Valuations and polynomial factorization

Brakl, F.

Mathematisch Instituut
Universiteit Leiden

Master Thesis

Valuations and polynomial factorization

Author:
Filip Brakl

Supervisor:
Peter Bruin

Contents

0 Introduction

Let (K, v) be a valued field and denote its value group by Γ.

In [16], Maclane introduced the concept of key polynomials in order to understand extensions of v to the field $K(x)$. The idea is that for a given valuation μ on $K(x)$, a key polynomial $\phi \in K[x]$, allows us to augment μ; to obtain a ν with $\mu \leq \nu$, such that $\mu(\phi) < \nu(\phi)$. He then showed how to obtain μ as a certain "limit" of a sequence of augmentations when Γ is discrete and rank one. This work was motivated by a conjecture of Ore, who believed a description like this would lead to algorithms for prime ideal decomposition in number fields. MacLane solved the conjecture by finding an algorithm to compute all extensions of v to the field $K[x]/(g)$ defined by an irreducible polynomial $g \in K[x]$ [15]. His ideas were later re-interpreted as a factorization algorithm over the completion K_v.

Decades down the line, still in the discrete rank one case, J. Montes introduced certain residual polynomial operators which led to the design of a practical algorithm following the exact pattern Ore had foreseen [11].

In [26], [28] and [27], Vaquié introduced limit key polynomials and limit augmentations, allowing him to drop the "discrete rank one" assumption, leading to a full generalization of MacLane's result on extensions of v to $K(x)$. However, to generalize MacLane's algorithm [15] to henselian fields of arbitrary rank is still an open problem.

The aim of this thesis is to present Vaquié's theory of key polynomials, use it to describe the best known algorithm for factoring polynomials over henselian fields, and explore how existence of defect currently obstructs its termination in the general case. We also obtain an algorithm to compute splitting fields of separable defectless polynomials.

To read this thesis, one only needs to know some abstract algebra and basics of Galois theory.

Those more inclined towards algebraic geometry might also find the theory presented here relevant; MacLane's results were independently generalized by Novacoski and Spivakovsky in [23] and Decaup, Mahboub and Spivakovsky in [9], in order to attack local uniformization in positive characteristic, a crucial step in their programme to prove resolution of singularities. These authors introduce certain abstract key polynomials, which do kind of the "opposite" of key polynomials; an abstract key polynomial $\phi \in K[x]$ allows us to truncate μ to obtain a valuation $\nu \leq \mu$. Nevertheless, abstract key polynomials and key polynomials are intimately linked, see [22] and [1] for comparison theorems.

Mixing the "bottom up" approach of key polynomials with the "top down" approach of abstract key polynomials has recently led to a better understanding of the defect of extensions of (not necessarily discrete, nor henselian) rank one valued fields [21].

Another program to prove local uniformization is due to Teissier who considers deformations of spectra of certain graded rings [25].

What all these approaches have in common is their use of the graded ring, $\mathcal{G}_\mu$, associated to μ. It is an important and useful object in its own right. It has been shown in [6] that $\mathcal{G}_\mu$ is isomorphic to the semigroup ring $k_\mu[t^{\Gamma_\mu}]$, where k_μ is the residue field

of μ, with a certain twisted multiplication. Moreover, in [21], that $\mathcal{G}_\mu \cong \mathcal{G}_{\mu^h}$ as graded rings, where μ^h is the extension of μ to $K^h[x]$. Hence, $\mathcal{G}_\mu$ considers the value group, residue field and henselization of μ simultaneously.

For our purposes, we mainly look at images of $f \in K[x]$ under the initial term mapping $\text{in}_\mu : K[x] \longrightarrow \mathcal{G}_\mu$. Key polynomials are the $\phi \in K[x]$ such that $\text{in}_\mu(\phi)$ is a prime element, and satisfy some additional properties. We will see that $\mathcal{G}_\mu$ possesses unique factorization for homogeneous elements, which leads to certain residual polynomial operators $R : K[x] \longrightarrow \kappa[y]$ where κ is a finite extension of the residue field k of (K, v). These operators allow us to find the prime factorization over the "smaller field" κ instead of working with the whole of $\mathcal{G}_\mu$. They make the polynomial factorization algorithm we present here constructive and enable its implementation on a computer.

In our proof of termination, however, we follow the philosophy of avoiding the specifics of these operators wherever possible. Namely, we exploit that the set of monic irreducible polynomials over K, $\text{Irr}(K)$, forms an ultrametric space when (K, v) is henselian. We then use that the ultrametric structure is intimately linked to Vaquié's characterization of defectless polynomials as key polynomials of inductive valuations.

Since every valued field (K, v) embeds into an algebraic extension (K^h, v^h) that is henselian and immediate, it may be possible to find the factorization of $g \in K[x]$ over K^h working only within K. This is accomplished in [3], currently under the severe restriction $\deg(g) < \text{char}(k)$, where k is the residue field of (K, v). One direction for future work is to try and mirror the well-known approach of representing an element of $\overline{\mathbb{Q}}$ by its minimal polynomial over $\mathbb{Q}$ and a high precision complex approximation, to perform computations in K^h. Another is to relax the conditions we are forced to impose on (K, v) to guarantee termination of our algorithms.

If $g \in K[x]$ is defectless, there exists a sequence of choices such that the algorithm terminates. However, since it is an open problem to control the "quality" of these choices via the constructive methods of residual polynomial operators, we are forced to assume in our proof that the worst possible choices are made. Under the assumption that every strictly increasing infinite sequence in Γ is not bounded, we show that in finitely many steps a "good enough" approximation $\phi \in \text{Irr}(K)$ to an irreducible factor of g is constructed regardless of the choices made. This leads to a polynomial factorization algorithm for defectless, monic, square-free (not necessarily separable) $g \in K[x]$.

It is an object of ongoing research to drop the "defectless assumption". The solution would be to modify these algorithms to handle limit augmentations. The main obstacle is that there exist examples, even in the discrete rank one case (with $p = \text{char}(k) > 0$ and K not perfect), where it is impossible to distinguish between an ordinary augmentation and a limit augmentation in finitely many steps by current methods.

Finally, we give an algorithm to find the splitting field of separable $g \in K[x]$, which uses the polynomial factorization as a subroutine. The idea is to replace an irreducible factor of $g \in K[x]$ by a sufficiently good approximation to it. This operation does not change the splitting field thanks to Krasner's lemma. We point out that running the polynomial factorization algorithm over the splitting field allows one to approximate the roots of g to arbitrary precision. Such approximations can be used in particular to

explicitly describe Galois groups of polynomials over local fields, which was the initial motivation for this project.

0.1 Overview

In **Section 1**, we give basic definitions and results about valuations on an arbitrary field K and their extensions to the polynomial ring $K[x]$. We then describe valuations μ on $K[x]$ in terms of data associated to the extension μ/v, where v is the restricion of μ to K. We introducte the set $\mathcal{T}$ of all extensions of v to $K[x]$ that take values in the divisible hull $\Gamma_{\mathbb{Q}}$ of $\Gamma = v(K^{\times})$. The set $\mathcal{T}$ parametrizes the equivalence classes of commensurable extensions of v to $K[x]$ and has a natural partial ordering.

All valuations on $K[x]$ with non-trivial support are maximal elements of $\mathcal{T}$, while valuations strictly below such maximal elements are precisely the residue-transcendental extensions of v to $K[x]$. We observe that for each $F \in \mathrm{Irr}(K)$, there is at least one valuation $\nu \in \mathcal{T}$ with support $FK[x]$. We think of all the $\mu \in \mathcal{T}$ with $\mu \leq \nu$ as "approaching" the irreducible polynomial F.

In **Section 2**, we introduce the graded ring $\mathcal{G}_\mu$ of a valuation μ on $K[x]$. The ring $\mathcal{G}_\mu$ comes equipped with a natural mapping $\mathrm{in}_\mu : K[x] \longrightarrow \mathcal{G}_\mu$ whose image is the set of homogeneous elements of $\mathcal{G}_\mu$. A key polynomial is an element of $K[x]$ whose image in $\mathcal{G}_\mu$ is a prime element and satisfies some additional properties. The set of key polynomials for a valuation μ on $K[x]$ is denoted $\mathrm{KP}(\mu)$. A key polynomial $\phi \in \mathrm{KP}(\mu)$ allow us to augment μ to a valuation ν with $\mu < \nu$ by prescribing the value ν takes on a ϕ.

Next, we turn to the study of algebraic properties of the ring $\mathcal{G}_\mu$. The main property of interest for us, is that the ring $\mathcal{G}_\mu$ has unique factorization for homogeneous elements. Another important property is that if $\mathrm{KP}(\mu) \neq \emptyset$, the ring $\mathcal{G}_\mu$ is a polynomial ring; $\mathcal{G}_\mu = \mathcal{G}_\mu^0[Y]$, where $\mathcal{G}_\mu^0$ is the subring of $\mathcal{G}_\mu$ generated by all the units and Y is the image of a key polynomial of minimal degree.

A characterization of units of $\mathcal{G}_\mu$ then leads to the definition of certain residual polynomial operators $R : K[x] \longrightarrow \kappa[y]$ where $\kappa \subset \mathcal{G}_\mu^0$ is a finite extension of the residue field k of (K, v). Crucially, these operators allows us to find the prime factorization $\mathrm{in}_\mu(f)$ in practice; they reduce the problem of working with $\mathcal{G}_\mu$ to working with a polynomial ring over a finite extension of the residue field. Moreover, these operators also help us determine the whole of $\mathrm{KP}(\mu)$.

The algebraic structure of $\mathcal{G}_\mu$ is related to the structure of the partially ordered set $\mathcal{T}$ via tangent directions. Namely, if $\mu < \nu$ are two valuations in $\mathcal{T}$, the tangent direction $\mathbf{t}(\mu, \nu) \subset K[x]$, defined purely in terms of the values μ and ν take on $K[x]$, consists of key polynomials. The set of key polynomials, $\mathrm{KP}(\mu)$, is the union of all tangent directions $\mathbf{t}(\mu, \nu)$ where $\mu < \nu$.

We spend the rest of this section reviewing the definitions and basic properties of augmentations and state some consequences of a celebrated structure theorem for valuations on $K[x]$. In order to state our results in full generality, we introduce limit key polynomials $\mathrm{KP}_\infty(\mu)$ and limit augmentations. The structure theorem implies the every $\mu \in \mathcal{T}$ that is residue-transcendental or has non-trivial support is the end node of a finite

sequence of augmentations (each augmentation being either ordinary or limit)

$$v \longrightarrow \mu_0 \longrightarrow \mu_1 \longrightarrow \ldots \longrightarrow \mu_r \longrightarrow \mu_{r+1} = \mu.$$

where μ_0 is always some especially easy to describe "depth-zero" extension of v to $K[x]$. Imposing certain technical conditions on these chains of augmentations ensures that they are almost unique for a given $\mu \in \mathcal{T}$. The resulting chains are called MLV chains. Their existence provides the theoretical basis for working with valuations on $K[x]$ on a computer. Inductive valuations are defined as valuations that admit an MLV chain where all the augmentations are ordinary.

In **Section 3** we start with an overview of Newton polygons. These polygons display information about algebraic relationships in $\mathcal{G}_\mu$ that could otherwise be difficult to write down concisely. They are also important for computational purposes; if $\mu \longrightarrow \nu$ is an ordinary augmentation, then the value $\nu(f)$ can be straightforwardly calculated from the Newton polygon of f. We then define principal Newton polygons, which are well behaved with respect to products of polynomials leading to a sufficient criterion for a $g \in K[x]$ to be reducible.

We continue with an overview of the henselian property. A valued field (K, v) is henselian if v extends uniquely to the algebraic closure of K. We make precise how every valued field (K, v) embeds into a "smallest" henselian field extension $(K, v) \subset (K^h, v^h)$ called the henselization. We note that extensions of v to a finite simple extension $K[x]/(F)$ where $F \in \mathrm{Irr}(K)$ are in bijection with the irreducible factors of F over the henselization K^h.

Assuming from now that (K, v) is henselian, each $F \in \mathrm{Irr}(K)$ is identified with the unique element $v_F \in \mathcal{T}$ given by

$$v_F(g) = \overline{v}(g(\theta)), \qquad \text{for all } g \in K[x],$$

where θ is any root of g in an algebraic closure $\overline{K}$ of K and $\overline{v}$ is the unique extension of v to $\overline{K}$. We present a certain "generalisation of Hensel's lemma" that completely characterizes the relation $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(F)$, where $\phi \in \mathrm{KP}(\mu)$ and $F \in \mathrm{Irr}(K)$ in terms of tangent directions. The theorem also shows that some important algebraic invariants can be read off from the Newton polygon $N_{\mu,\phi}(F)$. One important consequence of the generalisation of Hensel's lemma is that for all $F \in \mathrm{Irr}(K)$ the image of F in the graded ring, $\mathrm{in}_\mu(F) \in \mathcal{G}_\mu$ is either a unit or a prime power.

Next, we show that the set of monic irreducible polynomials over a henselian field forms an ultrametric space. The distance function $u : \mathrm{Irr}(K) \times \mathrm{Irr}(K) \longrightarrow \Gamma_{\mathbb{Q}} \infty$, $u(F, G) = v_F(G)/\deg(G)$ is given by a classical formula that involves only the resultant and the valuation v. We now view a $g \in K[x]$ as the set of its distinct monic irreducible factors and introduce a certain constant, $r(g) \in \Gamma_{\mathbb{Q}}$, called the radius of separation. It has the following property. A $\phi \in \mathrm{Irr}(K)$ that is closer than $r(g)$ to some irreducible factor of g, is closest to a unique irreducible factor of g. The radius of separation satisfies $r(g) \leq \mathrm{kras}(g)$, where $\mathrm{kras}(g)$ is Krasner's constant of g. We also derive an effective bound on Krasner's constant of monic, separable $g \in K[x]$.

Finally, we consider the (henselian) defect of a finite extension of valued fields and define defectless polynomials. These polynomials turn out to be precisely the key polynomials of inductive valuations. Another characterization of defectless polynomials is by using certain sets of weighted values which are related to the ultrametric u. This has consequences for how close a $\phi \in \mathrm{Irr}(K)$ "can get" to a defectless $F \in \mathrm{Irr}(K)$ if $\deg(\phi) < \deg(F)$. Namely there exists a constant $\delta(F) \in \Gamma_{\mathbb{Q}}$ such that $u(F, \phi) > \delta(F)$ implies $\deg(\phi) \geq \deg(F)$.

In **Section 4**, we prove some technical results on how types (μ, ϕ), μ residue-transcendental and ϕ and $\phi \in \mathrm{KP}(\mu)$, "see" some irreducible factors $G \in \mathrm{Irr}(K)$ of a square-free polynomial $g \in K[x]$ via the relation $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(G)$.

We then show how a list of types that sees all the irreducible factors of g can be "refined" by performing ordinary augmentations. The motivation being that after a finite number of strict refinements, we will reach a list of types where each type sees a unique irreducible factor of g.

We then give algorithms based on these results to factorize monic, square-free $g \in K[x]$. These "factorizations" are up to a quality parameter $\gamma \in \Gamma_{\mathbb{Q}}$, which can be taken to be arbitrarily large. A pivotal role in these algorithms is played by residual polynomial operators, whose computation facilitates the refinement steps.

Next, we state the best known conditions under which these algorithms can be implemented. We then prove termination for square-free $g \in K[x]$ whose irreducible factors are defectless, subject to the following condition. We require that the value group $\Gamma := \Gamma_v$ contains no infinite strictly increasing bounded sequences. We also show that when this condition is satisfied, every separable polynomial is defectless. We conclude by giving an algorithm to find the splitting field of separable $g \in K[x]$.

1 Valuations and their extensions

1.1 Basic definitions and results about valuations

Let $(G, +, 0)$ be an abelian group and $\leq$ a binary relation on G such that for all $a, b, c \in G$

(1) $a \leq a$ (reflexive)
(2) $a \leq b$ and $b \leq a$ implies $a = b$ (antisymmetric)
(3) $a \leq b$ and $b \leq c$ implies $a \leq c$ (transitive)
(4) $a \leq b$ or $b \leq a$ (total)
(5) $a \leq b$ implies $a + c \leq b + c$ (addition invariant).

We say that $\leq$ is an **ordering** on G, and that $(G, \leq)$ is an **ordered abelian group**. We say G is an ordered abelian group when it is clear from context which ordering $\leq$ on G we are considering. For $a, b \in G$ we write $a < b$ when $a \leq b$ and $a \neq b$.

It is easy to show, by adding a strictly positive element to itself, that ordered abelian groups are torsion-free.

Let G be an ordered abelian group and consider the set $G \cup \{\infty\}$, where ∞ is a symbol. We extend the group law and ordering on G via the rules $\infty + a = a + \infty = \infty + \infty = \infty,\ a \leq \infty$ for all $a \in G$. We use the notation $G\infty := G \cup \{\infty\}$. All $a \in G$ satisfy $a < \infty$, so ∞ is the unique maximal element of $G\infty$.

In this thesis **ring** means commutative ring with unity $1 \neq 0$. If R is a field, we denote the set of all monic irreducible polynomials over R by $\mathrm{Irr}(R)$.

Definition 1.1. *Let R be a ring and G an ordered abelian group. A **valuation** on R with values in G is a mapping $\nu : R \longrightarrow G\infty$ with the following properties.*

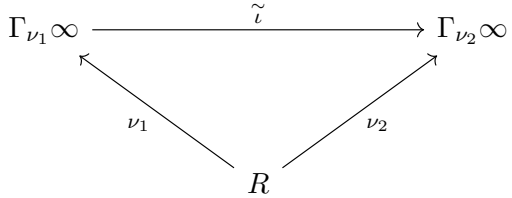
(1) $\nu(ab) = \nu(a) + \nu(b)$ for all $a, b \in R$.
(2) $\nu(a + b) \geq \min\{\nu(a),\ \nu(b)\}$ for all $a, b \in R$.
(3) $\nu(1) = 0$ and $\nu(0) = \infty$.

The set $\mathrm{supp}(\nu) := \{a \in R \mid \nu(a) = \infty\}$ is called the **support** of ν. The **value group** of ν is the subgroup of G generated by $\{\nu(a) \mid a \in R \backslash \mathrm{supp}(\nu)\}$, and is denoted by Γ_ν.

It is easy to see that the support of ν is a prime ideal of R.

Let $(G, \leq), (H, \leq')$ be two ordered abelian groups. We say that a group homomorphism $f : G \longrightarrow H$ is **order-preserving** if for all $a, b \in G$ we have $a \leq b \Longrightarrow f(a) \leq' f(b)$.

Definition 1.2. *Let ν_1, ν_2 be two valuations on a ring R. We say that ν_1 is **equivalent** to ν_2, and write $\nu_1 \sim \nu_2$, if there exists an order-preserving isomorphism $\iota : \Gamma_{\nu_1} \longrightarrow \Gamma_{\nu_2}$ of their value groups such that*



commutes, where $\widetilde{\iota}$ *is the extension of* ι *to a mapping* $\Gamma_1\infty \longrightarrow \Gamma_2\infty$ *that has* $\infty \mapsto \infty$.

Note that if $\nu_1 \sim \nu_2$, then $\operatorname{supp}(\nu_1) = \operatorname{supp}(\nu_2)$. We identify equivalent valuations unless stated otherwise.

Definition 1.3. *Let* R *be a ring* $S \subset R$ *a subring. A valuation* ν *on* R *restricts to a valuation* $\mu := \nu_{|S}$ *on* S. *We say that* ν *is an* ***extension*** *of* μ *and use the notation* ν/μ.

We have $\operatorname{supp}(\mu) \subset \operatorname{supp}(\nu)$ and $\Gamma_\mu \subset \Gamma_\nu$ in this case.

Let R be a ring and ν a valuation on R. The quotient ring $R/\operatorname{supp}(\nu)$ is a domain because the support is a prime ideal. We have canonical ring homomorphisms

$$R \twoheadrightarrow R/\operatorname{supp}(\nu) \hookrightarrow \operatorname{Frac}(R/\operatorname{supp}(\nu)). \tag{1}$$

Denote $K := \operatorname{Frac}(R/\operatorname{supp}(\nu))$ and for $a \in R$ write $\mathbf{a}$ for the image of a in K. Let $\overline{\nu}$ be the mapping given by

$$\overline{\nu}(\mathbf{a}) = \nu(a), \quad \overline{\nu}\big(\frac{\mathbf{a}}{\mathbf{b}}\big) = \overline{\nu}(\mathbf{a}) - \overline{\nu}(\mathbf{b}), \quad \text{for all } \mathbf{a}, \mathbf{b} \in K, \mathbf{b} \neq 0$$

The mapping $\overline{\nu}$ is a valuation with $\operatorname{supp}(\overline{\nu}) = \{0\}$ (since K is a field) and $\Gamma_{\overline{\nu}} = \Gamma_\nu$.

Observe that the composition Eq. (1) is injective if and only if $\operatorname{supp}(\nu) = \{0\}$. In this case, we have $R \hookrightarrow K$ and $\overline{\nu}/\nu$ is an extension of valuations. In particular if R is a field, we have $R = K$ and $\overline{\nu} = \nu$.

If K is an arbitrary field and ν a valuation on K, the **valuation ring** of ν is defined to be $\mathcal{O}_\nu := \{a \in K \mid \nu(a) \geq 0\}$ and the **maximal ideal** of ν is defined to be $\mathfrak{m}_\nu := \{a \in K \mid \nu(a) > 0\}$. It is easy to show using the definition, that $\mathcal{O}_\nu \subset K$ is a local ring whose maximal ideal is $\mathfrak{m}_\nu$. The **residue field** of ν is $k_\nu := \mathcal{O}_\nu/\mathfrak{m}_\nu$.

Definition 1.4. *In general, if* ν *is a valuation on a ring* R, *we define the valuation ring, maximal ideal and residue field of* ν *to be the corresponding objects for the induced valuation* $\overline{\nu}$ *on* $K := \operatorname{Frac}(R/\operatorname{supp}(\nu))$. *We abuse notation, following conventions in the literature, and write* $\mathcal{O}_\nu := \mathcal{O}_{\overline{\nu}}$, $\mathfrak{m}_\nu := \mathfrak{m}_{\overline{\nu}}$ *and* $k_\nu := k_{\overline{\nu}}$ *for these objects respectively.*

Remark 1.5. *In this thesis we will only consider valuations on a field or a polynomial ring over a field.*

In this case equivalence of valuations can be characterized in terms of support and valuation rings.

Lemma 1.6. *Let* K *be a field and* $K[x]$ *the polynomial ring over* K. *The following hold.*

(1) If v_1, v_2 *are two valuations on* K, *then* $v_1 \sim v_2$ *if and only if* $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.
(2) If ν_1, ν_2 *are two valuations on* $K[x]$, *then* $\nu_1 \sim \nu_2$ *if and only if* $\operatorname{supp}(\nu_1) = \operatorname{supp}(\nu_2)$ *and* $\mathcal{O}_{\nu_1} = \mathcal{O}_{\nu_2}$.

Proof. (1) [10, Proposition 2.1.3].

(2) By considering an order-preserving isomorphism as in Definition 1.2, the condition $\nu_1 \sim \nu_2$ implies that for all $f, g \in K[x]$, we have $\nu_1(f) \geq \nu_1(g) \iff \nu_2(f) \geq \nu_2(g)$. We

already know that $\text{supp}(\nu_1) = \text{supp}(\nu_2) =: \mathfrak{p}$ by definiton of equivalence. Let $\mathbf{f}, \mathbf{g} \in K[x]/\mathfrak{p},\ \mathbf{g} \neq 0$, then clearly $\mathbf{f}/\mathbf{g} \in \mathcal{O}_{\nu_1} := \mathcal{O}_{\overline{\nu_1}}$ if and only if $\nu_1(f) \geq \nu_1(g)$ if and only if $\mathbf{f}/\mathbf{g} \in \mathcal{O}_{\nu_2}$.

Conversely, $\overline{\nu_1}$ and $\overline{\nu_2}$ are valuations on the same field. As $\overline{\nu_1} \sim \overline{\nu_2}$ by Item (1) of Lemma 1.6, there exists an order preserving isomorphism $\iota : \Gamma_{\overline{\nu_1}} \longrightarrow \Gamma_{\overline{\nu_2}}$ as in Definition 1.2. Since $\Gamma_{\overline{\nu_i}} = \Gamma_{\nu_i}$ for $i = 1, 2$, by composing with $K[x] \twoheadrightarrow K[x]/\mathfrak{p} \hookrightarrow \text{Frac}(K[x]/\mathfrak{p})$, where $\mathfrak{p} := \text{supp}(\overline{\nu_1}) = \text{supp}(\overline{\nu_2})$, we observe that ι is an order-preserving isomorphism as in Definition 1.2 for the pair ν_1, ν_2 as well, and hence $\nu_1 \sim \nu_2$. □

Remark 1.7. *Note that (2) is clearly valid for arbitrary rings R, not just those of the form $R = K[x]$.*

We recall some definitions and results about valuations on fields.

Let K be a field and v a valuation on K, then we say that (K, v) is a **valued field**. Note that the function, $v(0) = \infty$ and $v(a) = 0$ for all non-zero $a \in K$, is a valuation on K with value group $\Gamma_v = \{0\}$.

We say that a valuation v on a field K is **trivial** if Γ_v is the trivial group.

It is clear that all trivial valuations on K are equivalent and given as above. The corresponding statement does not hold if Γ_v is not the trivial group.

Let (K, v) be a valued field. It is easy to see that each non-zero $a \in K$ satisfies $a \in \mathcal{O}_v$ or $1/a \in \mathcal{O}_v$. This implies $K = \text{Frac}(\mathcal{O}_v)$.

Definition 1.8. *We say that a subring $\mathcal{O}$ of a field K is a **valuation ring of** K if each non-zero $a \in K$ satisfies $a \in \mathcal{O}$ or $1/a \in \mathcal{O}$.*

Clearly, the valuation ring of v is a valuation ring of K. The following proposition collects some well-known facts about valuation rings, proofs can be found in any standard reference.

Proposition 1.9. *Let K be a field and $\mathcal{O} \subset K$ a valuation ring of K. The following hold.*

(1) $\mathcal{O}$ is a local ring.
(2) $\mathcal{O}$ is integrally closed.
(3) There exists a valuation v on K such that $\mathcal{O} = \mathcal{O}_v$.

The next proposition shows that, up to equivalence, valuations and valuation rings are essentially the same objects.

Proposition 1.10. *Let K be a field. The mapping $v \mapsto \mathcal{O}_v$ is a bijection*

$$\{v \text{ is a valuation on } K\}/\sim \longleftrightarrow \{\mathcal{O} \mid \mathcal{O} \text{ is a valuation ring of } K\}.$$

Proof. The mapping is well-defined and injective by Lemma 1.6, and surjective by Item (3) of Proposition 1.9. □

We now want to show that each (non-trivial) valuation on a subfield $K \subset L$ can be extended to a (non-trivial) valuation on L. This follows from the well-known Chevalley's theorem.

Theorem 1.11. *[10, Theorem 3.1.1] Let L be a field, $R \subset L$ a subring, and $\mathfrak{p} \subset R$ a prime ideal. Then there exists a valuation ring $\mathcal{O}$ of L that satisfies*

$$R \subset \mathcal{O} \quad \textit{and} \quad \mathfrak{m} \cap R = \mathfrak{p},$$

where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$.

Definition 1.12. *If (L, w) and (K, v) are valued fields such that L/K is a field extension and $w_{|K} = v$, we say (L, w) is an **extension of** (K, v). We use the notation $(K, v) \subset (L, w)$.*

Note that (L, w) being an extension of (K, v) is equivalent to $\mathcal{O}_w \cap K = \mathcal{O}_v$.

Proposition 1.13. *Let (K, v) be a valued field and L/K a field extension, then there exists a valuation w on L such that $w_{|K} = v$. Moreover, if v is non-trivial, then w is non-trivial.*

Proof. By applying Theorem 1.11 with $R = \mathcal{O}_v$ and $\mathfrak{p} = \mathfrak{m}_v$, we obtain a valuation ring $\mathcal{O}$ of L with $K \cap \mathcal{O} = \mathcal{O}_v$. Let $w : L \longrightarrow L^\times/\mathcal{O}^\times \infty$ be the *canonical valuation of* $(L, \mathcal{O})$; the valuation constructed in proof of [10, Proposition 2.1.12]. Since the canonical valuation of $(K, \mathcal{O}_v)$ is equivalent to v, we get an order preserving isomorphism $\Gamma_v \xrightarrow{\sim} K^\times/\mathcal{O}_v^\times$, which induces an order preserving injection $\Gamma_v \hookrightarrow L^\times/\mathcal{O}^\times$, hence $w_{|K} = v$.

If Γ_v is not trivial, then $\{0\} \subsetneq \Gamma_v \subset \Gamma_w$, so Γ_w is not trivial either. □

Definition 1.14. *We define the **ramification index**, $e(w/v)$, and **residue degree**, $f(w/v)$, of the extension w/v as*

$$e(w/v) = (\Gamma_w : \Gamma_v), \qquad f(w/v) = [k_w : k_v].$$

*If $e(w/v)$ or $f(w/v)$ are not finite, we denote $e(w/v) = \infty$ and $f(w/v) = \infty$, respectively. If $e(w/v) = f(w/v) = 1$, we say that w/v is **immediate**.*

Remark 1.15. *The above quantities are clearly multiplicative in towers.*

We will now define the notions of rank and rational rank, and finish this section by stating the well-known Abhyankar's inequality Theorem 1.23, that relates some invariants of an extension of valued fields.

Let G be an abelian group (not necessarily torsion-free), we define the **divisible hull of** G to be $G_{\mathbb{Q}} := G \otimes_{\mathbb{Z}} \mathbb{Q}$.

The divisible hull is a $\mathbb{Q}-$vector space in an obvious way and this vector space structure is unique.

Definition 1.16. *The **rational rank** of G, denoted* $\mathrm{rr}(G)$*, is defined to be* $\dim_{\mathbb{Q}}(G_{\mathbb{Q}})$.

Observe that the rational rank of G coincides with the maximal number (finite or infinite) of elements of G that are linearly independent over $\mathbb{Z}$. In particular, if G is finitely generated, it has finite rational rank.

Note that in general, we have $\mathrm{rr}(G) = 0$ if and only if G is a torsion group.

Now assume that G is torsion-free, then the natural homomorphism $g \mapsto g \otimes 1$ is injective, so $G \subset G_{\mathbb{Q}}$ via this map, which justifies the name "divisible hull" in our context. It is easy to check that each element of $G_{\mathbb{Q}}$ is of the form $g \otimes \frac{1}{n}$ where $n > 0$ is a positive integer. So, we may think of elements of $G_{\mathbb{Q}}$ as fractions with numerators in G and denominators in $\mathbb{N}$ that follow usual rules for addition and equality.

The divisible hull of a torsion-free abelian group G is the smallest divisible group containing G in the following sense.

Proposition 1.17. *If H is a divisible group that is torsion-free and $i : G \hookrightarrow H$ is an injective homomorphism, then there exists a unique injective homomorphism $G_{\mathbb{Q}} \hookrightarrow H$ such that i coincides with the composition*

$$G \hookrightarrow G_{\mathbb{Q}} \hookrightarrow H.$$

Proof. Since H is divisible and torsion-free, for each positive integer n and each $h \in H$ there is a unique element $y \in H$ that satisfies $ny = h$. We use the notation $\frac{h}{n} := y$.

Recall that each element of $G_{\mathbb{Q}}$ can be written $g \otimes \frac{1}{m}$ for $g \in G, m \in \mathbb{N}$.

Denote $i_1 : G \hookrightarrow G_{\mathbb{Q}}$, $g \mapsto g \otimes 1$ and let $i_2 : G_{\mathbb{Q}} \longrightarrow H$ be the mapping $g \otimes \frac{1}{n} \mapsto \frac{i(g)}{n}$. Clearly i_2 is a well defined injective homomorphism and we have $i_2 \circ i_1 = i$. Uniqueness of i_2 follows by the universal property of tensor product. □

The next result shows that taking the divisible hull of an ordered abelian group behaves well with respect to extensions of orderings.

Proposition 1.18. *Let $(G, \leq)$ be an ordered abelian group and let $G_{\mathbb{Q}} := G \otimes_{\mathbb{Z}} \mathbb{Q}$ be its divisible hull, then there exists a unique extension of the ordering $\leq$ to $G_{\mathbb{Q}}$.*

Proof. Recall that each element of $G_{\mathbb{Q}}$ can be written $g \otimes \frac{1}{m}$ for $g \in G, m \in \mathbb{N}$.

It is easy to check that the binary relation $\leq_1$ on $G_{\mathbb{Q}}$ given by

$$g \otimes \frac{1}{m} \leq_1 g' \otimes \frac{1}{n} \Longleftrightarrow ng \leq mg'$$

does not depend on the representations of $g \otimes \frac{1}{m}$ and $g' \otimes \frac{1}{n}$. Moreover, $\leq_1$ is an ordering on $G_{\mathbb{Q}}$ that coincides with $\leq$ on G, where G is viewed as a subgroup of $G_{\mathbb{Q}}$ via the inclusion $g \mapsto g \otimes 1$ and the inclusion is order preserving.

If $\leq_2$ is another extension of $\leq$ to $G_{\mathbb{Q}}$, clearly

$$g \otimes \frac{1}{m} \leq_2 g' \otimes \frac{1}{n} \Longleftrightarrow ng \otimes 1 \leq_2 mg' \otimes 1 \Longleftrightarrow ng \leq mg'$$

so $\leq_2$ coincides with $\leq_1$. □

So there is no danger of confusion when speaking of "the ordered-abelian group" $G_{\mathbb{Q}}$ for a given $(G, \leq)$.

Let $(G, \leq)$ be an ordered abelian group. We say that a subgroup $H \subset G$ is **convex** if it contains each interval whose endpoints lie in H. In other words H is convex if and only if for all $a, b \in H$, we have $\{a \leq g \leq b \mid g \in G\} =: [a, b]_G \subset H$. Denote by $\mathrm{Conv}(G)$ the set of all proper convex subgroups of G. It is easy to show that this set is totally ordered by inclusion.

Recall that two totally ordered sets $(S, \leq)$, $(T, \leq')$ are **order isomorphic** if there exists a bijective mapping $f : S \longrightarrow T$ such that for all $s, s' \in S$, we have $s \leq s' \Longrightarrow f(s) \leq' f(s')$. The **order type** of $(S, \leq)$ is its order isomorphisms class.

Definition 1.19. *The **rank** of G, denoted $\mathrm{rk}(G)$, is defined to be the order type of $\mathrm{Conv}(G)$.*

If G has finitely many proper convex subgroups, say n, we say that G **is of rank** n and write $\mathrm{rk}(G) = n$. This terminology is justified, because all totally ordered sets of cardinality n are order isomorphic. The corresponding statement does not hold for infinite totally ordered sets.

Proposition 1.20. *[10, Proposition 3.4.1] If G has finite rational rank, then G is of finite rank and we have*

$$\mathrm{rk}(G) \leq \mathrm{rr}(G).$$

Remark 1.21. *The inequality in the above result actually holds without any assumptions, but in this general case it is a more subtle statement about ordinals which we do not need for our purposes.*

Definition 1.22. *The rank and rational rank of a valuation are defined to be the rank and rational rank of its value group, respectively.*

The final result of this chapter implies that for an extension of valued fields, the transcendence degree of the induced residue field extension and "size increase" of the value group are controlled by the transcendence degree of the extension.

Theorem 1.23. *[10, Theorem 3.4.3] Let $(K, v) \subset (L, w)$ be an extension of valued fields, then*

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

1.2 Valuations on a polynomial ring

For a valuation μ on $K[x]$, denote the restriction of μ to K by v.

Theorem 1.24. *Every valuation μ on $K[x]$ is of exactly one of the following types.*

- ***Non-trivial support;*** $\mathrm{supp}(\mu) = FK[x]$ *for some $F \in \mathrm{Irr}(K)$, Γ_μ/Γ_v is a torsion group and the extension k_μ/k_v is algebraic.*

- ***Value-transcendental;*** $\operatorname{supp}(\mu) = 0$, Γ_μ/Γ_v *is not a torsion group and the extension* k_μ/k_v *is algebraic.*
- ***Residue-transcendental;*** $\operatorname{supp}(\mu) = 0$, Γ_μ/Γ_v *is a torsion group and the extension* k_μ/k_v *is transcendental.*
- ***Valuation-algebraic;*** $\operatorname{supp}(\mu) = 0$, Γ_μ/Γ_v *is a torsion group and the extension* k_μ/k_v *is algebraic.*

Proof. Observe that apriori μ could fall into one of 2^3 mutually exclusive cases according to $\operatorname{supp}(\mu)$ not/being trivial, Γ_μ/Γ_v not/being torsion and k_μ/k_v not/being algebraic.

Recall that $\overline{\mu}$ is a valuation on $L := \operatorname{Frac}(K[x]/\operatorname{supp}(\mu))$ that extends v and satisfies $\Gamma_{\overline{\mu}} = \Gamma_\mu$. The result will follow by applying Theorem 1.23 to the extension $(K, v) \subset (L, \overline{\mu})$.

Suppose $\operatorname{supp}(\mu)$ is non-trivial, then L/K is a (finite) algebraic extension, so $\operatorname{tr.deg}(L/K) = 0$ and we deduce that $\operatorname{rr}(\Gamma_\mu/\Gamma_v) = \operatorname{tr.deg}(k_\mu/k_v) = 0$ by Theorem 1.23, which is equivalent to k_μ/k_v algebraic and Γ_μ/Γ_v torsion; this eliminates 3 of the 8 cases.

If $\operatorname{supp}(\mu)$ is trivial, we have $L = K(x)$ so that $\operatorname{tr.deg}(L/K) = 1$, and we obtain $\operatorname{tr.deg}(k_\mu/k_v) + \operatorname{rr}(\Gamma_\mu/\Gamma_v) \leq 1$ by Theorem 1.23. Hence, it cannot happen that k_μ/k_v is transcendental and simultaneously Γ_μ/Γ_v is not torsion; this excludes the final case not found on our list and completes the proof. □

Valuations on $K[x]$ with Γ_μ/Γ_v a torsion group are sometimes called **commensurable** in the literature.

Let (K, v) be a valued field and Λ an ordered abelian group. Let $\mathcal{T} = \mathcal{T}(\Lambda)$ be the set of all valuations

$$\mu : K[x] \longrightarrow \Lambda\infty$$

whose restriction to K is v.

The set $\mathcal{T}$ admits a partial ordering. For $\mu, \nu \in \mathcal{T}$ define

$$\mu \leq \nu \text{ if and only if } \mu(f) \leq \nu(f) \text{ for all } f \in K[x].$$

We write $\mu < \nu$, when $\mu \leq \nu$ and $\mu \neq \nu$.

Abuse notation and denote the value group of v by $\Gamma := \Gamma_v$.

Remark 1.25. *In this thesis we will only consider the case* $\Lambda = \Gamma_{\mathbb{Q}}$. *From now on we denote* $\mathcal{T}(\Gamma_{\mathbb{Q}})$ *simply by* $\mathcal{T}$.

Proposition 1.26. *Let* μ *be a valuation on* $K[x]$ *that extends* v *such that* Γ_μ/Γ *is a torsion group. Then,* μ *is equivalent to an element of* $\mathcal{T}$. *Moreover, for all* $\mu, \mu' \in \mathcal{T}$

$$\mu \sim \mu' \iff \mu = \mu'.$$

Proof. Let μ be a valuation on $K[x]$ with Γ_μ/Γ a torsion group, then for each $\gamma \in \Gamma_\mu$ there exists some non-zero $n \in \mathbb{Z}$ depending on γ such that $n\gamma \in \Gamma$. It is easy to verify that $i : \Gamma_\mu \longrightarrow \Gamma_{\mathbb{Q}}$ given by $\gamma \mapsto n\gamma \otimes \frac{1}{n}$ is an injective order preserving homomorphism,

so the composition $\widetilde{i} \circ \mu$ is an element of $\mathcal{T}$, where $\widetilde{i}$ is the extension of i to a mapping $\Gamma_\mu \infty \longrightarrow \Gamma_{\mathbb{Q}} \infty$ that has $\infty \mapsto \infty$. We have $\mu \sim \widetilde{i} \circ \mu$ by construction.

We only need to show ($\Longrightarrow$).

Let $\mu, \mu' \in \mathcal{T}$, suppose $\mu \sim \mu'$ and let $\iota : \Gamma_\mu \longrightarrow \Gamma_{\mu'}$ be an order preserving isomorphism as in Definition 1.2. Since μ and μ' agree with v on K, the restriction of ι to Γ is the identity, let us show that this implies ι is the identity. Since $\Gamma_{\mathbb{Q}}/\Gamma$ is torsion and $\Gamma_\mu \subset \Gamma_{\mathbb{Q}}$, the group Γ_μ/Γ is torsion too, so for each $\gamma \in \Gamma_\mu$ there exists some non-zero $n \in \mathbb{Z}$ depending on γ such that $n\gamma \in \Gamma$. Hence $n\iota(\gamma) = \iota(n\gamma) = n\gamma$, which implies $n(\iota(\gamma) - \gamma) = 0$ from which the desired claim follows because $\Gamma_{\mathbb{Q}}$ is torsion-free. □

Therefore the set $\mathcal{T}$ parametrizes the equivalence classes of commensurable extensions of v to $K[x]$. Moreover, the notions "equivalent" and "equal" coincide within this set.

Remark 1.27. *In [14] a certain universal ordered group extension $\Gamma \hookrightarrow \mathbb{R}^{\mathbb{I}}_{\text{lex}}$ is constructed, where $\mathbb{I}$ is an ordered set that depends on* $\text{Conv}(\Gamma)$*, and the study of $\mathcal{T}(\mathbb{R}^{\mathbb{I}}_{\text{lex}})$ in [2] leads to a parametrization of all valuations on $K[x]$ whose restriction to K is equivalent to v.*

Recall that an element ν of a partially ordered set $\mathcal{T}$ is a **maximal element** of $\mathcal{T}$ if whenever $\nu \leq \mu$ for some $\mu \in \mathcal{T}$, then $\mu = \nu$.

Lemma 1.28. *Let $\nu \in \mathcal{T}$, then*

$$\nu \text{ has non-trivial support } \Longrightarrow \nu \text{ is a maximal element of } \mathcal{T}.$$

Proof. Let $\mu, \nu \in \mathcal{T}$, suppose ν has non-trivial support and $\nu \leq \mu$. Since non-zero prime ideals of $K[x]$ are maximal, we have $\text{supp}(\mu) = \text{supp}(\nu) =: \mathfrak{p}$ and hence, the valuations $\overline{\nu}, \overline{\mu}$ are extensions of v to the algebraic extension $L := \text{Frac}(K[x]/\mathfrak{p})$ that satisfy $\overline{\nu}(\alpha) \leq \overline{\mu}(\alpha)$ for all $\alpha \in L$. This shows $\mathcal{O}_{\overline{\nu}} \subset \mathcal{O}_{\overline{\mu}}$ and we deduce $\mathcal{O}_{\overline{\nu}} = \mathcal{O}_{\overline{\mu}}$ by [10, Lemma 3.2.8] (the valuation rings $\mathcal{O}_{\overline{\mu}}, \mathcal{O}_{\overline{\nu}}$ lie over $\mathcal{O}_v$). This shows, $\overline{\mu} \sim \overline{\nu}$, which implies $\overline{\mu} = \overline{\nu}$ by Proposition 1.26 and hence $\mu = \nu$ as required. □

The non-maximal elements can be characterized as follows.

Theorem 1.29. *Let $\mu \in \mathcal{T}$. The following are equivalent.*

(1) μ is not a maximal element of $\mathcal{T}$.
(2) μ is residue-transcendental.

Proof. A $\mu \in \mathcal{T}$ is a maximal element of $\mathcal{T}$ if and only if μ is valuation-algebraic or μ has non-trivial support by [20, Theorem 2.3] and Theorem 2.8. Hence a $\mu \in \mathcal{T}$ is not a maximal element of $\mathcal{T}$ if and only if μ is residue-transcendental by Theorem 1.24 using the fact that Γ_μ/Γ_v is a torsion group. □

Remark 1.30. *Combining Theorem 1.29 with Proposition 1.26 shows that the residue-transcendental extensions of v to $K[x]$ "are" precisely the non-maximal elements of $\mathcal{T}$.*

2 New valuations from a given one

2.1 Rings graded by ordered abelian groups

Let $(G, \leq)$ be an ordered abelian group.

If a ring R is a direct sum of additive subgroups R_g which satisfy $R_g R_h \subset R_{g+h}$ for all $g, h \in G$, then R is a $G-$**graded ring** and the direct sum decomposition $R = \bigoplus_{g \in G} R_g$ is called a **grading** of R by G. If an $r \in R$ is contained in some R_g it is called a **homogeneous element**. The subgroup R_0 is clearly a subring of R.

Each non-zero homogeneous element $r \in R_g$ is a **homogeneous element of grade** g, which we denote by $\mathrm{gr}(r) = g$.

Since the R_g are abelian groups, we have $0 \in R_g$ for all $g \in G$; hence the grade of the homogeneous element 0 is not defined.

If $r, s \in R$ are two homogeneous elements, their product is a homogeneous element, and if $rs \neq 0$, we have $\mathrm{gr}(rs) = \mathrm{gr}(r) + \mathrm{gr}(s)$. The direct sum decomposition of R implies that every element $r \in R$ is uniquely a sum $r = \sum_{g \in G} r_g$ where $r_g \in R_g$ and $r_g = 0$ for all but finitely many $g \in G$. In this case each non-zero r_g is called the **homogeneous component** of r of grade g.

The following construction is a source of examples of $G-$graded rings. Suppose that for each $g \in G$, we are have an abelian group R_g such that R_0 is a ring and for each pair $g, h \in G$ we have maps $R_g \times R_h \longrightarrow R_{g+h}$ that are associative and R_0-bilinear. Then, the abelian group

$$R = \bigoplus_{g \in G} R_g$$

has a natural multiplication operation given by

$$\Big(\sum_{g_1 \in G} r_{g_1} \Big) \Big(\sum_{g_2 \in G} s_{g_2} \Big) := \sum_{g_3 \in G} \Big(\sum_{g_1 + g_2 = g_3} r_{g_1} s_{g_2} \Big) \tag{2}$$

which makes R into a ring, graded by G in the obvious way.

Remark 2.1. *All definitions and results above depend on the structure of G as a commutative monoid, not on the ordering $\leq$.*

2.2 Graded ring of a valuation on a polynomial ring and key polynomials

Let μ be a valuation on $K[x]$. For each $\gamma \in \Gamma_\mu$, consider the abelian groups

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

and let $\mathcal{G}_\mu$ be the abelian group

$$\mathcal{G}_\mu = \bigoplus_{\gamma \in \Gamma_\mu} \mathcal{P}_\gamma / \mathcal{P}_\gamma^+.$$

Denote $\Delta_\mu = \mathcal{P}_0/\mathcal{P}_0^+$ and note that Δ_μ is a ring with multiplication given by

$$(f + \mathcal{P}_0^+)(g + \mathcal{P}_0^+) = fg + \mathcal{P}_0^+.$$

By "extending the multiplication" in the obvious way:

$$(f + \mathcal{P}_\gamma^+)(g + \mathcal{P}_\delta^+) = fg + \mathcal{P}_{\gamma+\delta}^+$$

we obtain associative $\Delta_\mu-$bilinear maps $\mathcal{P}_\gamma/\mathcal{P}_\gamma^+ \times \mathcal{P}_\delta/\mathcal{P}_\delta^+ \longrightarrow \mathcal{P}_{\gamma+\delta}/\mathcal{P}_{\gamma+\delta}^+$ for each pair $\gamma, \delta \in \Gamma_\mu$ which makes $\mathcal{G}_\mu$ into a ring with multiplication as in Eq. (2), graded by Γ_μ in the obvious way.

Definition 2.2. *We say that $\mathcal{G}_\mu$ is the **graded ring of** μ.*

The ring $\mathcal{G}_\mu$ comes naturally equipped with an **initial term mapping**

$$\mathrm{in}_\mu : K[x] \longrightarrow \mathcal{G}_\mu, \qquad \mathrm{in}_\mu(f) = \begin{cases} 0 & \text{if } f \in \mathrm{supp}(\mu) \\ f + \mathcal{P}_{\mu(f)}^+ & \text{otherwise} \end{cases}$$

Clearly $f \in K[x]$ satisfies $f \in \mathrm{supp}(\mu)$ if and only if $\mathrm{in}_\mu(f) = 0$. Therefore the set of non-zero homogeneous elements of $\mathcal{G}_\mu$ is

$$\mathcal{H}(\mathcal{G}_\mu) = \{\mathrm{in}_\mu(f) \mid f \in K[x] \backslash \mathrm{supp}(\mu)\}.$$

If $t \in \mathcal{H}(\mathcal{G}_\mu)$, the grade of t is $\mathrm{gr}(t) = \mu(f)$ for any $f \in K[x]$ such that $\mathrm{in}_\mu(f) = t$.

Lemma 2.3. *The mapping in_μ has the following properties for all $f, g \in K[x]$.*

(1) $\mathrm{in}_\mu(f)\,\mathrm{in}_\mu(g) = \mathrm{in}_\mu(fg)$.
(2) If $f, g \in K[x]\backslash\mathrm{supp}(\mu)$, then $\mathrm{in}_\mu(f) = \mathrm{in}_\mu(g)$ if and only if $\mu(f-g) > \mu(f) = \mu(g)$.
(3) If $\mu(f) > \mu(g)$, then $\mathrm{in}_\mu(f+g) = \mathrm{in}_\mu(g)$.
(4) If $\mu(f) = \mu(g) = \mu(f+g)$, then $\mathrm{in}_\mu(f+g) = \mathrm{in}_\mu(f) + \mathrm{in}_\mu(g)$.

Proof. Follows by definition in_μ and the defining properties of a valuation. □

Remark 2.4. *The ring $\mathcal{G}_\mu$ is an integral domain; indeed by the multiplicative property of in_μ there are no non-zero homogeneous zero divisors, so the corresponding statement holds for inhomogeneous elements by considering $st = 0$ for $s, t \in \mathcal{G}_\mu$ expressed as a sum of their homogeneous components.*

Actually, if G is an ordered abelian group and R is a $G-$graded ring, then every homogeneous component of a zero divisor is a zero divisor [24, Corollary 3.4].

Definition 2.5. *Let $f, g \in K[x]$. We say that f is $\mu-$equivalent to g if $\mathrm{in}_\mu(f) = \mathrm{in}_\mu(g)$. We write $f \sim_\mu g$ in this case.*

It is easy to see that the relation $\sim_\mu$ is an equivalence relation on $K[x]$.

Definition 2.6. *A $\phi \in K[x]$ is a **key polynomial** for μ if all the following hold.*

- ϕ *is* $\mu-$***irreducible****; the homogeneous element* $\text{in}_\mu(\phi)$ *is prime.*
- ϕ *is* $\mu-$***minimal****; if* $\text{in}_\mu(\phi) \mid \text{in}_\mu(f)$ *and* $f \neq 0$*, then* $\deg(\phi) \leq \deg(f)$*.*
- ϕ *is monic.*

The set of key polynomials for μ is denoted $\text{KP}(\mu)$. The equivalence relation $\sim_\mu$ restricts to an equivalence relation on the set $\text{KP}(\mu)$. For all $\phi \in \text{KP}(\mu)$, we denote its class by

$$[\phi]_\mu = \{Q \in \text{KP}(\mu) \mid \phi \sim_\mu Q\}.$$

Since all $Q \in [\phi]_\mu$ are $\mu-$minimal, all polynomials in $[\phi]_\mu$ have the same degree.

Let $\phi \in K[x]$ be a non-zero polynomial, then for each $f \in K[x]$ there exist uniquely determined $a_0, \ldots, a_r \in K[x]$ with $\deg(a_i) < \deg(\phi)$ for every i, $0 \leq i \leq r$, such that

$$f = a_0 + a_1\phi + \cdots + a_r\phi^r. \tag{3}$$

The expression is called **the** $\phi-$**expansion of** f.

Lemma 2.7. *Let* μ *be a valuation on* $K[x]$*, then the following hold.*

(1) Key polynomials are irreducible; that is $\text{KP}(\mu) \subset \text{Irr}(K)$.
(2) If $\text{KP}(\mu)$ *is non-empty, then* μ *has trivial support.*
(3) Let $\phi \in \text{KP}(\mu)$*, then for every* $f, g \in K[x]$ *with* $\deg(f) < \deg(\phi)$ *and* $\deg(g) < \deg(\phi)$*, if* $fg = q\phi + r$ *is the* $\phi-$*expansion of* fg*, then* $\mu(fg) = \mu(r) \leq \mu(q\phi)$*.*

Proof. (1)If $fg = \phi \in \text{KP}(\mu)$ for $f, g \in K[x]$ of strictly lower degree, then $\text{in}_\mu(\phi) \nmid \text{in}_\mu(f)$ and $\text{in}_\mu(\phi) \nmid \text{in}_\mu(g)$ because ϕ is $\mu-$minimal. This contradicts that $\text{in}_\mu(\phi)$ is a prime element.

(2)If $\phi \in \text{KP}(\mu)$ and $\text{supp}(\mu) = (G)$ for some $G \in \text{Irr}(K)$, then $G \neq \phi$ because $\text{in}_\mu(G) = 0$ is not a prime element. Hence, ϕ, G are co-prime so there exist non-zero $a, b \in K[x]$ such that $aG + b\phi = 1$ and we may assume $b \notin \text{supp}(\mu)$, because $\text{supp}(\mu)$ is a proper ideal. Hence $\infty = \mu(aG) > \mu(b\phi)$, so $\text{in}_\mu(1) = \text{in}_\mu(aG + b\phi) = \text{in}_\mu(b\phi)$, which implies $\text{in}_\mu(\phi)$ is a unit, contradiction. Hence $\text{supp}(\mu) = \{0\}$.

(3) [19, Lemma 2.6 (1)] □

The existence of key polynomials is characterized as follows.

Theorem 2.8. *[19, Theorem 4.4] Let* μ *be a valuation on* $K[x]$*. The following are equivalent.*

(1) $\text{KP}(\mu) = \emptyset$.
(2) Each non-zero homogeneous element of $\mathcal{G}_\mu$ *is a unit.*
(3) μ *has non-trivial support, or it is valuation-algebraic.*

Definition 2.9. *If* $\text{KP}(\mu) \neq \emptyset$*, we define the* ***degree*** *of* μ *as* $\deg(\mu) = \min\{\deg(Q) \mid Q \in \text{KP}(\mu)\}$*. A* $\phi \in \text{KP}(\mu)$ *that satisfies* $\deg(\phi) = \deg(\mu)$ *is said to be a* ***key polynomial of minimal degree for*** μ*.*

If $\text{supp}(\mu) = GK[x]$ *for some* $G \in \text{Irr}(K)$*, we define* $\deg(\mu) = \deg(G)$*.*

By Theorem 2.8, these definitions are independent.

Definition 2.10. *Let μ be a valuation on $K[x]$ and let $\phi \in K[x]\backslash K$. The map defined by*

$$\mu_\phi(f) = \min_{0\leq i\leq r}\{\mu(a_i\phi^i)\}$$

*for f in $K[x]$ as in Eq. (3) is called the **truncation** of μ by ϕ.*

The map μ_ϕ is not always a valuation, but it is useful for characterizing the property of being $\mu-$minimal.

Lemma 2.11. *[19, Proposition 2.3 (2)] A polynomial $\phi \in K[x]\backslash K$ is $\mu-$minimal if and only if $\mu = \mu_\phi$.*

The next result introduces an important numerical invariant of a valuation μ admitting key polynomials.

Theorem 2.12. *[19, Theorem 3.9] Let $\phi \in \mathrm{KP}(\mu)$, then each monic $f \in K[x]$ satisfies*

$$\frac{\mu(f)}{\deg(f)} \leq \frac{\mu(\phi)}{\deg(\phi)} =: \mathrm{wt}(\mu)$$

and equality holds if and only if f is $\mu-$minimal.

Proof. This slight reformulation of [19, Theorem 3.9], follows immediately by noting that all $\phi \in \mathrm{KP}(\mu)$ are monic and $\mu-$minimal. □

Remark 2.13. *In particular $\mu(\phi) = \mu(\phi')$ for all $\phi, \phi' \in \mathrm{KP}(\mu)$ with $\deg(\phi) = \deg(\phi')$.*

2.3 Structure of the graded ring

Throughout this section let μ be a valuation on $K[x]$ with $\mathrm{KP}(\mu) \neq \emptyset$. The main result of [19] implies that homogeneous elements of $\mathcal{G}_\mu$ possess unique factorization.

Theorem 2.14. *Each non-zero, non-unit homogeneous element of $\mathcal{G}_\mu$ is a product of homogeneous prime elements.*

Proof. By Theorem 2.8 and Theorem 1.24, μ is either value-transcendental or residue-transcendental. If μ is value-transcendental, the theorem follows by [19, Lemma 4.1] and [19, Theorem 4.2]. If μ is residue-transcendental, it follows from [19, Theorem 6.8]. □

Remark 2.15. *Since the factors are prime elements, the factorization is unique up to multiplication by units and re-ordering the factors.*

The proof of Theorem 2.14, also shows the following.

Theorem 2.16. *[2, cf. Theorem 2.5] Let $t \in \mathcal{G}_\mu$ be a homogeneous prime element, then there exists a $\phi \in \mathrm{KP}(\mu)$ and a homogeneous unit $u \in \mathcal{G}_\mu$ such that*

$$t = u \cdot \mathrm{in}_\mu(\phi).$$

Remark 2.17. *Hence, key polynomials are precisely the monic polynomials of minimal degree whose initial terms generate the principal homogeneous prime ideals of* $\mathcal{G}_\mu$.

An essential role in the proof of Theorem 2.14 is played by key polynomials of minimal degree. These key polynomials satisfy a stronger version of Item (3) of Lemma 2.7, below.

Theorem 2.18. *[19, Theorem 3.2] Let* $\phi \in \mathrm{KP}(\mu)$ *and suppose that* $\deg(\phi) = \deg(\mu)$. *Then for every* $f, g \in K[x]$ *with* $\deg(f) < \deg(\phi)$ *and* $\deg(g) < \deg(\phi)$, *if* $fg = q\phi + r$ *is the* $\phi-$*expansion of* fg, *then*

$$\mu(fg) = \mu(r) < \mu(q\phi).$$

Before we present some consequences of Theorem 2.18 for the structure of $\mathcal{G}_\mu$, we will show that each homogeneous element admits a "minimal expression" by discarding some terms of a $\phi-$expansion according to their $\mu-$value.

Definition 2.19. *Let* $\phi \in \mathrm{KP}(\mu)$. *For* $f \in K[x]$ *with* $\phi-$*expansion* $f = a_0 + \cdots + a_r\phi^r$, *we define*

$$S_{\mu,\phi}(f) = \{i \mid 0 \leq i \leq r,\ \mu(f) = \mu(a_i\phi^i)\}.$$

Lemma 2.20. *Let* f *in* $K[x]$ *and* $\phi \in \mathrm{KP}(\mu)$. *Then,*

$$\mathrm{in}_\mu(f) = \mathrm{in}_\mu\left(\sum_{i\in S} a_i\phi^i\right) = \sum_{i\in S} \mathrm{in}_\mu(a_i\phi^i)$$

where $S = S_{\mu,\phi}(f)$.

Proof. By Lemma 2.11, we have $\min\limits_{0\leq i\leq r}\{\mu(a_i\phi^i)\} = \mu(f)$, so $\mu(\sum_{i\notin S} a_i\phi^i) > \mu(f)$, which gives the first equality. The second equality follows by Item (4) of Lemma 2.3. □

Lemma 2.21. *[19, Lemma 2.10] Let* $\phi \in \mathrm{KP}(\mu)$ *and suppose* $f, g \in K[x]$ *satisfy* $\mathrm{in}_\mu(f) = \mathrm{in}_\mu(g)$, *then* $S_{\mu,\phi}(f) = S_{\mu,\phi}(g)$. *Moreover,* $\mathrm{in}_\mu(a_i) = \mathrm{in}_\mu(b_i)$ *for all* $i \in S_{\mu,\phi}(f)$, *where* $f = a_0 + \cdots + a_r\phi^r$ *and* $g = b_0 + \cdots + b_s\phi^s$ *are the* $\phi-$*expansions of* f *and* g.

We will now show that the ring $\mathcal{G}_\mu$ is a polynomial ring. Denote $n = \deg(\mu)$ and let $\mathcal{G}_\mu^0 \subset \mathcal{G}_\mu$ be the additive subgroup generated by the set

$$\{\mathrm{in}_\mu(f) \mid f \in K[x],\ \deg(f) < n\}.$$

Theorem 2.22. *[22, Proposition 4.2] The subgroup* $\mathcal{G}_\mu^0$ *is a subring of* $\mathcal{G}_\mu$ *and if* ϕ *is a key polynomial of minimal degree for* μ, *then the element* $Y := \mathrm{in}_\mu(\phi)$ *is transcendental over* $\mathcal{G}_\mu^0$ *and* $\mathcal{G}_\mu = \mathcal{G}_\mu^0[Y]$.

Proof. In order to show that $\mathcal{G}_\mu^0$ is a ring, we only need to show it is closed under multiplication, because it is already a subgroup. Denote $n = \deg(\mu)$. It is enough to show that for all $f, g \in K[x]$ with $\deg(f) < n$ and $\deg(g) < n$, we have $\mathrm{in}_\mu(f)\,\mathrm{in}_\mu(g) \in \mathcal{G}_\mu^0$.

Let $\phi \in \mathrm{KP}(\mu)$ be a key polynomial of minimal degree $\deg(\phi) = n$, let $f, g \in K[x]$ be such that $\deg(f) < n, \deg(g) < n$ and consider the $\phi-$expansion $fg = q\phi + r$. By Theorem 2.18, we deduce that $\mu(r) < \mu(q\phi)$ and hence $\mathrm{in}_\mu(fg) = \mathrm{in}_\mu(r) \in \mathcal{G}_\mu^0$.

Denote $Y := \mathrm{in}_\mu(\phi)$, to show $\mathcal{G}_\mu^0[Y] = \mathcal{G}_\mu$ it is enough to show that every homogeneous element of $\mathcal{G}_\mu$ belongs to $\mathcal{G}_\mu^0[Y]$, which follows at once by Lemma 2.20.

Suppose that Y satisfies an algebraic equation

$$t_0 + t_1 Y + \cdots + t_n Y^n = 0 \tag{4}$$

where $t_i \in \mathcal{G}_\mu^0$. We can assume $t_i = 0$ or $t_i = \mathrm{in}_\mu(f_i)$ with $\deg(f_i) < n$ and $\mu(f_i) < \infty$. Let

$$f = \sum_{i=0}^{n} f_i \phi^i.$$

By the assumption on the t_i's, Lemma 2.20 and the fact that $\mu_\phi = \mu$ we obtain

$$0 = \sum_{i \in S_{\mu,\phi}(f)} t_i Y^i = \mathrm{in}_\mu \left(\sum_{i \in S_{\mu,\phi}(f)} f_i \phi^i \right) = \mathrm{in}_\mu(f)$$

which shows that $t_i = 0$ for all $0 \leq i \leq n$. □

The above theorem shows that every element of $\mathcal{G}_\mu$ is a polynomial in $Y := \mathrm{in}_\mu(\phi)$ with coefficients in $\mathcal{G}_\mu^0$ and that this expression is unique for a fixed choice of $\phi \in \mathrm{KP}(\mu)$ of minimal degree.

Definition 2.23. *For non-zero $f \in K[x]$, we define the $\mu-$* ***degree*** $\deg_\mu(f) \in \mathbb{N}$ *as the degree of $\mathrm{in}_\mu(f)$ as a polynomial in $Y := \mathrm{in}_\mu(\phi)$ with coefficients in $\mathcal{G}_\mu^0$, for some $\phi \in \mathrm{KP}(\mu)$ of minimal degree.*

The quantity $\deg_\mu(f)$ does not depend on the choice of key polynomial of minimal degree, even though the coefficients of $\mathrm{in}_\mu(f)$ might.

Note that in general, we have $\max(S_{\mu,\phi}(f)) = \deg_\mu(f)$.

The homogeneous units are completely characterized as follows.

Lemma 2.24. *[19, Proposition 3.5] Let $f \in K[x]$ be non-zero, then the homogeneous element $\mathrm{in}_\mu(f)$ is a unit if and only if $\deg_\mu(f) = 0$.*

Therefore $\mathcal{G}_\mu^0$ is the subring of $\mathcal{G}_\mu$ generated by the set of homogeneous units.

Remark 2.25. *By [24, Lemma 5.1], every unit of $\mathcal{G}_\mu$ is a homogeneous element, so by Lemma 2.24, $\mathcal{G}_\mu^0$ is the subring of $\mathcal{G}_\mu$ generated by all the units of $\mathcal{G}_\mu$. Moreover, the relation "is associate to" preserves (in)homogeneity of elements.*

Definition 2.26. *For any valuation μ on $K[x]$, let $\Gamma_\mu^0 \subset \Gamma_\mu$ be the subgroup of grades of all homogeneous units in $\mathcal{G}_\mu$. The* ***relative ramification index*** *of μ is defined as*

$$e = e(\mu) = (\Gamma_\mu : \Gamma_\mu^0).$$

If μ is residue-transcendental, Γ_μ/Γ_v is a torsion group, so $(\Gamma_\mu : \Gamma_\mu^0)$ is finite. We have $\Gamma_\mu^0 = \{\mu(a) \mid a \in K[x], 0 \leq \deg(a) < \deg(\mu)\}$ by Lemma 2.24 and $\Gamma_\mu = \langle \Gamma_\mu^0, \mu(\phi)\rangle$ where $\phi \in \mathrm{KP}(\mu)$ is a key polynomial of minimal degree by Lemma 2.11. Hence $e := e(\mu)$ is the least positive integer such that $e\mu(\phi) \in \Gamma_\mu^0$.

2.4 Residual polynomial operators

Let μ be a residue-transcendental valuation on $K[x]$ and $\phi \in \mathrm{KP}(\mu)$ a key polynomial of minimal degree. Denote $Y := \mathrm{in}_\mu(\phi)$, then the non-zero coefficients of $\mathrm{in}_\mu(f) \in \mathcal{G}_\mu^0[Y]$ are homogeneous units by Lemma 2.24. The irreducible factorization of $\mathrm{in}_\mu(f) \in \mathcal{G}_\mu^0[Y]$ is the prime factorization of $\mathrm{in}_\mu(f)$ by Theorem 2.14.

The aim of this section is to show that this factorization can be found over a "small" subfield of $\mathcal{G}_\mu$ which is crucial for computational applications.

Denote by v the restriction of μ to K and observe that there is a canonical injection $k_v \hookrightarrow \Delta_\mu$ where $\Delta_\mu = \mathcal{P}_0/\mathcal{P}_0^+$ is the grade 0 part of $\mathcal{G}_\mu$.

Definition 2.27. *We define κ_μ to be the relative algebraic closure of k_v in Δ_μ.*

Clearly, κ_μ is a field because because k_v is. We denote $\kappa := \kappa_\mu$ when μ is clear from context.

Lemma 2.28. *The field κ_μ is contained in $\mathcal{G}_\mu^0$, satisfies $\kappa_\mu^\times = \Delta_\mu^\times$ and is explicitly given by $\kappa_\mu := \{\mathrm{in}_\mu(a) \mid a \in K[x], 0 \leq \deg(a) < \deg \mu, \mu(a) = 0\} \cup \{0\}$.*

Proof. Since κ_μ is a field and all units of $\mathcal{G}_\mu$ are contained in $\mathcal{G}_\mu^0$ by Remark 2.25, we have $\kappa_\mu \subset \mathcal{G}_\mu^0$. The explicit description shows $\kappa_\mu^\times = \Delta_\mu^\times$, see equation (9) in [19, Section 3, p.11]. □

Let $f \in K[x]$ be a non-zero polynomial and denote

$$S = S_{\mu,\phi}(f),\ \ell_0 = \min(S),\ \ell = \max(S),\ \mathrm{lc}_\mu(f) = \mathrm{in}_\mu(a_\ell)$$

Note that ℓ_0 is the order with which the prime element Y divides $\mathrm{in}_\mu(f) \in \mathcal{G}_\mu^0[Y]$ and $\ell = \deg_\mu(f)$. Let e be the relative ramification index of μ.

Lemma 2.29. *The positive integer e divides $(i - \ell_0)$ for all $i \in S$. Hence,*

$$\mathrm{in}_\mu(f) = Y^{\ell_0} P(Y^e)$$

for a unique polynomial $P \in \mathcal{G}_\mu^0[X]$, where X is an indeterminate. The polynomial P has a non-zero constant term and is of degree $d := (\ell - \ell_0)/e$.

Proof. Let $f = a_0 + \cdots + a_\ell \phi^\ell$ be the $\phi-$expansion of f. Recall that for all $i, j \in S$, we have $\mu(a_i\phi^i) = \mu(a_j\phi^j)$.

Denote $\gamma = \mu(\phi)$ and let $i \in S$, then $(i - \ell_0)\gamma = \mu(a_{\ell_0}) - \mu(a_i)$, so $(i - \ell_0)\gamma \in \Gamma_\mu^0$ and hence $e \mid (i - \ell_0)$.

For each $i \in S$, denote $j = (i - \ell_0)/e$ and let $X = Y^e$, we deduce

$$\begin{aligned}\mathrm{in}_\mu(f) = \sum_{i\in S} \mathrm{in}_\mu(a_i)Y^i &= Y^{\ell_0} \sum_{i\in S} \mathrm{in}_\mu(a_i)Y^{je} \\ &= Y^{\ell_0} \sum_{i\in S} \mathrm{in}_\mu(a_i)X^j \\ &= Y^{\ell_0} P(X).\end{aligned}$$

It is clear that $P_0 \neq 0$, because $P_0 = \mathrm{in}_\mu(a_{\ell_0})$. Clearly $deg_X(P) := (\ell - \ell_0)/e$. All coefficients of P are in $\mathcal{G}_\mu^0$, because the set of non-zero coefficients of P is precisely the set of non-zero coefficients of $\mathrm{in}_\mu(f) \in \mathcal{G}_\mu^0[Y]$, by construction. The uniqueness of P follows by Theorem 2.22, clearly Y transcendental means Y^e is transcendental too. □

We will now perform a change of variable to obtain a polynomial with coefficients in the field κ_μ. The idea is to divide the polynomial P in the above lemma by a suitable unit.

Theorem 2.30. *Let u be a unit of $\mathcal{G}_\mu$ with $\mathrm{gr}(u) = \mathrm{gr}(Y^e)$. There there exists a unique polynomial $R \in \kappa[y]$, where y is an indeterminate, such that*

$$\mathrm{in}_\mu(f) = \mathrm{lc}_\mu(f)Y^{\ell_0}u^d R\left(\frac{Y^e}{u}\right). \tag{5}$$

The polynomial R is monic and has a non-zero constant term.

Proof. We have $\mathrm{in}_\mu(f) = Y^{\ell_0}P(Y^e)$ for a unique $P \in \mathcal{G}_\mu^0[X]$ by Lemma 2.29. For each $i \in S$ denote $j = (i-\ell_0)/e$ and recall that $d := (\ell-\ell_0)/e = \deg_X(P)$ and $\mathrm{lc}_\mu(f) = \mathrm{in}_\mu(a_\ell)$. Let $u \in \mathcal{G}_\mu$ be an arbitrary unit, then

$$\begin{aligned}\frac{P(Y^e)}{u^d} = \sum_{i\in S} \frac{\mathrm{in}_\mu(a_i)Y^{je}}{u^d} &= \sum_{i\in S} \frac{\mathrm{in}_\mu(a_i)u^{j-d}Y^{je}}{u^j} \\ &= \sum_{i\in S} \mathrm{in}_\mu(a_i)u^{j-d}\left(\frac{Y^e}{u}\right)^j. \end{aligned}\tag{6}$$

Denote $\gamma = \mu(\phi) = \mathrm{gr}(Y)$, since $\mathrm{gr}(Y^e) = e\gamma \in \Gamma_\mu^0$, there exists a unit $u \in \mathcal{G}_\mu$ with $\mathrm{gr}(u) = \mathrm{gr}(Y^e)$. We claim that this condition ensures that for all $i \in S$,

$$\mathrm{gr}(\mathrm{in}_\mu(a_i)u^{j-d}\,\mathrm{in}_\mu(a_\ell)^{-1}) = 0.$$

Since $\ell, i \in S$, we have

$$\mathrm{gr}(\mathrm{in}_\mu(a_i)\,\mathrm{in}_\mu(a_\ell)^{-1}) = \mu(a_i) - \mu(a_\ell) = (\ell - i)\gamma$$

and from $\mathrm{gr}(u) = \mathrm{gr}(Y^e)$ we obtain

$$\mathrm{gr}(u^{j-d}) = \left(\frac{i-\ell_0}{e} - \frac{\ell-\ell_0}{e}\right)e\gamma = -(\ell - i)\gamma$$

which proves the claim. Denote $y := Y^e/u$ and observe that

$$R = \frac{P(Y^e)}{u^d \operatorname{lc}_\mu(f)} = \sum_{i \in S} \operatorname{in}_\mu(a_i) u^{j-d} \operatorname{in}_\mu(a_\ell)^{-1} y^j \tag{7}$$

belongs to $\kappa[y]$, satisfies Eq. (5) and is monic with a non-zero constant term by construction. The uniqueness of R follows by Theorem 2.22, clearly Y transcendental over $\mathcal{G}_\mu^0$ implies $y = \frac{Y^e}{u}$ is transcendental over $\kappa \subset \mathcal{G}_\mu^0$. □

Definition 2.31. *For a given non-zero $f \in K[x]$, we define the **residual polynomial** of f corresponding to the choice of $\phi \in \mathrm{KP}(\mu)$ of minimal degree and a homogeneous unit $u \in \mathcal{G}_\mu$ of grade $e\mu(\phi)$ to be the unique polynomial satisfying Eq.* (5) *and denote it $R_{\mu,\phi,u}(f)$.*

Remark 2.32. *Denote $R(f) := R_{\mu,\phi,u}(f)$, suppressing the dependence on the choice (ϕ, u). By Eq.* (5)*, $\operatorname{in}_\mu(f)$ is a unit times a power of the prime Y times $R(f)$, so in particular the homogeneous prime factors of $\operatorname{in}_\mu(f)$ that are not associate to Y are precisely the prime factors of $R(f)$. Hence up to multiplication by a unit, the prime factorization of $\operatorname{in}_\mu(f)$ is $\operatorname{in}_\mu(f) \sim_{unit} Y^{\ell_0}\psi_1^{n_1}\cdot\ldots\cdot\psi_k^{n_k}$ where $R(f) = \psi_1^{n_1}\cdot\ldots\cdot\psi_k^{n_k}$, $\psi_i \in \operatorname{Irr}(\kappa)$ is the irreducible factorization of $R(f) \in \kappa[y]$.*

Let us parametrize the coefficients of the residual polynomial. We know by Lemma 2.29 that each $i \in S$ satisfies $e \mid (i - \ell_0)$, so it is of the form $i = ej + \ell_0$ for a unique $0 \leq j \leq d$. For each $0 \leq j \leq d$, we define $\ell_j = ej + \ell_0$. Clearly, ℓ_0 and $\ell_d = \ell$ belong to S, but this is not necessarily true for an arbitrary j. For each $0 \leq j \leq d$, define the $j-$th **residual coefficient** of f to be

$$\zeta_j = \begin{cases} \operatorname{in}_\mu(a_{\ell_j}) u^{j-d} \operatorname{in}_\mu(a_\ell)^{-1} & \text{if } \ell_j \in S \\ 0 & \text{otherwise} \end{cases}$$

and by Eq. (7) we immediately deduce

$$R(f) = \zeta_0 + \zeta_1 y + \cdots + \zeta_{d-1} y^{d-1} + y^d.$$

Assigning a non-zero $f \in K[x]$ its residual polynomial with respect to the fixed choice (μ, ϕ, u) determines a residual polynomial operator:

$$R : K[x] \longrightarrow \kappa[y],$$

if we agree that $R(0) = 0$.

Proposition 2.33. *For all $f, g \in K[x]$, we have*

$$R(fg) = R(f)R(g).$$

Proof. It is clear that $\operatorname{lc}_\mu(fg) = \operatorname{lc}_\mu(f)\operatorname{lc}_\mu(g)$. We have $\ell_0(fg) = \ell_0(f) + \ell_0(g)$ because $\ell_0(fg)$ is the order with which the prime Y divides $\operatorname{in}_\mu(fg)$. Finally, $d(fg) = \deg_\mu(fg)/e = \deg_\mu(f)/e + \deg_\mu(g)/e = d(f) + d(g)$. Hence, $R(fg) = R(f)R(g)$ follows by Eq. (5). □

The next results shows that any choice of residual polynomial operator allows us to completely characterize key polynomials for μ.

Theorem 2.34. *[19, Props. 6.3, 6.6] Let μ be a residue-transcendental valuation, let $\phi \in KP(\mu)$ be a key polynomial of minimal degree $n := \deg(\mu)$, $u \in \mathcal{G}_\mu$ a homogeneous unit of grade $e\mu(\phi)$ and $R := R_{\mu,\phi,u}$ the residual polynomial operator corresponding to these choices.*

A monic $Q \in K[x]$ is a key polynomial for μ if and only if either

- $\deg(Q) = n$ *and* $\mathrm{in}_\mu(\phi) = \mathrm{in}_\mu(Q)$; *or*
- $\deg(Q) = en\deg(R(Q))$ *and $R(Q) \in \kappa[y]$ is irreducible.*

Moreover, for all $Q, Q' \in \mathrm{KP}(\mu)$, we have

$$\mathrm{in}_\mu(Q) \mid \mathrm{in}_\mu(Q') \Longleftrightarrow \mathrm{in}_\mu(Q) = \mathrm{in}_\mu(Q') \Longleftrightarrow R(Q) = R(Q')$$

and if these equivalent conditions hold, then $\deg(Q) = \deg(Q')$.

It is easy to construct a $Q \in \mathrm{KP}(\mu)$ with a prescribed $\psi \in \mathrm{Irr}(\kappa)\backslash\{y\}$ as shown in [19, Corollary 5.6]. We deduce a bijection

$$\mathrm{KP}(\mu)/\sim_\mu \longrightarrow \kappa[y], \qquad [Q]_\mu \mapsto \begin{cases} y & \text{if } \mathrm{in}_\mu(Q) = \mathrm{in}_\mu(\phi) \\ R(Q) & \text{otherwise} \end{cases} \tag{8}$$

which depends on $Y = \mathrm{in}_\mu(\phi)$ and the unit u. The variation of $R(Q)$ with respect to a different choice of unit and key polynomial of minimal degree is exhaustively discussed in [19, Section 5].

Remark 2.35. *We wish to stress that each choice (ϕ, u) as in Theorem 2.34 completely determines the set* $\mathrm{KP}(\mu)$.

2.5 Tangent directions

Let (K, v) be a valued field, denote $\Gamma := \Gamma_v$ and recall that $\mathcal{T} = \{\mu : K[x] \longrightarrow \Gamma_{\mathbb{Q}}\infty \mid \mu \text{ is a valuation and } \mu_{|K} = v\}$.

If $\mu, \nu \in \mathcal{T}$ satisfy $\mu \leq \nu$, we define the map

$$\mathcal{G}_\mu \longrightarrow \mathcal{G}_\nu,\ \mathrm{in}_\mu(f) \mapsto \begin{cases} \mathrm{in}_\nu(f) & \text{if } \mu(f) = \nu(f) \\ 0 & \text{if } \mu(f) < \nu(f). \end{cases}$$

It is easy to check that $\mathcal{G}_\mu \longrightarrow \mathcal{G}_\nu$ is a ring homomorphism that is injective if and only if $\mu = \nu$.

Definition 2.36. *For $\mu, \nu \in \mathcal{T}$ that satisfy $\mu < \nu$, let $\mathbf{t}(\mu, \nu)$ be the set of all monic polynomials $\phi \in K[x]$ of minimal degree such that $\mu(\phi) < \nu(\phi)$. We say that $\mathbf{t}(\mu, \nu)$ is the* ***tangent direction*** *of μ determined by ν.*

Clearly $\mathbf{t}(\mu,\nu)$ is non-empty, all $\phi \in \mathbf{t}(\mu,\nu)$ have the same degree and $\mathbf{t}(\mu,\nu) \subset K[x]\backslash K$.

Lemma 2.37. *[21, Lemma 2.6] Every $\phi \in \mathbf{t}(\mu,\nu)$ is a key polynomial for μ and $\mathbf{t}(\mu,\nu) = [\phi]_\mu$. Moreover for all non-zero $f \in K[x]$, we have*

$$\mu(f) < \nu(f) \Longleftrightarrow \mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(f).$$

So tangent directions and $\mu-$equivalence classes of key polynomials are the same thing. Moreover, if we have some valuation ν strictly above μ, that realises $[\phi]_\mu$, the relation "$\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(f)$" can be checked solely from the values of ν.

Proposition 2.38. *Let $\mu \in \mathcal{T}$, then*

$$\mathrm{KP}(\mu) = \bigcup_{\nu\in\mathcal{T},\ \mu<\nu} \mathbf{t}(\mu,\nu).$$

Proof. By Theorem 2.8, a $\mu \in \mathcal{T}$ is maximal if and only if $\mathrm{KP}(\mu) = \emptyset$.

By Theorem 1.29 the non-maximal elements are precisely the residue-transcendental valuations. So if μ is non-maximal, we have $\mathbf{t}(\mu,\nu) \subset \mathrm{KP}(\mu)$ for all $\nu \in \mathcal{T}$ with $\mu < \nu$ by Lemma 2.37.

Conversely, a $\phi \in \mathrm{KP}(\mu)$ determines a certain valuation $v_\phi : K[x]/(\phi) \longrightarrow \Gamma_{\mathbb{Q}}\infty$ on the field $K_\phi := K[x]/(\phi)$ that extends v, [19, Proposition 2.12]. Composing v_ϕ with the canonical surjection $K[x] \twoheadrightarrow K[x]/(\phi)$ gives an $\nu_\phi \in \mathcal{T}$ with support (ϕ) that satisfies $\mu < \nu_\phi$ and $\mu(f) = \nu_\phi(f)$ for all $f \in K[x]$ with $\deg(f) < \deg(\phi)$. Since $\mu(\phi) < \nu_\phi(\phi) = \infty$, we have $\phi \in \mathbf{t}(\mu,\nu_\phi)$ by definition of tangent direction. □

Remark 2.39. *The union in the above result is far from being disjoint; note that if $\mu,\nu_1,\nu_2 \in \mathcal{T}$ satisfy $\mu < \nu_1 < \nu_2$ then $\phi \in \mathbf{t}(\mu,\nu_1) \Longrightarrow \phi \in \mathbf{t}(\mu,\nu_2)$ and hence $\mathbf{t}(\mu,\nu_1) = \mathbf{t}(\mu,\nu_2)$ because these tangent directions are non-disjoint μ-equivalence classes by Lemma 2.37.*

The following lemma characterizes when a given key polynomial determines a given tangent direction.

Lemma 2.40. *[21, Lemma 2.7] Let $\mu \in \mathcal{T}$ and let $\phi \in \mathrm{KP}(\mu)$. For each $\nu \in \mathcal{T}$ with $\mu < \nu$, we have*

$$\mathbf{t}(\mu,\nu) = [\phi]_\mu \Longleftrightarrow \mu(\phi) < \nu(\phi).$$

2.6 Depth zero valuations and ordinary augmentations

It is easy to check that for each $\gamma \in \Gamma_{\mathbb{Q}}\infty$ and each $a \in K$, the **depth-zero valuation** $\nu = [v; x-a, \gamma]$ that acts on $(x-a)-$expansions as

$$\nu\Big(\sum_{0\le i\le r} a_i(x-a)^i\Big) = \min_{0\le i\le r}\{v(a_i) + i\gamma\}$$

is a valuation on $K[x]$ with $\nu(x-a)=\gamma$ and satisfies $\nu \in \mathcal{T}$. Moreover, ν has non-trivial support if and only if $\gamma < \infty$. In this case $(x-a) \in \mathrm{KP}(\nu)$ is a key polynomial of minimal degree. If $\gamma = \infty$, then ν is the unique $\nu \in \mathcal{T}$ with support $(x-a)K[x]$.

Lemma 2.41. *Let $\mu \in \mathcal{T}$ and $\gamma \in \Gamma_{\mathbb{Q}}\infty$. If $\phi \in \mathrm{KP}(\mu)$ and $\gamma > \mu(\phi)$, then the map ν acting on $\phi-$expansions as*

$$\nu\Big(\sum_{0\le i\le r} a_i\phi^i\Big) = \min_{0\le i\le r}\{\mu(a_i)+i\gamma\}.$$

is a valuation on $K[x]$ that satisfies $\nu \in \mathcal{T}$ and $\mu < \nu$.

Proof. The arguments of Maclane in the rank one case [16, Theorem 3.1], work in general. The only more recent reference seems to be [22, Corollary 2.4]. □

Definition 2.42. *The valuation ν above is called the **ordinary augmentation** of μ with respect to ϕ and γ. We denote it by $\nu = [\mu; \phi, \gamma]$.*

The following properties of ordinary augmentations due to Maclane were generalised by Vaquié, see [28, Section 1.1] or [20, Proposition 2.1].

Lemma 2.43. *Let $\nu = [\mu; \phi, \gamma]$ be an ordinary augmentation of μ. The following all hold.*

(1) $\nu(\phi) = \gamma$ and $\mathbf{t}(\mu, \nu) = [\phi]_\mu$.
(2) ν has non-trivial support if and only if $\gamma < \infty$.
(3) If $\gamma = \infty$, the support of ν is $\phi K[x]$.
(4) If $\gamma < \infty$, then $\mathrm{KP}(\nu) \neq \emptyset$ and $\phi \in \mathrm{KP}(\nu)$ is a key polynomial of minimal degree.
(5) $\deg(\mu) \le \deg(\nu)$.

2.7 Limit augmentations

Let A be a well-ordered set without last element and $\mathcal{C} = (\rho_i)_{i\in A}$ a family of elements of $\mathcal{T}$. The family $\mathcal{C}$ is a **continuous family**, parametrized by A, if all the following hold:

- The map $i \mapsto \rho_i$ is an isomorphism of totally ordered sets.
- There exists an $i_0 \in A$ such that for all $i \ge i_0$ we have $\deg(\rho_i) = \deg(\rho_{i_0})$.

For a continuous family $\mathcal{C}$, we denote by $\deg(\mathcal{C})$ this "stable degree" $\deg(\rho_{i_0})$.

These definitions imply that the set $\{\rho_i\}_{i\in A}$ is totally ordered and each $\rho_i \in \mathcal{T}$ is non-maximal.

A polynomial $g \in K[x]$ is said to be $\mathcal{C}-$**stable** if there exists an $i_0 \in A$ such that $\rho_i(f) = \rho_{i_0}(f)$ for all $i \ge i_0$, in this case we denote $\rho_{\mathcal{C}}(f) := \rho_{i_0}(f)$.

Definition 2.44. *A $\phi \in K[x]$ is a **limit key polynomial** for $\mathcal{C}$ if all the following hold.*

- *ϕ is not $\mathcal{C}-$stable.*
- *ϕ is of minimal degree among polynomials that are not $\mathcal{C}-$stable.*

- ϕ *is monic.*

The set of limit key polynomials for $\mathcal{C}$ is denoted $\mathrm{KP}_\infty(\mathcal{C})$. We say that $\mathcal{C}$ is **essential** if there exists a $\phi \in \mathrm{KP}_\infty(\mathcal{C})$ with $\deg(\phi) > \deg(\mathcal{C})$. If $\mathrm{KP}_\infty(\mathcal{C}) = \emptyset$, then all $f \in K[x]$ are $\mathcal{C}-$stable and $\rho_{\mathcal{C}}$ is a valuation, $\rho_{\mathcal{C}} \in \mathcal{T}$, called the **stable limit** of the continuous family $\mathcal{C}$. Stable limits are valuation-algebraic [20, Proposition 3.1].

If $\mathrm{KP}_\infty(\mathcal{C}) \neq \emptyset$, a limit key polynomial can be used to obtain a valuation as follows (cf. [28, Proposition 1.22] or [22, Theorem 5.16]).

Lemma 2.45. *Let $\mathcal{C} \subset \mathcal{T}$ be a continuous family and $\gamma \in \Gamma_{\mathbb{Q}}\infty$. If $\phi \in \mathrm{KP}_\infty(\mathcal{C})$ and $\gamma > \rho_i(\phi)$ for all $i \in A$, then the map ν acting on $\phi-$expansions as*

$$\nu\Big(\sum_{0\leq i\leq r} a_i\phi^i\Big) = \min_{0\leq i\leq r}\{\rho_{\mathcal{C}}(a_i) + i\gamma\}.$$

is a valuation on $K[x]$ that satisfies $\nu \in \mathcal{T}$ and $\rho_i < \nu$ for all $i \in A$.

Definition 2.46. *The valuation ν above is called the **limit augmentation** of μ with respect to $\mathcal{C}$ and γ. We denote it by $\nu = [\mathcal{C}; \phi, \gamma]$.*

Limit augmentations satisfy the following properties, see [19, Corollary 7.13] and [21, Section 2.4].

Lemma 2.47. *Let $\mathcal{C} = (\rho_i)_{i\in A}$ be a continuous family and $\nu = [\mathcal{C}; \phi, \gamma]$ a limit augmentation. Denote $i_{\min} = \min(A)$ and $\mu := \rho_{i_{\min}}$. The following all hold.*

(1) $\nu(\phi) = \gamma$ and $\mathbf{t}(\mu, \nu) = \mathbf{t}(\rho_i, \nu)$ for all $i > i_{\min}$.
(2) ν has non-trivial support if and only if $\gamma < \infty$.
(3) If $\gamma = \infty$, the support of ν is $\phi K[x]$.
(4) If $\gamma < \infty$, then $\mathrm{KP}(\nu) \neq \emptyset$ and $\phi \in \mathrm{KP}(\nu)$ is a key polynomial of minimal degree.
(5) $\deg(\nu) = \deg(\phi)$.

Let $\mu, \nu \in \mathcal{T}$, from now on we will use the notation $\mu \longrightarrow \nu$ to describe an augmentation. This means that, either

$$\begin{aligned} &\nu = [\mu; \phi, \gamma], \quad \phi \in \mathrm{KP}(\mu), \quad \gamma > \mu(\phi), \text{ or} \\ &\nu = [\mathcal{C}; \phi, \gamma], \quad \phi \in \mathrm{KP}_\infty(\mathcal{C}), \quad \gamma > \rho_i(\phi) \text{ for all } i \in A, \end{aligned}$$

where $\mathcal{C} = (\rho_i)_{i\in A}$ is a continuous family such that $\mu = \rho_{i_{\min}}$ where $i_{\min} := \min(A)$.

Definition 2.48. *The **inertia degree** of an augmentation $\mu \longrightarrow \nu$ is $f(\mu \longrightarrow \nu) = [\kappa_\nu : \kappa_\mu]$*

2.8 Chains of augmentations

Let $\mu \in \mathcal{T}$ and suppose that μ is residue-transcendental (non-maximal) or that μ has trivial support. By a celebrated theorem of Vaquié ([28], or [20]), μ can be obtained from v after a finite number of augmentations:

$$v \longrightarrow \mu_0 \longrightarrow \mu_1 \longrightarrow \dots \longrightarrow \mu_r \longrightarrow \mu_{r+1} = \mu. \tag{9}$$

The initial step $v \longrightarrow \mu_0$ only has a formal purpose; it indicates that μ_0 is a depth-zero valuation. For each augmentation in Eq. (9), denote

- $\mu_{n+1} = [\mu_n; \phi_{n+1}, \gamma_{n+1}]$ if $\mu_n \longrightarrow \mu_{n+1}$ is ordinary
- $\mu_{n+1} = [\mathcal{C}_n; \phi_{n+1}, \gamma_{n+1}]$ if $\mu_n \longrightarrow \mu_{n+1}$ is limit.

The canonical ring homomorphisms $\mathcal{G}_{\mu_n} \longrightarrow \mathcal{G}_{\mu_{n+1}}$ induce a tower of fields

$$k = \kappa_{\mu_0} \longrightarrow \cdots \longrightarrow \kappa_{\mu_{r+1}} = \kappa_\mu.$$

Hence, we have

$$[\kappa_\mu : k] = f(\mu_0 \longrightarrow \mu_1) \dots f(\mu_r \longrightarrow \mu). \tag{10}$$

Results in [20, Section 5.1] show that the extensions $\kappa_{\mu_{n+1}}/\kappa_{\mu_n}$ are finite.

Unfortunately, the associated value groups do not necessarily form a chain. In order to overcome this, some (strong) conditions need to be imposed on the chain Eq. (9).

Definition 2.49. *The chain Eq.* (9) *is said to be a* ***Maclane-Vaquié*** *(MLV) chain for μ if every augmentation in the chain satisfies:*

- *If $\mu_n \longrightarrow \mu_{n+1}$ is ordinary, then* $\deg(\mu_n) < \deg(\mu_{n+1})$.
- *If $\mu_n \longrightarrow \mu_{n+1}$ is limit, then $\mathcal{C}_n$ is essential,* $\deg(\mu_n) = \deg(\mathcal{C}_n)$ *and* $\phi_n \notin \mathbf{t}(\mu_n, \mu_{n+1})$.

In this case, we have $\mu(\phi_n) = \gamma_n$ for all n.

Theorem 2.50. *[20, Theorem 4.3] If $\mu \in \mathcal{T}$ is residue-transcendental or has non-trivial support, then there exists an MLV chain for μ.*

As shown in [20, Section 4], if Eq. (9) is an MLV chain for μ, the value groups satisfy

$$\Gamma_{-1} := \Gamma \subset \Gamma_{\mu_0} \subset \cdots \subset \Gamma_{\mu_{r+1}} = \Gamma_\mu,$$

such that $\Gamma_{\mu_{n-1}} = \Gamma^0_{\mu_n}$ for all $0 \leq n \leq r+1$. Hence, we have

$$(\Gamma_\mu : \Gamma) = e(\mu_0) \cdots e(\mu_{r+1}). \tag{11}$$

Suppose that μ has non-trivial support $\mathrm{supp}(\mu) = GK[x]$, then the ramification index $e(\overline{\mu}/v)$ and residue degree $f(\overline{\mu}/v)$ of the induced valuation $\overline{\mu}$ on $K[x]/(G)$ can be computed using Eq. (11) and Eq. (10), due to the equality $k_{\overline{\mu}} = \kappa_\mu$ which follows from [20, Theorem 5.4].

Definition 2.51. *A $\mu \in \mathcal{T}$ is* ***inductive*** *if there exists an MLV chain for μ such that all augmentations in the chain are ordinary.*

Remark 2.52. *It is an object of ongoing research to develop computer algorithms to handle all MLV chains. The algorithms we will encounter in this thesis only involve inductive valuations.*

3 Irreducible polynomials over henselian fields

3.1 Convex hulls

Let Γ be an ordered abelian group and consider the rational vector space $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$. Let $P = (s, \alpha)$ and $Q = (t, \beta)$ be two points in $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$, the **segment** joining P and Q is the set

$$S = \{P + (1 - \epsilon)Q \mid \epsilon \in \mathbb{Q},\ 0 \leq \epsilon \leq 1\} \subset \mathbb{Q} \times \Gamma_{\mathbb{Q}}.$$

The segment joining P and Q is a single point if and only if $P = Q$. If $s \neq t$, we define the **slope** of S to be

$$\text{slope}(S) = \frac{\beta - \alpha}{t - s} \in \Gamma_{\mathbb{Q}}.$$

A subset of $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$ is **convex**, if it contains every segment joining a pair of points in the subset.

Let $C \subset \mathbb{Q} \times \Gamma_{\mathbb{Q}}$ be non-empty finite subset, the **convex hull** of C is the smallest convex subset containing C. Clearly, the convex hull of C coincides with C if and only if C is a single point, because the segment joining two distinct points of C is infinite and contained in the convex hull.

In general, the border of this hull consists of finitely many chained segments joining some of the points of C.

If all the points in C have pairwise distinct abscissas there exists a unique leftmost point $P \in C$ and a unique rightmost point $Q \in C$ and we have $P \neq Q$ if and only if C is not a single point. In general there exist two chains of segments on the border of the hull joining P and Q called the **upper convex hull** and **lower convex hull** of C.

These chains of segments are determined by the condition that the lower convex hull contains all the points in C that lie on the border of the convex hull and simultaneously on or below the segment joining P and Q. Therefore the lower convex hull coincides with the upper convex hull if and only if all the points in C lie on the segment joining P and Q.

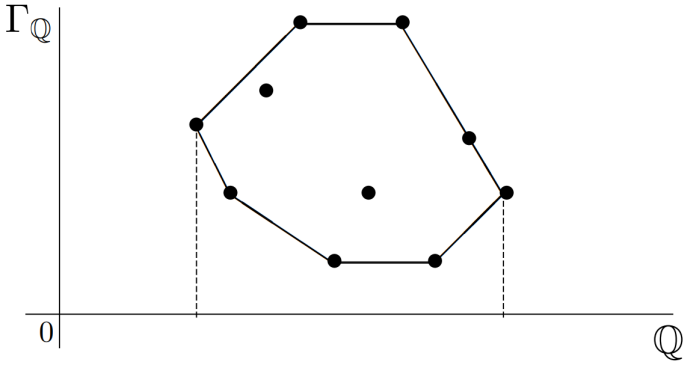
3.2 Types draw Newton polygons

For the rest of this chapter fix a valued field (K, v) and denote its value group $\Gamma := \Gamma_v$. Recall that the set $\mathcal{T} := \mathcal{T}(\Gamma_{\mathbb{Q}})$ of all $\Gamma_{\mathbb{Q}}$-valued extensions of v to $K[x]$ is partially ordered. Moreover, for all $\mu \in \mathcal{T}$ the property of being non-maximal is equivalent to $\text{KP}(\mu) \neq \emptyset$.

Definition 3.1. *A **type** is a pair (μ, ϕ) where $\mu \in \mathcal{T}$ is non-maximal and $\phi \in \text{KP}(\mu)$.*

Let (μ, ϕ) be a type and $f = a_0 + a_1\phi + \cdots + a_r\phi^r$ the $\phi-$expansion of a non-zero $f \in K[x]$.

Figure 1: Convex hull of a finite set of points with different abscissas.



Definition 3.2. *The **Newton polygon** of f with respect to (μ, ϕ) is the lower convex hull of the finite set*

$$C = \{(i, \mu(a_i)) \mid 0 \leq i \leq r,\ \mu(a_i) < \infty\} \subset \mathbb{Q} \times \Gamma_{\mathbb{Q}}.$$

We use the notation $N_{\mu,\phi}(f)$ and agree that the Newton polygon of the zero polynomial is the empty set.

Therefore a type (μ, ϕ) determines a **Newton polygon operator**

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

where $\mathcal{P}(\mathbb{Q} \times \Gamma_{\mathbb{Q}})$ is the power set of $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$.

Let $N := N_{\mu,\phi}(g)$ for some non-zero polynomial $g \in K[x]$. If N is a single point, we say that N has an **empty set of sides**. Otherwise, N is uniquely a chain of segments $\{S_1, \ldots, S_k\}$ of strictly increasing slopes called the **sides** of N.

The **vertices** of N are the left and right endpoints of N and all the points of N joining two different sides. The vertices of N are elements of C, but not every element of C is necessarily a vertex.

The **length** $\ell(N)$ of N is defined as the abscissa of the right endpoint of N. We have

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

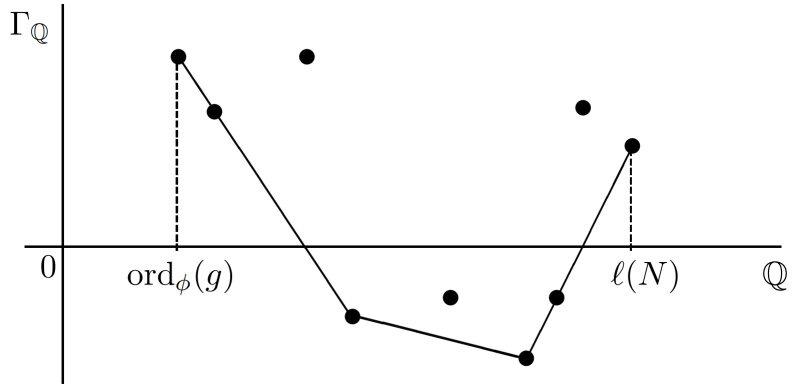
The abscissa of the left endpoint of N is equal to the order with which ϕ divides f in $K[x]$. It is denoted $\mathrm{ord}_{\phi}(f)$.

Clearly, for all non-zero $f, g \in K[x]$ we have

$$\ell(N_{\mu,\phi}(fg)) \geq \ell(N_{\mu,\phi}(f)) + \ell(N_{\mu,\phi}(g)).$$

It is easy to construct examples where this inequality is strict.

Figure 2: Newton polygon $N = N_{\mu,\phi}(g)$ of $g \in K[x]$



Example 3.3. *If $f, g \in K[x]$ satisfy $\deg(f),\ \deg(g) < \deg(\phi)$ and $\deg(fg) \geq \deg(\phi)$, the Newton polygons $N_{\mu,\phi}(f)$ and $N_{\mu,\phi}(g)$ are both a single point of the form $(0, \alpha)$ where α is equal to $\mu(f)$ and $\mu(g)$ respectively, while $N_{\mu,\phi}(fg)$ has length at least one.*

Definition 3.4. *For all $\lambda \in \Gamma_{\mathbb{Q}}$, the $\lambda-$**component** $S_\lambda(N) \subset N$ is the intersection of N with the line L of slope $-\lambda$ that first touches N from below. In other words,*

$$S_\lambda(N) = \{(n, \alpha) \in N \mid \alpha + n\lambda \text{ is minimal}\}.$$

The abscissas of the left and right endpoints of $S_\lambda(N)$ are denoted $n_\lambda \leq n'_\lambda$.

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

Definition 3.5. *We say that N is **one-sided** of slope $-\lambda$, if $N = S_\lambda(N),\ n_\lambda = 0$, and $n_{\lambda'} > 0$.*

Definition 3.6. *The **principal Newton polygon** $N^+_{\mu,\phi}(f)$ is the polygon formed by all the sides of $N_{\mu,\phi}(f)$ whose slope is less than $-\mu(\phi)$. If $N_{\mu,\phi}(f)$ has no sides whose slope is less than $-\mu(\phi)$, then $N^+_{\mu,\phi}(f)$ is defined to be the left endpoint of $N_{\mu,\phi}(f)$.*

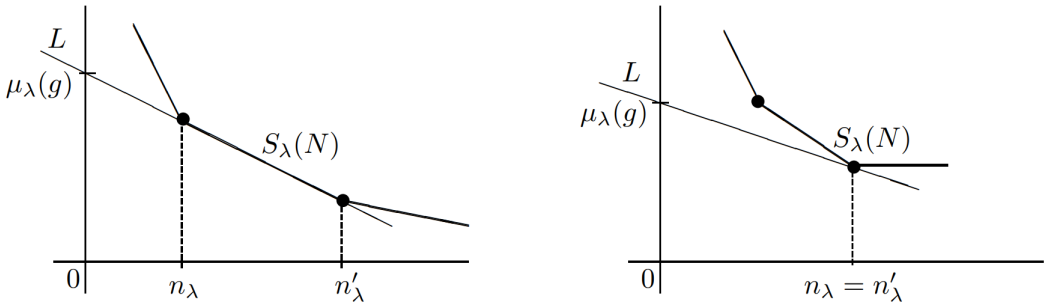
Remark 3.7. *It is easy to check that the set $S_{\mu,\phi}(f) := \{0 \leq i \leq r \mid \mu(a_i\phi^i) = \mu(f)\}$ coincides with the set of abscissas of points in C lying on the segment $S_{\mu(\phi)}(N)$, so Newton polygons display some information about algebraic relations in the graded ring $\mathcal{G}_\mu$.*

In particular, the length of $N^+_{\mu,\phi}(f)$ is the order with which $\mathrm{in}_\mu(\phi)$ divides $\mathrm{in}_\mu(f)$ in $\mathcal{G}_\mu$. We have

$$\ell(N^+_{\mu,\phi}(f)) = \min\big(S_{\mu,\phi}(f)\big) = \mathrm{ord}_{\mathrm{in}_\mu(\phi)}(\mathrm{in}_\mu(f)). \tag{12}$$

The next lemma shows how the values of an augmentation can be computed from Newton polygons.

Figure 3: λ-component of $N = N_{\mu,\phi}(g)$, the line L has slope $-\lambda$ and cuts the vertical axis at $(0, \mu_\lambda(g))$, if $\lambda > \mu(\phi)$ if $\mu_\lambda = [\mu; \phi, \lambda]$.



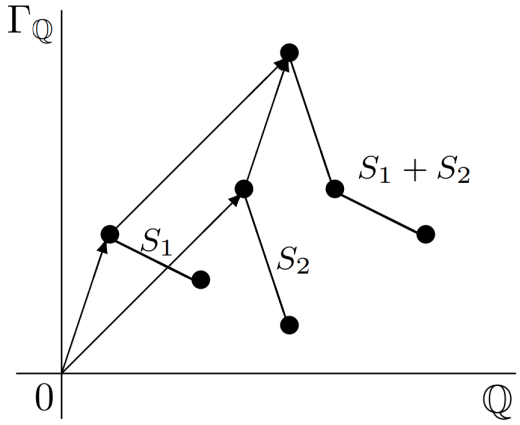
Lemma 3.8. *Let (μ, ϕ) be a type. For $\lambda > \mu(\phi)$, let $\mu_\lambda = [\mu; \phi, \lambda]$. Then, for all non-zero $f \in K[x]$, the line of slope $-\lambda$, which first touches $N_{\mu,\phi}(f)$ from below, intersects the vertical axis at a point whose ordinate is $\mu_\lambda(f)$.*

Proof. This line cuts the vertical axis at the point with ordinate the common value $\alpha + n\lambda$, for all $(n, \alpha) \in S_\lambda(N_{\mu,\phi}(g))$. The result follows by Remark 3.7 as $\mu_\lambda(f) = \min_{0 \le i \le r} \{\mu(a_i) + i\lambda\}$ where $f = a_0 + \cdots + a_r\phi$ is the $\phi-$expansion of f. □

There is an addition law for Newton polygons. Consider two polygons $N,\ N'$. If one of these, say N', is a single point $N' = \{P\}$, then the sum $N + N'$ is the ordinary vector sum $N+P$ in $\mathbb{Q}\times\Gamma_{\mathbb{Q}}$. If both $N,\ N'$ have a non-empty set of sides, let $S_1, \ldots, S_k, S'_1, \ldots S'_l$ be their sides respectively. The left endpoint of the sum $N + N'$ is the vector sum in $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$ of the left endpoints of N and N', denote this point by P. The sides of $N + N'$ are obtained as follows. Join the sides in the multiset $\{S_1, \ldots, S_k, S'_1, \ldots S'_l\}$ to the point P ordered by increasing slope from left to right.

This addition law is clearly commutative and associative, so it deserves its name. Note that by construction $\ell(N + N') = \ell(N) + \ell(N')$.

Figure 4: Addition of two segments



Principal Newton polygons behave well with respect to products, as the following result shows.

Theorem 3.9. *Let (μ, ϕ) be a type, then for all non-zero $f, g \in K[x]$ we have*

$$N^+_{\mu,\phi}(fg) = N^+_{\mu,\phi}(f) + N^+_{\mu,\phi}(g).$$

Proof. This result is well-known, see [21, Theorem 4.1] or [8, Theorem 4.8] □

By Example 3.3, the analogous statement for the entire Newton polygons is false.

Remark 3.10. *One immediate consequence of Theorem 3.9, is that if the principal polygon of a polynomial has two or more sides, this polynomial is not irreducible.*

3.3 Henselization

Let (K, v) be a non-trivially valued field and fix an algebraic closure $\overline{K}$ of K, denote $\Gamma := \Gamma_v$.

Proposition 3.11. *For each extension $\overline{v}$ of v to $\overline{K}$, the value group $\Gamma_{\overline{v}}$ is divisible and satisfies $\Gamma_{\overline{v}} = \Gamma_{\mathbb{Q}}$. The residue field $k_{\overline{v}}$ is an algebraic closure of k_v.*

Proof. The first statement is by [10, p. 79] and the second by [10, Theorem 3.2.11] applied to the tower $K \subset K^{sep} \subset \overline{K}$ where K^{sep} is the separable closure of K in $\overline{K}$. □

Let K^{sep} be the separable closure of K inside $\overline{K}$. Fix an extension $\overline{v}$ of v to $\overline{K}$ and consider the **decomposition group**

$$D_{\overline{v}/v} = \{\sigma \in \mathrm{Gal}(K^{sep}/K) \mid \overline{v} \circ \sigma = v\}.$$

Let K^h be the fixed field of $D_{\overline{v}/v}$ and define v^h to be the restriction of $\overline{v}$ to K^h. Clearly, K^h/K is a separable field extension and v^h is an extension of v.

Theorem 3.12. *The valuation v^h extends uniquely to $\overline{K}$ and the extension $(K, v) \subset (K^h, v^h)$ is immediate.*

Proof. Consider the tower of fields $K \subset K^h \subset K^{sep} \subset \overline{K}$. Since $\overline{K}/K^{sep}$ is purely inseparable, for all $\sigma \in \mathrm{Aut}(\overline{K}/K)$, we have $\overline{v} \circ \sigma = \overline{v} \iff \sigma \in \mathrm{Aut}(\overline{K}/K^h)$, so v^h has a unique extension to $\overline{K}$. The extension $(K, v) \subset (K^h, v^h)$ is immediate, [5, Appendix: Corollary 2]. □

We say that (K^h, v^h) is the **henselization** of (K, v) inside $\overline{K}$ determined by $\overline{v}$. The valued field (K^h, v^h) has the following universal property.

Proposition 3.13. *[5, Appendix: Proposition 13] If (L, w) is an extension of (K, v) such that w extends uniquely to $\overline{K}$, then there exists a unique $K-$embedding $i : K^h \hookrightarrow L$ such that $i(\mathcal{O}_{v^h}) = \mathcal{O}_w \cap i(K^h)$ and $i_{|K} = \mathrm{id}_K$.*

Therefore the henselization of a valued field is unique up to valuation preserving $K-$isomorphism.

Definition 3.14. *We say that a valued field (K, v) is **henselian** if v extends uniquely to $\overline{K}$.*

Proposition 3.15. *For a valued field (K, v), the following are equivalent.*

(1) (K, v) is henselian.
(2) $(K^h, v^h) = (K, v)$.
(3) v extends uniquely to every finite separable extension of K.

Proof. (1) $\implies$ (2) $\implies$ (3) is clear. Let us show (3) $\implies$ (1). Since K^{sep} is the compositum of all finite separable extensions v extends uniquely to K^{sep} and hence to $\overline{K}$ because $\overline{K}/K^{sep}$ is purely inseparable; [10, Corollary 3.2.10]. □

The property of being henselian is hereditary; if $(K, v) \subset (L, w)$ is an algebraic extension of valued fields and (K, v) is henselian, then so is (L, w).

The extensions of v to finite simple extensions of K are determined by how irreducible polynomials over K factor over K^h.

Theorem 3.16. *[21, Section 3] Let (K, v) be a valued field and let $F \in \mathrm{Irr}(K)$. The extensions of v to the field $K[x]/(F)$ are in bijection with the distinct irreducible factors of F over K^h.*

3.4 A generalisation of Hensel's lemma

For the rest of this chapter, assume that (K, v) is a non-trivially valued henselian field. Denote $\Gamma := \Gamma_v$ and recall that $\mathcal{T} := \mathcal{T}(\Gamma_{\mathbb{Q}})$ is the set of $\Gamma_{\mathbb{Q}}-$valued extensions of v to $K[x]$. By Theorem 3.16, there is a bijection

$$\mathrm{Irr}(K) \longleftrightarrow \{\nu \in \mathcal{T} \mid \mathrm{supp}(\nu) \text{ is non-trivial } \}$$

that sends an $F \in \mathrm{Irr}(K)$ to the unique element $v_F \in \mathcal{T}$ with support $FK[x]$. Each v_F is a maximal element in $\mathcal{T}$ by Lemma 1.28

Let $\overline{v}$ be the unique extension of v to a fixed algebraic closure $\overline{K}$ of K. We can assume that $\overline{v}$ is $\Gamma_{\mathbb{Q}}-$valued by Proposition 3.11, so we deduce that v_F equals the composition

$$K[x] \twoheadrightarrow K[x]/(F) \xrightarrow{\overline{v}} \Gamma_{\mathbb{Q}}\infty$$

by Proposition 1.26. Let $F \in \mathrm{Irr}(K)$ and denote by $Z(F)$ the multiset of its roots in $\overline{K}$. By the henselian property, we have

$$v_F(g) = \overline{v}(g(\theta)), \quad \text{for all } g \in K[x] \text{ and all } \theta \in Z(F)$$

These valuations are related to each other and the resultant as follows.

Lemma 3.17. *For all $F, G \in \mathrm{Irr}(K)$, we have*

$$\frac{v_G(F)}{\deg(F)} = \frac{v\big(\mathrm{Res}(F,G)\big)}{\deg(F)\deg(G)} = \frac{v_F(G)}{\deg(G)}$$

where Res *is the resultant.*

Proof. Denote $Z(F), Z(G)$ the multisets of roots of F and G respectively. By definition, we have

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

Fix $\theta \in Z(F)$ and $\alpha \in Z(G)$, then as $\overline{v}(G(\theta))$ and $\overline{v}(F(\alpha))$ do not depend on the choice of θ and α by the henselian property, we obtain

$$\overline{v}(\mathrm{Res}(F,G)) = \deg(F) v_F(G) = \deg(G) v_G(F).$$

Finally, as $\mathrm{Res}(F,G) \in K[x]$, we can replace $\overline{v}$ by v in the above equality. □

The next result is the main result of this chapter.

Theorem 3.18. *[21, Theorem 4.4] Let $\mu \in \mathcal{T}$ and $\phi \in \mathrm{KP}(\mu)$, then for all $F \in \mathrm{Irr}(K)$ we have:*

$$\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(F) \iff \mu < v_F \text{ and } \boldsymbol{t}(\mu, v_F) = [\phi]_\mu.$$

Moreover, if these conditions hold, then:

(1) Either $F = \phi$ or the Newton polygon $N_{\mu,\phi}(F)$ is one-sided of slope $-v_F(\phi)$.
(2) $\deg(\phi) \mid \deg(F)$, and we have $\ell = \deg(F)/\deg(\phi)$ where ℓ is the length of $N_{\mu,\phi}(F)$.
(3) $\mathrm{in}_\mu(F) = \mathrm{in}_\mu(\phi)^\ell$.

Remark 3.19. *Let $F \in \mathrm{Irr}(K)$ and suppose that $\mathrm{in}_\mu(F)$ is not a unit, then there exists a homogeneous prime element $t \in \mathcal{G}_\mu$ such that $t \mid \mathrm{in}_\mu(F)$ by Theorem 2.14. There exists a $\phi \in \mathrm{KP}(\mu)$ and a homogeneous unit $u \in \mathcal{G}_\mu$ such that $t = u\,\mathrm{in}_\mu(\phi)$ by Theorem 2.16. Hence, $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(F)$ which shows $\mathrm{in}_\mu(F)$ is a power of the prime $\mathrm{in}_\mu(\phi)$ by Theorem 3.18. We conclude that for each $F \in \mathrm{Irr}(K)$, either $\mathrm{in}_\mu(F)$ is a unit or $\mathrm{in}_\mu(F)$ is a prime power.*

This has an obvious consequence for testing irreducibility of polynomials; if $in_\mu(g)$ has two non-associate prime factors, where $g \in K[x]$, then g is not irreducible.

3.5 Irreducible polynomials form an ultrametric space

Let X be a set and $(\Gamma, \leq)$ a totally ordered set. Let ∞ be a symbol and extend $\leq$ to $\Gamma\infty := \Gamma \cup \{\infty\}$ via the rule $\gamma < \infty$ for all $\gamma \in \Gamma$.

Let $u : X \times X \longrightarrow \Gamma\infty$ a function such that for all $a, b, c \in X$:

(1) $u(a,b) = \infty \iff a = b$
(2) $u(a,b) = u(b,a)$
(3) $u(a,b) \geq \min\{u(a,c), u(c,b)\}$.

Then u is called an **ultrametric** on X and (X,u) is called an **ultrametric space**. In contrast to metric spaces, two points $a, b \in X$ are close if $u(a,b)$ is large.

Theorem 3.20. *[4, Corollary 3.3] Let (K,v) be a henselian valued field and denote $\Gamma := \Gamma_v$. The function $u : \mathrm{Irr}(K) \times \mathrm{Irr}(K) \longrightarrow \Gamma_{\mathbb{Q}}\infty$ given by*

$$u(F,G) = \frac{v\big(\operatorname{Res}(F,G)\big)}{\deg(F)\deg(G)}$$

is an ultrametric.

Remark 3.21. *It may be possible to prove this theorem in a more elementary way than in [4] by generalising the original arguments of Krasner for the $p-$adic case, [12].*

Remark 3.22. *By Lemma 3.17, we have $u(F,G) = \frac{v_F(G)}{\deg(G)}$ for all $F, G \in \mathrm{Irr}(K)$. In view of Theorem 3.18, the distance $u(F,\phi)$, where (μ,ϕ) is a type, is the natural way to define the quality of an approximation to v_F.*

The next result shows how an approximation to v_F can be improved.

Lemma 3.23. *Let $F \in \mathrm{Irr}(K)$ and let (μ,ϕ) be a type with $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(F)$. Suppose $\phi \neq F$, denote $v_F(\phi) = \lambda < \infty$ and consider the augmentation $[\mu;\phi,\lambda] =: \mu_\lambda$. We have $\mathbf{t}(\mu_\lambda, v_F) \neq [\phi]_{\mu_\lambda}$, and for each $\phi' \in \mathbf{t}(\mu_\lambda, v_F)$, the type (μ_λ,ϕ') satisfies $\mathrm{in}_{\mu_\lambda}(\phi') \mid \mathrm{in}_{\mu_\lambda}(F)$ and $u(F,\phi') > u(F,\phi)$.*

Proof. Since $\lambda = \mu_\lambda(\phi) = v_F(\phi)$, we have $\phi \notin \mathbf{t}(\mu_\lambda, v_F)$ by definition of tangent direction. Hence $\mathbf{t}(\mu_\lambda, v_F) \neq [\phi]_{\mu_\lambda}$ because tangent directions are equivalence classes of key polynomials by Lemma 2.37. For all $\phi' \in \mathbf{t}(\mu_\lambda, v_F)$, the type (μ_λ,ϕ') satisfies $\mathrm{in}_{\mu_\lambda}(\phi') \mid \mathrm{in}_{\mu_\lambda}(F)$ by Theorem 3.18. Since $\phi \in \mathrm{KP}(\mu_\lambda)$ by Lemma 2.43, we deduce

$$u(F,\phi') = \frac{v_F(\phi')}{\deg(\phi')} > \frac{\mu_\lambda(\phi')}{\deg(\phi')} = \frac{\mu_\lambda(\phi)}{\deg(\phi)} = u(F,\phi)$$

by Theorem 2.12. □

The rest of this section is about approaching a $g \in K[x]$, viewed as a set of points in $\mathrm{Irr}(K)$. The following lemma shows the well-known fact: "all triangles in an ultrametric space are isoceles".

Lemma 3.24. *Let (X,u) be an ultrametric space and $a, b, c \in X$. Then,*

$$u(a,c) \neq u(c,b) \Longrightarrow \min\{u(a,c), u(c,b)\} = u(a,b)$$

Proof. We have $\min\{u(a,c), u(c,b)\} \leq u(a,b)$ by the triangle inequality. Suppose that $\min\{u(a,c), u(c,b)\} < u(a,b)$ and suppose without loss of generality that $u(a,c) < u(c,b)$. By the triangle inequality, we have

$$u(a,c) < \min\{u(a,b), u(b,c)\} \leq u(a,c)$$

which is a contradiction, hence $\min\{u(a,c), u(c,b)\} = u(a,b)$ as required. □

Let (X,u) be an ultrametric space. Let $S = \{x_1, \ldots, x_k\}$ be a non-empty finite set $S \subset X$. We define the **radius of separation** $r(S)$ to be

$$r(S) = \begin{cases} -\infty & \text{if } S \text{ is a single point} \\ \max\{u(x_i, x_j) \mid i \neq j\} & \text{otherwise} \end{cases}$$

Lemma 3.25. *Let (X,u) be an ultrametric space. Let $S = \{x_1, \ldots, x_k\}$ be a non-empty finite set $S \subset X$. Suppose $y \in X$ satisfies $r(S) < u(y, x_i)$ for some i, then for all $i \neq j$ we have $u(y, x_j) \leq r(S)$.*

Proof. The claim is vacuously true if S is a single point.

Choose any $j \neq i$. By the ultrametric triangle inequality, we have

$$\min\{u(y, x_i), u(x_i, x_j)\} \leq u(y, x_j).$$

As $u(x_i, x_j) < u(y, x_i)$ by assumption, we have $u(x_i, x_j) = u(y, x_j)$ by Lemma 3.24 as required. □

Remark 3.26. *The moral of the above lemma is that if you get closer than $r(S)$ to S, you are closest to a unique point of S and all other points of S are at least $r(S)$ away.*

Let $g \in K[x]$ be non-constant and denote the set of its distinct irreducible factors by $\mathcal{F}(g) := \{G \in \mathrm{Irr}(K) \mid G \text{ divides } g\}$. Define the **radius of separation of** g to be $r(\mathcal{F}(g))$ and denote it $r(g)$. In other words,

$$r(g) = \begin{cases} -\infty & \mathcal{F}(g) \text{ is a singleton} \\ \max\{u(F,G) \mid F, G \in \mathrm{Irr}(K),\ F \text{ and } G \text{ divide g},\ F \neq G\} & \text{otherwise} \end{cases}$$

Let us show how $r(g)$ is related to Krasner's constant. Recall that a non-constant polynomial $g \in K[x]$ is **purely inseparable** if g has exactly one root in an algebraic closure. A non-constant $g \in K[x]$ is **separable** if the number of distinct roots of g in an algebraic closure is equal to the degree of g. It follows from these definitions that a non-constant $g \in K[x]$ is simultaneously separable and purely inseparable if and only if $\deg(g) = 1$. Let $\overline{v}$ be the unique extension of v to a fixed algebraic closure $\overline{K}$ of K.

Definition 3.27. *Let $g \in K[x]$ be non-constant, we define **Krasner's constant** of g to be*

$$\mathrm{kras}(g) = \begin{cases} -\infty & \textit{if } g \textit{ is purely inseparable} \\ \max\{\overline{v}(\theta' - \theta) \mid \theta \neq \theta' \textit{ are roots of } g \textit{ in } \overline{K}\} \in \Gamma_{\mathbb{Q}} & \textit{otherwise} \end{cases}$$

By the henselian property, this definition does not depend on $\overline{v}$.

Lemma 3.28. *For all $F, G \in \mathrm{Irr}(K)$ with $F \neq G$, we have $u(F,G) \leq \mathrm{kras}(FG)$.*

Proof. Let $\overline{K}$ be an algebraic closure of K and $\overline{v}$ an extension of v to K. Fix a $\theta \in Z(F)$ and write $Z(G) = \{\alpha_1, \dots \alpha_{\deg(G)}\}$. We have

$$u(F,G) = \frac{\overline{v}(G(\theta))}{\deg(G)} = \frac{1}{\deg(G)} \sum_{i=1}^{\deg(G)} \overline{v}(\theta - \alpha_i) \leq \mathrm{kras}(FG)$$

because an average is bounded by the maximum of its terms. □

Remark 3.29. *Clearly for all non-constant $h \in K[x]$, if $h \mid g$, then $\mathrm{kras}(h) \leq \mathrm{kras}(g)$. Hence, $r(g) \leq \mathrm{kras}(g)$ by the lemma above.*

We conclude this section by giving a basic effective bound on Krasner's constant of a separable polynomial.

Lemma 3.30. *Let $f \in K[x]$ be a monic, separable polynomial with $deg(f) \geq 2$. Write Δ for the discriminant, let $S := \{\frac{v(a_0)}{n}, \dots, \frac{v(a_{n-1})}{1}\}$. Then,*

$$kras(f) \leq \frac{v(\Delta_f)}{2} - \frac{(n(n-1)-2)}{2} min(S).$$

Proof. We will work inside a fixed algebraic closure $\overline{K}$ of K, denote the unique extensions of v to $\overline{K}$ by $\overline{v}$.

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, fix some non-zero $A \in K$ and let $g = x^n + Aa_{n-1}x^{n-1} + \cdots + A^n a_0$. Note that f and g have the same degree and are both monic. Moreover, α is a root of f if and only if $\beta := A\alpha$ is a root of g. Let $Z(f) = \{\alpha_1, \dots, \alpha_n\}$ and $Z(g) = \{\beta_1, \dots, \beta_n\}$ where $\beta_i = A\alpha_i$. We have

$$\begin{aligned}
\mathrm{kras}(g) &= \max\{\overline{v}(\beta_i - \beta_j) \mid i \neq j\} \\
&= \max\{\overline{v}(\alpha_i - \alpha_j) + v(A) \mid i \neq j\} \\
&= \max\{\overline{v}(\alpha_i - \alpha_j) \mid i \neq j\} + v(A) = \mathrm{kras}(f) + v(A).
\end{aligned}$$

Moreover we have

$$\begin{aligned}
\Delta_g &= \prod_{i<j} (\beta_i - \beta_j)^2 = \prod_{i<j} (A\alpha_i - A\alpha_j)^2 \\
&= A^{2\frac{n(n-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\
&= A^{n(n-1)} \Delta_f.
\end{aligned}$$

Let μ be the depth-zero valuation that acts on $x-$expansions as $\mu(a_0 + a_1 x + \cdots + a_r x^r) = \min\limits_{0 \leq i \leq r} \{\mu(a_i)\}$ (Gauss valuation).

For any non-zero $A \in K$ such that $0 \leq \mu(g)$, we have $0 \leq \overline{v}(\beta_i)$ for all $1 \leq i \leq n$ because valuation rings are integrally closed. This shows $\overline{v}(\beta_i - \beta_j) \geq 0$ for all $i \neq j$. Hence, $\frac{v(\Delta_g)}{2} \geq \operatorname{kras}(g)$, which shows

$$\frac{v(\Delta_g)}{2} \geq \operatorname{kras}(f) + v(A).$$

Hence

$$\frac{n(n-1)-2}{2} v(A) + \frac{v(\Delta_f)}{2} \geq \operatorname{kras}(f).$$

Note that

$$\mu(g) \geq 0 \iff v(A^{n-i}a_i) \geq 0 \text{ for all } 0 \leq i \leq n-1 \iff -v(A) \geq \min(S)$$

and the result follows by taking any non-zero $A \in K$ with $v(A) = -\min(S)$. □

3.6 The defect

Let w be the unique extension of v to a finite extension L/K.

Definition 3.31. *The **defect** of w/v is*

$$d(w/v) = \frac{[L:K]}{e(w/v)f(w/v)}.$$

The **characteristic exponent** of (K, v) is the natural number $p = \operatorname{char}(k_v)$ if $\operatorname{char}(k_v) > 0$ and $p = 1$ otherwise. By a lemma of Ostrowski [13, Lemma 11.17], we have

$$d(w/v) = p^k \tag{13}$$

for some $k \in \mathbb{N}$.

Let $F \in \operatorname{Irr}(K)$ and let $\overline{v_F}$ be the valuation on $K[x]/(F)$ induced by v_F, then by definition

$$\deg(F) = d(\overline{v_F}/v)e(\overline{v_F}/v)f(\overline{v_F}/v).$$

Definition 3.32. *We say that $F \in \operatorname{Irr}(K)$ is **defectless** if $d(\overline{v_F}/v) = 1$.*

Obviously all linear $F \in K[x]$ are defectless. We can find more examples using Eq. (13). Clearly, if $\operatorname{char}(k_v) = 0$, then $p = 1$ so all $F \in \operatorname{Irr}(K)$ are defectless. If $p = \operatorname{char}(k_v) > 0$, then each $F \in \operatorname{Irr}(K)$ with $p \nmid \deg(F)$ is defectless.

Vaquié characterized the property of being defectless as follows [29], [20, Corollary 6.1] or [21, Corollary 6.16].

Theorem 3.33. *An $F \in \operatorname{Irr}(K)$ is defectless if and only if v_F is inductive.*

We will now present a related characterization of this property in terms of "weighted values". Fix an $F \in K[x]$ and for arbitrary non-constant $g \in K[x]$, define

$$\operatorname{wt}(g) = \frac{v_F(g)}{\deg(g)} \in \Gamma_{\mathbb{Q}}$$

Remark 3.34. *Observe that if g is monic and irreducible, by definition $wt(g) = u(F, g)$.*

Assume that $n := \deg(F) > 1$ and for each $1 < m \leq n$ consider the following set

$$W_m = \{\mathrm{wt}(g) \mid g \in K[x],\ g \text{ monic, and } 1 \leq \deg(g) < m\}.$$

Clearly, $W_2 \subset W_3 \subset \cdots \subset W_n$.

The following theorem is also due to Vaquié [29], see also [7, Theorem 5.7].

Theorem 3.35. *An $F \in \mathrm{Irr}(K)$ with $n := \deg(F) > 1$ is defectless if and only if W_m contains a maximal element for each $1 < m \leq n$.*

Definition 3.36. *The **Okutsu bound** of a defectless $F \in \mathrm{Irr}(K)$ of degree $n := \deg(F)$ is $\delta(F) = \max(W_n)$ if $n > 1$ and $\delta(F) = -\infty$ otherwise.*

By Remark 3.34, we immediately get the following.

Corollary 3.37. *Let $F \in \mathrm{Irr}(K)$ be a defectless polynomial, then for all $\phi \in \mathrm{Irr}(K)$*

$$u(F, \phi) > \delta(F) \Longrightarrow \deg(\phi) \geq \deg(F).$$

Even if F is not defectless, the sets W_m for each $1 < m \leq n$ are bounded above by an element of $\Gamma_{\mathbb{Q}}$ provided F is separable.

Proposition 3.38. *[4, Corollary 3.3] If F is separable, then every $\gamma \in W_n$ satisfies $\gamma \leq \mathrm{kras}(F)$.*

Hence, Corollary 3.37 also holds with "defectless" replaced by "separable" and $\delta(F)$ by $\mathrm{kras}(F)$.

If $F \in \mathrm{Irr}(K)$ is not separable and $d(\overline{v_F}/v) > 1$, the set W_n may be unbounded in $\Gamma_{\mathbb{Q}}$.

Remark 3.39. *By Theorem 3.35, it is impossible to get arbitrarily close to a defectless polynomial by a monic polynomial of strictly lower degree. In particular if (μ, ϕ) is a type such that $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(F)$, then $\deg(\phi) \mid \deg(F)$ by Theorem 3.18 so if additionally $u(F, \phi) > \delta(F)$, we have $\deg(\phi) = \deg(F)$ by Corollary 3.37.*

4 Polynomial factorization over henselian fields

4.1 Types partition the set of irreducible factors

In this section, we think of a type (μ, ϕ) as "seeing" a certain subset of the distinct irreducible factors of $g \in K[x]$ via the relation "$\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(g)$" in view of Theorem 3.18. We prove some technical results that will enable us to show termination of our algorithms.

Fix a monic, non-constant $g \in K[x]$ and a type (μ, ϕ). For the rest of this section assume that g is square-free (but not necessarily separable).

Definition 4.1. *For all $\lambda \in \Gamma_{\mathbb{Q}}$ consider the following sets.*

$$\begin{aligned}
\mathcal{F}(g) &= \{G \in \mathrm{Irr}(K) \mid G \text{ divides } g\}.\\
\mathcal{F}_\mu(g) &= \{G \in \mathcal{F}(g) \mid \mu < v_G\}.\\
\mathcal{F}_{\mu,\phi}(g) &= \{G \in \mathcal{F}(g) \mid \mu < v_G \text{ and } \mathbf{t}(\mu, v_G) = [\phi]_\mu\}.\\
\mathcal{F}_{\mu,\phi}(g)(\lambda) &= \{G \in \mathcal{F}_{\mu,\phi}(g) \mid v_G(\phi) = \lambda\}.
\end{aligned}$$

Remark 4.2. *By Theorem 3.18, we have $\mathcal{F}_{\mu,\phi}(g) = \{G \in \mathcal{F}(g) \mid \mathrm{in}_\mu(\phi) \text{ divides } \mathrm{in}_\mu(G)\}$.*

Lemma 4.3. *The following are equivalent.*

(1) $\mathcal{F}_{\mu,\phi}(g) \neq \emptyset$.
(2) $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(g)$.
(3) $\ell(N^+_{\mu,\phi}(g)) > 0$.

Proof. Since $\mathcal{F}_{\mu,\phi}(g) = \{G \in \mathcal{F}(g) \mid \mathrm{in}_\mu(\phi) \text{ divides } \mathrm{in}_\mu(G)\}$, $\mathrm{in}_\mu(\phi)$ is a prime element, and $\mathrm{in}_\mu(ab) = \mathrm{in}_\mu(a)\,\mathrm{in}_\mu(b)$ for all $a, b \in K[x]$, we have (1) $\iff$ (2).

By Eq. (12), the non-negative integer $\ell(N^+_{\mu,\phi}(g))$ is the order with which the prime $\mathrm{in}_\mu(\phi)$ divides $\mathrm{in}_\mu(g)$, which shows (2) $\iff$ (3). □

Definition 4.4. *We say that (μ, ϕ)* ***singles out*** *an irreducible factor of g if $\mathcal{F}_{\mu,\phi}(g) = \{G\}$ for some $G \in \mathrm{Irr}(K)$ and $\deg(\phi) = \deg(G)$.*

So the above definition implies that the type (μ, ϕ) singles out an irreducible factor of g if and only if $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(G)$ for a unique $G \in \mathcal{F}(g)$ and ϕ satisfies the additional condition that $\deg(\phi) = \deg(G)$.

Remark 4.5. *If (μ, ϕ) singles out an irreducible factor G of g, then $\mathrm{in}_\mu(G) = \mathrm{in}_\mu(\phi)$ by Theorem 3.18, $\deg(G) = \deg(\phi)$ and G is monic. Hence, $G \in \mathrm{KP}(\mu)$. It follows from Theorem 3.33 that if G is not defectless, then the valuation μ is not inductive; if μ is inductive and $G \in \mathrm{KP}(\mu)$ is not defectless, we have $v_G = [\mu; G, \infty]$, contradiction.*

The property "singles out" can be completely characterized in terms of the length of the principal polygon of g.

Proposition 4.6. *The following are equivalent.*

(1) *(μ, ϕ) singles out an irreducible factor of g*
(2) $\ell(N^+_{\mu,\phi}(g)) = 1$

Proof. By Theorem 3.18, for each $G \in \mathrm{Irr}(K)$, if $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(G)$, then either $\phi = G$ or $N_{\mu,\phi}(G)$ is one sided of slope $-v_G(\phi) < -\mu(\phi)$. In both cases, we have $N_{\mu,\phi}(G) = N^+_{\mu,\phi}(G)$ by definition of principal Newton polygon. So, if $\mathcal{F}_{\mu,\phi}(g) = \{G\}$, then $\ell(N^+_{\mu,\phi}(g)) = \ell(N^+_{\mu,\phi}(G)) = \deg(G)/\deg(\phi)$ where the first equality is by Theorem 3.9 and Eq. (12), and the second equality is by Theorem 3.18. Clearly, (1) $\implies$ (2).

Conversely, since $\ell(N^+_{\mu,\phi}(g)) \geq \ell(N^+_{\mu,\phi}(FG)) \geq 2$ for $F, G \in \mathcal{F}_{\mu,\phi}(g)$ with $F \neq G$, the set $\mathcal{F}_{\mu,\phi}(g)$ is a one element set and hence (2) $\implies$ (1). □

Proposition 4.7. *Suppose that* $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(g)$ *and* $\phi \nmid g$. *Then,*

$$\mathcal{F}_{\mu,\phi}(g) = \bigsqcup_{\lambda} \mathcal{F}_{\mu,\phi}(g)(\lambda)$$

where $-\lambda$ *runs over the slopes of sides of* $N^+_{\mu,\phi}(g)$.

Proof. Let $g_1 \in K[x]$ be the product of all $G \in \mathcal{F}_{\mu,\phi}(g)$ and define $g_2 := g/g_1$. By Theorem 3.9, we have $N^+_{\mu,\phi}(g) = N^+_{\mu,\phi}(g_1) + N^+_{\mu,\phi}(g_2)$. By construction $\mathrm{in}_\mu(\phi) \nmid \mathrm{in}_\mu(g_2)$, and hence $\ell(N^+_{\mu,\phi}(g_2)) = 0$ which shows that $N^+_{\mu,\phi}(g_2)$ is a single point of the form $(0,\alpha) \in \mathbb{Q} \times \Gamma_{\mathbb{Q}}$. Hence $N^+_{\mu,\phi}(g)$ is $N^+_{\mu,\phi}(g_1)$ shifted vertically by α, so in particular these two polygons have the same number of sides, length of sides and slopes of sides.

By our assumptions and Theorem 3.18, $\mathcal{F}_{\mu,\phi}(g) \neq \emptyset$, each $G \in \mathcal{F}_{\mu,\phi}(g)$ satisfies $N_{\mu,\phi}(G) = N^+_{\mu,\phi}(G)$ and this polygon is one sided of slope $-v_G(\phi)$. Hence, the set $\{\mathrm{slope}(S) \mid S \text{ is a side of } N^+_{\mu,\phi}(g_1)\}$ is equal to $\{-v_G(\phi) \mid G \in \mathcal{F}_{\mu,\phi}(g)\}$ by Theorem 3.9, which completes the proof. □

Lemma 4.8. *Suppose* (μ,ϕ) *singles out an irreducible factor* $G \in \mathcal{F}(g)$. *If* $\phi \neq G$, *then*

$$u(G,\phi) = \frac{\lambda}{\deg(\phi)}$$

where $-\lambda = \mathrm{slope}(N^+_{\mu,\phi}(g))$.

Proof. Follows immediately from Theorem 3.18 and Proposition 4.6. □

We will now show how $\mathcal{F}_{\mu,\phi}(g)(\lambda)$ can be partitioned according to the tangent directions of the augmented valuation $\mu_\lambda = [\mu;\phi,\lambda]$.

Definition 4.9.

$$\mathbf{T}_\mu(g) = \{\mathbf{t}(\mu, v_G) \mid G \in \mathcal{F}_\mu(g)\}.$$

Proposition 4.10. *Suppose that* $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(g)$ *and* $\phi \nmid g$. *Let* $-\lambda$ *be the slope of a side of* $N^+_{\mu,\phi}(g)$ *and let* $\mu_\lambda = [\mu,\phi,\lambda]$. *For each* $\mathbf{t} \in \mathbf{T}_{\mu_\lambda}(g)$ *with* $\mathbf{t} \neq [\phi]_{\mu_\lambda}$ *make an arbitrary choice* $\phi'_{\mathbf{t}} \in \mathbf{t}$, *then*

$$\mathcal{F}_{\mu,\phi}(g)(\lambda) = \bigsqcup_{\mathbf{t} \in \mathbf{T}_{\mu_\lambda}(g),\ \mathbf{t} \neq [\phi]_{\mu_\lambda}} \mathcal{F}_{\mu_\lambda,\phi'_{\mathbf{t}}}(g).$$

Proof. The LHS is contained in the RHS by Lemma 3.23.

Note that the RHS is cointained in $\mathcal{F}_{\mu_\lambda}(g)$ and each $G \in \mathcal{F}_{\mu_\lambda}(g)$ satisfies $\lambda = \mu_\lambda(\phi) \leq v_G(\phi)$. So for each such G, we have $\lambda < v_G(\phi)$ if and only if $\mathbf{t}(\mu_\lambda, v_G) = [\phi]_{\mu_\lambda}$ by Theorem 3.18. Hence each G on the RHS satisfies $v_G(\phi) = \lambda > \mu(\phi)$, which shows $\mathbf{t}(\mu, v_G) = [\phi]_\mu$ by Lemma 2.40 and hence $G \in \mathcal{F}_{\mu,\phi}(g)(\lambda)$.

If (μ,ϕ_1) and (μ,ϕ_2) are any two types such that $G \in \mathcal{F}_{\mu,\phi_1}(g) \cap \mathcal{F}_{\mu,\phi_2}(g)$ for some $G \in \mathrm{Irr}(K)$, we have $[\phi_1]_\mu = \mathbf{t}(\mu, v_G) = [\phi_2]_\mu$ by Theorem 3.18, so RHS is a disjoint union because the $\phi'_{\mathbf{t}}$ come from distinct tangent directions. □

Definition 4.11. *Let $T = \{(\mu_1, \phi_1), \ldots, (\mu_k, \phi_k)\}$ be a non-empty finite multi-set of types such that for all $1 \leq i, j \leq k$*

(1) $\mathcal{F}_{\mu_i,\phi_i}(g) \neq \emptyset$
(2) $\mathcal{F}_{\mu_i,\phi_i}(g) \cap \mathcal{F}_{\mu_j,\phi_j}(g) \neq \emptyset$ if and only if $i = j$
(3) $\bigcup \mathcal{F}_{\mu_i,\phi_i}(g) = \mathcal{F}(g)$

*We say that T **partitions** g.*

Remark 4.12. *These conditions imply that the elements of the multiset T are distinct, in other words T equals its underlying set. Moreover, $|T| \leq |\mathcal{F}(g)|$ and every $G \in \mathcal{F}(g)$ has $G \in \mathcal{F}_{\mu_i,\phi_i}(g)$ for a unique index i.*

For a pair of distinct types in T, it may still happen that either $\mu_i = \mu_j$ or $\phi_i = \phi_j$.

Proposition 4.13. *There exists a set of types that partitions g.*

Proof. Choose any $\gamma \in \Gamma := \Gamma_v$ that satisfies $\gamma < \min\{\overline{v}(\theta) \mid \theta \in \overline{K},\ g(\theta) = 0\}$ and let μ be the depth-zero valuation $\mu = [v; x, \gamma]$. Let $f = a_0 + a_1 x + \cdots + a_r x^r$ be the $x-$expansion of $f \in K[x]$, then by construction

$$\mu(f) = \min_{0 \leq i \leq r} \{v(a_i) + \gamma i\} \leq \min_{0 \leq i \leq r} \{v_G(a_i x^i)\} \leq v_G(f)$$

for all $G \in \mathcal{F}(g)$. Since $\mu(x) = \gamma < \overline{v}(\theta) = v_G(x)$, where $\theta \in Z(G)$ by construction, we deduce $\mathbf{t}(\mu, v_G) = [x]_\mu$ which shows $\mathcal{F}_{\mu,x}(g) = \mathcal{F}(g)$ so the singleton $\{(\mu, x)\}$ partitions g. □

Remark 4.14. *The values $-\overline{v}(\theta)$ where $\theta \in Z(g)$, are the slopes of sides of the classical Newton polygon $N_{v,x}(g)$, which is easy to compute [3, Theorem 4.1].*

Clearly, if T partitions g, then $\bigcup \mathcal{F}_{\mu_i,\phi_i}(g)$ is a partition of $\mathcal{F}(g)$. It may happen that two different sets of types that partition g determine the same partition of $\mathcal{F}(g)$.

Definition 4.15. *Let X be a set and α, β be two partitions of X. We say that β **is finer than** α if every element of β is a subset of some element of α. We say β is **strictly finer than** α if β is finer than α and some element of β is a proper subset of an element of α.*

If T, T' are two sets of types that partition g, we say T' **is (strictly) finer than** T if the corresponding statement holds for the partitions of $\mathcal{F}(g)$ determined by T' and T respectively.

Before we state and prove the final result of this section, we introduce some notation.

For a Newton polygon N, we denote the set of slopes of its sides by

$$\text{slopes}(N) := \{\text{slope}(S) \mid S \text{ is a side of } N\}.$$

Recall that for a type (μ, ϕ) and $-\lambda \in \text{slopes}(N^+_{\mu,\phi}(g))$, we denote $\mu_\lambda := [\mu; \phi, \lambda]$.

The result below is the main result of this section. It follows at once from Proposition 4.7 and Proposition 4.10.

Theorem 4.16. *Let T be a set of types that partitions g and suppose that all $(\mu, \phi) \in T$ satisfy $\phi \nmid g$. For each triple $((\mu, \phi), \lambda, \mathbf{t})$ where $(\mu, \phi) \in T$, $-\lambda \in \operatorname{slopes}(N^+_{\mu,\phi}(g))$ and $\mathbf{t} \in \mathbf{T}_{\mu_\lambda}(g) \backslash \{[\phi]_{\mu_\lambda}\}$, make an arbitrary choice $\phi'_{(\mu,\phi),\lambda,\mathbf{t}} \in \mathbf{t}$. Then, the multiset*

$$T' = \{(\mu_\lambda, \phi'_{(\mu,\phi),\lambda,\mathbf{t}}) : (\mu, \phi) \in T,\ -\lambda \in \operatorname{slopes}(N^+_{\mu,\phi}(g)),\ \mathbf{t} \in \mathbf{T}_{\mu_\lambda}(g) \backslash \{[\phi]_{\mu_\lambda}\}\}$$

partitions g and T' is finer than T.

Remark 4.17. *Let $g = G_1 \dots G_k$ be the irreducible factorization of g, then Theorem 4.16 gives us a recipe to produce a sequence $T_1, T_2, \dots$ of sets of types that partition g such that T_{i+1} is finer than T_i. Clearly, if we can ensure that T_{i+1} is strictly finer than T_i sufficiently many times in this sequence, we will reach the finest partition $\mathcal{F}(g) = \bigsqcup\{G_i\}$.*

Definition 4.18. *Let T be a set of types that partitions g. We say that T* ***singles out the irreducible factors of*** *g if the partition determined by T is the finest partition and each $(\mu, \phi) \in T$ singles out an irreducible factor of g.*

4.2 An OM factorization algorithm

The aim of this section is to make the "refinement step" Theorem 4.16 constructive and show this leads to a polynomial factorization algorithm.

Let $g \in K[x]$ be monic, square-free and let T be a set of types that partitions g. We can assume that all $(\mu, \phi) \in T$ satisfy $\phi \nmid g$, otherwise we can divide g by ϕ and consider $T \backslash \{(\mu, \phi)\}$. Let $(\mu, \phi) \in T$, then $\mathcal{F}_{\mu,\phi}(g)$ is non-empty and the set $\{-v_G(\phi) \mid G \in \mathcal{F}_{\mu,\phi}(g)\}$ coincides with the set of slopes of sides of $N^+_{\mu,\phi}(g)$. Let $-\lambda$ be one of these slopes and consider the augmented valuation $\mu_\lambda = [\mu; \phi, \lambda]$. Let e be the relative ramification index of μ_λ and let $u \in \mathcal{G}_{\mu_\lambda}$ be a unit of grade $e\mu_\lambda(\phi)$. Denote the residual polynomial operator $R_{\mu_\lambda,\phi} := R_{\mu_\lambda,\phi,u}$ suppressing its dependence on u in view of Remark 2.35. We give a constructive version of Proposition 4.10 below.

Algorithm 1: extensions

Input:

- a non-trivially valued henselian field $\mathbf{K} := (K, v)$
- a monic, square-free $g \in K[x]$;
- a type (μ, ϕ) with $\operatorname{in}_\mu(\phi) \mid \operatorname{in}_\mu(g)$ and $\phi \nmid g$
- a $\lambda \in \Gamma_{\mathbb{Q}}$ such that $-\lambda$ is the slope of a side of $N^+_{\mu,\phi}(g)$.

Output:

- the list of types $(\mu_\lambda, \phi'_{\mathbf{t}})$ where $\phi'_{\mathbf{t}}$ is a choice $\phi'_{\mathbf{t}} \in \mathbf{t}$ for each $\mathbf{t} \in \mathbf{T}_{\mu_\lambda}(g)$ with $\mathbf{t} \neq [\phi]_{\mu_\lambda}$

1 compute and factorize the residual polynomial $R_{\mu_\lambda,\phi}(g) = \psi_1^{n_1} \dots \psi_s^{n_s}$ into powers of distinct monic irreducible polynomials $\psi_i \in \operatorname{Irr}(\kappa_{\mu_\lambda})$
2 for each $1 \leq i \leq s$ choose $\phi'_i \in \operatorname{KP}(\mu_\lambda)$ such that $R_{\mu_\lambda,\phi}(\phi'_i) = \psi_i$, Eq. (8)
3 return the list $[(\mu_\lambda, \phi'_i) \mid 1 \leq i \leq s]$

Proposition 4.19. *The algorithm Algorithm 1 has the right output.*

Proof. Factorize $\mathrm{in}_{\mu_\lambda}(g) = t_0^{m_0} t_1^{m_1} \dots t_k^{m_k}$, where $t_i \in \mathcal{G}_{\mu_\lambda}$ are pairwise non-associate homogeneous prime elements and $n_i > 0$ for all $0 \leq i \leq k$. By Eq. (5), we have

$$\mathrm{in}_{\mu_\lambda}(g) = \mathrm{lc}_{\mu_\lambda}(g)\, \mathrm{in}_{\mu_\lambda}(\phi)^{\ell_0} u^d R_{\mu_\lambda,\phi}(g)$$

where $\ell_0 = \ell(N^+_{\mu_\lambda,\phi}(g))$ is the order with which the prime $\mathrm{in}_{\mu_\lambda}(\phi)$ divides $\mathrm{in}_{\mu_\lambda}(g)$ and $d \in \mathbb{N}$. Since the elements $\psi_i \in \mathcal{G}_{\mu_\lambda}$ are pairwise non-associate prime elements, we have $s = k$ and without loss of generality $\ell_0 = n_0$ and $m_i = n_i$ for all $1 \leq i \leq s$. By Eq. (8), the classes $[\phi'_i]$ are distinct for all $1 \leq i \leq k$. Hence, the $\mathrm{in}_{\mu_\lambda}(\phi'_i)$ are pairwise non-associate, because $\mathrm{in}_{\mu_\lambda}(Q) \mid \mathrm{in}_{\mu_\lambda}(Q') \iff [Q]_{\mu_\lambda} = [Q']_{\mu_\lambda}$ for all $Q, Q' \in \mathrm{KP}(\mu_\lambda)$ by Theorem 2.34. Hence,

$$\mathrm{in}_{\mu_\lambda}(g) \sim_{unit} \mathrm{in}_{\mu_\lambda}(\phi)^{\ell_0}\, \mathrm{in}_{\mu_\lambda}(\phi'_1)^{n_1} \cdot \dots \cdot \mathrm{in}_{\mu_\lambda}(\phi'_s)^{n_s}$$

is the prime factorization of $\mathrm{in}_{\mu_\lambda}(g)$.

By Theorem 3.18 a $G \in \mathcal{F}_{\mu_\lambda}(g)$ satisfies $\lambda < v_G$ if and only if $\mathbf{t}(\mu_\lambda, v_G) = [\phi]_{\mu_\lambda}$ if and only if $\mathrm{in}_{\mu_\lambda}(G)$ is a positive integer power of the prime $\mathrm{in}_{\mu_\lambda}(\phi)$. We deduce that $\{[\phi'_i]_{\mu_\lambda} \mid 1 \leq i \leq s\} = \mathbf{T}_{\mu_\lambda}(g) \backslash [\phi]_{\mu_\lambda}$. □

By the above, we can obtain a set of types T' that is finer than T. This leads to an algorithm that either correctly guesses some irreducible factors of g or outputs a list of types that singles out all the irreducible factors of g. Moreover, each type in the list approximates its irreducible factor with quality at least $\gamma \in \Gamma_{\mathbb{Q}}$.

Algorithm 2: OMalgorithm

Input:

- a non-trivially valued henselian field (K, v)
- a monic, square-free $g \in K[x]$
- a $\gamma \in \Gamma_{\mathbb{Q}}$

Output:

- either a non-empty list that consists of some elements of $\mathcal{F}(g)$ or
- a non-empty list T, of types, that singles out the irreducible factors of g, such that each $(\mu, \phi) \in T$ satisfies $\phi \notin \mathcal{F}(g)$ and $u(G_{\mu,\phi}, \phi) > \gamma$ where $G_{\mu,\phi} \in \mathcal{F}(g)$ is the irreducible factor singled out by (μ, ϕ).

$T \leftarrow$ an arbitrary choice of a list of types that partitions g; for example $T \leftarrow [(\mu, \phi)]$ as in Proposition 4.13
if *some* $(\mu, \phi) \in T$ *satisfies* $\phi \mid g$ **then**
    return the list $[\phi : (\mu, \phi) \in T \text{ and } \phi \mid g]$
else if *for all* $(\mu, \phi) \in T$*, we have* $\ell(N^+_{\mu,\phi}(g)) = 1$ *and* $\frac{-\operatorname{slope}(N^+_{\mu,\phi}(g))}{\deg(\phi)} > \gamma$ **then**
    return T
else
    Initialise an empty list $T' = []$
    forall $(\mu, \phi) \in T$ **do**
        forall $S \in \operatorname{sides}(N^+_{\mu,\phi}(g))$ **do**
            initialise an empty list $E = [],\ \lambda \leftarrow -\operatorname{slope}(S)$
            $E \leftarrow \operatorname{extensions}(\mu, \phi, \lambda, g)$
            append the contents of E to T'
    $T \leftarrow T'$ and **goto** 2.

Proposition 4.20. *If Algorithm 2 terminates, it has the right output.*

Proof. We will go through the flow of the algorithm starting from the beginning. If 2. and 4. are not satisfied, then the set T' in 13. is a set of types that partitions g by Theorem 4.16 and Proposition 4.19. Hence, whenever we are are in 2. or 4., we can assume the set T partitions g. If 2. is satisfied, the output is clearly correct. If 4. is satisfied, then 2. wasn't satisfied so all $(\mu, \phi) \in T$ have $\phi \nmid g$ and we deduce the output is correct by Proposition 4.6 and Lemma 4.8. □

The output of the above algorithm naturally leads to the following.

Definition 4.21. *Let $g \in K[x]$ be a monic, square-free polynomial. Let $g = G_1 \cdot \cdots \cdot G_k$ where $G_i \in \mathrm{Irr}(K)$ for all $1 \leq i \leq k$ be its factorization into irreducibles. Let $\gamma \in \Gamma_{\mathbb{Q}}$. A γ-**factorization** of g is a multiset $\{\phi_1, \ldots, \phi_k\}$ where $\phi_i \in \mathrm{Irr}(K)$, such that, up to a suitable re-ordering, the following hold for each $1 \leq i \leq k$.*

(1) $\deg(\phi_i) = \deg(G_i)$.
(2) $u(G_i, \phi_i) > \gamma$.

For example the set $\mathcal{F}(g)$ is a $\gamma-$factorization of g for all $\gamma \in \Gamma_{\mathbb{Q}}$.

Remark 4.22. *Clearly, if S_1 is a $\gamma-$factorization of g_1 and S_2 is a $\gamma-$factorization of g_2, then $S_1 \cup S_2$ (union of multisets) is a $\gamma-$factorization of $g_1 g_2$.*

We can compute $\gamma-$factorizations using Algorithm 2 as follows.

Algorithm 3: OMfactorization

Input:

- a non-trivially valued henselian field $\mathbf{K} := (K, v)$
- a monic, square-free $g \in K[x]$
- a $\gamma \in \Gamma_{\mathbb{Q}}$

Output:

- a $\gamma-$factorization of g

1 FACTORS $\leftarrow$ []
2 $f \leftarrow g$
3 $T \leftarrow$ OMalgorithm$(\mathbf{K}, f, \gamma)$
4 **if** $f = 1$ **then**
5 $\quad$ **return** FACTORS
6 **else if** T *is a list of types* **then**
7 $\quad$ append the contents of the list $[\phi : (\mu, \phi) \in T]$ to FACTORS
8 $\quad$ **return** FACTORS
9 **else**
10 $\quad$ append the contents of the list T to FACTORS
11 $\quad$ $f \leftarrow \frac{f}{\prod_{G \in T} G}$; divide f by the product of $G \in T$
12 $\quad$ **goto** 3.

Proposition 4.23. *If Algorithm 3 terminates, it has the right output.*

Proof. Suppose the algorithm is running. It follows from Algorithm 2, that if 6. is true, Algorithm 3 immediately terminates. Suppose that Algorithm 3 terminated in 4., then in particular 6. was never true while the algorithm was running, so the list FACTORS consists of all the elements of $\mathcal{F}(g)$, which is clearly the right output.

If Algorithm 3 terminated in 6., this was preceded by some number (possibly zero) of instances when Algorithm 2 returned some subset of $\mathcal{F}(g)$ and these irreducible factors were "divided out" in 11. and subsequently stored in the list FACTORS. If there were zero such instances, then Algorithm 3 has the right output because it is just the output of Algorithm 2 "with the valuations dropped". Suppose there was at least one instance when Algorithm 2 returned a list of elements of $\mathcal{F}(g)$ and let h be the product of all $\phi \in$ FACTORS immediately before 6. is checked, then $fh = g$. Hence, the output is correct in this case by Remark 4.22. □

4.3 Termination

Let us state the strongest known conditions under which there exist computer algorithms performing all steps of Algorithm 2 (and hence also Algorithm 3).

Conditions 4.24. *Suppose that the rational rank of* Γ *(and hence also the rank; Proposition 1.20) is finite and we have algorithms performing the following tasks.*

- *Field operations in K and k and computation of the valuation $v : K^\times \twoheadrightarrow \Gamma$.*
- *Computation of the residue class $\mathcal{O}_v \twoheadrightarrow k$ and a section $k \to \mathcal{O}_v$.*
- *Polynomial factorization in $\kappa[y]$ for each finite extension of κ/k.*

If Conditions 4.24 are satisfied, there exist algorithms performing all steps of Algorithm 2 (and hence Algorithm 3).

Indeed, we only need to perform the following tasks to carry out all steps of the algorithm.

- Computation of Newton polygons.
- Computation of residual polynomial operators $R : K[x] \longrightarrow \kappa[y]$.
- Construction of $Q \in K[x]$ such that $R(Q) = \psi$ for each $\psi \in \mathrm{Irr}(\kappa)\backslash\{y\}$.

All the above can be carried out for inductive valuations by recursive procedures descending their MLV chains. See, [8], and for greater detail [18].

Remark 4.25. *It has been recently shown that the graded ring of a residue-transcendental μ on $K[x]$ is isomorphic to the semigroup ring $k_\mu[t^{\Gamma_\mu}]$ if we consider a certain twisted multiplication on $\mathcal{G}_\mu$. This twisted multiplication can be made to agree with the usual one for instance when Γ has finite rational rank [6, Theorem 1.2]. It may be possible to exploit this isomorphism to give an alternative proof of [8, Theorem 5.16]; a result that enables the computation of the operators $R : K[x] \longrightarrow \kappa[y]$ in practice.*

The following characterization of the property "discrete and rank-one" for ordered abelian groups, will be frequently used.

Proposition 4.26. *Let Γ be an ordered abelian group and assume $\Gamma \neq \{0\}$. The following are equivalent.*

(1) every infinite strictly increasing sequence is unbounded
(2) Γ is discrete and rank one.

Proof. $\Longrightarrow$

Suppose (1) holds and Γ has no least positive element. Then, there exists a strictly decreasing infinite sequence $\{x_n\}_{n\geq 0} \subset \Gamma$ with $x_n > 0$ for all n. Thus, the sequence $\{-x_n\}_{n\geq 0}$ is a strictly increasing infinite sequence bounded above by 0, contradiction. This shows Γ has a least positive element.

Let $\{0\} \subsetneq H \subseteq \Gamma$ be a convex subgroup, we want to show $H = \Gamma$. Fix some positive $h \in H$ and note that the infinite sequence $h < 2h < 3h < \dots$ is strictly increasing, so for each positive $g \in \Gamma$ there is some $n \in \mathbb{N}$ such that $g \leq nh$ by (1). Hence the interval $[0, nh]_\Gamma$ contains g, because H is convex. For negative $g \in \Gamma$, we obtain $g \in H$ by applying the previous argument to $-g$. Hence $H = \Gamma$ as required.

$\Longleftarrow$

It is well-known that the discrete rank one condition implies that Γ is order-isomorphic to $\mathbb{Z}$ with the standard ordering. Hence (1) holds for Γ because it is clearly preserved by order-isomorphisms. □

We say a monic, square-free polynomial $g \in K[x]$ is **defectless** if all $G \in \mathcal{F}(g)$ are defectless. Abuse notation and write $\Gamma := \Gamma_v$.

Proposition 4.27. *If every infinite strictly increasing sequence in Γ is unbounded and g is defectless, then Algorithm 2 terminates.*

Proof. If we "guess" an exact factor of g during the flow of the algorithm, it gets detected in 2. and the algorithm terminates. Suppose this does not happen. If (μ, ϕ) is a type and $G \in \mathrm{Irr}(K)$ satisfies $\mathrm{in}_\mu(\phi) \mid \mathrm{in}_\mu(G)$ and $\phi \neq G$, then each $\phi' \in \mathbf{t}(\mu_\lambda, v_G)$ satisfies $u(G, \phi') > u(G, \phi)$ by Lemma 3.23. Notice that for any such type, we have $\deg(\phi) \mid \deg(G)$ by Theorem 3.18, which shows $u(G, \phi) = \frac{v(\mathrm{Res}\, G, \phi)}{\deg(G)\deg(\phi)} \in \frac{1}{\deg^2(G)}\Gamma \subset \Gamma_{\mathbb{Q}}$. By our assumption on sequences, $\frac{1}{\deg^2(G)}\Gamma$ contains no strictly increasing bounded sequences. Hence, in finitely many steps $u(G, \phi) > r(g)$ for some $(\mu, \phi) \in T$ and some $G \in \mathcal{F}(g)$, which shows $v_G(\phi) > v_F(\phi)$ for all $F \in \mathcal{F}(g)$ with $F \neq G$ by Lemma 3.25. So if we denote $\lambda = v_G(\phi)$, we have $\mathcal{F}_{\mu,\phi}(g)(\lambda) = \{G\}$ and hence $\mathcal{F}_{\mu_\lambda,\phi'}(g) = \{G\}$ where $\phi' \in \mathbf{t}(\mu_\lambda, v_G)$ is an arbitrary choice. Since g is defectless, we are guaranteed to reach $u(G, \phi') > \delta(G)$ in finitely many such "improvement steps", by our assumption on sequences. Hence $\deg(\phi') = \deg(G)$ by Remark 3.39 (nothing needs to be said if $\deg(G) = 1$). Hence, after finitely many iterations, the partition determined by T singles out the irreducible factors of g. Moreover, the condition $u(G, \phi) > \gamma$ will hold for all $(\mu, \phi) \in T$, in finitely many steps too, again by our assumption on sequences.

□

Remark 4.28. *The only proof of termination of a similar algorithm, that is available in the literature, seems to be [11, Theorem 4.8].*

Proposition 4.29. *If every infinite strictly increasing sequence in Γ is unbounded, then every separable $G \in \mathrm{Irr}(K)$ is defectless.*

Proof. By Proposition 4.13, there exists a type (μ_0, ϕ_0) such that $\mathrm{in}_{\mu_0}(\phi_0) \mid \mathrm{in}_{\mu_0}(G)$ and μ_0 is a depth-zero valuation. If $G = \phi_0$, then $v_G = [\mu_0; G, \infty]$ so G is defectless by Theorem 3.33. Otherwise, we obtain a type (μ_1, ϕ_1) such that $\mathrm{in}_{\mu_1}(\phi_1) \mid \mathrm{in}_{\mu_1}(G)$ and $u(G, \phi_1) > u(G, \phi_0)$ by Lemma 3.23. Continuing in this fashion, either $G = \phi_i \in \mathrm{KP}(\mu_i)$ for some i in which case G is defectless by Theorem 3.33 or the sequence $u(G, \phi_i)$ is infinite and strictly increasing, hence there exists a j such $u(G, \phi_j) > \mathrm{kras}(F)$ so for all $i \geq j$, we have $\deg(G) = \deg(\phi_i)$ by Proposition 3.38 and Theorem 3.18. Hence, $G \in \mathrm{KP}(\mu_i)$, so again G is defectless by Theorem 3.33. □

Remark 4.30. *By [13, Corollary 11.28], it follows that if (K, v) is a local field and $(K, v) \subset (L, w)$ is a finite extension, then $d(w/v) = 1$. Hence all $F \in \mathrm{Irr}(K)$ are defectless. It follows by Proposition 4.27 that over local fields Algorithm 2 terminates for arbitrary input polynomials.*

Example 4.31. *There exists a henselian valued field (K, v) whose value group Γ is discrete and of rank one and not all $F \in \mathrm{Irr}(K)$ are defectless [13, Example 11.40].*

4.4 Computation of splitting fields

Fix an algebraic closure $\overline{K}$ of K and let $\overline{v}$ be the unique extension of v to $\overline{K}$. We recall Krasner's lemma.

Theorem 4.32. *[10, Theorem 4.1.7] Let $\alpha \in \overline{K}$ and let $G = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, $\alpha_1 = \alpha$, be its minimal polynomial over K. Suppose $\beta \in \overline{K}$ satisfies*

$$\overline{v}(\beta - \alpha) > \max\{\overline{v}(\alpha_i - \alpha) \mid \alpha_i \neq \alpha\} =: \operatorname{kras}(G).$$

Then $K(\alpha, \beta)$ is purely inseparable over $K(\beta)$. In particular, if α is separable, then $\alpha \in K(\beta)$.

Corollary 4.33. *Let $G \in \operatorname{Irr}(K)$ be a separable polynomial. Suppose a $\phi \in \operatorname{Irr}(K)$ satisfies $\deg(\phi) = \deg(G)$ and $u(G, \phi) > \operatorname{kras}(G)$. Then, ϕ is separable, and if we denote $Z(G) = \{\alpha_1, \dots, \alpha_n\}$, $Z(\phi) = \{\beta_1, \dots, \beta_n\}$, there exists a renumbering such that $K(\alpha_i) = K(\beta_i)$ for all $1 \leq i \leq n$.*

Proof. Let us show that the assumption $u(G, \phi) > \operatorname{kras}(G)$ implies that for each $i \in \{1, \dots, n\}$ there exists a unique $j \in \{1, \dots, n\}$ such that

$$\overline{v}(\beta_i - \alpha_j) > \operatorname{kras}(G).$$

Fix an i, there exist a j as above since $u(G, \phi)$ is the average of $\overline{v}(\beta_i - \alpha_j)$ where j varies over $\{1, \dots, n\}$ For a fixed i, a j as above is unique because if j' also has this property, we would have

$$\overline{v}(\beta_i - \alpha_j) > \operatorname{kras}(G) \geq \overline{v}(\alpha_j - \alpha_{j'})$$

and similarly

$$\overline{v}(\beta_i - \alpha_{j'}) > \operatorname{kras}(G) \geq \overline{v}(\alpha_i - \alpha_{j'}).$$

However, this contradicts the ultrametric triangle inequality, which says

$$\overline{v}(\alpha_i - \alpha_{j'}) \geq \min\{\overline{v}(\beta_i - \alpha_j), \overline{v}(\beta_i - \alpha_{j'})\}.$$

Thus after renumbering we can assume that for each i we have

$$\overline{v}(\beta_i - \alpha_i) > \operatorname{kras}(G).$$

By Theorem 4.32, we conclude $\alpha_i \in K(\beta_i)$ and hence $K(\beta_i) = K(\alpha_i)$ by equality of degrees. In particular, the β_i (and therefore ϕ) are separable over K. □

Remark 4.34. *Hence $G, \phi \in \operatorname{Irr}(K)$ satisfying conditions of Corollary 4.33 have the same splitting field. This implies that if $g \in K[x]$ is monic, separable and $\{\phi_1, \dots \phi_k\}$ is any $\operatorname{kras}(g)-$factorization of g, then g and $h = \phi_1 \dots \phi_k$ have the same splitting field; renumber the indices so that each pair (G_i, ϕ_i) satisfies conditions of Corollary 4.33 and use that the splitting field of g is the compositum of the splitting fields of the G_i.*

This leads to the following.

Algorithm 4: Splitting field

Input:

- a non-trivially valued henselian field $\mathbf{K} := (K, v)$
- a monic, separable $g \in K[x]$

Output:

- The splitting field of g

```
1  γ ← any value ≥ kras(g)
2  L ← K
3  T ← OMfactorization(L, g, γ)
4  if g splits completely over L; | T | = deg(g) then
5      return L
6  else
7      choose any φ ∈ T with deg(φ) > 1
8      L ← L[x]/(φ) and w ← v_φ, the unique extension of v to L
9      L ← (L, w)
10     goto 3.
```

Lemma 4.35. *Suppose (K, v) satisfies Conditions 4.24 and every strictly increasing infinite sequence in Γ is unbounded, then for each separable $\phi \in \mathrm{Irr}(K)$, the extension field $(L, w) := (K[x]/(\phi), \overline{v_\phi})$ satisfies Conditions 4.24.*

Proof. Obviously, we could modify Algorithm 3 to simply store all the sequences of augmentations that lead to a $\gamma-$factorization. Hence, we can assume we have access to an MLV chain for v_ϕ (by storing only those augmentations $\mu_i \longrightarrow \mu_{i+1}$ with $\deg(\mu_i) < \deg_{i+1}$). Denote $\mu \longrightarrow v_\phi$, the last augmentation in such a chain and recall that $v_\phi = [\mu; \phi, \infty]$.

Let us show Conditions 4.24 hold for (L, w).

It is clear Γ_w has finite rational rank.

We can compute w using the fact that $\overline{v_\phi}(f + (\phi)) = v_\phi(f) = \min\{\mu(a_i) \mid 0 \leq i \leq r\}$ where $f = a_0 + \cdots + a_r\phi^r$ is the $\phi-$expansion of $f \notin \phi K[x]$. The computation of μ in turn follows from having an MLV chain for it and Lemma 3.8.

We clearly have algorithms for field operations in $L = K[x]/(F)$.

Since an MLV chain provides a computation of k_w, [20, Theorem 5.4], we have algorithms for field operations in k_w and we can compute the residue map $\mathcal{O}_w \longrightarrow k_w$.

The computation of a section $k_w \longrightarrow \mathcal{O}_w$, follows from [8, Proposition 5.11].

We have algorithms for performing polynomial factorization over all finite extensions κ/k_w, because we already assume this for k and k_w/k is a finite extension. □

Remark 4.36. *Clearly if every strictly increasing infinite sequence in Γ is unbounded and $(K, v) \subset (L, w)$ is an arbitrary finite extension, the corresponding statement holds for Γ_w as $e(w/v)\Gamma_w \subset \Gamma$. See also [14, Theorem 3.2].*

By Lemma 4.35, Remark 4.36 and Corollary 4.33, we immediately obtain (use Lemma 3.30 to pick $\gamma > \operatorname{kras}(g)$) our final proposition, below.

Proposition 4.37. *If every strictly increasing infinite sequence in* Γ *is unbounded, then Algorithm 4 terminates and has the right output.*

Compare the splitting field algorithm presented here with [17, Algorithm 6], the starting point of this project.

References

[1] Maria Alberich-Carramiñana, Alberto F F. Boix, Julio Fernández, Jordi Guàrdia, Enric Nart, and Joaquim Roé. Of limit key polynomials. *Illinois Journal of Mathematics*, 65(1):201–229, 2021.

[2] Maria Alberich-Carramiñana, Jordi Guàrdia, Enric Nart, and Joaquim Roé. Valuative trees over valued fields. *Journal of Algebra*, 614:71–114, 2023.

[3] Maria Alberich-Carramiñana, Jordi Guàrdia, Enric Nart, Adrien Poteaux, Joaquim Roé, and Martin Weimann. Polynomial factorization over henselian fields, 2022. `arXiv:2207.02139`.

[4] Maria Alberich-Carramiñana, Jordi Guàrdia, Joaquím Roé, and Enric Nart. Okutsu frames of irreducible polynomials over henselian fields, 2023. `arXiv:2111.02811`.

[5] James Ax. A metamathematical approach to some problems in number theory. In *AMS Symposium*, pages 161–190, 1973.

[6] MS Barnabé, J Novacoski, and Mark Spivakovsky. On the structure of the graded algebra associated to a valuation. *Journal of Algebra*, 560:667–679, 2020.

[7] Nathalia Moraes de Oliveira and Enric Nart. Defectless polynomials over henselian fields and inductive valuations. *Journal of Algebra*, 541:270–307, 2020.

[8] Nathália Moraes de Oliveira and Enric Nart. Computation of residual polynomial operators of inductive valuations. *Journal of Pure and Applied Algebra*, 225(9):106668, 2021.

[9] Julie Decaup, W Mahboub, and M Spivakovsky. Abstract key polynomials and comparison theorems with the key polynomials of Mac Lane-Vaquié. *Illinois Journal of Mathematics*, 62(1-4):253–270, 2018.

[10] Antonio J Engler and Alexander Prestel. *Valued fields*. Springer Science & Business Media, 2005.

[11] Jordi Guàrdia, Jesús Montes, and Enric Nart. Newton polygons of higher order in algebraic number theory. *Transactions of the American Mathematical Society*, 364(1):361–416, 2012.

[12] Marc Krasner. Nombre des extensions d'une degre donne d'un corps β-adique. *Les tendances géométriques en algèbre et théorie des nombres*, 1966.

[13] Franz-Viktor Kuhlmann. Book on valuation theory. *(in preparation)*, 2011. URL: `https://math.usask.ca/~fvk/Fvkbook.htm`.

[14] Franz-Viktor Kuhlmann and Enric Nart. Cuts and small extensions of abelian ordered groups. *Journal of Pure and Applied Algebra*, 226(11):107103, 2022.

[15] Saunders Mac Lane. A construction for prime ideals as absolute values of an algebraic field. 1936.

[16] Saunders MacLane. A construction for absolute values in polynomial rings. *Transactions of the American Mathematical Society*, 40(3):363–395, 1936.

[17] Jonathan Milstead, Sebastian Pauli, and Brian Sinclair. Constructing splitting fields of polynomials over local fields. In *Collaborative Mathematics and Statistics Research: Topics from the 9th Annual UNCG Regional Mathematics and Statistics Conference*, pages 101–124. Springer, 2015.

[18] Nathália Moraes de Oliveira. *Inductive valuations and defectless polynomials over henselian fields*. PhD thesis, Universitat Autònoma de Barcelona, 2019.

[19] Enric Nart. Key polynomials over valued fields, 2018. `arXiv:1803.08406`.

[20] Enric Nart. Maclane-Vaquié chains of valuations on a polynomial ring. *Pacific Journal of Mathematics*, 311(1):165–195, 2021.

[21] Enric Nart and Josnei Novacoski. The defect formula. *Advances in Mathematics*, 428:109153, 2023.

[22] Josnei Novacoski. On Maclane-Vaquié key polynomials. *Journal of Pure and Applied Algebra*, 225(8):106644, 2021.

[23] Josnei Novacoski and Mark Spivakovsky. Key polynomials and pseudo-convergent sequences. *Journal of Algebra*, 495:199–219, 2018.

[24] Abolfazl Tarizadeh and Johan Öinert. Homogeneity in commutative graded rings. *arXiv preprint arXiv:2108.10235*, 2021. URL: `https://arxiv.org/abs/2108.10235`.

[25] Bernard Teissier. Valuations, Deformations, and Toric geometry. *arXiv preprint math/0303200*, 2003. URL: `https://arxiv.org/abs/math/0303200`.

[26] Michel Vaquié. Famille admise associée a une valuation de K[x]. In *Séminaires et Congres*, volume 10, pages 391–428, 2005.

[27] Michel Vaquié. Algebre graduée associée a une valuation de K[x]. *Adv. Stud. Pure Math*, 46:259–271, 2007.

[28] Michel Vaquié. Extension d'une valuation. *Transactions of the American Mathematical Society*, 359(7):3439–3481, 2007.

[29] Michel Vaquié. Famille admissible de valuations et défaut d'une extension. *Journal of Algebra*, 311(2):859–876, 2007.