DEFECTLESS POLYNOMIALS OVER HENSELIAN FIELDS AND INDUCTIVE VALUATIONS

NATHÁLIA MORAES DE OLIVEIRA AND ENRIC NART

Abstract. Let \((K, v)\) be a henselian valued field. Let \(\mathcal{P}^{\text{defless}} \subset K[x]\) be the set of monic, irreducible polynomials which are defectless and have degree greater than one. For a certain equivalence relation \(\approx\) on \(\mathcal{P}^{\text{defless}}\), we establish a canonical bijection \(\mathcal{M} \rightarrow \mathcal{P}^{\text{defless}} / \approx\), where \(\mathcal{M}\) is a discrete MacLane space, constructed in terms of inductive valuations on \(K[x]\) extending \(v\).

Introduction

Let \((K, v)\) be a valued field, with value group \(\Gamma = v(K^*)\). In a pioneering work, S. MacLane studied the extensions of the valuation \(v\) to the polynomial ring \(K[x]\) in one indeterminate, in the case \(v\) discrete of rank one \([9, 10]\).

Starting with any extension \(\mu_0\) on \(K[x]\), he considered inductive valuations \(\mu\), obtained after a finite number of augmentation steps:

\[
\mu_0 \xrightarrow{\phi_1; \gamma_1} \mu_1 \xrightarrow{\phi_2; \gamma_2} \cdots \xrightarrow{\phi_{r-1}; \gamma_{r-1}} \mu_{r-1} \xrightarrow{\phi_r; \gamma_r} \mu_r = \mu,
\]

involving the choice of certain key polynomials \(\phi_i \in K[x]\) and elements \(\gamma_i \in \Gamma \otimes \mathbb{Q}\).

MacLane proved that all extensions of \(v\) to \(K[x]\) can be obtained as a certain limit of inductive valuations. These ideas lead to an efficient algorithm for polynomial factorization over \(K_v[x]\), where \(K_v\) is the completion of \(K\) at \(v\).

This algorithm facilitates an efficient resolution of many arithmetic-geometric tasks in number fields and function fields of algebraic curves \([5]\).

M. Vaquié generalized MacLane’s theory to arbitrary valued fields \([15]\). The graded algebra \(G_\mu\) attached to a valuation \(\mu\) on \(K[x]\), and some ideal theory considerations in the degree-zero subring \(\Delta_\mu \subset G_\mu\), are crucial for the development of the theory.

Let \((K^h, v^h)\) be a henselization of \((K, v)\). In analogy with the discrete, rank-one case, MacLane-Vaquié’s theory should lead to the design of efficient polynomial factorization algorithms over \(K^h[x]\), which in turn could contribute to the computational resolution of arithmetic-geometric tasks in algebraic varieties of higher dimension.

For instance, F.J. Herrera, W. Mahboub, M.A. Olalla and M.Spivakovskiy use similar key polynomials as a tool to attack the local uniformization theorem for quasi-excellent noetherian schemes in positive and mixed characteristic \([6, 7]\).

In our approach, the underlying basic idea is to approximate a prime (monic, irreducible) polynomial \(F \in K^h[x]\) by adequate key polynomials of (not necessarily inductive) valuations \(\mu\) on \(K[x]\) such that \(\mu(F)\) is sufficiently large.

Key words and phrases. defectless polynomial, graded algebra of a valuation, henselian field, key polynomial, MacLane chain, Newton polygon, residual polynomial operator, inductive valuation.

Partially supported by grants MTM2016-75980-P from MEC, and 204224/2014-4 from CNPq.
If we restrict our attention to inductive valuations, their key polynomials can approximate only defectless prime polynomials of henselian valued fields, as shown by Vaquié in [16]. A prime polynomial \( F \in K^h[x] \) is defectless if \( \deg(F) = e(F)f(F) \), where \( e(F) \), \( f(F) \) are the ramification index and residual degree, respectively, of the extension of \( K^h \) obtained by adjoining a root of \( F \).

In this paper, we study constructive methods to produce approximations to defectless prime polynomials, by key polynomials for inductive valuations. To this end, we generalize to arbitrary henselian fields the results of [2], where only the discrete rank-one case was considered.

Let \( P_{\text{dless}} \subseteq K^h[x] \) be the subset of prime defectless polynomials of degree greater than one. We define an Okutsu equivalence relation \( \approx \) on \( P_{\text{dless}} \) as follows:

\[
F \approx G \iff \deg(F) = \deg(G), \quad v^h(\text{Res}(F,G)) > \deg(F)^2 w(F),
\]

for a certain bound \( w(F) \in \Gamma \otimes \mathbb{Q} \) defined in section [3].

If \( F, G \in P_{\text{dless}} \) are separable and Okutsu equivalent, they determine two extensions of \( K^h \) with isomorphic maximal tame subextensions (Theorem 5.16).

Our main result parameterizes the quotient set \( P_{\text{dless}}/\approx \) by a discrete MacLane space \( \mathbb{M} \), constructed in terms of inductive valuations (Theorem 5.14).

The space \( \mathbb{M} \) consists of pairs \((\mu, \mathcal{L})\), where \( \mu \) is an inductive valuation and \( \mathcal{L} \) is a (strong) maximal ideal of \( \Delta_\mu \). The maximal spectrum of \( \Delta_\mu \) is in canonical bijection with the set of \( \mu \)-equivalence classes of key polynomials for \( \mu \) [13]. Hence, we may assign to each pair \((\mu, \mathcal{L}) \in \mathbb{M} \) the \( \mu \)-equivalence class of key polynomials determined by \( \mathcal{L} \), which coincides with an Okutsu equivalence class in \( P_{\text{dless}} \).

All prime defectless polynomials in the class attached to \((\mu, \mathcal{L})\) share all discrete arithmetic invariants deduced from (optimal) MacLane chains of \( \mu \), as in [11].

These results, combined with the computational techniques of [11], yield an algorithm for polynomial factorization in \( K^h[x] \) of separable defectless polynomials in \( K[x] \); that is, separable polynomials all whose prime factors in \( K^h[x] \) are defectless.

For each prime factor \( F \in K^h[x] \), this algorithm computes an Okutsu equivalent approximation to \( F \) in \( K[x] \), together with all arithmetic invariants of \( F \) that can be read in an optimal MacLane chain of the inductive valuation \( \mu \) corresponding to \( F \) through the above mentioned bijection.

1. Valuations on polynomial rings and key polynomials

Throughout this paper, we fix a valued field \((K, v)\). Let

\[
\mathfrak{m} \subset \mathcal{O} \subset K, \quad k = \mathcal{O}/\mathfrak{m}
\]

be the maximal ideal, valuation ring and residue class field of the valuation \( v \).

Let \( \Gamma = v(K^* ) \) be the value group, and denote \( \mathbb{Q}\Gamma = \Gamma \otimes \mathbb{Q} \).

In this section, we review some basic facts on valuations on \( K[x] \), mainly extracted from [11], [13] and [15].

1.1. Graded algebra of a valuation on \( K[x] \) and key polynomials. Let \( \mu \) be a valuation on \( K[x] \) extending \( v \). It extends in an obvious way to a valuation on \( K(x) \).

Let \( \Gamma_\mu = \mu(K(x)^*) \) be the value group, and denote the maximal ideal, valuation ring and residue class field, by

\[
\mathfrak{m}_\mu \subset \mathcal{O}_\mu \subset K(x), \quad k_\mu = \mathcal{O}_\mu/\mathfrak{m}_\mu.
\]
For any $\alpha \in \Gamma_\mu$, consider the abelian groups:
\[ \mathcal{P}_\alpha = \{ g \in K[x] \mid \mu(g) \geq \alpha \} \supset \mathcal{P}_\alpha^+ = \{ g \in K[x] \mid \mu(g) > \alpha \}. \]

The graded algebra of $\mu$ over $K[x]$ is the integral domain:
\[ \mathcal{G}_\mu = \text{gr}_\mu(K[x]) = \bigoplus_{\alpha \in \Gamma_\mu} \mathcal{P}_\alpha/\mathcal{P}_\alpha^+. \]

There is a natural map $H_\mu : K[x] \rightarrow \mathcal{G}_\mu$, given by $H_\mu(0) = 0$ and
\[ H_\mu(g) = g + \mathcal{P}_{\mu(g)}^+ \in \mathcal{P}_{\mu(g)}/\mathcal{P}_{\mu(g)}^+, \quad \text{if } g \neq 0. \]

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

**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 $\mathcal{G}_\mu$.
We say that $g$ is $\mu$-irreducible if $H_\mu(g)\mathcal{G}_\mu$ is a non-zero prime ideal.
We say that $g$ is $\mu$-minimal if $g \mid_\mu f$ for all 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.** 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 $\text{KP}(\mu)$.
A key polynomial is necessarily irreducible in $K[x]$.

**Lemma 1.4.** Let $\phi \in \text{KP}(\mu)$, and let $f \in K[x]$ be a monic polynomial such that $\phi \mid_\mu f$ and $\deg(f) = \deg(\phi)$. Then, $\phi \sim_\mu f$ and $f$ is a key polynomial for $\mu$ too.

The weight of $\mu$ is the following upper bound $w(\mu) \in \mathbb{Q}\Gamma$ for weighted $\mu$-values.

**Theorem 1.5.** Let $\phi \in \text{KP}(\mu)$. For any monic non-constant $f \in K[x]$ we have
\[ \mu(f)/\deg(f) \leq w(\mu) := \mu(\phi)/\deg(\phi), \]
and equality holds if and only if $f$ is $\mu$-minimal.

Let $\Delta = \Delta_\mu = \mathcal{P}_0/\mathcal{P}_0^+ \subset \mathcal{G}_\mu$ be the subring of homogeneous elements of degree zero. There are canonical injective ring homomorphisms:
\[ k \hookrightarrow \Delta \hookrightarrow k_\mu. \]
The algebraic closure of $k$ in $\Delta$ is a subfield $\kappa = \kappa(\mu) \subset \Delta$ such that $\kappa^* = \Delta^*$.
Let $I(\Delta)$ be the set of ideals in $\Delta$, and consider the residual ideal operator:
\[ \mathcal{R} = \mathcal{R}_\mu : K[x] \rightarrow I(\Delta), \quad g \mapsto (H_\mu(g)\mathcal{G}_\mu) \cap \Delta. \]
This operator $\mathcal{R}$ translates questions about the action of $\mu$ on $K[x]$ into ideal-theoretic considerations in the $k$-algebra $\Delta$.

**Theorem 1.6.** If $\text{KP}(\mu) \neq \emptyset$, the residual ideal operator induces a bijection:

$$\mathcal{R}: \text{KP}(\mu)/\sim_\mu \longrightarrow \text{Max}(\Delta).$$

**Valuation attached to a key polynomial.** For any positive integer $m$ we denote:

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

**Proposition 1.7.** Take $\phi \in \text{KP}(\mu)$ and let $m = \deg(\phi)$. Consider the maximal ideal $p = \phi K[x]$, the field $K_\phi = K[x]/p$, and the onto mapping:

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

where $a_0 \in K[x]$ is the remainder of the division of $f$ by $\phi$. Then, $v_{\mu,\phi}$ is a valuation on $K_\phi$ extending $v$, with value group $\Gamma_{\mu,m}$. Moreover, $\Gamma_{\mu} = \langle \Gamma_{\mu,m}, \mu(\phi) \rangle$.

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

$$\mathfrak{m}_{\mu,\phi} \subset \mathcal{O}_{\mu,\phi} \subset K_{\phi}, \quad k_{\mu,\phi} = \mathcal{O}_{\mu,\phi}/\mathfrak{m}_{\mu,\phi}.$$

**Proposition 1.8.** If $\phi \in \text{KP}(\mu)$, then $\mathcal{R}(\phi)$ is the kernel of the onto homomorphism

$$\Delta \longrightarrow k_{\mu,\phi}, \quad g + \mathcal{P}_0^+ \longrightarrow (g + p) + \mathfrak{m}_{\mu,\phi}.$$

If $\phi$ has minimal degree in $\text{KP}(\mu)$, the mapping $\kappa \mapsto \Delta \rightarrow k_{\mu,\phi}$ is an isomorphism.

Thus, if $\text{KP}(\mu) \neq \emptyset$, we have $[\kappa : k] < \infty$. We define the residual degree of $\mu$ as

$$f(\mu) := [\kappa : k].$$

1.2. **Commensurable extensions.** The extension $\mu/v$ is commensurable if $\Gamma_{\mu}/\Gamma$ is a torsion group. In this case, there is a canonical embedding

$$\Gamma_{\mu} \hookrightarrow \mathbb{Q}\Gamma.$$

By composing $\mu$ with this embedding, we obtain a $\mathbb{Q}\Gamma$-valued valuation on $K[x]$. Conversely, any $\mathbb{Q}\Gamma$-valued extension of $v$ to $K[x]$ is commensurable over $v$.

Two commensurable extensions of $v$ are equivalent if and only if their corresponding $\mathbb{Q}\Gamma$-valued valuations coincide. Hence, we may identify the set of equivalence classes of commensurable valuations extending $v$ with the set

$$\mathcal{V} := \mathcal{V}(K,v) = \{\mu: K[x] \rightarrow \mathbb{Q}\Gamma \cup \{\infty\} \mid \mu \text{ valuation, } \mu|_K = v\}.$$

There is a natural partial ordering in the set of all mappings from $K[x]$ to any fixed ordered group:

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

In particular, $(\mathcal{V}, \leq)$ is a partially ordered set.

**Lemma 1.9.** Let $\mu$ be a valuation on $K[x]$ extending $v$. The following conditions are equivalent.

1. $\mu/v$ is commensurable and $\text{KP}(\mu) \neq \emptyset$.
2. $\mu$ is residually transcendental; that is, $k_{\mu}/k$ is a transcendental extension.
3. $\mu/v$ is commensurable and $\mu$ is not maximal in $(\mathcal{V}, \leq)$. 
Let us denote the set of equivalence classes of commensurable extensions of $v$ admitting key polynomials by

$$\mathcal{V}^\text{KP} = \mathcal{V}^\text{KP}(K, v) \subset \mathcal{V}.$$  

For $\mu \in \mathcal{V}^\text{kp}$, let $\phi_{\text{min}}$ be a key polynomial for $\mu$ of minimal degree $m$ in $\text{KP}(\mu)$. By Proposition [17, Prop. 1.7] $\Gamma_{\mu,m} = \Gamma_{\mu,\phi_{\text{min}}}$ and $\Gamma_{\mu}/\Gamma_{\mu,m}$ is a finite cyclic group generated by $\mu(\phi_{\text{min}})$. Thus, we may define the absolute and relative ramification indices of $\mu$ as

$$e(\mu) := (\Gamma_{\mu} : \Gamma) < \infty, \quad e_{\text{rel}}(\mu) := (\Gamma_{\mu} : \Gamma_{\mu,m}) < \infty.$$  

Let us describe the structure of the residue class field $k_\mu$. For all $a \in K[x]$ with $\deg(a) < m$ the homogeneous element $H_\mu(a)$ is a unit in $G_\mu$ [13, Prop. 3.5].

**Theorem 1.10.** For $\mu \in \mathcal{V}^\text{kp}$, take $\phi_{\text{min}} \in \text{KP}(\mu)$ of minimal degree $m$. Let $e = e_{\text{rel}}(\mu)$ and take $a \in K[x]$ with $\deg(a) < m$ such that $\mu(a) = -e\mu(\phi_{\text{min}})$. Denote

$$\epsilon = H_\mu(a) \in G_\mu^*, \quad \xi = H_\mu(\phi_{\text{min}})^e \epsilon \in \Delta.$$  

Then, $\xi$ 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 $\Delta \hookrightarrow k_\mu$.

1.3. Newton polygons. Let $\mu$ be a valuation in the space $\mathcal{V}^\text{kp}$.

The choice of a key polynomial $\phi$ for $\mu$ determines a Newton polygon operator

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

where $\mathcal{P}(\mathbb{Q} \times \mathbb{Q} \Gamma)$ 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 $f \in K[x]$ is nonzero and has a canonical $\phi$-expansion as in (3), then $N := N_{\mu,\phi}(f)$ is defined to be the lower convex hull of the finite cloud of points

$$C = \{Q_s \mid s \geq 0\}, \quad Q_s = (s, \mu(a_s)).$$  

Thus, $N$ is either a single point or a chain of segments, ordered from left to right by increasing slopes, called the sides of the polygon.

The abscissa of the left endpoint of $N$ is $\text{ord}_\phi(f)$ in $K[x]$.

The abscissa of the right endpoint of $N$ is called the length of $N$, and is denoted:

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

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

---

**Figure 1.** Newton polygon $N = N_{\mu,\phi}(f)$ of $f \in K[x]$
Definition 1.11. Let \( f \in K[x] \), \( N = N_{\mu, \phi}(f) \) and \( \lambda \in \mathbb{Q}\Gamma \).

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 \( s_{\lambda}(f) \leq s'_{\lambda}(f) \).

We say that \( N = N_{\mu, \phi}(f) \) is one-sided of slope \(-\lambda\) if

\[
N = S_{\lambda}(N), \quad s_{\lambda}(f) = 0, \quad s'_{\lambda}(f) > 0.
\]

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

Since \( \phi \) is \( \mu \)-minimal, Lemma 1.2 shows that

\[
\mu(f) = \min\{\mu(a_s s^s) \mid s \geq 0\} = \min\{\mu(a_s) + s\mu(\phi) \mid s \geq 0\}.
\]

Hence, \( \mu(f) \) is the ordinate of the point where the vertical axis meets the line of slope \(-\mu(\phi)\) containing the \( \mu(\phi) \)-component of \( N_{\mu, \phi}(f) \). (see Figure 3)

Definition 1.12. The principal Newton polygon \( N_{\mu, \phi}(f) \) is the polygon formed by the sides of \( N_{\mu, \phi}(f) \) of slope less than \(-\mu(\phi)\).

If \( N_{\mu, \phi}(f) \) has no sides of slope less than \(-\mu(\phi)\), then \( N_{\mu, \phi}(f) \) is defined to be the left endpoint of \( N_{\mu, \phi}(f) \).

Lemma 1.13. The integer \( \ell \left(N_{\mu, \phi}(f)\right) = s_{\mu(\phi)}(f) \) is the order with which the prime element \( H_\mu(\phi) \) divides \( H_\mu(f) \) in the graded algebra \( \mathcal{G}_\mu \).

There is a natural addition law for Newton polygons. Consider two polygons \( N, N' \) with sides \( S_1, \ldots, S_k; S'_1, \ldots, S'_{k'} \), respectively.

The left endpoint of the sum \( N + N' \) is the vector sum in \( \mathbb{Q} \times \mathbb{Q}\Gamma \) 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.

Theorem 1.14. For any non-zero \( g, h \in K[x] \) we have

\[
N_{\mu, \phi}(gh) = N_{\mu, \phi}(g) + N_{\mu, \phi}(h).
\]

1.4. Residual polynomial operator. For \( \mu \in V^k \), take \( \phi_{\min} \in K\mathcal{P}(\mu) \) of minimal degree \( m \). Denote \( e = e_{\text{crit}}(\mu) \) and \( \gamma = \mu(\phi_{\min}) \).

Let \( \epsilon \in \mathcal{G}_\mu^* \) be a unit of degree \(-e\gamma\). By Theorem 1.10 the element \( \xi = H_\mu(\phi_{\min})^e \epsilon \) is transcendental over \( \kappa \) and satisfies \( \Delta = \kappa[\xi] \).
The choice of the pair \( \phi_{\text{min}}, \epsilon \) determines a residual polynomial operator;

\[
R := R_{\mu, \phi_{\text{min}}, \epsilon} : K[x] \rightarrow \kappa[y],
\]

where \( y \) is another indeterminate. We agree that \( R(0) = 0 \).

For a non-zero \( f \in K[x] \) with \( \phi_{\text{min}} \)-expansion \( f = \sum_{s \leq \delta} a_s \phi_{\text{min}}^s \), let us denote

\[
S = S_\gamma(N_{\mu, \phi_{\text{min}}}(f)), \quad s(f) = s_\gamma(f), \quad s'(f) = s'_{\gamma}(f).
\]

**Definition 1.15.** The degree of \( S \) is the integer \( d = (s'(f) - s(f))/\epsilon \). Denote \( s_j = s_0 + j\epsilon, \quad r c_j(f) = H_\mu(a_{s_j})\epsilon^{-j} \in G_\mu^*, \quad 0 \leq j \leq d \).

These units \( r c_j(f) \) of degree \( \mu(a_{s_j}) + j\epsilon \) are called residual coefficients of \( f \).

For any point \( Q_s \in C \) as in (1), we have

\[
Q_s \in S \iff s = s_j, \quad \text{deg}(r c_j(f)) = \mu(f) - s_0 \gamma, \quad \text{for some } 0 \leq j \leq d.
\]

By construction, \( Q_{s_0} = Q_{s(f)} \) and \( Q_{s_d} = Q_{s'(f)} \) lie on \( S \), but for \( 0 < j < d \), the point \( Q_{s_j} \in C \) may lie strictly above \( S \). We define

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

with coefficients:

\[
\zeta_j = \begin{cases} 
    r c_j(f)/r c_d(f) \in \kappa^*, & \text{if } Q_{s_j} \text{ lies on } S, \\
    0, & \text{otherwise}.
\end{cases}
\]

Let us emphasize that \( \zeta_0 \) is always nonzero. In other words,

\[
y \nmid R(f), \quad \forall f \in K[x].
\]

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

**Theorem 1.16.** For \( \mu \in \mathbb{V}^{kp} \) and any \( f \in K[x] \),

\[
H_\mu(f) = r c_d(f)H_\mu(\phi_{\text{min}}^{s(f)})R(f)(\xi).
\]

**Corollary 1.17.** Let \( \mu \in \mathbb{V}^{kp} \) and \( f, g \in K[x] \). Then,

1. \( R(fg) = R(f)R(g) \).
2. \( f \sim_\mu g \iff r c_d(f) = r c_d(g), s(f) = s(g) \) and \( R(f) = R(g) \).

The (non-canonical) operator \( R \) is a down-to-earth representation of the canonical operator \( \mathcal{R} \), and it facilitates a characterization of key polynomials for \( \mu \).

\[
\mathcal{R}(f) = \xi^{[s(f)/\epsilon]} R(f)(\xi) \Delta, \quad \forall f \in K[x].
\]
Theorem 1.18. For \( \mu \in \mathbb{V}^{kp} \), take \( \phi_{\text{min}} \in KP(\mu) \) of minimal degree \( m \). A monic \( f \in K[x] \) is a key polynomial for \( \mu \) if and only if either

1. \( \deg(f) = m \) and \( f \sim_{\mu} \phi_{\text{min}} \), in which case \( R(\phi) = \xi \Delta \), or
2. \( \deg(f) = m \cdot \deg(R(f)) \) and \( R(f) \) is irreducible in \( \kappa[y] \), in which case \( R(\phi) = R(f)(\xi) \Delta \) and \( N_{\mu,\phi_{\text{min}}}(f) \) is one-sided of slope \( -\mu(\phi_{\text{min}}) \).

Corollary 1.19. For \( \mu \in \mathbb{V}^{kp} \), take \( \phi \in KP(\mu) \). Then, if \( \phi \sim_{\mu} \phi_{\text{min}} \), we have

\[
e(v_{\mu,\phi}/v) = e(\mu)/e_{\text{rel}}(\mu), \quad f(v_{\mu,\phi}/v) = f(\mu),
\]

whereas in the case \( \phi \not\sim_{\mu} \phi_{\text{min}} \), we get

\[
e(v_{\mu,\phi}/v) = e(\mu), \quad f(v_{\mu,\phi}/v) = f(\mu) \deg(R(\phi)).
\]

Proof. The statements in the case \( \phi \sim_{\mu} \phi_{\text{min}} \) follow from Propositions 1.7 and 1.8.

If \( \phi \not\sim_{\mu} \phi_{\text{min}} \), then \( e(v_{\mu,\phi}/v) = e(\mu) \) by [13, Cor. 6.4].

Also, \( R(\phi) = R(\phi)(\xi) \Delta \) by Theorem 1.18. Hence, the statement about \( f(v_{\mu,\phi}/v) \) follows from Proposition 1.8 and Theorem 1.10.

\[\kappa_{\mu,\phi} \cong \Delta/R(\phi) = \kappa[\xi]/(R(\phi)(\xi)) \cong \kappa[y]/(R(\phi)),\]

so that \( \kappa_{\mu,\phi} = \deg(R(\phi)) \). Also, \( \kappa: k = f(\mu) \) by definition.

Corollary 1.20. Let \( \phi, \phi' \in KP(\mu) \). The following conditions are equivalent, and they imply \( \deg(\phi) = \deg(\phi') \).

1. \( \phi \sim_{\mu} \phi' \).
2. \( \phi \rlap{\mid}_{\mu} \phi' \).
3. \( R(\phi) = R(\phi') \).
4. \( \kappa_{\mu,\phi} = \kappa_{\mu,\phi'} \)

2. Inductive valuations

Most of the results of this section are extracted from [11] and [13].

2.1. Augmentation of valuations. Let \( \mu \) be an extension of \( v \) to \( K[x] \) admitting key polynomials. Let \( \iota: \Gamma_{\mu} \to \Gamma' \) be an order-preserving embedding of \( \Gamma_{\mu} \) into another abelian ordered group.

Definition 2.1. Take \( \phi \in KP(\mu) \) and \( \gamma \in \Gamma' \) any element such that \( \mu(\phi) < \gamma \).

The augmented valuation \( \mu' = [\mu; \phi, \gamma] \) is defined as follows on \( \phi \)-expansions:

\[
\mu': K[x] \to \Gamma' \cup \{\infty\}, \quad \sum_{0 \leq s} a_s \phi^s \mapsto \min \{\mu(a_s) + s\gamma \mid 0 \leq s\}.
\]

There is a canonical homomorphism of graded algebras:

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

Proposition 2.2. Let \( \mu' = [\mu; \phi, \gamma] \), and let \( f \in K[x] \) be a non-zero polynomial.

(a) The valuation \( \mu' \) extends \( v \) and satisfies \( \mu(f) \leq \mu'(f) \).

Equality holds if and only if \( \phi \rlap{\mid}_{\mu} f \). In this case, \( H_{\mu'}(f) \) is a unit in \( G_{\mu'} \).

(b) The polynomial \( \phi \) is a key polynomial for \( \mu' \) of minimal degree, and

\[N_{\mu',\phi}(f) = N_{\mu,\phi}(f).\]
Definition 2.3. A key polynomial \( \phi \) for \( \mu \) is said to be proper if there exists some \( \phi_{\min} \in \text{KP}(\mu) \) of minimal degree such that \( \phi \not\sim_{\mu} \phi_{\min} \).

Lemma 2.4. Let \( \phi \) be a proper key polynomial for \( \mu \). Then,

1. \( \Gamma_{\mu, \phi} = \Gamma_{\mu, \deg(\phi)} = \Gamma_{\mu} \).
2. All augmentations \( \mu' = [\mu; \phi, \gamma] \) have \( \Gamma_{\mu'} = \langle \Gamma_{\mu}, \gamma \rangle \supset \Gamma_{\mu} \).

2.2. The minimal extension of \( v \) to \( K[x] \). Consider the ordered group \( (\mathbb{Z} \times \Gamma)_{\text{lex}} \) with the lexicographical order, and the following valuation on \( K[x] \):

\[
\mu_{-\infty} : K[x] \rightarrow (\mathbb{Z} \times \Gamma)_{\text{lex}} \cup \{ \infty \}, \quad f \mapsto (-\deg(f), v(\text{lc}(f)))
\]

where \( \text{lc}(f) \in K^* \) is the leading coefficient of a non-zero polynomial \( f \).

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

The set of key polynomials of \( \mu_{-\infty} \) is

\[
\text{KP}(\mu_{-\infty}) = \{ x + a \mid a \in K \},
\]

and all these key polynomials are \( \mu_{-\infty} \)-equivalent.

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

\[
\mathbb{Q} \Gamma \hookrightarrow (\mathbb{Z} \times \mathbb{Q} \Gamma)_{\text{lex}} , \quad \gamma \mapsto (0, \gamma).
\]

This embedding allows the comparison of all \( \mu \in V \) with \( \mu_{-\infty} \). Clearly,

\[
\mu_{-\infty} < \mu, \quad \forall \mu \in V.
\]

Consider augmentations of \( \mu_{-\infty} \) of the form:

\[
\mu_0(x + a, \gamma) := [\mu_{-\infty}; x + a, (0, \gamma)], \quad a \in K, \quad \gamma \in \mathbb{Q} \Gamma.
\]

By dropping the first (null) coordinate of all values of these valuations, we obtain equivalent valuations with values in \( \mathbb{Q} \Gamma \). We denote these valuations, which now belong to the space \( V \), with the same symbol \( \mu_0(x + a, \gamma) \). They act as follows:

\[
\mu_0(x + a, \gamma) : \sum_{0 \leq s} a_s(x + a)^s \mapsto \min \{ v(a_s) + s\gamma \mid 0 \leq s \},
\]

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

2.3. MacLane chains. A valuation \( \mu \) on \( K[x] \) is said to be \textit{inductive} if it is attained after a finite number of augmentation steps starting with the minimal valuation:

\[
(8) \quad \mu_{-\infty} \xrightarrow{\phi_0, \gamma_0} \mu_0 \xrightarrow{\phi_1, \gamma_1} \mu_1 \xrightarrow{\phi_2, \gamma_2} \cdots \xrightarrow{\phi_{r-1}, \gamma_{r-1}} \mu_{r-1} \xrightarrow{\phi_r, \gamma_r} \mu_r = \mu,
\]

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

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

We do not consider \( \mu_{-\infty} \) to be an inductive valuation; thus, inductive valuations belong to the space \( V^{\text{kp}} \). The integer \( r \geq 0 \) is the \textit{length} of the chain \( (8) \).

By Proposition 2.2 every \( \phi_i \) is a key polynomial for \( \mu_i \) of minimal degree. Hence, Theorem 1.5 shows that the sequence of weights \( w(\mu_i) \in \mathbb{Q} \Gamma \) grows strictly:

\[
w(\mu_i) = \mu_i(\phi_i) / \deg(\phi_i) \geq \mu_{i-1}(\phi_i) / \deg(\phi_i) = w(\mu_{i-1}).
\]

Since \( w(\mu_i) = \gamma_i / \deg(\phi_i) \), the sequence \( \gamma_0 < \cdots < \gamma_r \) grows strictly too.
Lemma 2.5. For a chain of augmentations as in (8), consider $f \in K[x]$ such that $\phi_i \nmid f$ for some $1 \leq i \leq r$. Then, $\mu_{i-1}(f) = \mu_i(f) = \cdots = \mu_r(f)$.

Since every $\phi_{i+1}$ is $\mu_i$-minimal, [13, Prop. 3.7] shows that
\[
1 = \deg(\phi_0) | \deg(\phi_1) | \cdots | \deg(\phi_{r-1}) | \deg(\phi_r).
\]

Definition 2.6. A MacLane chain is a chain of augmentations (8) such that
\[
\phi_i \nmid \phi_{i+1}, \quad 0 < i \leq r.
\]
In particular, $\phi_i$ is a proper key polynomial for $\mu_{i-1}$ (cf. Definition 2.5).

An optimal MacLane chain is a chain of augmentations (8) with
\[
1 = \deg(\phi_0) < \deg(\phi_1) < \cdots < \deg(\phi_r).
\]

Obviously, the truncation of a MacLane chain at the $i$-th node is a MacLane chain of the intermediate valuation $\mu_i$. By Lemma 2.5 in a MacLane chain, $\mu(\phi_i) = \mu_i(\phi_i) = \gamma_i, \quad 0 \leq i \leq r$.

All inductive valuations admit optimal MacLane chains. For these chains, there is a strong unicity statement.

Proposition 2.7. Consider an optimal MacLane chain as in (8) and another optimal MacLane chain
\[
\mu_{\infty} \xrightarrow{\phi_0^* \gamma_0^*} \mu_0^* \xrightarrow{\phi_1^* \gamma_1^*} \cdots \xrightarrow{\phi_r^* \gamma_r^*} \mu_r^* = \mu^*.
\]
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 (8), the intermediate valuations $\mu_0, \ldots, \mu_{r-1}$, the slopes $\gamma_0, \ldots, \gamma_r \in Q \Gamma$ and the positive integers $\deg(\phi_0), \ldots, \deg(\phi_r)$, are intrinsic data of $\mu$.

Definition 2.8. The MacLane depth of an inductive valuation $\mu$ is the length $r$ of any optimal MacLane chain of $\mu$.

A key polynomial $\phi$ for an inductive valuation $\mu$ is defectless [16, [11, Cor. 5.14]:
\[
\deg(\phi) = e(v_{\mu,\phi}/v)f(v_{\mu,\phi}/v).
\]

In particular, the valuation $v_{\mu,\phi}$ is the unique extension of $v$ to the field $K_\phi$. Therefore, whenever we deal with a key polynomial $\phi$ for an inductive valuation $\mu$, we shall use the following simplified notation:
\[
v_\phi = v_{\mu,\phi}, \quad k_\phi = k_{\mu,\phi}, \quad e(\phi) = e(v_{\mu,\phi}/v), \quad f(\phi) = f(v_{\mu,\phi}/v).
\]

Take an optimal MacLane chain of $\mu$ as in (8), and denote $\mu_{-1} = v, \kappa_{-1} = k$.

By Lemma 2.4 the value groups of the intermediate valuations form a chain:
\[
\Gamma_{v_{\phi_i}} = \Gamma_{\mu_{i-1}, \deg(\phi_i)} = \Gamma_{\mu_{i-1}} \subset \Gamma_{\mu_i} = \langle \Gamma_{\mu_{i-1}}, \gamma_i \rangle, \quad 0 \leq i \leq r.
\]
Thus, every quotient $\Gamma_{\mu_i}/\Gamma_{\mu_{i-1}}$ is a finite cyclic group generated by $\gamma_i$.

The relative ramification indices are intrinsic invariants of $\mu$:
\[
e_i := (\Gamma_{\mu_i} : \Gamma_{\mu_{i-1}}) = e_{\text{rel}}(\mu_i), \quad 0 \leq i \leq r.
\]
Also, the canonical homomorphisms $G_{\mu - 1} \rightarrow G_\mu$ induce a tower of fields

$$\kappa_0 = \text{Im}(k \rightarrow \Delta_{\mu_0}) \rightarrow \cdots \rightarrow \kappa_i = \text{Im}(\Delta_{\mu_{i-1}} \rightarrow \Delta_{\mu_i}) \rightarrow \cdots \rightarrow \kappa_r.$$ 

By Propositions 2.2 and 1.8, $\kappa_i = \kappa(\mu_i) \simeq k_{\phi_i}$ for all $0 \leq i \leq r$.

Let $R_i = R_{\mu_i, \phi_i, e_i}$ be the residual polynomial operators, determined by adequate units $e_i \in G_{\mu_i}^\ast$ of degree $-e_i(\mu_i(\phi_i))$.

The relative residual degrees are intrinsic invariants of $\mu$ too:

$$f_{i-1} := [\kappa_i : \kappa_{i-1}] = \text{deg}(R_{i-1}(\phi_i)), \quad 0 < i \leq r,$$

the last equality by Corollary 1.19.

Corollary 1.19 provides as well a computation of the ramification index and residual degree of any $\phi \in KP(\mu)$ such that $\phi \sim_{\mu} \phi_r$:

$$e(\phi) = e(\mu) = e_0 \cdots e_r, \quad f(\phi) = f(\mu) \text{deg}(R_r(\phi)) = f_0 \cdots f_{r-1} \text{deg}(R_r(\phi)).$$

3. Proper Key Polynomials and Types

### 3.1. Proper key polynomials

Let $\mu$ be an extension of $v$ to $K[x]$ with $KP(\mu) \neq \emptyset$.

A key polynomial $\phi$ for $\mu$ is proper if there exists a key polynomial for $\mu$, of minimal degree, which is not $\mu$-equivalent to $\phi$ (Definition 2.3).

By Corollary 1.20, properness is a property of $\mu$-equivalence classes of key polynomials for $\mu$.

If $\mu/v$ is an incommensurable extension, then there is only one $\mu$-equivalence class of key polynomials [13, Thm. 5.3]. Hence, this single class is improper.

In this section, we study properness of key polynomials for valuations $\mu \in \mathcal{V}^{kp}$.

By Theorem 1.6, the set $KP(\mu)/\sim_{\mu}$ is in canonical bijection with $\text{Max}(\Delta)$. Hence, it makes sense to talk about proper maximal ideals in $\Delta$.

Let us fix some notation.

- $\phi_{\text{min}}$ key polynomial for $\mu$ of minimal degree $m$ in the set $KP(\mu)$.
- $e = e_{\text{rel}}(\mu) = (\Gamma_{\mu} : \Gamma_{\mu,m})$ relative ramification index of $\mu$.
- $R = R_{\mu, \phi_{\text{min}}, e}$ residual polynomial operator, for $e \in G_\mu^\ast$ of degree $-e\mu(\phi_{\text{min}})$.
- $\xi = H_{\mu}(\phi_{\text{min}})^e \in \Delta$.
- $[\phi] = [\phi]_\mu$ $\mu$-equivalence class of $\phi$ in the set $KP(\mu)$.
- $s_{\mu, \phi}(f)$ order with which $H_\mu(\phi)$ divides $H_\mu(f)$ in $G_\mu$, for all $f \in K[x]$.
- $s(f) = s_{\mu, \phi_{\text{min}}}(f)$ notation coherent with that of (5), by Lemma 1.13.

Theorem 1.18 shows that all key polynomials for $\mu$ have degree multiple of $m$:

$$\text{deg}(\phi) = \begin{cases} m, & \text{if } \phi \in [\phi_{\text{min}}], \\ em \text{deg}(R(\phi)), & \text{if } \phi \not\in [\phi_{\text{min}}]. \end{cases}$$ (9)

Let us show that properness of a key polynomial is determined by its degree.

**Lemma 3.1.** A key polynomial $\phi \in KP(\mu)$ is proper if and only if $em \mid \text{deg}(\phi)$.

**Proof.** If $\phi$ is proper, then $em \mid \text{deg}(\phi)$ by (9).

 Conversely, suppose that $em \mid \text{deg}(\phi)$. If $e > 1$, then (9) shows that $\phi \not\in [\phi_{\text{min}}]$.

If $e = 1$, then $\Gamma_{\mu} = \Gamma_{\mu,m}$, and there exists $a \in K[x]$ with $\text{deg}(a) < m$ such that $\mu(a) = \mu(\phi_{\text{min}})$. The polynomial $\phi' = \phi_{\text{min}} + a$ has $R(\phi') = y + H_{\mu}(a)e \in k[y]$.

By Theorem 1.18, $\phi'$ is another key polynomial of minimal degree, and $[\phi'] \neq [\phi_{\text{min}}]$. Hence, either $\phi \not\in [\phi']$ or $\phi \not\in [\phi_{\text{min}}]$. \qed
Corollary 3.2.

(1) If \( e = 1 \), all key polynomials for \( \mu \) are proper.
(2) If \( e > 1 \), then \( \lfloor \phi_{\min} \rfloor \) is the only improper class.

This class coincides with the set of all key polynomials of degree \( m \).

Definition 3.3. We say that \( f \in K[x] \) is \( \mu \)-proper if either \( f = 0 \), or \( \phi \mid f \) for all improper \( \phi \in \text{KP}(\mu) \).

The next result is an immediate consequence of Corollary 3.2.

Corollary 3.4. If \( e = 1 \), all polynomials are \( \mu \)-proper.
If \( e > 1 \), then \( f \in K[x] \) is \( \mu \)-improper if and only if \( 0 < s(f) < \infty \).

Lemma 3.5. If at least one of the polynomials \( g, h \in K[x] \) is \( \mu \)-proper, then
\[
\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h).
\]

Proof. By Theorem 1.10 and (7), \( \mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h) \) is equivalent to:
\[
y^{s(gh)/e}R(gh) = y^{s(g)/e}R(g)y^{s(h)/e}R(h).
\]
Since \( s(gh) = s(g) + s(h) \) and \( R(gh) = R(g)R(h) \) (Corollary 1.17), this amounts to
\[
\lceil (s(g) + s(h))/e \rceil = \lceil s(g)/e \rceil + \lceil s(h)/e \rceil.
\]
If \( e = 1 \) this equality is obvious. If \( e > 1 \) it holds too, because either \( s(g) = 0 \) or \( s(h) = 0 \), by Corollary 3.3.

Proposition 3.6. Let \( \phi \in \text{KP}(\mu) \) and \( L = \mathcal{R}(\phi) \in \text{Max}(\Delta) \). For any \( f \in K[x] \):
\[
\text{ord}_{\mathcal{L}}(\mathcal{R}(f)) = \begin{cases} 
s_{\mu,\phi}(f), & \text{if } \mathcal{L} \text{ is proper}, \\ \lceil s_{\mu,\phi}(f)/e \rceil, & \text{if } \mathcal{L} \text{ is improper}. \\
\end{cases}
\]
where \( \text{ord}_{\mathcal{L}}(\mathcal{R}(f)) \) is the largest non-negative integer \( n \) such that \( \mathcal{L}^n \mid \mathcal{R}(f) \) in \( \Delta \).

Proof. Let \( \mathcal{P} \) be a set of representatives of key polynomials under \( \mu \)-equivalence. For any non-zero \( f \in K[x] \), there is a unique factorization:
\[
f \sim_{\mu} \prod_{\phi \in \mathcal{P}} \phi^{\alpha_{\phi}}, \quad a_{\phi} = s_{\mu,\phi}(f), \quad \forall \phi \in \mathcal{P},
\]
up to units in \( G_{\mu} [13, \text{Thm. 6.8}] \).

If we apply \( \mathcal{R} \) to both terms of this factorization, Lemma 3.5 shows that:
\[
\mathcal{R}(f) = \mathcal{R} \left( \prod_{\phi \in \mathcal{P}} \phi^{\alpha_{\phi}} \right) = \prod_{\phi \in \mathcal{P}} \mathcal{R}(\phi^{\alpha_{\phi}}).
\]
For all proper \( \phi \in \mathcal{P} \) we have \( \mathcal{R}(\phi^{\alpha_{\phi}}) = \mathcal{R}(\phi)^{\alpha_{\phi}} \) by Lemma 3.5. Thus, \( \mathcal{R}(\phi) \) divides \( \mathcal{R}(f) \) with exponent \( a_{\phi} \).

If \( e > 1 \), the unique improper \( \phi \in \mathcal{P} \) satisfies \( [\phi] = [\phi_{\min}] \). By Corollary 1.20 \( R(\phi) = R(\phi_{\min}) = 1 \). Hence, (7) implies
\[
\mathcal{R}(\phi) = \xi \Delta, \quad \mathcal{R}(\phi^{a_{\phi}}) = \xi^{[a_{\phi}/e]} \Delta = \mathcal{R}(\phi)^{[a_{\phi}/e]},
\]
so that \( \mathcal{R}(\phi) \) divides \( \mathcal{R}(f) \) with exponent \( [a_{\phi}/e] \).

\[\square\]
Corollary 3.7. Let $\phi \in \text{KP}(\mu)$ such that $\phi \not\sim^*_\mu \phi_{\min}$. Then, $R(\phi) \in \kappa[y]$ is a monic irreducible polynomial, and

$$\text{ord}_{R(\phi)}(R(f)) = s_{\mu,\phi}(f), \quad \forall f \in K[x].$$

Proof. Denote $\psi = R(\phi)$ and $L = R(\phi) \in \text{Max(}\Delta).$ By Theorem 1.18 and (6), $\psi$ is monic irreducible, $\psi \neq y$, and $L = \psi(\xi)\Delta$. By (7),

$$\mathcal{R}(f) = \xi^{[s(f)/e]} R(f)(\xi)\Delta.$$ 

Since $\psi \neq y$ and $\phi$ is proper, we get $\text{ord}_\psi(R(f)) = \text{ord}_L(R(f)) = s_{\mu,\phi}(f)$, by Theorem 1.10 and Proposition 3.6.

3.2. Valuations bounded by semivaluations.

Lemma 3.8. [15] Thm. 1.15] Let $\mu, \mu^*$ be a valuation and a semivaluation, respectively, which extend $v$ to $K[x]$, and take values into a common ordered group.

Suppose that $\mu < \mu^*$, and let $\phi \in K[x]$ be a monic polynomial with minimal degree satisfying $\mu(\phi) < \mu^*(\phi)$. Then, $\phi$ is a key polynomial for $\mu$ and

$$\mu < [\mu; \phi, \gamma] \leq \mu^*, \quad \text{for } \gamma = \mu^*(\phi).$$

Moreover, for any $f \in K[x]$, the equality $\mu(f) = \mu^*(f)$ holds if and only if $\phi \equiv^*_\mu f$.

Actually, the subset $\Phi_{\mu,\mu^*} \subset \text{KP}(\mu)$ of monic polynomials of minimal degree satisfying $\mu(\phi) < \mu^*(\phi)$ is a $\mu$-equivalence class of key polynomials.

In fact, for any $\phi \in \Phi_{\mu,\mu^*}$, $\phi' \in \text{KP}(\mu)$, Lemma 3.8 and Corollary 1.20 show that

$$\phi' \in \Phi_{\mu,\mu^*} \iff \phi \equiv^*_\mu \phi' \iff \phi' \sim^*_\mu \phi.$$

Theorem 3.9. Let $\mu^*$ be a $\mathbb{Q}[\Gamma]$-valued semivaluation on $K[x]$. Then, the interval $(\mu_{-\infty}, \mu^*) \subset \mathbb{V}$ is totally ordered.

Proof. Let $\eta, \eta' \in \mathbb{V}$ such that $\eta < \mu^*, \eta' < \mu^*$. Take $\phi \in \Phi_{\eta,\mu^*}, \phi' \in \Phi_{\eta',\mu^*}$.

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

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

Hence, $\eta' > \eta$, because for any $g \in K[x]$ with $\phi$-expansion $g = \sum_{0 \leq s} a_s \phi^s$, we have:

$$\eta'(g) = \text{Min}_{0 \leq s} \{\eta'(a_s \phi^s)\} \geq \text{Min}_{0 \leq s} \{\eta(a_s \phi^s)\} = \eta(g).$$

Now, suppose $\deg(\phi) = \deg(\phi')$. Then, $\phi = \phi' + a$ for some $a \in K[x]$ with $\deg(a) < \deg(\phi)$. By the $\eta'$-minimality of $\phi'$ we have $\eta'(\phi) \leq \eta'(\phi')$.

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

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

Hence, $\phi \in \Phi_{\eta',\mu^*}$, and this implies $\phi' \sim^*_{\eta'} \phi$ by the remarks preceding this theorem. Thus, $\eta'(\phi) = \eta'(\phi') \leq \eta(\phi)$, and for any $\phi$-expansion $g = \sum_{0 \leq s} a_s \phi^s \in K[x]$, we get

$$\eta(g) = \text{Min}_{0 \leq s} \{\eta(a_s \phi^s)\} \geq \text{Min}_{0 \leq s} \{\eta'(a_s \phi^s)\} = \eta'(g).$$

Therefore, $\eta' \leq \eta$. 

3.3. Semivaluations attached to prime polynomials over henselian fields.

From now on, we assume that the valued field $(K, v)$ is henselian.

We still denote by $v$ its unique extension to a fixed algebraic closure $\overline{K}$ of $K$.

Let $\mathbb{P} = \mathbb{P}(K)$ be the set of all prime (monic, irreducible) polynomials in $K[x]$.

For any $F \in \mathbb{P}$ we denote
- $K_F = K[x]/(FK[x])$ finite extension of $K$ determined by $F$.
- $\mathcal{O}_F \supseteq m_F$ valuation ring and maximal ideal of $v$ over $K_F$.
- $k_F = \mathcal{O}_F/m_F$ residue field.
- $e(F), f(F)$ ramification index and residual degree of $K_F/K$.
- $d(F) = \deg(F)/e(F)\cdot f(F)$ defect of $F$.
- $Z(F)$ multiset of roots of $F$ in $\overline{K}$, counting multiplicities if $F$ is inseparable.

Let us consider the semivaluation:

$$v_F : K[x] \rightarrow K_F \stackrel{v}{\rightarrow} \mathbb{Q} \cap \{\infty\},$$

with support $v_F^{-1}(\infty) = FK[x]$. By the henselian property,

$$v_F(f) = v(f(\theta)), \quad \forall f \in K[x], \forall \theta \in Z(f).$$

**Lemma 3.10.** For all $F, G \in \mathbb{P}$, we have $v_G(F)/\deg(F) = v_F(G)/\deg(G)$.

**Proof.** The lemma follows from

$$\text{Res}(F, G) = \prod_{\theta \in Z(F)} G(\theta) = \pm \prod_{\alpha \in Z(G)} F(\alpha),$$

since $v(G(\theta)), v(F(\alpha))$ are constant for $\theta \in Z(F), \alpha \in Z(G)$, respectively. \qed

Let $\mu$ be a valuation on $K[x]$ admitting a key polynomial $\phi \in K[x]$.

In section 1.1 we attached to $\phi$ a valuation $v_{\mu, \phi}$ on the field $K_\phi$. By the unicity of $v$, we must have $v_{\mu, \phi} = v$. Hence, the semivaluation on $K[x]$ induced by $v_{\mu, \phi}$ coincides
with the semivaluation $v_{\phi}$ determined by the prime polynomial $\phi \in \mathbb{P}$.

More precisely, for any $f \in K[x]$ with $\phi$-expansion $f = \sum_{0 \leq s} a_s \phi^s$,

$$v_{\phi}(f) = v_{\mu, \phi}(f + \phi K[x]) = \mu(a_0).$$

By Lemma 1.2, $\mu < v_{\phi}$, regardless of the way we embedd $\Gamma_\mu$ into some group containing $\mathbb{Q} \Gamma$. By Lemma 3.8 for any non-zero $f \in K[x]$ we have

$$\mu(f) = v_{\phi}(f) \iff \phi \mid_\mu f.$$  

(10)

3.4. Types over henselian fields. In this section, we introduce types and we generalize the results of [12] to henselian valued fields of arbitrary rank.

A type is a pair $t = (\mu, \mathcal{L})$ belonging to the set

$$\mathbb{T} = \{(\mu, \mathcal{L}) \mid \mu \in \mathcal{Y}_K, \mathcal{L} \in \text{Max}(\Delta_\mu), \mathcal{L} \text{ proper}\}.\]$$

A type encodes a certain set of prime polynomials. A representative of the type $t = (\mu, \mathcal{L})$ is a prime polynomial in the set

$$\text{Rep}(t) = \{\phi \in \text{KP}(\mu) \mid \mathcal{R}_\mu(\phi) = \mathcal{L}\} \subset \mathbb{P}.$$

By Theorem 1.6, $\text{Rep}(t)$ is a proper equivalence class of key polynomials for $\mu$.

Any type $t \in \mathbb{T}$ determines a mapping

$$\text{ord}_t : K[x] \rightarrow \mathbb{N}, \quad f \mapsto \text{ord}_\mathcal{L}(\mathcal{R}_\mu(f)) = s_{\mu, \phi}(f), \forall \phi \in \text{Rep}(t).$$

The last equality is a consequence of Proposition 3.6.
Lemma 3.11. Suppose that \((K, v)\) is henselian, and let \(\mu, \mu'\) be two valuations admitting a common key polynomial \(\phi \in \text{KP}(\mu) \cap \text{KP}(\mu')\). Suppose that the value groups of \(\mu, \mu'\) have been embedded into some common ordered group. Then,

\begin{align*}
(1) \quad & \mu(\phi) = \mu'(\phi) \implies \mu = \mu', \\
(2) \quad & \mu(\phi) < \mu'(\phi) \implies \mu' = [\mu; \phi, \gamma], \text{ with } \gamma = \mu'(\phi).
\end{align*}

Proof. Since \(\mu, \mu' < v_{\phi}\), Theorem 3.9 shows that \(\mu \leq \mu'\), after eventually exchanging the valuations. Moreover, (10) shows that

\[\mu(a) = \mu'(a), \quad \forall a \in K[x] \text{ with } \text{deg}(a) < \text{deg}(\phi).\]

If \(\mu(\phi) = \mu'(\phi)\), then \(\mu = \mu'\) because they coincide on \(\phi\)-expansions.

If \(\mu(\phi) < \mu'(\phi)\), denote \(\mu_* = [\mu; \phi, \mu'(\phi)]\). Then, \(\phi\) is a common key polynomial for \(\mu'\) and \(\mu_*\). Since \(\mu'(\phi) = \mu_*(\phi)\), item (1) shows that \(\mu' = \mu_*\). \(\square\)

Theorem 3.12. Suppose that \((K, v)\) is henselian. For all \(t, t^* \in \mathbb{T}\) the following conditions are equivalent.

\begin{align*}
(1) \quad & t = t^*, \\
(2) \quad & \text{ord}_t = \text{ord}_{t^*}. \\
(3) \quad & \text{Rep}(t) = \text{Rep}(t^*). 
\end{align*}

Proof. It is obvious that (1) implies (2). Let \(t = (\mu, \mathcal{L}), \ t^* = (\mu^*, \mathcal{L}^*)\).

Let us show that (2) implies (3). Suppose that \(\text{ord}_t = \text{ord}_t^*\). Take \(\phi \in \text{Rep}(t)\), \(\phi^* \in \text{Rep}(t^*)\). By Proposition 3.6

\[1 = \text{ord}_t(\mathcal{R}_\mu(\phi)) = \text{ord}_{t^*}(\mathcal{R}_{\mu^*}(\phi)) = s_{\mu^*, \phi^*}(\phi).\]

Thus, \(\phi^* \mid_{\mu^*} \phi\). Since \(\phi^*\) is \(\mu^*\)-minimal, we have \(\text{deg}(\phi) \geq \text{deg}(\phi^*)\). The symmetry of the argument implies \(\text{deg}(\phi^*) = \text{deg}(\phi)\).

By Lemma 3.14 \(\phi\) is a key polynomial for \(\mu^*\), and \(\phi^* \sim_{\mu^*} \phi\). Therefore,

\[\mathcal{R}_{\mu^*}(\phi) = \mathcal{R}_{\mu^*}(\phi^*) = \mathcal{L}^*,\]

so that \(\phi\) is a representative of \(t^*\). This shows that \(\text{Rep}(t) \subseteq \text{Rep}(t^*)\).

By the symmetry of the argument, equality holds.

Finally, let us prove that (3) implies (1). Take any \(\phi \in \text{Rep}(t) = \text{Rep}(t^*)\).

We need only to show that \(\mu = \mu^*\), because then \(\mathcal{L} = \mathcal{R}_{\mu}(\phi) = \mathcal{R}_{\mu^*}(\phi) = \mathcal{L}^*\).

Let us show that the assumption \(\mu \neq \mu^*\) leads to a contradiction. By Lemma 3.11 after eventually exchanging the valuations, this assumption leads to

\[\mu^* = [\mu; \phi, \gamma], \quad \gamma = \mu^*(\phi) > \mu(\phi).\]

By Proposition 2.2 \(\phi\) is a key polynomial for \(\mu^*\) of minimal degree.

Since \(\mathcal{L}^*\) is proper, Corollary 3.2 shows that \(e_{rel}(\mu^*) = 1\), and this implies

\[\gamma = \mu^*(\phi) \in \Gamma_{\mu^*, \text{deg}(\phi)} = \Gamma_{\mu, \text{deg}(\phi)} = \Gamma_{\mu},\]

the last equalities by the definition of the augmented valuation and Lemma 2.3.

Thus, there exists \(a \in K[x]\) with \(\text{deg}(a) < \text{deg}(\phi)\) and \(\mu(a) = \gamma > \mu(\phi)\). Therefore,

\[\phi + a \sim_{\mu} \phi \implies \phi + a \in \text{Rep}(t), \quad \phi + a \not\sim_{\mu^*} \phi \implies \phi + a \not\in \text{Rep}(t^*).\]

This shows that \(\text{Rep}(t) \neq \text{Rep}(t^*)\), against our assumption. \(\square\)
If we dropped properness of the maximal ideal \( \mathcal{L} \) from the definition of a type, there would be different types with the same sets of representatives.

On the other hand, we may still have types \( t \neq t' \) with \( \text{Rep}(t) \cap \text{Rep}(t') \neq \emptyset \). In order to avoid this situation, we introduce \textit{strong} types.

**Definition 3.13.** A key polynomial \( \phi \in \text{KP}(\mu) \) is said to be strong if \( \deg(\phi) \) is strictly larger than the minimal degree of key polynomials for \( \mu \).

A maximal ideal \( \mathcal{L} \in \text{Max}(\Delta_\mu) \) is strong if \( \mathcal{L} = \mathcal{R}_\mu(\phi) \) for some strong \( \phi \in \text{KP}(\mu) \). A type \( t = (\mu, \mathcal{L}) \) is strong if \( \mathcal{L} \) is strong.

By Corollary 3.2, a strong key polynomial is necessarily proper, and the converse is true if \( e_{\text{rel}}(\mu) > 1 \). Let us denote by \( T^{\text{str}} \subset T \) the subset of strong types.

**Lemma 3.14.** Let \( t, t' \in T^{\text{str}} \). If \( \text{Rep}(t) \cap \text{Rep}(t') \neq \emptyset \), then \( t = t' \).

**Proof.** Let \( t = (\mu, \mathcal{L}), \ t^* = (\mu^*, \mathcal{L}^*) \), and take \( \phi \in \text{Rep}(t) \cap \text{Rep}(t^*) \). The assumption \( t, t' \in T^{\text{str}} \) implies that \( \phi \) is a strong key polynomial simultaneously for \( \mu \) and \( \mu^* \).

Arguing as in the proof of Theorem 3.12, we need only to show that \( \mu = \mu^* \).

By Lemma 3.11 the assumption \( \mu \neq \mu^* \) leads to (13), after eventually exchanging the valuations. By Proposition 2.2, \( \phi \) is a key polynomial for \( \mu^* \) of minimal degree. This contradicts the fact that \( \phi \) is strong. \( \square \)

4. Key polynomials as \( \mu \)-factors of prime polynomials

We keep assuming that the valued field \( (K, v) \) is henselian.

In this section, we find out arithmetic properties of a prime polynomial \( F \in \mathbb{P} \), derived from the existence of a valuation \( \mu \in \mathbb{V}^{\text{kp}} \) admitting a key polynomial \( \phi \) such that \( \phi |_\mu F \).

**Theorem 4.1.** Let \( F \in \mathbb{P} \), and let \( \phi \in \text{KP}(\mu) \) for some valuation \( \mu \in \mathbb{V}^{\text{kp}} \). Then,

\[
\phi |_\mu F \iff \mu(\phi) < v_F(\phi).
\]

Moreover, if this condition holds, then:

1. Either \( F = \phi \), or the Newton polygon \( N_{\mu,\phi}(F) \) is one-sided of slope \(-v_F(\phi)\).
2. \( F \sim_{\mu} \phi^\ell \) with \( \ell = \ell(N_{\mu,\phi}(F)) = \deg(F)/\deg(\phi) \).

In particular, \( \mathcal{R}(\phi) \) is a power of the maximal ideal \( \mathcal{R}(\phi) \) in \( \Delta \).

**Proof.** If \( F = \phi \) all statements of the theorem are trivial. Assume \( F \neq \phi \).

If \( \phi |_\mu F \), then \( \mu(F) = v_\phi(F) \) by (10). By Theorem 1.5 and Lemma 3.10, \( \mu(\phi) \geq \deg(\phi)\mu(\mu)/\deg(F) = \deg(\phi)v_\phi(F)/\deg(F) = v_F(\phi) \).

Now, suppose \( \phi |_\mu F \). Let \( \theta \in \overline{K} \) be a root of \( F \), and consider the minimal polynomial of \( \phi(\theta) \) over \( \overline{K} \):

\[
g = b_0 + b_1 x + \cdots + b_k x^k \in \overline{K}[x], \quad b_k = 1.
\]

All roots of \( g \) in \( \overline{K} \) have a constant \( v \)-value \( \gamma := v(\phi(\theta)) = v_F(\phi) \). Hence,

\[
v(b_0) = k\gamma, \quad v(b_j) \geq (k-j)\gamma, \quad 1 \leq j < k, \quad v(b_k) = 0.
\]

Let \( G = \sum_{j=0}^k b_j \phi^j \in \overline{K}[x] \). By (14), \( N_{\mu,\phi}(G) \) is one-sided of slope \(-\gamma \). Since \( G(\theta) = 0 \), the polynomial \( F \) divides \( G \) and Theorem 1.14 shows that

\[
N_{\mu,\phi}(G) = N_{\mu,\phi}(F) + N_{\mu,\phi}(F/G).
\]
Figure 4. Newton polygon $N_{\phi}(F)$ when $\phi \mid F$. We take $\gamma = v_F(\phi)$.

By Lemma 1.13, $\ell(N_{\phi}(F)) > 0$, since $\phi \mid F$. Thus, $N_{\phi}(F)$ has positive length too. This implies $\mu(\phi) < \gamma$ by the definition of the principal polygon (see section 1.3).

On the other hand, since $N_{\phi}(G) = N_{\phi}(F)$ is one-sided of slope $-\gamma$, (15) shows that $N_{\phi}(F)$ is one-sided of slope $-\gamma$ too.

This proves that $\phi \mid F$ if and only if $\mu(\phi) < \gamma$, and that (1) holds in this case.

Let us prove item (2) in the case $\phi \mid F$. Consider the $\phi$-expansion $F = \sum_{s=0}^{\ell} a_s \phi^s$. By Lemma 3.10

$$\mu(a_0) = v_F(F) = \deg(F) v_F(\phi) / \deg(\phi) = \deg(F) \gamma / \deg(\phi).$$

Therefore, from the fact that $N_{\phi}(F)$ is one-sided of slope $-\gamma$ we deduce:

$$\mu(a_\ell) = \mu(a_0) - \ell \gamma = \gamma \frac{\deg(F)}{\deg(\phi)} - \ell \gamma = \gamma \frac{\deg(a_\ell) + \ell \deg(\phi)}{\deg(\phi)} - \ell \gamma = \gamma \frac{\deg(a_\ell)}{\deg(\phi)}.$$

If $\deg(a_\ell) > 0$, then $a_\ell$ would be a monic polynomial contradicting Theorem 1.5

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

Hence, $a_\ell = 1$, so that the leading monomial of the $\phi$-expansion of $F$ is $\phi^\ell$. In particular, $\ell = \deg(F)/\deg(\phi)$.

Since $\mu(\phi) < \gamma$, we have $\mu(\phi^s) < \mu(a_s \phi^s)$ for all $s < \ell$. Thus, $F \sim_{\mu} \phi^\ell$. The statement about $R(F) = R(\phi^\ell)$ follows from Proposition 3.6.

Our next aim is Theorem 4.5 where we find another characterization of the property $\phi \mid F$, which provides more arithmetic information on $F$.

To this end, we need some auxiliary results.

Lemma 4.2. For any $\beta \in \overline{K}$ inseparable over $K$, and any $\rho \in Q \Gamma$, there exists $\beta_{sep} \in \overline{K}$ separable over $K$ such that

$$\deg_K(\beta_{sep}) = \deg_K(\beta), \quad v(\beta - \beta_{sep}) > \rho.$$

Proof. Let $g \in K[x]$ be the minimal polynomial of $\beta$ over $K$. We have $g' = 0$.

Consider the polynomial $g_{sep} = g + \pi x \in K[x]$, where $\pi \in K^*$ satisfies

$$v(\pi) > \deg_K(\beta) \rho - v(\beta).$$

Since $g_{sep}' = \pi \neq 0$, this polynomial is separable. On the other hand,

$$\sum_{\alpha \in Z(g_{sep})} v(\beta - \alpha) = v(g_{sep}(\beta)) = v(\pi \beta) = v(\pi) + v(\beta) > \deg_K(\beta) \rho.$$

Hence, there exists $\alpha \in Z(g_{sep})$ such that $v(\beta - \alpha) > \rho$. We may take $\beta_{sep} = \alpha$. \qed
Lemma 4.3. Let $F \in \mathbb{P}$, $\mu \in \mathbb{V}^{kp}$ and $\phi \in \text{KP}(\mu)$ such that $\phi \mid_{\mu} F$. Let $\theta \in Z(F)$.

Then, for all $\beta \in \mathbb{K}$ with $\deg_K(\beta) < \deg(\phi)$, we have

$$v(\theta - \beta) < \text{Max} \{v(\theta - \alpha) \mid \alpha \in Z(\phi)\}.$$ 

Proof. Denote $\delta = \text{Max} \{v(\theta - \alpha) \mid \alpha \in Z(\phi)\}$, and fix $\alpha \in Z(\phi)$ with $v(\theta - \alpha) = \delta$.

Let $\beta \in \mathbb{K}$ with $\deg_K(\beta) < \deg(\phi)$. We want to show that $v(\theta - \beta) < \delta$, or equivalently, $v(\alpha - \beta) < \delta$.

By Lemma 4.2, we may assume that $\theta, \alpha$ and $\beta$ are separable over $K$. Consider a finite Galois extension $M/K$ containing $\theta, \alpha$ and $\beta$, and denote $G = \text{Gal}(M/K)$.

Let us assume that $v(\alpha - \beta) \geq \delta$, and show that this leads to a contradiction.

For all $\sigma \in G$ we get:

$$v(\alpha - \sigma(\beta)) = v(\alpha - \theta + \theta - \sigma(\alpha) + (\sigma(\alpha) - \sigma(\beta)))$$

$$\geq \text{Min} \{v(\alpha - \theta), v(\theta - \sigma(\alpha)), v(\sigma(\alpha) - \sigma(\beta))\} = v(\theta - \sigma(\alpha)),$$

because $v(\theta - \sigma(\alpha)) \leq \delta = v(\alpha - \theta)$ and $v(\sigma(\alpha) - \sigma(\beta)) = v(\alpha - \beta) \geq \delta$.

Therefore, if $g \in K[x]$ is the minimal polynomial of $\beta$ over $K$, we get

$$\frac{\#G}{\deg(g)} v(g(\alpha)) = \sum_{\sigma \in G} v(\alpha - \sigma(\beta)) \geq \sum_{\sigma \in G} v(\theta - \sigma(\alpha)) = \frac{\#G}{\deg(\phi)} v(\phi(\theta)).$$

By Theorem 4.1, this inequality implies

$$\mu(g) / \deg(g) = v(g(\alpha)) / \deg(g) \geq v(\phi(\theta)) / \deg(\phi) > \mu(\phi) / \deg(\phi),$$

which contradicts Theorem 1.5. \qed

Proposition 4.4. Let $F \in \mathbb{P}$, $\mu \in \mathbb{V}^{kp}$ and $\phi \in \text{KP}(\mu)$ such that $\phi \mid_{\mu} F$.

Then, for all $g \in K[x]$ with $\deg(g) < \deg(\phi)$, we have $v_\phi(g) = v_F(g)$.

Proof. Take $\theta \in Z(F)$ and $\alpha \in Z(\phi)$ such that $v(\theta - \alpha) = \text{Max} \{v(\theta - \alpha') \mid \alpha' \in Z(\phi)\}$.

Write $g = c \prod_j (x - \beta_j)$ with $c \in K$, $\beta_j \in \mathbb{K}$. Since $\deg_K(\beta_j) < \deg(\phi)$, Lemma 4.3 shows that $\theta - \beta_j \sim_v \alpha - \beta_j$ for all $j$. Therefore, $g(\theta) \sim_v g(\alpha)$.

In particular, $v(g(\theta)) = v(g(\alpha))$. \qed

Theorem 4.5. Let $F \in \mathbb{P}$. A valuation $\mu \in \mathbb{V}^{kp}$ admits a key polynomial $\phi$ such that $\phi \mid_{\mu} F$ if and only if $\mu < v_F$. In this case, for all non-zero $f \in K[x],$

$$(16) \quad \mu(f) = v_F(f) \iff \phi \mid_{\mu} f.$$ 

Proof. By Lemma 3.8, the condition $\mu < v_F$ implies the existence of $\phi \in \text{KP}(\mu)$ satisfying (16). In particular, $\phi \mid_{\mu} F$.

Conversely, suppose that $\phi \mid_{\mu} F$ for some $\phi \in \text{KP}(\mu)$. By Proposition 4.4, for any $a \in K[x]$ with $\deg(a) < \deg(\phi)$ we have $v_F(a) = v_\phi(a) = \mu(a)$.

On the other hand, $v_F(\phi) \geq \mu(\phi)$ by Theorem 4.1. Hence, for any $f \in K[x]$ with $\phi$-expansion $f = \sum_{0 \leq s} a_s \phi^s$, we have

$$v_F(f) \geq \text{Min} \{v_F(a_s \phi^s) \mid 0 \leq s\} \geq \text{Min} \{\mu(a_s \phi^s) \mid 0 \leq s\} = \mu(f).$$

Hence, $\mu < v_F$, and Lemma 3.8 shows that $\phi$ satisfies (16). \qed

Theorem 4.5 provides a practical device for the computation of $v_F$. For any given $f \in K[x]$, one seeks a pair $\mu, \phi$ such that $\phi \mid_{\mu} F$ and $\phi \mid_{\mu} f$, leading to $v_F(f) = \mu(f)$.

This yields a very efficient routine for the computation of the valuations attached to prime ideals in number fields, or places of function fields of curves [4 5].
Corollary 4.6. Let $F \in \mathbb{P}$, $\mu \in \mathbb{V}^{kp}$ and $\phi \in \text{KP}(\mu)$ such that $\phi \mid_\mu F$. Then,

$$e(\phi) \mid e(F), \quad f(\phi) \mid f(F), \quad d(\phi) \mid d(F).$$

Proof. Take arbitrary roots $\alpha \in Z(\phi), \theta \in Z(F)$.

The elements of $\Gamma_\phi$ are of the form $v(g(\alpha))$ for $g \in K[x]$ with $\deg(g) < \deg(\phi)$. By Proposition 4.4, these values coincide with $v(g(\theta)) \in \Gamma_{v_F}$. This proves $e(\phi) \mid e(F)$.

By Theorem 4.5, $\mu < v_F$, and this determines a canonical ring homomorphism

$$\Delta_\mu \longrightarrow k_F, \quad g + \mathcal{P}_0^+((\mu) \longrightarrow g(\theta) + m_F.$$ 

The kernel $\mathcal{L}_F$ of this homomorphism is a non-zero prime ideal of $\Delta_\mu$. Since this ring is a PID, $\mathcal{L}_F$ is a maximal ideal.

Clearly, $\mathcal{R}_\mu(F) \subset \mathcal{L}_F$. By Theorem 4.1, there exists a positive integer $n$ such that $\mathcal{R}_\mu(\phi^n) = \mathcal{R}_\mu(F) \subset \mathcal{L}_F$. Thus, $\mathcal{R}_\mu(\phi) = \mathcal{L}_F$, because both are maximal ideals.

By Proposition 3.8, $k_\phi \simeq \Delta_\mu/\mathcal{R}_\mu(\phi) = \Delta_\mu/\mathcal{L}_F$, which is isomorphic to a subfield of $k_F$. This proves $f(\phi) \mid f(F)$.

The fact that $d(\phi) \mid d(F)$ follows from [16].

If $\phi \mid_\mu F$, we may think $\phi$ as a “germ” of an approximation to $F$, and the value $v_F(\phi)$ as a measure of the quality of the approximation.

By Lemma 3.8, the valuation $\mu' = [\mu; \phi, v_F(\phi)]$ is closer to $v_F$, and it is natural to expect that any $\phi' \in \text{KP}(\mu')$, such that $\phi' \mid_{\mu'} F$, will be a better approximation to $F$.

The next result is a crucial step for an efficient computation of these approximations. The prime polynomial $F$ is usually unknown in practice, but the key polynomial $\phi'$ may be constructed by using only some “residual” information about $F$.

Lemma 4.7. Take $F \in \mathbb{P}$, $\mu \in \mathbb{V}^{kp}$, $\phi \in \text{KP}(\mu)$ such that $\phi \mid_\mu F$ and $\phi \neq F$.

For $\mu' = [\mu; \phi, v_F(\phi)]$, let $\kappa' = \kappa(\mu')$ and $R' = R_{\mu', \phi, \epsilon'}$ be the residual polynomial operator (section 1.4), for some $\epsilon' \in \mathbb{Q}_{\mu'}^*$ of degree $-\epsilon'v_F(\phi)$, where $\epsilon' = \epsilon_{rel}(\mu')$.

Then, $R'(F) \in \kappa'[y]$ is the power of some monic irreducible polynomial $\psi \in \kappa'[y]$.

Moreover, take any monic polynomial $\phi' \in K[x]$ of degree $\epsilon' \deg(\psi) \deg(\phi)$ such that $R'(\phi') = \psi$. Then, $\phi'$ is a proper key polynomial for $\mu'$ such that $\phi' \mid_{\mu'} F$, and $v_F(\phi) < v_F(\phi'), \quad e(\phi') = e(\phi)\epsilon', \quad f(\phi') = f(\phi)\deg(\psi), \quad d(\phi') = d(\phi)$.

Proof. By Proposition 2.2 and Theorem 4.1, $N_{\mu', \phi}(F) = N_{\mu, \phi}(F)$ is one-sided of slope $-v_F(\phi) = -\mu(\phi)$, and length $\ell = \deg(F)/\deg(\phi)$.

By the definition of $R'$, $\deg(R'(F)) = \ell\epsilon' > 0$ and $y \not| R'(F)$. Let $\psi$ be a monic irreducible factor of $R'(F)$ in $\kappa'[y]$.

Take a monic $\phi' \in K[x]$ such that $\deg(\phi') = \epsilon' \deg(\psi) \deg(\phi)$ and $R'(\phi') = \psi$.

Since $\phi$ is a key polynomial for $\mu'$ of minimal degree, Theorem 1.18 shows that $\phi' \not|_{\mu'} \phi$. In particular, $\phi'$ is a proper key polynomial for $\mu'$.

By Corollary 3.7, $s_{\mu', \phi'}(F) = \ord_{\psi}(R'(F)) > 0$, so that $\phi' \mid_{\mu'} F$.

By using Theorems 4.1 and 4.5, we deduce

$$v_F(\phi') > \mu'(\phi') = \deg(\phi') \mu'(\phi)/\deg(\phi) \geq \mu'(\phi) = v_F(\phi),$$

and $F \sim_{\mu'} (\phi')^\ell$, for $\ell = \deg(F)/\deg(\phi')$. By Corollary 1.17, $R'(F) = R'(\phi')^\ell = \psi^\ell$.

Now, by Corollary 1.19 applied to $\phi$ and $\phi'$ as key polynomials for $\mu'$, we get

$$e(\phi') = e(\mu') = e(\phi)\epsilon', \quad f(\phi') = f(\mu')\deg(\psi) = f(\phi)\deg(\psi).$$

Finally, $d(\phi') = d(\phi)$ follows from $\deg(\phi') = \epsilon' \deg(\psi) \deg(\phi) = e(\phi') f(\phi') d(\phi)$. □
A generalization of Hensel’s lemma. Theorems 4.1 and 4.5 provide a fundamental result concerning factorization of polynomials over henselian fields.

For \( \mu \in \mathbb{V}^p \), \( \phi \in \text{KP}(\mu) \) and \( \gamma \in \mathbb{Q} \Gamma \) such that \( \gamma > \mu(\phi) \), let us denote

- \( \mu_\gamma = [\mu; \phi, \gamma] \).
- \( e_\gamma = e_{\text{rel}}(\mu_\gamma) \) relative ramification index of \( \mu_\gamma \).
- \( \kappa_\gamma = \kappa(\mu_\gamma) \) algebraic closure of \( k \) in \( \Delta_{\mu_\gamma} \).
- \( R_{\mu_\gamma} : K[x] \to \kappa_\gamma[y] \) operator \( R_{\mu_\gamma, \phi, e_\gamma} \), for some \( e_\gamma \in \mathcal{G}_{\mu_\gamma}^p \) of degree \(-e_\gamma \gamma\).

**Theorem 4.8.** Let \( \phi \in \text{KP}(\mu) \) for some \( \mu \in \mathbb{V}^p \). Let \( f \in K[x] \) be a monic polynomial. For each slope \(-\gamma \) of the principal Newton polygon \( N_{\mu, \phi}^p(f) \), let

\[
R_{\mu_\gamma}(f) = \prod_{\psi} \psi^{a_{\gamma, \psi}}
\]

be the factorization of \( R_{\mu_\gamma}(f) \) into a product of powers of pairwise different monic irreducible polynomials \( \psi \in \kappa_\gamma[y] \).

Then, \( f \) factorizes in \( K[x] \) into a product of monic polynomials:

\[
f = f_0 \phi^{\text{ord}_\phi(f)} \prod_{(\gamma, \psi)} f_{\gamma, \psi}.
\]

If \( \ell = \ell \left( N_{\mu, \phi}^p(f) \right) \), the degrees of the factors are:

\[
\text{deg}(f_0) = \text{deg}(f) - \ell \text{deg}(\phi), \quad \text{deg}(f_{\gamma, \psi}) = e_\gamma a_{\gamma, \psi} \text{deg}(\psi) \text{deg}(\phi).
\]

Moreover, for any pair \((\gamma, \psi)\), it holds:

1. \( N_{\mu, \phi}(f_{\gamma, \psi}) \) is one-sided of slope \(-\gamma \) and length \( e_\gamma a_{\gamma, \psi} \text{deg}(\psi) \).
2. \( R_{\mu_\gamma}(f_{\gamma, \psi}) = \psi^{a_{\gamma, \psi}} \).
3. For every prime factor \( F \) of \( f_{\gamma, \psi} \), we have \( v_F(\phi) = \gamma \) and

\[
e(\phi) e_\gamma \mid e(F), \quad f(\phi) \text{deg}(\psi) \mid f(F), \quad d(\phi) \mid d(F).
\]

4. If \( a_{\gamma, \psi} = 1 \), then \( f_{\gamma, \psi} \) is irreducible and it is a key polynomial for \( \mu_\gamma \), with

\[
e(f_{\gamma, \psi}) = e(\phi) e_\gamma, \quad f(f_{\gamma, \psi}) = f(\phi) \text{deg}(\psi), \quad d(f_{\gamma, \psi}) = d(\phi).
\]

**Proof.** Let \( f = F_1 \cdots F_t \) be the factorization of \( f \) into a product of prime polynomials in \( K[x] \). These prime factors are not necessarily pairwise different.

Let us group these prime factors according to some of their properties with respect to the pair \( \mu, \phi \).

- The factor \( f_0 \) is the product of all \( F_j \) satisfying \( f_{\gamma, \psi} \mid \mu F_j \).
- The factor \( \phi^{\text{ord}_\phi(f)} \) is the product of all \( F_j \) equal to \( \phi \).
- 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 \( \psi \).

By Theorem 4.1, the factors \( F_j \neq \phi \) such that \( \phi \mid \mu F_j \) have one-sided Newton polygon \( N_{\mu, \phi}(F_j) \) of slope \(-\gamma \), with \( \gamma = v_{F_j}(\phi) > \mu(\phi) \). By Lemma 4.7, \( R_{\mu_\gamma}(F_j) \) is a power of some irreducible \( \psi \in \kappa_\gamma[y] \).

By Theorem 1.11, \(-\gamma\) is one of the slopes of \( N_{\mu, \phi}^p(f) \), and by Corollary 1.17, \( \psi \) is one of the irreducible factors of \( R_{\mu_\gamma}(f) \). Therefore, every prime factor \( F_j \) such that \( F_j \neq \phi \) and \( \phi \mid \mu F_j \) falls into one (and only one) of the factors \( f_{\gamma, \psi} \).

This proves the factorization (17).
By Lemma 1.13 and Theorem 4.1, for all $1 \leq j \leq t$ we have

$$\ell_j := \ell \left( N_{\mu,\phi}^{pp}(F_j) \right) = s_{\mu,\phi}(F_j) = \begin{cases} 0, & \text{if } \phi \not|_{\mu} F_j, \\ \deg(F_j)/\deg(\phi), & \text{if } \phi \mid_{\mu} F_j. \end{cases}$$

By Theorem 1.14, $\ell = \ell_1 + \cdots + \ell_t$. Hence,

$$\deg(f) - \deg(f_0) = \sum_{\phi \mid_{\mu} F_j} \deg(F_j) = \sum_{\phi \mid_{\mu} F_j} \ell_j \deg(\phi) = \sum_{j=1}^{t} \ell_j \deg(\phi) = \ell \deg(\phi).$$

Now, for each pair $(\gamma, \psi)$, let $J(\gamma, \psi)$ be the set of indices $j$ such that $F_j$ is a prime factor of $f_{\gamma,\psi}$. For all $j \in J(\gamma, \psi)$,

$$\ell_j = \ell \left( N_{\mu,\phi}^{pp}(F_j) \right) = e_{\gamma} \deg \left( R_{\mu,\gamma}(F_j) \right) = e_{\gamma} \deg(\psi) \ord_{\psi} R_{\mu,\gamma}(F_j).$$

On the other hand, $R_{\mu,\gamma}(F_j) \in \kappa_{\mu}^{\ast}$ is a constant for all $j \notin J(\gamma, \psi)$. In fact, $R_{\mu,\gamma}(\phi) = 1$, and for $\phi \not|_{\mu} F_j$, the condition $\ell \left( N_{\mu,\phi}^{pp}(F_j) \right) = 0$ implies that the $\gamma$-component of $N_{\mu,\phi}(F_j)$ is reduced to a single point (cf. section 1.3).

Corollary 4.17 shows that $R_{\mu,\gamma}(f_{\gamma,\psi}) = \prod_{j \in J(\gamma, \psi)} R_{\mu,\gamma}(F_j)$. Hence,

$$a_{\gamma,\psi} = \ord_{\psi} R_{\mu,\gamma}(f) = \ord_{\psi} R_{\mu,\gamma}(f_{\gamma,\psi}) = \sum_{j \in J(\gamma, \psi)} \ord_{\psi} R_{\mu,\gamma}(F_j),$$

We may conclude that

$$\deg(f_{\gamma,\psi}) = \sum_{j \in J(\gamma, \psi)} \deg(F_j) = \sum_{j \in J(\gamma, \psi)} \ell_j \deg(\phi) = e_{\gamma} a_{\gamma,\psi} \deg(\psi) \deg(\phi).$$

Moreover, items (1) and (2) follow from Theorem 1.14 and Corollary 1.17 having in mind equations (18) and (19).

Consider a monic polynomial $\phi_{\gamma,\psi} \in K[x]$ of degree $e_{\gamma} \deg(\psi) \deg(\phi)$ such that $R_{\mu,\gamma}(\phi_{\gamma,\psi}) = \psi$. By Lemma 4.7, $\phi_{\gamma,\psi}$ is a key polynomial for $\mu_{\gamma}$ such that $\phi_{\gamma,\psi} \mid_{\mu_{\gamma}} F$ for each prime factor of $f_{\gamma,\psi}$ and

$$e(\phi_{\gamma,\psi}) = e_{\gamma} e(\phi), \quad f(\phi_{\gamma,\psi}) = \deg(\psi) f(\phi), \quad d(\phi_{\gamma,\psi}) = d(\phi).$$

Thus, item (3) follows from Corollary 1.6.

If $a_{\gamma,\psi} = 1$, we may take $\phi_{\gamma,\psi} = f_{\gamma,\psi}$, by items (1) and (2). This proves item (4). 

**Remarks.**

1. Theorem 4.8 has been recently found by Jakhr-Khanduja-Sangwan, with a slightly different formulation [8]. The authors use the language of minimal pairs of definition of residually transcendental valuations.

   Our proof is shorter and more accessible, mainly because the residual polynomial operator is a more malleable tool than the classical technique of lifting polynomials from $\kappa[y]$ to $K[x]$.

2. This result is valid for an arbitrary valued field $(K, v)$, as long as the valuation $\mu$ is inductive. In this case, $\mu$ may be lifted to the henselization $K^h$ of $(K, v)$, and $\phi$ is still a key polynomial of the lifted valuation.

   In this way, it may be used to detect information about the prime factors in $K^h[x]$ of any given $f \in K[x]$. 

5. **Defectless polynomials and inductive valuations**

We keep assuming that \((K, v)\) is a henselian valued field.

Let \(F \in \mathbb{P}\) be a prime polynomial, and let \(\mu \in \mathbb{V}^p\) admitting a key polynomial \(\phi\) such that \(\phi \mid_\mu F\). We may think of \(\phi\) as a germ of an approximation to \(F\).

The iteration of the procedure of Lemma \[1.7\] yields a MacLane chain based on the initial valuation \(\mu\), with strictly better approximations:

\[
\mu \xrightarrow{\phi_0} \mu' \xrightarrow{\phi_1'} \mu'' \xrightarrow{\phi_2''} \cdots, \quad \gamma = v_F(\phi) < \gamma' = v_F(\phi') < \gamma'' = v_F(\phi'') < \cdots
\]

We say that this process *converges* to \(F\) if after a finite number of steps we reach a valuation \(\mu^{(n)}\) such that \(F\) is a key polynomial for \(\mu^{(n)}\).

Since \(\phi^{(n)} \mid_{\mu^{(n)}} F\), Lemma \[1.4\] and Corollary \[1.20\] show that the process converges if and only if we reach a key polynomial with \(\deg(\phi^{(n)}) = \deg(F)\).

In this section, we discuss this convergence when \(F\) is defectless; that is, when it has trivial defect \(d(F) = 1\).

### 5.1. Okutsu frames of defectless polynomials

Consider a prime polynomial \(F \in \mathbb{P}\) of degree \(n > 1\), and a fixed root \(\theta \in Z(F) \subset K\).

For any integer \(1 < m \leq n\), consider the set of weighted values

\[
W_m(F) = \left\{ \frac{v(g(\theta))}{\deg(g)} \mid g \in K[x] \text{ monic, } 0 < \deg(g) < m \right\} \subset \mathbb{Q}\Gamma.
\]

**Definition 5.1.** Suppose that the set \(W_n(F)\) contains a maximal value:

\[
w(F) := \text{Max}(W_n(F)).
\]

We say that \(\phi, F\) is a distinguished pair of polynomials if \(\phi \in K[x]\) is a monic polynomial of minimal degree among the monic polynomials satisfying

\[
0 < \deg(\phi) < n, \quad v(\phi(\theta))/\deg(\phi) = w(F).
\]

**Definition 5.2.** We say that \(F\) is an Okutsu polynomial if all sets \(W_m(F)\) contain a maximal element, for \(1 < m \leq n\).

Suppose that \(F\) is an Okutsu polynomial, and \(\phi, F\) is a distinguished pair.

If \(\deg(\phi) > 1\), we may consider a monic \(\phi' \in K[x]\) of minimal degree such that

\[
0 < \deg(\phi') < \deg(\phi), \quad \frac{v(\phi'(\theta))}{\deg(\phi')} = w'(F) := \text{Max}(W_{\deg(\phi)}(F)).
\]

By the minimality of \(\deg(\phi)\), we necessarily have \(w'(F) < w(F)\).

An iteration of this argument leads to a finite sequence

\[
\phi_0, \phi_1, \ldots, \phi_r, \phi_{r+1} = F
\]

of monic polynomials in \(K[x]\) such that

\[
1 = \deg(\phi_0) < \deg(\phi_1) < \cdots < \deg(\phi_r) < \deg(F),
\]

whose weighted values \(w_i(F) := v(\phi_i(\theta))/\deg(\phi_i)\) satisfy:

\[
\deg(g) < \deg(\phi_{i+1}) \implies \frac{v(g(\theta))}{\deg(g)} \leq w_i(F) < w_{i+1}(F), \quad 0 \leq i \leq r,
\]

for all monic polynomials \(g \in K[x]\) of positive degree.

Note that \(w_r(F) = w(F)\) and \(w_{r+1}(F) = \infty\).
**Definition 5.3.** 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 (20) and (21).

The length $r$ of the frame is called the Okutsu depth of $F$. Clearly, the Okutsu depth, the degrees $\deg(\phi_1), \ldots, \deg(\phi_r)$, and the values $w_1(F), \ldots, w_r(F) = w(F) \in \Phi$ are intrinsic data of $F$.

For instance, any key polynomial $\phi$ (of degree greater than one) for an inductive valuation $\mu$ is an Okutsu polynomial. Also, any optimal MacLane chain of $\mu$ determines an Okutsu frame of $\phi$.

**Lemma 5.4.** Consider an optimal MacLane chain of an inductive valuation:
\[ (22) \quad \mu_{-\infty}^{-\rightarrow} \phi_{0,T} \mu_0^{-\rightarrow} \phi_1^{-\rightarrow} \gamma_1 \mu_1^{-\rightarrow} \phi_2^{-\rightarrow} \gamma_2 \cdots \phi_{r-1}^{-\rightarrow} \gamma_{r-1} \mu_{r-1}^{-\rightarrow} \phi_r^{-\rightarrow} \gamma_r \mu_r = \mu. \]

Let $F \in \mathbb{P}$ and $\phi \in \text{KP}(\mu)$ such that $\phi \mid_\mu F$. Then,
\[ v_F(\phi_i) = \gamma_i, \quad 0 \leq i < r, \quad \text{and} \quad \phi_i \mid_{\mu_i} F, \quad 0 < i \leq r. \]
Moreover, if $\phi \mid_\mu \phi_r$, then $v_F(\phi_r) = \gamma_r$ as well.

**Proof.** By Theorem 4.3, $\mu < v_F$ and $\gamma_i = \mu(\phi_i) = v_F(\phi_i)$ for all $0 \leq i < r$. In fact, $\phi \mid_\mu \phi_i$, because $\deg(\phi_i) < \deg(\phi_r) \leq \deg(\phi)$. Also, $\gamma_r = \mu(\phi_r) = v_F(\phi_r)$, if $\phi \mid_\mu \phi_r$.

By Theorem 4.11, $\phi_i \mid_{\mu_i} F$ for $0 \leq i < r$, since $\mu_i(\phi_i) < \gamma_i = \mu(\phi_i) \leq v_F(\phi_i)$. \qed

**Theorem 5.5.** Let $\mu$ be an inductive valuation admitting an optimal MacLane chain as in (22). Then, all $\phi \in \text{KP}(\mu)$ with $\deg(\phi) > 1$ are Okutsu polynomials, and

1. If $\deg(\phi) > \deg(\phi_r)$, then $[\phi_0, \ldots, \phi_r]$ is an Okutsu frame of $\phi$.
2. If $\deg(\phi) = \deg(\phi_r)$, then $[\phi_0, \ldots, \phi_r]$ is an Okutsu frame of $\phi$.

Moreover, $w(\phi) = w(\mu)$ in the first case, and $w(\phi) = w(\mu_{r-1})$ in the second case.

**Proof.** Suppose $\deg(\phi) > \deg(\phi_r)$. Then, for all $\alpha \in Z(\phi)$, equation (10) shows that
\[ v(\phi(\alpha)) = \mu(\phi_r), \quad v(g(\alpha)) = \mu(g), \]
for all monic $g \in K[x]$ with $\deg(g) < \deg(\phi)$. Also, by Theorem 1.5,
\[ v(\phi(\alpha)) / \deg(g) = \mu(g) / \deg(g) \leq w(\mu) = \mu(\phi_r) / \deg(\phi_r) = v(\phi(\alpha)) / \deg(\phi_r), \]
and equality holds if and only if $g$ is $\mu$-minimal.

By Proposition 2.2, $\phi_r$ is a key polynomial for $\mu$ of minimal degree. By [13, Thm. 3.7], there are no $\mu$-minimal monic polynomials $g$ with $\deg(g) < \deg(\phi_r)$.

Therefore, $\phi_r, \phi$ is a distinguished pair, and $w(\phi) = w(\mu)$.

Since the MacLane chain is optimal, we have $\deg(\phi_{i+1}) > \deg(\phi_i)$ for all $0 \leq i < r$, and this argument shows that $\phi_i, \phi_{i+1}$ is a distinguished pair and $w(\phi_{i+1}) = w(\mu_i)$.

On the other hand, take $\alpha_{i+1} \in Z(\phi_{i+1})$. By Lemma 5.4 the tautology $\phi \mid_\mu \phi$ implies $\phi_{i+1} \mid_{\mu_i} \phi$, and Proposition 1.4 shows that
\[ g \in K[x], \deg(g) < \deg(\phi_{i+1}) \implies v(g(\alpha_{i+1})) = v(g(\alpha)). \]
Thus, $W_{\deg(\phi_{i+1})}(\phi)$ contains a maximal value and $w_{i+1}(\phi) = w(\phi_{i+1}) = w(\mu_i)$.

This ends the proof of (1).

Suppose $\deg(\phi) = \deg(\phi_r)$. By Lemma 5.4, $\phi_r \mid_{\mu_{r-1}} \phi$, so that $\phi$ is a key polynomial for $\mu_{r-1}$ by Lemma 1.4. Since $\deg(\phi) = \deg(\phi_{r-1})$, item (2) follows from the previous argument applied to the optimal MacLane chain of $\mu_{r-1}$ deduced by truncation. \qed
Conversely, any Okutsu frame of an Okutsu polynomial arises in this way.

**Theorem 5.6.** Let $F$ be an Okutsu polynomial, and let $[\phi_0, \ldots, \phi_r]$ be an Okutsu frame of $\phi_{r+1} := F$. For all $0 \leq i \leq r$, the mapping

$$
\mu_i : K[x] \to \mathbb{Q} \Gamma \cup \{\infty\}, \quad \sum_{0 \leq s} a_s \phi_i^s \mapsto \min\{v_F(a_s \phi_i^s) \mid 0 \leq s\}
$$

is a valuation admitting $\phi_{i+1}$ as a key polynomial.

Also, $\mu_r$ admits an optimal MacLane chain as in (22), with $\gamma_i = v_F(\phi_i)$ for all $i$.

**Proof.** The coefficients $a_s \in K$ of any $\phi_0$-expansion satisfy $v_F(a_s) = v(a_s)$. Hence, $\mu_0 = \mu_0(\phi_0, \gamma_0)$ by the definition of the depth-zero valuations in section 2,2.

Also, we saw that $\mu_0(\phi_0, \gamma_0)$ is equivalent to the augmentation $[\mu_\infty; \phi_0, (0, \gamma_0)]$; thus, $\phi_0$ is a key polynomial for $\mu_0$, by Proposition 2.2.

Now, suppose that for some $0 \leq i \leq r$, we know that $\mu_i$ is a valuation and $\phi_i$ is a key polynomial for $\mu_i$ such that $\mu_i(\phi_i) = \gamma_i$.

The theorem will follow from a recursive argument if we deduce that $\phi_{i+1}$ is a key polynomial for $\mu_i$ too; and moreover $\mu_{i+1} = [\mu_i; \phi_{i+1}, \gamma_{i+1}]$ for $i < r$.

In fact, $\mu_i < v_F$ by the definition of $\mu_i$. Let $\phi \in K[x]$ be a monic polynomial of minimal degree such that $\mu_i(\phi) < v_F(\phi)$. By Lemma 3.8, $\phi$ is a key polynomial for $\mu_i$. Theorem 1.3 shows that

$$
(23) \quad \frac{v(\phi(\theta))}{\deg(\phi)} > \frac{\mu_i(\phi)}{\deg(\phi)} = w(\mu_i) = \frac{\mu_i(\phi_i)}{\deg(\phi_i)} = \frac{v(\phi_i(\theta))}{\deg(\phi_i)} = w_i(F),
$$

$$
(24) \quad \frac{v(\phi_{i+1}(\theta))}{\deg(\phi_{i+1})} = w_{i+1}(F) = w_i(F) = w(\mu_i) \geq \frac{\mu_i(\phi_{i+1})}{\deg(\phi_{i+1})}.
$$

By (21) and (23), we have $\deg(\phi) \geq \deg(\phi_{i+1})$. Also, (24) implies $\deg(\phi) \leq \deg(\phi_{i+1})$, by the minimality of $\deg(\phi)$. Hence, $\deg(\phi) = \deg(\phi_{i+1})$.

By Lemma 3.8, $\phi_{i+1}$ is a key polynomial for $\mu_i$ (and it is $\mu_i$-equivalent to $\phi$).

Finally, if $i < r$ then $\mu_{i+1} = [\mu_i; \phi_{i+1}, \gamma_{i+1}]$ by the very definition of the augmented valuation.

**Theorem 5.7.** For any prime polynomial $F \in \mathbb{P}$ with $\deg(F) > 1$, 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 5.5 and 5.6, items (1) and (2) are equivalent. Also, (1) implies (3) by [16], or [14] Cor. 5.14.

Finally, the implication (3) $\Rightarrow$ (1) follows from the results of Vaquié in [15, 16]. In fact, suppose that $F$ is defectless. As shown in section 4, there exists a MacLane chain, of arbitrarily large length, of inductive valuations in the interval $(\mu_\infty, v_F) \subset V$:

$$
\mu_\infty \phi_0, \gamma_0 \mu_0 \phi_1, \gamma_1 \ldots \phi_{n-1}, \gamma_{n-1} \mu_{n-1} \phi_n, \gamma_n \mu_n \phi_{n+1}, \gamma_{n+1} \ldots
$$

with key polynomials satisfying $\phi_n \mid_{\mu_{n-1}} F$ for all $n$.

If $\deg(\phi_n) = \deg(F)$ for some $n$, then Lemma 1.4 shows that $F$ is a key polynomial for $\mu_{n-1}$ and we are done.
Otherwise, since \( \deg(\phi_n) | \deg(\phi_{n+1}) \), this degree becomes constant for a sufficiently large \( n \). Thus, we get a continuous MacLane chain which may be augmented to a certain limit augmented valuation by using a certain limit key polynomial \([15]\).

This limit augmented valuation lies still in the interval \( (\mu_{-\infty}, v_F) \), but it is no more inductive. The main result of \([16]\) shows that in this case \( F \) has some defect. \( \square \)

**Remark.** The implication \( (3) \Rightarrow (1) \) may be deduced from the work by Aghigh and Khanduja too, who use the technique of complete distinguished chains of algebraic elements over \( K \) \([1]\).

The next result follows immediately from Theorems 5.5, 5.6 and 5.7.

**Corollary 5.8.** 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 \( \phi_i, \phi_{i+1} \) is a distinguished pair for all \( 0 \leq i \leq r \).

In this case, \( \phi_i \) is a defectless polynomial and \( [\phi_0, \ldots, \phi_{i-1}] \) is an Okutsu frame of \( \phi_i \). Moreover, \( w_i(F) = w(\phi_{i+1}) \) for all \( 1 \leq i \leq r \).

### 5.2. Canonical inductive valuation attached to a defectless polynomial.

Let \( F \) be a defectless (prime) polynomial of degree greater than one.

With the notation of Theorem 5.6, \( F \) is a strong key polynomial for the valuation \( \mu_r \), which is defined in terms of \( \phi_r \)-expansions and satisfies

\[
\mu_r(\phi_r) = v_F(\phi_r) = \deg(\phi_r)w(F),
\]

since \( \phi_r, F \) is a distinguished pair.

Since \( F \) is \( \mu_r \)-minimal, Lemma 1.2 shows that the valuation \( \mu_r \) may be defined in terms of \( F \)-expansions. By \([10]\) and Theorem 1.5, this valuation is determined by

\[
\mu_r(a) = v_F(a), \quad \forall a \in K[x] \text{ with } \deg(a) < \deg(F),
\]

\[
\mu_r(F) = \deg(F)\mu_r(\phi_r) = \deg(F)w(F).
\]

Hence, we may define this valuation \( \mu_r \) avoiding any mention to \( \phi_r \).

**Definition 5.9.** Let \( F \) be a defectless polynomial with \( \deg(F) > 1 \).

The Okutsu bound of \( F \) is defined as \( \delta_0(F) = \deg(F)w(F) \in \mathbb{Q}\Gamma \).

There is a canonical inductive valuation \( \mu_F \) admitting \( F \) as a strong key polynomial, determined by the following action on \( F \)-expansions:

\[
f = \sum_{0 \leq s} a_s F^s \implies \mu_F(f) = \min \{ v_F(a_s) + s\delta_0(F) \mid 0 \leq s \}.
\]

The polynomial \( F \) is a key polynomial for infinitely many inductive valuations. Among them, the valuation \( \mu_F \) is distinguished by the fact of being minimal.

**Lemma 5.10.** Let \( F \in \mathbb{P} \) be a defectless polynomial with \( \deg(F) > 1 \).

1. The Okutsu depth of \( F \) is equal to the MacLane depth of \( \mu_F \).
2. If \( \phi, F \) is a distinguished pair, then \( \phi \) is a key polynomial for \( \mu_F \) of minimal degree.
3. The interval \( (\mu_F, v_F) \subset V \) consists of all augmentations
   \[
   \mu = [\mu_F; F, \gamma], \quad \gamma \in (\delta_0(F), \infty) \subset \mathbb{Q}\Gamma.
   \]
4. The valuation \( \mu_F \) is the minimal element in the interval \( (\mu_{-\infty}, v_F) \) which admits \( F \) as a key polynomial.
Proof. Items (1) and (2) are an immediate consequence of Theorem 5.6.

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 Lemma 3.8, \( F \) is a key polynomial for \( \mu \). By Lemma 3.11, \( \mu = [\mu_F; F, \gamma] \) for \( \gamma = \mu(F) > \mu_F(F) = \delta_0(F) \). This proves item (3).

If a valuation \( \mu < \mu_F \) admits \( F \) as a key polynomial, then \( \mu_F = [\mu; F, \delta_0(F)] \) by Lemma 3.11. This contradicts item (2), because \( F \) would be a key polynomial for \( \mu_F \) of minimal degree. Since the interval \( (\mu_{-\infty}, v_F) \) is totally ordered (Theorem 3.9), this argument ends the proof of item (4). \( \square \)

Corollary 5.11. Let \( F \in \mathbb{P} \) be a defectless polynomial with \( \deg(F) > 1 \). Then, all valuations in \( (\mu_{-\infty}, v_F) \) are inductive.

Proof. Take \( \mu \in (\mu_{-\infty}, v_F) \subset \mathbb{V} \). Since \( \mu_F \) is inductive and \( (\mu_{-\infty}, \mu_F) \) is totally ordered, we need only to discuss the cases \( \mu < \mu_F \) and \( \mu > \mu_F \).

If \( \mu > \mu_F \), then \( \mu \) is inductive because it is an augmentation of \( \mu_F \) (Lemma 5.10).

If \( \mu < \mu_F \), consider a MacLane chain of \( \mu_F = \mu_r \) as in Theorem 5.6.

If we agree that \( \mu_{-1} = \mu_{-\infty} \), our valuation \( \mu \) fits into

\[ \mu_{i-1} < \mu < \mu_i = [\mu_{i-1}; \phi_i, \gamma_i], \quad 0 \leq i < r. \]

Since \( \mu \leq \mu_i < v_{\phi_i} \), Lemma 3.8 shows that \( \phi_i \in KP(\mu) \), because it is a monic polynomial of minimal degree satisfying \( \mu(\phi_i) < v_{\phi_i}(\phi_i) = \infty \).

Hence, \( \mu \) is an augmentation of \( \mu_{i-1} \) by Lemma 3.11. \( \square \)

5.3. Strong types parameterize defectless prime polynomials. Let us denote by \( \mathbb{P}_{dless} \) the set of all defectless prime polynomials in \( K[x] \) of degree greater than 1.

Lemma 5.12. Let \( \mu \) be an inductive valuation and \( F \in \mathbb{P}_{dless} \).

Then, \( \mu = \mu_F \) if and only if \( F \) is a strong key polynomial for \( \mu \).

Proof. If \( \mu = \mu_F \), then \( F \) is obviously a strong key polynomial for \( \mu \).

Conversely, if \( F \in KP(\mu) \) is strong, then \( F \) is a common representative of the two strong types \( (\mu, \mathcal{R}_\mu(F)), (\mu_F, \mathcal{R}_{\mu_F}(F)) \). By Lemma 3.14, \( \mu = \mu_F \). \( \square \)

Lemma 5.13. Let \( F, G \in \mathbb{P}_{dless} \) be two defectless polynomials of the same degree. The following conditions are equivalent:

1. \( v_F(G) > \delta_0(F) \).
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 \( \deg(F-G) < \deg(F) \), by the definition of \( \mu_F \) we have

\[ \mu_F(F-G) = v_F(F-G) = v_F(G). \]

Since \( \delta_0(F) = \mu_F(F) \), items (1) and (2) are equivalent.

Suppose \( F \sim_{\mu_F} G \). Lemma 1.4 shows that \( G \) is a strong key polynomial for \( \mu_F \).

By Lemma 5.12, \( \mu_F = \mu_G \) and Corollary 1.20 shows that \( \mathcal{R}(F) = \mathcal{R}(G) \).

Hence, (2) implies (3). The opposite implication follows from Corollary 1.20. \( \square \)

The symmetry of condition (3) shows that \( \approx \) is an equivalence relation on the set \( \mathbb{P}_{dless} \). Let us parameterize the quotient set \( \mathbb{P}_{dless}/\approx \) by an adequate space.
Theorem 5.14. Consider the MacLane space \( \mathcal{M} = \{(\mu, \mathcal{L}) \in \mathbb{T}^{\text{str}} \mid \mu \text{ inductive}\} \), of strong types based on inductive valuations. The following mapping is bijective:

\[
\mathcal{M} \rightarrow \mathbb{P}^{\text{dless}} / \sim, \quad t = (\mu, \mathcal{L}) \mapsto \text{Rep}(t).
\]

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

Proof. For any \( t = (\mu, \mathcal{L}) \in \mathcal{M} \), the set \( \text{Rep}(t) \) is a \( \mu \)-equivalence class of strong key polynomials for \( \mu \). By Lemma 5.12

\[
(25) \quad \mu = \mu_\phi, \quad \forall \phi \in \text{Rep}(t).
\]

By Lemma 5.13, \( \text{Rep}(t) \) is an Okutsu equivalence class. Therefore, the mapping \( \mathcal{M} \rightarrow \mathbb{P}^{\text{dless}} / \sim \) is well defined. By Theorem 3.12, it is injective.

Obviously, \( F \) is a representative of the type \((\mu_F, \mathcal{R}_{\mu_F}(F))\); thus, our mapping is bijective. By (25), the inverse mapping is determined by \( F \mapsto (\mu_F, \mathcal{R}_{\mu_F}(F)) \). \( \square \)

By Theorems 5.5 and 5.6, two Okutsu equivalent polynomials \( F, G \in \mathbb{P}^{\text{dless}} \) have the same Okutsu depth, Okutsu frames and numerical invariants attached to any optimal MacLane chain of the common inductive valuation \( \mu_F = \mu_G \). In particular, as shown in section 2.3, they have the same ramification index and residual degree:

\[
e(F) = e(\mu_F) = e(G), \quad f(F) = f(\mu_F) \deg(R(F)) = f(G),
\]

where \( R \) is any choice of a residual polynomial operator over \( \mu_F \).

Finally, let us shows that two separable Okutsu equivalent polynomials determine two extensions of \( K \) having isomorphic maximal tame subextensions.

Definition 5.15. A polynomial \( F \in \mathbb{P}^{\text{dless}} \) is tame if the following conditions hold:

- The finite extension \( k_F/k \) is separable.
- The ramification index \( e(F) \) is not divisible by \( \text{char}(K) \).

It is easy to check that a tame \( F \) is necessarily separable over \( K \).

A separable algebraic field extension \( L/K \) is tame if every \( \theta \in L \) is defectless and has a tame minimal polynomial over \( K \).

Recall the definition of the tame ramification subgroup:

\[
G^{\text{tame}} = \{\sigma \in \text{Gal}(K^s/K) \mid \sigma(c) \sim_v c, \quad \forall c \in K^s\},
\]

where \( K^s \subset \overline{K} \) is the separable closure of \( K \).

Its fixed field \( (K^s)^{G^{\text{tame}}} \subset K^s \) is the unique maximal tame extension of \( K \) in \( \overline{K} \).

Also, for any algebraic extension \( L/K \), the subfield

\[
L^{\text{tame}} := L \cap (K^s)^{G^{\text{tame}}} \subset L
\]

is the unique maximal tame subextension of \( K \) in \( L/K \).

Theorem 5.16. Let \( F, G \in \mathbb{P}^{\text{dless}} \) be separable and Okutsu equivalent. For \( \theta \in Z(F) \), take \( \omega \in Z(G) \) such that \( v(\theta - \omega) = \max \{v(\theta - \omega') \mid \omega' \in Z(G)\} \).

Then, \( K(\theta)^{\text{tame}} = K(\omega)^{\text{tame}} \).

Proof. By Lemma 5.13 \( G \) is a key polynomial for \( \mu_F \) and \( G |_{\mu_F} F \). By Lemma 4.3

\[
\beta \in \overline{K}, \quad \deg_K(\beta) < \deg(G) \implies v(\theta - \beta) < v(\theta - \omega).
\]

As we argued along the proof of Proposition 4.4 this implies

\[
(26) \quad g(\theta) \sim_v g(\omega), \quad \forall g \in K[x] \text{ with } \deg(g) < \deg(G).
\]
Let $M/K$ be a finite Galois extension containing $\theta$ and $\omega$. The subfields $K(\theta)$ and $K(\omega)^\text{tame} \subset M$ are the fixed fields of the following subgroups of $\text{Gal}(M/K)$:

- $H_\theta = \{ \sigma \in H \mid \sigma(\theta) = \theta \}$,
- $H_\omega^\text{tame} = \{ \sigma \in H \mid \sigma(c) \sim_v c, \quad \forall c \in K(\omega) \}$.

Any $c \in K(\omega)$ may be written as $c = g(\omega)$ for some $g \in K[x]$ with $\deg(g) < \deg(G)$. Hence, $H_\theta \subset H_\omega^\text{tame}$, because for all $\sigma \in H_\theta$, (26) shows that $\sigma(g(\omega)) \sim_v \sigma(g(\theta)) = g(\theta) \sim_v g(\omega)$.

By Galois theory, $K(\omega)^\text{tame} \subset K(\theta)$, and this implies $K(\omega)^\text{tame} \subset K(\theta)^\text{tame}$, by the maximality of $K(\theta)^\text{tame}$. By the symmetry of the argument, $K(\theta)^\text{tame} = K(\omega)^\text{tame}$. □

**Corollary 5.17.** Suppose that $F, G \in \mathcal{P}_{\text{dless}}$ are separable and $F \approx G$. If $F$ is tame, then for all $\theta \in Z(F)$ there exists a root $\omega \in Z(G)$ such that $K(\theta) = K(\omega)$.

### References

[1] K. Aghigh, S. K. Khanduja, *On chains associated with elements algebraic over a henselian valued field*, Algebra Colloq. 12 (2005), no. 4, 607–616.

[2] J. Fernández, J. Guàrdia, J. Montes, E. Nart, *Residual ideals of MacLane valuations*, J. Algebra 427 (2015), 30–75.

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

[4] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. 13 (2013), 729–762.

[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, M.A. Olalla Acosta, M. Spivakovsky, *Valuations in algebraic field extensions*, J. Algebra 312 (2007), no. 2, 1033–1074.

[7] F.J. Herrera Govantes, W. Mahloub, M.A. Olalla Acosta, M. Spivakovsky, *Key polynomials for simple extensions of valued fields*, preprint, [arXiv:1406.0657][math.AG], 2018.

[8] A. Jakhar, S.K. Khanduja, N. Sangwan, *On factorization of polynomials in henselian valued fields*, Comm. Algebra 46 (2018), no. 7, 3205–3221.

[9] S. MacLane, *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. 40 (1936), pp. 363–395.

[10] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. J. 2 (1936), pp. 492–510.

[11] N. Moraes de Oliveira, E. Nart, *Computation of residual polynomial operators of inductive valuations*, preprint, [arXiv:1901.04937][math.AG].

[12] E. Nart, *On the equivalence of types*, J. Théor. Nombres Bordeaux 28 (2016), no. 3, 743–771.

[13] E. Nart, *Key polynomials over valued fields*, Publ. Mat. 64 (2020), no. 1, to appear, arXiv:1803.08406[math.AG].

[14] K. Okutsu, *Construction of integral basis I, II*, Proc. Japan Acad. Ser. A 58 (1982), 47–49, 87–89.

[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. 

---

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