COMPUTATION OF RESIDUAL POLYNOMIAL OPERATORS OF
INDUCTIVE VALUATIONS

NATHÁLIA MORAES DE OLIVEIRA AND ENRIC NART

Abstract. Let \((K, v)\) be a valued field, and \(\mu\) an inductive valuation on \(K[x]\) extending \(v\). Let \(G_{\mu}\) be the graded algebra of \(\mu\) over \(K[x]\), and \(\kappa\) the maximal subfield of the subring of \(G_{\mu}\) formed by the homogeneous elements of degree zero.

In this paper, we find an algorithm to compute the field \(\kappa\) and the residual polynomial operator \(R_{\mu}: K[x] \to \kappa[y]\), where \(y\) is another indeterminate, without any need to perform computations in the graded algebra.

This leads to an OM algorithm to compute the factorization of separable defectless polynomials over henselian fields.

Introduction

In a pioneering work along the 1920s, Ø. Ore conjectured the existence of an algorithm to compute prime ideal decomposition in the number field defined by an irreducible polynomial \(f \in \mathbb{Q}[x]\), based in the iteration of two major steps \[13, 14\]:

- Computation of Newton polygons of \(\phi\)-expansions of \(f\), with respect to key polynomials \(\phi\) for some auxiliary valuations on \(\mathbb{Q}[x]\).
- Factorization in the residue class fields of the above valuations, of certain residual polynomials associated to the sides of the Newton polygons.

In the 1930s, S. MacLane found an algorithm to solve a more general problem: given a discrete rank one valuation \(v\) on a field \(K\), to find all its extensions to a field extension \(L = K[x]/f\) determined by an irreducible polynomial \(f \in K[x]\) \[7, 8\]. Any such extension may be identified to a valuation \(\mu\) on \(K[x]\) with support \(fK[x]\). MacLane’s algorithm constructs a chain of augmentations of valuations on the polynomial ring \(K[x]\)

\[
\mu_0 < \mu_1 < \cdots < \mu_i < \cdots < \mu
\]

which get arbitrarily close to \(\mu\). In these augmentation steps, certain key polynomials for the valuations \(\mu_i\) play an essential role. This algorithm can be reinterpreted as a polynomial factorization algorithm in \(\hat{K}[x]\), where \(\hat{K}\) is the completion of \(K\) at \(v\).

In the 40s, computers were born, and grew up in the 50s and 60s. Algorithmic arithmetic geometry appeared in the 60s and consolidated in the 70s as a mature mathematical discipline, but the “old” ideas of Ore and MacLane were forgotten.

In the 80s, K. Okutsu stressed the role of key polynomials in the computation of integral bases of local fields \[12, 2\]. In 1999, J. Montes developed certain residual polynomial operators which led to the design of a practical algorithm following the exact pattern that Ore had foreseen \[9, 3, 4\]. This algorithm is known as the OM algorithm, named after Ore, MacLane, Okutsu and Montes.

The OM algorithm is very efficient in the resolution of many arithmetic-geometric tasks in number fields and function fields of algebraic curves. For an account on these applications, we refer the reader to the survey \[5\] and the references quoted there.

Key words and phrases. inductive valuation, MacLane chain, Newton polygon, residual polynomial.

Partially supported by grant MTM2016-75980-P from the Spanish MEC.
MacLane’s theory was generalized by M. Vaquié to the case of an arbitrary valued field \((K,v)\), not necessarily rank-one nor discrete \([15, 16, 17]\). The graded algebra \(G_\mu\) attached to a valuation \(\mu\) on \(K[x]\) is crucial for the development of the theory. In this context, limit augmentations and the corresponding limit key polynomials appear as a new feature.

In analogy with the case of dimensions 0,1, MacLane-Vaquié’s theory should lead to the development of efficient algorithms for the resolution of arithmetic-geometric tasks involving valuations of function fields of algebraic varieties of higher dimension.

A prototype of OM algorithm in this general frame was described by F.J. Herrera Govantes, W. Mahboub, M.A. Olalla Acosta and M. Spivakovsky in \([6]\). The main obstacle for this procedure to become a real algorithm is the existence of limit augmentations. Another difficulty is the need to factorize polynomials in the graded algebra, which would be very onerous in practical implementations.

The first obstacle disappears if we deal with defectless extensions of \(K\). In this case, the auxiliary valuations \(\mu_i\) in \((1)\) are all inductive \([16, 10]\); that is, no limit augmentations are involved in their construction.

In this paper, we present an OM algorithm to compute extensions of valuations of arbitrary rank to defectless field extensions. More precisely, for each extension of \(v\) to an inductive valuation \(\mu_r\) on \(K[x]\) of length \(r\) in the chain \((1)\) of augmentations, we construct in a recursive way a tower of field extensions of the residue class field \(k\):

\[
k = \kappa_0 \subset \kappa_1 \subset \cdots \subset \kappa_r,
\]

and residual polynomial operators

\[
R_\mu : K[x] \longrightarrow \kappa_i[y], \quad 0 \leq i \leq r,
\]

which facilitate the design of an OM algorithm completely analogous to the classical one.

In the construction of these objects we avoid any computation in the graded algebra. In particular, these ideas provide an efficient polynomial factorization algorithm for separable defectless polynomials over henselian fields.

The definition of \(R_\mu\) involves the choice of rational functions in \(K(x)\) whose images in the graded algebra \(G_\mu\) have certain prescribed properties. For our algorithmic approach we need to construct these rational functions for the operators \(R_\mu, \ldots, R_{\mu_{r-1}}\) in a coherent way. To this end, we generalize the methods of \([1]\), where this problem was solved for discrete rank-one valuations.

Section 3 of the paper is devoted to the construction of the adequate rational functions in \(K(x)\). In section 4 we discuss Newton polygons. In section 5 we define the operators \(R_\mu\) and give some applications. Our main result is Theorem 5.16 where we prove the recursivity of the residual polynomial operators.

1. Valuations on polynomial rings

Let \((K,v)\) be a valued field with non-trivial group \(\Gamma = v(K^*)\) and residue class field \(k\).

Let \(\mu\) be a valuation on the polynomial ring \(K[x]\), extending \(v\). Let \(\Gamma_\mu\) be the value group, and denote by \(k_\mu\) its residue class field.

We suppose that \(\mu\) has trivial support; that is, \(\mu\) is the restriction to \(K[x]\) of some valuation on the field \(K(x)\).

For any \(\alpha \in \Gamma_\mu\), consider the abelian groups:

\[
P_\alpha = \{ g \in A \mid \mu(g) \geq \alpha \} \supset P_\alpha^+ = \{ g \in A \mid \mu(g) > \alpha \}.
\]

The graded algebra of \(\mu\) over \(K[x]\) is the integral domain:

\[
G_\mu := \text{gr}_\mu(K[x]) = \bigoplus_{\alpha \in \Gamma_\mu} P_\alpha/P_\alpha^+.
\]
Let $\Delta = \Delta_\mu = \mathcal{P}_0/\mathcal{P}_0^+ \subset G_\mu$ be the subring of homogeneous elements of degree zero. There are canonical injective ring homomorphisms:

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

In particular, $\Delta$ and $G_\mu$ are equipped with a canonical structure of $k$-algebra.

The initial term mapping $H_\mu : K[x] \to G_\mu$ is given by $H_\mu(0) = 0$ and

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

if $g \neq 0$. For all $g, h \in K[x]$ we have $H_\mu(gh) = H_\mu(g)H_\mu(h)$ and

$$(2) \quad H_\mu(g + h) = H_\mu(g) + H_\mu(h), \text{ if } \mu(g) = \mu(h) = \mu(g + h).$$

The next definitions translate properties of the action of $\mu$ on $K[x]$ into algebraic relationships in the graded algebra $G_\mu$.

**Definition 1.1.** Let $g, h \in K[x]$.

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

We say that $g$ is $\mu$-divisible by $h$, and we write $h \mid_\mu g$, if $H_\mu(h) \mid H_\mu(g)$ in $G_\mu$.

We say that $g$ is $\mu$-irreducible if $H_\mu(g)G_\mu$ is a non-zero prime ideal.

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

The property of $\mu$-minimality admits a relevant characterization.

**Lemma 1.2.** Let $\phi \in K[x]$ be a non-constant polynomial. Let

$$f = \sum_{0 \leq s} a_s \phi^s, \quad a_s \in K[x], \quad \deg(a_s) < \deg(\phi)$$

be the canonical $\phi$-expansion of $f \in K[x]$. Then, $\phi$ is $\mu$-minimal if and only if

$$\mu(f) = \text{Min}\{\mu(a_s \phi^s) \mid 0 \leq s\}, \quad \forall f \in K[x].$$

**Definition 1.3.** Let $I(\Delta)$ be the set of ideals in $\Delta$, and consider the residual ideal operator:

$$\mathcal{R} = \mathcal{R}_\mu : K[x] \to I(\Delta), \quad g \mapsto (H_\mu(g)G_\mu) \cap \Delta.$$

This operator $\mathcal{R}$ translates questions about the action of $\mu$ on $K[x]$ into ideal-theoretic considerations in the $k$-algebra $\Delta$.

**Definition 1.4.** A MacLane-Vaquié key polynomial for $\mu$ is a monic polynomial in $K[x]$ which is simultaneously $\mu$-minimal and $\mu$-irreducible.

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

A key polynomial is necessarily irreducible in $K[x]$.

For any positive integer $m$ we denote:

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

**Proposition 1.5.** Take $\phi \in \text{KP}(\mu)$ and let $m = \deg(\phi)$. Consider the maximal ideal $\mathfrak{p} = \phi K[x]$, the field $K_\phi = K[x]/\mathfrak{p}$, and the onto mapping:

$$v_\phi : K_\phi^* \to \Gamma_{\mu,m}, \quad v_\phi(f + \mathfrak{p}) = \mu(a_0), \quad \forall f \in K[x] \setminus \mathfrak{p},$$

where $a_0 \in K[x]$ is the common 0-th coefficient of the $\phi$-expansion of all polynomials in the class $f + \mathfrak{p}$. Then,

1. The set $\Gamma_{\mu,m}$ is a subgroup of $\Gamma_\mu$ and $\langle \Gamma_{\mu,m}, \mu(\phi) \rangle = \Gamma_\mu$.
2. The mapping $v_\phi$ is a valuation on $K_\phi$ extending $v$, with value group $\Gamma_{\mu,m}$.

Denote the maximal ideal, the valuation ring and the residue class field of $v_\phi$ by:

$$\mathfrak{m}_\phi \subset \mathcal{O}_\phi \subset K_\phi, \quad k_\phi = \mathcal{O}_\phi/\mathfrak{m}_\phi.$$
Theorem 1.8. Suppose \( \mu/\nu \) commensurable and \( \text{KP}(\mu) \neq \emptyset \). Take \( \phi \in \text{KP}(\mu) \) of minimal degree, and let \( e = (\Gamma_\mu: \Gamma_{\mu, \text{deg}(\phi)}) \). Let \( \xi \in G'_\mu \) be a unit of degree \(-e\mu(\phi)\).

Then, \( \xi = H_{\mu}(\phi)e \in \Delta \) is transcendental over \( \kappa \), and

\[
\Delta = \kappa[\xi], \quad \text{Frac}(\Delta) = \kappa(\xi) \simeq k_\mu,
\]

the last isomorphism being induced by the canonical embedding \( \Delta \rightarrow k_\mu \).

Definition 1.9. Let \( \iota : \Gamma_\mu \rightarrow \Gamma' \) be an order-preserving embedding of \( \Gamma_\mu \) into another abelian ordered group. Take \( \phi \in \text{KP}(\mu) \) and \( \gamma \in \Gamma' \) any element such that \( \mu(\phi) < \gamma \).

The augmented valuation of \( \mu \) with respect to these data is the mapping

\[
\mu' : K[x] \rightarrow \Gamma' \cup \{\infty\}
\]

which assigns to any \( f \in K[x] \), with \( \phi \)-expansion \( f = \sum_{0 \leq s} a_s \phi^s \), the value:

\[
\mu'(f) = \text{Min} \left\{ \mu'(a_s \phi^s) | 0 \leq s \right\} = \text{Min} \left\{ \mu(a_s) + s\gamma | 0 \leq s \right\}.
\]

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

There is a canonical homomorphism of graded algebras:

\[
\mathcal{G}_\mu \rightarrow \mathcal{G}_{\mu'}, \quad H_\mu(f) \mapsto \begin{cases} H_{\mu'}(f), & \text{if } \mu(f) = \mu'(f), \\ 0, & \text{if } \mu(f) < \mu'(f). \end{cases}
\]

Proposition 1.10. Let \( \mu' = [\mu; \phi, \gamma] \), and let \( f \in K[x] \) be a non-zero polynomial.

(a) The valuation \( \mu' \) extends \( \nu \) and satisfies \( \mu(f) \leq \mu'(f) \) for all \( f \in K[x] \).

Equality holds if and only if \( \phi \not\mid f \). In this case, \( H_{\mu'}(f) \) is a unit in \( \mathcal{G}_{\mu'} \).

(b) The kernel of the homomorphism \( \mathcal{G}_\mu \rightarrow \mathcal{G}_{\mu'} \) is the prime ideal \( H_{\mu}(\phi) \mathcal{G}_\mu \).

(c) The polynomial \( \phi \) is a key polynomial for \( \mu' \) of minimal degree.

(d) The value group of \( \mu' \) is \( \Gamma_{\mu'} = \langle \Gamma_{\mu, \text{deg}(\phi)}, \gamma \rangle \subset \Gamma' \).

Propositions 1.10, 1.6, and 1.7 provide a precise description of the kernel and image of the canonical homomorphism \( \Delta_\mu \rightarrow \Delta_{\mu'} \).
Lemma 1.11. Let $\mu' = [\mu; \phi, \gamma]$. Then,
\[
\ker(\Delta_\mu \to \Delta_{\mu'}) = R(\phi), \quad \im(\Delta_\mu \to \Delta_{\mu'}) = \kappa_{\mu'} \hookrightarrow k_{\mu'},
\]
where $\kappa_{\mu'} \simeq k_\phi$ is the algebraic closure of $k$ simultaneously in $\Delta_{\mu'}$ and in $k_{\mu'}$.

2. Valuations of depth zero

Let us fix an order-preserving embedding of abelian ordered groups:
\[
\Gamma_Q \hookrightarrow (Z \times \Gamma_Q)_{\text{lex}}, \quad \gamma \mapsto (0,\gamma),
\]
where in $(Z \times \Gamma_Q)_{\text{lex}}$ we consider the lexicographical order.

Consider the following valuation on $K[x]$ extending $v$:
\[
\mu_{-\infty} : K[x] \to (Z \times \Gamma)_{\text{lex}} \cup \{\infty\}, \quad f \mapsto (-\deg(f), v(\text{lc}(f)))
\]
where $\text{lc}(f) \in K^*$ is the leading coefficient of a non-zero polynomial $f$.

Since $\Gamma_{\mu_{-\infty}} = (Z \times \Gamma)_{\text{lex}}$, the extension $\mu_{-\infty}/v$ is incommensurable.

The following (trivial) observation is left to the reader.

Lemma 2.1. Let $f, g \in K[x]$ be non-zero polynomials.

1. $f \sim_{\mu_{-\infty}} \text{lc}(f)x^{\deg(f)}$.
2. $f \sim_{\mu_{-\infty}} g \iff \deg(f) = \deg(g), \text{lc}(f) \sim_v \text{lc}(g)$.

The following result is an immediate consequence of Lemma 2.1.

Corollary 2.2. Let $y$ be an indeterminate, to which we assign degree $(-1,0)$.
There is an isomorphism of graded algebras
\[
gr_v(K)[y] \to G_{\mu_{-\infty}}, \quad y \mapsto H_{\mu_{-\infty}}(x).
\]
It induces an isomorphism $k \simeq \Delta_{\mu_{-\infty}} \simeq k_{\mu_{-\infty}}$ of $k$-algebras.
Moreover, $\mathcal{KP}(\mu_{-\infty}) = \{x + a \mid a \in K\}$ and all key polynomials are $\mu_{-\infty}$-equivalent.

Definition 2.3. A valuation $\mu$ on $K[x]$ is said to have depth zero if it is commensurable over $v$, and it is equivalent to some augmentation of $\mu_{-\infty}$.

By Corollary 2.2, a valuation of depth zero must be of the form:
\[
\mu_{x+a,\gamma} = [\mu_{-\infty}; x + a, (0,\gamma)], \quad a \in K, \quad \gamma \in \Gamma_Q.
\]
It is easy to check under what conditions two of these augmentations coincide:
\[
\mu_{x+a,\gamma} = \mu_{x+b,\gamma} \iff v(a - b) \geq \gamma = \gamma_*.
\]

By Proposition 1.10, the value group of these valuations is:
\[
\Gamma_{\mu_{x+a,\gamma}} = \langle \{0\} \times \Gamma, (0,\gamma) \rangle.
\]

By dropping the first (null) coordinate, we obtain equivalent valuations with values in $\Gamma_Q$, thus belonging to the space $V$. We denote them with the same symbol $\mu_{x+a,\gamma}$.

Their value group is $\Gamma_{\mu_{x+a,\gamma}} = \langle \Gamma, \gamma \rangle$ and they act as follows:
\[
\mu_{x+a,\gamma} : \sum_{0 \leq s} a_s(x + a)^s \mapsto \min \{v(a_s) + s\gamma \mid 0 \leq s\}.
\]

For instance, the depth-zero valuation $\mu_{x,0}$ is known as Gauss’ valuation.
Absolute minimality of $\mu_{-\infty}$. Thanks to the embedding (3), we may compare the values of $\mu_{-\infty}$ with those of the valuations in $\mathbb{V}$. We clearly have

$$\mu_{-\infty}(f) \leq \mu(f), \quad \forall f \in K[x], \quad \forall \mu \in \mathbb{V}. \tag{4}$$

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

**Theorem 2.4.** Let $\eta : K[x] \to \Gamma' \cup \{\infty\}$ be a valuation extending $v$, with respect to some order-preserving embedding $\iota : \Gamma \hookrightarrow \Gamma'$.

Then, after embedding $\Gamma_Q \hookrightarrow \Gamma'_Q$ by $\iota \otimes Q$, the following conditions are equivalent.

1. $\eta(f) \leq \mu(f)$, for all $f \in K[x]$ and all $\mu \in \mathbb{V}$.
2. $\eta(x) < \gamma$, for all $\gamma \in \Gamma_Q$.
3. The valuation $\eta$ is equivalent to $\mu_{-\infty}$.

**Proof.** Suppose condition (1) is satisfied. Then, our valuation $\eta$ satisfies:

$$\eta(x) \leq \mu_{x,\gamma}(x) = \gamma, \quad \forall \gamma \in \Gamma_Q.$$  

Since $v$ is non-trivial, the group $\Gamma_Q$ has no minimal element, and the last inequality must be strict. This proves (2).

Now, suppose that condition (2) is satisfied. We deduce immediately

$$\eta(x^m) < \gamma < \eta(x^{-m}), \quad \forall \gamma \in \Gamma_Q, \forall m \in \mathbb{Z}_{>0}. \tag{5}$$

This property implies:

$$f \sim_{\eta} \text{lcm}(f)^{\deg(f)}, \quad \forall f \in K[x], \quad f \neq 0. \tag{6}$$

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

$$n < m \implies \eta(x^{m-n}) < \nu(b/a) \implies \eta(ax^m) < \eta(bx^n). \tag{7}$$

Hence, we get an order-preserving group isomorphism

$$j : (\mathbb{Z} \times \Gamma)_{\text{lex}} \hookrightarrow \Gamma_{\eta}, \quad (m, \alpha) \mapsto \alpha - \eta(x^m).$$

In fact, (6) shows that $j$ is onto. And, if $(m, \alpha) \in \text{Ker}(j)$, then (5) implies

$$\eta(x^m) = \alpha \in \Gamma_Q \implies m = 0 \implies \alpha = 0.$$  

Thus $j$ is a group isomorphism. Also, $j$ preserves the ordering:

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

If $n < m$, this inequality follows from (7). If $n = m$, it follows from $\eta|_K = v$.

This proves (3), because the following diagram commutes:

$$\begin{array}{ccc}
(Z \times \Gamma)_{\text{lex}} & \xrightarrow{j} & \Gamma_{\eta} \\
\mu_{-\infty} & \hookrightarrow & \eta \\
\end{array}$$

$$K(x)^* \tag{8}$$

In fact, for any non-zero $f \in K[x]$, equation (6) shows that

$$\eta(f) = \eta\left(\text{lcm}(f)^{\deg(f)}\right) = j(-\deg(f), \nu(\text{lcm}(f))) = j(\mu_{-\infty}(f)).$$

Finally, suppose that $\eta$ and $\mu_{-\infty}$ are equivalent. That is, there exists an order-preserving isomorphism $j$ such that diagram (8) commutes.

Since $\eta|_K = v = \mu_{-\infty}|_K$, the isomorphism $j \otimes Q$ maps $\{0\} \times \Gamma_Q$ into $\iota(\Gamma_Q)$. Hence, by applying $j$ to the inequalities in (4), we obtain the inequalities in item (1). $\square$
3. Inductive valuations

A valuation \( \mu \) on \( K[x] \) extending \( v \) is said to be \textit{inductive} if it is attained after a finite number of augmentation steps starting with the minimal valuation \( \mu_{-\infty} \):

\[
\mu_{-\infty} \xrightarrow{\phi_0; \gamma_0} \mu_1 \xrightarrow{\phi_1; \gamma_1} \cdots \xrightarrow{\phi_r; \gamma_r} \mu_r = \mu,
\]

with values \( \gamma_0, \ldots, \gamma_r \in \Gamma_Q \), and intermediate valuations

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

Inductive valuations are commensurable over \( v \), because we do not consider \( \mu_{-\infty} \) to be an inductive valuation. The integer \( r \geq 0 \) is the \textit{length} of the chain (9).

By Proposition 3.10, every \( \phi_i \) is a key polynomial for \( \mu_i \) of minimal degree. Since every \( \phi_{i+1} \) is \( \mu_i \)-minimal, [11, Prop. 3.7] shows that

\[
1 = \deg(\phi_0) | \deg(\phi_1) | \cdots | \deg(\phi_{r-1}) | \deg(\phi_r).
\]

**Lemma 3.1.** For a chain of augmentations as in (9), take \( f \in K[x] \) 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 3.10 \( \mu_{i-1}(f) = \mu_i(f) \) and \( H_{\mu_i}(f) \) is a unit. Thus, \( \phi_{i+1} \nmid_{\mu_{i}} f \) since \( H_{\mu_i}(\phi_{i+1}) \) is a prime element in \( G_{\mu_i} \); hence, the argument may be iterated. \( \square \)

3.1. MacLane chains of valuations. Let us impose a technical condition on the augmentations to ensure that the value groups \( \Gamma_{\mu_0}, \ldots, \Gamma_{\mu_r} \) form a chain.

For a chain as in (9) and any index \( 0 \leq i < r \), [11, Prop. 6.6] shows that:

\[
\phi_{i+1} \mid_{\mu_i} \phi_i \iff \phi_{i+1} \sim_{\mu_i} \phi_i \implies \deg(\phi_i) = \deg(\phi_{i+1}).
\]

**Definition 3.2.** A chain of augmented valuations as in (9) is called a MacLane chain if it satisfies \( \phi_{i+1} \mid_{\mu_i} \phi_i \) for all \( 0 \leq i < r \).

If \( \deg(\phi_0) < \cdots < \deg(\phi_r) \), we say that it is an \textit{optimal} MacLane chain.

Obviously, the truncation of a MacLane chain at the \( i \)-th node is a MacLane chain of the intermediate valuation \( \mu_i \).

As an immediate application of Lemma 3.1 in a MacLane chain one has:

\[
\mu(\phi_i) = \mu_i(\phi_i) = \gamma_i, \quad 0 \leq i \leq r.
\]

All inductive valuations admit optimal MacLane chains, as the next result shows.

**Lemma 3.3.** [15] Sec. 1.2 Consider a chain of two augmented valuations

\[
\mu \xrightarrow{\phi; \gamma} \mu' \xrightarrow{\phi; \gamma} \mu
\]

with \( \deg(\phi_\ast) = \deg(\phi) \). Then, \( \phi_\ast \) is a key polynomial for \( \mu \), and \( \mu_\ast = [\mu; \phi_\ast; \gamma_\ast] \).

Thus, the length of a MacLane chain of \( \mu \) is not an intrinsic datum of \( \mu \). However, there is a strong unicity statement if we consider only optimal MacLane chains.

The next result follows from [11 Prop. 3.6]. Although that paper deals with rank one valuations, the arguments used in the proof are valid for arbitrary valuations.

**Proposition 3.4.** Consider an optimal MacLane chain as in (9) and another optimal MacLane chain

\[
\mu_{-\infty} \xrightarrow{\phi_0; \gamma_0} \mu_0 \xrightarrow{\phi_1; \gamma_1} \cdots \xrightarrow{\phi_{t-1}; \gamma_{t-1}} \mu_{t-1} \xrightarrow{\phi_t; \gamma_t} \mu_t = \mu^*.
\]

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

\[
\deg(\phi_i) = \deg(\phi_i^*), \quad \mu_{i-1}(\phi_i - \phi_i^*) \geq \gamma_i = \gamma_i^* \quad \text{for all} \quad 0 \leq i \leq r.
\]

In this case, we also have \( \mu_i = \mu_i^* \) for all \( 0 \leq i \leq r \).
Therefore, in any optimal MacLane chain of an inductive valuation \( \mu \) as in \([9]\), the intermediate valuations \( \mu_0, \ldots, \mu_{r-1} \), the values \( \gamma_0, \ldots, \gamma_r \in \Gamma_i \) and the positive integers \( \deg(\phi_0), \ldots, \deg(\phi_r) \), are intrinsic data of \( \mu \).

The depth of \( \mu \) is the length \( r \) of any optimal MacLane chain of \( \mu \).

The next result is an immediate consequence of \([11]\) Cor. 6.4.

**Lemma 3.5.** Consider a MacLane chain as in \([9]\), and denote \( \mu_{-1} := v \).

The value groups of the valuations \( \mu_i \) and \( v_{\phi_i} \) are:

\[
\Gamma_{v_{\phi_i}} = \Gamma_{\mu_{i-1}} \subset \Gamma_{\mu_i} = \langle \Gamma_{\mu_{i-1}}, \gamma_i \rangle, \quad 0 \leq i \leq r.
\]

In particular, we have a chain of ordered groups

\[
\Gamma_{\mu_{-1}} := \Gamma \subset \Gamma_{\mu_0} \subset \cdots \subset \Gamma_{\mu_r} = \Gamma_{\mu},
\]

and every quotient \( \Gamma_{\mu_{i-1}} / \Gamma_{\mu_{i-1}} \) is a finite cyclic group generated by \( \gamma_i \).

From now on, we shall use the following notation, for all \( 0 \leq i \leq r \).

\[
m_i = \deg(\phi_i), \quad e_i = (\Gamma_{\mu_i} : \Gamma_{\mu_{i-1}}), \quad h_i = e_i \gamma_i \in \Gamma_{\mu_{i-1}}.
\]

The identification \( \Gamma_{\mu_{i-1}} = v \left( K_{\phi_i}^* \right) \) yields a computation of the ramification index of the extension \( K_{\phi_i}/K \) in terms of these data:

\[
e(\phi_i) = (\Gamma_{\mu_{i-1}} : \Gamma) = e_0 \cdots e_{i-1}.
\]

**Chain of homomorphisms between the graded algebras.** Some more data supported by a MacLane chain are derived from the chain of homomorphisms:

\[
\mathcal{G}_{\mu_0} \rightarrow \mathcal{G}_{\mu_1} \rightarrow \cdots \rightarrow \mathcal{G}_{\mu_{r-1}} \rightarrow \mathcal{G}_{\mu}.
\]

Denote \( \Delta_i = \Delta_{\mu_i} \) for \( 0 \leq i \leq r \). By Lemma \([1,11]\) there is a sequence of fields

\[
\kappa_0 = \text{Im}(k \rightarrow \Delta_0), \quad \kappa_i = \text{Im}(\Delta_{i-1} \rightarrow \Delta_i), \quad 1 \leq i \leq r,
\]

where \( \kappa_i \) is isomorphic to the residue class field \( k_{\phi_i} \) of the extension \( K_{\phi_i}/K \) determined by \( \phi_i \). In particular, \( \kappa_i \) is a finite extension of \( k \).

We identify \( k \) with \( \kappa_0 \), and each field \( \kappa_i \subset \Delta_i \) with its image under the canonical map \( \Delta_i \rightarrow \Delta_j \) for \( j \geq i \). Thus, we consider as inclusions the canonical embeddings:

\[
k = \kappa_0 \subset \kappa_1 \subset \cdots \subset \kappa_r.
\]

The residual degree of the extension \( K_{\phi_i}/K \) can be computed as:

\[
f(\phi_i) = [\kappa_i : \kappa_0] = f_0 \cdots f_{i-1}, \quad f_{i-1} = [\kappa_i : \kappa_{i-1}], \quad 1 \leq i \leq r.
\]

**3.2. Chain of finitely-generated value subgroups.** If the group \( \Gamma_{\mu} \) is not finitely-generated, the homomorphism \( \mu : K(x)^* \rightarrow \Gamma_{\mu} \) does not admit a section.

In this section, the index \( i \) takes any integer value \( 0 \leq i \leq r \).

Let us choose finitely-generated subgroups \( \Gamma_i \subset \Gamma_{\mu_i} \). In section \([3,3]\) we shall construct a section \( \Gamma_{\mu_i} \hookrightarrow K(x)^* \) of \( \mu_i \).

Since \( \Gamma_{\mu_i} = \Gamma + \langle \gamma_0, \ldots, \gamma_i \rangle \), there exist \( \alpha_i \in \Gamma \) such that \( h_i \in \alpha_i + \langle \gamma_0, \ldots, \gamma_{i-1} \rangle \).

**Definition 3.6.** We fix a finitely-generated subgroup \( \Gamma_{-1} \subset \Gamma \) containing \( \alpha_0, \ldots, \alpha_r \). This choice determines finitely-generated subgroups

\[
\Gamma_i := \Gamma_{\mu_i}^{fg} := \langle \Gamma_{i-1}, \gamma_i \rangle = \langle \Gamma_{-1}, \gamma_0, \ldots, \gamma_i \rangle \subset \Gamma_{\mu_i}.
\]

By construction, \( h_i = e_i \gamma_i \in \Gamma_{i-1} \) for all \( i \).
These finitely-generated groups form a chain $\Gamma_{-1} \subset \Gamma_0 \subset \cdots \subset \Gamma_r$, with
\begin{equation}
\Gamma_i \cap \Gamma_{\mu_i-1} = \Gamma_{i-1}, \quad \Gamma_i / \Gamma_{i-1} \simeq \mathbb{Z} / e_i \mathbb{Z}.
\end{equation}

Finitely-generated ordered groups are free as $\mathbb{Z}$-modules. Take a basis of $\Gamma_{-1}$:
\begin{equation}
\Gamma_{-1} = t_0,1 \mathbb{Z} \oplus \cdots \oplus t_{0,k} \mathbb{Z}.
\end{equation}
From this basis, we shall derive specific bases for the other groups:
\begin{equation}
\Gamma_i = t_{i,1,1} \mathbb{Z} \oplus \cdots \oplus t_{i,1,k} \mathbb{Z},
\end{equation}
by a recurrent procedure. To this end, let us write:
\begin{equation}
\gamma_i = (t_{i,1} \cdots t_{i,k}) u \in (\Gamma_{-1}) \mathbb{Q}, \quad u = (h_{i,1} / e_{i,1} \cdots h_{i,k} / e_{i,k})^t \in \mathbb{Q}^k \times 1
\end{equation}
with $h_{i,j}, e_{i,j}$ coprime integers with $e_{i,j} > 0$, for all $1 \leq j \leq k$.

**Notation.** Denote $e'_{i,j} = e_{i,1} \cdots e_{i,j-1} / (d_{i,1} \cdots d_{i,j-1})$, $d_{i,j} = \gcd(e_{i,j}, e'_{i,j})$, $1 < j \leq k$.

There are uniquely determined integers $\ell_{i,j}, \ell'_{i,j}$ satisfying Bézout identities
\begin{equation}
\ell_{i,j} h_{i,j} e'_{i,j} + \ell'_{i,j} e_{i,j} = d_{i,j}, \quad 0 \leq \ell_{i,j} < e_{i,j} / d_{i,j}, \quad 1 \leq j \leq k.
\end{equation}

**Lemma 3.7.** $e_{i,1} \cdots e_{i,k} / (d_{i,1} \cdots d_{i,k}) = \text{lcm} (e_{i,1}, \ldots, e_{i,k}) = e_i$.

**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 sequences of less than $k$ integers. Then, $e'_{i,k} = \text{lcm} (e_{i,1}, \ldots, e_{i,k-1})$. Hence,
\begin{equation}
\text{lcm} (e_{i,1}, \ldots, e_{i,k}) = \text{lcm}(e'_{i,k}, e_{i,k}) = e'_{i,k} e_{i,k} / d_{i,k} = e_{i,1} \cdots e_{i,k} / (d_{i,1} \cdots d_{i,k}) .
\end{equation}

The identity $\text{lcm} (e_{i,1}, \ldots, e_{i,k}) = e_i$ follows from $e_i \mathbb{Z} = \{ e \in \mathbb{Z} \mid e \gamma_i \in \Gamma_{\mu_i-1} \}$.

**Lemma 3.8.** The following family $t_{i+1,1}, \ldots, t_{i+1,k}$ is a basis of $\Gamma_i$:
\begin{equation}
(t_{i+1,1} \cdots t_{i+1,k}) = (t_{i,1} \cdots t_{i,k}) Q, \quad Q = \begin{pmatrix}
(d_{i,1} / e_{i,1}) & \cdots & 0 \\
q_{m,j} & \cdots & d_{i,k} / e_{i,k}
\end{pmatrix},
\end{equation}
where $q_{m,j} = \ell_{i,j} e'_{i,m} h_{i,m} / e_{i,m}$, for $m > j$.

**Proof.** Consider the chain of $\mathbb{Z}$-modules $\Gamma_{i-1} \subset \Gamma_i \subset \Lambda$, where $\Lambda$ is the $\mathbb{Z}$-module generated by $t_{i,1} / e_{i,1}, \ldots, t_{i,k} / e_{i,k}$. By Lemma 3.7
\begin{equation}
(\Lambda : \Gamma_i) = (\Lambda : \Gamma_{i-1}) / (\Gamma_i : \Gamma_{i-1}) = e_{i,1} \cdots e_{i,k} / e_i = d_{i,1} \cdots d_{i,k}.
\end{equation}

On the other hand, let $\Gamma'$ be the $\mathbb{Z}$-module generated by $t_{i+1,1}, \ldots, t_{i+1,k}$. Let us show that $\Gamma' \subset \Gamma_i$. In fact, by using the Bézout identities, we get
\begin{equation}
t_{i+1,j} = \begin{pmatrix}
\ell_{i,j} & \ell'_{i,j} e_{i,j} \\
e_{i,j} & e_{i,j}
\end{pmatrix} \left( \begin{array}{c}
h_{i,j+1} / e_{i,j+1} t_{i,j+1} + \cdots + h_{i,k} / e_{i,k} t_{i,k} \\
h_{i,j} / e_{i,j} t_{i,j} + \cdots + h_{i,k} / e_{i,k} t_{i,k}
\end{array} \right)
\end{equation}
\begin{equation}
= \ell'_{i,j} t_{i,j} + \ell_{i,j} e'_{i,j} \left( \begin{array}{c}
\gamma_i - h_{i,1} / e_{i,1} t_{i,1} - \cdots - h_{i,j-1} / e_{i,j-1} t_{i,j-1}
\end{array} \right),
\end{equation}
for all $1 \leq j \leq k$. Now, by Lemma 3.7
\begin{equation}
e'_{i,j} / e_{i,t} = \text{lcm}(e_{i,1}, \ldots, e_{i,j-1}) / e_{i,t} \in \mathbb{Z}, \quad 1 \leq t < j.
\end{equation}
Hence, (15) expresses each $t_{i+1,j}$ as a $\mathbb{Z}$-linear combination of $t_{i,1}, \ldots, t_{i,j}, \gamma_i \in \Gamma_i$.

Consider the chain of $\mathbb{Z}$-modules $\Gamma' \subset \Gamma_i \subset \Lambda$.
The lower triangular matrix $P = \text{diag}(c_{i,1}, \ldots, c_{i,k})Q$ has integer coefficients and $\det(P) = d_{i,1} \cdots d_{i,k}$. We may rewrite the claimed basis of $\Gamma_i$ as:

$$(t_{i+1,1} \cdots t_{i+1,k}) = ((1/e_{i,1}) t_{i,1} \cdots (1/e_{i,k}) t_{i,k}) P.$$ 

Hence, $(\Lambda: \Gamma) = \det(P) = d_{i,1} \cdots d_{i,k} = (\Lambda: \Gamma_i)$. This proves $\Gamma' = \Gamma_i$. \hfill $\square$

### 3.3. Rational functions of a MacLane chain.

Our aim in this section is to construct an element $y_i \in \Delta_i$ which is transcendental over $\kappa_i$ and satisfies $\Delta_i = \kappa_i[y_i]$.

As indicated in Theorem 1.8, we may take

$$y_i = H_{\mu_i}(\phi_i)^{\epsilon_i} \epsilon_i,$$

for an arbitrary unit $\epsilon_i \in G^{\mu_i}_K$ of degree $-e_i \gamma_i = -h_i$. We shall construct this unit as the image in $G_{\mu_i}$ of an element in $K(x)$ with $\mu_i$-value equal to $-h_i$.

To this end, we construct in a recursive way rational functions $\pi_{i+1,j} \in K(x)^*$, for $-1 \leq i \leq r$, whose $\mu_i$-values attain the chosen basis $t_{i+1,1}, \ldots, t_{i+1,k}$ of $\Gamma_i$.

This will determine group homomorphisms

$$\pi_{i+1}: \Gamma_i \rightarrow K(x)^*, \quad \alpha \mapsto \pi_{i+1}^\alpha, \quad \mu_i(\pi_{i+1}^\alpha) = \alpha,$$

where we agree that $\mu_i = v$ and define

$$\pi_{i+1}^\alpha = \pi_{i+1,1}^{n_1} \cdots \pi_{i+1,k}^{n_k}, \quad \text{if } \alpha = n_1 t_{i+1,1} + \cdots + n_k t_{i+1,k}, \quad n_1, \ldots, n_k \in \mathbb{Z}.$$

**Definition 3.9.** Choose arbitrary $\pi_{0,j} \in K$ such that $v(\pi_{0,j}) = \iota_{0,j}$ for all $1 \leq j \leq k$.

For $0 \leq i \leq r$ and $1 \leq j \leq k$ we define

$$Y_i = \phi_i^{\epsilon_i} \pi_i^{-h_i}, \quad \pi_{i+1,j} = \left(\phi_i \pi_i^{-h_i/e_i,1} \cdots e_{i,j-1}^{e_{i,j-1}} \right)^{\ell_{i,j,1}} \pi_{i,j}. $$

In the definition of $\pi_{i+1,j}$, the rational functions $\pi_{i,1}, \ldots, \pi_{i,j-1}$ appear with integer exponents, because $e_{i,j}/e_{i,t}$ is an integer for $t < j$, as shown in (16).

For $i \geq 0$, it is easy to deduce from the definition that:

$$\pi_{i+1,j} = a \phi_i^{n_0} \cdots \phi_i^{n_{i-1}} \phi_i^{\ell_{i,j,1}} \pi_{i,j},$$

for some $a \in K^*$ and certain (eventually negative) integer exponents $n_0, \ldots, n_{i-1}$. Since $\phi_{i+1}^{1/\mu_i} \phi_i \ell \leq i$, Lemma 3.1 shows that

$$\mu_i(Y_i) = \mu_{i+1}(Y_i) = \cdots = \mu(Y_i), \quad \mu_i(\pi_{i+1,j}) = \mu_{i+1}(\pi_{i+1,j}) = \cdots = \mu(\pi_{i+1,j}).$$

Clearly, $\mu_i(Y_i) = 0$ by the definition of $Y_i$. Let us compute the other stable value.

**Lemma 3.10.** For all $-1 \leq i \leq r, 1 \leq j \leq k$, we have $\mu_i(\pi_{i+1,j}) = \iota_{i+1,j}$.

**Proof.** 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 $i-1$. Then $\mu_i(\pi_{i,j}) = \mu_{i-1}(\pi_{i,j}) = \iota_{i,j}$ by (15). Hence,

$$\mu_i(\pi_{i+1,j}) = \ell_{i,j,1} \pi_{i,j} \left(\gamma_i \frac{e_{i,j}}{e_{i,j-1}} \iota_{i,j-1} + \ell_{i,j-1} \iota_{i,j-1} \iota_{i,1} - \iota_{i,j-1} \iota_{i,1} \right),$$

for all $1 \leq j \leq k$, as shown in (15). \hfill $\square$

Our next aim is to establish certain relationships between the rational functions of Definition 3.9. To this end we introduce some more notation.

**Definition 3.11.** Take an index $0 \leq i \leq r$. Denote:

$$L_i' = \ell_{i,1} \cdots \ell_{i,k}, \quad L_{i,j} = \ell_{i,j} \ell_{i,j+1} \cdots \ell_{i,k}, \quad 1 \leq j \leq k.$$ 

Consider the function $L_i: (\Gamma_{i-1})^\mu \rightarrow \mathbb{Q}$ defined as

$$L_i((t_{i,1} \cdots t_{i,k})^\mu) = (L_{i,1} \cdots L_{i,k})^\mu, \quad \forall \mu \in \mathbb{Q}^{k \times 1}.$$
Lemma 3.12. For all \( 0 \leq i \leq r \), we have \( L'_i + L_i(\gamma_i) = 1/e_i \).

Proof. The following identity is an immediate consequence of (14):

\[
\ell'_{i,j} e'_{i,j} + \ell_{i,j} h_{i,j} e_{i,j} = d_{i,j} e_{i,j} = d_{i,1} \ldots d_{i,j} e_{i,1} \ldots e_{i,j} =: \frac{1}{e'_{i,j+1}}, \quad 1 \leq j \leq k.
\]

Now, we claim that:

\[
L'_i + L_i h_{i,1} e_{i,1} + \cdots + L_i h_{i,j} e_{i,j} = \ell'_{i,j+1} \cdots \ell'_{i,k} \frac{1}{e'_{i,j+1}}, \quad 1 \leq j \leq k.
\]

For \( j = k \), this identity proves the lemma, since \( e'_{i,k+1} = e_i \) by Lemma 3.7.

Let us apply an inductive argument. For \( j = 1 \), (20) follows directly from (19), having in mind that \( e'_{i,1} = 1 \). Now, if (20) holds for \( j - 1 \):

\[
L'_i + L_i h_{i,1} e_{i,1} + \cdots + L_i h_{i,j-1} e_{i,j-1} = \ell'_{i,j} \cdots \ell'_{i,k} \frac{1}{e'_{i,j}},
\]

we deduce the identity (20) for \( j \), just by adding \( L_i h_{i,j} e_{i,j} / e'_{i,j} \) to both sides of the equality, and by applying (19) to the right-hand side. \( \square \)

Lemma 3.13. For \( 0 \leq i \leq r \), let \( Q \) be the matrix introduced in Lemma 3.8. Then,

\[
e_i(L_{i,1} \ldots L_{i,k})Q = (\ell_{i,1} e'_{i,1} \cdots \ell_{i,k} e'_{i,k}).
\]

Proof. The statement is equivalent to the following identity:

\[
L_i e_{i,j} d_{i,j} + L_i q_{j+1,j} + \cdots + L_i k_{j,j} = \frac{1}{e_i} \ell_{i,j} e'_{i,j}, \quad 1 \leq j \leq k,
\]

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,

\[
L_i e_{i,j} d_{i,j} + L_i h_{i,j+1} e_{i,j+1} + \cdots + L_i k_{j,j} h_{i,j} e_{i,j} = \frac{1}{e_i}.
\]

By Lemma 3.12, this is equivalent to

\[
L'_i + L_i h_{i,1} e_{i,1} + \cdots + L_i h_{i,j} e_{i,j} = L_i d_{i,j} e_{i,j} = \ell'_{i,j+1} \cdots \ell'_{i,k} \frac{1}{e'_{i,j+1}},
\]

which was proven in (20). \( \square \)

Let us rewrite the identities in Definition 3.9 by using formal logarithms:

\[
(\log \pi_{i+1,1} \cdots \log \pi_{i+1,k}) = \log \phi_i (\ell_{i,1} e'_{i,1} \cdots \ell_{i,k} e'_{i,k}) + (\log \pi_{i,1} \cdots \log \pi_{i,k}) A,
\]

where \( A = (a_{m,j}) \in \mathbb{Q}^{k \times k} \) is the matrix with entries:

\[
a_{m,j} = \begin{cases} 0, & \text{if } m > j \\ \ell'_{i,j}, & \text{if } m = j \\ -\ell_{i,j} e'_{i,j} h_{i,m} / e_{i,m}, & \text{if } m < j \end{cases}.
\]

Lemma 3.14. Let \( 0 \leq i \leq r \). Consider the matrix \( B = u (L_{i,1} \ldots L_{i,k}) \in \mathbb{Q}^{k \times k} \), where \( u \) is the column-vector defined in (13).

1. If \( \alpha = (i_{i,1} \cdots i_{i,k}) \) \( v \), for some \( v \in \mathbb{Q}^{k \times 1} \), then \( Bv = L_i(\alpha)u \).
2. \( A = (I - e_i B)Q \).
3. The vector \( u \) is an eigenvector of the matrix \( I - e_i B \), with eigenvalue \( e_i L'_i \).
Proof. Item (1) follows from the definition of the operator \(L_i\). By Lemma 3.13
\[
(I - e_i B)Q = Q - e_i u (L_{i,1} \cdots L_{i,k}) Q = Q - u (\ell_{i,1} e'_{i,1} \cdots \ell_{i,k} e'_{i,k}).
\]
Hence, item (2) is equivalent to
\[
q_{m,j} - a_{m,j} = \ell_{i,j} e'_{i,j} h_{i,m}/e_{i,m}, \quad \forall i, m, j.
\]
If \(m > j\) (\(a_{m,j} = 0\)), or \(m < j\) (\(q_{m,j} = 0\)), the identity is obvious. If \(m = j\), it follows from \(\ell_{i,m} h_{i,m} e_{i,m} = d_{i,m} - \ell'_{i,m} e_{i,m}\). Finally,
\[
(I - e_i B)u = u - e_i L_i(\gamma_i)u = e_i L'_i u,
\]
by the first item and Lemma 3.12 \(\square\)

Proposition 3.15. For all \(0 \leq i \leq r\), we have \(\phi_i/\pi_{i+1}^{1} = Y_i^{L_i^i}\).

Proof. By (21) and Lemmas 3.12 and 3.14
\[
\log \left( \frac{\phi_i}{\pi_{i+1}^{1}} \right) = \log \phi_i - (\log \pi_{i+1} \cdots \log \pi_{i+1}) (Q^{-1}u) \log \phi_i - (\log \pi_{i+1} \cdots \log \pi_{i,k}) A Q^{-1}u
\]
\[
= (1-e_i L_i(\gamma_i)) \log \phi_i - (\log \pi_{i+1} \cdots \log \pi_{i,k}) (I-e_i B)u
\]
\[
= \log e_i L'_i - (\log \pi_{i+1} \cdots \log \pi_{i,k}) e_i L'_i u = \log Y_i^{L_i^i},
\]
because \((\log \pi_{i+1} \cdots \log \pi_{i,k}) e_i u = \log \pi_{i+1}^{\gamma_i} = \log \pi_{i+1}^{h_i} \square\)

The restriction of \(\pi_{i+1}\) to the subgroup \(\Gamma_{i-1} \subset \Gamma_{i}\) does not coincide with \(\pi_{i}\). The next result computes the quotient of these two homomorphisms on \(\Gamma_{i-1}\).

Proposition 3.16. For all \(0 \leq i \leq r\) and \(\beta \in \Gamma_{i-1}\), we have \(\pi_{i+1}/\pi_{i} = Y_i^{L_i(\beta)}\).

Proof. Let \(b\) be the column vector determined by \(\beta = (i_{1,1} \cdots i_{k,i})^T\). By (21) and Lemmas 3.13 and 3.14
\[
\log \left( \frac{\pi_{i+1}}{\pi_{i}} \right) = (\log \pi_{i+1} \cdots \log \pi_{i+1}) Q^{-1}b - (\log \pi_{i+1} \cdots \log \pi_{i,k}) b
\]
\[
= \log e_i L_i(\beta) \log \phi_i - (\log \pi_{i+1} \cdots \log \pi_{i,k}) e_i B b
\]
\[
= \log e_i L_i(\beta) - (\log \pi_{i+1} \cdots \log \pi_{i,k}) e_i L_i(\beta) u = \log Y_i^{L_i(\beta)},
\]
because \((\log \pi_{i+1} \cdots \log \pi_{i,k}) e_i u = \log \pi_{i+1}^{\gamma_i} = \log \pi_{i+1}^{h_i} \square\)

The next result follows immediately from Propositions 3.15 and 3.16.

Proposition 3.17. Let \((s, u) \in \mathbb{Z}_{\geq 0} \times \Gamma_{r-1}\). Then, \(\phi_i^s \pi_{i+1}^{u+e_i u} = (Y_i)^{L_i^s} s^{-L_r(u)}\).

Images in \(G_\mu\) of the rational functions. By (17), the rational functions \(Y_i, \pi_{i,j}\) introduced in Definition 3.9 are the product of some \(a \in K^*\) by powers of \(\phi_0, \ldots, \phi_i\) with integer exponents. The exponent of \(\phi_i\) is \(e_i\) and 0, respectively.

For \(0 \leq j < i\), the exponent of \(\phi_j\) may be negative, but the element \(H_{\mu_k}(\phi_j)\) is a unit in \(G_\mu\), by Proposition 1.10. 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 3.18. For \(0 \leq i \leq r\), \(1 \leq j \leq k\), we define
\[
x_i = H_{\mu_i}(\phi_i) \in G_\mu, \quad y_i = H_{\mu_i}(Y_i) \in \Delta_i, \quad p_{i,j} = H_{\mu_i}(\pi_{i,j}) \in G_\mu^*.
\]
Also, we define group homomorphisms:
\[
p_i: \Gamma_{i-1} \rightarrow G_{\mu_i}^*, \quad \alpha \mapsto p_i^\alpha = H_{\mu_i}(\pi_{i}^\alpha) = p_{i,1}^{\alpha_1} \cdots p_{i,k}^{\alpha_k},
\]
if $\alpha = n_1 \epsilon_{i,1} + \cdots + n_k \epsilon_{i,k} \in \Gamma_{i-1}$, with $n_1, \ldots, n_k \in \mathbb{Z}$.

**Lemma 3.19.** Let $(s, u), (s', u') \in \mathbb{Z}_{\geq 0} \times \Gamma_{\mu_{\nu-1}}$ such that $u + s \gamma_{\nu} = u' + s' \gamma_{\nu}$.

Then, there exists $j \in \mathbb{Z}$ such that

$$s' = s + je_{\nu}, \quad u' = u - jh_{\nu}, \quad x_{\nu}^s \ell_{\nu}^{u'} = x_{\nu}^s \ell_{\nu}^u.$$ 

**Proof.** From $(s' - s) \gamma_{\nu} = u - u' \in \Gamma_{\mu_{\nu-1}}$, we deduce $s' - s = je_{\nu}$ for some $j \in \mathbb{Z}$. Then, $u' = u - je_{\nu} \gamma_{\nu} = u - jh_{\nu}$. The lemma follows then from $y_{\nu} = x_{\nu}^s \ell_{\nu}^u$.

**Definition 3.20.** Suppose $0 \leq i < r$ and let $\alpha \in \Gamma_{\nu-1}$. Since $\phi_{i+1}^{-1} \phi_i$, Proposition 4.10 shows that the elements $x_i, y_i, \ell_{i}^{\alpha} \in \mathcal{G}_{\mu_i}$ are mapped to units in $\mathcal{G}_{\mu_j}$, for all $j > i$, under the canonical homomorphism. We denote these images respectively by

$$x_i \in \mathcal{G}_{\mu_j}, \quad z_i \in \Delta_j = \kappa_j, \quad \ell_{i}^{\alpha} \in \mathcal{G}_{\mu_j}.$$

**Lemma 3.21.** If $0 \leq i < r$, then $\kappa_{i+1} = \kappa_i[z_i] = k[z_0, \ldots, z_i]$.

**Proof.** By Theorem 1.8, $\Delta_i = \kappa_i[y_i]$. Hence, $\kappa_{i+1} = \text{Im}(\Delta_i \rightarrow \Delta_{i+1}) = \kappa_i[z_i]$.

In optimal MacLane chains, the elements $x_i, \ell_{i}^{\alpha}, y_r, z_i \in \mathcal{G}_{\mu}$ are “almost” independent of the chain. Their precise variation is analyzed in section 5.6.

4. **Newton polygons**

In this section, we study the Newton polygon operator attached to some $\mu \in \mathbb{V}$ with respect to a key polynomial. We generalize the results of [1, Sec.2] (where $\mu$ was assumed to have rank one), up to a different normalization of the Newton polygons.

4.1. **Newton polygon operator.** Consider two points $P = (s, \alpha), Q = (t, \beta)$ in the $\mathbb{Q}$-vector space $\mathbb{Q} \times \Gamma_{\nu}$. The segment joining $P$ and $Q$ is the subset

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

If $P = Q$, then $S = \{P\}$. If $s \neq t$, this segment has a natural slope

$$\text{sl}(S) = (\beta - \alpha)/(t - s) \in \Gamma_{\nu}.$$ 

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

Let $\mu : K[x] \rightarrow \Gamma_{\nu} \cup \{\infty\}$ be a valuation in the space $\mathbb{V}$. The choice of a key polynomial $\phi$ for $\mu$ determines a **Newton polygon operator**

$$N_{\mu,\phi} : K[x] \rightarrow \mathcal{P}(\mathbb{Q} \times \Gamma_{\nu}),$$

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

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

$$g = \sum_{0 \leq s} a_s \phi_s, \quad \text{deg}(a_s) < \text{deg}(\phi)$$

is the canonical $\phi$-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

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

Thus, $N$ is either a single point or a chain of segments, called the **sides** of the polygon. From left to right, these sides have increasing slopes.
Figure 1. Newton polygon \( N = N_{\mu',\phi}(g) \) of \( g \in K[x] \)

\[
\begin{array}{c}
\text{Figure 2.} \ \lambda\text{-component of } N_{\mu',\phi}(g). \ \text{The line } L \text{ has slope } -\lambda.
\end{array}
\]

The abscissa of the left endpoint of \( N \) is \( s = \text{ord}_\phi(g) \).
The abscissa of the right endpoint of \( N \) is called the \textit{length} of \( N \), and is denoted:
\[
\ell(N) = \lfloor \deg(g) / \deg(\phi) \rfloor.
\]
The left and right endpoints of \( N \), together with the points joining two different sides are called \textit{vertices} of \( N \).

**Definition 4.1.** Let \( g \in K[x] \), \( N = N_{\mu',\phi}(g) \) and \( \lambda \in \Gamma_Q \).

The \( \lambda \)-component \( S_\lambda(N) \subset N \) is the intersection of \( N \) with the line of slope \(-\lambda\) which first touches \( N \) from below. In other words,
\[
S_\lambda(N) = \{(s, u) \in N \mid u + s\lambda \text{ is minimal}\}.
\]
The abscissas of the endpoints of \( S_\lambda(N) \) are denoted \( s_{\mu,\phi,\lambda}(g) \leq s'_{\mu,\phi,\lambda}(g) \).

If \( N \) has a side \( S \) of slope \(-\lambda\), then \( S_\lambda(N) = S \). Otherwise, \( S_\lambda(N) \) is a vertex of \( N \). Figure 2 illustrates both possibilities.

**Definition 4.2.** We say that \( N = N_{\mu',\phi}(g) \) is one-sided of slope \(-\lambda\) if
\[
N = S_\lambda(N), \quad s_{\mu,\phi,\lambda}(g) = 0, \quad s'_{\mu,\phi,\lambda}(g) > 0.
\]

Since \( \mu(g) = \min\{\mu(a_s\phi^s) \mid s \geq 0\} \), the next observation follows immediately.

**Remark 4.3.** For any non-zero \( g \in K[x] \), the value \( \mu(g) \in \Gamma_Q \) 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 \( N_{\mu',\phi}(g) \). (see Figure 3)

Let \( S \) be a side of \( N_{\mu',\phi}(g) \) with slope \( \text{sl}(S) < -\mu(\phi) \). Then, the augmented valuation \([\mu; \phi, -\text{sl}(S)]\) contains relevant arithmetic information about \( g \), with respect to \( \phi \).

This motivates the next definition.

**Definition 4.4.** The principal Newton polygon \( N_{\mu,\phi}^{pp}(g) \) 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 \( N_{\mu',\phi}(g) \).

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

**Lemma 4.5.** Let \( N = N_{\mu',\phi}(g) \) be the Newton polygon of a non-zero \( g \in K[x] \).

1. The length \( \ell \left( N^{pp}_{\mu',\phi}(g) \right) \) coincides with the order with which the prime element \( H_{\mu}(\phi) \) divides \( H_{\mu}(g) \) in the graded algebra \( G_{\mu} \).
2. If \( h \in K[x] \) satisfies \( g \sim_{\mu} h \), then \( S_{\mu}(\phi)(g) = S_{\mu}(\phi)(h) \).

**Proof.** The points \((s, \mu(a_s)) \in S_{\mu}(\phi)(g)\) are those with \( s \) belonging to the set

\[
I(g) = \{ s \in \mathbb{Z}_{\geq 0} \mid \mu(a_s \phi^s) = \mu(g) \}.
\]

Clearly, \( \ell \left( N^{pp}_{\mu',\phi}(g) \right) = \min(I) \). By [11, Lem. 2.8], this non-negative integer is the order with which \( H_{\mu}(\phi) \) divides \( H_{\mu}(g) \) in \( G_{\mu} \).

Finally, if \( g \sim_{\mu} h \), then [11, Lem. 2.10] shows that \( I(g) = I(h) \). Hence, the two segments \( S_{\mu}(\phi)(g), S_{\mu}(\phi)(h) \) have endpoints with the same abscissas \( s < s' \). On the other hand, the ordinates \( u, u' \) of their endpoints are determined by the abscissas and the common value

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

Hence, these segments coincide. \( \square \)

4.2. **Newton polygons with respect to augmented valuations.** Let us fix a valuation \( \mu \in V \) and a key polynomial \( \phi \in KP(\mu) \). Consider the augmentation

\[
\mu' = [\mu; \phi, \gamma], \quad \gamma = \mu'(\phi) > \mu(\phi), \quad \gamma \in \Gamma_{\phi}.
\]

Take a non-zero \( g \in K[x] \), with \( \phi \)-expansion \( g = \sum_{0 \leq s} a_s \phi^s \). Let us denote

\[
(22) \quad S_{\gamma}(\phi) = S_{\gamma}(N_{\mu,\phi}(g)), \quad s(g) = s_{\mu,\phi,\gamma}(g), \quad s'(g) = s'_{\mu,\phi,\gamma}(g),
\]

and let \( u(g) \in \Gamma_{\phi} \) be the ordinate of the left endpoint of \( S_{\gamma}(g) \).

By Proposition 1.10, \( \phi \) is a key polynomial for \( \mu' \) of minimal degree.

The Newton polygon \( N_{\mu',\phi}(g) \) is related to \( N_{\mu,\phi}(g) \) in an obvious way:

\[
N_{\mu',\phi}(g) = N_{\mu,\phi}(g), \quad N^{pp}_{\mu',\phi}(g) \not\subseteq N^{pp}_{\mu,\phi}(g).
\]

In fact, since \( \mu'(a_s) = \mu(a_s) \) for all \( s \), these polygons have the same cloud of points. But their principal parts are different because \( \mu'(\phi) > \mu(\phi) \).

Since \( S_{\gamma}(g) \) coincides with the \( \mu'(\phi) \)-component of \( N_{\mu',\phi}(g) \), the results in the last section show that \( N_{\mu,\phi}(g) \) yields information about \( g, \mu', \phi \).
The claimed identity \( u \) the statement is equivalent to the equalities

Proof. Since the involved segments either have the same slope or consist of a single point,

Let Theorem 4.8.

\( \Gamma \)

The first two equalities follow from Lemma 4.6. In order to prove the third, consider the

For non-zero \( g, h \in K[x] \) 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 \( \mathcal{G}_{\mu'} \). In particular, \( s(gh) = s(g) + s(h) \).

\( \mu, \phi \)

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

Proof. Item (1) follows directly from Lemma 4.5. Since \( \phi \) is a key polynomial for \( \mu' \) of

minimal degree, item (2) follows from [11, Cor. 3.4].

4.3. Addition of Newton polygons. We admit that a point in the space \( \mathbb{Q} \times \Gamma_{\mathbb{Q}} \) is a segment whose right and left endpoints coincide.

There is a natural addition of segments in \( \mathbb{Q} \times \Gamma_{\mathbb{Q}} \). 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.

We keep dealing with an arbitrary valuation \( \mu \in \mathbb{V} \), and a key polynomial \( \phi \in \mathcal{K}_P(\mu) \).

Also, for any \( \gamma \in \Gamma_{\mathbb{Q}}, \gamma > \mu(\phi) \), we keep using the notation of [22].

Lemma 4.7. For non-zero \( g, h \in K[x] \), and any \( \gamma \in \Gamma_{\mathbb{Q}}, \gamma > \mu(\phi) \), 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 Lemma 4.6. In order to prove the third, consider the augmented valuation \( \mu' = [\mu; \phi, \gamma] \). By Remark 4.3

\[ u(g) + s(g)\gamma = \mu'(g), \quad u(h) + s(h)\gamma = \mu'(h), \quad u(gh) + s(gh)\gamma = \mu'(gh). \]

The claimed identity \( u(gh) = u(g) + u(h) \) follows from \( \mu'(gh) = \mu'(g) + \mu'(h) \) and \( s(gh) = s(g) + s(h) \).

The addition of segments may be extended to an addition law for Newton polygons, just

by identifying a Newton polygon with the sum of its sides.

As an immediate consequence of Lemma 4.7, we get the Theorem of the product for principal Newton polygons.

Theorem 4.8. Let \( \phi \) be a key polynomial for the valuation \( \mu \in \mathbb{V} \). Then, for any non-zero \( g, h \in K[x] \) we have \( N_{\mu, \phi}(gh) = N_{\mu, \phi}(g) + N_{\mu, \phi}(h) \).

The analogous statement for entire Newton polygons is false (cf. [1, Sec. 2]).
5. Residual polynomial operators of inductive valuations

Consider a MacLane chain of an inductive valuation $\mu$ on $K[x]$:

$$
\mu_{-\infty} \xrightarrow{\phi_0, \gamma_0} \mu_0 \xrightarrow{\phi_1, \gamma_1} \cdots \xrightarrow{\phi_{r-1}, \gamma_{r-1}} \mu_{r-1} \xrightarrow{\phi_r, \gamma_r} \mu_r = \mu.
$$

We use the simplified notation $G = G_\mu$, $\Delta = \Delta_\mu$, and we shall freely use all data associated with the MacLane chain in section 3.

Specially relevant to our purpose is the tower of finite field extensions:

$$
(23) \quad k = \kappa_0 \subset \kappa_1 \subset \cdots \subset \kappa_r; \quad \kappa_i = \text{Im}(\Delta_{i-1} \to \Delta_i) \subset \Delta_i, \quad 1 \leq i \leq r.
$$

Each $\kappa_i$ is the algebraic closure of $k$ in $\Delta_i$, and it satisfies $\Delta_i^+ = \kappa_i^+$.

Also, we shall make use of the Newton polygon operators

$$
N_i := N_{\mu_{i-1}, \phi_i}, \quad 0 \leq i \leq r.
$$

5.1. Definition of the residual polynomial operator. For a non-zero $f \in K[x]$ consider the canonical $\phi_r$-expansion:

$$
(24) \quad f = \sum_{s=0}^{\ell} a_s \phi_r^s, \quad \deg(a_s) < \deg(\phi_r).
$$

By the definition of an augmented valuation,

$$
\mu(f) = \text{Min}\{ \mu(a_s \phi_r^s) \mid s \geq 0 \} = \text{Min}\{ \mu_{r-1}(a_s) + s\gamma_r \mid s \geq 0 \}.
$$

In the case $r = 0$, we have $a_s \in K$ and we agree that $\mu_{-1} = v$.

The Newton polygon $N_r(f)$ is the lower convex hull of the cloud of points:

$$
C = \{ Q_s \mid s \geq 0 \} \subset \mathbb{Z}_{\geq 0} \times \Gamma_{r-1}, \quad Q_s = (s, \mu_{r-1}(a_s)).
$$

Let $S_{\gamma_r}(f) \subset \mathbb{Q} \times \Gamma_\mathbb{Q}$ be the $\gamma_r$-component of $N_r(f)$ (Definition 4.1). Let

$$(s_0, u_0) := (s_r(f), u_r(f)), \quad (s'_r(f), u'_r(f))$$

be the left and right endpoints of $S_{\gamma_r}(f)$, respectively.

By Remark 3.3 for any point $(s, u) \in N_r(f)$, we have

$$(s, u) \in S_{\gamma_r}(f) \iff u + s \gamma_r = \mu(f) = u_0 + s_0 \gamma_r.$$

By Lemma 3.19 $d := (s'_r(f) - s_r(f))/\epsilon_r$ is an integer, and if we take

$$
s_j = s_0 + j\epsilon_r, \quad u_j = u_0 - j\epsilon_r, \quad P_j = (s_j, u_j), \quad 0 \leq j \leq d,
$$

then, $S_{\gamma_r}(f) \cap (\mathbb{Z}_{\geq 0} \times \Gamma_{r-1}) = \{ P_0, P_1, \ldots, P_d \}$.

By construction, the endpoints of $S_{\gamma_r}(f)$ belong to the cloud $C$. That is, $P_0 = Q_{s_0}$, $P_d = Q_{s_d}$. However, for $0 < j < d$, the point $Q_{s_j} \in C$ may lie strictly above $P_j$.

In [11] Sec. 5, a normalized (monic) residual polynomial of $f$ was considered:

$$
\tilde{R}_r(f) = \zeta_0 + \zeta_1 y + \cdots + \zeta_{d-1} y^{d-1} + y^d \in \kappa_r[y],
$$

with coefficients

$$
\zeta_j = p_r^{-h_r(d-j)} H_\mu(a_{s_d})^{-1} H_\mu(a_{s_j}) \in \kappa_r^*,
$$

if $Q_{s_j}$ lies on $N_r(f)$, and $\zeta_j = 0$ otherwise.

The main aim of the paper is to find an efficient algorithm to compute the chain of fields (23) and the polynomial $\tilde{R}_r(f)$. To this end, we consider a non-normalized version of the residual polynomial, defined only on a certain subset of $K[x]$.

Consider the subset of polynomials having attainable $\mu$-values:

$$
K[x]_{\mu-\text{att}} = \left\{ g \in K[x] \mid \mu(g) \in \Gamma_{\mu}^g \right\} \subset K[x],
$$

where $\Gamma_{\mu}^g = \Gamma_r \subset \Gamma_\mu$ is the finitely-generated subgroup introduced in section 3.2.
Lemma 5.1. Let \( f \in K[x] \) be a non-zero polynomial, with \( \phi_r \)-expansion as in \([24]\).

1. There is a constant \( a \in K^* \) such that \( af \) has attainable \( \mu \)-value.
2. If \( f \) is monic and \( \mu \)-minimal, then it has attainable \( \mu \)-value.
3. If \( f \) has attainable \( \mu \)-value and \( Q_s \in S_{\gamma_r}(f) \), then the coefficient \( a_s \in K[x] \) has attainable \( \mu_{r-1} \)-value.

Proof. The first item follows from \( \Gamma_{\mu} = \Gamma + \langle \gamma_0, \ldots, \gamma_r \rangle = \Gamma + \Gamma_r \).

If \( f \) is monic and \( \mu \)-minimal, then \( a_\ell = 1 \) and \( \mu(f) = \mu(\phi_r^f) = \ell \gamma_r \in \Gamma_{\mu}^{d_g} \) by \([11]\) Prop. 3.7.

The condition \( Q_s \in S_{\gamma_r}(f) \) implies \( \mu(f) = \mu_{r-1}(a_s) + s \gamma_r \). If \( \mu(f) \in \Gamma_r \), then \( [12] \) shows that \( \mu_{r-1}(a_s) \in \Gamma_{\mu_{r-1}} \cap \Gamma_r = \Gamma_{r-1} \). \( \square \)

Definition 5.2. Let us define a residual polynomial operator:

\[ R_r : K[x]_{\mu \text{-att}} \to \kappa_r[y], \quad f \mapsto R_r(f) = c_0 + c_1 y + \cdots + c_d y^d. \]

We agree that \( R_r(0) = 0 \), and for a non-zero \( f \in K[x]_{\mu \text{-att}} \) as in \([24]\), we take

\[ c_j = \begin{cases} \mu_{r-1}(a_s) h_{\mu}(a_s_j) \in \kappa_r^*, & \text{if } Q_s \text{ lies on } N_r(f), \\ 0, & \text{otherwise.} \end{cases} \]

Since \( \deg(a_s_j) < \deg(\phi_r) \), \( H_{\mu}(a_s_j) \) is a unit in \( G \) \([11]\) Prop. 3.5]. By Proposition 1.10 and Lemma 5.1 \( \mu(a_s_j) = \mu_{r-1}(a_s_j) \in \Gamma_{r-1} \). Therefore, if \( Q_s \) lies on \( N_r(f) \), the coefficient \( c_j \) is a homogeneous unit of degree zero; that is, \( c_j \in \Delta^* = \kappa_r^* \).

If we normalize \( R_r(f) \), we obtain the normalized residual polynomial \( \hat{R}_r(f) \):

\[ c_d^{-1} R_r(f) = \hat{R}_r(f). \]

In fact, if \( Q_s \) lies on \( N_r(f) \), then

\[ p_r^{-\mu_{r-1}(a_s)} / p_r^{-\mu_{r-1}(a_{s,d})} = p_r^{\mu_{r-1}(a_s)-\mu_{r-1}(a_{s,d})} = p_r^{u_{d}-u_j} = p_r^{-h_r(d-j)}. \]

The operator \( \hat{R}_r \) depends on the choice of \( \phi \) and the unit \( e = p_r^{-h_r} \), while \( R_r \) depends on the choice of \( \phi \) and the homomorphism \( p_r \) from Definition 3.18.

In section 5.4 we shall prove that the operator \( R_r \) admits a recursive computation involving the previous operators \( R_0, \ldots, R_{r-1} \) attached to the intermediate valuations \( \mu_0, \ldots, \mu_{r-1} \) of the MacLane chain of \( \mu \).

If \( \Gamma \) is finitely generated, we may take \( \Gamma_{r-1} = \Gamma \) as a universal choice for this subgroup. This implies \( \Gamma_i = \Gamma_{\mu_i} \) for all \( i \). Then, \( K[x]_{\mu \text{-att}} = K[x] \) and the residual polynomial \( R_r(f) \) is defined for all \( f \in K[x] \).
Otherwise, if any situation involving a finite number of polynomials, we may always assume that the subgroup \( \Gamma_{-1} \) is sufficiently large to allow the application of the operator \( R_r \) to all the given polynomials.

5.2. Basic properties of the operator \( R_r \). The first basic properties of \( R_r \) follow immediately from the fact that \( c_0, c_d \neq 0 \).

Lemma 5.3. Let \( f \in K[x]_{\mu-\text{att}} \) be a non-zero polynomial. Then,

\[
\deg(R_r(f)) = (s_r(f) - s_r(f))/e_r \quad \text{and} \quad R_r(f)(0) \in \kappa_r^*.
\]

The essential property of the operator \( R_r \) is described in the next result.

Theorem 5.4. For any \( f \in K[x]_{\mu-\text{att}} \), we have

\[
H_\mu(f) = x_r^{s_r(f)} p_r^{u_r(f)} R_r(f)(y_r).
\]

Proof. Recall the notation \( s_0 = s_r(f), u_0 = u_r(f) \). Consider the set of indices

\[
J = \{ 0 \leq j \leq d \mid Q_{s_j} \text{ lies on } N_r(f) \} = \{ 0 \leq j \leq d \mid \mu(a_{s_j} \phi_r^s) = \mu(f) \}.
\]

All indices \( s \notin \{ s_j \mid j \in J \} \) have \( \mu(a_s \phi_r^s) > \mu(f) \). Hence,

\[
f \sim_\mu f_J, \quad \text{where} \quad f_J = \sum_{j \in J} a_{s_j} \phi_r^s.
\]

If \( f \in K[x]_{\mu-\text{att}} \), Lemma 5.3 shows that \( u_0 = \mu_{r-1}(a_{s_0}) \in \Gamma_{r-1} \). Thus,

\[
f_J = \phi_r^{s_0} \pi_r^{u_0} \sum_{j \in J} b_j Y_r \quad \text{and} \quad b_j = \pi_r^{j/h_r-u_0} a_{s_j} \in K(x),
\]

where \( \pi_r^{u_0}, Y_r = \phi_r^{e_r} \pi_r^{-h_r} \in K(x) \) are the rational functions introduced in section 3.3.

For all \( j \in J \), we have \( \mu_{r-1}(a_{s_j}) = u_0 - j h_r \). Therefore,

\[
H_\mu(b_j) = \pi_r^{j/h_r-u_0} H_\mu(a_{s_j}) = \pi_r^{-\mu_{r-1}(a_{s_j})} H_\mu(a_{s_j}) = c_j.
\]

Since \( f \sim_\mu f_J \), the result follows from the application of \( H_\mu \) to both sides of equation

\[
(26)
\]

having in mind equation \( (2) \).

Thus, the 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 \( R_r(f)(y_r) \in \Delta \).

We now derive from Theorem 5.4 some more basic properties of the operator \( R_r \).

Theorem 5.5. Consider the \( \kappa_r \)-algebra isomorphism \( \kappa_r[y] \simeq \Delta \) induced by \( y \mapsto y_r \). For each \( g \in K[x] \) having \( \mu(g) = 0 \), the inverse isomorphism assigns

\[
H_\mu(g) \mapsto y^{s_r(g)/e_r} R_r(g).
\]

Proof. Let \( g \in K[x] \) with \( \mu(g) = 0 \). By Lemma 3.19 applied to the pairs \( (s_r(g), u_r(g)) \) and \( (0, 0_r) \), there exists an integer \( j \geq 0 \) such that

\[
s_r(g) = j e_r, \quad \text{and} \quad x_r^{s_r(g)} p_r^{u_r(g)} = y_r^j.
\]

By Theorem 5.4 \( H_\mu(g) = y_r^j R_r(g)(y_r) \).

Corollary 5.6. Let \( f, g \in K[x]_{\mu-\text{att}} \). Then, \( R_r(fg) = R_r(f)R_r(g) \).

Proof. Since \( H_\mu(fg) = H_\mu(f)H_\mu(g) \) and \( p_r \) is a group homomorphism, the statement follows from Theorems 5.4 and 1.8 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 4.7.
Corollary 5.7. Let \( f, g \in K[x]_{\mu\text{-att}} \). Then,

\[
\begin{align*}
f \sim_{\mu} g & \iff s_r(f) = s_r(g), \; u_r(f) = u_r(g) \quad \text{and} \quad R_r(f) = R_r(g). \\
f \mid_{\mu} g & \iff s_r(f) \leq s_r(g) \quad \text{and} \quad R_r(f) \mid R_r(g) \quad \text{in} \quad \kappa_r[y].
\end{align*}
\]

Proof. If \( f \sim_{\mu} g \), then \( S_{\gamma_r}(f) = S_{\gamma_r}(g) \) by Lemma 4.6. In particular, these segments have the same left endpoint: \( (s_r(f), u_r(f)) = (s_r(g), u_r(g)) \). By Theorem 5.4, \( R_r(f)(y_r) = R_r(g)(y_r) \), and we deduce \( R_r(f) = R_r(g) \) from Theorem 1.8.

Conversely, the equalities \( (s_r(f), u_r(f)) = (s_r(g), u_r(g)) \) and \( R_r(f) = R_r(g) \) lead to \( H_{\mu_r}(f) = H_{\mu_r}(g) \) by Theorem 5.4.

The second equivalence follows from the analogous statement for the normalized operator \( \hat{R}_r \). \( \square \)

Corollary 5.8. Let \( f, g \in K[x]_{\mu\text{-att}} \) such that \( \mu(f) = \mu(g) \). Then,

\[
y^{[s_r(f)/e_r]} R_r(f) + y^{[s_r(g)/e_r]} R_r(g) = \begin{cases} 
y^{[s_r(f) + g]/e_r} R_r(f + g), & \text{if} \; \mu(f + g) = \mu(f), \\
0, & \text{if} \; \mu(f + g) > \mu(f).
\end{cases}
\]

Proof. If \( \mu(f + g) > \mu(f) \), we have \( f \sim_{\mu} -g \). By Corollary 5.7,

\[
R_r(f) = R_r(-g) = -R_r(g) \quad \text{and} \quad s_r(f) = s_r(-g) = s_r(g).
\]

Hence, \( y^{[s_r(f)/e_r]} R_r(f) + y^{[s_r(g)/e_r]} R_r(g) = 0 \).

Denote \( h = f + g \), and suppose that \( \mu(h) = \mu(f) = \mu(g) \). Then,

\[
\mu(f) = u_r(f) + s_r(f)\gamma_r = u_r(g) + s_r(g)\gamma_r = u_r(h) + s_r(h)\gamma_r.
\]

By Lemma 3.19, the following integer divisions have a common remainder \( 0 \leq \ell < e_r \):

\[
s_r(f) = j_f e_r + \ell, \quad s_r(g) = j_f e_r + \ell, \quad s_r(h) = j_h e_r + \ell.
\]

Take \( u = \mu(f) - \ell\gamma_r = u_r(f) + j_f h_r \in \Gamma_{-1} \). By Lemma 3.19,

\[
\begin{align*}
x_r^{s_r(f)} p_r^{u_r(f)} &= x_r^{\ell} p_r^u y_r^{j_f}, \\
x_r^{s_r(g)} p_r^{u_r(g)} &= x_r^{\ell} p_r^u y_r^{j_f}, \\
x_r^{s_r(h)} p_r^{u_r(h)} &= x_r^{\ell} p_r^u y_r^{j_h}.
\end{align*}
\]

On the other hand, the identity from (2) and Theorem 5.4 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 (27) and Theorem 1.8, this identity is equivalent to

\[
y^{j_f} R_r(f) + y^{j_h} R_r(g) = y^{j_h} R_r(h).
\]

This ends the proof, because \( j_f = \lfloor s_r(f)/e_r \rfloor, j_g = \lfloor s_r(g)/e_r \rfloor, j_h = \lfloor s_r(h)/e_r \rfloor \). \( \square \)

Residual polynomial of a constant. Take \( a \in K^* \) with \( \alpha := v(a) \in \Gamma_{-1} \). Clearly,

\[
S_{\gamma_r}(a) = N_r(a) = \{(0, \alpha)\}, \quad s_r(a) = s'_{\gamma_r}(a) = 0.
\]

By definition, \( R_r(a) = p_r^{-\alpha} H_{\mu_r}(a) \in \kappa_r^* \) is a constant. If \( r = 0 \), then \( R_0(a) = a/\pi_0^\alpha \in k^* \). If \( r > 0 \), we apply Proposition 3.10,

\[
\pi_r^\alpha = \pi_{r-1}^\alpha Y_{\Gamma_{r-1}}^{L_{\Gamma_{r-1}}(a)} \quad \Rightarrow \quad p_r^\alpha = p_{r-1}^\alpha z_{\gamma_{r-1}}^{L_{\Gamma_{r-1}}(a)},
\]

because \( z_{\gamma_{r-1}} \) is the image of \( y_{\gamma_{r-1}} = H_{\mu_{r-1}}(Y_{\Gamma_{r-1}}) \) under the homomorphism \( \mathcal{G}_{\mu_{r-1}} \to \mathcal{G} \).

By Proposition 1.10, \( H_0(a) \) is the image of \( H_{\mu_{r-1}}(a) \) under the same homomorphism. This leads to the following recurrence:

\[
R_r(a) = z_{\gamma_{r-1}}^{-L_{\Gamma_{r-1}}(a)} R_{r-1}(a) = \cdots = z_{\gamma_{r-1}}^{-L_{\Gamma_{r-1}}(a)} \cdots z_0^{-L_0(a)} R_0(a).
\]

In particular, if \( v(a) = 0 \), we have \( R_r(a) = R_0(a) = \overline{a} \in k^* \).

Lemma 5.9.
(1) If \( f \in K[x] \) is monic and \( \mu \)-minimal, then \( R_r(f) \) is a monic polynomial.
(2) \( R_r(\phi^s_r) = 1 \) for any integer \( s \geq 0 \).

**Proof.** If \( f \) is monic and \( \mu \)-minimal, then \( f \in K[x]_{\mu\text{-att}} \) by Lemma 5.1.

The leading monomial of the \( \phi_r \)-expansion of \( f \) is \( \phi_r^s(f) \) by [11] Prop. 3.7. Thus, for \( d = \deg(R_r(f)) \), we have \( a_d = 1 \) and \( c_d = \mu^{\mu^{\mu - 1}} H_\mu(1) = 1 \).

Finally, \( R_r(\phi_r) = 1 \) by definition. By Corollary 5.6, \( R_r(\phi^s_r) = R_r(\phi_r)^s = 1 \). \( \square \)

**Existence of polynomials with a prescribed residual polynomial.**

**Lemma 5.10.** Consider two polynomials \( \varphi, \psi \in \kappa_r[y] \) 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

\[
x^s_r p^u_r \varphi(y_r) = x^{s'}_r p^{u'}_r \psi(y_r).
\]

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 (28) implies

\[
s \gamma_r + u = \deg(x^s_r p^u_r) = \deg(x^{s'}_r p^{u'}_r) = s' \gamma_r + u'.
\]

Suppose \( s \leq s' \). By Lemma 3.19 there exists an integer \( j \geq 0 \) satisfying

\[
s' = s + j \epsilon_r, \quad u' = u - j \gamma_r, \quad x^{s'}_r p^{u'}_r = x^s_r p^u_r y_r^j.
\]

Hence, (28) implies \( \varphi(y_r) = y_r^j \psi(y_r) \). By Theorem 1.8, \( \varphi = y_r^j \psi \). Since neither \( \varphi \) nor \( \psi \) are divisible by \( y \), we have \( j = 0 \). This implies \( s' = s' \), \( u = u' \) and \( \varphi = \psi \). \( \square \)

**Proposition 5.11.** Let \((s, u) \in \mathbb{Z}_{\geq 0} \times \Gamma_r^{-1} \), and \( \psi \in \kappa_r[y] \) a polynomial with \( \psi(0) \neq 0 \). Then, there exists a polynomial \( f \in K[x]_{\mu\text{-att}} \) such that

\[
s_r(f) = s, \quad u_r(f) = u, \quad R_r(f) = \psi.
\]

**Proof.** Take \( f \in K[x] \) such that \( H_\mu(f) \) is the homogeneous element \( x_s^r p^u_r \psi(y_r) \in \mathcal{G} \). Since \( \mu(f) = u + s \gamma_r \in \Gamma_r \), this polynomial has attainable \( \mu \)-value. By Theorem 5.4, \( x^s_r p^u_r \psi(y_r) = H_\mu(f) = x^{s_r(f)} p^{u_r(f)} R_r(f)(y_r) \).

The result follows from Lemma 5.10. \( \square \)

5.3. **Characterization of key polynomials for \( \mu \).**

**Theorem 5.12.** A monic \( \phi \in K[x] \) is a key polynomial for \( \mu \) 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 \( \kappa_r[y] \).

In case (1), \( R_\mu(\phi) = y_r \Delta \). In case (2), \( R_r(\phi) \) is monic, \( R_\mu(\phi) = R_r(\phi)(y_r) \Delta \), and \( N_r(\phi) \) is one-sided of slope \(-\gamma_r \).

**Proof.** In case (2), \( \phi \) is \( \mu \)-minimal by [11] Prop. 3.7. Hence, \( R_r(\phi) \) is monic by Lemma 5.9. On the other hand, we prove below that \( N_r(\phi) \) is one-sided of slope \(-\gamma_r \). The rest of statements were proved in [11] Prop. 6.3 for the normalized residual polynomial \( \hat{R}_r(f) \). By equation (25), they hold for \( R_r(f) \) too.

Suppose that \( \phi \) satisfies (2). Since \( S_{\gamma_r}(\phi) \subset N_r(\phi) \), the equality \( N_r(\phi) = S_{\gamma_r}(\phi) \) will follow from the fact that the endpoints of both polygons have the same abscissas.

Both left endpoints have abscissa 0. Since \( \ell(N_r(\phi)) = \deg(\phi)/m_r = s' \gamma_r \), both right endpoints have the same abscissa too.

Since \( s' \gamma_r > 0 \), \( N_r(\phi) \) is one-sided of slope \(-\gamma_r \), according to Definition 4.2. \( \square \)
Consider $\phi_1, \ldots, \phi_r$ as key polynomials of $\mu_0, \ldots, \mu_{r-1}$, respectively. By the definition of a MacLane chain, all these key polynomials fall in the second case of Theorem 5.12.

**Corollary 5.13.** Consider an index $0 \leq i < r$.

1. The Newton polygon $N_i(\phi_{i+1})$ is one-sided of slope $-\gamma_i$.
2. The residual polynomial $R_i(\phi_{i+1})$ is the minimal polynomial of $z_i$ over $\kappa_i$.

In particular, $\text{deg}(R_i(\phi_{i+1})) = [\kappa_{i+1} : \kappa_i] = f_i$.

**Proof.** By Theorem 5.12, $N_i(\phi_{i+1})$ is one-sided of slope $-\gamma_i$, and $R_i(\phi_{i+1})$ is monic irreducible. By Theorem 5.4, $H_{\mu_i}(\phi_{i+1})$ is associate to $R_i(\phi_{i+1})(y_i)$ in the graded algebra $G_{\mu_i}$.

By Proposition 1.10, the homomorphism $\varphi: G_{\mu_i} \rightarrow G_{\mu_i+1}$ vanishes on both elements. Thus, $R_i(\phi_{i+1})(z_i) = 0$, because it is the image of $R_i(\phi_{i+1})(y_i)$ under this homomorphism. □

Finally, we may deduce from these results a well-known property of key polynomials for inductive valuations: they are defectless (see [16]).

**Corollary 5.14.** A key polynomial $\phi \in KP(\mu)$ satisfies $\text{deg}(\phi) = e(\phi)f(\phi)$.

In particular, the valuation $v_\phi$ is the unique extension of $v$ to the field $K_\phi$.

**Proof.** Consider a MacLane chain of $\mu$ as in (9). By Theorem 5.12 we have two possibilities for a key polynomial $\phi$ for $\mu$. Let us discuss separately each case.

If $\text{deg}(\phi) = \text{deg}(\phi_r)$ and $\phi \sim_\mu \phi_r$, then Propositions 1.6 and 1.7 show that

$$
\Gamma_{v_\phi} = \Gamma_{\mu, \text{deg}(\phi)} = \Gamma_{\mu, \text{deg}(\phi_r)} = \Gamma_{v_{\phi_r}}, \quad k_\phi \simeq k_{\phi_r}.
$$

Thus, $e(\phi) = e(\phi_r) = e_0 \cdots e_{r-1}$ and $f(\phi) = f(\phi_r) = f_0 \cdots f_{r-1}$, by (10) and (11).

On the other hand, Theorem 5.12 and Corollary 5.13 show that

$$
\text{deg}(\phi) = \text{deg}(\phi_r) = e_{r-1}f_{r-1}m_{r-1} = e_{r-1}f_{r-1} \cdots e_0 f_0 = e(\phi_r)f(\phi_r) = e(\phi)f(\phi).
$$

Finally, for any $\gamma \in Q$, $\gamma \geq \gamma_r$, consider the augmented valuation $\mu' = [\mu; \phi, \gamma]$. If $\phi \not\sim_\mu \phi_r$, we may extend our MacLane chain of $\mu$ to a MacLane chain of $\mu'$:

$$
\mu_{-\infty} \xrightarrow{\phi_0, \gamma_0} \mu_0 \xrightarrow{\phi_1, \gamma_1} \cdots \xrightarrow{\phi_{r-1}, \gamma_{r-1}} \mu_{r-1} \xrightarrow{\phi_r, \gamma_r} \mu_r \xrightarrow{\phi, \gamma} \mu'.
$$

Hence, $\text{deg}(\phi) = e(\phi)f(\phi)$ by the same argument we used for $\phi_r$. □

### 5.4 Recursive computation of the operator $R_r$

From an algorithmic perspective, Lemma 3.21 and Corollary 5.13 show how to build the tower [23] of residue fields with the irreducible polynomials $R_i(\phi_{i+1}) \in \kappa_i[x]$. The fields may be constructed as

$$
\kappa_{i+1} = \kappa_i[x]/(R_i(\phi_{i+1})),
$$

and we may identify the generator $z_i \in \kappa_{i+1}$ with the class of $x$ in this quotient.

On the other hand, the algorithmic computation of the operator $R_r$ is based on explicit formulas for the coefficients of the residual polynomials $R_r(f) \in \kappa_r[x]$, in terms of the previous operators $R_0, \ldots, R_{r-1}$.

**Definition 5.15.** For some $0 \leq i < r$, let $a \in K[x]_{\mu_{i+1}}$. We define $e_i(a) = (z_i)^{\ell_i} s_i(a) - L_i(u_i(a)) \in \kappa_{i+1}^*$, where $(s_i(a), u_i(a))$ is the left endpoint of $S_{\gamma_i}(a)$, the $\gamma_i$-component of $N_i(a)$.

**Theorem 5.16.** For $f = \sum_{0 \leq a} a_s \phi_s \in K[x]_{\mu_{i+1}}$, let $R_r(f) = c_0 + \cdots + c_d y^d \in \kappa_r[y]$. For each $j$ such that $c_j \neq 0$, denote $s_j = s_r(f) + j e_r$. Then,

$$
c_j = \begin{cases} 
a_s/\pi_0, & \text{if } r = 0, \\
e_r(a_s) R_{r-1}(a_s)(z_{r-1}), & \text{if } r > 0. 
\end{cases}
$$
Proof. If \( r = 0 \), the statement is based on the equality
\[
p_0^{-v(a)}H_{\mu_0}(a) = a/\pi_0^{v(a)}, \quad \forall a \in K^*,
\]
which is a consequence of the identification \( k = \kappa_0 \) established in section 3.1.

Suppose \( r > 0 \). It suffices to prove the equality
\[
(29) \quad p_r^{-\mu r-1}(a) H_\mu(a) = \epsilon_r-1(a) R_{r-1}(a)(z_{r-1}), \quad \forall a \in K[x] \text{ with } \deg(a) < m_r.
\]
Take a non-zero \( a \in K[x] \) with \( \deg(a) < m_r \). By Theorem 5.3
\[
(30) \quad H_{\mu r-1}(a) = x_{a-1}^r p_{r-1}^{u_{r-1}}(a) y_{r-1}, \quad s = s_{r-1}(a_{s_j}), \ u = u_{r-1}(a_{s_j}).
\]
Since \( \deg(a) < m_r = \deg(\phi_r) \), we have \( \mu_{r-1}(a) = \mu(a) \), so that \( H_\mu(a) \) 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 (30), we get
\[
H_\mu(a) = x_{a-1}^r p_{r-1}^{u_{r-1}}(a) (z_{r-1}).
\]
Hence, the claimed identity (29) is equivalent to:
\[
p_r^{-\mu r-1}(a) x_{a-1}^r p_{r-1}^{u_{r-1}} = \epsilon_r-1(a) = (z_{r-1})^{L_{r-1}} s^{-L_r-1}(u).
\]
Since \( \mu r_{r-1}(a) = u + s \gamma_{r-1} \), this identity follows from Proposition 3.17 by applying \( H_{\mu r-1} \)
to a similar identity between the corresponding rational functions.

This yields an algorithm to compute the operator \( R_r \).

Also, it is easy to deduce from Theorem 5.16 an algorithm to compute polynomials in \( K[x] \) with a prescribed residual polynomial, in the spirit of Proposition 5.11.

The latter algorithm may be used to construct key polynomials \( \phi \) such that \( R_r(\phi) \) is a prescribed monic irreducible polynomial in \( \kappa_r[y] \).

5.5. Dependence of \( R_r \) on the choice of \( \Gamma_{-1} \) and its basis. Let \( \Gamma'_{-1} \subset \Gamma \) be another finitely-generated subgroup satisfying the conditions of Definition 3.6 and let \( u'_{0,1}, \ldots, u'_{0,k'} \)
be a \( \mathbb{Z} \)-basis of \( \Gamma'_{-1} \). With respect to these choices, let
\[
y_{i}(p_{i})^\alpha \in \mathcal{G}_{\mu_{i}}, \quad 0 \leq i \leq r; \quad z_{i} \in \mathcal{G}_{\mu_{i+1}}, \quad 0 \leq i < r,
\]
be the corresponding elements described in Definitions 3.18 and 3.20.

Also, let \( R'_r \) be the corresponding residual polynomial operator.

There is a natural family of group homomorphisms:
\[
\tau_i: \Gamma_{i-1} \cap \Gamma'_{i-1} \longrightarrow \kappa^*_i, \quad \alpha \mapsto (p_{i})^\alpha/p_{i}^\alpha, \quad 0 \leq i \leq r.
\]
In fact, this quotient \( (p_{i})^\alpha/p_{i}^\alpha \) of two units belongs to \( \mathcal{G}_{\mu_{i}} \cap \Delta_i = \Delta_i^* = \kappa^*_i \).

Lemma 5.17.
\[
y_{i} = \tau_i(h_{i}) y_{i}, \quad 0 \leq i \leq r; \quad z_{i} = \tau_i(h_{i}) z_{i}, \quad 0 \leq i < r.
\]
Proof. By construction, \( h_{i} \in \Gamma_{i-1} \cap \Gamma'_{i-1} \). Then, from \( y_{i} = x_{i}^\epsilon_i (p_{i})^{-h_{i}}, \ y_{i} = x_{i}^\epsilon_i p_{i}^{-h_{i}}, \) we deduce \( y_{i} = \tau_i(h_{i}) y_{i}. \) The other identity follows from this one by applying the homomorphism \( \mathcal{G}_{\mu_{i}} \to \mathcal{G}_{\mu_{i+1}} \).

Theorem 5.18. Suppose that \( f \in K[x] \) has \( \mu(f) \in \Gamma^f_{\mu} \cup (\Gamma'_{\mu})^f \). Then,
\[
R_r(f)(y) = \xi R'_r(f)(\xi y), \quad \text{where} \quad \xi = \tau_r(u_r(f)), \quad \zeta = \tau_r(-h_r) \in \kappa^*_r.
\]
Proof. Let us denote for simplicity \( s = s_r(f) \), \( u = u_r(f) \). By Theorem 5.4
\[
x^s_r p^u_r R_r(f)(y_r) = H_\mu(f) = x^s_r (p^u_r)^{u_r} R'_r(f)(y'_r).
\]
By Lemma 5.17 this is equivalent to
\[
R_r(f)(y) = \tau_r(u) R'_r(f)(\tau_r(-h_r)y).
\]
By Theorem 5.8 \( R_r(f)(y) = \tau_r(u) R'_r(f)(\tau_r(-h_r)y) \). \( \square \)

5.6. **Dependence of \( R_r \) on the choice of an optimal MacLane chain.** In this section, we discuss the variation of the elements \( x_r, y_r, z_{r-1}, p^0_{r+1} \in \mathcal{G} \) and the operator \( R_r \), when we consider different optimal MacLane chains of \( \mu \).

By Proposition 3.4, two optimal MacLane chains of \( \mu \) have the same length \( r \), the same intermediate valuations \( \mu_0, \ldots, \mu_r \), and the same values \( \gamma_0, \ldots, \gamma_r \in \Gamma_Q \). They may differ only in the choice of the key polynomials, which must be related as follows:
\[
\phi^*_r = \phi_r + a_r, \quad \deg(a_r) < m_r, \quad \mu_r(a_r) \geq \gamma_r, \quad 0 \leq r \leq r.
\]
In particular, both chains support the same invariants \( m_r, e_r \in \mathbb{Z}_{>0}, h_r \in \Gamma_{r-1} \).

**Lemma 5.19.** If \( \phi^*_r \not\sim_\mu \phi_r \), then \( e_r = 1 \).

**Proof.** The condition \( \phi^*_r \not\sim_\mu \phi_r \) is equivalent to \( \mu(a_r) = \mu(\phi_r) = \gamma_r \). Since \( \mu(a_r) = \mu_{r-1}(a_r) \in \Gamma_{r-1} \), this leads to \( \gamma_r \in \Gamma_{r-1} \), which implies \( e_r = 1 \). \( \square \)

We mark with a superscript \( ( )^* \) all data and operators attached to the MacLane chain determined by the choice of the key polynomials \( \phi^*_0, \ldots, \phi^*_r \).

**Theorem 5.20.** With the above notation,
\begin{enumerate}
  \item The group homomorphisms \( p^*_i \) and \( p_i \) coincide for all \( 0 \leq i \leq r + 1 \).
  \item If \( \phi^*_r \sim_\mu \phi_r \), then \( x^*_r = x_r, \quad y^*_r = y_r, \quad R^*_r = R_r \).
  \item If \( \phi^*_r \not\sim_\mu \phi_r \), then \( x^*_r = x_r + p^*_r y_r, \quad y^*_r = y_r + \eta_r \), where \( \eta_r = R_r(a_r) \in \kappa^*_r \).
  Moreover, for a non-zero \( g \in K[x]_{\mu,\text{att}} \) we have
  \[
  y^{*(g)}(\eta^*_r) R_r(g)(y) = (y + \eta^*_r)^{*(g)} R^*_r(g)(y + \eta).
  \]
\end{enumerate}

**Proof.** Let us first prove by induction on \( r \) all statements concerning \( p^*_r, x^*_r \) and \( y^*_r \).

By Definition 3.18 \( p^*_0 = p_0 \), because the choice of \( \pi^*_0, \pi_0 \in \kappa^*_0 \) is independent of the MacLane chain. Suppose \( p^*_i = p_i \) for all \( 0 \leq i \leq r \).

If \( \phi^*_r \sim_\mu \phi_r \), then \( x^*_r = H_\mu(\phi^*_r) = H_\mu(\phi_r) = x_r \), leading to \( y^*_r = y_r \) and \( p^*_r = p_{r+1} \) for all \( j \), by Definitions 3.3 and 3.18. Hence, \( p^*_r = p_{r+1} \).

If \( \phi^*_r \not\sim_\mu \phi_r \), then \( e_r = 1 \) by Lemma 5.19 By (14), \( \ell_{r,j} = 0, \ell'_{r,j} = 1 \) for all \( j \). Thus,
\[
\pi^*_r = \pi^*_r, \quad \pi^*_{r+1,j} = \pi^*_{r+j}, \quad 1 \leq j \leq k,
\]
by Definition 3.3. Hence, \( v^*_r = v_r, v^*_{r+1} = v_r = v_{r+1} \).

Also, since \( \deg(a_r) < m_r \), we get
\[
s_r(a_r) = 0, \quad u_r(a_r) = \mu_{r-1}(a_r) = \mu(a_r) = \mu(\phi_r) = \gamma_r = h_r.
\]
Hence, \( a_r \) has an attainable \( \mu \)-value, and Theorem 5.4 shows that
\[
H_\mu(a_r) = p^*_r R_r(a_r) = p^*_r \eta.
\]
By using equation (2), we get in this case
\[
x^*_r = H_\mu(\phi^*_r) = H_\mu(\phi_r) + H_\mu(a_r) = x_r + p^*_r \eta,
\]
leading to \( y^*_r = x^*_r(p^*_r)^{-h_r} = x^*_r(p^*_r)^{-h_r} = x_r p^*_r \eta + y = y_r + \eta \).

Finally, let us prove the statements concerning \( R_r \).
Let \( g \in K[x] \) be a non-zero polynomial with attainable \( \mu \)-value.
Case $\phi_r^* \sim \mu_r$. Since $x_r^* = x_r$, $y_r^* = y_r$, and $p_r^* = p_r$, Theorem 5.4 shows that
\[ x_r^{s_r(g)} p_r^{u_r(g)} R_r(g)(y_r) = H_\mu(g) = x_r^{s_r(g)} p_r^{u_r(g)} R_r^*(g)(y_r). \]
By Lemma 5.10, $s_r^*(g) = s_r(g)$, $u_r^*(g) = u_r(g)$, and $R_r^*(g) = R_r(g)$.

Case $\phi_r^* \not\sim \mu_r$. Recall that $e_r = 1$ and $p_r^* = p_r$. By Theorem 5.4,
\[ x_r^{s_r(g)} p_r^{u_r(g)} R_r(g)(y_r) = H_\mu(g) = (x_r^{s_r^*(g)} p_r^{u_r^*(g)} R_r^*(g)(y_r)^*). \]
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 (31), as a consequence of Theorem 1.8.

References

[1] J. Fernández, J. Guàrdia, J. Montes, E. Nart, Residual ideals of MacLane valuations, J. Algebra 427 (2015), 30–75.
[2] J. Guàrdia, J. Montes, E. Nart, Okutsu invariants and Newton polygons, Acta Arith. 145 (2010), 83–108.
[3] 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.
[4] 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.
[5] J. Guàrdia, E. Nart, Genetics of polynomials over local fields, in Arithmetic, geometry, and coding theory, Contemp. Math. vol. 637 (2015), 207–241.
[6] F.J. Herrera Govantes, W. Mahboub, M.A. Olalla Acosta, M. Spivakovsky, Key polynomials for simple extensions of valued fields, preprint, arXiv:1406.0657v4 [math.AG], 2018.
[7] S. MacLane, A construction for absolute values in polynomial rings, Trans. Amer. Math. Soc. 40 (1936), pp. 363–395.
[8] S. MacLane, A construction for prime ideals as absolute values of an algebraic field, Duke Math. J. 2 (1936), pp. 492–510.
[9] J. Montes, Polignos de orden superior y aplicaciones aritméticas, Tesi doctoral, Universitat de Barcelona, 1999.
[10] N. Moraes de Oliveira, E. Nart, Defectless polynomials over henselian fields and inductive valuations, J. Algebra 541 (2020), 270–307.
[11] E. Nart, Key polynomials over valued fields, Publ. Mat. 64 (2020), 3–42.
[12] K. Okutsu, Construction of integral basis, I, II, Proceedings of the Japan Academy, Ser. A 58 (1982), 47–49, 87–89.
[13] O. Ore, Zur Theorie der algebraischen Körper, Acta Math. 44 (1923), pp. 219–314.
[14] O. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, Math. Annalen 99 (1928), 84–117.
[15] M. Vaquié, Extension d’une valuation, Trans. Amer. Math. Soc. 359 (2007), no. 7, 3439–3481.
[16] M. Vaquié, Famille admissible de valuations et défaut d’une extension, J. Algebra 311 (2007), no. 2, 859–876.
[17] M. Vaquié, Extensions de valuation et polygone de Newton, Ann. Inst. Fourier (Grenoble) 58 (2008), no. 7, 2503–2541.

Department de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalunya, Spain

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