q$, this segment contains a single point $S = \{P\}$.

If $s \neq t$, this segment has a natural *slope*

$$\mathrm{sl}(S) := \mathrm{sl}(P, Q) := (\beta - \alpha)/(t - s) \in \mathbb{Q}\Gamma,$$

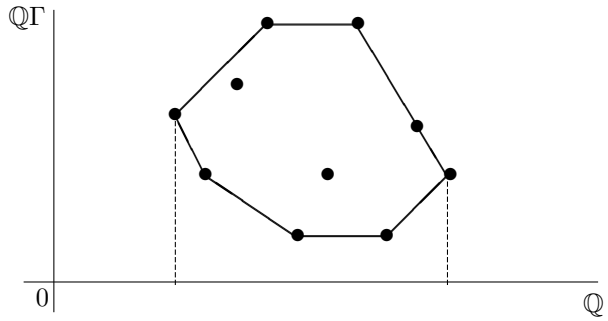
uniquely determined by the pair P, Q, regardless of the order in which these points are considered.

If $s = t$, but $\alpha \neq \beta$, we may agree that $\mathrm{sl}(S) = \infty$.

A subset of $\mathbb{Q} \times \mathbb{Q}\Gamma$ is *convex* if it contains the segment joining any two points in the subset. The *convex hull* of a finite subset $\mathcal{C} \subset \mathbb{Q} \times \mathbb{Q}\Gamma$ is the smallest convex subset of $\mathbb{Q} \times \mathbb{Q}\Gamma$ containing $\mathcal{C}$.

The border of this hull is a sequence of chained segments. If the points in $\mathcal{C}$ have different abscissas, the leftmost and rightmost points are joined by two different chains of segments along the border, called the *upper* and *lower* convex hull of $\mathcal{C}$, respectively.

Figure 3.1: Convex hull of a finite set of points with different abscissas



3.2 Newton polygon operator attached to μ, ϕ

Let $\mu\colon K[x] \to \mathbb{Q}\Gamma \cup \{\infty\}$ be a valuation in $\mathbb{V}$.

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

$$N_{\mu,\phi}\colon\ K[x] \longrightarrow \mathcal{P}\left(\mathbb{Q} \times \mathbb{Q}\Gamma\right),$$

where $\mathcal{P}\left(\mathbb{Q} \times \mathbb{Q}\Gamma\right)$ is the set of subsets of the rational space $\mathbb{Q} \times \mathbb{Q}\Gamma$.

The Newton polygon of the zero polynomial is the empty set. If

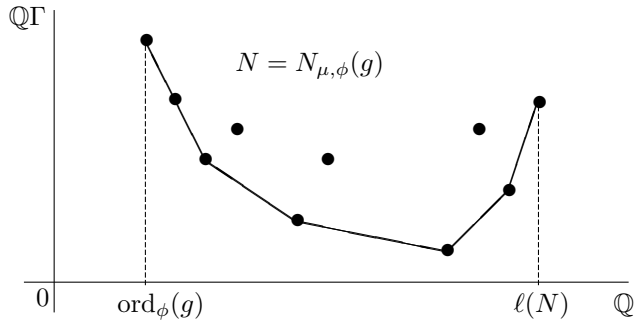
$$g = \sum\nolimits_{0 \le s} a_s \phi^s, \qquad \deg(a_s) < \deg(\phi)$$

is the canonical ϕ-expansion of a non-zero $g \in K[x]$, then $N := N_{\mu,\phi}(g)$ is defined to be the lower convex hull of the finite cloud of points

$$\mathcal{C} = \{(s, \mu(a_s)) \mid s \in \mathbb{Z}_{\ge 0}\} \subset \mathbb{Q} \times \mathbb{Q}\Gamma.$$

Figure 3.2 displays the typical shape of such a polygon.

Figure 3.2: Newton polygon of $g \in K[x]$



The abscissa of the left endpoint of N is the smallest integer s such that $a_s \neq 0$. In other words, $s = \mathrm{ord}_\phi(g)$.

The abscissa of the right endpoint of N is called the *length* of N, and is denoted $\ell(N)$. Clearly,

$$\ell(N) = \lfloor \deg(g)/\deg(\phi) \rfloor\,.$$

If N is not a single point, we formally write

$$N = S_1 \vdash \cdots \vdash S_k, \qquad \mathrm{sl}(S_1) < \cdots < \mathrm{sl}(S_k),$$

where the segments S_i are the *sides* of N ordered by their increasing slopes.

The left and right endpoints of N, together with the points joining two different sides are called *vertices* of N.

The points $P = (s, \alpha)$ lying on a side S are characterized by the following property:

$$\begin{aligned} &\mathrm{sl}(S) \geq \mathrm{sl}(P, Q), \quad \forall\, Q = (t, \beta) \in \mathcal{C}, \text{ with } t < s, \\ &\mathrm{sl}(S) \leq \mathrm{sl}(P, Q), \quad \forall\, Q = (t, \beta) \in \mathcal{C}, \text{ with } t > s. \end{aligned}$$

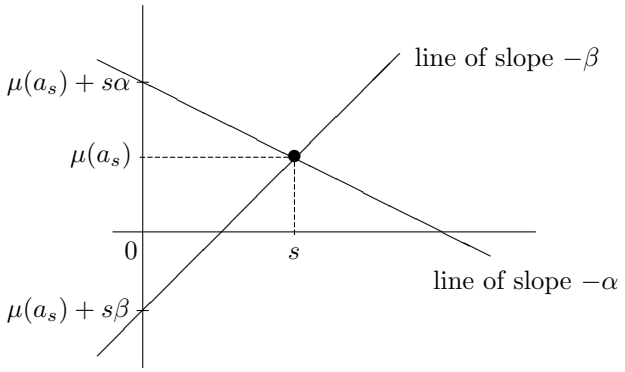
λ-component of a Newton polygon

The next (trivial) observation is emphasized because we are often going to use it in what follows.

Remark 3.1. *For any $\lambda \in \mathbb{Q}\Gamma$, the line of slope $-\lambda$ passing through the point $(s, \mu(a_s)) \in \mathcal{C}$ meets the vertical axis at a point with ordinate $\mu(a_s) + s\lambda$.*

Figure 3.3 illustrates Remark 3.1 for positive and negative values of λ.

Figure 3.3: Lines passing through a point of the cloud $\mathcal{C}$. Note that $\alpha > 0$ and $\beta < 0$.



Definition 3.2. *Let $N = N_{\mu,\phi}(g)$ be the Newton polygon of some non-zero polynomial $g \in K[x]$, and let $\lambda \in \mathbb{Q}\Gamma$.*

The λ-component *$S_\lambda(N) \subset N$ is the intersection of N with the line of slope $-\lambda$ which first touches N from below.*

The left and right endpoints of $S_\lambda(N)$ are denoted

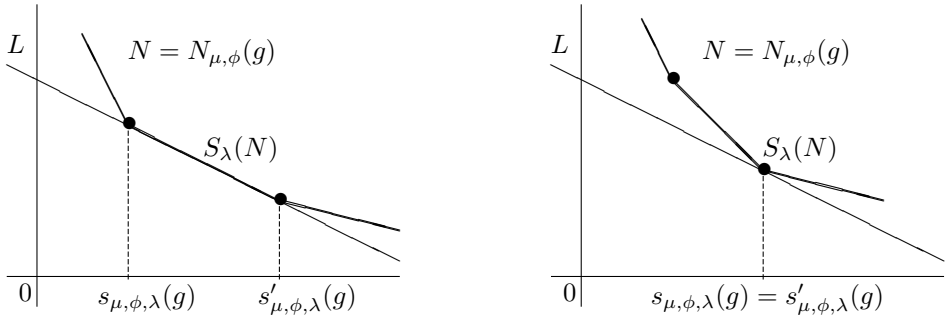
$$(s_{\mu,\phi,\lambda}(g), u_{\mu,\phi,\lambda}(g)), \quad (s'_{\mu,\phi,\lambda}(g), u'_{\mu,\phi,\lambda}(g)) \ \in \ \mathbb{Z}_{\geq 0} \times \Gamma_\mu.$$

Definition 3.3. *We say that $N = N_{\mu,\phi}(g)$ is* one-sided *of slope $-\lambda$ if*

$$N = S_\lambda(N), \qquad s_{\mu,\phi,\lambda}(g) = 0, \qquad s'_{\mu,\phi,\lambda}(g) > 0.$$

If N has a side S of slope $-\lambda$, then $S_\lambda(N) = S$. Otherwise, $S_\lambda(N)$ is a vertex of N. Figure 3.4 illustrates both possibilities.

Figure 3.4: λ-component of $N_{\mu,\phi}(g)$. In both pictures the line L has slope $-\lambda$.



Principal Newton polygons

By Remark 3.1,

$$S_\lambda(N) = \{(s,u) \in N \mid u + s\lambda \text{ is minimal}\},$$

and the line of slope $-\lambda$ containing $S_\lambda(N)$ meets the vertical axis at the point with ordinate

$$\text{Min}\{\mu(a_s) + s\lambda \mid 0 \leq s\}. \tag{3.1}$$

Since ϕ is μ-minimal, Lemma 1.16 shows that this value (3.1) coincides with $\mu(g)$ if we take $\lambda = \mu(\phi)$. The next remark follows.

Remark 3.4. *For any non-zero $g \in K[x]$, the value $\mu(g) \in \mathbb{Q}\Gamma$ is the ordinate of the point where the vertical axis meets the line of slope $-\mu(\phi)$ containing the $\mu(\phi)$-component of the Newton polygon $N_{\mu,\phi}(g)$.*

As a consequence, the $\mu(\phi)$-component of $N_{\mu,\phi}(g)$ plays a special role. In Lemma 3.6 below some particular data attached to this component are described.

On the other hand, the sides of $N_{\mu,\phi}(g)$ with slope strictly lower than $-\mu(\phi)$ contain as well rich arithmetic information about the polynomial g, with respect to the key polynomial ϕ.

More precisely, if $-\gamma$ is a slope of $N_{\mu,\phi}(g)$ with $\gamma > \mu(\phi)$, then the augmented valuation $\mu' = [\mu; \phi, \gamma]$ will contain relevant information about g, with respect to ϕ.

This motivates the next definition.

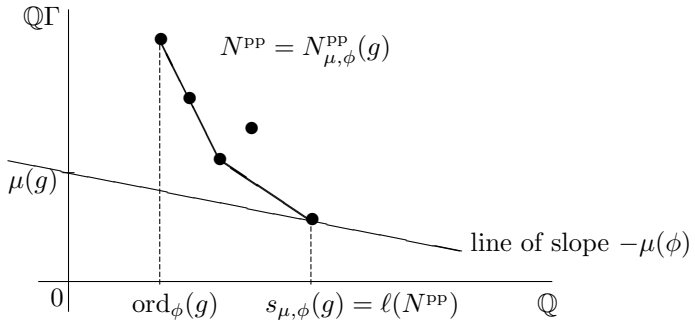
Definition 3.5. *The* principal Newton polygon $N^{pp}_{\mu,\phi}(g)$ *is the polygon formed by the sides of $N_{\mu,\phi}(g)$ of slope less than $-\mu(\phi)$.*

If $N_{\mu,\phi}(g)$ has no sides of slope less than $-\mu(\phi)$, then $N^{pp}_{\mu,\phi}(g)$ is defined to be the left endpoint of $N_{\mu,\phi}(g)$.

Figure 3.5 displays a principal Newton polygon, and illustrates the computation of $\mu(g)$ according to Remark 3.4.

The length of a principal Newton polygon has an interesting algebraic interpretation in terms of the graded algebra $\mathcal{G}_\mu$, as shown in item (2) of the next lemma.

Figure 3.5: Principal Newton polygon of $g \in K[x]$



Lemma 3.6. *Let $N = N_{\mu,\phi}(g)$ be the Newton polygon of a non-zero $g \in K[x]$.*

(1) The abscissas of the endpoints of the $\mu(\phi)$-component of N are

$$s_{\mu,\phi,\mu(\phi)}(g) = s_{\mu,\phi}(g), \qquad s'_{\mu,\phi,\mu(\phi)}(g) = s'_{\mu,\phi}(g),$$

where $s_{\mu,\phi}(g)$, $s'_{\mu,\phi}(g)$ are the invariants introduced in (1.4).

(2) The length of the principal polygon $N^{pp}_{\mu,\phi}(g)$ is equal to the order with which the prime element $H_\mu(\phi)$ divides $H_\mu(g)$ in the graded algebra $\mathcal{G}_\mu$:

$$\ell\left(N^{pp}_{\mu,\phi}(g)\right) = s_{\mu,\phi}(g).$$

(3) If $h \in K[x]$ satisfies $g \sim_\mu h$, then $S_{\mu(\phi)}(g) = S_{\mu(\phi)}(h)$.

Proof. Recall the notation from (1.4),

$$I_\phi(g) = \{s \in \mathbb{Z}_{\geq 0} \mid \mu(a_s\phi^s) = \mu(g)\},$$
$$s_{\mu,\phi}(g) = \mathrm{Min}(I_\phi(g)), \quad s'_{\mu,\phi}(g) = \mathrm{Max}(I_\phi(g)).$$

By Lemma 1.16, $\mu(g) = \mathrm{Min}\{\mu(a_s\phi^s) \mid 0 \leq s\}$. By Remark 3.1, the points $(s, \mu(a_s))$ lying on $S_{\mu(\phi)}(g)$ are precisely those with $s \in I_\phi(g)$. This proves (1).

It is obvious that $\ell\left(N^{\rm pp}_{\mu,\phi}(g)\right)$ is equal to the abscissa $s_{\mu,\phi,\mu(\phi)}(g)$ of the left endpoint of $S_{\mu(\phi)}(g)$. We have just seen that this abscissa is equal to $s_{\mu,\phi}(g)$, and it was proved in Lemma 1.23 that this integer is the order with which the prime element $H_\mu(\phi)$ divides $H_\mu(g)$ in the graded algebra $\mathcal{G}_\mu$. This proves (2).

Finally, if $g \sim_\mu h$, then Lemma 1.23 shows that $I_\phi(g) = I_\phi(h)$. By item (1), the two segments $S_{\mu(\phi)}(g)$, $S_{\mu(\phi)}(h)$ have endpoints with the same abscissas.

Hence, these segments coincide. In fact, the ordinates u, u' of their endpoints are determined by the abscissas s, s', and the common value

$$\mu(g) = \mu(h) = u + s\mu(\phi) = u' + s'\mu(\phi).$$

□

3.3 Newton polygons with respect to augmented valuations

For the rest of the chapter we fix a valuation $\nu \in \mathbb{V}$ and an augmentation

$$\mu = [\nu; \phi, \gamma]$$

with respect to some key polynomial $\phi \in \mathrm{KP}(\nu)$ and some value $\gamma \in \mathbb{Q}\Gamma$. Recall that

$$\gamma = \mu(\phi) > \nu(\phi).$$

Consider a non-zero $g \in K[x]$, with ϕ-expansion $g = \sum_{0 \leq s} a_s \phi^s$.
Throughout this section we denote

$$\begin{aligned} &S_\gamma(g) := S_\gamma\left(N_{\nu,\phi}(g)\right), \\ &s(g) := s_{\nu,\phi,\gamma}(g), \qquad s'(g) := s'_{\nu,\phi,\gamma}(g), \qquad u(g) := u_{\nu,\phi,\gamma}(g). \end{aligned} \tag{3.2}$$

By Proposition 2.2, ϕ is a key polynomial for μ of minimal degree among all polynomials in the set $\mathrm{KP}(\mu)$.

So, it makes sense to consider the Newton polygon $N_{\mu,\phi}(g)$, which is related to $N_{\nu,\phi}(g)$ in an obvious way:

$$N_{\mu,\phi}(g) = N_{\nu,\phi}(g). \tag{3.3}$$

In fact, they have the same finite cloud of points:

$$\deg(a_s) < \deg(\phi) \implies \phi \nmid_\nu a_s \implies \mu(a_s) = \nu(a_s),$$

the last implication by Proposition 2.2.

This trivial observation has a relevant consequence. We saw in the last section that certain information about g, μ, ϕ can be read in the Newton polygon $N_{\mu,\phi}(g)$. When we deal with an augmented valuation, this information can be read already in the Newton polygon $N_{\nu,\phi}(g)$ with respect to the "small" valuation ν from which we constructed μ by augmentation.

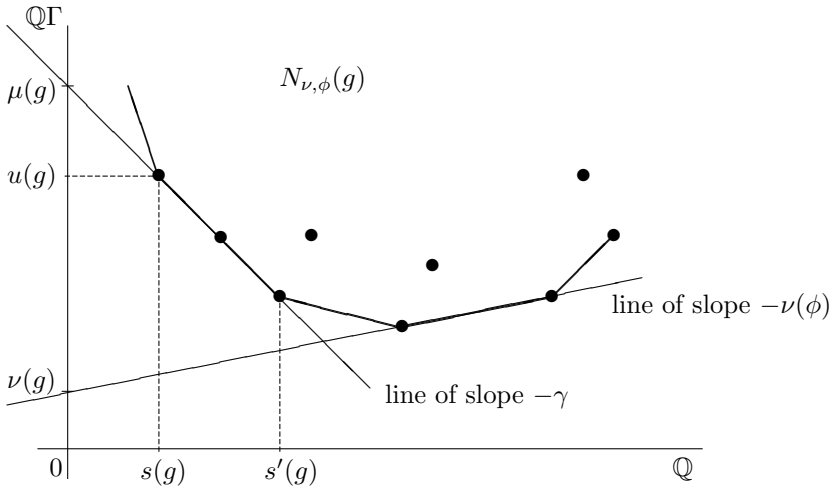
For instance, Figure 3.6 shows how to read the value $\mu(g)$, as indicated in Remark 3.4. In order to be able to quote this computation of $\mu(g)$, we state it as an independent result.

Lemma 3.7. *Consider the augmented valuation $\mu = [\nu; \phi, \gamma]$. For any non-zero $g \in K[x]$, the line of slope $-\gamma$ which first touches the polygon $N_{\nu,\phi}(g)$ from below meets the vertical axis at the point $(0, \mu(g))$.*

In the same vein, Lemma 3.6 shows that certain algebraic information concerning the graded algebra $\mathcal{G}_\mu$ can be read directly in the γ-component of $N_{\nu,\phi}(g)$.

Again, we state in an independent lemma the result of applying Lemma 3.6 to the augmented valuation μ.

Figure 3.6: $N_{\nu,\phi}(g)$ contains information about the augmented valuation $\mu = [\nu; \phi, \gamma]$



Lemma 3.8. *Let $g, h \in K[x]$ be non-zero polynomials.*

(1) The integer $s(g)$ is the order with which the prime element $H_\mu(\phi)$ divides $H_\mu(g)$ in the graded algebra $\mathcal{G}_\mu$.

(2) $s'(gh) = s'(g) + s'(h)$.

(3) If $g \sim_\mu h$, then $S_\gamma(g) = S_\gamma(h)$.

Proof. By Lemma 3.6,

$$s(g) = s_{\nu,\phi,\gamma}(g) = s_{\mu,\phi,\gamma}(g) = s_{\mu,\phi}(g),$$

is the order with which the prime element $H_\mu(\phi)$ divides $H_\mu(g)$ in the graded algebra $\mathcal{G}_\mu$. This proves (1).

The right endpoint of $S_\gamma(g)$ equals the left endpoint of $S_{\epsilon\gamma}(g)$, for $0 < \epsilon < 1$ sufficiently close to 1. Hence, $s'(g) = s'_{\nu,\phi,\gamma}(g) = s_{\nu,\phi,\epsilon\gamma}(g)$.

By item (1) applied to the augmented valuation $\mu' = [\nu; \phi, \epsilon\gamma]$, we deduce that $s'(g)$ is the order with which the prime element $H_{\mu'}(\phi)$ divides $H_{\mu'}(g)$ in the graded algebra $\mathcal{G}_{\mu'}$. This proves (2) (see equation (1.5)).

Item (3) follows directly from item (3) of Lemma 3.6. □

Remark. In item (2) of Lemma 3.8, it is essential that μ is an augmented valuation.

The analogous statement for an arbitrary valuation holds only if ϕ is a key polynomial of minimal degree [23].

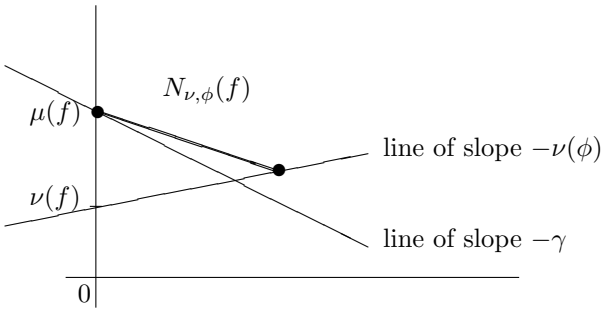
An example

Newton polygons constitute a malleable tool, wich enables us to "visualize" sophisticated relationships in the graded algebra $\mathcal{G}_\mu$, whose checking by purely algebraic techniques may require some onerous work.

As an example, let us show that the converse implication of Lemma 2.5 is false.

For instance, consider a polynomial f with Newton polygon $N_{\nu,\phi}(f)$ as indicated in Figure 3.7. That is, $N_{\nu,\phi}(f)$ is one-sided of slope greater than $-\gamma$ (Definition 3.3).

Figure 3.7: An example where $\phi \mid_\nu f$ but $H_\mu(f)$ is a unit in $\mathcal{G}_\mu$



Then, the line of slope $-\gamma$ first touching the polygon from below meets the polygon only at the point $(0, \mu(f))$. Thus, $S_\gamma(f) = \{(0, \mu(f))\}$, so that $s(f) = s'(f) = 0$.

By Lemma 3.8, $s_{\mu,\phi}(f) = s'_{\mu,\phi}(f) = 0$, and Proposition 1.24 shows that $H_\mu(f)$ is a unit in $\mathcal{G}_\mu$.

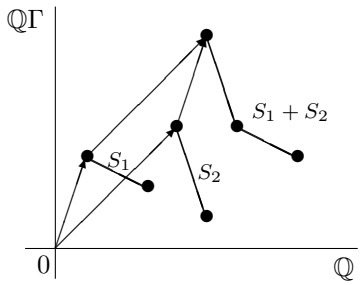
On the other hand, since $\nu(\phi) < \gamma$ and $N_{\nu,\phi}(f)$ has a positive length, the line of slope $-\nu(\phi)$ first touching the polygon from below will meet the vertical axis at a point whose ordinate will be smaller than $\mu(f)$. Therefore, $\nu(f) < \mu(f)$, and Proposition 2.2 shows that $\phi \mid_\nu f$.

3.4 Addition of Newton polygons

There is a natural addition of segments in the space $\mathbb{Q} \times \mathbb{Q}\Gamma$. We admit that a point is a segment whose right and left endpoints coincide.

The sum $S_1 + S_2$ of two segments is the ordinary vector sum if at least one of the segments is a single point. Otherwise, $S_1 + S_2$ is the polygon whose left endpoint is the vector sum of the two left endpoints 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. 3.8).

Figure 3.8: Addition of two segments



We keep dealing with an arbitrary valuation $\nu \in \mathbb{V}$, and a key polynomial $\phi \in \mathrm{KP}(\nu)$. Also, for any $\gamma \in \mathbb{Q}\Gamma$, $\gamma > \nu(\phi)$, we keep using the notation of (3.2).

Lemma 3.9. *For non-zero $g, h \in K[x]$, and any $\gamma \in \mathbb{Q}\Gamma$, $\gamma > \nu(\phi)$, we have*

$$S_\gamma(gh) = S_\gamma(g) + S_\gamma(h).$$

Proof. Since the involved segments either have the same slope or consist of a single point, 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 (1.5) and Lemma 3.8.

In order to prove the third, consider the augmented valuation $\mu = [\nu; \phi, \gamma]$. By Lemma 3.7,

$$u(g) + s(g)\gamma = \mu(g), \qquad u(h) + s(h)\gamma = \mu(h), \qquad u(gh) + s(gh)\gamma = \mu(gh).$$

Since $s(gh) = s(g) + s(h)$, the claimed identity $u(gh) = u(g) + u(h)$ follows from $\mu(gh) = \mu(g) + \mu(h)$. □

The addition of segments may be extended to an addition law for Newton polygons in a natural way [9, Sec. 1]. Given two polygons

$$N = S_1 \vdash \cdots \vdash S_k, \qquad N' = S'_1 \vdash \cdots \vdash S'_{k'},$$

the left endpoint of the sum $N + N'$ is the vector sum of the left endpoints of N and N', whereas the sides of $N + N'$ are obtained by joining all sides in the multiset $\{S_1, \ldots, S_k, S'_1, \ldots, S'_{k'}\}$, ordered by increasing slopes.

As an immediate consequence of Lemma 3.9, we get the *Theorem of the product for principal Newton polygons.*

Theorem 3.10. *Let ϕ be a key polynomial for the valuation $\nu \in \mathbb{V}$. Then, for any non-zero $g, h \in K[x]$ we have $N^{pp}_{\nu,\phi}(gh) = N^{pp}_{\nu,\phi}(g) + N^{pp}_{\nu,\phi}(h)$.* □

The analogous statement for entire Newton polygons is false.

For instance, consider $g, h \in K[x]_{\deg(\phi)}$ such that $\deg(gh) \geq \deg(\phi)$. Both polygons $N_{\nu,\phi}(g)$ and $N_{\nu,\phi}(h)$ are a single point, while $N_{\nu,\phi}(gh)$ has a side of length one.

Chapter 4

Valuations of depth zero

In this chapter, we construct *valuations of depth zero*, which are in a certain sense "very small" commensurable extensions of v to $K[x]$.

These valuations will be constructed as an augmentation of an incommensurable valuation $\mu_{-\infty}$, which is a kind of minimal extension of v to $K[x]$.

We analyze the structure of the graded algebra of the valuation $\mu_{-\infty}$ and describe its set of key polynomials.

Also, we determine the structure of the graded algebra of the depth-zero valuations. The set of key polynomials for the depth-zero valuations is determined in chapter 6, where we describe $\mathrm{KP}(\mu)$, in general, for all valuations μ of *finite depth*.

4.1 The minimal extension of v to $K[x]$

Let us fix a certain order-preserving embedding of abelian ordered groups:

$$\Gamma \hookrightarrow (\mathbb{Z} \times \Gamma)_{\mathrm{lex}}\,, \qquad \gamma \longmapsto (0, \gamma).$$

Consider the following mapping:

$$\mu_{-\infty}\colon K[x] \longrightarrow (\mathbb{Z} \times \Gamma)_{\mathrm{lex}} \cup \{\infty\}, \qquad f \longmapsto (-\deg(f), v\,(\mathrm{lc}(f)))$$

where $\mathrm{lc}(f) \in K^*$ is the leading coefficient of a non-zero polynomial f, and we agree that $\mu_{-\infty}(0) = \infty$.

Clearly, if $f = \sum_{0\le s} a_s x^s$, then

$$\mu_{-\infty}(f) = \mathrm{Min}\{\mu_{-\infty}(a_s x^s) \mid 0 \le s\} = \mathrm{Min}\{(-s, v(a_s)) \mid 0 \le s\}. \tag{4.1}$$

Lemma 4.1. *This mapping $\mu_{-\infty}$ is a valuation on $K[x]$ extending v.*

Proof. Clearly, $\mu_{-\infty|K} = v$ and $\mu_{-\infty}^{-1}(\infty) = \{0\}$.

On the other hand, if $f = \sum_{0\le s} a_s x^s$ and $g = \sum_{0\le s} b_s x^s$, (4.1) shows that

$$\begin{aligned} \mu_{-\infty}(f+g) &= \mathrm{Min}\{(-s, v_s(a_s + b_s)) \mid 0 \le s\} \\ &\ge \mathrm{Min}\{\mathrm{Min}\{(-s, v_s(a_s)), (-s, v(b_s))\} \mid 0 \le s\} \end{aligned}$$

$$= \operatorname{Min}\{\mu_{-\infty}(f), \mu_{-\infty}(g)\}.$$

Finally,

$$\mu_{-\infty}(fg) = (-\deg(fg), v(\operatorname{lc}(fg))) = \mu_{-\infty}(f) + \mu_{-\infty}(g),$$

because $\deg(fg) = \deg(f) + \deg(g)$ and $\operatorname{lc}(fg) = \operatorname{lc}(f)\operatorname{lc}(g)$. □

The value group of this valuation $\mu_{-\infty}$ is

$$\Gamma_{\mu_{-\infty}} = (\mathbb{Z} \times \Gamma)_{\text{lex}}.$$

Hence, $\mu_{-\infty}$ is an incommensurable extension of v.

The valuation ring and maximal ideal of the extension of $\mu_{-\infty}$ to $K(x)$ are

$$\mathcal{O}_{\mu_{-\infty}} = \{f/g \mid \deg(f) \le \deg(g),\ v(\operatorname{lc}(f)) \ge v(\operatorname{lc}(g))\},$$
$$\mathfrak{m}_{\mu_{-\infty}} = \{f/g \mid \deg(f) < \deg(g) \ \text{ or } \ \deg(f) = \deg(g),\ v(\operatorname{lc}(f)) > v(\operatorname{lc}(g))\}.$$

The next (trivial) observation is useful to analyze the structure of the residue class field $k_{\mu_{-\infty}}$, the graded algebra $\mathcal{G}_{\mu_{-\infty}}$, and the set $\operatorname{KP}(\mu_{-\infty})$.

Lemma 4.2. *Let $f, g \in K[x]$ be non-zero polynomials.*

(1) $f \sim_{\mu_{-\infty}} \operatorname{lc}(f)x^{\deg(f)}$.

(2) $f \sim_{\mu_{-\infty}} g \iff \deg(f) = \deg(g), \quad \operatorname{lc}(f) \sim_v \operatorname{lc}(g)$.

Corollary 4.3. *Let y be an indeterminate, to which we assign degree $(-1, 0)$.*
There is an isomorphism of graded $\mathcal{G}_v$-algebras

$$\mathcal{G}_v[y] \quad \xrightarrow{\sim} \quad \mathcal{G}_{\mu_{-\infty}}, \qquad y \longmapsto H_{\mu_{-\infty}}(x).$$

In particular, it induces an isomorphism $k \simeq \Delta_{\mu_{-\infty}} \simeq k_{\mu_{-\infty}}$ of k-algebras.

Proof. Clearly, this $\mathcal{G}_v$-homomorphism is onto and preserves degree. Also, it has a trivial kernel by Lemma 4.2.

In particular, it induces an isomorphism $k \simeq \Delta_{\mu_{-\infty}}$ between the subrings of degree zero. Finally, it is easy to deduce from item (1) of Lemma 4.2 that the canonical embedding $\Delta_{\mu_{-\infty}} \hookrightarrow k_{\mu_{-\infty}}$ is an isomorphism. In any case, this holds in general for incommensurable extensions (see Theorem 1.28). □

Corollary 4.4. *The set of key polynomials for $\mu_{-\infty}$ is*

$$\operatorname{KP}(\mu_{-\infty}) = \{x + a \mid a \in K\}.$$

All these polynomials are $\mu_{-\infty}$-equivalent.

Proof. By item (1) of Lemma 4.2, $x \mid_{\mu_{-\infty}} f$ for any non-constant polynomial f. Thus, any polynomial f with $\deg(f) > 1$ is not $\mu_{-\infty}$-irreducible.

On the other hand, x is a key polynomial for $\mu_{-\infty}$. In fact, x is $\mu_{-\infty}$-minimal by (4.1), as a consequence of Lemma 1.16. Also, x is $\mu_{-\infty}$-irreducible by Lemma 4.2.

Finally, $x + a \sim_{\mu_{-\infty}} x$ for all $a \in K$, by Lemma 4.2. Thus, Lemma 1.18 shows that all these polynomials are key polynomials for $\mu_{-\infty}$ too. □

Minimality of $\mu_{-\infty}$ among all extensions of v to $K[x]$

Our fixed embedding $\Gamma \hookrightarrow (\mathbb{Z} \times \Gamma)_{\text{lex}}$ induces an embedding

$$\mathbb{Q}\Gamma \hookrightarrow (\mathbb{Q} \times \mathbb{Q}\Gamma)_{\text{lex}}\,.$$

Hence, we may think that the valuation $\mu_{-\infty}$ and all semivaluations in $\mathbb{V}$ take values in the common group $(\mathbb{Q} \times \mathbb{Q}\Gamma)_{\text{lex}}$.

In particular, we may compare their values. We clearly have

$$\mu_{-\infty}(f) \leq \mu(f), \qquad \forall\, f \in K[x], \quad \forall\, \mu \in \mathbb{V}. \tag{4.2}$$

In a certain sense, this property characterizes $\mu_{-\infty}$.

Theorem 4.5. *Consider an arbitrary valuation η on $K[x]$*

$$\eta\colon K[x] \longrightarrow \Gamma' \cup \infty,$$

which extends v with respect to a certain fixed embedding $\iota\colon \Gamma \hookrightarrow \Gamma'$.

Then, the following conditions are equivalent.

(1) With respect to the embedding $\mathbb{Q}\Gamma \hookrightarrow \mathbb{Q}\Gamma'$ induced by ι,

$$\eta(f) \leq \mu(f), \qquad \forall\, f \in K[x], \quad \forall\, \mu \in \mathbb{V}.$$

(2) With respect to the embedding $\mathbb{Q}\Gamma \hookrightarrow \mathbb{Q}\Gamma'$ induced by ι,

$$\eta(x) < \gamma, \qquad \forall\, \gamma \in \mathbb{Q}\Gamma.$$

(3) The valuation η is equivalent to $\mu_{-\infty}$.

Proof. Suppose condition (1) is satisfied.

By Corollary 4.4, x is a key polynomial for $\mu_{-\infty}$. Since

$$\mu_{-\infty}(x) = (-1, 0) < (0, \gamma), \qquad \forall\, \gamma \in \mathbb{Q}\Gamma,$$

we may consider augmented valuations

$$\mu_\gamma = [\mu_{-\infty}; x, (0, \gamma)], \qquad \forall\, \gamma \in \mathbb{Q}\Gamma.$$

By Proposition 2.2, the value group of these valuations is:

$$\Gamma_{\mu_\gamma} = \big\langle\, \{0\} \times \Gamma, (0, \gamma) \,\big\rangle \subset \{0\} \times \mathbb{Q}\Gamma.$$

By dropping the first (null) coordinate of these values, we may think that $\Gamma_{\mu_\gamma} = \big\langle\, \Gamma, \gamma \,\big\rangle \subset \mathbb{Q}\Gamma$. After this reinterpretation of the value group, we get

$$\mu_\gamma \in \mathbb{V}, \qquad \mu_\gamma(x) = \gamma, \quad \forall\, \gamma \in \mathbb{Q}\Gamma.$$

By assumption, our valuation η satisfies:

$$\eta(x) \leq \mu_\gamma(x) = \gamma, \qquad \forall\, \gamma \in \mathbb{Q}\Gamma,$$

after identifying γ with its image $\iota(\gamma) \in \mathbb{Q}\Gamma'$.

Since we exclude from our considerations the case v trivial (see section 1.4), our group $\mathbb{Q}\Gamma$ has no minimal element, and the last inequality must be strict:

$$\eta(x) < \gamma, \qquad \forall\, \gamma \in \mathbb{Q}\Gamma.$$

This proves (2).

Assume now that condition (2) is satisfied. We deduce immediately

$$\eta(x^m) < \gamma < \eta(x^{-m}), \qquad \forall\, \gamma \in \mathbb{Q}\Gamma,\ \forall\, m \in \mathbb{Z}_{>0}. \tag{4.3}$$

This property implies:

$$f \sim_\eta \operatorname{lc}(f)\, x^{\deg(f)}, \quad \forall\, f \in K[x],\ f \neq 0. \tag{4.4}$$

In fact, any two non-zero monomials ax^m, bx^n of different degree, have different η-value, and the smallest value is that of the monomial of maximal degree:

$$n < m \implies \eta(x^{m-n}) < v(b/a) \implies \eta(ax^m) < \eta(bx^n). \tag{4.5}$$

Now, we claim that the group homomorphism

$$j\colon\ (\mathbb{Z} \times \Gamma)_{\text{lex}} \longrightarrow \Gamma_\eta, \qquad (m, \alpha) \longmapsto \alpha - \eta(x^m),$$

is an order-preserving isomorphism.

In fact, (4.4) shows that j is onto. Also, $(m, \alpha) \in \operatorname{Ker}(j)$ implies

$$\eta(x^m) = \alpha \implies m = 0 \implies \alpha = 0,$$

in order not to contradict (4.3). Thus j is a group isomorphism.

Finally, j preserves the ordering:

$$(n, v(a)) \leq (m, v(b)) \implies j(n, v(a)) = \eta(ax^{-n}) \leq \eta(bx^{-m}) = j(m, v(a)).$$

If $n < m$, this inequality follows from (4.5). And for $n = m$ it is obvious, because $\eta(a) = v(a)$ and $\eta(b) = v(b)$.

This ends the proof of the claim.

Finally, η and $\mu_{-\infty}$ are equivalent valuations because the following diagram commutes:

$$\begin{array}{ccc} (\mathbb{Z} \times \Gamma)_{\text{lex}} & \xrightarrow[\sim]{j} & \Gamma_\eta \\ & {\scriptstyle \mu_{-\infty}}\nwarrow \quad \nearrow {\scriptstyle \eta} & \\ & K(x)^* & \end{array} \tag{4.6}$$

In fact, for any non-zero polynomial $f \in K[x]$, we have

$$\mu_{-\infty}(f) = \left(-\deg(f), v\left(\operatorname{lc}(f)\right)\right), \qquad \eta(f) = \eta\left(\operatorname{lc}(f)\, x^{\deg(f)}\right),$$

the last equality by (4.4). Thus, $j \circ \mu_{-\infty} = \eta$. This proves (3).

Finally, suppose that η and $\mu_{-\infty}$ are equivalent. That is, there exists an order-preserving isomorphism j such that diagram (4.6) commutes.

Since $\eta_{|K} = v = \mu_{-\infty|K}$, the isomorphism $j \otimes \mathbb{Q}$ maps the subgroup $\{0\} \times \mathbb{Q}\Gamma$ into $\iota(\mathbb{Q}\Gamma)$. Hence, by applying j to the inequalities in (4.2), we obtain the inequalities in item (1). □

Unicity of $\mu_{-\infty}$ under field extension

Let L/K be a field extension and let w be a valuation on L extending v.

We may consider an analogous minimal valuation on $L[x]$:

$$\mu_{-\infty,L}\colon L[x] \longrightarrow (\mathbb{Z}\times\Gamma)_{\text{lex}}\cup\{\infty\}, \qquad f\longmapsto(-\deg(f), w(\operatorname{lc}(f)))$$

Clearly, the restriction of $\mu_{-\infty,L}$ to $K[x]$ is $\mu_{-\infty}$.

Corollary 4.6. *Any valuation ρ on $L[x]$ extending $\mu_{-\infty}$ is equivalent to $\mu_{-\infty,L}$.*

Proof. If $\rho_{|K[x]}=\mu_{-\infty}$, then clearly $\rho(x)<\gamma$ for all $\gamma\in\mathbb{Q}\Gamma$.
The result follows from Theorem 4.5. □

4.2 Valuations of depth 0

Definition 4.7. *A valuation μ on $K[x]$ is said to have* depth zero *if it satisfies*

- *It is commensurable over v.*
- *It is equivalent to a valuation which can be obtained as an augmentation of $\mu_{-\infty}$.*

By Corollary 4.4, a key polynomial for $\mu_{-\infty}$ is of the form $x+a$ for an arbitrary $a\in K$. In order to build an augmentation of $\mu_{-\infty}$ which is commensurable over v, we must take any $\gamma\in\mathbb{Q}\Gamma$ and consider $(0,\gamma)$ as the augmented value of $x+a$. Let us denote the corresponding augmentation by

$$\mu_0(x+a,\gamma) := [\mu_{-\infty};\, x+a,\, (0,\gamma)].$$

Lemma 2.3 shows under what conditions two of these augmentations coincide:

$$\mu_0(x+a,\gamma)=\mu_0(x+b,\gamma_*) \iff v(a-b)\geq\gamma=\gamma_*.$$

By Propositon 2.2, the value group of these valuations is:

$$\Gamma_{\mu_0(x+a,\gamma)} = \big\langle\, \{0\}\times\Gamma,\, (0,\gamma)\,\big\rangle.$$

By dropping the first (null) coordinate, we obtain equivalent valuations with values in $\mathbb{Q}\Gamma$. We denote these valuations in $\mathbb{V}$ with the same symbol:

$$\mu_0(x+a,\gamma)\colon K[x] \longrightarrow \mathbb{Q}\Gamma\cup\{0\}.$$

By definition, they act as follows on non-zero polynomials:

$$\mu_0(x+a,\gamma)\colon \sum_{0\leq s} a_s(x+a)^s \longmapsto \operatorname{Min}\{v(a_s)+s\gamma \mid 0\leq s\},$$

and the value group is $\Gamma_{\mu_0(x+a,\gamma)}=\big\langle\,\Gamma,\,\gamma\,\big\rangle$.

Remark. *In particular, Gauss' valuation has depth zero:* $\mu_{\text{Gauss}}=\mu_0(x,0)$.

Our aim is to determine the structure of the residue class field and the graded algebra of these valuations of depth zero.

From now on, we fix one of these valuations and we denote it simply by:

$$\mu_0 := \mu_0(x+a, \gamma).$$

Notation.

- $\phi_0 = x + a$
- $e \in \mathbb{Z}_{>0}$ minimal positive integer such that $e\gamma \in \Gamma$
- $h = e\gamma \in \Gamma$
- $\pi^h \in K^*$ choice of an element such that $v\left(\pi^h\right) = h$
- $Y_0 = \phi_0^e/\pi^h \in K[x]$ has $\mu_0(Y_0) = 0$
- $p^h = H_{\mu_0}(\pi^h) \in \mathcal{G}_{\mu_0}^*$ has degree h.
- $x_0 = H_{\mu_0}(\phi_0) \in \mathcal{G}_{\mu_0}$ has degree γ.
- $y_0 = H_{\mu_0}(Y_0) = x_0^e\, p_0^{-h} \in \Delta \subset \mathcal{G}_{\mu_0}$

Remarks.

(1) Note that for any $m \in \mathbb{Z}$, we have $m\gamma \in \Gamma$ if and only if $e \mid m$.

(2) The elements $\pi^h \in K^*$, $p^h \in \mathcal{G}_{\mu_0}^*$ are not h-th powers. Since h may not be an integer, this would make no sense.

In section 5.2 we shall give a better motivation for the use of this notation.

Since ϕ_0 is a key polynomial for μ_0 of minimal degree (one), Proposition 1.25 shows that $\kappa \simeq k_{\phi_0}$ has dimension one as a k-vector space. Thus, $k = \kappa$ is algebraically closed inside Δ.

Since x_0 is a prime element in $\mathcal{G}_{\mu_0}$, the element $y_0 = p^{-h}\, x_0^e$ is associate to a power of x_0, because p^h is a unit. In particular, $y_0 \notin k$, because in k all non-zero elements are units. Thus, $y_0 \in \Delta \setminus k$ is transcendental over k.

By Theorem 1.28 and the remarks following it, we have

$$\Delta = k[y_0].$$

Also, the residue class field k_{μ_0} is isomorphic to the field of fractions of Δ, and the class of $Y_0 \in \mathcal{O}_{\mu_0}$ modulo the maximal ideal is a Hauptmodul of the extension k_{μ_0}/k.

Theorem 4.8. *The graded algebra $\mathcal{G}_{\mu_0}$ may be described as follows as a $\mathcal{G}_v$-algebra:*

$$\mathcal{G}_{\mu_0} = \mathcal{G}_v[x_0] = \mathcal{G}_v[y_0, x_0],$$

where $y_0 \in \Delta$ is transcendental over $\mathcal{G}_v$, and x_0 (of degree γ) is algebraic over $\mathcal{G}_v[y_0]$ with minimal equation $x_0^e = p^h\, y_0$.

Proof. All non-zero polynomials $f \in K[x]$ admit a ϕ_0-expansion with coefficients in K. Therefore, $\mathcal{G}_{\mu_0} = \mathcal{G}_v[x_0]$, because all homogeneous elements $H_{\mu_0}(f)$ belong to $\mathcal{G}_v[x_0]$. In particular, $\mathcal{G}_{\mu_0} = \mathcal{G}_v[x_0] = \mathcal{G}_v[y_0, x_0]$.

Imagine a minimal homogeneous algebraic equation of y_0 over $\mathcal{G}_v$. Since y_0 has degree zero, all coefficients of the equation have degree zero. Thus, they all belong to k (identified to Δ_v). Hence, there is no such algebraic equation because y_0 is transcendental over k.

Let us check the minimality of the algebraic equation of x_0 over $\mathcal{G}_v[y_0]$. Suppose we have a homogeneous relation

$$\sum_{m\in\mathbb{N}} \zeta_m\, x_0^m = 0, \qquad \zeta_m \in \mathcal{G}_v[y_0].$$

By applying the identity $x_0^e = p^h\, y_0$, we may assume that $0 \le m < e$.

Then, this sum cannot have two different monomials:

$$\deg(\zeta_m\, x_0^m) = \deg(\zeta_n\, x_0^n) \implies (m-n)\gamma = \deg(\zeta_n) - \deg(\zeta_m) \in \Gamma,$$

and this implies $m \equiv n \pmod{e}$, leading to $m = n$ by our assumption on the exponents. Therefore, our relation takes the form $\zeta x_0^m = 0$. Since $\mathcal{G}_{\mu_0}$ is an integral domain, we have necessarily $\zeta = 0$. □

Chapter 5

Inductive valuations

A valuation μ on $K[x]$ is said to be *inductive* if it is attained after a finite number of augmentation steps starting with the minimal valuation $\mu_{-\infty}$:

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu, \tag{5.1}$$

with values $\gamma_0, \ldots, \gamma_r \in \mathbb{Q}\Gamma$, and intermediate valuations

$$\mu_0 = \mu_0(\phi_0, \gamma_0), \qquad \mu_i = [\mu_{i-1}; \phi_i, \gamma_i], \quad 1 \leq i \leq r.$$

The non-negative integer $r \geq 0$ is the *length* of the chain (5.1).

Note that μ_0 is an inductive valuation because it is the last valuation of a chain of augmentations of length $r = 0$.

However, we do not want to consider $\mu_{-\infty}$ as an inductive valuation, because it is incommensurable over v.

Since the value group of an inductive valuation is a subgroup of $\mathbb{Q}\Gamma$, all inductive valuations belong to our space $\mathbb{V}$. Let us denote by

$$\mathbb{V}^{\mathrm{ind}} := \mathbb{V}^{\mathrm{ind}}(K, v) \subset \mathbb{V}$$

the subset of all inductive valuations.

By Proposition 2.2, the family of all intermediate inductive valuations in a chain like (5.1) is totally ordered in $\mathbb{V}$:

$$\mu_0 < \mu_1 < \cdots < \mu_r = \mu,$$

and every polynomial ϕ_i is a key polynomial for μ_i of minimal degree.

Since every ϕ_{i+1} is μ_i-minimal, item (2) of Proposition 1.26 shows that

$$1 = \deg(\phi_0) \mid \deg(\phi_1) \mid \cdots \mid \deg(\phi_{r-1}) \mid \deg(\phi_r).$$

Also, Theorem 1.27 shows that,

$$C(\mu_i) = \frac{\mu_i(\phi_{i+1})}{\deg(\phi_{i+1})} = \frac{\mu_i(\phi_i)}{\deg(\phi_i)} > \frac{\mu_{i-1}(\phi_i)}{\deg(\phi_i)} = C(\mu_{i-1}). \tag{5.2}$$

Therefore, the constants $C(\mu_i) \in \mathbb{Q}\Gamma$ grow strictly:

$$\gamma_0 = C(\mu_0) < C(\mu_1) < \cdots < C(\mu_r) = C(\mu).$$

Since $C(\mu_i) = \gamma_i/\deg(\phi_i)$, the sequence $\gamma_0 < \cdots < \gamma_r$ grows strictly too.

Nevertheless, as mentioned in section 2, the value groups $\Gamma_{\mu_0}, \ldots, \Gamma_{\mu_r}$ of a sequence of augmentations do not always form a chain.

In the next section, we shall impose a technical condition on chains like (5.1), to ensure that these value groups form a chain.

Before of that, let us mention a property which is valid for arbitrary chains of augmentations.

Lemma 5.1. *For a chain of augmented valuations as in* (5.1)*, consider $f \in K[x]$ such that $\phi_i \nmid_{\mu_{i-1}} f$ for some $1 \leq i \leq r$. Then, $\mu_{i-1}(f) = \mu_i(f) = \cdots = \mu_r(f)$.*

Proof. By Proposition 2.2, $\mu_{i-1}(f) = \mu_i(f)$. By Lemma 2.5, $H_{\mu_i}(f)$ is a unit, so that it is not divisible by the prime element $H_{\mu_i}(\phi_{i+1}) \in \mathcal{G}_{\mu_i}$.

Thus, $\phi_{i+1} \nmid_{\mu_i} f$ and the argument may be iterated. □

5.1 MacLane chains of valuations

Lemma 5.2. *For a chain of augmented valuations as in (5.1), the following conditions are equivalent:*

(1) $\phi_{i+1} \nmid_{\mu_i} \phi_i$ *for all* $0 \leq i < r$.

(2) $\phi_{i+1} \not\sim_{\mu_i} \phi_i$ *for all* $0 \leq i < r$.

Moreover, these conditions are satisfied if

(3) $1 = \deg(\phi_0) < \deg(\phi_1) < \cdots < \deg(\phi_r)$.

Proof. By the μ_i-minimality of ϕ_{i+1}, the condition $\phi_{i+1} \mid_{\mu_i} \phi_i$ implies $\deg(\phi_i) = \deg(\phi_{i+1})$. And this leads to $\phi_{i+1} \sim_{\mu_i} \phi_i$ by Lemma 1.18.

Hence, any of the conditions (2) or (3) implies (1). Obviously, (1) implies (2). □

Definition 5.3. *A chain of augmented valuations as in (5.1) is called a* MacLane chain *if it satisfies condition (1) of Lemma 5.2.*

If it satisfies (3), we say that it is an optimal MacLane chain.

As an immediate application of Lemma 5.1, in a MacLane chain like (5.1) one has:

$$\mu(\phi_i) = \mu_i(\phi_i) = \gamma_i, \qquad 0 \leq i \leq r. \tag{5.3}$$

Also, for any $0 \leq i \leq r$, the truncation of a MacLane at the i-th node

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{i-1},\gamma_{i-1}}{\longrightarrow} \mu_{i-1} \overset{\phi_i,\gamma_i}{\longrightarrow} \mu_i,$$

is a MacLane chain of the intermediate valuation μ_i.

The purpose of using MacLane chains is clarified by the next two results, which are an immediate consequence of Lemma 2.7.

Lemma 5.4. *In a MacLane chain as in* (5.1)*, the value groups of the valuations are*

$$\Gamma_{\mu_0} = \big\langle\, \Gamma, \gamma_0 \,\big\rangle, \qquad \Gamma_{\mu_i} = \big\langle\, \Gamma_{\mu_{i-1}}, \gamma_i \,\big\rangle, \quad 1 \le i \le r,$$

In particular, $\Gamma \subset \Gamma_{\mu_0} \subset \cdots \subset \Gamma_{\mu_r} = \Gamma_\mu$.

Lemma 5.5. *In a MacLane chain as in* (5.1)*, the value groups of the semivaluations* v_{ϕ_i} *are* $\Gamma_{v_{\phi_0}} = \Gamma$*, and* $\Gamma_{v_{\phi_i}} = \Gamma_{\mu_{i-1}}$ *for* $1 \le i \le r$.

On the other hand, the imposition of the technical conditions of Lemma 5.2 does not restrict the set of valuations admitting chains like (5.1).

More precisely, as the next result shows, *every inductive valuation admits an optimal MacLane chain.*

Lemma 5.6. *Consider a chain of two augmented valuations*

$$\mu \ \xrightarrow{\phi,\gamma}\ \mu' \ \xrightarrow{\phi_*,\gamma_*}\ \mu_*$$

with $\deg(\phi_*) = \deg(\phi)$*. Then,* ϕ_* *is a key polynomial for* μ*, and* $\mu_* = [\mu; \phi_*, \gamma_*]$.

Proof. By Lemma 2.4, $\phi_* \sim_\mu \phi$. Thus, Lemma 1.18 shows that ϕ_* is a key polynomial for μ.

By the very definition of augmentations, $\mu_* = [\mu'; \phi_*, \gamma_*]$ and $\mu'' := [\mu; \phi_*, \gamma_*]$ coincide, since both coincide with μ on polynomials of degree less than $\deg(\phi)$. □

In particular, the length of a MacLane chain joining an inductive valuation μ with $\mu_{-\infty}$ is not an intrinsic invariant of μ.

However, there is a strong unicity statement if we consider only *optimal* MacLane chains.

Proposition 5.7. *Consider an optimal MacLane chain as in* (5.1) *and any other optimal MacLane chain*

$$\mu_{-\infty} = \mu^*_{-\infty} \ \xrightarrow{\phi_0^*,\gamma_0^*}\ \mu_0^* \ \xrightarrow{\phi_1^*,\gamma_1^*}\ \cdots \ \longrightarrow\ \mu_{t-1}^* \ \xrightarrow{\phi_t^*,\gamma_t^*}\ \mu_t^* = \mu^*.$$

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

$$\deg(\phi_i) = \deg(\phi_i^*), \quad \mu_{i-1}(\phi_i - \phi_i^*) \ge \gamma_i = \gamma_i^* \ \text{ for all } \ 0 \le i \le r.$$

In this case, we also have $\mu_i = \mu_i^*$ *and* $\phi_i \sim_{\mu_{i-1}} \phi_i^*$ *for all* $0 \le i \le r$.

Proof. The sufficiency of the conditions is a consequence of Lemma 2.3.

Conversely, suppose $\mu = \mu^*$ and, for instance, $r \le t$.

Let us prove the following implication for all $0 \le i \le r$:

$$\mu_{i-1} = \mu^*_{i-1} \implies \deg(\phi_i) = \deg(\phi_i^*), \ \ \mu_{i-1}(\phi_i - \phi_i^*) \ge \gamma_i = \gamma_i^*.$$

In fact, suppose $\mu = \mu^*$ and $\mu_{i-1} = \mu^*_{i-1}$. Since $\mu_{i-1} < \mu_i < \mu$, Proposition 2.2 and Lemma 5.1 show that

$$\mu_{i-1}(f) = \mu_i(f) \iff \phi_i \nmid_{\mu_{i-1}} f \iff \mu_{i-1}(f) = \mu(f),$$

for any non-zero polynomial $f \in K[x]$. This implies

$$\deg(\phi_i) = \mathrm{Min}\{\deg(f) \mid f \in K[x],\ \mu_{i-1}(f) < \mu(f)\} = \deg(\phi_i^*).$$

The optimality of both chains and the minimality of the key polynomials imply $\phi_{i+1} \nmid_{\mu_i} \phi_i^*$ and $\phi_{i+1}^* \nmid_{\mu_i^*} \phi_i$. By Lemma 5.1 and equation (5.3),

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

Write $\phi_i^* = \phi_i + a_i$, with $a_i \in K[x]_{\deg(\phi_i)}$. By the very definition of the augmented valuations μ_i, μ_i^* acting on ϕ_i-expansions and ϕ_i^*-expansions, respectively, we get

$$\gamma_i = \mu_i^*(\phi_i) \leq \gamma_i^* = \mu_i(\phi_i^*) \leq \gamma_i.$$

This proves $\gamma_i = \gamma_i^*$. Also, since $\phi_i \nmid_{\mu_{i-1}} a_i$, Lemma 5.1 shows that

$$\mu_{i-1}(a_i) = \mu(a_i) \geq \mathrm{Min}\{\mu(\phi_i), \mu(\phi_i^*\} = \gamma_i.$$

Lemma 2.3 asserts then $\mu_i = \mu_i^*$ and $\phi_i \sim_{\mu_{i-1}} \phi_i^*$. This leads by a recursive argument to $\mu = \mu_r = \mu_r^*$. Finally, the inequality $r < t$ would imply $\mu < \mu^*$, against our assumption. Thus, $r = t$. □

Therefore, in any optimal MacLane chain of an inductive valuation μ as in (5.1), the intermediate valuations $\mu_0, \ldots, \mu_{r-1}$, the values $\gamma_0, \ldots, \gamma_r \in \mathbb{Q}\Gamma$ and the positive integers $\deg(\phi_0), \ldots, \deg(\phi_r)$, are intrinsic data of μ, whereas the key polynomials $\phi_0, \ldots, \phi_r$ admit different choices.

Definition 5.8. *The* depth *of an inductive valuation μ is the length r of any optimal MacLane chain of μ.*

Accordingly, inductive valuations are called finite-depth *valuations too.*

5.2 Discrete data associated with a MacLane chain

Let us fix an inductive valuation μ equipped with a MacLane chain of length r as in (5.1). We associate with this chain several data and operators.

Througouht this section, the index i takes any integer value $0 \leq i \leq r$, and we agree that:

$$\mu_{-1} := v, \qquad \Gamma_{\mu_{-1}} = \Gamma_v = \Gamma, \qquad \mu_{-1}(\phi_0) := 0_\Gamma =: C(\mu_{-1}).$$

Newton polygon operators

We consider Newton polygon operators

$$N_i := N_{\mu_{i-1},\phi_i} \colon\ K[x] \longrightarrow \mathcal{P}\left(\mathbb{Q} \times \mathbb{Q}\Gamma\right).$$

See chapter 2 for the definition of N_{μ_{i-1},ϕ_i}.

Note that the operator $N_0 = N_{v,\phi_0}$ coincides with the operator $N_{\mu_{-\infty},\phi_0}$. In fact, the coefficients of the ϕ_0-expansion of any non-zero $f \in K[x]$ are elements in K, and the valuations v and $\mu_{-\infty}$ coincide over K.

Chain of value groups

Recall the results of Lemma 2.7:

$$\Gamma_{\mu_i} = \left\langle \Gamma_{\mu_{i-1}}, \gamma_i \right\rangle, \qquad v\left(K_{\phi_i}^*\right) = \Gamma_{\mu_{i-1}}.$$

All indices in the chain of groups, $\Gamma \subset \Gamma_{\mu_0} \subset \cdots \subset \Gamma_{\mu_r} = \Gamma_\mu$ are finite.
Actually, every quotient $\Gamma_{\mu_i}/\Gamma_{\mu_{i-1}}$ is a finite cyclic group. Let us denote

$$e_i = \left(\Gamma_{\mu_i} \colon \Gamma_{\mu_{i-1}}\right), \qquad e_i\mathbb{Z} = \left\{e \in \mathbb{Z} \mid e\gamma_i \in \Gamma_{\mu_{i-1}}\right\}. \tag{5.4}$$

The identification $\Gamma_{\mu_{i-1}} = v\left(K_{\phi_i}^*\right)$ allows a computation of the ramification index of the extension K_{ϕ_i}/K in terms of these data:

$$e(\phi_i) = \left(\Gamma_{\mu_{i-1}} \colon \Gamma\right) = e_0 \cdots e_{i-1}. \tag{5.5}$$

Numerical data

We define

$$\begin{aligned} m_i &= \deg(\phi_i) \in \mathbb{Z}_{>0}, \\ \lambda_i &= \gamma_i - \mu_{i-1}(\phi_i) \in \mathbb{Q}\Gamma, \\ C(\mu_i) &= \mu_i(\phi_i)/\deg(\phi_i) = \gamma_i/m_i \in \mathbb{Q}\Gamma, \\ h_i &= e_i\gamma_i \in \Gamma_{\mu_{i-1}}. \end{aligned}$$

According to our initial assumptions, $\lambda_0 = \gamma_0$ is an arbitrary element in $\mathbb{Q}\Gamma$, while λ_i is a *positive* element in $\mathbb{Q}\Gamma$ for $i > 0$.

By (5.2), we have recursive formulas

$$C(\mu_i) = C(\mu_{i-1}) + \frac{\lambda_i}{m_i}, \qquad \gamma_i = \frac{m_i}{m_{i-1}}\,\gamma_{i-1} + \lambda_i.$$

The following explicit formulas follow:

$$\mu_{i-1}(\phi_i) = \frac{m_i}{m_{i-1}}\,\gamma_{i-1}, \qquad C(\mu_i) = \frac{\lambda_0}{m_0} + \cdots + \frac{\lambda_i}{m_i}. \tag{5.6}$$

If the MacLane chain is optimal, Proposition 5.7 shows that these data are intrinsic invariants of μ. In this case, we refer to them as

$$\gamma_i(\mu), \quad m_i(\mu), \quad e_i(\mu), \quad \lambda_i(\mu), \quad h_i(\mu),$$

respectively.

Chain of finitely-generated value subgroups

If the ordered group Γ_{μ_i} is not finitely-generated, the group homomorphism

$$K(x)^* \xrightarrow{\mu_i} \Gamma_{\mu_i}$$

does not admit a section.

Any finitely-generated subgroup $\Gamma_i \subset \Gamma_{\mu_i}$ is free as a $\mathbb{Z}$-module. Hence, it admits a group homomorphism

$$\pi_i \colon \Gamma_i \longrightarrow K(x)^*, \qquad \alpha \longmapsto \pi_i^\alpha$$

such that $\mu_i \circ \pi_i = \mathrm{id}_{\Gamma_i}$. In other words, the choice of Γ_i would allow the choice of elements $\pi_i^\alpha \in K(x)^*$ satisfying

$$\mu_i(\pi_i^\alpha) = \alpha, \qquad \pi_i^{\alpha+\beta} = \pi_i^\alpha \pi_i^\beta, \quad \forall\, \alpha, \beta \in \Gamma_i. \tag{5.7}$$

We proceed to choose finitely-generated subgroups $\Gamma_i \subset \Gamma_{\mu_i}$ satisfying some natural conditions.

Since $\Gamma_{\mu_i} = \Gamma + \left\langle \gamma_0, \dots, \gamma_i \right\rangle$, there exist $\alpha_i \in \Gamma$ such that

$$h_i \in \alpha_i + \left\langle \gamma_0, \dots, \gamma_{i-1} \right\rangle.$$

Definition 5.9. *We fix a finitely-generated subgroup $\Gamma_{-1} := \Gamma^{\mathrm{fg}} \subset \Gamma$ containing $\alpha_0, \dots, \alpha_r$. This choice determines finitely-generated subgroups*

$$\Gamma_i := \Gamma_{\mu_i}^{\mathrm{fg}} := \left\langle \Gamma_{i-1}, \gamma_i \right\rangle = \left\langle \Gamma_{-1}, \gamma_0, \dots, \gamma_i \right\rangle \subset \Gamma_{\mu_i}.$$

By construction, $h_i = e_i \gamma_i \in \Gamma_{i-1}$ for all i. Since,

$$\Gamma_{\mu_i} = \left\langle \Gamma_{\mu_{i-1}}, \gamma_i \right\rangle, \qquad \Gamma_i = \left\langle \Gamma_{i-1}, \gamma_i \right\rangle,$$

the next result follows immediately.

Lemma 5.10. *These finitely-generated subgroups satisfy*

$$\Gamma_i \cap \Gamma_{\mu_{i-1}} = \Gamma_{i-1}, \qquad \forall\, 0 \le i \le r.$$

In particular, they form a chain

$$\Gamma^{\mathrm{fg}} = \Gamma_{-1} \subset \Gamma_0 \subset \cdots \subset \Gamma_{r-1} \subset \Gamma_r = \Gamma_\mu^{\mathrm{fg}},$$

with cyclic quotients of consecutive terms. More precisely, $(\Gamma_i \colon \Gamma_{i-1}) = e_i$.

Residual polynomial operators

Definition 5.11. *We say that $g \in K[x]$* has attainable μ-value *if $\mu(g) \in \Gamma_\mu^{\mathrm{fg}}$.*

Denote by $K[x]_{\mu\text{-at}} \subset K[x]$ the subset of polynomials having attainable μ-values.

Lemma 5.12. *Let $g \in K[x]$ be a non-zero polynomial.*

(1) There is a constant $a \in K^*$ such that ag has attainable μ-value.

(2) If g is monic and μ-minimal, then it has attainable μ-value.

In particular, all key polynomials for μ have attainable μ-values.

Proof. The first item follows from $\Gamma_\mu = \Gamma + \left\langle \gamma_0, \dots, \gamma_r \right\rangle = \Gamma + \Gamma_\mu^{\mathrm{fg}}$.

If g is monic and μ-minimal, then Proposition 1.26 shows that $\deg(g) = \ell m_r$ and $\mu(g) = \ell\mu(\phi_r) = \ell\gamma_r \in \Gamma_\mu^{\mathrm{fg}}$. □

The choice of the subgroup Γ^{fg} is relevant for the definition of residual polynomial operators

$$R_i := R_{\mu_i,\phi_i} \colon K[x]_{\mu_i\text{-at}} \longrightarrow k_i[y],$$

where k_i is a certain finite extension of k.

We postpone to the next chapter the definition of these operators.

The subgroup Γ^{fg} is not universally fixed. It will be assumed that Γ^{fg} is sufficiently large to include the values of any finite family of polynomials involved in any particular argument or statement where we apply the operators R_i.

Bases of the finitely-generated value subgroups

Let us choose a basis of Γ^{fg} as a $\mathbb{Z}$-module:

$$\Gamma^{\mathrm{fg}} = \Gamma_{-1} = \iota_{0,1}\,\mathbb{Z} \oplus \cdots \oplus \iota_{0,k}\,\mathbb{Z}.$$

From this basis, we shall derive specific bases for the other groups:

$$\Gamma_i = \iota_{i+1,1}\,\mathbb{Z} \oplus \cdots \oplus \iota_{i+1,k}\,\mathbb{Z}.$$

These bases are constructed by a recurrent procedure. To this end, let us write:

$$\gamma_i = \frac{h_{i,1}}{e_{i,1}}\,\iota_{i,1} + \cdots + \frac{h_{i,k}}{e_{i,k}}\,\iota_{i,k} \in \mathbb{Q}\Gamma_{\mu_{i-1}},$$

with $h_{i,j}$, $e_{i,j}$ coprime integers with $e_{i,j} > 0$, for all $1 \le j \le k$. Clearly,

$$e_i = \operatorname{lcm}(e_{i,1}, \dots, e_{i,k}). \tag{5.8}$$

Let us introduce some more numerical data associated with these numerators $h_{i,j}$ and denominators $e_{i,j}$.

Notation. Denote $e'_{i,1} = d_{i,1} = 1$, and:

$$\begin{aligned} &e'_{i,j} = e_{i,1}\cdots e_{i,j-1}/d_{i,1}\cdots d_{i,j-1}, && d_{i,j} = \gcd\left(e_{i,j}, e'_{i,j}\right), \quad 1 < j \le k,\\ &e'_{i,k+1} = e_{i,1}\cdots e_{i,k}/d_{i,1}\cdots d_{i,k}. \end{aligned}$$

Lemma 5.13. $e'_{i,k+1} = \operatorname{lcm}(e_{i,1}, \dots, e_{i,k}) = e_i$.

Proof. For $k = 1$ the statement is trivial, and for $k = 2$ it is well known.

Take $k > 1$ and assume that the statement holds for families of less than k integers. Then, $e'_{i,k} = \operatorname{lcm}(e_{i,1}, \dots, e_{i,k-1})$. Hence,

$$\operatorname{lcm}(e_{i,1}, \dots, e_{i,k}) = \operatorname{lcm}(e'_{i,k}, e_{i,k}) = e'_{i,k} e_{i,k}/d_{i,k} = e'_{i,k+1}.$$

The identity $\operatorname{lcm}(e_{i,1}, \dots, e_{i,k}) = e_i$ was mentioned in (5.8). □

Since $\gcd\left(h_{i,j}e'_{i,j}, e_{i,j}\right) = d_{i,j}$, we have Bézout identities:

$$\ell_{i,j} h_{i,j} e'_{i,j} + \ell'_{i,j} e_{i,j} = d_{i,j}, \quad 0 \le \ell_{i,j} < \frac{e_{i,j}}{d_{i,j}}, \quad 1 \le j \le k, \tag{5.9}$$

for uniquely determined integers $\ell_{i,j}$, $\ell'_{i,j}$.

Definition 5.14. *Consider the following lower triangular matrix $Q = (q_{m,j}) \in \mathbb{Q}^{k\times k}$:*

$$Q = \begin{pmatrix} d_{i,1}/e_{i,1} & & & \\ & d_{i,2}/e_{i,2} & & 0 \\ q_{m,j} & & \ddots & \\ & & & d_{i,k}/e_{i,k} \end{pmatrix},$$

with $q_{m,j} = \ell_{i,j} e'_{i,j} h_{i,m}/e_{i,m}$, for $m > j$. Then, we define

$$(\iota_{i+1,1} \cdots \iota_{i+1,k}) := (\iota_{i,1} \cdots \iota_{i,k})\, Q. \tag{5.10}$$

Lemma 5.15. *The family $\iota_{i+1,1}, \dots, \iota_{i+1,k}$ is a basis of Γ_i.*

Proof. Let Λ be the $\mathbb{Z}$-module generated by $\iota_{i,1}/e_{i,1}, \dots, \iota_{i,k}/e_{i,k}$. Consider the chain of $\mathbb{Z}$-modules:

$$\Gamma_{i-1} \subset \Gamma_i \subset \Lambda.$$

By Lemma 5.13, we have

$$(\Lambda \colon \Gamma_i) = (\Lambda \colon \Gamma_{i-1}) \,/\, (\Gamma_i \colon \Gamma_{i-1}) = e_{i,1} \cdots e_{i,k}/e_i = d_{i,1} \cdots d_{i,k}.$$

On the other hand, let Γ' be the $\mathbb{Z}$-module generated by $\iota_{i+1,1}, \dots, \iota_{i+1,k}$, as defined in (5.10). Let us show that $\Gamma' \subset \Gamma_i$.

In fact, for every $1 \le j \le k$,

$$\begin{aligned} \iota_{i+1,j} &= \frac{d_{i,j}}{e_{i,j}}\,\iota_{i,j} + \ell_{i,j} e'_{i,j} \left(\frac{h_{i,j+1}}{e_{i,j+1}}\,\iota_{i,j+1} + \cdots + \frac{h_{i,k}}{e_{i,k}}\,\iota_{i,k} \right) \\ &= \ell'_{i,j}\iota_{i,j} + \ell_{i,j} e'_{i,j} \left(\frac{h_{i,j}}{e_{i,j}}\,\iota_{i,j} + \frac{h_{i,j+1}}{e_{i,j+1}}\,\iota_{i,j+1} + \cdots + \frac{h_{i,k}}{e_{i,k}}\,\iota_{i,k} \right) \\ &= \ell'_{i,j}\iota_{i,j} + \ell_{i,j} e'_{i,j} \left(\gamma_i - \frac{h_{i,1}}{e_{i,1}}\,\iota_{i,1} - \cdots - \frac{h_{i,j-1}}{e_{i,j-1}}\,\iota_{i,j-1} \right), \end{aligned} \tag{5.11}$$

by using the Bézout identities (5.9).

Now, for any index $1 \le t < j$, the quotient $e'_{i,j}/e_{i,t}$ is an integer:

$$\frac{e'_{i,j}}{e_{i,t}} = \frac{e'_{i,t}}{d_{i,t}} \frac{e_{i,t+1}}{d_{i,t+1}} \cdots \frac{e_{i,j-1}}{d_{i,j-1}} \in \mathbb{Z}. \tag{5.12}$$

Hence, $\iota_{i+1,j}$ belongs to Γ_i, because we expressed it as a linear combination of the elements $\iota_{i,1}, \dots, \iota_{i,j}, \gamma_i \in \Gamma_i$, with integer coefficients.

Thus, we may consider the chain of $\mathbb{Z}$-modules:

$$\Gamma' \subset \Gamma_i \subset \Lambda.$$

The lower triangular matrix $P = \operatorname{diag}(e_{i,1}, \dots, e_{i,k})Q$ has integer coefficients and $\det(P) = d_{i,1} \cdots d_{i,k}$. We may rewrite (5.10) as:

$$(\iota_{i+1,1} \ \cdots \ \iota_{i+1,k}) = \left(\frac{1}{e_{i,1}} \iota_{i,1} \ \cdots \ \frac{1}{e_{i,k}} \iota_{i,k} \right) P.$$

Hence, $(\Lambda \colon \Gamma') = \det(P) = d_{i,1} \cdots d_{i,k} = (\Lambda \colon \Gamma_i)$. This proves $\Gamma' = \Gamma_i$. □

Chain of homomorphisms between the graded algebras

Some more data are derived from the chain of homomorphisms:

$$\mathcal{G}_{\mu_0} \longrightarrow \mathcal{G}_{\mu_1} \longrightarrow \quad \cdots \quad \longrightarrow \mathcal{G}_{\mu_{r-1}} \longrightarrow \mathcal{G}_{\mu}.$$

Denote $\Delta_i = \Delta_{\mu_i}$ for $0 \leq i \leq r$. By Lemma 2.6, we may consider a sequence of fields

$$k_0 = \operatorname{Im}(k \to \Delta_0), \qquad k_i = \operatorname{Im}(\Delta_{i-1} \to \Delta_i), \quad 1 \leq i \leq r,$$

where k_i is isomorphic to the residue class field k_{ϕ_i} of the extension K_{ϕ_i}/K determined by ϕ_i. In particular, k_i is a finite extension of k.

Moreover, $k_i^* = \Delta_i^*$, so that these fields capture all units of the rings Δ_i.

We abuse of language and identify k with k_0 and each field $k_i \subset \Delta_i$ with its image under the canonical map $\Delta_i \to \Delta_j$ for $j \geq i$. In other words, we consider as inclusions the canonical embeddings:

$$k = k_0 \subset k_1 \subset \cdots \subset k_r. \tag{5.13}$$

Let us denote

$$f_{i-1} = [k_i \colon k_{i-1}], \qquad 1 \leq i \leq r.$$

Thus, the residual degree of the extension K_{ϕ_i}/K can be computed as:

$$f(\phi_i) = [k_i \colon k_0] = f_0 \cdots f_{i-1}. \tag{5.14}$$

Let us anticipate some properties of these numerical data, which will be proved in due time.

Remarks.

(1) For $i > 0$, the field k_i is obtained by adjoining to the field k_{i-1} a root of the polynomial $R_{i-1}(\phi_i)$. In particular, $f_{i-1} = \deg(R_{i-1}(\phi_i))$.

(2) A key polynomial of an inductive valuation satisfies $\deg(\phi) = e(\phi)f(\phi)$. In particular,

$$m_i = e_{i-1}f_{i-1}m_{i-1} = (e_0 \cdots e_{i-1})(f_0 \cdots f_{i-1}), \qquad 0 \leq i \leq r.$$

5.3 Rational functions of a MacLane chain

Our main aim in this section is to construct an element $y_i \in \Delta_i$ which is transcendental over k_i and satisfies $\Delta_i = k_i[y_i]$.

As indicated in Theorem 1.28, this amounts to the construction of a rational function $Y_i = \phi_i^{e_i}/u_i$ where u_i is a polynomial satisfying

$$\deg(u_i) < m_i, \qquad \mu_i(u_i) = \mu_i(\phi_i^{e_i}) = e_i\gamma_i = h_i.$$

By Lemma 2.5, $H_{\mu_i}(u_i)$ is a unit in $\mathcal{G}_{\mu_i}$ and we may take

$$y_i = H_{\mu_i}(\phi_i^{e_i})H_{\mu_i}(u_i)^{-1}.$$

Caution. *Actually, we shall construct this unit $H_{\mu_i}(u_i)$ as the image in $\mathcal{G}_{\mu_i}$ of a certain rational function $u_i \in K(x)$ with value $\mu_i(u_i) = h_i$.*

By Lemma 1.24, the element $H_{\mu_i}(u_i)$ will coincide with the homogeneous element in $\mathcal{G}_{\mu_i}$ determined by a polynomial of degree less than m_i.

This problem raises the question of the construction of rational functions in $K(x)$ with prescribed μ_i-values in the group Γ_{μ_i}. Thanks to our choice of a finitely-generated subgroup $\Gamma_i \subset \Gamma_{\mu_i}$, and a $\mathbb{Z}$-basis of this subgroup, this question amounts to the choice of rational functions whose μ_i-values attain the chosen basis $\iota_{i+1,1}, \dots, \iota_{i+1,k}$.

We proceed to construct these rational functions in a recursive way.

Initially, we choose arbitrary elements $\pi_{0,j} \in K$ such that

$$v(\pi_{0,j}) = \iota_{0,j}, \qquad 1 \le j \le k.$$

Starting with these elements, we shall construct in a recursive way rational functions $\pi_{i+1,j} \in K(x)$ such that

$$\mu_i(\pi_{i+1,j}) = \iota_{i+1,j}, \qquad -1 \le i \le r, \quad 1 \le j \le k.$$

An element $\alpha \in \Gamma_i$ can be written in a unique way as

$$\alpha = \alpha_1\,\iota_{i+1,1} + \cdots + \alpha_k\,\iota_{i+1,k}, \qquad \alpha_1, \dots, \alpha_k \in \mathbb{Z}.$$

Then, we shall denote by π_{i+1}^{α}, the following element:

$$\pi_{i+1}^{\alpha} := \pi_{i+1,1}^{\alpha_1} \dots \pi_{i+1,k}^{\alpha_k} \in K(x), \qquad \mu_i\left(\pi_{i+1}^{\alpha}\right) = \alpha.$$

We recall that these choices determine a group homomorphism

$$\pi_{i+1}\colon \Gamma_i \longrightarrow K(x)^*, \qquad \alpha \longmapsto \pi_{i+1}^{\alpha}.$$

We are ready to give a recursive definition of our rational functions $Y_i \in K(x)$ and $\pi_{i+1,j} \in K(x)$.

Definition 5.16. *For $0 \le i \le r$, define*

$$Y_i = \phi_i^{e_i}\,\pi_i^{-h_i},$$
$$\pi_{i+1,j} = \left(\phi_i\,\pi_{i,1}^{-h_{i,1}/e_{i,1}} \cdots \pi_{i,j-1}^{-h_{i,j-1}/e_{i,j-1}}\right)^{\ell_{i,j}e'_{i,j}}\ \pi_{i,j}^{\ell'_{i,j}},\ 1 \le j \le k.$$

In the definition of $\pi_{i+1,j}$, the rational functions $\pi_{i,1},\dots,\pi_{i,j-1}$ appear with integer exponents, because $e'_{i,j}/e_{i,t}$ is an integer for $t<j$, as shown in (5.12).

For $i\geq 0$, it is easy to deduce from the definition that:

$$\pi_{i+1,j}=\pi_0^{\beta}\phi_0^{n_0}\cdots\phi_{i-1}^{n_{i-1}}\phi_i^{\ell_{i,j}e'_{i,j}}, \tag{5.15}$$

for a certain $\beta\in\Gamma_{-1}$ and certain (eventually negative) integer exponents $n_0,\dots,n_{i-1}$. Since $\phi_{i+1}\nmid_{\mu_i}\phi_\ell$ for $\ell\leq i$, Lemma 5.1 shows that

$$\begin{aligned}&\mu_i(\pi_{i+1,j})=\mu_{i+1}(\pi_{i+1,j})=\cdots=\mu(\pi_{i+1,j}),\\&\mu_i(Y_i)=\mu_{i+1}(Y_i)=\cdots=\mu(Y_i),\end{aligned} \tag{5.16}$$

Let us compute these stable values.

Lemma 5.17. *For every pair of indices $0\leq i\leq r$, $1\leq j\leq k$, we have*

$$\mu_i(Y_i)=0,\qquad \mu_i(\pi_{i+1,j})=\iota_{i+1,j}.$$

Proof. The first identity follows immediately from the definition of the rational function Y_i.

Let us prove the second identity. For $i=-1$, $\mu_{-1}(\pi_{0,j})=\iota_{0,j}$ for all j by definition.

Suppose $i\geq 0$ and the identity holds for lower indices. Then,

$$\mu_i(\pi_{i,j})=\mu_{i-1}(\pi_{i,j})=\iota_{i,j},$$

for all j, by (5.16). Thus,

$$\mu_i(\pi_{i+1,j})=l_{i,j}e'_{i,j}\left(\gamma_i-\frac{h_{i,1}}{e_{i,1}}\,\iota_{i,1}-\cdots-\frac{h_{i,j-1}}{e_{i,j-1}}\,\iota_{i,j-1}\right)+l'_{i,j}\,\iota_{i,j}=\iota_{i+1,j},$$

as shown in (5.11). □

Our next aim is to establish certain relationships between the rational functions of Definition 5.16. To this end we introduce some more notation.

Definition 5.18. *Take an index $0\leq i\leq r$. Denote:*

$$L'_i=\ell'_{i,1}\cdots\ell'_{i,k},\qquad L_{i,j}=\ell_{i,j}\,\ell'_{i,j+1}\cdots\ell'_{i,k},\quad 1\leq j\leq k.$$

Consider the function

$$L_i\colon\mathbb{Q}\Gamma_{i-1}\longrightarrow\mathbb{Q},\qquad \alpha\mapsto L_{i,1}\,\alpha_1+\cdots+L_{i,k}\,\alpha_k,$$

if $\alpha=\alpha_1\,\iota_{i,1}+\cdots+\alpha_k\,\iota_{i,k}$, with $\alpha_1,\dots,\alpha_k\in\mathbb{Q}$.

Lemma 5.19. *For all $0\leq i\leq r$, we have $L'_i+L_i(\gamma_i)=1/e_i$.*

Proof. Consider the following identity:

$$\frac{\ell'_{i,j}}{e'_{i,j}} + \frac{\ell_{i,j} h_{i,j}}{e_{i,j}} = \frac{d_{i,j}}{e'_{i,j} e_{i,j}} = \frac{d_{i,1} \dots d_{i,j}}{e_{i,1} \dots e_{i,j}} = \frac{1}{e'_{i,j+1}}, \quad 1 \le j \le k. \tag{5.17}$$

Now, we claim that:

$$L'_i + L_{i,1} \frac{h_{i,1}}{e_{i,1}} + \dots + L_{i,j} \frac{h_{i,j}}{e_{i,j}} = \ell'_{i,j+1} \dots \ell'_{i,k} \frac{1}{e'_{i,j+1}}, \quad 1 \le j \le k. \tag{5.18}$$

For $j = k$, this identity proves the lemma, since $e'_{i,k+1} = e_i$ by Lemma 5.13.

Let us prove (5.18) by induction on j. For $j = 1$, it follows directly from (5.17), having in mind that $e'_{i,1} = 1$:

$$L'_i + L_{i,1} \frac{h_{i,1}}{e_{i,1}} = \ell'_{i,2} \dots \ell'_{i,k} \left(\frac{\ell'_{i,1}}{e'_{i,1}} + \frac{\ell_{i,1} h_{i,1}}{e_{i,1}} \right) = \ell'_{i,2} \dots \ell'_{i,k} \frac{1}{e'_{i,2}}.$$

Now, if we assume that (5.18) holds for $j - 1$:

$$L'_i + L_{i,1} \frac{h_{i,1}}{e_{i,1}} + \dots + L_{i,j-1} \frac{h_{i,j-1}}{e_{i,j-1}} = \ell'_{i,j} \dots \ell'_{i,k} \frac{1}{e'_{i,j}},$$

we deduce the identity (5.18) for j, just by adding $L_{i,j} h_{i,j} / e'_{i,j}$ to both sides of the equality, and applying (5.17) to the right-hand side. □

Lemma 5.20. *For $0 \le i \le r$, let $Q \in \mathbb{Q}^{k \times k}$ be the matrix introduced in Definition 5.14. Then,*

$$(L_{i,1} \ \dots \ L_{i,k})\, Q = \frac{1}{e_i} \ (\ell_{i,1} e'_{i,1} \ \dots \ \ell_{i,k} e'_{i,k}).$$

Proof. The statement is equivalent to the following identity:

$$L_{i,j} \frac{d_{i,j}}{e_{i,j}} + L_{i,j+1}\, q_{j+1,j} + \dots + L_{i,k}\, q_{k,j} = \frac{1}{e_i}\, \ell_{i,j} e'_{i,j}, \quad 1 \le j \le k,$$

where $q_{m,j} = \ell_{i,j} e'_{i,j} h_{i,m} / e_{i,m}$ are the entries of Q for $m > j$. Equivalently,

$$L_{i,j} \ \frac{d_{i,j}}{\ell_{i,j} e_{i,j} e'_{i,j}} + L_{i,j+1} \ \frac{h_{i,j+1}}{e_{i,j+1}} + \dots + L_{i,k} \ \frac{h_{i,k}}{e_{i,k}} = \frac{1}{e_i}.$$

By Lemma 5.19, this is equivalent to

$$L'_i + L_{i,1} \frac{h_{i,1}}{e_{i,1}} + \dots + L_{i,j} \frac{h_{i,j}}{e_{i,j}} = L_{i,j} \frac{d_{i,j}}{l_{i,j} e_{i,j} e'_{i,j}} = \ell'_{i,j+1} \cdots \ell'_{i,k} \frac{1}{e'_{i,j+1}},$$

which was proven in (5.18). □

Recall the definition of the rational functions

$$\pi_{i+1,j} = \left(\phi_i \, \pi_{i,1}^{-h_{i,1}/e_{i,1}} \cdots \pi_{i,j-1}^{-h_{i,j-1}/e_{i,j-1}} \right)^{\ell_{i,j} e'_{i,j}} \ \pi_{i,j}^{\ell'_{i,j}}, \quad 1 \le j \le k.$$

Let us rewrite these identities using formal logarithms:

$$\log \pi_{i+1,j} = \ell_{i,j} e'_{i,j} \left(\log \phi_i - \frac{h_{i,1}}{e_{i,1}} \log \pi_{i,1} - \cdots - \frac{h_{i,j-1}}{e_{i,j-1}} \log \pi_{i,j-1} \right) + \ell'_{i,j} \log \pi_{i,j}.$$

We may unify all these identities for $1 \le j \le k$ in a single identity:

$$(\log \pi_{i+1,1} \cdots \log \pi_{i+1,k}) = \log \phi_i \, \left(\ell_{i,1} e'_{i,1} \cdots \ell_{i,k} e'_{i,k} \right) + (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, A, \qquad (5.19)$$

where $A = (a_{m,j}) \in \mathbb{Q}^{k \times k}$ is the matrix with entries:

$$a_{m,j} = \begin{cases} 0, & \text{if } m > j \\ \ell'_{i,j}, & \text{if } m = j \\ -\ell_{i,j} e'_{i,j} \dfrac{h_{i,m}}{e_{i,m}}, & \text{if } m < j \end{cases}.$$

Lemma 5.21. *Let $0 \le i \le r$. Consider the column-vector*

$$\mathbf{u} = (h_{i,1}/e_{i,1} \ldots \, h_{i,k}/e_{i,k})^t \in \mathbb{Q}^{k \times 1},$$

and the matrix $B = \mathbf{u} \, (L_{i,1} \ldots L_{i,k}) \in \mathbb{Q}^{k \times k}$.

(1) For any k-dimensional column-vector $\mathbf{v}$ we have

$$B\mathbf{v} = L_i(\alpha)\mathbf{u}, \text{ where } \alpha = (\iota_{i,1} \cdots \iota_{i,k}) \, \mathbf{v}.$$

(2) $A = (I - e_i B)Q$.

(3) The vector $\mathbf{u}$ is an eigenvector of the matrix $I - e_i B$, with eigenvalue $e_i L'_i$.

Proof. The first item follows immediately from the definition of the operator L_i.

By Lemma 5.20,

$$(I - e_i B)Q = Q - e_i \mathbf{u} \, (L_{i,1} \ldots L_{i,k}) \, Q = Q - \mathbf{u} \left(\ell_{i,1} e'_{i,1} \ldots \ell_{i,k} e'_{i,k} \right).$$

Hence, item (2) is equivalent to $Q - A = \mathbf{u} \left(\ell_{i,1} e'_{i,1} \ldots \ell_{i,1} e'_{i,1} \right)$, or equivalently,

$$q_{m,j} - a_{m,j} = \frac{h_{i,m}}{e_{i,m}} \, \ell_{i,j} e'_{i,j}, \quad \forall, m, j.$$

If $m > j$ ($a_{m,j} = 0$), or $m < j$ ($q_{m,j} = 0$), the identity is obvious.

If $m = j$, the desired equality follows from $\ell_{i,m} h_{i,m} e'_{i,m} = d_{i,m} - \ell'_{i,m} e_{i,m}$.

Finally, by the first item,

$$(I - e_i B)\mathbf{u} = \mathbf{u} - e_i L_i(\gamma_i)\mathbf{u} = e_i L'_i \, \mathbf{u},$$

by Lemma 5.19. □

Proposition 5.22. *For all $0 \le i \le r$, and $\beta \in \Gamma_{i-1}$, we have*

$$\pi_{i+1}^{\beta}/\pi_i^{\beta} = Y_i^{L_i(\beta)}.$$

Proof. Write $\beta = \beta_1\iota_{i,1} + \cdots + \beta_k\iota_{i,k}$, with $\beta_1, \ldots, \beta_k \in \mathbb{Z}$. By definition,

$$\log \pi_{i+1}^{\beta} = (\log \pi_{i+1,1} \cdots \log \pi_{i+1,k})\, Q^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix}.$$

By (5.19) and Lemmas 5.20 and 5.21,

$$\begin{aligned} \log \pi_{i+1}^{\beta} &= \log \phi_i \, \left(\ell_{i,1}e'_{i,1} \, \cdots \, \ell_{i,k}e'_{i,k}\right) \, Q^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} + (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, AQ^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} \\ &= e_iL_i(\beta) \log \phi_i + (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, (I - e_iB) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} \\ &= \log \phi_i^{e_iL_i(\beta)} + \log \pi_i^{\beta} - (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, e_iL_i(\beta)\mathbf{u} \end{aligned}$$

Hence,

$$\log\left(\pi_{i+1}^{\beta}/\pi_i^{\beta}\right) = \log \phi_i^{e_iL_i(\beta)} - \log \pi_i^{h_iL_i(\beta)} = \log Y_i^{L_i(\beta)},$$

because $(\log \pi_{i,1} \cdots \log \pi_{i,k}) \, e_i\mathbf{u} = \log \pi_i^{e_i\gamma_i} = \log \pi_i^{h_i}$. □

Proposition 5.23. *For all $0 \le i \le r$, we have $\phi_i/\pi_{i+1}^{\gamma_i} = Y_i^{L'_i}$.*

Proof. By (5.19) and Lemmas 5.19, 5.20 and 5.21,

$$\begin{aligned} \log\left(\phi_i/\pi_{i+1}^{\gamma_i}\right) &= \log \phi_i - (\log \pi_{i+1,1} \cdots \log \pi_{i+1,k}) \, Q^{-1}\mathbf{u} \\ &= \left(1 - \left(\ell_{i,1}e'_{i,1} \, \cdots \, \ell_{i,k}e'_{i,k}\right) \, Q^{-1}\mathbf{u}\right) \log \phi_i - (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, AQ^{-1}\mathbf{u} \\ &= (1 - e_iL_i(\gamma_i)) \log \phi_i - (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, (I - e_iB)\mathbf{u} \\ &= \log \phi_i^{e_iL'_i} - (\log \pi_{i,1} \cdots \log \pi_{i,k}) \, e_iL'_i\mathbf{u} \\ &= \log \phi_i^{e_iL'_i} - \log \pi_i^{h_iL'_i} = \log Y_i^{L'_i}. \end{aligned}$$

because $(\log \pi_{i,1} \cdots \log \pi_{i,k}) \, e_i\mathbf{u} = \log \pi_i^{e_i\gamma_i} = \log \pi_i^{h_i}$. □

Proposition 5.24. *Let $(s, u) \in \mathbb{Z}_{\ge 0} \times \Gamma_{r-1}$. Then,*

$$\phi_r^s\pi_r^u/\pi_{r+1}^{u+s\gamma_r} = (Y_r)^{L'_r \, s - L_r(u)}.$$

Proof. By Proposition 5.22, $\pi_r^u/\pi_{r+1}^u = Y_r^{-L_r(u)}$. Hence, the claimed identity is equivalent to $\phi_r^s \,/\, \pi_{r+1}^{s\gamma_r} = Y_r^{L'_r \, s}$, which follows from Proposition 5.23. □

Elements in $\mathcal{G}_\mu$ determined by the rational functions

According to (5.15), the rational functions Y_i, $\pi_{i,j}$ introduced in Definition 5.16 are a product of an element in K^* by powers of $\phi_0, \dots, \phi_i$ with integer exponents. The exponent of ϕ_i is non-negative in the two cases: e_i, and 0, respectively.

For $0 \le j < i$, the exponent of ϕ_j may be negative, but the element $H_{\mu_i}(\phi_j)$ is a unit in $\mathcal{G}_{\mu_i}$, by Lemma 2.5.

Therefore, it makes sense to consider the image in the graded algebra of these rational functions, and the image of $\pi_{i,j}$ will be a unit.

Definition 5.25. *For $0 \le i \le r$ we define:*

$$\begin{aligned} x_i &= H_{\mu_i}(\phi_i), \\ y_i &= H_{\mu_i}(Y_i) \in \Delta_{\mu_i}, \\ p_{i,j} &= H_{\mu_i}(\pi_{i,j}) \in \mathcal{G}^*_{\mu_i}, \quad 1 \le j \le k. \end{aligned}$$

Also, for any $\alpha = \alpha_1\iota_{i,1} + \cdots + \alpha_k\iota_{i,k} \in \Gamma_{i-1}$, we define

$$p_i^\alpha = H_{\mu_i}(\pi_i^\alpha) = p_{i,1}^{\alpha_1} \cdots p_{i,k}^{\alpha_k} \in \mathcal{G}^*_{\mu_i}.$$

Note that $x_i = H_{\mu_i}(\phi_i)$ is a prime element in $\mathcal{G}_{\mu_i}$, of degree γ_i. Hence, $y_i = x_i^{e_i}\, p_i^{-h_i}$ is associate to the e_i-th power of this prime element.

Also, we can think of the symbol p_i as a group homomorphism:

$$p_i \colon \Gamma_{i-1} \longrightarrow \mathcal{G}^*_{\mu_i}, \qquad \alpha \longmapsto p_i^\alpha.$$

Lemma 5.26. *Let (s,u), $(s',u') \in \mathbb{Z}_{\ge 0} \times \Gamma_{\mu_{r-1}}$ such that $s\gamma_r + u = s'\gamma_r + u'$.*

Then, there exists $j \in \mathbb{Z}$ such that

$$s' = s + je_r, \quad u' = u - jh_r, \quad x_r^{s'}\, p_r^{u'} = x_r^s\, p_r^u\, y_r^j.$$

Proof. By (5.4), from $(s'-s)\gamma_r = u - u' \in \Gamma_{\mu_{r-1}}$, we deduce $s' - s = je_r$ for some $j \in \mathbb{Z}$. Then, $u' = u - je_r\gamma_r = u - jh_r$.

The lemma follows then easily from $y_r = x_r^{e_r}\, p_r^{-h_r}$. □

Definition 5.27. *Suppose $0 \le i < r$ and let $\alpha \in \Gamma_{i-1}$. By (5.15), (5.16) and Lemma 2.5, the elements x_i, $p_i^\alpha \in \mathcal{G}_{\mu_i}$ are mapped to units in $\mathcal{G}_{\mu_{i+1}}$ under the canonical homomorphism. We denote these images by the same symbol x_i, $p_i^\alpha \in \mathcal{G}^*_\mu$, respectively.*

On the other hand, we denote by $z_i \in k_{i+1} \subset k_\mu$ the image of y_i under the canonical homomorphism

$$\Delta_{\mu_i} \twoheadrightarrow k_{i+1} \subset \Delta_{\mu_{i+1}}, \qquad y_i \mapsto z_i.$$

By the same argument as above, z_i is a unit; that is, $z_i \ne 0$.

Remark 5.28. *We shall see in Corollary 6.6 that $k_{i+1} = k_i[z_i] = k_0[z_0, \dots, z_i]$.*

Also, we shall prove in Corollary 6.18 that $R_i(\phi_{i+1})$ is the minimal polynomial of z_i over k_i. In particular, $\deg(R_i(\phi_{i+1})) = f_i$.

In optimal MacLane chains, the elements $x_i, p_i^\alpha, y_r, z_i \in \mathcal{G}_\mu$ are "almost" independent of the chain. Their precise variation is analyzed in section 6.6.

Chapter 6

Residual polynomial operators of inductive valuations

Consider a MacLane chain of an inductive valuation $\mu \in \mathbb{V}^{\text{ind}}$:

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu.$$

Throughout this chapter we denote

$$\mathcal{G} = \mathcal{G}_\mu, \qquad \Delta = \Delta_\mu, \qquad \mathcal{R} = \mathcal{R}_\mu,$$

and we shall freely use all data and operators associated with our fixed MacLane chain in Chapter 5.

We fixed a finitely-generated subgroup $\Gamma^{\text{fg}} \subset \Gamma$, leading to a chain of finitely-generated subgroups

$$\Gamma^{\text{fg}} = \Gamma_{-1} \subset \Gamma_0 \subset \cdots \subset \Gamma_r = \Gamma_\mu^{\text{fg}},$$

such that

$$h_i = e_i\gamma_i \in \Gamma_i = \Gamma_{-1} + \left\langle \gamma_1, \ldots, \gamma_i \right\rangle \subset \Gamma_{\mu_i}, \qquad 0 \le i \le r.$$

Also, we constructed group homomorphisms

$$p_i \colon \Gamma_{i-1} \longrightarrow \mathcal{G}_{\mu_i}^*, \qquad \alpha \longmapsto p_i^\alpha, \qquad 0 \le i \le r,$$

such that p_i^α is a homogeneous unit of degree α in the graded algebra $\mathcal{G}_{\mu_i}$.

Recall the existence of a tower of finite field extensions:

$$k = k_0 \subset k_1 \subset \cdots \subset k_r \subset \Delta.$$

After Lemma 2.6, these fields are defined as

$$k_i = \text{Im}\left(\Delta_{i-1} \to \Delta_i\right), \qquad 1 \le i \le r.$$

Each k_i is the algebraic closure of k in Δ_i, and it satisfies $\Delta_i^* = k_i^*$.

Recall the definition of the subset of polynomials having attainable μ-values:

$$K[x]_{\mu\text{-at}} = \left\{ g \in K[x] \mid \mu(g) \in \Gamma_\mu^{\text{fg}} \right\} \subset K[x].$$

In this chapter, we introduce residual polynomial operators:

$$R_i := R_{\mu_i,\phi_i} \colon K[x]_{\mu_i\text{-at}} \longrightarrow k_i[y], \quad 0 \le i \le r,$$

playing an essential role in the whole theory.

Each operator R_i is determined by the MacLane chain of μ_i obtained by truncation of the given MacLane chain of μ. Thus, it suffices to describe R_r.

Why don't we use the general operator R_μ introduced in section 1.7?

Because we are interested in a *constructive* way to deal with inductive valuations. As we shall see in Theorem 10.7, inductive valuations are useful to detect information about the irreducible factors of any given polynomial $f \in K[x]$, over a henselization K^h of the valued field (K, v).

We want to be able to design algorithms which capture this information.

To this end, we need residual polynomial operators of each of the intermediate valuations μ_i, and they require choices of pairs ϕ_i, u_i at each level.

The choice of the parameter $u_i \in K(x)^*$ is delicate. We must choose it in a coherent way for the different levels of the MacLane chains, thus allowing a recursive (hence constructive) computation of the residual polynomial operators.

This aim will be fulfilled in section 6.4.

6.1 Definition of the operator R_r

We define $R_r(0) = 0$.

For a non-zero $f \in K[x]$ consider the canonical ϕ_r-expansion:

$$f = \sum\nolimits_{0 \le s} a_s \phi_r^s, \quad \deg(a_s) < \deg(\phi_r).$$

By the definition of an augmented valuation,

$$\mu(f) = \operatorname{Min}\{\mu\left(a_s\phi_r^s\right) \mid s \ge 0\} = \operatorname{Min}\{\mu_{r-1}\left(a_s\right) + s\gamma_r \mid s \ge 0\}.$$

The Newton polygon $N_r(f)$ is the lower convex hull of the set of points:

$$\mathcal{C} = \{Q_s := (s, \mu_{r-1}\left(a_s\right)) \mid s \ge 0\} \subset \mathbb{Z}_{\ge 0} \times \Gamma_{\mu_{r-1}}.$$

Let $S_{\gamma_r}(f) \subset \mathbb{Q} \times \mathbb{Q}\Gamma$ be the γ_r-component of $N_r(f)$ (cf. Definition 3.2). Let

$$(s_0, u_0) := (s_r(f), u_r(f)), \quad (s_r'(f), u_r'(f)) \in \mathbb{Z}_{\ge 0} \times \Gamma_{\mu_{r-1}}$$

be the left and right endpoints of $S_{\gamma_r}(f)$, respectively.

By Remark 3.1, for any point $(s, u) \in N_r(f)$, we have

$$(s, u) \in S_{\gamma_r}(f) \iff u + s\gamma_r = \mu(f) = u_0 + s_0\gamma_r. \tag{6.1}$$

If we impose that $(s, u) \in \mathbb{Z}_{\ge 0} \times \Gamma_{\mu_{r-1}}$, Lemma 5.26 shows that

$$(s, u) \in S_{\gamma_r}(f) \cap \left(\mathbb{Z}_{\ge 0} \times \Gamma_{\mu_{r-1}}\right) \implies s = s_0 + je_r, \quad u = u_0 - jh_r, \quad j \in \mathbb{Z}.$$

Since both endpoints of S_{γ_r} belong to $\mathbb{Z}_{\geq 0} \times \Gamma_{\mu_{r-1}}$, the integer j runs on:

$$0 \leq j \leq d := (s'_r(f) - s_r(f))/e_r.$$

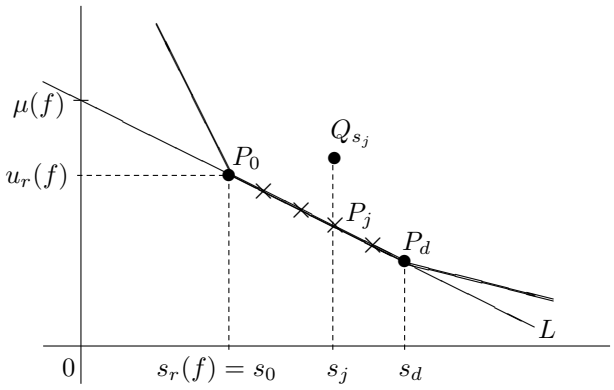
This non-negative integer d is called the *degree* of the segment $S_{\gamma_r}(f)$. We have $d = 0$ if and only if $N_r(f)$ has no sides of slope $-\gamma_r$.

In other words, if we denote $s_j = s_0 + je_r$, $u_j = u_0 - je_r$, we have seen that

$$S_{\gamma_r}(f) \cap \left(\mathbb{Z}_{\geq 0} \times \Gamma_{\mu_{r-1}}\right) = \{P_0, P_1, \ldots, P_d\},$$

where $P_j = (s_j, u_j)$ for $0 \leq j \leq d$.

Figure 6.1: Newton polygon $N_r(f)$ for $g \in K[x]$. The line L has slope $-\gamma_r$



Definition 6.1. *For a non-zero $f \in K[x]$ with attainable μ-value, we define*

$$R_r(f) = c_0 + c_1\, y + \cdots + c_d\, y^d \in k_r[y],$$

where the coefficients $c_j \in k_r$ are defined as

$$c_j := \begin{cases} p_r^{-\mu_{r-1}(a_{s_j})} H_\mu(a_{s_j}) \in k_r^*, & \text{if } Q_{s_j} \text{ lies on } N_r(f), \\ 0, & \text{otherwise.} \end{cases}$$

By Lemma 2.5, $H_\mu(a_{s_j})$ is a unit in $\mathcal{G}$. By Proposition 2.2, $\mu(a_{s_j}) = \mu_{r-1}(a_{s_j})$.

Therefore, if Q_{s_j} lies on $N_r(f)$, the coefficient c_j is a homogeneous unit of degree zero; that is, $c_j \in \Delta^* = k_r^*$.

Note that $p_r^{-\mu_{r-1}(a_{s_j})}$ is well defined only if $\mu_{r-1}(a_{s_j}) \in \Gamma_{r-1}$. The next lemma guarantees this.

Lemma 6.2. *If $f = \sum_{0 \leq s} a_s \phi_r^s$ has attainable μ-value, then for all s such that Q_s lies on $S_{\gamma_r}(f)$, the coefficient a_s has attainable μ_{r-1}-value.*

Proof. By (6.1), the condition $Q_s \in S_{\gamma_r}(f)$ leads to $\mu(f) = \mu_{r-1}(a_s) + s\gamma_r$.

Thus, the condition $\mu(f) \in \Gamma_r$ implies $\mu_{r-1}(a_s) \in \Gamma_{\mu_{r-1}} \cap \Gamma_r = \Gamma_{r-1}$. The last equality by Lemma 5.10. □

If Γ is finitely generated, we may take $\Gamma^{\rm fg} = \Gamma$ as a universal choice for this subgroup. This implies $\Gamma_i = \Gamma_{\mu_i}$ for all i. Then, $K[x]_{\mu\text{-at}} = K[x]$ and the residual polynomial $R_r(f)$ is defined for all $f \in K[x]$.

Otherwise, the finitely-generated subgroup $\Gamma^{\rm fg} \subset \Gamma$, and the finitely-generated subgroups $\Gamma_i \subset \Gamma_{\mu_i}$ derived from this choice, play only an instrumental role.

In any particular instance where we use the operator R_r, we may think that $\Gamma^{\rm fg}$ is chosen to be sufficiently large to ensure that all involved polynomials have attainable μ-values.

Therefore, for simplicity in the exposition of the results, we adopt the following convention.

Convention. *In any statement or argument involving a finite number of polynomials, we shall implictly assume that the subgroup $\Gamma^{\rm fg}$ is sufficiently large to allow the application of the operator R_r to all the involved polynomials.*

6.2 Basic properties of the operator R_r

We keep with the notation from the preceding section.

Let us first summarize two basic properties of R_r, which follow immediately from the fact that $c_0, c_d \neq 0$, because $Q_{s_0} = P_{s_0}$ and $Q_{s_d} = P_{s_d}$ both lie on $S_{\gamma_r}(f)$.

Lemma 6.3. *Let $f \in K[x]$ be a non-zero polynomial.*

(1) $\deg(R_r(f)) = (s_r'(f) - s_r(f))/e_r$.

(2) $R_r(f)(0) \in k_r^*$.

The essential property of the operator R_r is displayed in the next result.

Theorem 6.4. *For any $f \in K[x]$, we have*

$$H_\mu(f) = x_r^{s_r(f)} p_r^{u_r(f)} R_r(f)(y_r).$$

Proof. Since $s \notin \{s_0, \dots, s_d\}$ implies $\mu\left(a_s \phi_r^s\right) > \mu(f)$, we have

$$f \sim_\mu f_{S_{\gamma_r}}, \quad \text{where} \quad f_{S_{\gamma_r}} := \phi_r^{s_0}\left(a_{s_0} + a_{s_1}\phi_r^{e_r} + \cdots + a_{s_d}\phi_r^{de_r}\right).$$

Assuming that $f \in K[x]_{\mu\text{-at}}$ has attainable μ-value, Lemma 6.2 shows that $u_0 = \mu_{r-1}(a_{s_0}) \in \Gamma_{r-1}$. Thus, we may write

$$f_{S_{\gamma_r}} = \phi_r^{s_0}\pi_r^{u_0}\left(b_0 + b_1 Y_r + \cdots + b_d Y_r^d\right), \tag{6.2}$$

where $(s_0, u_0) = (s_r(f), u_r(f))$, $Y_r = \phi_r^{e_r}\pi_r^{-h_r} \in K(x)$, and

$$b_j = \pi_r^{jh_r - u_0} a_{s_j} \in K(x), \qquad 0 \le j \le d.$$

Since $h_r = e_r\gamma_r$, we have $\mu\left(\phi_r^{je_r}\right) = jh_r$. Thus, from $\mu(f) = u_0 + s_0\gamma_r$ we get

$$\mu_{r-1}(b_j) = jh_r - u_0 + \mu_{r-1}(a_{s_j}) = \mu\left(a_{s_j}\phi_r^{s_j}\right) - \mu\left(f\right) \geq 0,$$

and equality may be characterized as follows

$$\mu_{r-1}(b_j) = 0 \iff Q_{s_j} \text{ lies on } S_{\gamma_r}(f) \iff \mu_{r-1}(a_{s_j}) = u_0 - jh_r.$$

Therefore, when equality holds, we have

$$H_\mu(b_j) = p_r^{jh_r - u_0} H_\mu(a_{s_j}) = p_r^{-\mu_{r-1}(a_{s_j})} H_\mu(a_{s_j}) = c_j.$$

Since $f \sim_\mu f_{S_{\gamma_r}}$, the result follows from the application of H_μ to both sides of equation (6.2), having in mind equation (1.3). □

Thus, any non-zero homogeneous element $H_\mu(f)$ splits into a product of a power of the prime x_r, times a unit, times a degree-zero element $R_r(f)(y_r) \in \Delta$.

Remark. *Lemma 6.3 and Theorem 6.4 are the first instances where we applied the above Convention. Rigorous statements would assume that* $f \in K[x]_{\mu\text{-at}}$.

We shall not warn the reader anymore about this Convention.

We now derive from Theorem 6.4 some more basic properties of the operator R_r. We start with a result giving a more complete form to Theorem 1.28.

Theorem 6.5. *The mapping* $k_r[y] \to \Delta$ *induced by* $y \mapsto y_r$ *is an isomorphism of* k_r*-algebras. The inverse isomorphism assigns*

$$H_\mu(g) \longmapsto y^{s_r(g)/e_r} R_r(g),$$

for each $g \in K[x]$ *having* $\mu(g) = 0$.

Proof. Let $g \in K[x]$ with $\mu(g) = 0$. By Lemma 5.26, applied to the pairs $(s_r(g), u_r(g))$ and $(0, 0_\Gamma)$, there exists an integer $j \geq 0$ such that

$$s_r(g) = je_r, \quad \text{and} \quad x_r^{s_r(g)}\, p_r^{u_r(g)} = y_r^j.$$

By Theorem 6.4, $H_\mu(g) = y_r^j\, R_r(g)(y_r)$ is a polynomial in y_r with coefficients in k_r. This proves that the mapping $k_r[y] \to \Delta$ is onto.

On the other hand, Δ is a domain which is not a field, because $y_r \in \Delta$ is not a unit in $\mathcal{G}$. In fact, y_r is associate to the e_r-th power of the prime element x_r.

Thus, the mapping is 1-1 because the kernel vanishes, being a prime ideal of $k_r[y]$ which is not maximal. □

Corollary 6.6. *If* $r > 0$, *then* $k_r = k_{r-1}[z_{r-1}] = k[z_0, \ldots, z_{r-1}]$.

Proof. Theorem 6.5 applied to the valuation μ_{r-1} shows that $\Delta_{r-1} = k_{r-1}[y_{r-1}]$. Therefore, $k_r = \mathrm{Im}\,(\Delta_{r-1} \to \Delta) = k_{r-1}[z_{r-1}]$. □

Corollary 6.7. *Let $f, g \in K[x]$. Then, $R_r(fg) = R_r(f)R_r(g)$.*

Proof. Since $H_\mu(fg) = H_\mu(f)H_\mu(g)$, the statement follows from equation (5.7) and Theorems 6.4 and 6.5, as long as:

$$s_r(fg) = s_r(f) + s_r(g) \quad \text{and} \quad u_r(fg) = u_r(f) + u_r(g).$$

These identities follow from Lemma 3.9. □

Corollary 6.8. *Let $f, g \in K[x]$. Then,*

$$\begin{aligned} f \sim_\mu g \quad &\iff \quad s_r(f) = s_r(g),\ u_r(f) = u_r(g) \ \ \textit{and} \ \ R_r(f) = R_r(g). \\ f \mid_\mu g \quad &\iff \quad s_r(f) \le s_r(g) \ \ \textit{and} \ \ R_r(f) \mid R_r(g) \ \ \textit{in} \ \ k_r[y]. \end{aligned}$$

Proof. If $f \sim_\mu g$, then $S_{\gamma_r}(f) = S_{\gamma_r}(g)$ by Lemma 3.8. In particular, these segments have the same left endpoint: $(s_r(f), u_r(f)) = (s_r(g), u_r(g))$. Thus, $R_r(f)(y_r) = R_r(g)(y_r)$ by Theorem 6.4, and we deduce $R_r(f) = R_r(g)$ from Theorem 6.5.

Conversely, the equalities $(s_r(f), u_r(f)) = (s_r(g), u_r(g))$ and $R_r(f) = R_r(g)$ imply $H_\mu(f) = H_\mu(g)$ by Theorem 6.4.

If $f \mid_\mu g$, then $fh \sim_\mu g$ for some $h \in K[x]$. By the first item and Corollary 6.7, we get $R_r(g) = R_r(fh) = R_r(f)R_r(h)$. Thus $R_r(f) \mid R_r(g)$. By Lemma 3.9, $s_r(g) = s_r(f)+s_r(h)$, so that $s_r(f) \le s_r(g)$.

Conversely, $s_r(f) \le s_r(g)$ and $R_r(f) \mid R_r(g)$ imply $H_\mu(f) \mid H_\mu(g)$ by Theorem 6.4, having in mind that p_r^α is a unit for all $\alpha \in \mathcal{G}_{\mu_{r-1}}$. □

Corollary 6.9. *Let $f, g \in K[x]$ such that $\mu(f) = \mu(g)$. Then,*

$$y^{\lfloor s_r(f)/e_r \rfloor} R_r(f) + y^{\lfloor s_r(g)/e_r \rfloor} R_r(g) = \begin{cases} y^{\lfloor s_r(f+g)/e_r \rfloor} R_r(f+g), & \text{if } \mu(f+g) = \mu(f), \\ 0, & \text{if } \mu(f+g) > \mu(f). \end{cases}$$

Proof. If $\mu(f+g) > \mu(f)$, we have $f \sim_\mu -g$. By Corollary 6.8,

$$R_r(f) = R_r(-g) = -R_r(g) \quad \text{and} \quad s_r(f) = s_r(-g) = s_r(g).$$

Hence,

$$y^{\lfloor s_r(f)/e_r \rfloor} R_r(f) + y^{\lfloor s_r(g)/e_r \rfloor} R_r(g) = y^{\lfloor s_r(f)/e_r \rfloor} \left(R_r(f) + R_r(g)\right) = 0.$$

Denote $h = f + g$. If $\mu(h) = \mu(f) = \mu(g)$, we have

$$\mu(f) = u_r(f) + s_r(f)\gamma_r = u_r(g) + s_r(g)\gamma_r = u_r(h) + s_r(h)\gamma_r.$$

By Lemma 5.26, $s_r(f) \equiv s_r(g) \equiv s_r(h) \pmod{e_r}$.

Thus, we can consider the divisions with remainder

$$s_r(f) = j_f e_r + \ell, \qquad s_r(g) = j_g e_r + \ell, \qquad s_r(h) = j_h e_r + \ell,$$

for some common non-negative integer $0 \le \ell < e_r$. Note that $j_f = \lfloor s_r(f)/e_r \rfloor$.

Take $u = \mu(f) - \ell\gamma_r = u_r(f) + j_f h_r \in \Gamma_{r-1}$. By Lemma 5.26,

$$x_r^{s_r(f)}\, p_r^{u_r(f)} = x_r^{\ell}\, p_r^{u}\, y_r^{j_f}, \quad x_r^{s_r(g)}\, p_r^{u_r(g)} = x_r^{\ell}\, p_r^{u}\, y_r^{j_g}, \quad x_r^{s_r(h)}\, p_r^{u_r(h)} = x_r^{\ell}\, p_r^{u}\, y_r^{j_h}. \tag{6.3}$$

On the other hand, the identity from (1.3) and Theorem 6.4 show that

$$x_r^{s_r(f)} p_r^{u_r(f)} R_r(f)(y_r) + x_r^{s_r(g)} p_r^{u_r(g)} R_r(g)(y_r) = x_r^{s_r(h)} p_r^{u_r(h)} R_r(h)(y_r).$$

By (6.3), this identity is equivalent to

$$y_r^{j_f} R_r(f)(y_r) + y_r^{j_g} R_r(g)(y_r) = y_r^{j_h} R_r(h)(y_r).$$

By Theorem 6.5, this identity still holds if we replace y_r with the indeterminate y. In this way we get precisely the identity predicted by the corollary. □

Computation of the residual ideal operator

We now establish a tight connection between the canonical operator $\mathcal{R}_\mu$ and the (non-canonical) operator R_r.

Theorem 6.10. *For any non-zero $f \in K[x]$,*

$$\mathcal{R}_\mu(f) = y_r^{\lceil s_r(f)/e_r \rceil} R_r(f)(y_r)\Delta.$$

Proof. By definition, an element in $\mathcal{R}_\mu(f)$ is of the form $H_\mu(g)$ for some $g \in K[x]$ such that $f \mid_\mu g$ and $\mu(g) = 0$. By Theorem 6.5,

$$H_\mu(g) = y_r^{s_r(g)/e_r} R_r(g)(y_r).$$

On the other hand, Corollary 6.8 shows that $s_r(f) \le s_r(g)$ and $R_r(f) \mid R_r(g)$.

Therefore, $H_\mu(g)$ belongs to $y_r^{\lceil s_r(f)/e_r \rceil} R_r(f)(y_r)\Delta$.

Conversely, if $q = \lceil s_r(f)/e_r \rceil$, then Theorem 6.4 shows that

$$y_r^q R_r(f)(y_r) = H_\mu(f) x_r^{qe_r - s_r(f)} p_r^{-qh_r - u_r(f)} \in \mathcal{R}_\mu(f),$$

because $qe_r \ge s_r(f)$ and p_r^α is a unit for all $\alpha \in \Gamma_{r-1}$. □

Residual polynomial of a constant

By Corollary 6.7, $R_r(1) = 1$. However, it is not so easy to compute the residual polynomial of a general constant.

For any $a \in K^*$, the polynomial $R_r(a) \in k_r[y]$ is constant, because

$$S_{\gamma_r}(a) = N_r(a) = \{(0, v(a))\},$$

so that $s_r(a) = s_r'(a) = 0$. By Lemma 6.3, $\deg(R_r(a)) = 0$.

Denote $\alpha = v(a) \in \Gamma_{-1}$. By definition,

$$R_r(a) = p_r^{-\alpha} H_\mu(a).$$

If $r = 0$, this amounts to $R_0(a) = \overline{a/\pi_0^\alpha} \in k^*$.

If $r > 0$, then Proposition 5.22 shows that

$$\pi_r^\alpha = \pi_{r-1}^\alpha \, Y_{r-1}^{L_{r-1}(\alpha)}.$$

Hence, $p_r^\alpha = p_{r-1}^\alpha z_{r-1}^{L_{r-1}(\alpha)}$, because p_r^α is the image under the canonical homomorphism $\mathcal{G}_{\mu_{r-1}} \to \mathcal{G}$ of the element

$$H_{\mu_{r-1}}\left(\pi_{r-1}^\alpha \, Y_{r-1}^{L_{r-1}(\alpha)}\right) = p_{r-1}^\alpha \, y_{r-1}^{L_{r-1}(\alpha)}.$$

By Proposition 2.2, $H_\mu(a)$ is also the image of $H_{\mu_{r-1}}(a)$ under the homomorphism $\mathcal{G}_{\mu_{r-1}} \to \mathcal{G}$. This leads to the following recurrence:

$$R_r(a) = z_{r-1}^{-L_{r-1}(\alpha)} R_{r-1}(a) = \cdots = z_{r-1}^{-L_{r-1}(\alpha)} \cdots z_0^{-L_0(\alpha)} R_0(a).$$

In particular, if $v(a) = 0$, we have $R_r(a) = R_0(a) = \overline{a} \in k^*$.

In spite of this difficulty, for certain "nice" polynomials we may guarantee that the residual polynomial is monic.

Lemma 6.11.

(1) If $f \in K[x]$ is monic and μ-minimal, then $R_r(f)$ is a monic polynomial.

(12) $R_r(\phi_r^s) = 1$ for any integer $s \geq 0$.

Proof. If $f \in K[x]$ is monic and μ-minimal, then Lemma 1.26 shows that the leading monomial of the ϕ_r-expansion of f is ϕ_r^ℓ, with $\ell = s_r'(f)$.

Hence, for $d = (\ell - s_r(f))/e_r = \deg(R_r(f))$, we have

$$s_d = \ell, \qquad a_{s_d} = 1,$$

with the notation of section 6.1. Hence, $c_d = p_r^{-\mu_{r-1}(1)} H_\mu(1) = 1$.

Finally, for any integer $s \geq 0$, $S_{\gamma_r}(\phi_r^s) = N_r(\phi_r^s) = \{(s, 0)\}$, so that $R_r(\phi_r^s)$ is a constant polynomial.

On the other hand, ϕ_r^s is monic and μ-minimal because it satisfies the conditions of Lemma 1.26. By the previous item $R_r(\phi_r^s) = 1$. □

Existence of polynomials with a prescribed residual polynomial

We end this section with a pair of useful results. The first one states that the decomposition of Theorem 6.4 is unique, in a certain sense.

The second one establishes the existence of polynomials f with prescribed values of $s_r(f)$, $u_r(f)$ and $R_r(f)$.

Lemma 6.12. *Consider two polynomials $\varphi, \psi \in k_r[y]$ such that $\varphi(0) \neq 0$, $\psi(0) \neq 0$. Suppose that for two pairs (s, u), $(s', u') \in \mathbb{Z}_{\geq 0} \times \Gamma_{r-1}$ we have*

$$x_r^s \, p_r^u \, \varphi(y_r) = x_r^{s'} \, p_r^{u'} \, \psi(y_r). \tag{6.4}$$

Then, $s = s'$, $u = u'$ and $\varphi = \psi$.

Proof. Since $\varphi(y_r)$ and $\psi(y_r)$ have degree zero in $\mathcal{G}$, the equality (6.4) implies

$$s\gamma_r + u = \deg(x_r^s\, p_r^u) = \deg(x_r^{s'}\, p_r^{u'}) = s'\gamma_r + u'.$$

Suppose $s \leq s'$. By Lemma 5.26, there exists an integer $j \geq 0$ satisfying

$$s' = s + je_r, \quad u' = u - jh_r, \quad x_r^{s'}\, p_r^{u'} = x_r^s\, p_r^u\, y_r^j.$$

Hence, (6.4) implies

$$\varphi(y_r) = y_r^j\, \psi(y_r).$$

By Theorem 6.5, we have $\varphi = y^j\, \psi$. Since neither φ nor ψ are divisible by y, we must have necessarily $j = 0$. This implies $s = s'$, $u = u'$ and $\varphi = \psi$. □

Proposition 6.13. *Let $(s, u) \in \mathbb{Z}_{\geq 0} \times \Gamma_{r-1}$, and $\psi \in k_r[y]$ a polynomial with $\psi(0) \neq 0$. Then, there exists a polynomial $f \in K[x]_{\mu\text{-at}}$ such that*

$$s_r(f) = s, \qquad u_r(f) = u, \qquad R_r(f) = \psi.$$

Proof. There is certainly $f \in K[x]$ such that $H_\mu(f)$ is the non-zero homogeneous element $x_r^s\, p_r^u\, \psi(y_r)$. Since $\mu(f) = u + s\gamma_r \in \Gamma_r$, this polynomial has attainable μ-value.

By Theorem 6.4, we have

$$x_r^s\, p_r^u\, \psi(y_r) = H_\mu(f) = x_r^{s_r(f)}\, p_r^{u_r(f)}\, R_r(f)(y_r).$$

The result follows from Lemma 6.12. □

6.3 Characterization of key polynomials for μ

In this section, we use the properties of the residual operators to characterize the key polynomials for μ.

Our main result, Proposition 6.16, reproduces Proposition 1.30 which was proven in [23] for an arbitrary valuation admitting key polynomials.

However, we shall give a complete proof of the result. On one hand, we add a significant property about the Newton polygon of a key polynomial; on the other hand, the result is crucial for the proof of Corollary 6.19, which contains an exclusive property of inductive valuations: their key polynomials are defectless polynomials over the henselization of (K, v) (see Theorem 8.6 too).

Let us first characterize the homogeneous prime elements in $\mathcal{G}$. By Theorem 6.5, the prime elements in Δ are those of the form $\psi(y_r)$ for $\psi \in k_r[y]$ an irreducible polynomial.

An element in Δ which is a prime in $\mathcal{G}$, is a prime in Δ, but the converse is not true. Let us discuss what primes in Δ remain prime in $\mathcal{G}$.

Lemma 6.14. *Let $\psi \in k_r[y]$ be a monic irreducible polynomial.*

(1) If $\psi \neq y$, then $\psi(y_r)$ is a prime element in $\mathcal{G}$.

(2) If $\psi = y$, then y_r is a prime element in $\mathcal{G}$ if and only if $e_r = 1$.

Proof. Suppose $\psi \neq y$. Since ψ is irreducible, we have $\psi(0) \neq 0$.
Suppose $\psi(y_r)$ divides the product of two homogeneous elements in $\mathcal{G}$. Say

$$\psi(y_r)H_\mu(f) = H_\mu(g)H_\mu(h).$$

Since $\psi(y_r)$ has degree zero, we have $\mu(f) = \mu(gh)$. By Theorem 6.4,

$$x_r^{s_r(f)}\, p_r^{u_r(f)}\, \psi(y_r)R_r(f)(y_r) = x_r^{s_r(gh)}\, p_r^{u_r(gh)}\, R_r(g)(y_r)R_r(h)(y_r).$$

By Lemma 6.12, we have $\psi\, R_r(f) = R_r(g)R_r(h)$. Since ψ is irreducible, it divides either $R_r(g)$ or $R_r(h)$, and this leads to $\psi(y_r)$ dividing either $H_\mu(g)$ or $H_\mu(h)$ in $\mathcal{G}$.

The element y_r is associate to $x_r^{e_r}$ in $\mathcal{G}$. Since x_r is a prime element, its e_r-th power is prime if and only if $e_r = 1$. □

Besides these prime elements belonging to Δ, we know that x_r is another prime element in $\mathcal{G}$, of degree γ_r.

The next result shows that there are no other homogeneous prime elements in $\mathcal{G}$, up to multiplication by units.

Proposition 6.15. *A polynomial $f \in K[x]$ is μ-irreducible if and only if one of the two following conditions is satisfied:*

(1) $s_r(f) = s_r'(f) = 1$.

(2) $s_r(f) = 0$ *and* $R_r(f)$ *is irreducible in* $k_r[y]$.

In the first case, $H_\mu(f)$ is associate to x_r. In the second case, to $R_r(f)(y_r)$.

Proof. Let us assume that Γ^{fg} is large enough to contain $\mu(f)$. By Theorem 6.25, the property of $R_r(f)$ being irreducible does not depend on the choice neither of Γ^{fg} nor its basis.

By Theorem 6.4,

$$H_\mu(f) = x_r^{s_r(f)}\, p_r^{u_r(f)}\, R_r(f)(y_r).$$

Since $p_r^{u_r(f)}$ is a unit and x_r is a prime, $H_\mu(f)$ is a prime if and only if one of the two following conditions is satisfied:

(i) $s_r(f) = 1$ and $R_r(f)(y_r)$ is a unit.

(ii) $s_r(f) = 0$ and $R_r(f)(y_r)$ is a prime in $\mathcal{G}$.

The homogeneous element of degree zero $R_r(f)(y_r)$ is a unit in $\mathcal{G}$ if and only if it is a unit in Δ. By Theorem 6.5, this is equivalent to $\deg(R_r(f)) = 0$, which is equivalent to $s_r'(f) = s_r(f)$, by Lemma 6.3. Thus, (i) is equivalent to (1), and $H_\mu(f)$ is associate to x_r in this case.

Since $R_r(f) \neq y$, (ii) is equivalent to (2) by Lemma 6.14. Clearly, $H_\mu(f)$ is associate to $R_r(f)(y_r)$ in this case. □

Putting together this characterization of μ-irreducibility with the characterization of μ-minimality from Proposition 1.26, we get the following characterization of key polynomials.

Proposition 6.16. *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) $\deg(\phi) = \deg(\phi_r)$ *and* $\phi \sim_\mu \phi_r$.

(2) $s_r(\phi) = 0$, $\deg(\phi) = e_r m_r \deg(R_r(\phi))$ *and* $R_r(\phi)$ *is irreducible in* $k_r[y]$.

In the first case, $\mathcal{R}(\phi) = y_r\Delta$. *In the second case,*

$R_r(\phi)$ *is monic,* $\mathcal{R}(\phi) = R_r(\phi)(y_r)\Delta$, *and* $N_r(\phi)$ *is one-sided of slope* $-\gamma_r$.

Proof. If ϕ satisfies (1), then ϕ is a key polynomial by Lemma 1.18.
Also, $\mathcal{R}(\phi) = \mathcal{R}(\phi_r) = y_r\Delta$ by Theorem 6.10, since $s_r(\phi_r) = 1$ and $R_r(\phi_r) = 1$.

If ϕ satisfies (2), then ϕ is μ-irreducible by Proposition 6.15. On the other hand, $\deg(R_r(\phi)) = s'_r(\phi)/e_r$ by Lemma 6.3; thus, $\deg(\phi) = s'_r(\phi)m_r$ and ϕ is μ-minimal too, by Proposition 1.26. Thus, ϕ is a key polynomial for μ.

Then, $R_r(\phi)$ is monic by Lemma 6.11, and $\mathcal{R}(\phi) = R_r(\phi)(y_r)\Delta$ by Theorem 6.10.

Also, $N_r(\phi) = S_{\gamma_r}(\phi)$ because the endpoints of both polygons coincide. In fact, since $S_{\gamma_r}(\phi) \subset N_r(\phi)$, it suffices to check that their endpoints have the same abscissas. Both left endpoints have abscissa 0, and the right endpoint of $N_r(\phi)$ has abscissa $\ell(N_r(\phi)) = \deg(\phi)/m_r = s'_r(\phi)$.

Since $s_r(\phi) = 0$ and $s'_r(\phi) > 0$, $N_r(\phi)$ is one-sided of slope $-\gamma_r$, according to Definition 3.3.

Conversely, suppose ϕ is a key polynomial for μ. Since ϕ is μ-minimal, it has

$$\deg(\phi) = s'_r(\phi)m_r, \qquad \mu(\phi) = \mu\left(\phi_r^{s'_r(\phi)}\right),$$

by Proposition 1.26.

Since ϕ is μ-irreducible, it satisfies one of the conditions of Proposition 6.15.

If $s_r(\phi) = s'_r(\phi) = 1$, we get $\deg(\phi) = m_r$. Also, if we write $\phi = \phi_r + a$, we must have $\mu(a) > \mu(\phi)$, because otherwise the point $(0, \mu(a))$ would belong to $S_{\gamma_r}(\phi)$, contradicting the property $s_r(\phi) = 1$. Thus, $\phi_r \sim_\mu \phi$, and ϕ satisfies (1).

If $s_r(\phi) = 0$ and $R_r(\phi)$ is irreducible in $k_r[y]$, then $\deg(R_r(\phi)) = s'_r(\phi)/e_r$ by Lemma 6.3. Thus, $\deg(\phi) = s'_r(\phi)m_r = e_r m_r \deg(R_r(\phi))$, and ϕ satisfies (2). □

Consider $\phi_0, \dots, \phi_r$ as key polynomials of $\mu_0, \dots, \mu_r$, respectively. Obviously, these key polynomials fall in the first case of Proposition 6.16.

Consider $\phi_1, \dots, \phi_r$ as key polynomials of $\mu_0, \dots, \mu_{r-1}$, respectively. By the definition of a MacLane chain, all these key polynomials fall in the second case of Proposition 6.16. This justifies the next observation.

Corollary 6.17. *The Newton polygon $N_i(\phi_{i+1})$ is one-sided of slope $-\gamma_i$, for all $0 \le i \le r$.*

Also, we may derive from Proposition 6.16 a crucial property of residual polynomials of key polynomials.

Corollary 6.18. *The residual polynomial $R_i(\phi_{i+1})$ is the minimal polynomial of z_i over k_i, for all $0 \le i < r$. In particular,*

$$\deg(R_i(\phi_{i+1})) = [k_{i+1} \colon k_i] = f_i.$$

Proof. By Proposition 6.16, $s_i(\phi_{i+1}) = 0$ and $R_i(\phi_{i+1})$ is monic and irreducible.

By Theorem 6.4, $H_{\mu_i}(\phi_{i+1})$ is associate to $R_i(\phi_{i+1})(y_i)$. By Proposition 2.2, the homomorphism $\mathcal{G}_{\mu_i} \to \mathcal{G}_{\mu_{i+1}}$ vanishes on these elements.

Therefore, $R_i(\phi_{i+1})(z_i) = 0$, because $R_i(\phi_{i+1})(z_i)$ is the image of $R_i(\phi_{i+1})(y_i)$ under this homomorphism. □

Finally, we deduce from these results a crucial property of key polynomials for inductive valuations.

Corollary 6.19. *Any key polynomial ϕ for an inductive valuation μ satisfies*

$$\deg(\phi) = e(\phi)f(\phi).$$

In particular, the valuation v_ϕ is the unique extension of v to the field K_ϕ.

Proof. Consider a MacLane chain of μ as in (5.1). By Proposition 6.16 we have two possibilities for a key polynomial ϕ for μ. Let us discuss separatedly each case.

Suppose $\deg(\phi) = \deg(\phi_r)$ and $\phi \sim_\mu \phi_r$. Then, Proposition 1.21 shows that

$$\Gamma_{v_\phi} = \Gamma_{\mu,\deg(\phi)} = \Gamma_{\mu,\deg(\phi_r)} = \Gamma_{v_{\phi_r}},$$

so that $e(\phi) = e(\phi_r)$.

Also, since $\mathcal{R}(\phi) = \mathcal{R}(\phi_r)$, Proposition 1.22 shows that $k_\phi \simeq k_{\phi_r}$, so that $f(\phi) = f(\phi_r)$. Hence, it suffices to prove the statement for ϕ_r. By (5.5) and (5.14) we have

$$e(\phi_r) = e_0 \cdots e_{r-1}, \qquad f(\phi_r) = f_0 \cdots f_{r-1}.$$

On the other hand, Proposition 6.16 and Corollary 6.18 show that

$$\deg(\phi_r) = e_{r-1}f_{r-1}m_{r-1} = \cdots = e_{r-1}f_{r-1} \cdots e_0f_0 = e(\phi_r)f(\phi_r).$$

Finally, suppose $\phi \not\sim_\mu \phi_r$. For an arbitrary $\gamma \in \mathbb{Q}\Gamma$, $\gamma > \gamma_r$, we may consider the augmented valuation $\mu' = [\mu; \phi, \gamma]$. Since $\phi \not\sim_\mu \phi_r$, we may extend our MacLane chain of μ to a MacLane chain of μ':

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r \overset{\phi,\gamma}{\longrightarrow} \mu'.$$

Hence, $\deg(\phi) = e(\phi)f(\phi)$ by the same argument we used for ϕ_r. □

This property is exclusive of inductive valuations. In section 8.4, we shall see an example of a valuation admitting a key polynomial ϕ such that v admits more than one extension to K_ϕ.

As an application of Corollary 6.19 let us see a kind of characterization of augmented valuations.

Lemma 6.20. *Suppose that the valuations $\mu, \mu^* \in \mathbb{V}^{\text{ind}}$ admit a common key polynomial, $\phi \in \mathrm{KP}(\mu) \cap \mathrm{KP}(\mu^*)$. Then,*

(1) $\mu(\phi) = \mu^*(\phi) \implies \mu = \mu^*$.

(2) $\mu(\phi) < \mu^*(\phi) \implies \mu^* = [\mu;\, \phi, \gamma]$, *with* $\gamma = \mu^*(\phi)$.

Proof. Since both semivaluations $v_{\mu,\phi}$, $v_{\mu^*,\phi}$, determined by μ, μ^*, respectively extend v to the field K_ϕ, Corollary 6.19 shows that $v_{\mu,\phi} = v_{\mu^*,\phi}$. In other words,

$$\mu(a) = \mu^*(a), \qquad \forall\, a \in K[x]_{\deg \phi}.$$

Item (1) follows immediately, since μ and μ^* coincide on ϕ-expansions.

If $\mu(\phi) < \mu^*(\phi)$, denote $\mu' = [\mu;\, \phi, \gamma]$, with $\gamma = \mu^*(\phi)$. Then, ϕ is a common key polynomial for μ' and μ^* and both valuations have the same value on ϕ. Thus, item (1) applied to these valuations shows that $\mu' = \mu^*$. □

This has an interesting consequence: any valuation in $\mathbb{V}$ which is "under" an inductive valuation, is inductive too.

Proposition 6.21. *Suppose that two valuations* $\mu^*, \mu \in \mathbb{V}$ *satisfy* $\mu^* < \mu$. *Suppose that* μ *is inductive, and consider a MacLane chain:*

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu.$$

Then, there exists an index $-1 \le i < r$ *such that*

$$\textit{either}\ \ \mu^* = \mu_i, \quad \textit{or}\ \ \mu^* = [\mu_i;\, \phi_{i+1}, \mu^*(\phi_{i+1})],$$

where we agree that $\mu_{-1} = \mu_{-\infty}$. *In particular,* μ^* *is inductive.*

Proof. Suppose that $\mu^* \neq \mu_i$ for all $-1 \le i < r$. Then, by Theorem 2.13, there exists an index i such that

$$\mu_i < \mu^* < \mu_{i+1}.$$

For any $a \in K[x]_{\deg(\phi_{i+1})}$, from $\phi_{i+1} \nmid_\mu a$ we deduce that $\mu_i(a) = \mu_{i+1}(a)$; hence, $\mu_i(a) = \mu^*(a) = \mu_{i+1}(a)$.

On the other hand, $\mu^*(\phi_{i+1}) < \mu_{i+1}(\phi_{i+1})$. In fact, otherwise, for any $f \in K[x]$ with ϕ_{i+1}-expansion $f = \sum_{0\le s} a_s \phi_{i+1}^s$ we would have

$$\mu^*(f) \ge \operatorname{Min}\left\{\mu^*\left(a_s\phi_{i+1}^s\right) \mid 0 \le s\right\} \ge \operatorname{Min}\left\{\mu_{i+1}\left(a_s\phi_{i+1}^s\right) \mid 0 \le s\right\} = \mu_{i+1}(f),$$

against our assumption.

Therefore, ϕ_{i+1} is a monic polynomial of minimal degree such that $\mu^*(\phi_{i+1}) < \mu_{i+1}(\phi_{i+1})$. By Proposition 2.9, ϕ_{i+1} is a key polynomial for μ^*. Hence, Lemma 6.20 shows that $\mu^* = [\mu_i;\, \phi_{i+1}, \mu^*(\phi_{i+1})]$. □

6.4 Recursive computation of the residual coefficients

From an algorithmic perspective, Corollaries 6.6 and 6.18 show how to construct the tower of residue fields

$$k = k_0 \subset k_1 \subset \cdots \subset k_r \tag{6.5}$$

solely from the knowledge of the irreducible polynomials

$$\psi_i := R_i(\phi_{i+1}) \in k_i[x].$$

Each field k_{i+1} may be constructed as $k_{i+1} = k_i[x]/(\psi_i)$, and we may identify the generator $z_i \in k_{i+1}$ with the class of x in this quotient.

In order to perform this construction, we need to compute the residual polynomials $R_r(f) = R_{\mu,\phi_r}(f) \in k_r[x]$ in a direct way, using only the tower (6.5) and the valuations $\mu_0, \dots, \mu_{r-1}$, but with no appeal to the valuation μ.

This requires the computation of the coefficients c_j introduced in Definition 6.1 by some direct formula in terms of all previous data. To this aim is devoted this section.

Definition 6.22. *For some $0 \le i < r$, let $a \in K[x]$ be a non-zero polynomial with attainable μ_i-value. We define*

$$\epsilon_i(a) = (z_i)^{L_i' s_i(a) - L_i(u_i(a))} \in k_{i+1}^*,$$

where $(s_i(a), u_i(a))$ is the left endpoint of $S_{\gamma_i}(a)$, the γ_i-component of $N_i(a)$.

Theorem 6.23. *Let $f \in K[x]$ with ϕ_r-expansion $f = \sum_{0 \le s} a_s \phi_r^s$.*

Suppose that f has attainable μ-value and let

$$R_r(f) = c_0 + c_1 y + \cdots + c_d y^d \in k_r[y]$$

be the residual polynomial of f. Then, for each j such that $c_j \ne 0$ we have

$$c_j = \begin{cases} \overline{a_{s_j} \pi_0^{-v(a_{s_j})}}, & \text{if } r = 0, \\ \epsilon_{r-1}(a_{s_j})\, R_{r-1}(a_{s_j})(z_{r-1}), & \text{if } r > 0, \end{cases}$$

where $s_j = s_r(f) + j e_r$.

Proof. Suppose $r = 0$. It suffices to prove the equality

$$p_0^{-v(a)} H_{\mu_0}(a) = \overline{a \pi_0^{-v(a)}}, \qquad \forall\, a \in K^*.$$

This is an immediate consequence of the identification

$$k^* \ \xrightarrow[\sim]{} \ k_0^*, \qquad \overline{b} \ \longmapsto \ H_{\mu_0}(b),$$

for all $b \in K^*$ with $\mu_0(b) = 0$.

Suppose $r > 0$. It suffices to prove the equality

$$p_r^{-\mu_{r-1}(a)} H_\mu(a) = \epsilon_{r-1}(a)\, R_{r-1}(a)(z_{r-1}), \qquad \forall\, a \in K[x]_{m_r}. \tag{6.6}$$

Take a non-zero $a \in K[x]_{m_r}$. By Theorem 6.4,

$$H_{\mu_{r-1}}(a) = x_{r-1}^s p_{r-1}^u R_{r-1}(a)(y_{r-1}), \quad s = s_{r-1}(a_{s_j}),\ u = u_{r-1}(a_{s_j}). \tag{6.7}$$

Since $\deg(a) < m_r = \deg(\phi_r)$, we have $\phi_r \nmid_\mu a$, and Proposition 2.2 shows that $\mu_{r-1}(a) = \mu(a)$. Hence, $H_\mu(a)$ is the image of $H_{\mu_{r-1}}(a)$ under the canonical homomorphism $\mathcal{G}_{\mu_{r-1}} \to \mathcal{G}$.

By applying this homomorphism to the identity (6.7),we get

$$H_\mu(a) = x^s_{r-1} p^u_{r-1} R_{r-1}(a)(z_{r-1}).$$

Hence, the claimed identity (6.6) is equivalent to:

$$p_r^{-\mu_{r-1}(a)} x^s_{r-1} p^u_{r-1} = \epsilon_{r-1}(a) = (z_{r-1})^{L'_{r-1}\, s - L_{r-1}(u)}.$$

Since $\mu_{r-1}(a) = u + s\gamma_{r-1}$, this identity follows from Proposition 5.24, by applying $H_{\mu_{r-1}}$ to a similar identity between the corresponding rational functions. □

Another crucial application of this recursive construction of the residual coefficients is the design of a concrete algorithm to compute polynomials in $K[x]$ with a prescribed residual polynomial. More precisely, to make effective the result of Proposition 6.13.

In particular, this algorithm may be used to construct key polynomials ϕ such that $\mathcal{R}(\phi)$ is a prescribed maximal ideal of Δ. In other words, to make effective the bijection of Theorem 1.32.

6.5 Dependence of R_r on the choice of Γ^{fg} and its basis

Let $\Gamma'_{-1} \subset \Gamma$ be another finitely-generated subgroup satisfying the conditions of Definition 5.9, and let $\iota'_{0,1}, \dots \iota'_{0,k'}$ be a $\mathbb{Z}$-basis of Γ'_{-1}.

With respect to these choices, let

$$\begin{aligned} x'_i,\, y'_i,\, (p'_i)^\alpha &\in \mathcal{G}_{\mu_i}, && 0 \le i \le r, \\ z'_i &\in \mathcal{G}^*_{\mu_{i+1}}, && 0 \le i < r, \end{aligned}$$

be the corresponding elements described in Definitions 5.25 and 5.27.

The choice of two subgroups Γ_{-1}, Γ'_{-1}, and respective bases in them, determines a family of group homomorphisms:

$$\tau_i \colon \Gamma_{i-1} \cap \Gamma'_{i-1} \longrightarrow k_i^*, \qquad \alpha \mapsto (p'_i)^\alpha / p_i^\alpha, \qquad 0 \le i \le r.$$

In fact, this quotient $(p'_i)^\alpha / p_i^\alpha$ of two units belongs to

$$\mathcal{G}^*_{\mu_i} \cap \Delta_i = \Delta_i^* = k_i^*.$$

Caution! The following natural diagrams do not commute!

$$\begin{array}{ccc} \Gamma_{i-1} & \subset & \Gamma_i \\ p_i \downarrow & & \downarrow p_{i+1} \\ \mathcal{G}^*_{\mu_i} & \longrightarrow & \mathcal{G}^*_{\mu_{i+1}} \end{array} \qquad\qquad \begin{array}{ccc} \Gamma_{i-1} \cap \Gamma'_{i-1} & \subset & \Gamma_i \cap \Gamma'_i \\ \tau_i \downarrow & & \downarrow \tau_{i+1} \\ k_i^* & \subset & k_{i+1}^* \end{array}$$

In fact, by applying $H_{\mu_{i+1}}$ to the identity of Proposition 5.22 we get

$$p_{i+1}^{\alpha} = p_i^{\alpha}\, z_i^{L_i(\alpha)}.$$

From this, we deduce

$$\frac{\tau_{i+1}(\alpha)}{\tau_i(\alpha)} = \frac{(p'_{i+1})^{\alpha}\, p_i^{\alpha}}{(p'_i)^{\alpha}\, p_{i+1}^{\alpha}} = \frac{(z'_i)^{L'_i(\alpha)}}{z_i^{L_i(\alpha)}}.$$

Lemma 6.24. *For all $0 \le i \le r$, we have*

$$x'_i = x_i, \qquad y'_i = \tau_i(-h_i) y_i.$$

In particular, $z'_i = \tau_i(-h_i) z_i$ for $0 \le i < r$.

Proof. The first statement is obvious: $x'_i = H_{\mu_i}(\phi_i) = x_i$.

By the construction of the finitely-generated subgroups, h_i belongs to $\Gamma_{i-1} \cap \Gamma'_{i-1}$. Then, from $y'_i = (x'_i)^{e_i}(p'_i)^{-h_i}$, $y_i = x_i^{e_i}\, p_i^{-h_i}$, we deduce $y_i = \tau_i(h_i) y'_i$. □

Theorem 6.25. *Let R'_r be the residual polynomial operator associated with the choice of Γ'_{-1} and its basis.*

Let $f = \sum_{0 \le s} a_s \phi_r^s$ be the ϕ_r-expansion of a non-zero polynomial having attainable μ-value for Γ^{fg} and $(\Gamma')^{\mathrm{fg}}$. Then,

$$R_r(f)(y) = \xi\, R'_r(f)(\zeta y),$$

for $\xi = \tau_r\left(u_r(f)\right)$, $\zeta = \tau_r\left(-h_r\right) \in k_r^*$.

Proof. Let us denote for simplicity $s = s_r(f)$, $u = u_r(f)$. By Theorem 6.4,

$$x_r^s\, p_r^u\, R_r(f)(y_r) = H_{\mu}(f) = (x'_r)^s\, (p'_r)^u\, R'_r(f)(y'_r).$$

By Lemma 6.24, this is equivalent to

$$R_r(f)(y_r) = \tau_r(u)\, R'_r(f)\, (\tau_r(-h_r) y_r)\,.$$

By Theorem 6.5, the same identity holds in $k_r[y]$ if we replace y_r with the indeterminate y. This proves the lemma. □

6.6 Dependence of R_r on the choice of an optimal MacLane chain

In this section, we discuss the variation of the elements x_r, y_r, z_r, $p_{r+1}^{\alpha} \in \mathcal{G}$, and the operators S_{γ_r}, R_r, when we consider different optimal MacLane chains.

We saw in Proposition 5.7 that two optimal MacLane chains of the valuation μ have the same length r, the same intermediate valuations $\mu_0, \ldots, \mu_r$, and the same values $\gamma_0, \ldots, \gamma_r \in \mathbb{Q}\Gamma$. They may differ only in the choice of the key polynomials:

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu.$$

$$\mu_{-\infty} \overset{\phi_0^*,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1^*,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1}^*,\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r^*,\gamma_r}{\longrightarrow} \mu_r = \mu,$$

which must be related as follows:

$$\phi_i^* = \phi_i + a_i, \qquad \deg(a_i) < m_i, \qquad \mu_i(a_i) \geq \gamma_i, \quad 0 \leq i \leq r.$$

In particular, both chains support the same invariants

$$m_i,\, e_i,\, f_{i-1} \in \mathbb{Z}_{\geq 0}, \qquad h_i \in \Gamma_{i-1}, \qquad 0 \leq i \leq r,$$

where we agree formally that $f_{-1} = 1$.

Lemma 6.26. *If $\phi_r^* \not\sim_\mu \phi_r$, then $e_r = 1$ and a_r has attainable μ-value.*

Proof. Since $\phi_r \nmid_\mu a_r$, we have $\mu(a_r) = \mu_{r-1}(a_r) \in \Gamma_{\mu_{r-1}}$ by Proposition 2.2.

Thus, the condition $\phi_r^* \not\sim_\mu \phi_r$, which is equivalent to $\mu(a_r) = \mu(\phi_r) = \gamma_r$, leads to $\gamma_r \in \Gamma_{\mu_{r-1}}$. This implies $e_r = 1$, and $\mu(a_r) = \gamma_r \in \Gamma_r = \Gamma_{r-1}$. □

We use the standard notation for all data and operators attached to the upper MacLane chain and we mark with a superscript $(\,)^*$ all data and operators attached to the lower one.

Theorem 6.27. *With the above notation.*

(1) $p_{i,j}^* = p_{i,j}$ *for all* $0 \leq i \leq r+1,\ 1 \leq j \leq k$.

(2) If $\phi_r^* \sim_\mu \phi_r$, *then* $x_r^* = x_r, \quad y_r^* = y_r, \quad S_{\gamma_r}^* = S_{\gamma_r}, \quad R_r^* = R_r$.

(3) If $\phi_r^* \not\sim_\mu \phi_r$, *then* $x_r^* = x_r + p_r^{h_r}\eta, \quad y_r^* = y_r + \eta$, *where* $\eta = R_r(a_r) \in k_r^*$.

Moreover, for a non-zero $g \in K[x]$ with attainable μ-value we have

$$y^{s_r(g)} R_r(g)(y) = (y+\eta)^{s_r^*(g)} R_r^*(g)(y+\eta). \tag{6.8}$$

In particular, $s_r^*(g) = \operatorname{ord}_{y+\eta}(R_r(g))$.

Proof. Since the choice of $\pi_{0,1}, \ldots \pi_{0,k} \in K^*$ had nothing to do with the MacLane chains, we have $p_{0,j}^* = H_\mu(\pi_{0,j}) = p_{0,j}$ for all j.

Suppose we have $p_{i,j}^* = H_\mu(\pi_{i,j}) = p_{i,j}$ for all j, and all $0 \leq i \leq r$. In particular,

$$(p_r^*)^\alpha = p_r^\alpha, \qquad \forall\, \alpha \in \Gamma_{r-1}.$$

Case $\phi_r^* \sim_\mu \phi_r$. By definition,

$$x_r^* = H_\mu(\phi_r^*) = H_\mu(\phi_r) = x_r.$$

This leads to $y_r^* = y_r$ and $p_{r+1,j}^* = p_{r+1,j}$ for all j, by the recurrent definition of these rational functions (Definition 5.16).

Case $\phi_r^* \not\sim_\mu \phi_r$. Lemma 6.26 shows that $e_r = 1$ and a_r has atainable μ-value.

Since $\deg(a_r) < m_r$, we get

$$s_r(a_r) = 0, \qquad u_r(a_r) = \mu_{r-1}(a_r) = \mu(a_r) = \gamma_r = h_r.$$

By Theorem 6.4,

$$H_\mu(a_r) = p_r^{h_r} R_r(a_r) = p_r^{h_r}\eta.$$

Hence, by using (1.3), we have in this case

$$x_r^* = H_\mu(\phi_r^*) = (H_\mu(\phi_r) + H_\mu(a_r)) = x_r + p_r^{h_r}\eta,$$

which leads to $y_r^* = x_r^*(p_r^*)^{-h_r} = x_r p_r^{-h_r} + \eta = y_r + \eta$.

Also, $e_r = 1$ implies $\ell_{r,j} = 0$, $\ell'_{r,j} = 1$ for all j, by (5.9). Thus,

$$\pi^*_{r+1,j} = \pi^*_{r,j}, \qquad \pi_{r+1,j} = \pi_{r,j}, \quad 1 \le j \le k,$$

by the definition of these rational functions (Definition 5.16).

Hence, $p^*_{r+1,j} = p^*_{r,j} = p_{r,j} = p_{r+1,j}$ for all j.

Finally, let us prove the statements concerning S_{γ_r} and R_r in items (2) and (3).

Let $g \in K[x]$ be a non-zero polynomial with attainable μ-value.

Case $\phi_r^* \sim_\mu \phi_r$. We have already seen that $x_r^* = x_r$, $y_r^* = y_r$, and $(p_r^*)^\alpha = p_r^\alpha$ for all $\alpha \in \Gamma_{r-1}$. By Theorem 6.4,

$$x_r^{s_r(g)}\, p_r^{u_r(g)} R_r(g)(y_r) = H_\mu(g) = x_r^{s_r^*(g)}\, p_r^{u_r^*(g)} R_r^*(g)(y_r).$$

By Lemma 6.12, $s_r^*(g) = s_r(g)$, $u_r^*(g) = u_r(g)$, and $R_r^*(g) = R_r(g)$.

This proves $R_r^* = R_r$ already. Also, $S^*_{\gamma_r}(g)$ and $S_{\gamma_r}(g)$ have the same left endpoint $(s_r(g), u_r(g))$ and the same slope $-\gamma_r$; thus, these segments coincide if their right endpoints have the same abscissa. This follows from Lemma 6.3:

$$s_r'(g) = e_r \deg(R_r(g)) + s_r(g) = e_r \deg(R_r^*(g)) + s_r^*(g) = (s_r^*)'(g).$$

Hence $S^*_{\gamma_r}(g) = S_{\gamma_r}(g)$.

This argument works for an arbitrary non-zero $f \in K[x]$, by enlarging Γ^{fg} to ensure that $\mu(f) \in \Gamma^{\mathrm{fg}}_\mu$. Therefore, $S^*_{\gamma_r} = S_{\gamma_r}$, and this ends the proof of item (2).

Case $\phi_r^* \not\sim_\mu \phi_r$. Recall that $e_r = 1$ and $(p_r^*)^\alpha = p_r^\alpha$ for all $\alpha \in \Gamma_{r-1}$. By Theorem 6.4,

$$x_r^{s_r(g)}\, p_r^{u_r(g)} R_r(g)(y_r) = H_\mu(g) = (x_r^*)^{s_r^*(g)}\, p_r^{u_r^*(g)} R_r^*(g)(y_r^*).$$

Since $x_r = p_r^{h_r} y_r$ and $x_r^* = p_r^{h_r} y_r^* = p_r^{h_r}(y_r + \eta)$, we deduce

$$y_r^{s_r(g)} p_r^{u_r(g)+s_r(g)h_r} R_r(g)(y_r) = (y_r+\eta)^{s_r^*(g)} p_r^{u_r^*(g)+s_r^*(g)h_r} R_r^*(g)(y_r+\eta).$$

Since $u_r(g) + s_r(g)h_r = \mu(g) = u_r^*(g) + s_r^*(g)h_r$, we may drop the powers of p_r:

$$y_r^{s_r(g)} R_r(g)(y_r) = (y_r+\eta)^{s_r^*(g)} R_r^*(g)(y_r+\eta).$$

This proves (6.8), as a consequence of Theorem 6.5.

Since $R_r^*(g)$ is not divisible by y, the polynomial $R_r^*(g)(y+\eta)$ is not divisible by $y+\eta$. Hence, $s_r^*(g) = \mathrm{ord}_{y+\eta}(R_r(g))$. □

Chapter 7

Structure of the graded algebra

We keep dealing with an inductive valuation $\mu \in \mathbb{V}^{\text{ind}}$ equipped with a MacLane chain of length r as in (5.1), and the corresponding data described in sections 5.2 and 5.3.

Throughtout this chapter we use the notation:

$$\mathcal{G} = \mathcal{G}_\mu, \qquad \Delta = \Delta_\mu, \qquad \kappa = k_r, \qquad \mathcal{R} = \mathcal{R}_\mu.$$

We recall that $\kappa \subset \Delta$ is the algebraic closure of k, and the maximal subfield of Δ.

In this chapter, we study the structure of $\mathcal{G}$ as a $\mathcal{G}_v$-algebra.

7.1 Generators and relations for $\mathcal{G}$

From the fact that μ restricted to K coincides with v, we deduce a natural embedding of graded k-algebras:

$$\mathcal{G}_v \hookrightarrow \mathcal{G}, \qquad H_v(a) \longmapsto H_\mu(a), \quad \forall\, a \in K.$$

This embedding extends in an obvious way to an embedding of graded κ-algebras:

$$\mathcal{G}_v \otimes_k \kappa \hookrightarrow \mathcal{G}, \qquad H_v(a) \otimes c \longmapsto c\, H_\mu(a).$$

By Theorem 6.5, we deduce an embedding of Δ-algebras:

$$\mathcal{G}_v \otimes_k \Delta \hookrightarrow \mathcal{G}, \qquad H_v(a) \otimes \psi(y_r) \longmapsto \psi(y_r)\, H_\mu(a),$$

for all $\psi \in \kappa[y]$.

By identifying these algebras $\mathcal{G}_v \otimes_k \kappa$, $\mathcal{G}_v \otimes_k \Delta$ with their images in $\mathcal{G}$, we clearly have:

$$\mathcal{G}_v \otimes_k \Delta = (\mathcal{G}_v \otimes_k \kappa)\,[y_r].$$

Recall the elements $x_0, \dots, x_r \in \mathcal{G}$, introduced in Definitions 5.25 and 5.27.
They are homogeneous elements of degree $\gamma_0, \dots, \gamma_r$, respectively.
Also, $x_0, \dots, x_{r-1}$ are units, while x_r is a prime element.

Lemma 7.1. *For any $\alpha \in \Gamma_{r-1}$, we have $p_r^\alpha \in (\mathcal{G}_v \otimes_k \kappa)\,[x_0, \dots, x_{r-1}]$.*

Proof. By definition, $p_0^\beta \in \mathcal{G}_v$ for all $\beta \in \Gamma_{-1}$. For $r > 0$, we may assume that $p_{r-1}^\beta \in (\mathcal{G}_v \otimes_k \kappa)[x_0, \dots, x_{r-2}]$ for all $\beta \in \Gamma_{r-2}$, by a recurrent argument.

By Lemma 1.24, there exists $a \in K[x]$ with $\deg(a) < m_r$ such that $H_\mu(a) = p_r^\alpha$. Since $\mu(a) = \mu_{r-1}(a)$, this element $H_\mu(a)$ is the image of $H_{\mu_{r-1}}(a)$ under the canonical homomorphism $\mathcal{G}_{\mu_{r-1}} \to \mathcal{G}$.

By Theorem 6.4, $H_{\mu_{r-1}}(a) = x_{r-1}^s p_{r-1}^u R_{r-1}(a)(y_{r-1})$, for certain $s \in \mathbb{Z}_{\geq 0}$, $u \in \Gamma_{r-2}$. Hence, the image of this element under the homomorphism $\mathcal{G}_{\mu_{r-1}} \to \mathcal{G}$ is

$$H_{\mu_{r-1}}(a) \;\mapsto\; x_{r-1}^s p_{r-1}^u R_{r-1}(a)(z_{r-1}) \in (\mathcal{G}_v \otimes_k \kappa)[x_0, \dots, x_{r-1}],$$

because $R_{r-1}(a)(z_{r-1}) \in \kappa$. □

Theorem 7.2. *The graded algebra of μ admits the following description:*

$$\mathcal{G} = (\mathcal{G}_v \otimes_k \kappa)[y_r, x_0, \dots, x_r] = (\mathcal{G}_v \otimes_k \Delta)[x_0, \dots, x_r],$$

where $y_r, x_0, \dots, x_r$ have degree 0, γ_0, $\dots$, γ_r, respectively.

Moreover. these elements satisfy the relations

$$x_0^{e_0} = p_0^{h_0} z_0, \;\dots,\; x_{r-1}^{e_{r-1}} = p_{r-1}^{h_{r-1}} z_{r-1}, \quad x_r^{e_r} = p_r^{h_r} y_r. \tag{7.1}$$

Proof. Let $H_\mu(g)$ be a homogeneous element in $\mathcal{G}$, for some non-zero $g \in K[x]$. Lemma 5.12 shows the existence of $a \in K^*$ such that ag has attainable μ-value. By Theorem 6.4,

$$H_\mu(g) = H_\mu(a^{-1}) H_\mu(ag) = H_\mu(a)^{-1}\, x_r^s\, p_r^u\, R_r(ag)(y_r),$$

for certain $s \in \mathbb{Z}_{\geq 0}$, $u \in \Gamma_{r-1}$.

Since $R_r(ag)(y_r)$ belongs to Δ, Lemma 7.1 shows that $H_\mu(g)$ is a polynomial in $x_0, \dots, x_r$ with coefficients in $\mathcal{G}_v \otimes_k \Delta$.

Let us check that (7.1) are the only relations satisfied by $x_0, \dots, x_r$ as generators of $\mathcal{G}$ as a $(\mathcal{G}_v \otimes_k \Delta)$-algebra. Suppose we have a homogeneous relation

$$\sum\nolimits_{(m_0,\dots,m_r)\in\mathbb{N}^r} a_{m_0,\dots,m_r}\, x_0^{m_0} \cdots x_r^{m_r} = 0, \quad a_{m_0,\dots,m_r} \in \mathcal{G}_v \otimes_k \Delta.$$

By applying (7.1), we may assume that $0 \leq m_i < e_i$, for $1 \leq i \leq r$.

Then, this sum cannot have two different monomials, In fact,

$$\begin{aligned} \deg(a\, x_0^{m_0} \cdots x_r^{m_r}) &= \deg(b\, x_0^{n_0} \cdots x_r^{n_r}) \\ &\Longrightarrow \;\; (m_0 - n_0)\gamma_0 + \cdots + (m_r - n_r)\gamma_r = \deg(b) - \deg(a) \in \Gamma. \end{aligned}$$

From $(m_r - n_r)\gamma_r \in \Gamma_{\mu_{r-1}}$, we deduce $m_r \equiv n_r \pmod{e_r}$, and this implies $m_r = n_r$ by our assumption on the exponents. By iterating this argument, we conclude that $m_i = n_i$ for all i.

Thus, our relation takes the form $a\, x_0^{m_0} \cdots x_r^{m_r} = 0$. Since $\mathcal{G}$ is an integral domain, we necessarily have $a = 0$. □

By Lemma 6.24, the generators $x_0, \dots, x_r$ do not depend on the choice of the finitely-generated subgroup Γ^{fg}.

If the group $\Gamma = \Gamma_v$ is finitely generated, then Γ_μ is finitely generated too, and we could decribe $\mathcal{G}$ as a polynomial ring over Δ, on indeterminates representing a $\mathbb{Z}$-basis of the group.

Actually, since $K[x]$ is not a field, we have to distinguish those values of Γ_μ which are not represented by units in $\mathcal{G} = \mathrm{gr}_\mu(K[x])$.

These values are determined in Lemma 9.1, for an arbitrary valuation admitting key polynomials. For our inductive valuation μ equipped with a MacLane chain of length r, that result can be stated as follows:

Lemma 7.3. *For any $\alpha \in \Gamma_\mu$, we have*

$$\big(\mathcal{P}(\alpha)/\mathcal{P}^+(\alpha)\big) \cap \mathcal{G}^* \neq \emptyset \iff \alpha \in \Gamma_{\mu_{r-1}}.$$

Hence, we may use a basis of $\Gamma_{\mu_{r-1}}$ to parameterize the homogeneous parts of the graded algebra corresponding to values which admit units, and add an specific description of the rest of homogenous parts.

Theorem 7.4. *Suppose that $\Gamma = \Gamma^{\mathrm{fg}}$ is finitely generated. The graded algebra of μ admits the following description:*

$$\mathcal{G} = \kappa\left[y_r, p_{r,1}^{\pm 1}, \dots, p_{r,k}^{\pm 1}\right][x_r] = \Delta\left[p_{r,1}^{\pm 1}, \dots, p_{r,k}^{\pm 1}\right][x_r].$$

The elements $y_r, p_{r,1}, \dots, p_{r,k}$ are algebraically independent over κ.

The element x_r is algebraic over $\Delta\left[p_{r,1}^{\pm 1}, \dots, p_{r,k}^{\pm 1}\right]$, and it has minimal equation $x_r^{e_r} = p_r^{h_r} y_r$.

Proof. Theorem 6.4 shows that x_r, y_r, and $\left\{p_{r,j}^{\pm 1} \mid 1 \le j \le k\right\}$ generate $\mathcal{G}$ as an κ-algebra.

Let us prove that $y_r, p_{r,1}, \dots, p_{r,k}$ are algebraically independent over κ. Suppose

$$\sum_{n,\, m_1,\dots,m_k \in \mathbb{Z}_{\ge 0}} c_{n,m_1,\dots,m_k}\, y_r^n\, p_{r,1}^{m_1} \dots p_{r,k}^{m_k} = 0, \qquad c_{n,m_1,\dots,m_k} \in \kappa. \tag{7.2}$$

and let us show that all coefficients $c_{n,m_1,\dots,m_k}$ vanish.

We may suppose that (7.2) is a homogeneous equation. Since $\deg(y_r) = 0$ and

$$\deg\left(p_{r,1}^{m_1} \dots p_{r,k}^{m_k}\right) = m_0\, \iota_{r,1} + \dots + m_k\, \iota_{r,k} \in \Gamma_{r-1} = \Gamma_{\mu_{r-1}},$$

the vector $(m_1, \dots, m_k)$ is uniquely determined by the degree of the equation, because $\iota_{r,1}, \dots, \iota_{r,k}$ is a basis of Γ_{r-1}. Hence, (7.2) takes the form:

$$p_{r,1}^{m_1} \dots p_{r,k}^{m_k} \sum_{n \in \mathbb{Z}_{\ge 0}} c_{n,m_1,\dots,m_k}\, y_r^n = 0,$$

and this implies $c_{n,m_1,\dots,m_k} = 0$ for all n, by Theorem 6.5.

Finally, let us show that the equation $x_r^{e_r} = p_r^{h_r} y_r$ is minimal. Suppose

$$\epsilon_0 + \epsilon_1\, x_r + \dots + \epsilon_m\, x_r^m = 0, \quad m < e_r, \quad \epsilon_i \in \Delta\left[\{p_{r,j}^{\pm 1} \mid 1 \le j \le k\}\right].$$

All terms in this equation have different degree. In fact,

$$\deg(\epsilon_i\, x_r^i) = \deg(\epsilon_j\, x_r^j) \implies (i-j)\gamma_r = \deg(\epsilon_j) - \deg(\epsilon_i) \in \Gamma_{r-1},$$

and this implies $e_r \mid (i-j)$, leading to $i = j$.

Hence, $\epsilon_i\, x_r^i = 0$, for all i, which implies $\epsilon_i = 0$ for all i. □

PART III

Defectless polynomials over henselian fields

Chapter 8

Lifting inductive valuations to the henselization

8.1 Henselization of a valued field

A valued field (K, v) is said to be *henselian* if v admits a unique extension to any algebraic extension of K.

This condition is equivalent to the fact that (K, v) satisfies Hensel's lemma.

Hensel's lemma. Let $f, g, h \in \mathcal{O}[x]$ satisfy $\overline{f} = \overline{g}\,\overline{h}$, with $\overline{g}$, $\overline{h}$ relatively prime in $k[x]$. Then, there exist $g_1, h_1 \in \mathcal{O}[x]$ with

$$f = g_1 h_1, \qquad \overline{g}_1 = \overline{g}, \qquad \overline{h}_1 = \overline{h}, \qquad \deg(g_1) = \deg(g).$$

The completion of a valued field of rank 1 is henselian, but this is not true for valued fields of higher rank.

However, there is a *henselization* of (K, v), which is a kind of minimal henselian extension (K^h, v^h), satisfying a certain universal property.

This henselization plays a crucial role in the study of valuations of rank greater than one, analogous to the role played by the completion for valuations of rank one.

We may realize a henselization of (K, v) as a subfield of any given separable closure K^s of K. By fixing any extension $\tilde{v}$ of v to K^s, we may consider the *decomposition subgroup*

$$D_{\tilde{v}} = \{\sigma \in \mathrm{Gal}(K^s/K) \mid \tilde{v} \circ \sigma = \tilde{v}\},$$

which is a closed subgroup of $\mathrm{Gal}(K^s/K)$. Then, we may define $K^h \subset K^s$ to be the fixed field of $D_{\tilde{v}}$. We consider on K^h the valuation v^h obtained by restriction of $\tilde{v}$.

This valued field (K^h, v^h) has the following properties:

- (K^h, v^h) is henselian.
- A different choice of $\tilde{v}$ leads to a conjugate decomposition group; hence to a K-conjugate subfield of K^s.
- (K, v) is henselian if and only if $K = K^h$.

- If (L, v') is a henselian extension of (K, v), then there exists a unique K-embedding $\iota\colon K^h \hookrightarrow L$ such that v^h is the restriction of v' to K^h.

- v^h/v is an immediate extension.

Suppose that v has rank one. The completion K_v of K with respect to the v-adic topology is henselian. Hence, there is an embedding of valued fields $K^h \subset K_v$. Since K is dense in K_v, we deduce that K is dense in K^h.

For valuations of higher rank this property does not hold. We shall see a concrete example in section 8.4.

Finite extensions of K and K^h

Let $F \in K^h[x]$ be a monic irreducible polynomial, and let $K_F = K^h[x]/(F)$ be the finite extension of K^h obtained by adjoining a root of F. Since K^h is henselian, the valuation v^h admits a unique extension w to K_F. Let us denote

$$e(F) = e(w/v^h), \qquad f(F) = f(w/v^h).$$

We have the following numerical relationship:

$$\deg(F) = e(F)f(F)d(F),$$

where $d(F)$ is a natural number called the *defect* of F.

If the characteristic of k_v is zero, the defect is trivial: $d(F) = 1$.

If the characteristic of k_v is $p > 0$, the defect is a power of p.

If $d(F) = 1$ we say that F is *defectless*.

Now, let $f \in K[x]$ be a monic irreducible polynomial, and let L be the extension of K obtained by adjoining a root of f.

Suppose f separable. Let

$$f = F_1 \cdots F_m$$

be the factorization of f into a product of monic irreducible polynomials in $K^h[x]$. Then, there are m extensions $w_1, \ldots, w_m$ of v to L, and they satisfy:

$$e(w_i/v) = e(F_i), \qquad f(w_i/v) = f(F_i), \qquad 1 \leq i \leq m.$$

In particular,

$$\sum_{i=1}^{m} e(w_i/v)f(w_i/v) \leq [L\colon K]. \tag{8.1}$$

On the other hand, if f is purely inseparable, then v admits a unique extension to L.

8.2 Restricting valuations on polynomial rings

Denote the set of equivalence classes of valuations on $K[x]$ extending v by

$$\mathrm{Val}(K, v).$$

Let L/K be a field extension and let w be a valuation on L extending v.

By Chevalley's extension theorem [5, Thm. 3.1.1], the restriction mapping

$$\mathrm{res}\colon\ \mathrm{Val}\,(L, w) \longrightarrow \mathrm{Val}(K, v), \qquad \rho \longmapsto \mathrm{res}(\rho) = \rho_{|_{K[x]}}$$

is onto.

Definition 8.1. *Let $\rho \in \mathrm{Val}(L, w)$ and $\mu = \mathrm{res}(\rho) \in \mathrm{Val}(K, v)$. We say that the canonical embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ is a* strong isomorphism *if*

$$\forall\, F \in L[x],\ \exists\, f \in K[x] \quad \textit{such that} \quad \deg(f) = \deg(F) \quad \textit{and} \quad f \sim_\rho F.$$

This property may occur only when w/v is immediate. In fact, the condition of strong isomorphism restricted to polynomials of degree zero is equivalent to w/v immediate, by Lemma 1.10.

In section 8.4 we shall see an example of extension ρ/μ such that w/v is immediate and $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ is an isomorphism which is not strong.

Suppose that $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ is an isomorphism, and take $\phi \in K[x]$.

Then, ϕ is μ-irreducible if and only if it is ρ-irreducible. In fact, $H_\mu(\phi)$ is prime if and only if its image $H_\rho(\phi)$ under the above isomorphism is prime.

If ϕ is ρ-minimal, then it is μ-minimal, but the converse implication is false.

However, if the isomorphism is strong and ϕ is μ-minimal, then it is ρ-minimal too. These arguments prove the following result.

Lemma 8.2. *Let $\rho \in \mathrm{Val}(L, w)$ and $\mu = \mathrm{res}(\rho) \in \mathrm{Val}(K, v)$. Suppose that the canonical embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ is a strong isomorphism. Then, a polynomial $\phi \in K[x]$ is a key polynomial for μ if and only if it is a key polynomial for ρ.*

Let us see a concrete example of strong isomorphism.

Lemma 8.3. *Suppose w/v is an immediate extension. Then, the canonical embedding*

$$\mathcal{G}_{\mu_{-\infty}} \hookrightarrow \mathcal{G}_{\mu_{-\infty,L}}$$

is a strong isomorphism.

Proof. Any polynomial $F \in L[x]$ is $\mu_{-\infty,L}$-equivalent to a monomial ξx^m, for some $\xi \in L$. By Lemma 1.10, there exists $c \in K$ such that $c \sim_{\mu_{-\infty,L}} \xi$. Hence, the polynomial $f = cx^m \in K[x]$ satisfies $f \sim_{\mu_{-\infty,L}} F$. □

We recall that for valuations on the polynomial ring $L[x]$ whose values are embedded into a common ordered group, there is partial ordering $\leq$ defined as:

$$\rho \leq \rho' \iff \rho(f) \leq \rho'(f), \quad \forall\, f \in L[x].$$

If L/K is algebraic, there are no "comparable" valuations in the fibers of the restriction mapping.

Lemma 8.4. *Suppose L/K is an algebraic extension, and ρ, $\rho' \in \mathrm{Val}(L, w)$ have values embedded in a common ordered group. Then,*

$$\mathrm{res}(\rho) = \mathrm{res}(\rho'), \quad \rho \leq \rho' \quad \Longrightarrow \quad \rho = \rho'.$$

Proof. Suppose that $\rho < \rho'$. Let $F \in L[x]$ be a polynomial of minimal degree such that $\rho(F) < \rho'(F)$. Since

$$\rho_{|L} = w = \rho'_{|L},$$

the degree of F is positive, and we can suppose that F is monic.

Then, F is irreducible because ρ and ρ' coincide on any possible factor of F of smaller degree.

The prime ideal $FL[x] \cap K[x]$ cannot be zero, because this would lead to an embedding of $K[x]$ into the field $L[x]/(F)$, which is algebraic over K.

Hence, there is a monic irreducible polynomial $f \in K[x]$ such that

$$FL[x] \cap K[x] = fK[x].$$

Let us write $f = F\,G$ for some monic polynomial $G \in L[x]$.

Since f has coefficients in K, we have $\rho(f) = \rho'(f)$ by our assumptions. Hence,

$$\rho(f) = \rho'(f) = \rho'(F\,G) = \rho'(F) + \rho'(G) > \rho(F) + \rho(G) = \rho(f).$$

This contradiction shows that $\rho = \rho'$. □

It is well known that in a fiber of the restriction mapping of an algebraic field extension we cannot find valuations ρ, ρ' satisfying $\mathcal{O}_\rho \subset \mathcal{O}_{\rho'}$ [5, Lem. 3.2.8].

Lemma 8.4 has a certain analogy with this fact. However, we are in a different context, because the field extension $L(x)/K(x)$ is not algebraic.

Moreover, it is easy to find examples showing that the conditions $\rho \leq \rho'$ and $\mathcal{O}_\rho \subset \mathcal{O}_{\rho'}$ do not imply each other.

8.3 Lifting to the henselization

We are interested in the case $L = K^h$, $w = v^h$. As mentioned in section 8.1, w/v is immediate.

For simplicity, we omit the reference to the valuations v, v^h, and denote the spaces of inductive valuations and valuations on $K[x]$ and $K^h[x]$ extending v and v^h by

$$\mathbb{V}^{\mathrm{ind}}(K) \subset \mathrm{Val}(K), \qquad \mathbb{V}^{\mathrm{ind}}(K^h) \subset \mathrm{Val}(K^h),$$

respectively.

The restriction of an inductive valuation on $K^h[x]$ is not necessarily an inductive valuation on $K[x]$. We shall see an example in section 8.4.

Nevertheless, we may extend inductive valuations on $K[x]$ to inductive valuations on $K^h[x]$.

Proposition 8.5. *There is a lifting mapping*

$$\mathrm{lft}\colon \mathbb{V}^{\mathrm{ind}}(K) \longrightarrow \mathbb{V}^{\mathrm{ind}}\left(K^h\right) \subset \mathrm{Val}\left(K^h\right), \qquad \mu \longmapsto \mu^* = \mathrm{lft}(\mu)$$

such that $\mathrm{res} \circ \mathrm{lft} = \mathrm{id}_{\mathbb{V}^{\mathrm{ind}}(K)}$. *Also, any MacLane chain of an inductive valution*

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu, \tag{8.2}$$

determines a MacLane chain of its lift to $K^h[x]$, *with the same key polynomials* ϕ_i *and values* $\gamma_i \in \mathbb{Q}\Gamma$

$$\mu_{-\infty,K^h} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0^* \overset{\phi_0,\gamma_0}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1}^* \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r^* = \mu^*.$$

Moreover, the embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_{\mu^*}$ *is a strong isomorphism.*

Proof. Let $\mu \in \mathbb{V}^{\mathrm{ind}}(K)$, and consider a MacLane chain of μ as in (8.2).

Let us prove both statements by a recursive argument.

Suppose μ_{i-1}^* has been constructed, as the last valuation of a MacLane chain of length $i-1$, and satisfies:

- The restriction of μ_{i-1}^* to $K[x]$ is μ_{i-1}.
- The canonical mapping $\mathcal{G}_{\mu_{i-1}} \to \mathcal{G}_{\mu_{i-1}^*}$ is a strong isomorphism.

If $i = 0$, we take $\mu_{i-1}^* = \mu_{-\infty,K^h}$. In this case, the first assumption is obvious and the second one holds by Lemma 8.3.

By Lemma 8.2, ϕ_i is a key polynomial for μ_{i-1}^*. Moreover, if $i > 0$,

$$\phi_i \nmid_{\mu_{i-1}} \phi_{i-1} \implies \phi_i \nmid_{\mu_{i-1}^*} \phi_{i-1}.$$

In fact, the element $H_{\mu_{i-1}}(\phi_i)$ does not divide $H_{\mu_{i-1}}(\phi_{i-1})$ in $\mathcal{G}_{\mu_{i-1}}$. Since $\mathcal{G}_{\mu_{i-1}} \simeq \mathcal{G}_{\mu_{i-1}^*}$, the images of these elements in $\mathcal{G}_{\mu_{i-1}^*}$ preserve this property.

Therefore, if we define

$$\mu_i^* = \mathrm{lft}(\mu_i) = [\mu_{i-1}^*; \phi_i, \gamma_i],$$

we extend the previous MacLane chain to a MacLane chain of length i.

By the very definition of the augmented valuations, $\mathrm{res}(\mu_i^*) = \mu_i$.

Finally, let us check that $\mathcal{G}_{\mu_i} \hookrightarrow \mathcal{G}_{\mu_i^*}$ is a strong isomorphism. Let

$$F = \sum\nolimits_{0 \le s} \xi_s \phi_i^s \in K^h[x]$$

be the ϕ_r-expansion of some $F \in K^h[x]$. For each ξ_s, there exists $a_s \in K[x]$ such that

$$\deg(a_s) = \deg(\xi_s), \qquad a_s \sim_{\mu_{i-1}^*} \xi_s.$$

Hence, $f = \sum_{0 \le s} a_s \phi_i^s$ is the canonical ϕ_i-expansion of a certain polynomial $f \in K[x]$, satisfying $\deg(f) = \deg(F)$. Also,

$$\mu_i^*(f - F) = \mathrm{Min}_{0 \le s}\{\mu_{i-1}^*(a_s - \xi_s) + s\gamma_i\} > \mathrm{Min}_{0 \le s}\{\mu_{i-1}^*(a_s) + s\gamma_i\} = \mu_i^*(f).$$

Hence, $f \sim_{\mu_i^*} F$. An iteration of this argument proves the proposition. □

The existence of this lifting has a relevant consequence.

Theorem 8.6. *All key polynomials for inductive valuations are defectless polynomials in* $K^h[x]$.

Proof. Let $\mu \in \mathbb{V}^{\mathrm{ind}}(K)$ be an inductive valuation, and take $\phi \in \mathrm{KP}(\mu)$.

By Lemma 8.2 and Proposition 8.5, ϕ is a key polynomial for the lift of μ to $\mathbb{V}^{\mathrm{ind}}(K^h)$. Hence, it is irreducible in $K^h[x]$ by Lemma 1.19.

Finally, Corollary 6.19 shows that ϕ is defectless. □

Proposition 8.7. *For every* $\mu \in \mathbb{V}^{\mathrm{ind}}(K)$ *the valuation* $\mu^* = \mathrm{lft}(\mu)$ *is the unique element in* $\mathrm{Val}\left(K^h\right)$ *whose restriction to* $K[x]$ *is* μ.

Proof. Suppose that $\rho \in \mathrm{Val}\left(K^h\right)$ satisfies $\mathrm{res}(\rho) = \mu$. Let us show that $\mu^* \leq \rho$.

Consider a MacLane chain of μ as in (8.2). For a non-zero $F \in K^h[x]$, let

$$F = \sum_{s_0,\dots,s_r \in \mathbb{N}} a_{s_0,\dots,s_r} \phi_0^{s_0} \cdots \phi_r^{s_r}, \qquad a_{s_0,\dots,s_r} \in K^h$$

be its $(\phi_0, \dots, \phi_r)$-expansion.

In general, for $b \in K^h$, we have $\mu^*(b) = v^h(b) = \rho(b)$.

Since $\phi_0, \dots, \phi_r$ have coefficients in K, we have $\rho(\phi_i) = \mu^*(\phi_i)$ for all i. Therefore,

$$\rho(F) \geq \mathrm{Min}\{\rho\left(a_{s_0,\dots,s_r} \phi_0^{s_0} \cdots \phi_r^{s_r}\right)\} = \mathrm{Min}\{\mu^*\left(a_{s_0,\dots,s_r} \phi_0^{s_0} \cdots \phi_r^{s_r}\right)\} = \mu^*(F).$$

Thus, $\mu^* \leq \rho$. By Lemma 8.4, we deduce that $\mu^* = \rho$. □

Finally, Proposition 8.5 yields a criterion to decide when the restriction of an inductive valuation on $K^h[x]$ is an inductive valuation on $K[x]$.

Corollary 8.8. *Let* ρ *be an inductive valuation on* $K^h[x]$, *admitting an optimal MacLane chain*

$$\mu_{-\infty,K^h} \overset{F_0,\gamma_0}{\longrightarrow} \rho_0 \overset{F_1,\gamma_1}{\longrightarrow} \cdots \overset{F_{r-1},\gamma_{r-1}}{\longrightarrow} \rho_{r-1} \overset{F_r,\gamma_r}{\longrightarrow} \rho_r = \rho.$$

Then, the restriction of ρ *to* $K[x]$ *is an inductive valuation if and only if there exist monic polynomials* $\phi_0, \dots, \phi_r \in K[x]$ *such that*

$$\deg(\phi_i) = \deg(F_i), \qquad \rho_{i-1}\left(F_i - \phi_i\right) \geq \gamma_i, \qquad 0 \leq i \leq r, \tag{8.3}$$

where we agree that $\rho_{-1} = v^h$.

Proof. Suppose that $\mu = \mathrm{res}(\rho)$ is inductive. Consider an optimal MacLane chain

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{s-1},\gamma_{s-1}}{\longrightarrow} \mu_{s-1} \overset{\phi_s,\gamma_s}{\longrightarrow} \mu_s = \mu. \tag{8.4}$$

By Proposition 8.5, this chain lifts to an optimal MacLane chain

$$\mu_{-\infty,K^h} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0^* \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{s-1},\gamma_{s-1}}{\longrightarrow} \mu_{s-1}^* \overset{\phi_s,\gamma_s}{\longrightarrow} \mu_s^* = \mu^*.$$

By Proposition 8.7, $\mu^* = \rho$. Now, by the unicity of optimal MacLane chains (Proposition 5.7), necessarily $s = r$ and (8.3) holds.

Conversely, the conditions in (8.3) imply that ρ admits a MacLane chain

$$\mu_{-\infty,K^h} \overset{\phi_0,\gamma_0}{\longrightarrow} \rho_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \rho_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \rho_r = \rho,$$

by Proposition 5.7. Obviously, $\mu = \mathrm{res}(\rho)$ coincides with the inductive valuation (8.4) determined by all these data ϕ_i, γ_i. □

8.4 Example of a non-inductive valuation

Let p be a prime number and denote by ord_p the p-adic valuation on $\mathbb{Q}$.

Suppose that $p \equiv 1 \pmod 4$, and let $i_0 \in \mathbb{Z}$ such that $\mathrm{ord}_p(i_0^2+1) = 1$.

Consider the polynomial

$$\phi = x^2 + 1 \in \mathbb{Z}[x].$$

Since ϕ splits modulo p, the valuation ord_p has two extensions ν, ν' to the field $\mathbb{Q}(i)$ obtained by adjoining to $\mathbb{Q}$ a root i of ϕ.

Both extensions ν, ν' are immediate over ord_p. Clearly,

$$1 = \mathrm{ord}_p(i_0^2+1) = \nu(i_0^2+1) = \nu((i_0+i)(i_0-i)) = \nu(i_0+i) + \nu(i_0-i),$$

and similarly for ν'. We may distinguish these two extensions by

$$\nu(i-i_0) = 1, \quad \nu(i+i_0) = 0; \qquad \nu'(i-i_0) = 0, \quad \nu'(i+i_0) = 1.$$

Let $K = \mathbb{Q}(t)$, where t is an indeterminate. Let ord_t be the t-adic valuation, and for any $a \in K^*$, let the *initial coefficient* of a be

$$\mathrm{in}(a) = \left(t^{-\mathrm{ord}_t(a)} a\right)(0) \in \mathbb{Q}^*.$$

Consider the following valuation of rank two on K:

$$v\colon K^* \longrightarrow \mathbb{Z}^2_{\mathrm{lex}}, \qquad a \longmapsto v(a) = \left(\mathrm{ord}_t(a), \mathrm{ord}_p(\mathrm{in}(a))\right).$$

This valuation admits two extensions to the quadratic extension $L = K(i)$:

$$w(\xi) = \left(\mathrm{ord}_t(\xi), \nu(\mathrm{in}(\xi))\right), \qquad w'(\xi) = \left(\mathrm{ord}_t(\xi), \nu'(\mathrm{in}(\xi))\right), \quad \forall\, \xi \in L,$$

where $\mathrm{ord}_t(\xi)$ and $\mathrm{in}(\xi)$ have the obvious meaning.

Fact 1. *We may choose a henselization (K^h, v^h) of (K, v) such that*

$$(K, v) \subset (L, w) \subset (K^h, v^h).$$

Let $\mathrm{Gal}(L/K) = \{1, \tau\}$, where the automorphism τ is determined by $\tau(i) = -i$. Clearly,

$$w' = w \circ \tau, \qquad w = w' \circ \tau.$$

Hence, for any extension $\tilde{v}$ of w to K^s, the elements in the decomposition group $D_{\tilde{v}}$ restrict to the identity on L. In other words, $L \subset K^h$.

Fact 2. *K is not dense in K^h.*

In fact, $(\mathbb{Q}, \mathrm{ord}_p)$ is dense in $(\mathbb{Q}(i), \nu)$. Hence, by taking $q \in \mathbb{Q}$, the values

$$w(i-q) = (0, \nu(i-q)),$$

cover all elements in the subgroup $\{0\} \times \mathbb{Z}$.

On the other hand, for arbitrary polynomials $f, g \in \mathbb{Q}[t]$ we have

$$\mathrm{ord}_t(i - (f/g)) \leq 0.$$

This is obvious if $\mathrm{ord}_t(f/g) \neq 0$. In the case $\mathrm{ord}_t(f/g) = 0$, we have

$$\mathrm{ord}_t(i - (f/g)) = \mathrm{ord}_t(i - \mathrm{in}(f/g)) = \mathrm{ord}_t(i - (f(0)/g(0))) = 0,$$

because $i \neq f(0)/g(0) \in \mathbb{Q}$.

As a consequence,

$$\{w(i-a) \mid a \in K\} = \mathbb{Z}_{\leq 0} \times \mathbb{Z}, \tag{8.5}$$

so that there are no elements in K which are arbitrarily close to i.

This ends the proof of Fact 2.

Fact 3. *Consider the following depth-zero valuation on $K^h[x]$:*

$$\rho = \mu_0(x - i, \gamma) \in \mathbb{V}^{\mathrm{ind}}(K^h), \qquad \gamma = (1, 0),$$

and let $\mu = \mathrm{res}(\rho) \in \mathbb{V}(K)$.

For any $f \in K[x]$, with canonical ϕ-expansion $f = \sum_{0 \leq s} a_s \phi^s$, the valuation μ acts as follows:

$$\mu(f) = \mathrm{Min}\left\{w(a_s(i)) + s\gamma \mid 0 \leq s\right\}.$$

We claim that

$$cx + d \sim_\rho ci + d, \quad \forall\, c, d \in K. \tag{8.6}$$

In fact, if $c = 0$ the statement is obvious. If $c \neq 0$, we may assume $c = 1$, Then, by (8.5), we have

$$\rho((x + d) - (i + d)) = \rho(x - i) = \gamma > \rho(i + d).$$

This ends the proof of the claim.

Thus, $x + i \sim_\rho 2i$, and this leads to

$$\phi = (x + i)(x - i) \sim_\rho 2i(x - i). \tag{8.7}$$

In particular, $\rho(\phi) = \rho(x - i) = \gamma$.

Hence, the statement of Fact 3 is true for monomials. Since $\deg(a_s) \leq 1$, (8.6) shows that

$$\rho(a_s\phi^s) = \rho(a_s(i)) + s\gamma = w(a_s(i)) + s\gamma.$$

Therefore, we need only to show that $\rho(f) = \mathrm{Min}\left\{\rho\left(a_s\phi^s\right) \mid 0 \leq s\right\}$.

We may drop the monomials with larger ρ-value. Thus, we may suppose that all monomials have the same value; say $\rho(a_s\phi^s) = \delta$ for all s.

By (8.6) and (8.7), we have

$$a_s\phi^s \sim_\rho a_s(i)(2i)^s(x - i)^s.$$

Consider the polynomial $F = \sum_{0 \leq s} a_s(i)(2i)^s(x - i)^s$. All monomials have ρ-value equal to δ. Thus, by the definition of the augmented valuation ρ, we have $\rho(F) = \delta$. We may apply equation (1.3) to deduce that $F \sim_\rho f$. Hence, $\rho(f) = \delta$.

This ends the proof of Fact 3.

Fact 4. $\mathrm{res}^{-1}(\mu) = \{\rho\}$.

Suppose that $\rho' \in \mathrm{Val}(K^h)$ satisfies $\mathrm{res}(\rho') = \mu = \mathrm{res}(\rho)$. Then,

$$\rho'(i - i_0) = w(i - i_0) = (0, 1) > 0, \qquad \rho'(x + i_0) = \mu(x + i_0) = w(i + i_0) = 0.$$

Hence, $\rho'(x + i) = \rho'(x + i_0 + (i - i_0)) = 0$. Since $\rho'(\phi) = \gamma$, we deduce that $\rho'(x - i) = \gamma$.

This leads to $\rho' \geq \rho$, and this implies $\rho' = \rho$ by Lemma 8.4.

Fact 5. *The embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ is an isomorphism, but not a strong isomorphism.*

Consider the following elements of degre zero in the respective graded algebras:

$$y_\rho = H_\rho((x - i)/t) \in \Delta_\rho, \qquad y_\mu = H_\mu(\phi/t) \in \Delta_\mu.$$

By Theorem 1.28, y_μ and y_ρ are transcendental over $k = \mathbb{Z}/p\mathbb{Z}$, and

$$\Delta_\mu = k[y_\mu], \qquad \Delta_\rho = k[y_\rho].$$

By (8.7), the embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_\rho$ sends

$$y_\mu \longmapsto H_\rho(2i)\, y_\rho = H_\rho(2i_0)\, y_\rho.$$

Since $H_\rho(2i_0) \in k^*$, we deduce that the canonical embedding restricts to an isomorphism between Δ_μ and Δ_ρ.

Since $\Gamma_v = \Gamma_\mu = \Gamma_\rho$, the embedding is an isomorphism restricted to any homogeneous part:

$$\mathcal{P}_\alpha(\mu)/\mathcal{P}^+_\alpha(\mu) = H_\mu(a)\Delta_\mu \quad \xrightarrow{\sim} \quad H_\rho(a)\Delta_\rho = \mathcal{P}_\alpha(\rho)/\mathcal{P}^+_\alpha(\rho),$$

where a is any element in K^* with $v(a) = \alpha$.

However, this is not a strong isomorphism, because there is no polynomial $g \in K[x]$ of degree one such that $g \sim_\rho x - i$. In fact, by (8.6), $g \sim_\rho \xi$ for some $\xi \in L$. Since $x - i$ is ρ-minimal, it cannot be ρ-equivalent to a constant.

Fact 6. *The valuation μ is not inductive, and it admits the polynomial $\phi = x^2 + 1$ as a key polynomial of minimal degree.*

The valuation μ is not inductive by the criterion of Corollary 8.8. In fact, (8.5) shows that there is no $a \in K$ such that $v^h((x + a) - (x - i)) = v^h(a + i) \geq \gamma$.

We claim that all polynomials in $K[x]$ of degree one are μ-units, so that μ admits no key polynomial of degree one.

In fact, for any $c, d \in K$ (8.6) shows that $H_\rho(cx + d) = H_\rho(ci + d)$ is a unit in $\mathcal{G}_\rho$, because $ci + d \in L^*$. Since this element is the image of $H_\mu(cx + d)$ under the isomorphism $\mathcal{G}_\mu \to \mathcal{G}_\rho$, we deduce that $H_\mu(cx + d)$ is a unit in $\mathcal{G}_\mu$.

Also, the image of $H_\mu(\phi)$ under this isomorphism is $H_\rho(\phi)$, which is a prime element in $\mathcal{G}_\rho$ by (8.7). Hence, $H_\mu(\phi)$ is a prime element in $\mathcal{G}_\mu$.

On the other hand, ϕ is μ-minimal, because it cannot divide a non-zero homogeneous element $H_\mu(a)$ with $\deg(a) < 2$. In fact, such an $H_\mu(a)$ is a unit in $\mathcal{G}_\mu$, but $H_\mu(\phi)$ is not a unit.

This ends the proof of Fact 6.

Now, consider a kind of conjugate valuation over K, and its restriction:

$$\rho' = \mu_0(x + i, \gamma) \in \mathrm{Val}(L, w), \qquad \mu' = \mathrm{res}(\rho') \in \mathrm{Val}(K, v).$$

All previous facts for the pair ρ, μ, have its analogous counterpart for the pair ρ', μ'.

- $\mu'(f) = \mathrm{Min}\,\{w(a_s(-i)) + s\gamma \mid 0 \leq s\}$.
- $\mathrm{res}^{-1}(\mu') = \{\rho'\}$
- The embedding $\mathcal{G}_{\mu'} \hookrightarrow \mathcal{G}_{\rho'}$ is an isomorphism, but not a strong isomorphism.
- μ' is not an inductive valuation, and it admits $\phi = x^2 + 1$ as a key polynomial of minimal degree.

Therefore, this example shows that Lemma 6.20 does not hold for non-inductive valuations.

Fact 7. *Although μ and μ' have $\phi = x^2+1$ as a common key polynomial, these valuations are not comparable. Neither $\mu \leq \mu'$ nor $\mu \geq \mu'$.*

In fact,

$$\mu(x - i_0) = w(i - i_0) = 1 > 0 = w(i + i_0) = \mu'(x - i_0),$$
$$\mu(x + i_0) = w(i + i_0) = 0 < 1 = w(i - i_0) = \mu'(x + i_0).$$

Chapter 9

Proper key polynomials and types

9.1 Proper key polynomials

Let $\mu \in \mathbb{V}$ be a valuation admitting key polynomials. Let us emphasize two relevant numerical data of μ.

The *minimal degree* $m := m(\mu)$ of μ is the minimal degree of a key polynomial for μ.

By Theorem 1.27, all key polynomials for μ of degree m have a constant μ-value.

The *relative ramification index* $e := e(\mu)$ of μ is the minimal positive integer such that $e\mu(\phi)$ belongs to $\Gamma_{\mu,m}$, where ϕ is any key polynomial of degree m.

Example. For instance, if μ is an inductive valuation and it admits a MacLane chain of length r as in (5.1), then $m = m_r$ and $e = e_r$.

The subgroup $\Gamma_{\mu,m} \subset \Gamma_\mu$ admits an intrinsic description, as the subgroup of Γ_μ formed by all values α such that there is a unit in $\mathcal{G}$ of degree α.

Lemma 9.1. *Let $\mu \in \mathbb{V}$ be a valuation with $\mathrm{KP}(\mu) \neq \emptyset$. For any $\alpha \in \Gamma_\mu$, we have*

$$\big(\mathcal{P}(\alpha)/\mathcal{P}^+(\alpha)\big) \cap \mathcal{G}^* \neq \emptyset \iff \alpha \in \Gamma_{\mu,m},$$

where m is the minimal degree of a key polynomial for μ.

Proof. Let $\alpha \in \Gamma_{\mu,m}$, and take $a \in K[x]_m$ such that $\mu(a) = \alpha$. By Proposition 1.24, $H_\mu(a)$ is a unit in $\mathcal{P}(\alpha)/\mathcal{P}^+(\alpha)$.

Let ϕ be a key polynomial of degree m, and let $\gamma = \mu(\phi)$, so that $\Gamma_\mu = \big\langle\, \Gamma_{\mu,m}, \gamma \,\big\rangle$.

Any $\alpha \notin \Gamma_{\mu,m}$ can be written as

$$\alpha = \ell\gamma + \beta, \qquad 0 < \ell < e, \quad \beta \in \Gamma_{\mu,m}.$$

By the previous argument, there exists a unit $z \in \mathcal{G}^*$ of degree β. Then, $z\, H_\mu(\phi)^\ell$ has degree α, and there is no unit in $\mathcal{P}(\alpha)/\mathcal{P}^+(\alpha) = \big(z\, H_\mu(\phi)^\ell\big)\, \Delta$, because $H_\mu(\phi)$ is a prime element. □

Notation. *For any $\phi \in \mathrm{KP}(\mu)$ we denote by $[\phi]_\mu$, or simply $[\phi]$ if the valuation μ is clear from the context, the μ-equivalence class of ϕ in the set $\mathrm{KP}(\mu)$.*

Let us fix a key polynomial ϕ_0 of degree m. Proposition 1.30 shows that all key polynomials for μ have degree multiple of m:

$$\deg(\phi) = m \ \text{ if } \ \phi \in [\phi_0], \qquad \deg(\phi) \in em\mathbb{Z} \ \text{ if } \ \phi \notin [\phi_0]. \tag{9.1}$$

Let us introduce an intrinsic distinction between key polynomials, according to their degree.

Definition 9.2. *Let $\mu \in \mathbb{V}$ be a valuation, and let $\phi \in \mathrm{KP}(\mu)$.*

We say that ϕ is proper *if $\deg(\phi)$ is a multiple of em.*

Denote by $\mathrm{KP}(\mu)^{\mathrm{pr}} \subset \mathrm{KP}(\mu)$ the set of proper key polynomials for μ.

By Proposition 1.31, all key polynomials in the class $[\phi]$ share this property. Thus, it makes sense to talk about proper μ-equivalence classes of key polynomials.

Also, by Theorem 1.33, any prime element in $\mathcal{G}$ is associate to the prime element $H_\mu(\phi)$ determined by a key polynomial. Hence, it makes sense to talk about proper classes of prime elements in $\mathcal{G}$, up to units.

We may reformulate this remark in the context of maximal ideals of Δ as well. By Theorem 1.32, we may define a degree function:

$$\deg\colon \mathrm{Max}(\Delta) \ \longrightarrow \ m\,\mathbb{Z}_{\geq 0}, \qquad \mathcal{L} \ \longmapsto \ \deg(\mathcal{L}) = \deg(\phi),$$

where ϕ is any key polynomial such that $\mathcal{R}(\phi) = \mathcal{L}$.

The corresponding concept of *proper maximal ideal* has the obvious meaning.

The following remarks are an immediate consequence of (9.1).

Corollary 9.3.

1. *If $e = 1$ there are no improper classes in $\mathrm{KP}(\mu)/\!\sim_\mu$.*
2. *If $e > 1$, then $[\phi_0]$ is the only improper class. This class coincides with the set of all key polynomials of degree m.*

Corollary 9.4. *Suppose that μ is inductive and it admits a MacLane chain of length r as in (5.1). Then*

1. *If $e_r > 1$, the improper class is $[\phi_r]$.*
2. $\phi_i \in \mathrm{KP}(\mu_{i-1})^{\mathrm{pr}}, \qquad 1 \leq i \leq r.$

Remark. If μ is incommensurable, then $\mathrm{KP}(\mu)$ contains a single μ-equivalence class of key polynomials, all of them of the same degree [23, Thm. 4.2].

Hence, if we agree that the relative ramification index of μ is $e = \infty$, we may mimic all definitions given so far. In coherence with Corollary 9.3, the single class of $\mathrm{KP}(\mu)$ would be improper.

Theorems 1.32 and 1.28 yield bijections

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

where $\mathbb{P}(\kappa)$ is the set of monic irreducible polynomials with coefficients in κ.

The first bijection is canonical but the second one may depend on the choice of the pair ϕ_0, u, leading to a different Hauptmodul ξ, generating Δ as a κ-algebra, and a different operator $R = R_{\phi_0,u}$.

By Proposition 1.30, the composition of the above bijections maps:

$$[\phi] \longmapsto \begin{cases} y, & \text{if } [\phi] = [\phi_0], \\ R(\phi)(y), & \text{if } [\phi] \neq [\phi_0]. \end{cases} \tag{9.2}$$

Let us give still another characterization of properness, which follows immediately from Corollary 9.3.

Corollary 9.5. *For any $\phi \in \mathrm{KP}(\mu)$, the following conditions are equivalent.*

(1) ϕ is improper.

(2) $e > 1$ and y is the polynomial associated with $[\phi]$ by the bijection (9.2).

(3) $e > 1$ and $R(\phi) = 1$.

Corollary 9.6. *Suppose that μ is inductive. Then, a key polynomial $\phi \in \mathrm{KP}(\mu)$ 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.*

Proof. Suppose that μ admits a MacLane chain of length r such that $\phi \not\sim_\mu \phi_r$. If $e_r = 1$ then all key polynomials are proper. If $e_r > 1$, then ϕ is proper too, because the improper class is $[\phi_r]$, as shown in Corollary 9.4.

Conversely, suppose that ϕ is proper. Consider any MacLane chain of μ, and let r be its length. We know that $m = m_r$.

If $e > 1$, then Corollary 9.4 shows that the improper class is $[\phi_r]$. Hence, $\phi \notin [\phi_r]$.

Suppose that $e = 1$, so that $\Gamma_\mu = \Gamma_{\mu,m}$. If $\phi \sim_\mu \phi_r$, we may take $a \in K[x]_m$ with $\mu(a) = \mu(\phi_r)$. By Proposition 5.7, we may replace ϕ_r by $\phi_r^* = \phi_r + a$ as a key polynomial for μ_{r-1}, and we get another MacLane chain of μ for which $\phi_r^* \not\sim_\mu \phi$. □

Definition 9.7. *We say that $f \in K[x]$ is* μ-proper *if $H_\mu(f)$ is not divided by the improper class of prime elements in $\mathcal{G}$.*

The next result is an immediate consequence of Corollary 9.3.

Corollary 9.8. *If $e = 1$ there are no improper polynomials.*

If $e > 1$, then $f \in K[x]$ is improper if and only if $s_{\mu,\phi_0}(f) > 0$, where $[\phi_0]$ is the improper class.

Lemma 9.9. *If at least one of the polynomials $g, h \in K[x]$ is μ-proper, then*

$$\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h).$$

Proof. Let us denote $s = s_{\mu,\phi_0}$ for simplicity. By Lemma 1.29, $\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h)$ is equivalent to the following equality, up to factors in κ^*:

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

By Lemmas 3.8 and 1.29, $s(gh) = s(g) + s(h)$ and $R(gh) = R(g)R(h)$. Thus, we want to show that

$$\lceil (s(g) + s(h))/e\rceil = \lceil s(g)/e\rceil + \lceil s(h)/e\rceil.$$

If $e = 1$ this equality is obvious. If $e > 1$ it holds too, because one of the two polynomials is μ-proper, so that either $s(g) = 0$, or $s(h) = 0$, by Corollary 9.8. □

Proposition 9.10. *Let $\phi \in \mathrm{KP}(\mu)$ and $\mathcal{L} = \mathcal{R}(\phi) \in \mathrm{Max}(\Delta)$. For any non-zero $f \in K[x]$:*

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

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

Proof. Let $\mathcal{P} \subset \mathrm{KP}(\mu)$ be a set of representatives of key polynomials under μ-equivalence. If we apply $\mathcal{R}$ to both terms of the factorization (1.8), Lemma 9.9 shows that:

$$\mathcal{R}(f) = \mathcal{R}\left(\prod\nolimits_{\phi\in\mathcal{P}} \phi^{a_\phi}\right) = \prod\nolimits_{\phi\in\mathcal{P}} \mathcal{R}(\phi^{a_\phi}), \qquad a_\phi = s_{\mu,\phi}(f).$$

For all proper $\phi \in \mathcal{P}$ we have $\mathcal{R}(\phi^{a_\phi}) = \mathcal{R}(\phi)^{a_\phi}$ by Lemma 9.9.

Thus, $\mathcal{R}(\phi)$ divides $\mathcal{R}(f)$ with exponent a_ϕ.

For the unique improper $\phi_0 \in \mathcal{P}$ (if $e > 1$), we have $R(\phi_0) = 1$, and Lemma 1.29 shows that

$$\mathcal{R}(\phi) = \xi\Delta, \qquad \mathcal{R}(\phi^{a_\phi}) = \xi^{\lceil a_\phi/e\rceil}\Delta = \mathcal{R}(\phi)^{\lceil a_\phi/e\rceil}.$$

Thus, $\mathcal{R}(\phi)$ divides $\mathcal{R}(f)$ with exponent $\lceil a_\phi/e\rceil$. □

Corollary 9.11. *Let ϕ be a proper key polynomial for μ such that $\phi \not\sim_\mu \phi_0$. Then, $R(\phi) \in \kappa[y]$ is a monic irreducible polynomial, and*

$$\mathrm{ord}_{R(\phi)}\left(R(f)\right) = s_{\mu,\phi}(f), \qquad \forall\, f \in K[x].$$

Proof. Let us denote $\psi = R(\phi) \in \kappa[y]$ and $\mathcal{L} = \mathcal{R}(\phi) \in \mathrm{Max}\,(\Delta)$.

By Proposition 1.30, ψ is a monic irreducible polynomial, $\psi \neq y$, and $\mathcal{L} = \psi(\xi)\Delta$.

On the other hand, $\mathcal{R}(f) = \xi^{\lceil s(f)/e\rceil}\, R(f)(\xi)\Delta$, by Lemma 1.29. Since $\psi \neq y$, Theorem 1.28 shows that $\mathrm{ord}_\psi(R(f)) = \mathrm{ord}_{\mathcal{L}}(\mathcal{R}(f))$. Since $\mathcal{L}$ is proper, $\mathrm{ord}_{\mathcal{L}}(\mathcal{R}(f)) = s_{\mu,\phi}(f)$ by Proposition 9.10. □

9.2 Types

A *type* $\mathbf{t}$ is a pair $(\mu, \mathcal{L})$ belonging to the set

$$\mathbb{T} = \left\{(\mu, \mathcal{L}) \mid \mu \in \mathbb{V}^{\text{ind}}, \mathcal{L} \in \text{Max}(\Delta_\mu),\ \mathcal{L} \text{ proper}\right\}. \tag{9.3}$$

By Theorem 1.32, a proper maximal ideal $\mathcal{L}$ of Δ_μ corresponds to a proper equivalence class of key polynomials for μ. These key polynomials are called *representatives* of the type $\mathbf{t} = (\mu, \mathcal{L})$.

We denote the set of all representatives of a type $\mathbf{t}$ by

$$\text{Rep}(\mathbf{t}) = \{\phi \in \text{KP}(\mu) \mid \mathcal{R}_\mu(\phi) = \mathcal{L}\} \subset K[x].$$

Any type $\mathbf{t} \in \mathbb{T}$ determines a mapping

$$\text{ord}_{\mathbf{t}} \colon K[x] \longrightarrow \mathbb{N}, \qquad f \longmapsto \text{ord}_{\mathcal{L}}(\mathcal{R}_\mu(f)).$$

By Proposition 9.10,

$$\text{ord}_{\mathbf{t}}(f) = s_{\mu,\phi}(f), \qquad \forall\, \phi \in \text{Rep}(\mathbf{t}).$$

Our aim in this section is to show that any of these two objects, $\text{Rep}(\mathbf{t})$ or $\text{ord}_{\mathbf{t}}$, determine the type $\mathbf{t}$.

Theorem 9.12. *For $\mathbf{t} = (\mu, \mathcal{L})$, $\mathbf{t}^* = (\mu^*, \mathcal{L}^*) \in \mathbb{T}$, the following conditions are equivalent.*

(1) $\mathbf{t} = \mathbf{t}^*$.

(2) $\text{ord}_{\mathbf{t}} = \text{ord}_{\mathbf{t}^*}$.

(3) $\text{Rep}(\mathbf{t}) = \text{Rep}(\mathbf{t}^*)$.

Proof. It is clear that (1) implies (2). Let us show that (2) implies (3).

Take $\phi \in \text{Rep}(\mathbf{t})$; that is, $\phi \in \text{KP}(\mu)$ and $\mathcal{R}_\mu(\phi) = \mathcal{L}$. Since $\text{ord}_{\mathbf{t}} = \text{ord}_{\mathbf{t}^*}$, Proposition 9.10 shows that

$$1 = \text{ord}_{\mathcal{L}}(\mathcal{R}_\mu(\phi)) = \text{ord}_{\mathcal{L}^*}(\mathcal{R}_{\mu^*}(\phi)) = s_{\mu^*,\phi^*}(\phi), \tag{9.4}$$

where ϕ^* is any representative of $\mathbf{t}^*$. Thus, $\phi^* \mid_{\mu^*} \phi$. Since ϕ^* is μ^*-minimal, this implies $\deg(\phi) \geq \deg(\phi^*)$. By the symmetry of the argument, we deduce that $\deg(\phi^*) = \deg(\phi)$. Now, Lemma 1.18 shows that ϕ is a key polynomial for μ^*.

Therefore, $\mathcal{R}_{\mu^*}(\phi)$ is a maximal ideal of Δ_{μ^*}. By (9.4), $\mathcal{L}^* \mid \mathcal{R}_{\mu^*}(\phi)$, so that $\mathcal{R}_{\mu^*}(\phi) \subset \mathcal{L}^*$, leading to $\mathcal{R}_{\mu^*}(\phi) = \mathcal{L}^*$. Thus, ϕ is a representative of $\mathbf{t}^*$.

This shows that $\text{Rep}(\mathbf{t}) \subset \text{Rep}(\mathbf{t}^*)$. By the symmetry of the argument, equality holds.

Finally, let us prove that (3) implies (1). We need only to show that $\mu = \mu^*$, because then $\mathcal{L} = \mathcal{R}_\mu(\phi) = \mathcal{R}_{\mu^*}(\phi) = \mathcal{L}^*$ for any $\phi \in \text{Rep}(\mathbf{t}) = \text{Rep}(\mathbf{t}^*)$.

Suppose $\mu \neq \mu^*$, and let us show that this leads to $\text{Rep}(\mathbf{t}) \neq \text{Rep}(\mathbf{t}^*)$.

Take any $\phi \in \text{Rep}(\mathbf{t})$. Since $\phi \in \text{KP}(\mu) \cap \text{KP}(\mu^*)$, Lemma 6.20 shows that

$$\mu^* = [\mu;\, \phi, \gamma], \qquad \gamma = \mu^*(\phi) > \mu(\phi),$$

after eventually exchanging μ and μ^*.

If $e(\mu^*) > 1$, Corollary 9.3 would imply that $[\phi]_{\mu^*}$ is the improper class, against our assumption that $\mathcal{L}^*$ is proper. Therefore $e(\mu^*) = 1$, and this implies that $\gamma = \mu^*(\phi)$ belongs to Γ_μ. By Lemma 2.7, $\Gamma_\mu = \Gamma_{\mu,\deg(\phi)}$; thus, there exists $a \in K[x]_{\deg(\phi)}$ such that $\mu(a) = \gamma > \mu(\phi)$. Hence,

$$\phi + a \sim_\mu \phi \implies \phi + a \in \mathrm{Rep}(\mathbf{t}), \qquad \phi + a \not\sim_{\mu^*} \phi \implies \phi + a \notin \mathrm{Rep}(\mathbf{t}^*).$$

Thus, $\mathrm{Rep}(\mathbf{t}) \neq \mathrm{Rep}(\mathbf{t}^*)$. □

Let us emphasize that properness of the maximal ideal $\mathcal{L}$ is an essential condition in the definition of types. If this condition were dropped, there would be different types with the same sets of representatives.

Let us see an example. Suppose that $\Gamma = \mathbb{Z}$ and consider the following valuations of depth zero:

$$\mu = \mu_0(x, 0), \qquad \mu^* = \mu_0(x, 1/2).$$

Clearly,

$$[x]_\mu = \{x + a \mid a \in K,\ v(a) > 0\}, \qquad [x]_{\mu^*} = \{x + a \mid a \in K,\ v(a) > 1/2\}.$$

Therefore, $[x]_\mu = [x]_{\mu^*}$, while $\mu \neq \mu^*$.

Computational representation of types

From a computational perspective, a type $\mathbf{t} = (\mu, \mathcal{L})$ is represented as follows.

- μ is represented by a MacLane chain.
- $\mathcal{L}$ is represented by a monic irreducible polynomial $\psi \in k_r[y]$, $\psi \neq y$.

Here r is the length of the MacLane chain. The data of the chain provide an explicit isomorphism $k_r[y] \simeq \Delta$. Thus, a monic irreducible polynomial $\psi \in k_r[y]$ determines a maximal ideal $\mathcal{L} \in \mathrm{Max}(\Delta)$.

The properness of $\mathcal{L}$ is guaranteed by the condition $\psi \neq y$.

Chapter 10

Approaching defectless polynomials by key polynomials

In this chapter, we assume that (K, v) is a henselian field.

We still denote by v the canonical extension

$$v\colon \overline{K} \longrightarrow \mathbb{Q}\Gamma \cup \{\infty\}$$

of v to a valuation on $\overline{K}$.

Let $\mathbb{P} = \mathbb{P}(K)$ be the set of all monic irreducible polynomials in $K[x]$. We say that an element in $\mathbb{P}$ is a *prime polynomial*.

In this chapter, we study how far can we approximate a given prime polynomial $F \in K[x]$, by key polynomials of valuations on $K[x]$.

This problem distinguishes two phases. In section 10.1, we show that for any key polynomial ϕ of a valuation $\mu \in \mathbb{V}$, the condition

$$\phi \mid_\mu F \tag{10.1}$$

implies that $\mathcal{R}_\mu(F)$ is a power of the maximal ideal $\mathcal{R}_\mu(\phi)$ in Δ_μ.

This fact leads to a vast generalization of Hensel's lemma (Theorem 10.7).

In this way, by constructing (via the augmentation process) larger valuations admitting key polynomials for which (10.1) holds, we discover several invariants of F. Simultaneously, the key polynomials satisfying (10.1) are better approximations to F, in the sense that the resultant $\mathrm{Res}(F, \phi)$ has a larger v-value.

It has to be said that the degree of ϕ may be lower than the degree of F.

In a second phase, developed in section 10.4, we must determine under what conditions this approximation process is able to reach a valuation μ admitting F as a key polynomial.

Both phases are inspired in a pioneer work by Okutsu [24], who showed how to control the quality of the approximations when K is the completion of a discrete rank one valuation v. In this classical case, this process converges for any prime polynomial, and all involved valuations are inductive.

The connection of Okutsu's approach with inductive valuations was found in [7]. Finally, still restricted to discrete rank one valuations, in the paper [6] the main result of Okutsu was reinterpreted as the existence of a canonical bijection

$$\mathbb{M} \longrightarrow \mathbb{P}/\approx$$

between a certain *MacLane space* and the quotient of the set $\mathbb{P}$ of prime polynomials under certain *Okutsu equivalence* $\approx$.

For both phases, we follow closely the approach of [6]. The generalisation of these ideas to the case of a general valuation v is easy, but it has a crucial limitation. The second phase is only possible for *defectless* polynomials.

The extension of these ideas to arbitrary prime polynomials would require the use of *continuous MacLane chains* and their *limit augmentations* considered by Vaquié in [30]. We hope to be able to deal with the general case in a future work.

10.1 Prime polynomials vs key polynomials

Let $F \in \mathbb{P}$ be a prime polynomial and fix $\theta \in \overline{K}$ a root of F. Denote

- $K_F = K(\theta)$ the finite extension of K generated by θ.
- $\mathcal{O}_F$ the valuation ring of the unique extension of v to K_F.
- $\mathfrak{m}_F$ the maximal ideal of $\mathcal{O}_F$.
- $k_F = \mathcal{O}_F/\mathfrak{m}_F$ the residue class field.

Lemma 10.1. *Let $F, G \in \mathbb{P}$ be two prime polynomials, and let $\theta_F, \theta_G \in \overline{K}$ be roots of F, G, respectively. Then,*

$$v(F(\theta_G))/\deg(F) = v(G(\theta_F))/\deg(G).$$

Proof. By the henselian property, the value $v(F(\theta_G))$ does not depend on the choice of the root θ_G; hence,

$$\deg(G)v(F(\theta_G)) = v(\mathrm{Res}(F, G)) = \deg(F)v(G(\theta_F)),$$

because $\mathrm{Res}(F, G) = \prod_{\theta_F \in Z(F)} G(\theta_F) = \pm \prod_{\theta_G \in Z(G)} F(\theta_G)$, where $Z(F)$ is the multiset of roots of F in $\overline{K}$, with due count of multiplicities if F is inseparable. □

In this section, we look for properties of the prime polynomial F derived from the existence of a valuation $\mu \in \mathbb{V}$ admitting a key polynomial ϕ such that $\phi \mid_\mu F$.

Theorem 10.2. *Let $F \in \mathbb{P}$ be a prime polynomial, and let $\theta \in \overline{K}$ be a root of F. Let $\phi \in K[x]$ be a key polynomial for a valuation $\mu \in \mathbb{V}$. Then,*

$$\phi \mid_\mu F \iff v(\phi(\theta)) > \mu(\phi).$$

Moreover, if this condition holds, then:

(1) Either $F = \phi$, or the Newton polygon $N_{\mu,\phi}(F)$ is one-sided of slope $-v(\phi(\theta))$.

(2) The leading monomial of the ϕ-expansion of F is ϕ^ℓ, where $\ell = \ell(N_{\mu,\phi}(F))$.

(3) $F \sim_\mu \phi^\ell$. In particular, $\mathcal{R}_\mu(F)$ is a power of the maximal ideal $\mathcal{R}_\mu(\phi)$ in Δ_μ.

Proof. If $F = \phi$ all statements of the theorem are trivial. Assume $F \neq \phi$, and let $\alpha \in \overline{K}$ be a root of ϕ.

If $\phi \nmid_\mu F$, then $\mu(F) = v(F(\alpha))$ by Proposition 1.21. Thus, Theorem 1.27 and Lemma 10.1 show that

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

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

$$v(b_0) = k\gamma, \quad v(b_j) \geq (k-j)\gamma, \ 1 \leq j < k, \quad v(b_k) = 0. \tag{10.2}$$

Consider the polynomial $G = \sum_{j=0}^k b_j \phi^j \in K[x]$. The conditions in (10.2) imply that $N_{\mu,\phi}(G)$ is one-sided of slope $-\gamma$. Since $G(\theta) = 0$, the polynomial F divides G and Theorem 3.10 shows that

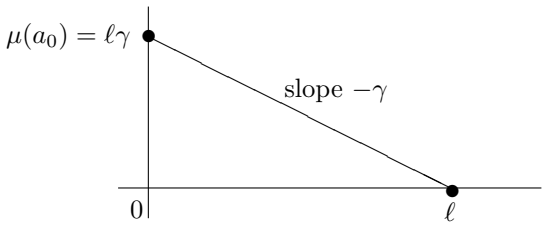
$$N^{\text{pp}}_{\mu,\phi}(G) = N^{\text{pp}}_{\mu,\phi}(F) + N^{\text{pp}}_{\mu,\phi}(G/F). \tag{10.3}$$

By Lemma 3.6, $\ell(N^{\text{pp}}_{\mu,\phi}(F)) = s_{\mu,\phi}(F) > 0$. Hence, $N^{\text{pp}}_{\mu,\phi}(G)$ has positive length too. By the definition of the principal polygon this means that $\gamma > \mu(\phi)$ (see section 3.2).

On the other hand, since $N^{\text{pp}}_{\mu,\phi}(G)$ is one-sided of slope $-\gamma$, (10.3) shows that $N_{\mu,\phi}(F)$ is one-sided of slope $-\gamma$ too.

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

Figure 10.1: Newton polygon $N_{\mu,\phi}(F)$ of a prime polynomial F such that $\phi \mid_\mu F$. The parameter γ is equal to $v(\phi(\theta))$, where θ is a root of F



Consider the ϕ-expansion $F = \sum_{s=0}^\ell a_s \phi^s$. By Lemma 10.1,

$$v(a_0(\alpha)) = v(F(\alpha)) = v(\phi(\theta)) \deg(F)/\deg(\phi) = \gamma \deg(F)/\deg(\phi).$$

Also, since $\deg(a_0) < \deg(\phi)$, Proposition 1.21 shows that $\mu(a_0) = v(a_0(\alpha))$. Therefore, from the fact that $N_{\mu,\phi}(F)$ is one-sided of slope $-\gamma$ we deduce:

$$\mu(a_\ell) + \ell\gamma = \mu(a_0) = v(a_0(\alpha)) = \gamma \frac{\deg(F)}{\deg(\phi)}$$

$$= \gamma \, \frac{\deg(a_\ell) + \ell \deg(\phi)}{\deg(\phi)} = \gamma \left(\frac{\deg(a_\ell)}{\deg(\phi)} + \ell \right).$$

If $\deg(a_\ell) > 0$, then a_ℓ would be a monic polynomial contradicting Theorem 1.27:

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

Hence, $a_\ell = 1$, so that the leading monomial of the ϕ-expansion of F is ϕ^ℓ.

Since $\gamma > \mu(\phi)$, Remarks 3.1 and 3.4 show that $\mu(\phi^\ell) < \mu(a_s\phi^s)$ for all $s < \ell$. Thus, $F \sim_\mu \phi^\ell$. The statement about $\mathcal{R}_\mu(F)$ follows from Proposition 9.10. □

We may think of ϕ as a kind of approximation to F. From any such approximation, it is possible to construct a sequence of approximations with a strictly increasing value of $v(\phi(\theta))$, which is a kind of measure of the quality of the approximation.

Corollary 10.3. *With the above notation, suppose that $\phi \mid_\mu F$ and $\phi \neq F$. Let $\mu' = [\mu; \phi, v(\phi(\theta))]$ and let κ' be the algebraic closure of k in $\Delta_{\mu'}$. Then,*

(1) There is a unique μ'-equivalence class of key polynomials $\phi' \in \mathrm{KP}(\mu')$ such that $\phi' \mid_{\mu'} F$. This class $[\phi']_{\mu'}$ is proper, and $v(\phi'(\theta)) > v(\phi(\theta))$.

(2) $R_{\mu'}(F) \in \kappa'[y]$ is the power of a monic irreducible polynomial $\psi \in \kappa'[y]$.

(3) Let e' be the relative ramification index of μ'. That is, e' is the least positive integer such that $e'\mu'(\phi) = e'v(\phi(\theta))$ belongs to $\Gamma_{\mu',\deg(\phi)} = \Gamma_{\mu,\deg(\phi)}$. Then,

$$e(\phi') = e(\phi)\, e', \qquad f(\phi') = f(\phi) \deg(\psi).$$

Proof. We fix ϕ as a key polynomial for μ' of minimal degree, and we take any $u \in K[x]_{\deg(\phi)}$ such that $\mu'(u) = \mu'(\phi^{e'})$. Consider the residual polynomial operator $R_{\mu'}$, which depends on the choice of the pair ϕ, u (see section 1.7).

By Theorem 10.2, $s_{\mu',\phi}(F) = 0$ and $s'_{\mu',\phi}(F) = \ell$. Hence, Lemma 1.29 shows that

$$\deg(R_{\mu'}(F)) = \ell/e' > 0.$$

Let ψ be a monic irreducible factor of $R_{\mu'}(F)$ in $\kappa'[y]$. By Theorems 1.32 and 1.28, there exists a unique μ'-equivalence class of key polynomials $\phi' \in \mathrm{KP}(\mu')$ such that $R_{\mu'}(\phi') = \psi$.

Since $R_{\mu'}(\phi) = 1$ and $R_{\mu'}(\phi') = \psi \neq 1$, Proposition 1.31 shows that $\phi' \not\sim_{\mu'} \phi$. By Corollary 9.3 the class $[\phi']_{\mu'}$ is proper.

By Corollary 9.11, $s_{\mu',\phi'}(F) = \mathrm{ord}_\psi(R_{\mu'}(F)) > 0$. Thus, $\phi' \mid_{\mu'} F$.

By using Theorems 10.2 and 1.27, we deduce

$$v(\phi'(\theta)) > \mu'(\phi') = \frac{\deg(\phi')}{\deg(\phi)}\, \mu'(\phi) \geq \mu'(\phi) = v(\phi(\theta)).$$

Also, $F \sim_{\mu'} (\phi')^{\ell'}$ by Theorem 10.2, where ℓ' is uniquely determined by

$$\ell \deg(\phi) = \deg(F) = \ell' \deg(\phi').$$

By the unique factorization in $\mathcal{G}_{\mu'}$ (Theorem 1.33), the class $[\phi']_{\mu'}$ is unique.

By Lemma 1.29, $R_{\mu'}(F) = R_{\mu'}(\phi')^{\ell'} = \psi^{\ell'}$. This proves (1) and (2).

Let us prove (3). By Proposition 1.21,

$$\Gamma_{v_\phi} = \Gamma_{\mu,\deg(\phi)}, \qquad \Gamma_{v_{\phi'}} = \Gamma_{\mu',\deg(\phi')}.$$

On the other hand, $\Gamma_{\mu',\deg(\phi')} = \Gamma_{\mu'}$ by Lemma 2.7. Therefore

$$e' = \big(\Gamma_{\mu'} \colon \Gamma_{\mu',\deg(\phi)}\big) = \big(\Gamma_{\mu',\deg(\phi')} \colon \Gamma_{\mu,\deg(\phi)}\big) = \Big(\Gamma_{v'_\phi} \colon \Gamma_{v_\phi}\Big).$$

This proves $e(\phi') = e(\phi)\, e'$.

Finally, the valuation $\mu'' = [\mu';\, \phi', v(\phi'(\theta))]$ admits ϕ' as a key polynomial of minimal degree. Let κ'' be the algebraic closure of k inside $\Delta_{\mu''}$. Proposition 1.25 shows that

$$\kappa' \simeq k_\phi, \qquad \kappa'' \simeq k_{\phi'}.$$

Also, κ'' is the image of the canonical homomorphism $\Delta_{\mu'} \to \Delta_{\mu''}$, and this determines an embedding $\kappa' \hookrightarrow \kappa''$.

Now, the proof of Corollary 6.18 can be mimicked in our situation, and shows that

$$[\kappa'' \colon \kappa] = \deg(R_{\mu'}(\phi')) = \deg(\psi).$$

This ends the proof of (3). □

The iteration of this procedure yields a MacLane chain based on the initial valuation μ, with strictly better approximations:

$$\mu \xrightarrow{\phi,\gamma} \mu' \xrightarrow{\phi',\gamma'} \mu'' \xrightarrow{\phi'',\gamma''} \cdots, \qquad v(\phi(\theta)) < v(\phi'(\theta)) < v(\phi''(\theta)) < \cdots$$

We emphasize that the initial key polynomial ϕ is not necessarily proper.

We say that this process *converges* to F if after a finite number of steps we reach a valuation μ such that F is a key polynomial for μ. Since key polynomials are minimal, they all have $\deg(\phi) \le \deg(F)$. By Lemma 1.18, the process converges if and only if we reach a key polynomial with $\deg(\phi) = \deg(F)$.

Going in the opposite direction, if μ is an inductive valuation, then the condition $\phi \mid_\mu F$ implies analogous properties of F with respect to the intermediate valuations of any MacLane chain of μ.

Corollary 10.4. *With the above notation, suppose that $\phi \mid_\mu F$ and μ admits a MacLane chain*

$$\mu_{-\infty} \xrightarrow{\phi_0,\gamma_0} \mu_0 \xrightarrow{\phi_1,\gamma_1} \mu_1 \xrightarrow{\phi_2,\gamma_2} \cdots \xrightarrow{\phi_{r-1},\gamma_{r-1}} \mu_{r-1} \xrightarrow{\phi_r,\gamma_r} \mu_r = \mu.$$

Then, if we agree that $\mu_{-1} = \mu_{-\infty}$, we have

$$\phi_i \mid_{\mu_{i-1}} F, \quad 0 \le i \le r; \qquad v(\phi_i(\theta)) = \gamma_i, \quad 0 \le i < r. \tag{10.4}$$

Moreover, if $\phi \not\sim_\mu \phi_r$, then $v(\phi_r(\theta)) = \gamma_r$ as well.

Proof. Suppose $\phi \not\sim_\mu \phi_r$. Then, Proposition 6.16 shows that $\deg(R_r(\phi)) > 0$.

Since $F \sim_\mu \phi^\ell$, we have $R_r(F) = R_r(\phi)^\ell$ by Corollaries 6.7 and 6.8. Then, by Lemma 6.3,

$$\ell(N_r^{\rm pp}(F)) \geq \ell(S_{\gamma_r}(F)) = e_r \deg(R_r(F)) > 0.$$

This implies that $\phi_r \mid_{\mu_{r-1}} F$ by Lemma 3.6.

Since $F \neq \phi_r$ (because $R_r(\phi_r) = 1$), Theorem 10.2 shows that $N_r(F)$ is one-sided of slope $-v(\phi_r(\theta))$. On the other hand, the slope of this one-sided polygon must be $-\gamma_r$, because otherwise $R_r(F)$ would be a constant. Therefore, $v(\phi_r(\theta)) = \gamma_r$.

Suppose $\phi \sim_\mu \phi_r$. Then, $\phi_r \mid_\mu F$ and Theorem 10.2 shows that

$$\mu_{r-1}(\phi_r) < \gamma_r = \mu(\phi_r) < v(\phi_r(\theta)).$$

Hence, $\phi_r \mid_{\mu_{r-1}} F$, again by Theorem 10.2.

Finally, since in a MacLane chain $\phi_i \not\sim_{\mu_{i-1}} \phi_{i-1}$ for all i, the iteration of these arguments ends the proof of (10.4). □

Let us remark that, although $\mu_{-\infty}$ is incommensurable, it satisfies Theorem 10.2 too. Actually, we have

$$\phi_0 \mid_{\mu_{-\infty}} F, \qquad \forall\, \phi_0 \in \mathrm{KP}(\mu_{-\infty}),\ \forall\, F \in \mathbb{P},$$

because $\phi_0 \sim_{\mu_{-\infty}} x$ and $F \sim_{\mu_{-\infty}} x^{\deg(F)}$. Also,

$$\mu_{-\infty}(\phi_0) = (-1, 0) < (0, v(\phi_0(\theta))), \qquad \forall\, \phi_0 \in \mathrm{KP}(\mu_{-\infty}),\ \forall\, F \in \mathbb{P},$$

where θ is a root of F in $\overline{K}$.

10.2 Semivaluation of a prime polynomial

For a given prime polynomial $F \in \mathbb{P}$, what valuations μ admit key polynomials ϕ such that $\phi \mid_\mu F$?

In order to address this question, let us consider the semivaluation $v_F \in \mathbb{V}$ determined as follows:

$$v_F \colon K[x] \longrightarrow\!\!\!\!\rightarrow K_F \xrightarrow{v} \mathbb{Q}\Gamma \cup \{\infty\}.$$

The support of v_F is the prime ideal $FK[x]$. Clearly,

$$v_F(f) = v(f(\theta)), \qquad \forall\, f \in K[x].$$

Now, we are able to answer the posed question for inductive valuations.

Theorem 10.5. *Let $F \in \mathbb{P}$ be a prime polynomial. For any inductive valuation $\mu \in \mathbb{V}^{\rm ind}$ we have*

$$\exists \phi \in \mathrm{KP}(\mu) \ \text{ such that } \ \phi \mid_\mu F \iff \mu < v_F.$$

In this case, for all non-zero $f \in K[x]$,

$$\mu(f) = v_F(f) \iff \phi \nmid_\mu f. \tag{10.5}$$

Proof. If $\mu < v_F$, we may consider $\phi \in K[x]$ monic with minimal degree among all polynomials satisfying $\mu(\phi) < v_F(\phi)$. By Lemma 2.9, ϕ is a key polynomial for μ, and condition (10.5) is satisfied. In particular, $\phi \mid_\mu F$.

Conversely, suppose that $\phi \mid_\mu F$ for some $\phi \in \mathrm{KP}(\mu)$. Take a MacLane chain of μ of length r, as in (5.1).

Let us prove simultaneously the inequality $\mu < v_F$ and the equivalence (10.5), by induction on the length r of the MacLane chain of μ.

Suppose that, either $r = 0$, or $r > 0$ and both statements hold for all valuations admitting MacLane chains of lower length.

If $\phi \sim_\mu \phi_r$, then $\phi_r \mid_\mu F$ and $\mu(\phi_r) < v(\phi_r(\theta))$ by Theorem 10.2.

If $\phi \not\sim_\mu \phi_r$, then $\mu(\phi_r) = v(\phi_r(\theta))$ by Corollary 10.4. In any case,

$$\mu(\phi_r) \leq v_F(\phi_r).$$

On the other hand, take $a \in K[x]_{\deg(\phi_r)}$. If $r = 0$, then $a \in K$ and $\mu(a) = v(a) = v_F(a)$. If $r > 0$, the condition $\phi_r \nmid_{\mu_{r-1}} a$ implies by the induction hypothesis:

$$\mu(a) = \mu_{r-1}(a) = v_F(a).$$

Therefore, $\mu < v_F$, because for any non-zero $f \in K[x]$ with ϕ_r-expansion $f = \sum_{0 \leq s} a_s \phi_r^s$, we have

$$v_F(f) \geq \mathrm{Min}\,\{v_F(a_s\phi_r^s) \mid 0 \leq s\} \geq \mathrm{Min}\,\{\mu\,(a_s\phi_r^s) \mid 0 \leq s\} = \mu(f).$$

Finally, let ϕ' be a monic polynomial of minimal degree satisfying $\mu(\phi') < v_F(\phi')$. By Proposition 2.9, ϕ' is a key polynomial for μ satisfying (10.5). In particular, $\phi' \mid_\mu \phi$, and this implies $\phi' \sim_\mu \phi$ by Proposition 1.31. Hence, ϕ satisfies (10.5) too. □

Remark. Theorem 10.5 provides a practical device for the computation of v_F.

Given $f \in K[x]$, we need only to find a pair (μ, ϕ) such that $\phi \mid_\mu F$ and $\phi \nmid_\mu f$, leading to $v(f(\theta)) = \mu(f)$.

This yields a very efficient routine for the computation of the valuations attached to prime ideals in number fields or places of function fields [10, 11].

Corollary 10.6. *Let μ be an inductive valuation, and ϕ a key polynomial for μ. Let $F \in K[x]$ be a prime polynomial such that $\phi \mid_\mu F$. Then,*

(1) For any $g \in K[x]$ with $\deg(g) < \deg(\phi)$, we have $v_\phi(g) = \mu(g) = v_F(g)$.

In particular, $e(\phi) \mid e(F)$.

(2) The residual field k_ϕ is contained in the residual field k_F, so that $f(\phi) \mid f(F)$.

Proof. If $g \in K[x]_{\deg(\phi)}$, then $\phi \nmid_\mu g$ and

$$v(g(\alpha)) = \mu(g) = v(g(\theta)),$$

by Proposition 1.21 and Theorem 10.5, respectively. This proves (1).

Let us prove (2). By Theorem 10.5, $\mu < v_F$. Hence, we have a canonical ring homomorphism

$$\Delta_\mu \longrightarrow k_F, \qquad g + \mathcal{P}_0^+(\mu) \longmapsto g(\theta) + \mathfrak{m}_F.$$

The kernel $\mathcal{L}_F$ of this homomorphism is a non-zero prime ideal of Δ_μ. Since this ring is a PID, $\mathcal{L}_F$ is a maximal ideal.

Clearly, $\mathcal{R}_\mu(F) \subset \mathcal{L}_F$. Hence, Theorem 10.2 shows that, $\mathcal{R}_\mu(F) = \mathcal{R}_\mu(\phi)^a \subset \mathcal{L}_F$ for a certain positive integer a. Thus, $\mathcal{R}_\mu(\phi) = \mathcal{L}_F$, because both are maximal ideals.

Therefore, $k_\phi \simeq \Delta_\mu/\mathcal{R}_\mu(\phi) = \Delta_\mu/\mathcal{L}_F$, which is isomorphic to a subfield of k_F. □

10.3 A generalization of Hensel's lemma

We now deduce from Theorem 10.2 the fundamental result concerning factorization of polynomials over K. It has to be considered as a vast generalization of Hensel's lemma.

Leu us introduce some useful notation.

Notation. Let ϕ be a key polynomial for the valuation $\mu \in \mathbb{V}$.

For each $\gamma \in \mathbb{Q}\Gamma$ such that $\gamma > \mu(\phi)$, we denote

- $\mu_\gamma := [\mu; \phi, \gamma]$.
- e_γ the relative ramification index of μ_γ.

  That is, the least positive integer such that $e_\gamma\gamma \in \Gamma_{\mu_\gamma,\deg(\phi)} = \Gamma_{\mu,\deg(\phi)}$.
- κ_γ the algebraic closure of k in Δ_{μ_γ}.
- $R_{\mu_\gamma}\colon K[x] \longrightarrow \kappa_\gamma[y]$ the residual polynomial operator determined by the pair ϕ, u, where $u \in K[x]_{\deg(\phi)}$ is any small polynomial with $\mu(u) = e_\gamma\mu_\gamma(\phi) = e_\gamma\gamma$.

Theorem 10.7. *Let ϕ be a key polynomial for the valuation $\mu \in \mathbb{V}$. Let $f \in K[x]$ be a monic polynomial.*

For each slope $-\gamma$ of the principal Newton polygon $N^{pp}_{\mu,\phi}(f)$, let

$$R_{\mu_\gamma}(f) = \prod\nolimits_\psi \psi^{a_\psi} \in \kappa_\gamma[y],$$

be the factorization of $R_{\mu_\gamma}(f)$ into a product of pairwise different monic irreducible polynomials $\psi \in \kappa_\gamma[y]$.

Then, f factorizes in $K[x]$ into a product of monic polynomials:

$$f = f_0\, \phi^{\mathrm{ord}_\phi(f)} \prod\nolimits_{(\gamma,\psi)} f_{\gamma,\psi},$$

where $-\gamma$ runs on the slopes of $N^{pp}_{\mu,\phi}(f)$ and, for each γ, ψ runs on the monic irreducible factors of $R_{\mu_\gamma}(f)$ in $\kappa_\gamma[y]$.

If we denote $\ell = \ell\left(N^{pp}_{\mu,\phi}(f)\right)$, the degrees of the factors are given by

$$\deg(f_0) = \deg(f) - \ell\deg(\phi), \qquad \deg(f_{\gamma,\psi}) = e_\gamma a_\psi \deg(\psi)\deg(\phi).$$

Moreover, for any pair (γ, ψ), it holds:

(1) $N_{\mu,\phi}(f_{\gamma,\psi})$ *is one-sided of length* $e_\gamma a_\psi \deg(\psi)$ *and slope* $-\gamma$.

(2) For all roots $\theta \in \overline{K}$ *of* $f_{\gamma,\psi}$, *we have* $v(\phi(\theta)) = \gamma$.

(3) If $a_\psi = 1$, *then* $f_{\gamma,\psi}$ *is irreducible.*

Proof. Let $f = F_1 \cdots F_t$ be the factorization of f into a product of prime polynomials in $K[x]$. We are not assuming that f is separabe, so that these irreducible factors are not necessarily pairwise different.

The idea is that we may group the factors $F_1, \dots, F_t$ according to some of their properties with respect to the pair μ, ϕ. The crucial point is that we are able to identify the degrees of the resulting factors of f in terms of computable discrete data.

- The factor f_0 is the product of all F_j satisfying $\phi \nmid_\mu F_j$.
- The factor $\phi^{\mathrm{ord}_\phi(f)}$ is the product of all F_j equal to ϕ.
- The factor $f_{\gamma,\psi}$ is the product of all F_j such that $\phi \mid_\mu F_j$, $N_{\mu,\phi}(F_j)$ is one-sided of slope $-\gamma$ and $R_{\mu_\gamma}(F_j)$ is a power of ψ.

By Lemma 3.6 we have

$$\ell_j := \ell\left(N^{\mathrm{pp}}_{\mu,\phi}(F_j)\right) = s_{\mu,\phi}(F_j), \qquad 1 \le j \le t,$$

so that $\ell_j = 0$ if $\phi \nmid_\mu F_j$, and $\ell_j = 1$ if $F_j = \phi$. By Theorem 10.2,

$$\phi \mid_\mu F_j \implies \deg(F_j) = \ell_j \deg(\phi).$$

By Theorem 3.10, $N^{\mathrm{pp}}_{\mu,\phi}(f) = \sum_{j=1}^t N^{\mathrm{pp}}_{\mu,\phi}(F_j)$, so that $\ell = \sum_{j=1}^t \ell_j$. Hence,

$$\deg(f) - \deg(f_0) = \sum_{\phi|_\mu F_j} \deg(F_j) = \sum_{\phi|_\mu F_j} \ell_j \deg(\phi) = \sum_{j=1}^t \ell_j \deg(\phi) = \ell \deg(\phi).$$

By Theorem 10.2 and Corollary 10.3, 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 a certain slope $-\gamma$, and $R_{\mu_\gamma}(F_j)$ is a power of some irreducible $\psi \in \kappa_\gamma[y]$. By Theorem 3.10, $-\gamma$ is one of the slopes of $N^{\mathrm{pp}}_{\mu,\phi}(f)$, and by Lemma 1.29, ψ is one of the irreducible factors of $R_{\mu_\gamma}(f)$.

Therefore, every irreducible factor F_j such that $F_j \neq \phi$ and $\phi \mid_\mu F_j$ falls into one (and only one) of the factors $f_{\gamma,\psi}$.

Also, for any $f_{\gamma,\psi}$, items (1), (2) follow from Theorems 3.10 and 10.2, respectively.

Finally, for any pair γ, ψ, Lemma 1.29 shows that

$$R_{\mu_\gamma}(f_{\gamma,\psi}) = \prod\nolimits_j R_{\mu_\gamma}(F_j),$$

for F_j running on all irreducible factor of $f_{\gamma,\psi}$. In particular,

$$a_\psi = \sum\nolimits_j \mathrm{ord}_\psi\, R_{\mu_\gamma}(F_j).$$

Hence, if $a_\psi = 1$, there can be only one such irreducible factor. □

If the valuation μ is inductive, we obtain more information about the irreducible factors of f.

Corollary 10.8. *With the above notation, suppose that μ is an inductive valuation. Then, for any pair γ, ψ we have:*

(1) All irreducible factors F_j of $f_{\gamma,\psi}$ satisfy

$$e(\phi)\, e_\gamma \mid e(F_j), \qquad f(\phi)\deg(\psi) \mid f(F_j).$$

(2) If $a_\psi = 1$, then $F = f_{\gamma,\psi}$ is a defectless polynomial with

$$e(F) = e(\phi)\, e_\gamma, \qquad f(F) = f(\phi)\deg(\psi).$$

Proof. By Corollary 10.3, there exists ϕ_γ key polynomial for μ_γ such that

$$R_{\mu_\gamma}(\phi_\gamma) = \psi, \qquad \phi_\gamma \mid_{\mu_\gamma} F_j,$$

for all prime factors F_j of $f_{\gamma,\psi}$. Now, by Corollaries 10.3 and 10.6, we have

$$e(\phi)\, e_\gamma = e(\phi_\gamma) \mid e(F_j), \qquad f(\phi)\deg(\psi) = f(\phi_\gamma) \mid f(F_j).$$

This proves (1).

Suppose $a_\psi = 1$. By Theorem 10.7, $F = f_{\gamma,\psi}$ is irreducible and satisfies:

$$\begin{aligned} &N_{\mu_\gamma,\phi}(F) = N_{\mu,\phi}(F) \ \text{ is one-sided of slope } -\gamma, \\ &R_{\mu_\gamma}(F) = \psi, \qquad \deg(F) = e_\gamma \deg(\psi)\deg(\phi). \end{aligned}$$

By Proposition 1.30, F is a key polynomial for μ_γ. By Theorem 8.6, F is a defectless polynomial. In particular,

$$e(F)f(F) = \deg(F) = e_\gamma \deg(\psi)\deg(\phi) = e_\gamma \deg(\psi) e(\phi) f(\phi).$$

Therefore, the equalities $e(F) = e(\phi)\, e_\gamma$, $f(F) = f(\phi)\deg(\psi)$ follow from item (1). □

Remark. These results, with a slightly different formulation, have been recently found by Jakhr-Khanduja [14]. The authors use the technique of *lifting* of residual polynomials instead of the residual polynomial operator.

Theorem 10.7 and Corollary 10.8 are valid for an arbitrary valued field (K, v), as long as the valuation μ is inductive. In this case, μ may be lifted to the henselization K^h, and ϕ is still a key polynomial of the lifted valuation (see section 8.3).

In this way, these results may be used to detect information about the prime factors in $K^h[x]$ of some given $f \in K[x]$. Actually, they constitute the key stone to design an OM algorithm of polynomial factorization over $K^h[x]$ of polynomials in $K[x]$, following the lines of the classical OM algorithm for discrete rank one valuations [9, 8, 10, 11].

However, as we shall see in the next section, this algorithm only works for polynomials $f \in K[x]$ all whose prime factors in $K^h[x]$ are defectless.

10.4 Okutsu frames of defectless polynomials

We keep dealing with a prime polynomial $F \in \mathbb{P}$ and a fixed root $\theta \in \overline{K}$ of F.

For any integer $1 < m \leq \deg(F)$, consider the set of values

$$\Lambda_m(F) = \left\{ \frac{v(g(\theta))}{\deg(g)} \;\middle|\; g \in K[x] \text{ monic }, \ 0 < \deg(g) < m \right\} \subset \mathbb{Q}\Gamma.$$

Definition 10.9. *Suppose that $n = \deg(F) > 1$ and $\Lambda_n(F)$ contains a maximal value. Denote*

$$C(F) := \operatorname{Max}\left(\Lambda_n(F)\right).$$

We say that ϕ, F is a distinguished pair *of polynomials if $\phi \in K[x]$ is a monic polynomial of minimal degree among the monic polynomials satisfying*

$$0 < \deg(\phi) < \deg(F), \qquad v(\phi(\theta))/\deg(\phi) = C(F).$$

Definition 10.10. *We say that F is an* Okutsu polynomial *if either $\deg(F) = 1$, or all sets $\Lambda_m(F)$, for $1 < m \leq \deg(F)$, contain a maximal element.*

Suppose that F is an Okutsu polynomial, and ϕ, F is a distinguished pair.

If $\deg(\phi) > 1$, then we may consider a monic polynomial $\phi' \in K[x]$ of minimal degree such that

$$0 < \deg(\phi') < \deg(\phi), \qquad \frac{v(\phi'(\theta))}{\deg(\phi')} = C'(F) := \operatorname{Max}\left(\Lambda_{\deg(\phi)}(F)\right).$$

Note that, by the minimality of $\deg(\phi)$, we necessarily have $C'(F) < C(F)$.

An iteration of this argument leads to a finite family

$$\phi_0, \phi_1, \ldots, \phi_r, \phi_{r+1} = F$$

of monic polynomials in $K[x]$ such that

$$1 = \deg(\phi_0) < \deg(\phi_1) < \cdots < \deg(\phi_r) < \deg(F), \tag{10.6}$$

whose weighted values $C_i(F) := v(\phi_i(\theta))/\deg(\phi_i)$ satisfy:

$$\deg(g) < \deg(\phi_{i+1}) \implies \frac{v(g(\theta))}{\deg(g)} \leq C_i(F) < C_{i+1}(F), \qquad 0 \leq i \leq r, \tag{10.7}$$

for any monic polynomial $g \in K[x]$ of positive degree.

Note that $C_r(F) = C(F)$ and $C_{r+1}(F) = \infty$.

Definition 10.11. *An* Okutsu frame *of an Okutsu polynomial F, is a list*

$$[\phi_0, \phi_1, \ldots, \phi_r]$$

of monic polynomials in $K[x]$ satisfying (10.6) and (10.7).

The length r of the frame is called the Okutsu depth *of F. Clearly, the depth r, the degrees $\deg(\phi_0), \ldots, \deg(\phi_r)$, and the values $C_0(F), \ldots, C_r(F) = C(F) \in \mathbb{Q}\Gamma$ are intrinsic data of F.*

If $\deg(F) = 1$, then we agree that the empty list [ ] is an Okutsu frame of F, and we say that F has Okutsu depth equal to $-\infty$.

Lemma 10.12. *Let $[\phi_0, \phi_1, \dots, \phi_r]$ be an Okutsu frame of an Okutsu polynomial F. Then, $\phi_0, \dots, \phi_r$ are prime polynomials too.*

Proof. For $0 \le i \le r$, suppose $\phi_i = ab$ with $\deg(a), \deg(b) < \deg(\phi_i)$. By (10.7),

$$v(a(\theta))/\deg(a), \quad v(b(\theta))/\deg(b) < C_i(F).$$

This leads to a contradiction:

$$C_i(F) = \frac{v(\phi_i(\theta))}{\deg(\phi_i)} = \frac{v(a(\theta)) + v(b(\theta))}{\deg(\phi_i)} < \frac{\deg(a)C_i(F) + \deg(b)C_i(F)}{\deg(\phi_i)} = C_i(F).$$

□

For instance, any key polynomial ϕ for an inductive valuation μ is an Okutsu polynomial, and any optimal MacLane chain of μ determines an Okutsu frame of ϕ.

Theorem 10.13. *Consider an optimal MacLane chain of an inductive valuation:*

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu.$$

Let ϕ be a key polynomial for μ. Then, ϕ is an Okutsu polynomial, and

(1) If $\deg(\phi) > \deg(\phi_r)$, then $[\phi_0, \dots, \phi_r]$ is an Okutsu frame of ϕ.

(2) If $\deg(\phi) = \deg(\phi_r)$, then $[\phi_0, \dots, \phi_{r-1}]$ is an Okutsu frame of ϕ.

Moreover, $C(\phi) = C(\mu)$ in the first case, and $C(\phi) = C(\mu_{r-1})$ in the second case.

Proof. Let $\alpha \in \overline{K}$ be a root of ϕ.

Suppose $\deg(\phi) > \deg(\phi_r)$, so that $\phi \nmid_\mu \phi_r$. For any monic $g \in K[x]_{\deg(\phi)}$ we have $\phi \nmid_\mu g$ too, so that

$$v(\phi_r(\alpha)) = \mu(\phi_r), \qquad v(g(\alpha)) = \mu(g),$$

by Proposition 1.21. By Theorem 1.27,

$$\frac{v(g(\alpha))}{\deg(g)} = \frac{\mu(g)}{\deg(g)} \le C(\mu) = \frac{\mu(\phi_r)}{\deg(\phi_r)} = \frac{v(\phi_r(\alpha))}{\deg(\phi_r)},$$

and equality holds if and only if g is μ-minimal.

By Propositions 2.2 and 1.26, ϕ_r is a key polynomial for μ of minimal degree, and there are no μ-minimal polynomials of degree less than $\deg(\phi_r)$.

Therefore, ϕ_r, ϕ is a distinguished pair, and $C(\phi) = C(\mu)$.

Since the MacLane chain is optimal, we have $\deg(\phi_{i+1}) > \deg(\phi_i)$ for all $0 \le i < r$, and this argument shows that ϕ_i, ϕ_{i+1} is a distinguished pair and $C(\phi_{i+1}) = C(\mu_i)$.

On the other hand, if $\alpha_{i+1} \in \overline{K}$ is a root of ϕ_{i+1}, Corollary 10.6 shows that

$$g \in K[x],\ \deg(g) < \deg(\phi_{i+1}) \implies v(g(\alpha_{i+1})) = v(g(\alpha)).$$

Thus, $\Lambda_{\deg(\phi_{i+1})}(\phi)$ contains a maximal value and $C(\phi_{i+1}) = C_{i+1}(\phi) = C(\mu_i)$.

This ends the proof of (1).

Suppose $\deg(\phi) = \deg(\phi_r)$. The tautology $\phi \mid_\mu \phi$ implies $\phi_r \mid_{\mu_{r-1}} \phi$ by (10.4). Hence, ϕ is a key polynomial for μ_{r-1} by Lemma 1.18.

Now, $\deg(\phi) > \deg(\phi_{r-1})$, and item (2) follows from the previous argument applied to the optimal MacLane chain of μ_{r-1} deduced by truncation. □

Conversely, any Okutsu frame of an Okutsu polynomial arises in this way.

Theorem 10.14. *Let F be an Okutsu polynomial, and let $[\phi_0, \dots, \phi_r]$ be an Okutsu frame of $\phi_{r+1} = F$. For all $0 \le i \le r$, denote $\gamma_i = v_F(\phi_i)$ and consider the mapping*

$$\mu_i \colon K[x] \longrightarrow \mathbb{Q}\Gamma \cup \{\infty\}, \qquad \sum_{0\le s} a_s \phi_i^s \longmapsto \operatorname{Min}\{v_F(a_s) + s\gamma_i \mid 0 \le s\}.$$

Then, μ_i is a valuation, ϕ_{i+1} is a key polynomial for μ_i, and μ_r admits an optimal MacLane chain

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r.$$

Proof. The coefficients $a_s \in K$ of any ϕ_0-expansion satisfy $v_F(a_s) = v(a_s)$. Hence, $\mu_0(\phi_0, \gamma_0) = \mu_0$ by the very definition of the depth-zero valuations.

In section 4.2 we saw that $\mu_0(\phi_0, \gamma_0)$ may be identified with the augmentation $[\mu_{-\infty};\, \phi_0, (0, \gamma_0)]$; thus, ϕ_0 is a key polynomial for μ_0, by Proposition 2.2.

Now, suppose that for some $0 \le i \le r$, we know that μ_i is a valuation and ϕ_i is a key polynomial for μ_i. Let us show that ϕ_{i+1} is a key polynomial for μ_i too.

First, note that $\mu_i < v_F$. In fact, for any polynomial $f = \sum_{0\le s} a_s \phi_i^s$,

$$v_F(f) \ge \operatorname{Min}\{v_F\left(a_s\phi_i^s\right) \mid 0 \le s\} = \mu_i(f).$$

Let $\phi \in K[x]$ be a monic polynomial of minimal degree such that $\mu_i(\phi) < v_F(\phi)$. By Proposition 2.9, ϕ is a key polynomial for μ_i and for any polynomial $f \in K[x]$,

$$\mu_i(f) < v_F(f) \iff \phi \mid_{\mu_i} f. \tag{10.8}$$

In particular, $\phi \mid_{\mu_i} F$, and Theorem 10.2 shows that $\mu_i(\phi) < v(\phi(\theta))$. On the other hand, Theorem 1.27 shows that

$$\frac{v(\phi(\theta))}{\deg(\phi)} > \frac{\mu_i(\phi)}{\deg(\phi)} = C(\mu_i) = \frac{\mu_i(\phi_i)}{\deg(\phi_i)} = \frac{v(\phi_i(\theta))}{\deg(\phi_i)} = C_i(F), \tag{10.9}$$

$$\frac{v(\phi_{i+1}(\theta))}{\deg(\phi_{i+1})} = C_{i+1}(F) > C_i(F) = C(\mu_i) \ge \frac{\mu_i(\phi_{i+1})}{\deg(\phi_{i+1})}. \tag{10.10}$$

By (10.7) and (10.9), we have $\deg(\phi) \ge \deg(\phi_{i+1})$. Also, (10.8) and (10.10) imply $\phi \mid_{\mu_i} \phi_{i+1}$, leading to $\deg(\phi) \le \deg(\phi_{i+1})$, by the μ_i-minimality of ϕ.

Hence, $\deg(\phi) = \deg(\phi_{i+1})$ and Lemma 1.18 shows that $\phi \sim_{\mu_i} \phi_{i+1}$ and ϕ_{i+1} is a key polynomial for μ_i.

Finally, the theorem will follow from a recursive argument, if we show that

$$\mu_{i+1} = [\mu_i;\, \phi_{i+1}, \gamma_{i+1}], \qquad 0 \le i < r.$$

In fact, let $f = \sum_{0 \leq s} a_s(\phi_{i+1})^s$ be the ϕ_{i+1}-expansion of a non-zero $f \in K[x]$. Since $\phi_{i+1} \mid_{\mu_i} F$, Corollary 10.6 shows that,

$$\deg(a_s) < \deg(\phi_{i+1}) \implies \mu_{i+1}(a_s) = \mu_i(a_s) = v_F(a_s).$$

Hence, $\mu_{i+1} = [\mu_i; \phi_{i+1}, \gamma_{i+1}]$ by the very definition of the augmented valuation. □

Theorem 10.15. *Let $F \in \mathbb{P}$ be a prime polynomial. The following conditions are equivalent:*

(1) F is the key polynomial of an inductive valuation.

(2) F is an Okutsu polynomial.

(3) F is defectless.

Proof. By Theorems 10.13 and 10.14, items (1) and (2) are equivalent. Also, Theorem 8.6 shows that (1) implies (3).

Hence, we need only to show that (3) implies (1). This follows immediately from the results of Vaquié in [30] and [31].

Suppose that F is a defectless polynomial with $\deg(F) > 1$. In section 10.1, we showed how to construct a MacLane chain of inductive valuations in the interval $(\mu_{-\infty}, v_F) \subset \mathbb{V}$:

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{n-1},\gamma_{n-1}}{\longrightarrow} \mu_{n-1} \overset{\phi_n,\gamma_n}{\longrightarrow} \mu_n \overset{\phi_{n+1},\gamma_{n+1}}{\longrightarrow} \cdots$$

of arbitrarily large length, with key polynomials satisfying $\phi_{i+1} \mid_{\mu_i} F$ for all i.

If at some stage we get $\deg(\phi_{n+1}) = \deg(F)$, then Lemma 1.18 shows that F is a key polynomial for the inductive valuation μ_n, and we are done.

Not getting $F \in \mathrm{KP}(\mu_n)$ for all finite n, implies that the degree of the key polynomials becomes stationary: there is an index n_0 such that $\deg(\phi_n) = \deg(\phi_m)$ for all $n, m \geq n_0$. Then, we get a *continuous MacLane chain* which may be augmented to a certain *limit augmented* valuation by using a certain *limit key polynomial* [30].

This limit augmented valuation lies still in the interval $(\mu_{-\infty}, v_F) \subset \mathbb{V}$, but it is no more inductive. The main result of [31] shows that in this case F has some defect. □

Remark. The implication (3) $\implies$ (1) may also be deduced from some work by Aghigh and Khanduja [2], who use the technique of *complete distinguished chains* linking the root θ of F with some element in K by a sequence of *distinguished pairs* of algebraic elements over K.

The last three theorems show that "MacLane chains of inductive valuations" and "Okutsu frames" are equivalent objects, only attachable to defectless polynomials.

This double perspective of the same objects has many consequences. The most important one is that any defectless polynomial determines a canonical inductive valuation.

Definition 10.16. *Let F be a defectless polynomial with* $\deg(F) > 1$. *The* Okutsu bound *of F is defined as*

$$\delta_0(F) = \deg(F)\, C(F) \in \mathbb{Q}\Gamma.$$

We may associate with F an inductive valuation

$$\mu_F \colon K[x] \to \mathbb{Q}\Gamma \cup \{\infty\},$$

determined by the following action on F-expansions $f = \sum_{0\le s} a_s F^s$:

$$\mu_F(f) = \operatorname{Min}\{v_F(a_s) + s\,\delta_0(F) \mid 0 \le s\}.$$

This valuation μ_F is a kind of limit of the process of "approaching F with key polynomials", described in section 10.1. Let us justify that μ_F is a valuation, and mention some of its basic properties.

Lemma 10.17. *Let F be a defectless polynomial with $\deg(F) > 1$.*

(1) The mapping μ_F is an inductive valuation, and F is a key polynomial for μ_F.

(2) If ϕ, F is a distinguished pair, then ϕ is a key polynomial of minimal degree for μ_F.

(3) The interval $(\mu_F, v_F) \subset \mathbb{V}$ consists of all augmentations

$$\mu = [\mu_F;\, F, \gamma], \qquad \gamma \in (\delta_0(F), \infty) \subset \mathbb{Q}\Gamma.$$

(4) If $\mu \in (\mu_{-\infty}, \mu_F)$ admits a key polynomial ϕ such that $\phi \mid_\mu F$, then $\deg(\phi) < \deg(F)$.

Proof. Let $[\phi_0, \dots, \phi_r]$ be an Okutsu frame of F. By Theorem 10.14, the inductive valuation $\mu := \mu_r$ admits F as a key polynomial. By Corollary 10.6,

$$a \in K[x], \quad \deg(a) < \deg(F) \implies \mu(a) = v_F(a).$$

Since F is μ-minimal, for any $f \in K[x]$ with F-expansion $f = \sum_{0\le s} a_s F^s$, Lemma 1.16 shows that

$$\mu(f) = \operatorname{Min}\{\mu(a_s F^s) \mid 0 \le s\} = \operatorname{Min}\{v_F(a_s) + s\,\mu(F) \mid 0 \le s\}. \tag{10.11}$$

Since $\phi_r \mid_\mu F$, Theorem 1.27 shows that

$$\mu(F) = \frac{\deg(F)}{\deg(\phi_r)}\,\mu(\phi_r) = \frac{\deg(F)}{\deg(\phi_r)}\,v_F(\phi_r) = \deg(F)C(F) = \delta_0(F).$$

Hence, the equality in (10.11) shows that $\mu_F = \mu$ is a valuation admitting F as a key polynomial.

Let r be the Okutsu depth of F. If ϕ, F is a distinguished pair, we can consider an Okutsu frame of F with $\phi = \phi_r$.

By Theorem 10.14, $\mu_F = \mu = [\mu_{r-1};\, \phi, \gamma_r]$, where we agree that $\mu_{-1} = \mu_{-\infty}$. By Proposition 2.2, ϕ is a key polynomial for μ_F of minimal degree.

Let $\mu \in \mathbb{V}$ be any valuation such that $\mu_F < \mu < v_F$. For any $a \in K[x]$ with $\deg(a) < \deg(F)$ we have $\mu_F(a) = \mu(a) = v_F(a)$.

Hence, F is a monic polynomial of minimal degree satisfying $\mu(F) < v_F(F) = \infty$. By Proposition 2.9, F is a key polynomial for μ. In particular, F is μ-minimal, and satisfies (10.11).

If $\mu(F) = \mu_F(F)$, this implies $\mu = \mu_F$. If $\mu(F) > \mu_F(F)$, this implies $\mu = [\mu_F;\, F, \mu(F)]$, with $\mu(F) \in (\delta_0(F), \infty)$.

Suppose that a valuation $\mu < \mu_F$ admits a key polynomial ϕ such that $\phi \mid_\mu F$. Since ϕ is μ-minimal, we have $\deg(\phi) \leq \deg(F)$.

By Lemma 1.18, the equality $\deg(\phi) = \deg(F)$ implies $\phi \sim_\mu F$ and F is a key polynomial for μ. Since F is a key polynomial for μ_F as well, Lemma 6.20 shows that $\mu_F = [\mu;\, F, \mu(F)]$. But this implies that F is a key polynomial for μ_F of minimal degree, contradicting item (2). Hence, necessarily $\deg(\phi) < \deg(F)$. □

Let us deduce some more properties of defectless polynomials from the fundamental Theorems 10.13, 10.14 and 10.15.

Corollary 10.18. *Let F be a defectless polynomial with $\deg(F) > 1$.*

The sequence $[\phi_0, \phi_1, \ldots, \phi_r]$ is an Okutsu frame of $\phi_{r+1} = F$ if and only if ϕ_i, ϕ_{i+1} is a distinguished pair for all $0 \leq i \leq r$.

In this case, each ϕ_i is a defectless polynomial and $[\phi_0, \ldots, \phi_{i-1}]$ is an Okutsu frame of ϕ_i. Moreover, $C_i(F) = C(\phi_{i+1})$ for all $1 \leq i \leq r$.

Proof. For $1 \leq i \leq r+1$, let $\alpha_i \in \overline{K}$ be a root of ϕ_i.

The pair ϕ_i, ϕ_{i+1} is distinguished if and only if $v(\phi_i(\alpha_{i+1}))/\deg(\phi_i)$ is maximal among all monic polynomials g of degree less than $\deg(\phi_{i+1})$.

By Theorem 10.14 and Corollary 10.6, all these polynomials g satisfy

$$v(g(\alpha_{i+1})) = v(g(\theta)).$$

This proves the first statement and $C_i(F) = C(\phi_{i+1})$ for all $1 \leq i \leq r$.

The second statements follows directly from Theorems 10.13 and 10.14. □

Maximal values of v_F on polynomials of a prescribed degree

Let us fix a degree $m < \deg(F)$, and consider the set of values

$$\Gamma_m(F) = \{v(g(\theta)) \mid g \in K[x] \text{ monic},\ \deg(g) = m\} \subset \mathbb{Q}\Gamma.$$

Definition 10.19. *A monic polynomial $g \in K[x]$ of degree less than $\deg(F)$ is said to be* F-maximal *if $v(g(\theta)) = \operatorname{Max}\big(\Gamma_{\deg(g)}(F)\big)$.*

Clearly, 1 is the only F-maximal polynomial of degree zero.

Let F be an defectless polynomial, with Okutsu frame $[\phi_0, \ldots, \phi_r]$. Let us denote $m_i = \deg(\phi_i)$ for $0 \leq i \leq r$.

By the definition of an Okutsu frame, the polynomials $\phi_0, \ldots, \phi_r$ are F-maximal of degree $m_0, \ldots, m_r$, respectively.

Also, since for any monic polynomial $g \in K[x]$ with $\deg(g) < \deg(F)$, we have

$$v_F(g)/\deg(g) \leq v_F(\phi_r)/m_r,$$

it is clear that all sets $\Gamma_m(F)$ admit upper bounds.

However, it is not clear from the definition of an Okutsu polynomial, if all these sets $\Gamma_m(F)$ contain a maximal value.

This was proved by Okutsu for the completion of a discrete rank one valuation [24, paper II, Thm. 1]. Actually, Okutsu found, for each degree $m < \deg(F)$, a concrete F-maximal polynomial of degree m.

His result works in our more general context.

Theorem 10.20. *Let F be an defectless polynomial, with Okutsu frame $[\phi_1, \dots, \phi_r]$. Let us denote $m_i = \deg(\phi_i)$ for $0 \le i \le r$.*

Any integer $0 < m < n$ may be written in a unique form as:

$$m = \sum_{i=0}^{r} \ell_i m_i, \qquad 0 \le \ell_i < m_{i+1}/m_i,$$

if we agree that $m_{r+1} = \deg(F)$.

Then, the polynomial $g = \prod_{i=0}^{r} \phi_i^{\ell_i}$ is an F-maximal polynomial of degree m.

Proof. As mentioned above, the result is obvious for $m \in \{0, m_0, m_1, \dots, m_r\}$, being $1, \phi_0, \dots, \phi_r$ F-maximal polynomials for these degrees, respectively.

Suppose that $m_i < m < m_{i+1}$, for some $0 \le i \le r$, where $m_{r+1} = \deg(F)$.

Consider the valuation $\mu_i = \mu_{\phi_{i+1}}$. By Theorem 10.14 and Corollary 10.4, ϕ_i and ϕ_{i+1} are key polynomials for μ_i, and $\phi_{i+1} \mid_{\mu_i} F$.

Take any monic $g \in K[x]$ of degree m, with ϕ_i-expansion $g = \sum_{s=0}^{\ell} a_s \phi_i^s$, where $\ell = \lfloor m/m_i \rfloor$. Corollary 10.6 shows that

$$v_F(g) = \mu_i(g) = \mathrm{Min}\{\mu_i(a_s\phi_i^s) \mid 0 \le s \le \ell\} \le \mu_i\left(a_\ell \phi_i^\ell\right) = v_F\left(a_\ell \phi_i^\ell\right),$$

where a_ℓ is a monic polynomial of degree $m - \ell m_i < m_i$.

Hence, if there exists an F-maximal polynomial a of degree $m - \ell m_i$, then $a\phi^\ell$ is an F-maximal polynomial of degree m.

A recursive argument shows that $g = \prod_{i=0}^{r} \phi_i^{\ell_i}$ is F-maximal of degree m. □

10.5 Types parameterize defectless polynomials

Definition 10.21. *Let μ be an inductive valuation in $\mathbb{V}$. A key polynomial $\phi \in \mathrm{KP}(\mu)$ is said to be* strong *if $\deg(\phi) > m(\mu)$. That is, $\deg(\phi)$ is strictly larger than the minimal degree of key polynomials for μ.*

A strong key polynomial is necessarily proper, but the converse is not true.

The next result is an immediate consequence of Theorems 10.13, 10.14, and Lemma 10.17.

Corollary 10.22. *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 defectless polynomial F with $\deg(F) > 1$ is equal to the MacLane depth of the canonical valuation μ_F. □

Lemma 10.23. *Let μ be an inductive valuation and F a defectless polynomial with $\deg(F) > 1$. Then, $\mu = \mu_F$ if and only if F is a strong key polynomial for μ.*

Proof. If $\mu = \mu_F$, then F is strong by Theorem 10.14 and Lemma 10.17.

Conversely, suppose that $F \in \mathrm{KP}(\mu)$ is strong. By Proposition 1.21, $\mu < v_F$. By Lemma 6.20, if $\mu \neq \mu_F$, then one of the valuations is an augmentation of the other:

$$\mu = [\mu_F;\, F, \mu(F)] \quad \text{or} \quad \mu_F = [\mu;\, F, \delta_0(F)].$$

This implies that F is a key polynomial of minimal degree for the larger valuation. This contradicts our hypotheses, because F is a strong key polynomial for both valuations. □

Notation. *Let us denote by $\mathbb{P}_0$ the set of all defectless polynomials in $K[x]$ of degree greater than 1.*

Lemma 10.24. *Let $F, G \in \mathbb{P}_0$ be two defectless polynomials of the same degree. The following conditions are equivalent:*

(1) $v(G(\theta)) > \delta_0(F)$, where $\theta \in \overline{K}$ 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.

Suppose $F \sim_{\mu_F} G$. Lemma 1.18 shows that G is a strong key polynomial for μ_F. By Lemma 10.23, $\mu_F = \mu_G$ and Proposition 1.31 shows that $\mathcal{R}(F) = \mathcal{R}(G)$. Hence, (2) implies (3).

The implication (3) $\Longrightarrow$ (2) follows directly from Proposition 1.31. □

The symmetry of condition (3) shows that $\approx$ is an equivalence relation on the set $\mathbb{P}_0$.

Two Okutsu equivalent defectless polynomials $F, G \in \mathbb{P}_0$ have the same numerical invariants attached to any optimal MacLane chain of the common canonical valuation $\mu_F = \mu_G$. In particular, equation (5.5) shows that they have the same ramification index

$$e(F) = e_0 \cdots e_r = e(G),$$

where r is their Okutsu depth. Hence, they have the same residual degree too:

$$f(F) = \deg(F)/e(F) = \deg(G)/e(G) = f(G).$$

Also, they have the same Okutsu frames, by Theorems 10.13 and 10.14.

Let us obtain a parameterization of the quotient set $\mathbb{P}_0/\approx$ by an adequate space. The *MacLane space* of the valued field (K, v) is defined to be the set of *strong types*:

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

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 Lemmas 10.23 and 10.24.

Theorem 10.25. *The following mapping is bijective:*

$$\mathbb{M} \longrightarrow \mathbb{P}_0/\approx, \qquad (\mu, \mathcal{L}) \mapsto \{\phi \in \mathrm{KP}(\mu) \mid \mathcal{R}_\mu(\phi) = \mathcal{L}\}\,.$$

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

Chapter 11

Invariants of algebraic elements over henselian fields

In this chapter, we use the techniques and results of Chapter 10 to reobtain some results on the computation of invariants of algebraic elements over henselian fields.

These results may be found in the literature as the combined contribution of several papers [1, 2, 3, 4, 15, 16, 29].

Our aim is to give a unified presentation of these results, with simplified proofs derived in a natural way from the techniques of Chapter 10.

Let (K, v) be a henselian field. We denote still by v the canonical extension of v to a fixed algebraic closure $\overline{K}$ of K.

Let $K \subset K^s \subset \overline{K}$ be the separable closure of K in $\overline{K}$.

Let Γ be the value group of the valuation v, and k its the residue class field.

Notation. For any $g \in K[x]$, we let $\mathrm{Z}(g) \subset \overline{K}$ be the set of its roots in $\overline{K}$.

Throughout the chapter, we fix an algebraic element $\theta \in \overline{K}$, and denote by

$$L = K(\theta)$$

the finite extension of K obtained by adjoining θ to K.

Let $f \in K[x]$ be the minimal (prime) polynomial of θ over K. Denote

$$n = \deg_K(\theta) = [L\colon K] = \deg(f).$$

Consider the following invariant of θ:

$$\omega_K(\theta) = \mathrm{Max}\{v(\theta - \theta') \mid \theta' \in \mathrm{Z}(f),\ \theta' \neq \theta\} \in \mathbb{Q}\Gamma.$$

This value is called *Krasner's constant*. By Krasner's lemma [5, Thm. 4.1.7], if θ is separable over K, then:

$$\alpha \in \overline{K}, \quad v(\theta - \alpha) > \omega_K(\theta) \implies L \subset K(\alpha). \tag{11.1}$$

Let us consider another invariant, which is not always well defined:

$$\delta_K(\theta) = \mathrm{Max}\{v(\theta - \alpha) \mid \alpha \in \overline{K},\ \deg_K(\alpha) < n\} \in \mathbb{Q}\Gamma.$$

Even in the case when θ is separable, this value may not be defined. By Krasner's lemma (11.1), $\omega_K(\theta)$ is an upper bound for the set $\{v(\theta-\alpha) \mid \alpha \in \overline{K},\ \deg_K(\alpha) < n\}$, but this does not guarantee that this set contains a maximal value.

We shall see in section 11.2 that $\delta_K(\theta)$ is well defined for defectless algebraic elements; that is, those for which L/K is a defectless extension.

This invariant $\delta_K(\theta)$ is called the *main invariant* of θ.

As we have just mentioned, if θ is separable, then $\delta_K(\theta) \leq \omega_K(\theta)$.

In section 11.3, we prove that equality holds in the tame case, and we give an explicit formula for $\delta_K(\theta) = \omega_K(\theta)$ in terms of the discrete invariants attached to an Okutsu frame of f.

11.1 Distinguished pairs of algebraic elements

Lemma 11.1. *For any given $\beta \in \overline{K}$ and $\rho \in \mathbb{Q}\Gamma$, there exists a separable $\beta_{sep} \in K^s$ such that:*

$$\deg_K(\beta_{sep}) = \deg_K(\beta), \qquad v(\beta - \beta_{sep}) > \rho.$$

Proof. If β is separable over K, we may take $\beta_{\rm sep} = \beta$.

Assume that β is inseparable over K. Then, its minimal polynomial $g \in K[x]$ over K satisfies $g' = 0$. Take any element $\pi \in K^*$ with

$$v(\pi) > \deg_K(\beta)\,\rho - v(\beta),$$

and consider the polynomial $g_{\rm sep} = g + \pi x \in K[x]$. Since $g'_{\rm sep} = \pi \neq 0$, this polynomial is separable. On the other hand,

$$\sum_{\alpha \in \mathrm{Z}(g_{\rm sep})} v(\beta-\alpha) = v\left(g_{\rm sep}(\beta)\right) = v(\pi\beta) = v(\pi) + v(\beta) > \deg_K(\beta)\,\rho.$$

Hence, there exists $\alpha \in \mathrm{Z}(g_{\rm sep})$ such that $v(\beta-\alpha) > \rho$. We may take $\beta_{\rm sep} = \alpha$. □

Definition 11.2. *Let $\alpha \in \overline{K}$ with $\deg_K(\alpha) < n$.*

We say that α, θ is a distinguished pair if the two following conditions are satisfied:

(1) $v(\theta-\alpha) = \mathrm{Max}\{v(\theta-\beta) \mid \beta \in \overline{K},\ \deg_K(\beta) < n\}$.

(2) $\beta \in \overline{K}, \quad \deg_K(\beta) < \deg_K(\alpha) \implies v(\theta-\beta) < v(\theta-\alpha)$.

Equivalently, α, θ is a distinguished pair if $v(\theta-\alpha) = \delta_K(\theta)$, and α has minimal degree among all algebraic elements with this property.

The aim of this section is to prove the following result.

Theorem 11.3. *For $\theta \in \overline{K}$ with $n = \deg_K(\theta) > 1$, let $f \in K[x]$ be its minimal polynomial over K.*

(1) Suppose that ϕ, f is a distinguished pair of prime polynomials (Definition 10.9). Take $\alpha \in \mathrm{Z}(\phi)$ such that $v(\theta-\alpha) = \mathrm{Max}\{v(\theta-\alpha') \mid \alpha' \in \mathrm{Z}(\phi)\}$.

Then, α, θ is a distinguished pair.

(2) Suppose that α, θ is a distinguished pair. Let $\phi \in K[x]$ be the minimal polynomial of α over K.

Then, ϕ, f is a distinguished pair of prime polynomials.

Proof. Let us first see that (1) implies (2). We assume that ϕ, f is a distinguished pair of prime polynomials.

Let $\delta = v(\theta - \alpha)$. Consider any $\beta \in \overline{K}$ with $\deg_K(\beta) < n$. We want to show:

(i) $v(\theta - \beta) \leq \delta$.

(ii) $v(\theta - \beta) = \delta \implies \deg_K(\beta) \geq \deg_K(\alpha)$.

Let $g \in K[x]$ be the minimal polynomial of β over K. We may assume that

$$v(\theta - \beta) = \mathrm{Max}\{v(\theta - \beta') \mid \beta' \in \mathrm{Z}(g)\}.$$

By Lemma 11.1, we may assume too, that θ, α and β are separable.

Consider a finite Galois extension M/K containing θ, α and β, and denote $G = \mathrm{Gal}(M/K)$. We claim that

$$v(\theta - \beta) \geq \delta \quad \implies \quad \frac{v(g(\theta))}{\deg(g)} \geq \frac{v(\phi(\theta))}{\deg(\phi)}. \tag{11.2}$$

In fact, assume that $v(\theta - \beta) \geq \delta$. Then, for any $\sigma \in G$ we get:

$$\begin{aligned} v(\theta - \sigma(\beta)) &= v(\theta - \sigma(\alpha) + \sigma(\alpha) - \sigma(\theta) + \sigma(\theta) - \sigma(\beta)) \\ &\geq \mathrm{Min}\{v(\theta - \sigma(\alpha)),\, v(\sigma(\alpha) - \sigma(\theta)),\, v(\sigma(\theta) - \sigma(\beta))\} \\ &= \mathrm{Min}\{v(\theta - \sigma(\alpha)),\, v(\alpha - \theta),\, v(\theta - \beta)\} = v(\theta - \sigma(\alpha)), \end{aligned} \tag{11.3}$$

because $v(\theta - \sigma(\alpha)) \leq \delta$, while $v(\alpha - \theta)$, $v(\theta - \beta) \geq \delta$. Therefore,

$$\frac{\#G}{\deg(g)}\, v(g(\theta)) = \sum_{\sigma \in G} v(\theta - \sigma(\beta)) \geq \sum_{\sigma \in G} v(\theta - \sigma(\alpha)) = \frac{\#G}{\deg(\phi)}\, v(\phi(\theta)). \tag{11.4}$$

This proves the claimed implication (11.2).

Now, if we had $v(\theta - \beta) > \delta$, then at least for the automorphism $\sigma = 1$ we would have $v(\theta - \sigma(\beta)) > \delta = v(\theta - \sigma(\alpha))$, leading to a strict inequality in (11.4). This would contradict the fact that ϕ, f is a distinguished pair. This argument proves (i).

On the other hand, the equality $v(\theta - \beta) = \delta$ is incompatible with a strict inequality in (11.4). In fact, suppose that for some $\sigma \in G$ we had

$$\delta = v(\theta - \beta) \geq v(\theta - \sigma(\beta)) > v(\theta - \sigma(\alpha)).$$

Then, the inequality in (11.3) becomes an equality, and this contradicts our assumptions:

$$v(\theta - \sigma(\beta)) = v(\theta - \sigma(\alpha)).$$

Thus, if $v(\theta-\beta)=\delta$, we must have an equality in (11.4). Since ϕ, f is a distinguished pair, this implies $\deg(g)\geq\deg(\phi)$. This proves (ii).

Let us now see that (1) implies (2). We assume that α, θ is a distinguished pair of algebraic elements. We keep the notation

$$\delta := v(\theta-\alpha)=\mathrm{Max}\{v(\theta-\alpha') \mid \alpha'\in \mathrm{Z}(\phi)\}.$$

Let $g\in K[x]$ be a monic polynomial with $\deg(g)<n$. We want to show:

(i) $\dfrac{v(g(\theta))}{\deg(g)}\leq\dfrac{v(\phi(\theta))}{\deg(\phi)}$.

(ii) $\dfrac{v(g(\theta))}{\deg(g)}=\dfrac{v(\phi(\theta))}{\deg(\phi)}\implies \deg(g)\geq\deg(\phi)$.

By Lemma 11.4 below, we may assume that g is irreducible and separable.

Also, by Lemma 11.1, we may assume that α and θ are separable too.

Take $\beta\in\mathrm{Z}(g)$ such that

$$v(\theta-\beta)=\mathrm{Max}\{v(\theta-\beta') \mid \beta'\in \mathrm{Z}(g)\}. \tag{11.5}$$

Let M/K be a finite Galois extension containing θ, α and β, and denote $G=\mathrm{Gal}(M/K)$. For all $\sigma\in G$, condition (11.5) implies

$$\begin{aligned} v(\theta-\sigma(\theta)) &= v\left(\theta-\sigma(\beta)+\sigma(\beta)-\sigma(\theta)\right)\\ &\geq \mathrm{Min}\{v(\theta-\sigma(\beta)),\, v(\sigma(\beta)-\sigma(\theta))\} \\ &= \mathrm{Min}\{v(\theta-\sigma(\beta)),\, v(\beta-\theta)\}=v(\theta-\sigma(\beta)).\end{aligned} \tag{11.6}$$

Now, we claim that

$$v\left(\theta-\sigma(\beta)\right)\leq v\left(\theta-\sigma(\alpha)\right), \qquad \forall\,\sigma\in G. \tag{11.7}$$

In fact, if $v\left(\theta-\sigma(\alpha)\right))=\delta$, then (11.7) is a consequence of the fact that α, θ is a distinguished pair.

If $v\left(\theta-\sigma(\alpha)\right))<\delta$, then (11.7) follows from (11.6):

$$v\left(\theta-\sigma(\beta)\right))\leq v\left(\theta-\sigma(\theta)\right))=v\left(\theta-\sigma(\alpha)+\sigma(\alpha)-\sigma(\theta)\right))=v\left(\theta-\sigma(\alpha)\right)),$$

because $v\left(\theta-\sigma(\alpha)\right)<\delta=v\left(\sigma(\alpha)-\sigma(\theta)\right)$. This ends the proof of (11.7).

Condition (i) follows immediately:

$$\frac{\#G}{\deg(g)}\,v(g(\theta))=\sum_{\sigma\in G}v(\theta-\sigma(\beta))\leq\sum_{\sigma\in G}v(\theta-\sigma(\alpha))=\frac{\#G}{\deg(\phi)}\,v(\phi(\theta)). \tag{11.8}$$

Also, if equality holds in (11.8), then

$$v(\theta-\sigma(\beta))=v(\theta-\sigma(\alpha)), \qquad \forall\,\sigma\in G.$$

In particular, for $\sigma=1$ we deduce $v(\theta-\beta)=v(\theta-\alpha)$, which implies

$$\deg(g)=\deg_K(\beta)\geq\deg_K(\alpha)=\deg(\phi),$$

because α, θ is a distinguished pair. This proves (ii). □

Lemma 11.4. *Let ϕ, $f \in K[x]$ be two prime polynomials with $\deg(\phi) < \deg(f)$. Then, for ϕ, f to be a distinguished pair it suffices to check that the two conditions:*

$$\textit{(i)} \quad \deg(g) < \deg(f) \implies \frac{v(g(\theta))}{\deg(g)} \leq \frac{v(\phi(\theta))}{\deg(\phi)},$$

$$\textit{(ii)} \quad \frac{v(g(\theta))}{\deg(g)} = \frac{v(\phi(\theta))}{\deg(\phi)} \implies \deg(g) \geq \deg(f),$$

hold for all monic, irreducible and separable polynomials $g \in K[x]$.

Proof. Let us first show that if conditions (i), (ii) hold for all monic irreducible polynomials in $K[x]$, then both conditions hold for all monic polynomials.

Let $g = h_1 \cdots h_t$ be a product of monic (not necessarily different) irreducible polynomials. Clearly, the average of the values $v(\theta - \beta)$ on $\beta \in \mathrm{Z}(g)$ is less than, or equal to, the maximum of the averages of the values $v(\theta - \beta)$, taken on the subsets

$$\mathrm{Z}(g) = \mathrm{Z}(h_1) \cup \cdots \cup \mathrm{Z}(h_t).$$

In other words,

$$\frac{v(g(\theta))}{\deg(g)} \leq \mathrm{Max}\left\{ \frac{v(h_i(\theta))}{\deg(h_i)} \;\middle|\; 1 \leq i \leq t \right\}.$$

Therefore, (i) and (ii) hold for g if they hold for $h_1, \ldots, h_t$.

Finally, let us show that if conditions (i), (ii) hold for all monic irreducible separable polynomials, then both conditions hold for all monic irreducible polynomials.

Let $g \in K[x]$ be monic and irreducible, but inseparable. Let $g_{\mathrm{sep}} = g + \pi x$, for $\pi \in K^*$ with $v(\pi)$ sufficiently large. As mentioned in the proof of Lemma 11.1, g_{sep} is a separable polynomial of the same degree.

Since (i) and (ii) hold for all irreducible factors of Γ_{sep}, they hold for g_{sep} too. Hence, if $v(\pi)$ is sufficiently large, both conditions hold for g. □

11.2 Complete distinguished chains of defectless algebraic elements

We keep with the notation of the previous section.

Definition 11.5. *Let $\alpha_0, \alpha_1, \ldots, \alpha_r, \theta = \alpha_{r+1} \in \overline{K}$ be algebraic elements with*

$$1 = \deg_K(\alpha_0) < \cdots < \deg_K(\alpha_r) < \deg_K(\theta).$$

We say that $[\alpha_0, \alpha_1, \ldots, \alpha_r]$ is a complete distinguished chain *for θ if α_i, α_{i+1} is a distinguished pair, for all $0 \leq i \leq r$.*

Theorem 11.6. *For $\theta \in \overline{K}$ with $n = \deg_K(\theta) > 1$, let $f \in K[x]$ be its minimal polynomial over K.*

(1) Let $[\phi_0, \ldots, \phi_r]$ be an Okutsu frame of f. For all $0 \leq i \leq r$, take $\alpha_i \in \mathrm{Z}(\phi_i)$ such that $v(\theta - \alpha_i) = \mathrm{Max}\{v(\theta - \alpha_i') \mid \alpha_i' \in \mathrm{Z}(\phi_i)\}$.

Then, $[\alpha_0, \ldots, \alpha_r]$ is a complete distinguished chain for θ.

(2) Let $[\alpha_0, \dots, \alpha_r]$ be a complete distinguished chain for θ. Let $\phi_0, \dots, \phi_r \in K[x]$ be the minimal polynomials over K of $\alpha_0, \dots, \alpha_r$, respectively.

Then, $[\phi_0, \dots, \phi_r]$ is an Okutsu frame of f.

Proof. In Corollary 10.18 we saw that $[\phi_0, \dots, \phi_r]$ is an Okutsu frame of $f = \phi_{r+1}$ if and only if each pair ϕ_i, ϕ_{i+1} is a distinguished pair of prime polynomials for all $0 \le i \le r$. Thus, the theorem follows from Theorem 11.3. □

Theorem 11.7 (Aghigh-Khanduja [1, 2])**.** *An algebraic element $\theta \in \overline{K}$ admits a complete distinguished chain over K if and only if it is defectless over K.*

Proof. This follows immediately from Theorems 10.15 and 11.6. □

Distinguished pairs and distinguished chains were introduced by N. Popescu-A. Zaharescu in 1995 [26], for K a complete discrete rank-one valued field.

However, this concept is equivalent to some sequences of algebraic elements studied by Okutsu in 1982 [24], also in the complete and discrete rank-one case.

Let us show the equivalence between the two concepts.

Definition 11.8. *Let $\alpha_0, \alpha_1, \dots, \alpha_r, \theta = \alpha_{r+1} \in \overline{K}$ be algebraic elements with*

$$1 = \deg_K(\alpha_0) < \cdots < \deg_K(\alpha_r) < \deg_K(\theta).$$

We say that $[\alpha_0, \alpha_1, \dots, \alpha_r]$ is a complete Okutsu sequence *for θ if the following conditions hold for all $\beta \in \overline{K}$ and all $0 \le i \le r$:*

(1) $\deg_K(\beta) < \deg_K(\alpha_{i+1}) \implies v(\theta - \beta) \le v(\theta - \alpha_i)$.

(2) $\deg_K(\beta) < \deg_K(\alpha_i) \implies v(\theta - \beta) < v(\theta - \alpha_i)$.

For the comparison of Okutsu sequences with distinguished chains we need an obvious remark.

Lemma 11.9. *Suppose α, θ is a distinguished pair of algebraic elements. Then, for all $\beta \in \overline{K}$ with $\deg_K(\beta) < \deg_K(\alpha)$, we have $v(\theta - \beta) = v(\alpha - \beta)$.*

Proof. By the definition of distinguished pair, $v(\theta - \beta) < v(\theta - \alpha)$. This implies immediately that $v(\alpha - \beta) = \mathrm{Min}\{v(\alpha - \theta), v(\theta - \beta)\} = v(\theta - \beta)$. □

Lemma 11.10. *A sequence $[\alpha_0, \alpha_1, \dots, \alpha_r]$ of elements in $\overline{K}$ is a complete distinguished chain for $\theta = \alpha_{r+1}$ if and only if it is a complete Okutsu sequence for θ.*

Proof. Let $\beta \in \overline{K}$ with $\deg_K(\beta) < \deg_K(\theta)$.

Suppose that $[\alpha_0, \alpha_1, \dots, \alpha_r]$ is a complete distinguished chain for θ. By definition, for all $0 \le i \le r$, the following conditions hold:

(i) $\deg_K(\beta) < \deg_K(\alpha_{i+1}) \implies v(\alpha_{i+1} - \beta) \le v(\alpha_{i+1} - \alpha_i)$.

(ii) $\deg_K(\beta) < \deg_K(\alpha_i) \implies v(\alpha_{i+1} - \beta) < v(\alpha_{i+1} - \alpha_i)$.

If $i = r$, then $\alpha_{i+1} = \theta$. If $i < r$, then Lemma 11.9 shows that $v(\theta - \beta) = v(\alpha_{i+1} - \beta)$.

In both cases, the conditions of Definition 11.8 coincide with (i) and (ii). Hence, $[\alpha_0, \alpha_1, \ldots, \alpha_r]$ is an Okutsu sequence for θ.

Conversely, suppose that $[\alpha_0, \alpha_1, \ldots, \alpha_r]$ is an Okutsu sequence for θ.

The conditions of Definition 11.8 for $i = r$ show that α_r, $\theta = \alpha_{r+1}$ is a distinguished pair.

Hence, we may apply Lemma 11.9 to conclude that

$$v(\theta - \beta) = v(\alpha_r - \beta), \qquad v(\theta - \alpha_j) = v(\alpha_r - \alpha_j),$$

for all $0 \leq j < r$ and all $\beta \in \overline{K}$ with $\deg_K(\beta) < \deg_K(\alpha_{j+1})$.

Therefore, the sequence $[\alpha_0, \ldots, \alpha_{r-1}]$ is a complete Okutsu sequence for α_r. The previous argument shows that α_{r-1}, α_r is a distinguished pair.

We may iterate this argument to conclude that $[\alpha_0, \alpha_1, \ldots, \alpha_r]$ is a complete distinguished chain for θ. □

Corollary 11.11. *Let $[\alpha_0, \ldots, \alpha_r]$ be a complete Okutsu sequence for $\theta \in \overline{K}$. Then, $[\alpha_0, \ldots, \alpha_i]$ is a complete Okutsu sequence for α_{i+1}, for all $1 \leq i < r$.*

Proof. This property is obviously true for complete distinguished chains. □

In the next section, we compute several invariants attached to tame algebraic elements. To this purpose, Okutsu sequences are a more feasible tool than complete distinguished chains.

11.3 Main invariant of tame algebraic elements

Definition 11.12. *Let $\theta \in \overline{K}$, with minimal polynomial $f \in K[x]$. Denote $L = K(\theta)$ and let k_L be the residue class field of (L, v).*

We say that $\theta \in \overline{K}$ is tame *if it satisfies the following conditions.*

- *f is defectless.*
- *The finite extension k_L/k is separable.*
- *The ramification index $e(L/K)$ is not divisible by* $\mathrm{char}(K)$.

It is easy to check that a tame θ is necessarily separable over K.

Recall the definition of the *ramification subgroup*:

$$G^{\mathrm{ram}}(K) = \{\sigma \in \mathrm{Gal}(K^s/K) \mid v(\sigma(c) - c) > v(c), \quad \forall\, c \in (K^s)^*\}\,.$$

Its fixed field $K^{\mathrm{ram}} = (K^s)^{G^{\mathrm{ram}}}$ is called the *ramification field* for the extension K^s/K. This field is the unique maximal tame extension of K in $\overline{K}$.

More precisely, for any algebraic extension L/K, the subfield $L \cap K^{\mathrm{ram}}$ is the unique maximal tame extension of K in L/K.

Notation. Let $[\alpha_0, \ldots, \alpha_r]$ be a complete Okutsu sequence for $\theta = \alpha_{r+1} \in \overline{K}$.

We shall usually denote

$$\delta_0 = v(\theta - \alpha_0) < \cdots < \delta_r = v(\theta - \alpha_r) < \delta_{r+1} = v(\theta - \alpha_{r+1}) = \infty.$$

By Lemmas 11.10 and 11.9, we have

$$\delta_i = v(\alpha_{i+1} - \alpha_i) = \delta_K(\alpha_{i+1}), \quad 0 \leq i \leq r.$$

The next result is inspired in the revision of the original ideas of Okutsu [24] that J. Guàrdia, J. Montes and E. Nart carried out in [7].

Proposition 11.13. *Let $[\alpha_0, \ldots, \alpha_r]$ be a complete Okutsu sequence for a separable $\theta = \alpha_{r+1} \in K^s$. Consider a separable $\beta \in K^s$ such that*

$$\deg(\beta) = m_i, \quad v(\theta - \beta) > \delta_{i-1},$$

for some $1 \leq i \leq r+1$. Let M/K be any finite Galois extension containing $K(\theta, \beta)$. Let $G = \mathrm{Gal}(M/K)$ and consider the subgroups

$$H_i = \{\sigma \in G \mid v(\theta - \sigma(\theta)) > \delta_{i-1})\} \supset \overline{H}_i = \{\sigma \in G \mid v(\theta - \sigma(\theta)) \geq \delta_i\}.$$

Let $M^{H_i} \subset M^{\overline{H}_i} \subset M$ be the respective fixed fields. Finally, let V be the maximal tame subextension of $K(\beta)/K$. Then,

$$V \subset M^{H_i} \subset K(\theta) \cap K(\beta).$$

Moreover, if $v(\theta - \beta) = \delta_i$ then

$$V \subset M^{H_i} \subset M^{\overline{H}_i} \subset K(\theta) \cap K(\beta).$$

Proof. First, let us show that $M^{H_i} \subset K(\theta) \cap K(\beta)$. For this, it suffices to show that all $\sigma \in G$ fixing θ or β belong to H_i.

If $\sigma(\theta) = \theta$, then $\sigma \in H_i$ because $v(\theta - \sigma(\theta)) = \infty > \delta_{i-1}$.

If $\sigma(\beta) = \beta$, then $v(\sigma(\theta) - \beta) = v(\sigma(\theta) - \sigma(\beta)) = v(\theta - \beta) > \delta_{i-1}$. Thus,

$$v(\theta - \sigma(\theta)) \geq \mathrm{Min}\{v(\theta - \beta),\, v(\beta - \sigma(\theta))\} > \delta_{i-1}.$$

In the case $v(\theta - \beta) = \delta_i$, the same argument shows that $M^{\overline{H}_i} \subset K(\theta) \cap K(\beta)$.

Finally let us prove that $V \subset M^{H_i}$. Since V is the maximal tame extension of $K(\beta)$, we have that $V = K^{\mathrm{ram}} \cap K(\beta)$, so we must prove that

$$H_i \subset \{\sigma \in G \mid v(\sigma(c) - c) > v(c), \quad \forall c \in K(\beta)^*\}.$$

Take $\sigma \in H_i$. Any $c \in K(\beta)^*$ can be written as $c = g(\beta)$ for some $g \in K[x]$ with $\deg(g) < m_i$. By the minimality of m_i, for any root ξ of g we have $v(\theta - \xi) \leq \delta_{i-1}$. Hence,

$$v(\beta - \xi) = \mathrm{Min}\,\{v(\beta - \theta),\, v(\theta - \xi)\} = v(\theta - \xi) \leq \delta_{i-1}. \tag{11.9}$$

Write $g(x) = a \prod_{\xi \in \mathrm{Z}(g)} (x - \xi)$. Then,

$$\frac{g(\sigma(\beta))}{g(\beta)} = \prod_{\xi} \frac{\sigma(\beta) - \xi}{\beta - \xi} = \prod_{\xi} \left(1 + \frac{\sigma(\beta) - \beta}{\beta - \xi}\right).$$

Since $\sigma \in H_i$, we have

$$v\left(\sigma(\beta)-\beta\right) \geq \operatorname{Min}\left\{v\left(\sigma(\beta)-\sigma(\theta)\right),\, v\left(\sigma(\theta)-\theta\right),\, v\left(\theta-\beta\right)\right\} > \delta_{i-1}.$$

By (11.9), this implies $v\left(\dfrac{\sigma(\beta)-\beta}{\beta-\xi}\right) > 0$, so that

$$v\left(\frac{\sigma(c)}{c}-1\right) = v\left(\frac{g(\sigma(\beta))}{g(\beta)}-1\right) > 0.$$

This proves that $V \subset M^{H_i}$. □

Lemma 11.14. *Let $[\alpha_0, \ldots, \alpha_r]$ be a complete Okutsu sequence for $\theta \in \overline{K}$.*

(1) If $f \in K[x]$ be the minimal polynomial of f, then

$$v(\theta-\theta') \geq v(\theta-\alpha_0), \qquad \forall\, \theta' \in \mathrm{Z}(f).$$

(2) If θ is tame over K, then $\alpha_0, \ldots, \alpha_r$ are tame over K.

Proof. By Theorem 11.7 and Lemma 11.10, θ is defectless.

By Theorem 10.15, f admits an Okutsu frame $[\phi_0, \ldots, \phi_r]$ with $\phi_0 = x - \alpha_0$. By Theorem 10.14, the inductive valuation v_f admits an optimal MacLane chain

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = v_f$$

Since $\phi_0 \mid_{\mu_0} f$, Theorem 10.2 shows that $N_{\mu_0,\phi_0}(f)$ is one sided of a certain slope $-\gamma_0$, and $v(\theta-\alpha_0) = \gamma_0$, for every root θ of f. Thus,

$$v(\theta-\theta') \geq \operatorname{Min}\{v(\theta-\alpha_0),\, v(\theta'-\alpha_0) = \gamma_0 = v(\theta-\alpha_0).$$

This proves (1).

By Lemma 11.10, $[\alpha_0, \ldots, \alpha_{i-1}]$ is a complete Okutsu sequence for α_i. Hence, all α_i are defectless by Theorem 11.7.

As indicated in (5.13), the maximal subfields k_i of the algebras Δ_{μ_i} form a chain of finite extensions of k:

$$k = k_0 \subset k_1 \subset \cdots \subset k_r \subset k_L.$$

By Proposition 1.25, each field k_i is isomorphic to the residue class fields k_{ϕ_i} of the extension $K(\alpha_i)/K$. Thus, the assumption that k_L/k is separable implies that all k_{ϕ_i}/k are separable too.

Finally, equation (5.5) shows that the ramification indices $e(\phi_i)$ divide each other:

$$1 = e(\phi_0) \mid \cdots e(\phi_i) \mid e(\phi_{i+1}) \mid \cdots \mid e(f).$$

Thus, if $e(f)$ is not divisible by the characteristic of K, all ramification indices $e(\phi_i)$ have the same property. This proves that $K(\alpha_i)/K$ is tame for all i. □

Theorem 11.15. *Let $\theta \in \overline{K}$ be an algebraic element of degree $n = \deg_K(\theta) > 1$. Let $[\alpha_0, \ldots, \alpha_r]$ be a complete Okutsu sequence for $\theta = \alpha_{r+1}$, and denote*

$$m_i = \deg_K(\alpha_i), \qquad \delta_i = v\left(\theta - \alpha_i\right), \qquad 0 \le i \le r+1.$$

If α_r is tame over K, then it holds:

(1) $K = K(\alpha_0) \subset K(\alpha_1) \subset \cdots \subset K(\alpha_r) \subset K(\theta)$.

(2) The following multisets of cardinality $n-1$ coincide:

$$\{v\left(\theta - \theta'\right) \mid \theta' \in \mathrm{Z}(f),\ \theta' \ne \theta\} = \left\{\delta_0^{t_0}, \ldots, \delta_r^{t_r}\right\},$$

where $t_i = \dfrac{n}{m_i} - \dfrac{n}{m_{i+1}}$ *for all* $0 \le i \le r$.

In particular, $\delta_r = \delta_K(\theta) = \omega_K(\theta)$.

Proof. Let M/K be a finite Galois extension of K containing $K(\theta, \alpha_1, \ldots, \alpha_r)$, and denote $G = \mathrm{Gal}(M/K)$.

Fix an index $0 \le i \le r$. Since $\deg_K(\alpha_i) = m_i$ and $v(\theta - \alpha_i) = \delta_i$, Proposition 11.13 applied to $\beta = \alpha_i$ shows that

$$V_i \subset M^{H_i} \subset M^{\overline{H}_i} \subset K(\alpha_i) \cap K(\theta),$$

where V_i is the maximal tame subextension of $K(\alpha_i)$.

By Lemma 11.14, $K(\alpha_i)/K$ is tame, so that $V_i = K(\alpha_i)$. Therefore,

$$V_i = M^{H_i} = M^{\overline{H}_i} = K(\alpha_i) \subset K(\theta). \tag{11.10}$$

Now, denote $H_0 := G$ and consider the chain of subgroups

$$G = H_0 \supset H_1 \supset \cdots \supset H_r \supset H_{r+1} = \mathrm{Gal}(M/K(\theta)). \tag{11.11}$$

The corresponding chain of fixed fields is that given in item (1).

Moreover, (11.10) implies

$$(H_i : H_{i+1}) = [K(\alpha_{i+1}) \colon K(\alpha_i)] = m_{i+1}/m_i > 1, \qquad 0 \le i \le r,$$

so that all inclusions in the chain (11.11) are strict. Hence, for any $\sigma \in G \setminus H_{r+1}$ there exists a unique $0 \le i \le r$ such that

$$\sigma \in \overline{H}_i = H_i, \qquad \sigma \notin H_{i+1}.$$

If $i > 0$, then $v\left(\theta - \sigma(\theta)\right) = \delta_i$, by the definition of the subgroups $\overline{H}_i$ and H_{i+1}.

If $i = 0$, then $\sigma \notin H_1$ implies $v\left(\theta - \sigma(\theta)\right) \le \delta_0$. By Lemma 11.14, we deduce that $v\left(\theta - \sigma(\theta)\right) = \delta_0$ in this case too.

Therefore, the underlying set of the multiset $\{v\left(\theta - \sigma(\theta)\right) \mid \sigma \in G,\ \sigma(\theta) \ne \theta\}$ is the set $\{\delta_0, \ldots, \delta_r\}$.

Now, it remains to find a concrete formula for the multiplicity t_i of each value δ_i.

Let $f \in K[x]$ be the minimal polynomial of θ over K. The natural action of G on $\mathrm{Z}(f)$ induces a bijection:

$$G/\operatorname{Gal}(M/K(\theta)) \longrightarrow \mathrm{Z}(f), \qquad \sigma \longmapsto \sigma(\theta).$$

For any $0 \leq i \leq r$, the restriction of this bijection to the subgroup $H_i/\operatorname{Gal}(M/K(\theta))$ determines a bijection:

$$H_i/\operatorname{Gal}(M/K(\theta)) \longrightarrow Z_i(f) := \{\theta' \in \mathrm{Z}(f) \mid v(\theta - \theta') \geq \delta_i\}.$$

Hence, the multiplicity t_i is equal to:

$$\begin{aligned} t_i = \#Z_i(f) - \#Z_{i+1}(f) &= \#H_i/\operatorname{Gal}(M/K(\theta)) - \#H_{i+1}/\operatorname{Gal}(M/K(\theta)) \\ &= [K(\theta)\colon K(\alpha_i)] - [K(\theta)\colon K(\alpha_{i+1})] = \frac{n}{m_i} - \frac{n}{m_{i+1}}. \end{aligned}$$

This ends the proof of item (2). □

We end this section with an explicit formula for the main invariant $\delta_K(\theta) = \omega_K(\theta)$ in terms of the discrete invariants attached to an Okutsu frame of the minimal polynomial $f \in K[x]$ of θ over K.

For $0 \leq i \leq r$, let ϕ_i be the minimal polynomial of α_i over K. By Theorem 10.15, $[\phi_0, \ldots, \phi_r]$ is an Okutsu frame of f. By Theorem 10.14, the inductive valuation v_f admits an optimal MacLane chain

$$\mu_{-\infty} \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \overset{\phi_{r-1},\gamma_{r-1}}{\longrightarrow} \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = v_f$$

where $\gamma_i = \mu_i(\phi_i) = v(\phi_i(\theta))$ for all i. Let us denote

$$\lambda_0 := \gamma_0, \qquad \lambda_i := \gamma_i - \mu_{i-1}(\phi_i), \quad 0 < i \leq r.$$

At the beginning of section 5.2, we saw that

$$\gamma_i = m_i \left(\frac{\lambda_0}{m_0} + \cdots + \frac{\lambda_i}{m_i} \right), \qquad 0 \leq i \leq r. \tag{11.12}$$

Proposition 11.16. *With the above notation, if α_r is tame over K, then*

$$\delta_i = \lambda_0 + \cdots + \lambda_i, \qquad 0 \leq i \leq r. \tag{11.13}$$

Proof. Let us prove the formula by a recurrent argument on i. For $i = 0$, we have $\phi_0 = (x - \alpha_0)$ and

$$\lambda_0 = \gamma_0 = v(\phi_0(\theta)) = v(\theta - \alpha_0) = \delta_0.$$

Now, suppose that $i > 0$ and $\delta_j = \lambda_0 + \cdots + \lambda_j$ for all $j < i$. Let us prove that (11.13) holds for i.

We claim that

$$v(\phi_i(\theta)) = \delta_i + t_0\delta_0 + \cdots + t_{i-1}\delta_{i-1}, \qquad t_j = \frac{m_i}{m_j} - \frac{m_i}{m_{j+1}}, \quad 0 \leq j < i. \tag{11.14}$$

In fact, since $[\alpha_0, \ldots, \alpha_{i-1}]$ is a complete Okutsu sequence for α_i, Theorem 11.15 yields an equality of multisets:

$$\{v(\alpha_i - \xi) \mid \xi \in \mathrm{Z}(\phi_i),\ \xi \neq \alpha_i\} = \left\{\delta_0^{t_0}, \ldots, \delta_{i-1}^{t_{i-1}}\right\}, \tag{11.15}$$

for the multiplicities $t_0, \ldots, t_{i-1}$ indicated in (11.14).

Now, for each $\xi \in \mathrm{Z}(\phi_i)$, $\xi \neq \alpha_i$, we have

$$v(\theta - \xi) = \mathrm{Min}\{v(\theta - \alpha_i),\, v(\alpha_i - \xi)\} = v(\alpha_i - \xi), \tag{11.16}$$

because $v(\theta - \alpha_i) = \delta_i$, while

$$v(\alpha_i - \xi) \leq \omega_K(\alpha_i) = \delta_K(\alpha_i) = \delta_{i-1} < \delta_i.$$

The equalities (11.15) and (11.16) prove the claimed identity (11.14), because

$$v(\phi_i(\theta)) = v(\theta - \alpha_i) + \sum_{\xi \in \mathrm{Z}(\phi_i),\, \xi \neq \alpha_i} v(\theta - \xi) = \delta_i + t_0\delta_0 + \cdots + t_{i-1}\delta_{i-1}.$$

Finally, from (11.14) and (11.12) we deduce

$$\delta_i + t_0\delta_0 + \cdots + t_{i-1}\delta_{i-1} = \gamma_i = \frac{m_i}{m_0}\,\lambda_0 + \cdots + \frac{m_i}{m_i}\,\lambda_i,$$

from which we may express δ_i as

$$\delta_i = \frac{m_i}{m_0}\,\lambda_0 + \cdots + \frac{m_i}{m_i}\,\lambda_i - t_0\delta_0 - \cdots - t_{i-1}\delta_{i-1}.$$

By applying the induction hypothesis, we may express δ_i as a linear combination

$$\delta_i = a_0\lambda_0 + \cdots + a_{i-1}\lambda_{i-1} + \lambda_i,$$

where, for $j < i$, each coefficient a_j takes the value:

$$a_j = \frac{m_i}{m_j} - t_j - t_{j+1} - \cdots - t_{i-1} = \frac{m_i}{m_i} = 1.$$

This ends the proof of the proposition. □

Bibliography

[1] K. Aghigh, S. Khanduja, *On the main invariant of elements algebraic over a henselian valued field*, Proceedings of the Edinburgh Mathematical Society **45** (2002), no. 1, 219–227.

[2] K. Aghigh, S. K. Khanduja, *On chains associated with elements algebraic over a henselian valued field*, Algebra Colloquium **12** (2005), no. 4, 607–616.

[3] R. Brown, J.L. Merzel, *Invariants of defectless irreducible polynomials*, Journal of Algebra and Its Applications, **9** (2010), no. 4, 603–631.

[4] R. Brown, J.L. Merzel, *The main invariant of a defectless polynomial*, Journal of Algebra and Its Applications, **12** (2013), no. 1, 1250122 (16 pages).

[5] A. J. Engler, A. Prestel, *Valued fields*, Springer, Berlin, 2005.

[6] J. Fernández, J. Guàrdia, J. Montes, E. Nart, *Residual ideals of MacLane valuations*, J. Algebra **427** (2015), 30–75.

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

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

[9] 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.

[10] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Foundations of Computational Mathematics **13** (2013), 729–762.

[11] J. Guàrdia, E. Nart, *Genetics of polynomials over local fields*, arXiv:1309.4340v2 [math.NT], to appear in Proceedings of AGCT14, Contemporary Mathematics.

[12] F.J. Herrera Govantes, M.A. Olalla Acosta, M. Spivakovsky, *Valuations in algebraic field extensions*, Journal of Algebra **312** (2007), no. 2, 1033–1074.

[13] F.J. Herrera Govantes, W. Mahboub, M.A. Olalla Acosta, M. Spivakovsky, *Key polynomials for simple extensions of valued fields*, preprint, arXiv:1406.0657 [math.AG], 2014.

[14] A. Jakhar, S.K. Khanduja, N. Sangwan, *On factorization of polynomials in henselian valued fields*, Communications in Algebra **46** (2018), no. 7, 3205–3221.

[15] S.K. Khanduja, *On a result of James Ax*, Journal of Algebra **172** (1995), 147–151.

[16] S.K. Khanduja, *Tame fields and tame extensions*, Journal of Algebra **201** (1998), 647–655.

[17] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40** (1936), pp. 363–395.

[18] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2** (1936), pp. 492–510.

[19] W. Mahboub, *Key polynomials*, Journal of Pure and Applied Algebra **217** (2013), no. 6, 989–1006.

[20] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.

[21] E. Nart, *Local computation of differents and discriminants*, Mathematics of Computation **83** (2014), no. 287, 1513–1534.

[22] E. Nart, *On the equivalence of types*, Journal de Thorie des Nombres de Bordeaux **28** (2016), no 3, 743–771.

[23] E. Nart, *Key polynomials over valued fields*, Publicacions Matemàtiques, to appear, arXiv:1803.08406 [math.AG].

[24] K. Okutsu, *Construction of integral basis, I, II*, Proceedings of the Japan Academy, Ser. A **58** (1982), 47–49, 87–89.

[25] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica **44** (1923), pp. 219–314.

[26] N. Popescu, A. Zaharescu, *On the structure of the irreducible polynomials over local fields*, Journal of Number Theory **52** (1995), 98–118.

[27] L. Popescu, N. Popescu, *On the residual transcendental extensions of a valuation. Key polynomials and augmented valuations*, Tsukuba Journal of Mathematics **15** (1991), 57–78.

[28] J.-C. San Saturnino, *Defect of an extension, key polynomials and local uniformization*, Journal of Algebra **481** (2017), 91–119.

[29] A.P. Singh, S. K. Khanduja, *On finite tame extensions of valued fields*, Communications in Algebra **33** (2005), no. 4, 1095-1105.

[30] M. Vaquié, *Extension d'une valuation*, Transactions of the American Mathematical Society **359** (2007), no. 7, 3439–3481.

[31] M. Vaquié, *Famille admissible de valuations et défaut d'une extension*, Journal of Algebra **311** (2007), no. 2, 859–876.

[32] M. Vaquié, *Extensions de valuation et polygone de Newton*, Annales de l'Institute Fourier (Grenoble) **58** (2008), no. 7, 2503–2541.