POLYNOMIAL FACTORIZATION OVER HENSELIAN FIELDS

MARIA ALBERICH-CARRAMIÑANA, JORDI GUÀRDIA, ENRIC NART, ADRIEN POTEAUX, JOAQUIM ROÉ, AND MARTIN WEIMANN

Abstract. We present an algorithm that, given an irreducible polynomial g over a general valued field (K, v), finds the factorization of g over the Henselianization of K under certain conditions. The analysis leading to the algorithm follows the footsteps of Ore, Mac Lane, Okutsu, Montes, Vaquié and Herrera-Olalla-Mahboub-Spivakovsky, whose work we review in our context. The correctness is based on a key new result (Theorem 4.10), exhibiting relations between generalized Newton polygons and factorization in the context of an arbitrary valuation. This allows us to develop a polynomial factorization algorithm and an irreducibility test that go beyond the classical discrete, rank-one case. These foundational results may find applications for various computational tasks involved in arithmetic of function fields, desingularization of hypersurfaces, multivariate Puiseux series or valuation theory.

Introduction

In a pioneering work along the 1920s, Ø. Ore conjectured the existence of an algorithm to compute the prime ideal decomposition of a prime number p in the number field $\mathbb{Q}[x]/(g)$ defined by an irreducible polynomial $g \in \mathbb{Q}[x]$ [36, 37]. Ore's proposal was based in the iteration of two "dissections":

- Computation of Newton polygons of g with respect to some valuations on $\mathbb{Q}[x]$.
- Factorization in certain residue fields, of residual polynomials of g associated to the sides of the Newton polygons.

In the 1930s, S. Mac Lane solved this problem in a more general context. For a given discrete rank-one valued field (K, v), he found an algorithm to compute all extensions of v to the field $K[x]/(g)$ defined by an irreducible polynomial $g \in K[x]$ [22, 23]. These extensions can be identified with certain valuations μ on $K[x]$ with support $gK[x]$, determined by the different irreducible factors of g in $K_v[x]$, where K_v is the completion of K at v. For each such μ, Mac Lane constructed a chain of augmentations of valuations on $K[x]$ getting arbitrarily close to it:

$$\mu_0 \ < \ \mu_1 \ < \ \cdots \ < \ \mu_n \ < \ \cdots \ < \ \mu$$

In these augmentations, some *key polynomials* for the valuations μ_n are involved. This procedure can be reinterpreted as a polynomial factorization algorithm in $K_v[x]$. If a valuation μ_n is sufficiently close to μ, then its key polynomial is an approximation to the irreducible factor of g in $K_v[x]$ intrinsically associated to μ.

Motivated by the computation of integral bases in finite extensions of local fields, K. Okutsu constructed similar approximations without using valuations on $K[x]$, nor key polynomials [35, 12]. Still in the discrete rank-one case, J. Montes developed in 1999 certain residual polynomial operators leading to the design of a practical algorithm following the exact pattern that Ore had foreseen [24, 13, 14, 41]. This algorithm is known as the *OM-algorithm*, named after Ore, Mac Lane, Okutsu and Montes.

Montes' ideas led to the computation of integral bases too [16, 6, 42]. More generally, the OM-algorithm is very efficient in the resolution of many arithmetic-geometric tasks in number fields and function fields of algebraic curves [17, 15, 40].

Date: November 14, 2023.

2010 *Mathematics Subject Classification.* 13P05,12Y05 (13A18,14Q15).

Key words and phrases. Key polynomial, Newton polygon, OM-algorithm, valuation, Henselian field.

Partially supported by grants PID2019-103849GB-I00 and PID2020-116542GB-I00 funded by MCIN/AEI/10.13039/501100011033 and by grants 2021-SGR-00603 and 2021-SGR-01468 funded by Generalitat de Catalunya.

Communicated by Christophe Ritzenthaler.

Mac Lane's theory was generalized to arbitrary valued fields, independently by M. Vaquié [43, 44, 45] and F.-J. Herrera, M.-A. Olalla, W. Mahboub and M. Spivakovsky [18, 19]. In this general frame, *limit augmentations* and the corresponding *limit key polynomials* appear as a new feature.

A prototype of a general OM-algorithm was sketched in [19]. Other partial approaches can be found in [11] and [25] too. However, none of these ideas crystallizes into a real algorithm, because of the existence of limit augmentations. Thus, the extension of Mac Lane's work [23] to a polynomial factorization algorithm over arbitrary Henselian fields is still an open problem.

Main results. In this paper, we present an executable OM-algorithm for arbitrary valued fields (Theorem 5.1) whose termination is guaranteed in cases strictly larger than what was previously known. This leads to new results about factorization of polynomials over Henselian fields.

Let K^h be a Henselization of (K, v). Denote p the residual characteristic of K. We assume that usual arithmetic operations in K are available and that univariate factorization over the residue field is available too (see Section 5.4 for details). We prove :

Theorem 0.1. *Assume that v has rank one (not necessarily discrete). There exists a deterministic algorithm which, given $g \in K[x]$ irreducible with $p > \deg(g)$ or $p = 0$, outputs*

(a) Approximations to all irreducible factors of g over $K^h[x]$ up to an arbitrary given precision

(b) All extensions of v to the field $K[x]/(g)$, together with a computation of their ramification indices and residual degrees.

For valuations of arbitrary rank we get :

Theorem 0.2. *Let v of arbitrary rank. There exists a deterministic algorithm which, given $g \in K[x]$ irreducible with $p \nmid \deg(g)$, tests if g is irreducible in $K^h[x]$. In such a case, the algorithm computes the ramification index and the residual degree of the unique extension of v to the field $K[x]/(g)$.*

Up to our knowledge, these results were known only for discrete rank one valuations. Notice that in such a case, they hold with no restriction on the residual characteristic and we can give precise complexity estimates [41]. The extension of this accurate complexity analysis to the more general setting of Theorem 0.1 and Theorem 0.2 is a delicate task, which goes beyond the scope of this paper.

Applications. In analogy with the 0- and 1-dimensional cases, this general theory should lead to the development of efficient algorithms for the resolution of arithmetic-geometric tasks involving valuations of function fields of algebraic varieties of higher dimension. In particular, Theorem 0.1 is relevant for local uniformization thanks to a recent theorem of Novacoski-Spivakovsky which asserts that local uniformization along rank one valuations implies local uniformization in its full generality [33, 34].

Another application concerns the computation of multivariate Puiseux series, in the vein of Mac Donald's algorithm [21]. This algorithm uses a non discrete rank one valuation, and Theorem 0.1 should improve [21] both from a complexity point of view (dealing with minimal residual extensions, in the vein of [8, 39]) and from a practical point of view (computing the relevant arithmetic information).

In the course of the paper, we will give an explicit illustration of such an application, by running our algorithm on a particular polynomial g of degree 1152 over a non discrete, rank-one valued field (Example 1.5). In Section 4.5, we provide the factorization of g over $K^h[x]$ (see also Section 6.2.6).

Higher rank valuations are useful to take into account arithmetic and geometric informations by mixing p-adic valuations ($p \in \mathbb{Z}$ a prime) and t-adic valuations (t a variable), as illustrated by additional examples in Section 5.5. As an application, we may hope to factorize polynomials in $\mathbb{Z}[t, x]$ using a rank-two lifting and recombination strategy.

Organisation. In Sections 1–3, we review the necessary background on valuations on $K[x]$, their graded algebras and Mac Lane–Vaquié chains of augmented valuations.

In Section 4, we discuss Newton polygons and extend Ore's dissections to this completely general setting. If v has rank one, then K is dense in K^h and the content of this section can be easily deduced from Montes' original arguments in the discrete case. However, for v of arbitrary rank, the key polynomials for a valuation μ on $K[x]$ extending v need not be irreducible over $K^h[x]$. Thus,

the description of the unique extension of μ to $K^h[x]$ is more subtle and the proof of the main result (Theorem 4.10) is more involved.

In Section 5, we present our general OM-algorithm and we prove that, if it terminates, it leads to a solution of the above mentioned problems (a) and (b). The only obstacle for this algorithm to terminate is the existence of infinite sequences of *refinement steps*. We show that there are exactly three different situations where infinite refinements occur, and we exhibit concrete examples of each one.

Finally, we present in Section 6 the proof of Theorems 0.1 and 0.2. The algorithms generalize similar constructions by Poteaux-Weimann in the discrete rank-one case [41]. Besides the underlying OM-algorithm, a key ingredient is the use of approximate roots which allow to compute efficiently optimal key polynomials under some assumptions on the residual characteristic (Proposition 6.3). A second ingredient is a valuated Hensel lifting for arbitrary valuations which allows to increase quadratically the precision of a given approximate factorization (Proposition 6.8). These results are illustrated on Example 1.5 in Subsection 6.2.6.

Acknowledgement. We warmly thank the referees, whose enlightening comments led us to improve the presentation, and Josnei Novacoski for sharing his insights about the content of Section 4.

Notation. For any field $\mathbb{K}$, we denote by $\mathrm{Irr}(\mathbb{K})$ the set of monic, irreducible polynomials in $\mathbb{K}[x]$.

1. Commensurable extensions of a valuation to the polynomial ring

Let (K, v) be a valued field with valuation ring $\mathcal{O}$, maximal ideal $\mathcal{M}$ and residue class field $k = \mathcal{O}/\mathcal{M}$. Let $\Gamma = v(K^*)$ be the value group and denote by $\Gamma_{\mathbb{Q}} = \Gamma \otimes \mathbb{Q}$ the divisible hull of Γ. In the sequel, we write $\Gamma_{\mathbb{Q}}\infty$ instead of $\Gamma_{\mathbb{Q}} \cup \{\infty\}$.

The equivalence classes of *commensurable* extensions of v to the polynomial ring $K[x]$ are parameterized by the set $\mathcal{T} = \mathcal{T}(K, \Gamma_{\mathbb{Q}})$ of all $\Gamma_{\mathbb{Q}}$-valued valuations on $K[x]$,

$$\mu\colon K[x] \longrightarrow \Gamma_{\mathbb{Q}}\infty,$$

whose restriction to K is v. The *support* of μ is the prime ideal

$$\mathfrak{p} = \mathrm{supp}(\mu) := \mu^{-1}(\infty) \in \mathrm{Spec}(K[x]).$$

The valuation μ induces a valuation $\overline{\mu}$ on the field L of fractions of $K[x]/\mathfrak{p}$. That is, $L = K(x)$ if $\mathfrak{p} = 0$, or $L = K[x]/\mathfrak{p}$ if $\mathfrak{p} = gK[x]$ for some $g \in \mathrm{Irr}(K)$.

The residue field k_μ of μ is, by definition, the residue field of $\overline{\mu}$. The *value group* of μ is the subgroup $\Gamma_\mu \subset \Gamma_{\mathbb{Q}}$ generated by $\mu\,(K[x] \setminus \mathfrak{p})$. By definition, μ/v commensurable means that the quotient Γ_μ/Γ is a torsion group. We say that μ is *residually transcendental* if the extension k_μ/k is transcendental. In this case, its transcendence degree is necessarily equal to one [20].

The set $\mathcal{T}$ admits a partial ordering. For $\mu, \nu \in \mathcal{T}$ we say that $\mu \leq \nu$ if

$$\mu(f) \leq \nu(f), \quad \forall\, f \in K[x].$$

The poset $\mathcal{T}$ has the structure of a tree. By this, we simply mean that all intervals $(-\infty, \mu\,] := \{\rho \in \mathcal{T} \mid \rho \leq \mu\}$ are totally ordered [25, Thm. 3.9].

A node $\mu \in \mathcal{T}$ is a *leaf* if it is a maximal element with respect to the ordering $\leq$. Otherwise, we say that μ is an *inner node*. We distinguish two kinds of leaves: *finite* and *infinite*. We denote

$$\mathcal{T} = \mathcal{T}^{\mathrm{inn}} \sqcup \mathcal{L}_{\mathrm{fin}} \sqcup \mathcal{L}_{\infty}$$

the subsets of inner nodes, finite leaves, and infinite leaves, respectively. For all $\mu \in \mathcal{T}$, the subset to which μ belongs can be characterized as follows [4, Sec. 1-2]:

- $\mu \in \mathcal{T}^{\mathrm{inn}}$ if and only if μ is residually transcendental.
- $\mu \in \mathcal{L}_{\mathrm{fin}}$ if and only if $\mathrm{supp}(\mu) \neq 0$.
- $\mu \in \mathcal{L}_{\infty}$ if and only if $\mathrm{supp}(\mu) = 0$ and k_μ/k is algebraic.

The infinite leaves of $\mathcal{T}$ are *valuation-algebraic* in the terminology of Kuhlmann [20]. They play no role in the polynomial factorization problem.

Let us fix an algebraic closure $\overline{K}$ of K, and an extension $\bar{v}$ of our base valuation v to $\overline{K}$. This determines a Henselization (K^h, v^h) of (K, v). If K^{sep} is the separable closure of K in $\overline{K}$, the field $K^h \subset K^{\mathrm{sep}}$ is the fixed field of the decomposition group

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

The valuation v^h is the restriction of $\bar{v}$ to K^h and it has a unique extension to $\overline{K}$, namely $\bar{v}$.

Theorem 1.1. [29, Thm. A] *Let $\mathcal{T}^h := \mathcal{T}(K^h, \Gamma_{\mathbb{Q}})$ be the tree of commensurable extensions of v^h to $K^h[x]$. Restriction of valuations induces an isomorphism of posets:*

$$\mathcal{T}^h \longrightarrow \mathcal{T}, \qquad \nu \longmapsto \nu_{|K[x]},$$

preserving inner nodes, finite leaves and infinite leaves.

Actually, the bijection between finite leaves of $\mathcal{T}^h$ and $\mathcal{T}$ is a classical fact. To any $F \in \mathrm{Irr}(K^h)$ we can associate a valuation $v_F \in \mathcal{L}_{\mathrm{fin}}(\mathcal{T}^h)$ defined as

$$v_F(q) := \bar{v}(q(\theta)) \quad \text{for all } q \in K^h[x],$$

where $\theta \in \overline{K}$ is a root of F. By the Henselian property, this construction does not depend on the choice of θ. Clearly, $\mathrm{supp}(v_F) = FK^h[x]$. We denote the restriction of v_F to $K[x]$ by:

$$w_F := (v_F)_{|K[x]} \in \mathcal{L}_{\mathrm{fin}}(\mathcal{T}).$$

Now, $\mathrm{supp}(w_F) = N_{K^h/K}(F)K[x]$, where $N_{K^h/K}(F) \in \mathrm{Irr}(K)$ is the monic generator of the prime ideal $\big(FK^h[x]\big) \cap K[x]$.

Proposition 1.2. [9, Sec. 17] *The following two mappings are bijective:*

$$\mathrm{Irr}(K^h) \longrightarrow \mathcal{L}_{\mathrm{fin}}(\mathcal{T}^h) \longrightarrow \mathcal{L}_{\mathrm{fin}}(\mathcal{T}), \qquad F \mapsto v_F \mapsto w_F.$$

More generally, for any polynomial $g \in \mathrm{Irr}(K)$, this construction facilitates the description of the extensions of v to the simple extension $K[x]/(g)$. Since K^h/K is a separable extension, we have $g = G_1 \cdots G_r$ with pairwise different $G_i \in \mathrm{Irr}(K^h)$. Since $N_{K^h/K}(G_i) = g$ for all i, each $w_{G_i} \in \mathcal{L}_{\mathrm{fin}}(\mathcal{T})$ induces a valuation $\overline{w}_{G_i}$ on the field $K[x]/(g)$.

Theorem 1.3. [9, Sec. 17] *The extensions of v to $K[x]/(g)$ are $\overline{w}_{G_1}, \ldots, \overline{w}_{G_r}$.*

In particular, $w_{G_1}, \ldots w_{G_r}$ are all finite leaves of $\mathcal{T}$ with support $gK[x]$.

Summary. The irreducible factors of g in $K^h[x]$ can be identified with the extensions of v to $K[x]/(g)$, which are in turn determined by some finite leaves of the tree $\mathcal{T}$. The main goal of the OM-algorithm is to solve the following problem :

Problem 1.4. *Compute, for each irreducible factor $G \in K^h[x]$ of g, a chain of valuations in $\mathcal{T}^{\mathrm{inn}}$ getting sufficiently close to w_G to determine the ramification index and residual degree of $\overline{w}_G$.*

The valuations in the chains will be constructed using some key polynomials which eventually give approximations of the irreducible factors of g. Hence, Problem 1.4 is closely related to irreducibility and factorization issues, as we will see in Section 6.

We now introduce a concrete polynomial with coefficients in a non-discrete valued field, to illustrate how our methods are able to solve Problem 1.4 in previously untractable situations.

Example 1.5. *Let $p = 1523$, and consider $K = \mathbb{F}_p(t_1, t_2)$ with the valuation v defined by $v(t_1) = 1$ and $v(t_2) = \sqrt{2}$. The value group $\Gamma := \mathbb{Z} + \sqrt{2}\mathbb{Z} \subset (\mathbb{R}, +)$ has rank one, but rational rank 2. The residue field is $k = \mathcal{O}/\mathcal{M} = \mathbb{F}_p$. Consider the following polynomials in $K[x]$:*

$$P = x^2 + x + 1, \qquad Q = P^{72} + 1406\, t_1^6\, t_2^4.$$

We aim to solve Problem 1.4 for the following polynomial of degree 1152:

$$g = Q^8 + 1410\, t_1^{57}\, t_2^{30}\, P^{36} \in K[x].$$

2. Graded algebra and key polynomials

Take any $\mu \in \mathcal{T}$ and let $\mathfrak{p} = \operatorname{supp}(\mu)$. For all $\alpha \in \Gamma_\mu$, consider the $\mathcal{O}$-modules:

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

The *graded algebras* of v and μ are the integral domains:

$$\mathcal{G}_v := \bigoplus\nolimits_{\alpha\in\Gamma} \left(\mathcal{P}_\alpha \cap K\right) / \left(\mathcal{P}^+_\alpha \cap K\right), \qquad \mathcal{G}_\mu := \bigoplus\nolimits_{\alpha\in\Gamma_\mu} \mathcal{P}_\alpha/\mathcal{P}^+_\alpha.$$

There is an obvious embedding of graded algebras $\mathcal{G}_v \hookrightarrow \mathcal{G}_\mu$.

Consider the *initial coefficient* mapping $\operatorname{in}_\mu \colon K[x] \to \mathcal{G}_\mu$, given by $\operatorname{in}_\mu \mathfrak{p} = 0$ and assigning to each $g \in K[x] \setminus \mathfrak{p}$ the following homogeneous element of *grade* $\mu(g)$:

$$\operatorname{in}_\mu g := g + \mathcal{P}^+_{\mu(g)} \in \mathcal{P}_{\mu(g)}/\mathcal{P}^+_{\mu(g)}.$$

In this section, we will see that for any inner node $\mu \in \mathcal{T}$, the factorization of $\operatorname{in}_\mu g$ in $\mathcal{G}_\mu$ determines the directions we need to take in the tree $\mathcal{T}$ to get closer to the finite leaves $w_G > \mu$ determined by the irreducible factors G of g in $K^h[x]$. Furthermore, we will show that this factorization can be efficiently computed by means of a residual polynomial operator.

2.1. Key polynomials.

The mapping in_μ is multiplicative but not additive. For instance, if $\mu(f) = \mu(g) = \alpha$, then,

$$\operatorname{in}_\mu f + \operatorname{in}_\mu g = \begin{cases} \operatorname{in}_\mu(f+g), & \text{if } \ \mu(f+g) = \alpha, \\ 0, & \text{if } \ \mu(f+g) > \alpha. \end{cases}$$

Definition 2.1. *Let g, $h \in K[x]$. We say that*

- *g, h are* μ-equivalent*, and write $g \sim_\mu h$, if $\operatorname{in}_\mu g = \operatorname{in}_\mu h$.*
- *g is* μ-divisible *by h, and write $h \mid_\mu g$, if $\operatorname{in}_\mu h \mid \operatorname{in}_\mu g$ in $\mathcal{G}_\mu$.*
- *g is μ-irreducible if $\operatorname{in}_\mu g$ is a prime element.*
- *g is μ-minimal if $g \nmid_\mu f$ for all nonzero $f \in K[x]$ with $\deg(f) < \deg(g)$.*

Consider the set $\mathcal{H}(\mathcal{G}_\mu) = \{\operatorname{in}_\mu g \mid g \in K[x] \setminus \mathfrak{p}\}$ of all nonzero homogeneous elements in $\mathcal{G}_\mu$. Let $\mathcal{H}(\mathcal{G}^*_\mu) \subset \mathcal{H}(\mathcal{G}_\mu)$ be the multiplicative group of all homogeneous units. Recall that $\pi \in \mathcal{H}(\mathcal{G}_\mu)$ is a prime element if the homogeneous principal ideal of $\mathcal{G}_\mu$ generated by π is a prime ideal. In this case, for all $t \in \mathcal{H}(\mathcal{G}_\mu)$ the order $n = \operatorname{ord}_\pi(t)$ is determined by the conditions $\pi^n \mid t$, $\pi^{n+1} \nmid t$.

For all $\phi \in K[x] \setminus K$ we define the *truncation* μ_ϕ as follows:

$$g = \sum\nolimits_{n\geq 0} a_n \phi^n, \quad \deg(a_n) < \deg(\phi) \qquad \Longrightarrow \qquad \mu_\phi(g) := \min_{n\geq 0} \left\{\mu\left(a_n \phi^n\right)\right\}.$$

This function μ_ϕ is not necessarily a valuation, but it is useful to characterize the μ-minimality of ϕ. Let us recall [27, Prop. 2.3].

Lemma 2.2. *A polynomial $\phi \in K[x] \setminus K$ is μ-minimal if and only if $\mu_\phi = \mu$.*

Definition 2.3. *A* (Mac Lane-Vaquié) key polynomial *for μ is a monic polynomial in $K[x]$ which is simultaneously μ-minimal and μ-irreducible. The set of key polynomials for μ is denoted* $\operatorname{KP}(\mu)$*. All key polynomials are irreducible in $K[x]$.*

Example. Consider Gauss' valuation:

$$\omega\left(\sum\nolimits_{n\geq 0} a_n x^n\right) = \min\left\{v(a_n) \mid n \geq 0\right\}. \tag{2.1}$$

Then, $\operatorname{KP}(\omega)$ is the set of all monic polynomials in $\mathcal{O}[x]$ whose reduction modulo $\mathcal{M}$ is irreducible. For instance, if $v(a) < 0$, then $\operatorname{in}_\omega(x+a) = \operatorname{in}_\omega a$ is a homogeneous unit, so that $x + a$ is neither ω-irreducible nor ω-minimal.

The existence of key polynomials characterizes the inner nodes of $\mathcal{T}$.

Theorem 2.4. [27, Thm. 4.4] *A valuation $\mu \in \mathcal{T}$ is a leaf if and only if $\operatorname{KP}(\mu) = \emptyset$. This is equivalent to $\mathcal{H}(\mathcal{G}_\mu) = \mathcal{H}(\mathcal{G}^*_\mu)$ too.*

From now on, we assume that μ is an inner node of $\mathcal{T}$ and $\phi \in \mathrm{KP}(\mu)$ is a key polynomial. Also, we denote

$$\pi := \mathrm{in}_\mu\, \phi, \qquad \overline{a} := \mathrm{in}_\mu\, a \ \text{ for all } a \in K[x].$$

Since ϕ is μ-minimal, Lemma 2.2 shows that μ acts on ϕ-expansions as follows

$$g = \sum\nolimits_{n\geq 0} a_n \phi^n, \ \ \deg(a_n) < \deg(\phi) \implies \mu(g) = \min_{n\geq 0} \{\mu\,(a_n\phi^n)\}\,. \tag{2.2}$$

Let us define

$$S_{\mu,\phi}(g) = \{n \geq 0 \mid \mu\,(a_n\phi^n) = \mu(g)\}\,. \tag{2.3}$$

For all nonzero $g \in K[x]$, we have

$$\overline{g} = \sum\nolimits_{n\in S_{\mu,\phi}(g)} \overline{a}_n \pi^n, \qquad \mathrm{ord}_\pi(\overline{g}) = \min\,(S_{\mu,\phi}(g))\,. \tag{2.4}$$

If ϕ is a key polynomial of minimal degree, then all these coefficients $\overline{a}_n$ derived from a ϕ-expansion are homogeneous units in $\mathcal{G}_\mu$ [27, Prop. 3.5].

Let $\mathcal{G}_\mu^0 \subset \mathcal{G}_\mu$ be the subalgebra generated by the set of all homogeneous units. Equivalently, $\mathcal{G}_\mu^0$ is the relative algebraic closure of $\mathcal{G}_v$ in the embedding $\mathcal{G}_v \hookrightarrow \mathcal{G}_\mu$. The following result is classically known (cf. for instance [32, Prop. 4.5]).

Theorem 2.5. *Let ϕ be a key polynomial of minimal degree for μ. Then, the prime $\pi = \mathrm{in}_\mu\,\phi$ is transcendental over $\mathcal{G}_\mu^0$ and $\mathcal{G}_\mu = \mathcal{G}_\mu^0[\pi]$.*

Definition 2.6. *For a nonzero $g \in K[x]$, its* μ-degree $\deg_\mu(g) \in \mathbb{N}$ *and its* leading coefficient $\mathrm{lc}_\mu(g) \in \mathcal{G}_\mu^0$ *are defined to be the degree and leading coefficient of $\mathrm{in}_\mu\, g$ as a polynomial in $\pi = \mathrm{in}_\mu\,\phi$ with coefficients in $\mathcal{G}_\mu^0$, for some $\phi \in \mathrm{KP}(\mu)$ of minimal degree.*

These definitions are independent of the choice of ϕ among all key polynomials of minimal degree for μ. Note that a homogeneous element $\mathrm{in}_\mu\, g$ is a unit if and only if $\deg_\mu(g) = 0$. Also, we have in general $\deg_\mu(g) = \max\,(S_{\mu,\phi}(g))$.

Definition 2.7. *The* degree *of an inner node $\mu \in \mathcal{T}$ is $\deg(\mu) := \deg(\phi)$, where $\phi \in \mathrm{KP}(\mu)$ is any key polynomial of minimal degree. For a finite leaf $w_F \in \mathcal{L}_{\mathrm{fin}}$ we let $\deg(w_F) := \deg(F)$.*

2.2. **Tangent directions of inner nodes.** A *tangent direction* of an inner node μ of $\mathcal{T}$ is a μ-equivalence class $[\,\phi\,]_\mu \subset \mathrm{KP}(\mu)$ containing all key polynomials having the same initial coefficient in $\mathcal{G}_\mu$. We denote the set of all tangent directions of μ by:

$$\mathbf{td}(\mu) := \mathrm{KP}(\mu)/\!\sim_\mu\,.$$

This terminology is justified by item (ii) of the following result.

Lemma 2.8. [4, Lem. 2.2, Prop. 2.4] *Let $\mu < \nu$ be two nodes in $\mathcal{T}$. Let $\mathbf{t}(\mu,\nu)$ be the set of monic polynomials $\phi \in K[x]$ of minimal degree satisfying $\mu(\phi) < \nu(\phi)$.*

(i) The set $\mathbf{t}(\mu,\nu)$ is a tangent direction of μ. Moreover, for any $\phi \in \mathbf{t}(\mu,\nu)$ and any nonzero $g \in K[x]$, the equality $\mu(g) = \nu(g)$ holds if and only if $\phi \nmid_\mu g$.

(ii) If $\mu < \nu'$ for some $\nu' \in \mathcal{T}$, then

$$\mathbf{t}(\mu,\nu) = \mathbf{t}(\mu,\nu') \iff (\mu,\nu\,] \cap (\mu,\nu'\,] \neq \emptyset.$$

Whenever $\mu < \nu$ in $\mathcal{T}$, there is an homomorphism of graded algebras $\mathcal{G}_\mu \to \mathcal{G}_\nu$, defined by

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

By Lemma 2.8, the kernel of $\mathcal{G}_\mu \to \mathcal{G}_\nu$ is the homogeneous prime ideal generated by $\mathrm{in}_\mu\,\phi$. The image is the subalgebra $\mathcal{G}_\nu^0$ [28, Cor. 2.6].

Let $\mathcal{HP}(\mathcal{G}_\mu) \subset \mathcal{H}(\mathcal{G}_\mu)$ be the subset of all homogeneous prime elements in $\mathcal{G}_\mu$. The multiplicative group $\mathcal{H}(\mathcal{G}_\mu^*)$ acts on $\mathcal{H}(\mathcal{G}_\mu)$ and $\mathcal{HP}(\mathcal{G}_\mu)$ by ordinary multiplication. We denote the orbit of any $t \in \mathcal{H}(\mathcal{G}_\mu)$ by

$$[\,t\,]_{\mathrm{unit}} := t\,\mathcal{H}(\mathcal{G}_\mu^*) \in \mathcal{H}(\mathcal{G}_\mu)/\mathcal{H}(\mathcal{G}_\mu^*).$$

Clearly, two homogeneous prime elements generate the same ideal if and only if they have the same class in $\mathcal{HP}(\mathcal{G}_\mu)/\mathcal{H}(\mathcal{G}_\mu^*)$. Thus, this quotient set can be identified with the set of all homogeneous principal prime ideals in $\mathcal{G}_\mu$. The next result, which follows easily from [27, Thm. 6.8], shows that all these prime ideals are generated by initial coefficients of key polynomials.

Theorem 2.9. *Let $\mu \in \mathcal{T}^{\mathrm{inn}}$.*

(i) *All $t \in \mathcal{H}(\mathcal{G}_\mu)$ factorize as a product of prime elements. The factorization is unique up to reordering the factors and multiplication by homogeneous units.*
(ii) *There is a canonical bijection:*

$$\mathbf{td}(\mu) \longrightarrow \mathcal{HP}(\mathcal{G}_\mu)/\mathcal{H}(\mathcal{G}_\mu^*), \qquad [\phi]_\mu \longmapsto [\mathrm{in}_\mu \phi]_{\mathrm{unit}}.$$

For a given $g \in \mathrm{Irr}(K)$, let $\mathcal{F}(g)$ be the set of monic irreducible factors of g in $K^h[x]$. Also, for all $\mu \in \mathcal{T}^{\mathrm{inn}}$, let us denote

$$\mathcal{F}_\mu(g) = \{G \in \mathcal{F}(g) \mid \mu < w_G\}.$$

As mentioned in Problem 1.4, the OM-algorithm aims to compute, for each $G \in \mathcal{F}(g)$, a chain of valuations in $\mathcal{T}^{\mathrm{inn}}$ getting sufficiently close to the valuation w_G. To this purpose, for a given valuation $\mu \in \mathcal{T}^{\mathrm{inn}}$, we need to compute the tangent directions of μ "pointing out" to leaves $w_G \in \mathcal{L}_{\mathrm{fin}}$ associated to some $G \in \mathcal{F}(g)$; that is, we need to solve :

Problem 2.10. *Compute the tangent directions of μ determined by the set $\mathcal{F}_\mu(g)$.*

To this aim, we use the following criterion of Barnabé-Novacoski [5, Thms. 1.1,1.3].

Theorem 2.11. *Let $\mu \in \mathcal{T}^{\mathrm{inn}}$ and $g \in \mathrm{Irr}(K)$. The image of the composition*

$$\mathcal{F}_\mu(g) \to \mathbf{td}(\mu) \to \mathcal{HP}(\mathcal{G}_\mu)/\mathcal{H}(\mathcal{G}_\mu^*), \qquad G \mapsto \mathbf{t}(\mu, w_G) \mapsto \mathbf{t}(\mu, w_G)\mathcal{H}(\mathcal{G}_\mu^*).$$

is the set of prime homogeneous factors of $\mathrm{in}_\mu g \in \mathcal{G}_\mu$, up to units. In particular, $\mathcal{F}_\mu(g) = \emptyset$ if and only if $\mathrm{in}_\mu g$ is a unit in $\mathcal{G}_\mu$.

Problem 2.10 is thus equivalent to :

Problem 2.12. *Given a nonzero $g \in K[x]$, compute the prime factorization of $\mathrm{in}_\mu g$ in $\mathcal{G}_\mu$.*

After Theorem 2.5, this amounts to factorizing $\mathrm{in}_\mu g$ in the algebra $\mathcal{G}_\mu^0[X]$ (where X is an indeterminate). However, working in this algebra is computationally painful. A crucial feature of the OM-algorithm is that it provides the factorization of $\mathrm{in}_\mu g$ by working in the subring

$$\Delta_\mu := \mathcal{P}_0/\mathcal{P}_0^+ \subset \mathcal{G}_\mu$$

of all homogeneous elements of grade zero, which is a polynomial ring with coefficients in a field. This is the aim of Section 2.3.

2.3. **Residual polynomial operators.** Let $\kappa := \kappa(\mu)$ be the relative algebraic closure of k in k_μ. There are canonical injective ring homomorphisms

$$k \hookrightarrow \kappa \hookrightarrow \Delta_\mu \hookrightarrow k_\mu.$$

Let $\Gamma_\mu^0 := \{\mu(a) \mid a \in K[x],\ 0 \le \deg(a) < \deg(\mu)\}$ be the subgroup of all grades of homogeneous units. By (2.2), we have $\Gamma_\mu = \langle\, \Gamma_\mu^0, \mu(\phi)\,\rangle$.

Definition 2.13. *The* relative ramification index *of μ is $e = e_{\mathrm{rel}}(\mu) := \big(\Gamma_\mu \colon \Gamma_\mu^0\big)$. This is the least positive integer such that $e\mu(\phi) \in \Gamma_\mu^0$.*

The following result is classical. A proof can be found in [27, Thms. 4.5, 4.6].

Theorem 2.14. *Let $\pi = \mathrm{in}_\mu \phi$ for a key polynomial ϕ of minimal degree. Take any homogeneous unit $u \in \mathcal{H}(\mathcal{G}_\mu^*)$ of grade $e\mu(\phi)$. Then, $\xi = \pi^e u^{-1} \in \Delta_\mu$ is transcendental over k and satisfies $\Delta_\mu = \kappa[\xi]$. Moreover, the canonical embedding $\Delta_\mu \hookrightarrow k_\mu$ induces an isomorphism $\kappa(\xi) \simeq k_\mu$.*

The pair ϕ, u determines a *residual polynomial operator*

$$R = R_{\mu,\phi,u}\colon\ K[x] \longrightarrow \kappa[y].$$

Let us recall its definition. We agree that $R(0) = 0$. Having in mind definition (2.3), for a nonzero $g \in K[x]$ with ϕ-expansion $g = \sum_{n\geq 0} a_n \phi^n$, let us denote

$$S := S_{\mu,\phi}(g), \quad \ell_0 := \min(S), \quad \ell := \max(S) = \deg_\mu(g),$$

Note that $\bar{a}_\ell = \mathrm{lc}_\mu(g)$. Let $\gamma = \mu(\phi)$. For all $n \in \mathbb{N}$ we have

$$n \in S \iff \mu(a_n) + n\gamma = \mu(a_{\ell_0}) + \ell_0\gamma \iff (n-\ell_0)\gamma = \mu(a_{\ell_0}) - \mu(a_n).$$

This implies $(n-\ell_0)\gamma \in \Gamma_\mu^0$, so that $n - \ell_0 = je$ for some $j \in \mathbb{N}$. Since $\ell \in S$, this shows in particular that $\ell - \ell_0 = de$ for some $d \in \mathbb{N}$. Let us denote

$$\ell_j := \ell_0 + je, \qquad 0 \leq j \leq d.$$

Note that $\ell_d = \ell$. Finally, for all $0 \leq j \leq d$, consider the *residual coefficient*

$$\zeta_j := \begin{cases} (\bar{a}_\ell)^{-1}\, u^{j-d}\, \bar{a}_{\ell_j} \in \Delta_\mu^* = \kappa^*, & \text{if } \ \ell_j \in S, \\ 0, & \text{otherwise.} \end{cases}$$

Definition 2.15. $R(g) := \zeta_0 + \zeta_1\, y + \cdots + \zeta_{d-1} y^{d-1} + y^d \in \kappa[y]$.

Since $\ell_0 \in S$, we have $\zeta_0 \neq 0$. The following result reflects the essential property of this operator.

Theorem 2.16. *For all nonzero $g \in K[x]$, $\mathrm{in}_\mu\, g = \mathrm{lc}_\mu(g)\, u^d\, \pi^{\ell_0}\, R(g)(\xi)$.*

Indeed, as $\mathrm{lc}_\mu(g) = \bar{a}_\ell$, this follows immediately from:

$$\bar{a}_\ell^{-1}\, \mathrm{in}_\mu\, g = \sum_{\ell_j \in S} \bar{a}_\ell^{-1} \bar{a}_{\ell_j}\, \pi^{\ell_j} = \pi^{\ell_0} \sum_{\ell_j \in S} \bar{a}_\ell^{-1} \bar{a}_{\ell_j}\, \pi^{je} = u^d \pi^{\ell_0} \sum_{\ell_j \in S} \zeta_j\, (\pi^e/u)^j.$$

Corollary 2.17. [27, Cor. 5.4] *For all $g, h \in K[x]$ we have $R(gh) = R(g)R(h)$.*

With this tool in hand, [27, Props. 6.3, 6.6] determine the whole set $\mathrm{KP}(\mu)$.

Theorem 2.18. *For a residually transcendental μ, take $\phi \in \mathrm{KP}(\mu)$ of minimal degree m. A monic $Q \in K[x]$ is a key polynomial for μ if and only if either*

- $\deg(Q) = m$ *and* $Q \sim_\mu \phi$, *or*
- $\deg(Q) = me\deg(R(Q))$ *and* $R(Q)$ *is irreducible in* $\kappa[y]$.

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

$$Q \mid_\mu Q' \iff Q \sim_\mu Q' \iff R(Q) = R(Q') \implies \deg(Q) = \deg(Q').$$

Corollary 2.19. *Let μ be a valuation on $K[x]$ admitting a key polynomial $\phi \in \mathrm{KP}(\mu)$. For any valuation $\mu < \nu$, we have*

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

Proof. If $\mathbf{t}(\mu,\nu) = [\phi]_\mu$, then $\mu(\phi) < \nu(\phi)$ by the definition of the tangent direction. Conversely, suppose $\mu(\phi) < \nu(\phi)$ and let $\mathbf{t}(\mu,\nu) = [\varphi]_\mu$. Then, $\varphi \mid_\mu \phi$, and this implies $\varphi \sim_\mu \phi$ by Theorem 2.18. □

It is easy to design a *lifting routine* [27, Cor. 5.6]

$$\mathrm{lift}_{\mu,\phi}\colon\ \mathrm{Irr}(\kappa) \setminus \{y\} \longrightarrow \mathrm{KP}(\mu), \qquad \psi \longmapsto Q,$$

to construct $Q \in \mathrm{KP}(\mu)$ with a given $R(Q) = \psi$. We deduce a bijection

$$\mathbf{td}(\mu) \longrightarrow \mathrm{Irr}(\kappa), \qquad [Q]_\mu \longmapsto \begin{cases} y, & \text{if } Q \sim_\mu \phi, \\ R(Q), & \text{otherwise,} \end{cases}$$

which depends on the choice of the pair ϕ, u. The variation of $R(Q)$ with respect to the pair ϕ, u is exhaustively discussed in [27, Sec. 5].

Solution of Problem 2.12. The efficient factorization of $\mathrm{in}_\mu g$ follows from Theorem 2.16. Let us factorize $R(g)$ as a product of powers of pairwise different irreducible polynomials in $\kappa[y]$:

$$R(g) = \psi_1^{n_1} \dots \psi_r^{n_r}, \qquad \psi_1, \dots, \psi_r \in \mathrm{Irr}(\kappa).$$

By [27, Lem. 6.1], we obtain a factorization $R(g)(\xi) = \psi_1(\xi)^{n_1} \dots \psi_r(\xi)^{n_r}$ as a product of homogeneous prime elements in $\mathcal{G}_\mu$. Take $Q_i \in \mathrm{KP}(\mu)$ lifting ψ_i and denote $\pi_i := \mathrm{in}_\mu Q_i$, for all i. By Theorem 2.16,

$$\pi_i \sim_{\mathrm{unit}} \psi_i(\xi) \quad \text{ for all } 1 \le i \le r,$$

where $\sim_{\mathrm{unit}}$ indicates equality up to multiplication by some unit. Therefore, we obtain the following factorization of $\mathrm{in}_\mu g$:

$$\mathrm{in}_\mu g \sim_{\mathrm{unit}} \pi^{\ell_0} \psi_1(\xi)^{n_1} \dots \psi_r(\xi)^{n_r} \sim_{\mathrm{unit}} \pi^{\ell_0} \pi_1^{n_1} \dots \pi_r^{n_r}. \tag{2.5}$$

The exponents $n_1, \dots, n_r$ are all positive, but $\ell_0 = \min(S_{\mu,\phi}(g))$ might vanish.

Example. Let ω be the Gauss' valuation on $K[x]$, as defined by (2.1). Consider the key polynomial $\phi = x$ and its corresponding homogeneous prime element $\pi = \mathrm{in}_\omega x \in \mathcal{G}_\omega$. Since $\omega(1) = 0 = \omega(x)$, we may consider $u = \mathrm{in}_\omega 1$ and $\xi = \pi$. We have natural identifications $k = \kappa$ and $\Delta_\omega = k[\pi]$. Given $g = \sum a_i x^i \in K[x]$, the residual polynomial $R_{\omega,\phi,u}(g) \in k[y]$ can be identified to the reduction $\bar{g} := g(y)/a_\ell \pmod{\mathcal{O}_v}$ where ℓ is the greatest exponent for which $\omega(g) = v(a_\ell)$. The factorization of (2.5) mimicks the factorization of $\bar{g}$ into a product of irreducible polynomials in $k[y]$. The exponent ℓ_0 is equal to $\mathrm{ord}_y(\bar{g})$.

Convention. Throughout the paper, we shall denote the operator $R_{\mu,\phi,u}$ simply by $R_{\mu,\phi}$, omitting its dependence on the choice of a suitable homogeneous unit $u \in \mathcal{G}_\mu$. Note that the degree of $R_{\mu,\phi}(g)$ does not depend on the choice of u.

Summary. Now that we know how to compute the direction in which we need to progress in the tree, we must build from an inner node $\mu \in \mathcal{T}$ and a tangent direction $[\phi]_\mu$ some suitable "augmented" valuations $\mu < \nu$. The next section is dedicated to describe the various kinds of augmentations (ordinary or limit) together with the chain they form in the tree $\mathcal{T}$. Also, we compute the residual degree and the ramification index of the end nodes of these chains.

3. Mac Lane–Vaquié chains

3.1. **Depth-zero valuations and ordinary augmentations.** For all $a \in K$, $\gamma \in \Gamma_{\mathbb{Q}}\infty$, we may construct the *depth-zero* valuation $\mu = [v;\, x-a, \gamma] \in \mathcal{T}$, defined in terms of $(x-a)$-expansions as

$$g = \sum\nolimits_{n\ge 0} a_n (x-a)^n \implies \mu(g) = \min\{v(a_n) + n\gamma \mid n \ge 0\}.$$

Note that $\mu(x-a) = \gamma$. If $\gamma < \infty$, then μ is an inner node of $\mathcal{T}$ and $x-a$ is a key polynomial for μ of minimal degree. If $\gamma = \infty$, then μ is the unique finite leaf of $\mathcal{T}$ with support $(x-a)K[x]$. In both cases, $\deg(\mu) = 1$.

Let μ be an inner node of $\mathcal{T}$. For all $\phi \in \mathrm{KP}(\mu)$ and all $\gamma \in \Gamma_{\mathbb{Q}}\infty$ such that $\mu(\phi) < \gamma$, we may construct the *ordinary* augmented valuation $\nu = [\mu;\, \phi, \gamma] \in \mathcal{T}$, defined in terms of ϕ-expansions as

$$g = \sum\nolimits_{n\ge 0} a_n \phi^n, \quad \deg(a_n) < \deg(\phi) \implies \nu(g) = \min\{\mu(a_n) + n\gamma \mid n \ge 0\},$$

Note that $\nu(\phi) = \gamma$, $\mu < \nu$ and $\mathbf{t}(\mu, \nu) = [\phi]_\mu$. If $\gamma < \infty$, then ν is an inner node of $\mathcal{T}$ and ϕ is a key polynomial for ν of minimal degree [27, Cor. 7.3]. If $\gamma = \infty$, then ν is a finite leaf of $\mathcal{T}$ with support $\phi K[x]$. In both cases, $\deg(\nu) = \deg(\phi)$.

3.2. **Limit augmentation of valuations.** Let $\mathcal{C} = (\rho_i)_{i\in A}$ be a totally ordered family of inner nodes of $\mathcal{T}$, not admitting a last element. Assume that A is a totally ordered set and $\rho_i < \rho_j$ if and only if $i < j$ in A.

We say that $\mathcal{C}$ has *stable degree* if $\deg(\rho_i)$ is stable for all sufficiently large $i \in A$. In this case, we denote this stable degree by $\deg(\mathcal{C})$.

We say that $g \in K[x]$ is *$\mathcal{C}$-stable* if for some index $i \in A$, we have $\rho_i(g) = \rho_j(g)$ for all $j > i$, and *$\mathcal{C}$-unstable* otherwise. We may define a *stability function* $\rho_{\mathcal{C}}(g) = \max\{\rho_i(g) \mid i \in A\}$, on the set of all $\mathcal{C}$-stable polynomials.

Definition 3.1. *A* limit key polynomial *for $\mathcal{C}$ is a monic $\mathcal{C}$-unstable polynomial of minimal degree. Let $\mathrm{KP}_\infty(\mathcal{C})$ be the set of all limit key polynomials. Since the product of stable polynomials is stable, all limit key polynomials are irreducible in $K[x]$.*

We say that $\mathcal{C}$ is an essential continuous family *of valuations if it has stable degree and admits limit key polynomials of degree greater than* $\deg(\mathcal{C})$.

For all $\phi \in \mathrm{KP}_\infty(\mathcal{C})$ and all $\gamma \in \Gamma_{\mathbb{Q}}\infty$ such that $\rho_i(\phi) < \gamma$ for all $i \in A$, we may construct the *limit augmented* valuation $\mu = [\mathcal{C}; \phi, \gamma] \in \mathcal{T}$, defined in terms of ϕ-expansions as:

$$g = \sum\nolimits_{n\geq 0} a_n\phi^n, \quad \deg(a_n) < \deg(\phi) \implies \mu(g) = \min\{\rho_{\mathcal{C}}(a_n) + n\gamma \mid n \geq 0\}.$$

Note that $\mu(\phi) = \gamma$ and $\rho_i < \mu$ for all $i \in A$.

If $\gamma < \infty$, then μ is an inner node of $\mathcal{T}$ and ϕ is a key polynomial for μ of minimal degree [27, Cor. 7.13]. If $\gamma = \infty$, then μ is a finite leaf of $\mathcal{T}$ with support $\phi K[x]$. In both cases, $\deg(\mu) = \deg(\phi)$.

3.3. **Mac Lane–Vaquié chains.** Take a chain of finite length r, of valuations in $\mathcal{T}$

$$v \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \longrightarrow \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu \tag{3.1}$$

in which $\mu_0 = [v; \phi_0, \gamma_0]$ is a depth-zero valuation, and each other node is an augmentation of the previous node, of one of the two types:

Ordinary augmentation: $\mu_{n+1} = [\mu_n; \phi_{n+1}, \gamma_{n+1}]$, for some $\phi_{n+1} \in \mathrm{KP}(\mu_n)$.

Limit augmentation: $\mu_{n+1} = [\mathcal{C}_n; \phi_{n+1}, \gamma_{n+1}]$, for some $\phi_{n+1} \in \mathrm{KP}_\infty(\mathcal{C}_n)$, where $\mathcal{C}_n$ is an essential continuous family whose first valuation is μ_n.

The continuous families $\mathcal{C}_n$ underlying the limit augmentations are omitted in the synthetic description (3.1) of the chain.

Definition 3.2. *A chain of mixed augmentations as in (3.1) is said to be a* Mac Lane–Vaquié (MLV) chain *if every augmentation step satisfies:*

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

In this case, we have $\mu(\phi_n) = \gamma_n$ for all n. As shown in [28, Sec. 4.1], the MLV chain induces a chain of value groups

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

such that $\Gamma_{\mu_{n-1}} = \Gamma^0_{\mu_n}$ for all $0 \leq n \leq r$, and

$$\Gamma_{\mu_n} = \left\langle \Gamma_{\mu_{n-1}}, \gamma_n \right\rangle \text{ if } \gamma_n < \infty, \qquad \Gamma_\mu = \Gamma_{\mu_{r-1}} \text{ if } \gamma_r = \infty. \tag{3.2}$$

For all $0 \leq n \leq r$, let us denote $e_n := e_{\mathrm{rel}}(\mu_n) = \left(\Gamma_{\mu_n} \colon \Gamma_{\mu_{n-1}}\right)$.

Also, the homomorphisms $\mathcal{G}_{\mu_n} \to \mathcal{G}_{\mu_{n+1}}$ induce a tower of finite and simple extensions of fields

$$\kappa(\mu_{-1}) := k \to \kappa(\mu_0) \to \cdots \to \kappa(\mu_r) = \kappa(\mu).$$

For all $0 \leq n < r$, let us denote

$$f_n := [\kappa(\mu_{n+1}) \colon \kappa(\mu_n)] = \deg\left(R_{\mu_n,\phi_n}(\phi_{n+1})\right),$$

the last equality by [28, Lem. 5.2,5.3].

If μ has nontrivial support $gK[x]$, then we can read in the MLV chain of μ the ramification index $e(\overline{\mu}/v) := (\Gamma_{\overline{\mu}} \colon \Gamma)$ and residual degree $f(\overline{\mu}/v) := [k_{\overline{\mu}} : k]$ of the valuation $\overline{\mu}$ induced by μ on the field $K[x]/(g)$. Obviously, $\Gamma_{\overline{\mu}} = \Gamma_\mu$ and (by definition) $k_{\overline{\mu}} = k_\mu$.

Proposition 3.3. [28, Thm. 5.4] *If $\gamma_r = \infty$, then μ is a finite leaf with $k_\mu = \kappa(\mu)$. In particular, $e(\overline{\mu}/v) = e_0 \cdots e_{r-1}$ and $f(\overline{\mu}/v) = f_0 \cdots f_{r-1}$.*

The following theorem is due to Mac Lane, for the discrete rank-one case [22], and Vaquié for the general case [44]. Another proof may be found in [28, Thm. 4.3].

Theorem 3.4. *All $\mu \in \mathcal{T}^{\mathrm{inn}} \sqcup \mathcal{L}_{\mathrm{fin}}$ are the end node of a finite MLV chain.*

The main advantage of MLV chains is that we may read in them several data intrinsically associated to the valuation μ, like the length of the chain, the positive integers $\deg(\mu_n)$, e_n, f_n for all $n \geq 0$, and the character "ordinary" or "limit" of each augmentation step [28, Sec. 4.3].

Definition 3.5. *The* depth *of μ is the length of any MLV chain with end node μ. We say that μ is* inductive *if all augmentations in its MLV chain are ordinary.*

3.4. **Inductive valuations and Henselization.** Let (K^h, v^h) be a Henselization of (K, v) and let μ^h be the unique common extension of μ and v^h to $K^h[x]$ (Theorem 1.1). The mapping $\mathrm{in}_\mu g \mapsto \mathrm{in}_{\mu^h} g$, for all $g \in K[x]$, induces an embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_{\mu^h}$ of graded algebras.

Theorem 3.6. [30, Thm. 1.2] *For all valuations μ on $K[x]$ the canonical embedding $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_{\mu^h}$ is an isomorphism of graded algebras.*

Lemma 3.7. *Let μ be an inductive valuation on $K[x]$, admitting a MLV chain as in (3.1). Then, $\mathrm{KP}(\mu) \subset \mathrm{KP}(\mu^h)$ and μ^h is inductive, admitting a MLV chain with the same length r and data (ϕ_n, γ_n) for all $0 \leq n \leq r$:*

$$v^h \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0^h \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1^h \overset{\phi_2,\gamma_2}{\longrightarrow} \cdots \longrightarrow \mu_{r-1}^h \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r^h = \mu^h.$$

Moreover, the numerical data $e_0, \ldots, e_r$; $f_0, \ldots, f_{r-1}$ attached to both chains coincide.

Proof. The first statement follows from [30, Sec. 5.2]. The value groups of both MLV chains coincide by (3.2); hence, both chains determine the same data $e_0, \ldots, e_r$. Finally, the two towers of fields $\kappa(\mu_n) \to \kappa(\mu_{n+1})$ and $\kappa(\mu_n^h) \to \kappa(\mu_{n+1}^h)$ are isomorphic by Theorem 3.6 and the commutativity of the diagrams

$$\begin{array}{ccc} \mathcal{G}_{\mu_n}^h & \longrightarrow & \mathcal{G}_{\mu_{n+1}}^h \\ \uparrow & & \uparrow \\ \mathcal{G}_{\mu_n} & \longrightarrow & \mathcal{G}_{\mu_{n+1}}. \end{array}$$

Hence, both chains determine the same data $f_0, \ldots, f_{r-1}$ as well. □

Summary. We have seen how to extend a valuation μ in a direction $[\phi]_\mu$ for a given parameter $\gamma \in \Gamma_\mathbb{Q}\infty$. The next section is devoted to show that, as in the discrete rank one case, the slopes of a certain Newton polygon provide the suitable $\gamma \in \Gamma_\mathbb{Q}\infty$ which are necessary to construct MLV chains solving our original Problem 1.4.

4. Newton polygons and double dissections

Consider two points $P = (n, \alpha)$, $Q = (m, \beta)$ in the $\mathbb{Q}$-vector space $\mathbb{Q} \times \Gamma_\mathbb{Q}$. The segment joining P and Q is the subset

$$S := \left\{ P + \delta \overrightarrow{PQ} \mid \ \delta \in \mathbb{Q},\ 0 \leq \delta \leq 1 \right\} \subset \mathbb{Q} \times \Gamma_\mathbb{Q}.$$

If $n \neq m$, this segment has a natural slope: $(\beta - \alpha)/(m - n) \in \Gamma_\mathbb{Q}$.

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

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

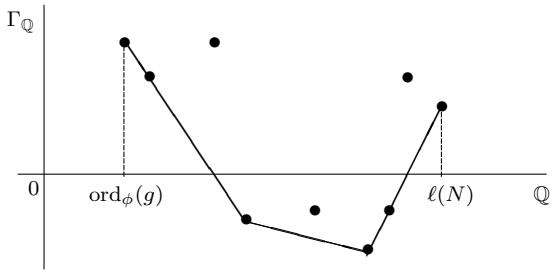
4.1. **Classical Newton polygons.** Let $\bar{v}$ be a fixed extension of v to $\overline{K}$ and (K^h, v^h) the corresponding Henselization of (K, v) . Let us recall the classical *Newton polygon* operator

$$N_{v,x} \colon K[x] \longrightarrow \mathcal{P}(\mathbb{Q} \times \Gamma_\mathbb{Q}),$$

where $\mathcal{P}(\mathbb{Q} \times \Gamma_\mathbb{Q})$ is the power set of the rational vector space $\mathbb{Q} \times \Gamma_\mathbb{Q}$. The Newton polygon of the zero polynomial is the empty set.

Definition 4.1. *For a nonzero $g = a_0 + \cdots + a_\ell x^\ell \in K[x]$, the Newton polygon $N_{v,x}(g)$ is the lower convex hull of the finite cloud of points $\{(n, v(a_n)) \mid n \geq 0\}$.*

FIGURE 1. Newton polygon $N = N_{\mu,\phi}(g)$ of a general $g \in K[x]$.



Thus, $N := N_{v,x}(g)$ is either a single point or a chain of segments, $S_1, \ldots, S_t$, called the *sides* of the polygon, ordered from left to right by increasing slopes. The abscissa of the left endpoint of N is $\mathrm{ord}_x(g)$. We define the *length* $\ell(S_i)$ of a side as the length of its projection to the x-axis.

For all $g \in K[x]$, let $Z(g)$ be the multiset of all roots of g in $\overline{K}$, counting multiplicities. Also, let $V(g)$ be the multiset of all values $\bar{v}(\theta) \in \Gamma_{\mathbb{Q}}$, for θ running on $Z(g) \setminus \{0\}$. Both multisets have cardinality $\ell = \deg(g)$. We indicate $\lambda^{(n)}$ for λ repeated n times.

Theorem 4.2. [31, Satz 6.3] *For a nonzero $g \in K[x]$, suppose that the sides of $N_{v,x}(g)$ have slopes $-\lambda_1 < \cdots < -\lambda_t$ and lengths $\ell_1, \ldots, \ell_t$. Then, $V(g) = \left\{\lambda_1^{(\ell_1)}, \ldots, \lambda_t^{(\ell_t)}\right\}$.*

By the Henselian property, all roots of an irreducible polynomial in $K^h[x]$ have the same $\bar{v}$-value. Hence, Theorem 4.2 determines a *slope factorization* of g :

$$g = x^{\mathrm{ord}_x(g)} F_1 \cdots F_t, \quad F_i \in K^h[x], \quad \deg(F_i) = \ell_i,$$

where F_i is the product of all irreducible factors of g in $K^h[x]$ such that the $\bar{v}$-value of its roots is λ_i. Therefore, the Newton polygon determines a *dissection* of the multiset $\mathcal{F}(g)$ of all irreducible factors of g in $K^h[x]$, counting multiplicities.

Moreover, for each irreducible factor $G \in K^h[x]$ of g, we have

$$G \mid F_i \implies [v;\, x, \lambda_i] \le w_G, \quad \text{for all } 1 \le i \le t.$$

Thus, it is natural to take $[v;\, x, \lambda_i]$ as the initial node of all MLV chains aiming to describe w_G for all irreducible factors G of F_i in $K^h[x]$.

Example 4.3. *Let us see how this applies to the polynomial $g = Q^8 + 1410\, t_1^{57}\, t_2^{30}\, P^{36}$ of Example 1.5. Recall that $P = x^2 + x + 1$ and $Q = P^{72} + 1406\, t_1^6\, t_2^4 \in \mathbb{F}_p(t_1, t_2)$, with $v(t_1) = 1$ and $v(t_2) = \sqrt{2}$.*

Since g has coefficients in $\mathcal{O}$, the whole classical Newton polygon $N_{x,v}(g)$ lies in the non-negative quadrant. Moreover, g is monic and its constant coefficient is $(1 + 1406 t_1^6 t_2^3)^8 + 1410\, t_1^{57}\, t_2^{30}$, which has value zero; therefore $N_{x,v}(g)$ consists of a single side of slope 0.

Thus, all MLV chains we are aiming to construct will have the same initial node: the Gauss' valuation $\mu_0 = [v;\, \phi_0, \gamma_0]$, where $\phi_0 = x$ and $\gamma_0 = 0$. Since $\Gamma_{\mu_0} = \Gamma$, we have $e_0 = 1$.

The dissection associated to $N_{x,v}(g)$ being trivial, we detect no reducibility at this stage.

4.2. **General Newton polygons.** A *type* is a pair (μ, ϕ), where μ is an inner node of $\mathcal{T}$ and ϕ is a key polynomial for μ. Any type (μ, ϕ) yields a Newton polygon operator

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

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

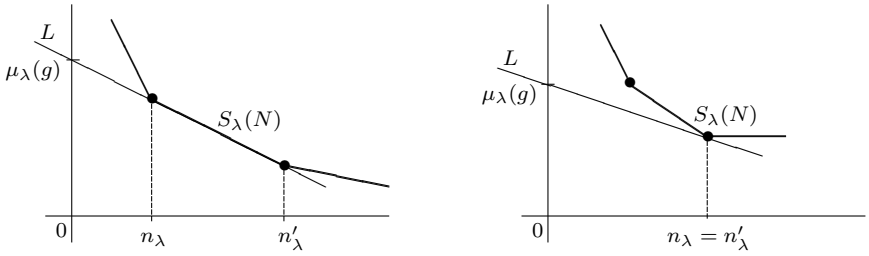
Definition 4.4. *For a nonzero $g \in K[x]$ with ϕ-expansion*

$$g = \sum\nolimits_{n \ge 0} a_n \phi^n, \quad a_n \in K[x], \quad \deg(a_n) < \deg(\phi),$$

we define $N := N_{\mu,\phi}(g)$ as the lower convex hull of the finite set $\{(n, \mu(a_n)) \mid n \ge 0\}$.

The abscissa of the left endpoint of N is $\mathrm{ord}_\phi(g)$ in $K[x]$. The abscissa $\ell(N) := \lfloor \deg(g)/\deg(\phi) \rfloor$ of the right endpoint of N is called the *length* of N. In Figure 1, we displayed the typical shape of such a polygon.

FIGURE 2. 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 $\lambda > \mu(\phi)$ and $\mu_\lambda = [\mu;\, \phi, \lambda]$.



Definition 4.5. *For all $\lambda \in \Gamma_{\mathbb{Q}}$, the* λ-component $S_\lambda(N) \subset N$ *is the intersection of N with the line of slope $-\lambda$ which first touches N from below. In other words,*

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

The abscissas of the endpoints of $S_\lambda(N)$ are denoted $n_\lambda \le n'_\lambda$. We say that N is one-sided *of slope $-\lambda$ if $N = S_\lambda(N)$, $n_\lambda = 0$ and $n'_\lambda > 0$.*

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

Definition 4.6. *The* principal Newton polygon $N^+_{\mu,\phi}(g)$ *is the polygon formed by the sides of $N_{\mu,\phi}(g)$ of slope less than $-\mu(\phi)$. If there are no such sides, then $N^+_{\mu,\phi}(g)$ is defined to be the left endpoint of $N_{\mu,\phi}(g)$.*

Clearly, $S_{\mu,\phi}(g)$ (as defined by (2.3)) coincides with the set of abscissas of the points lying on the segment $S_{\mu(\phi)}(g)$. In particular, $\ell\left(N^+_{\mu,\phi}(g)\right) = \min(S_{\mu,\phi}(g))$. Hence, the following result is an immediate consequence of (2.4).

Lemma 4.7. *The integer $\ell\left(N^+_{\mu,\phi}(g)\right)$ is the order with which the prime element* $\mathrm{in}_\mu\, \phi$ *divides* $\mathrm{in}_\mu\, g$ *in the graded algebra $\mathcal{G}_\mu$.*

Lemma 4.8. *Let (μ, ϕ) be a type. For $\lambda > \mu(\phi)$, let $\mu_\lambda = [\mu;\, \phi, \lambda]$. Then, for all nonzero $g \in K[x]$, the line of slope $-\lambda$ which first touches $N_{\mu,\phi}(g)$ from below, cuts the vertical axis at the point of ordinate $\mu_\lambda(g)$.*

Proof. The line of slope $-\lambda$ passing through (x, α) cuts the vertical axis at the ordinate $\alpha + \lambda x$. The minimal values of this ordinate are taken by $(x, \alpha) \in S_\lambda(N_{\mu,\phi}(g))$. □

4.3. **Dissection by Newton polygons.** Recall that $\mathcal{F}_\mu(g)$ is the set of irreducible factors $G \in K^h[x]$ of g such that $w_G > \mu$. Let us denote

$$\mathcal{F}_{\mu,\phi}(g) = \{G \in \mathcal{F}_\mu(g) \mid \mathbf{t}(\mu, w_G) = [\phi]_\mu\},$$
$$\mathcal{F}_{\mu,\phi}(g)(\lambda) = \{G \in \mathcal{F}_{\mu,\phi}(g) \mid w_G(\phi) = \lambda\}, \quad \text{for all } \lambda \in \Gamma_{\mathbb{Q}}.$$

We will show that the slopes of $N^+_{\mu,\phi}(g)$ determine a partition of $\mathcal{F}_{\mu,\phi}(g)$. A crucial point is the consideration of a special irreducible factor of ϕ in $K^h[x]$, determined by the valuation μ.

Definition 4.9. *The valuation $[\mu;\, \phi, \infty]$ has support $\phi K[x]$. As we saw in Section 1, there exists a unique irreducible factor $Q = Q_{\mu,\phi} \in \mathrm{Irr}(K^h)$ of ϕ such that*

$$[\mu;\, \phi, \infty] = w_Q.$$

We say that Q is the irreducible factor of ϕ over $K^h[x]$ determined by μ.

Theorem 4.10. *Let μ be an inner node of $\mathcal{T}$ and $\phi \in \mathrm{KP}(\mu)$. Denote $N = N^+_{\mu,\phi}(g)$ and let $Q \in \mathrm{Irr}(K^h)$ be the irreducible factor of ϕ determined by μ. Then,*

(i) *All $G \in \mathcal{F}_{\mu,\phi}(g)$ have degree a multiple of* $\deg(Q)$.

(ii) *For all* $\lambda \in \Gamma_{\mathbb{Q}}$*, we have*

$$\sum\nolimits_{G \in \mathcal{F}_{\mu,\phi}(g)(\lambda)} \deg(G) = \ell\left(S_\lambda(N)\right) \deg(Q).$$

In particular, if $\ell\left(S_\lambda(N)\right) = 1$*, then* $\mathcal{F}_{\mu,\phi}(g)(\lambda)$ *contains a unique irreducible factor of* g *in* $K^h[x]$*, and this factor has degree* $\deg(Q)$*.*

If v has rank one, then $\phi = Q$ and this theorem follows easily from Montes' original arguments in the discrete rank-one case. The proof in the general case is much more involved. We postpone it to Section 4.6, which is entirely devoted to this purpose.

Corollary 4.11. $\mathcal{F}_{\mu,\phi}(g) = \bigsqcup_\lambda \mathcal{F}_{\mu,\phi}(g)(\lambda)$ *where* $-\lambda$ *runs over the slopes of* $N^+_{\mu,\phi}(g)$*.*

Proof. Immediate from Theorem 4.10. □

4.4. **Dissection by factorization of residual polynomials.** For $g \in K[x]$ and our fixed type (μ, ϕ) as above, let $-\lambda_1 < \cdots < -\lambda_t$ be the slopes of $N^+_{\mu,\phi}(g)$. Let us assume that $\phi \nmid g$ in $K[x]$, so that $n_{\lambda_1} = 0$.

For each slope $-\lambda$ of $N^+_{\mu,\phi}(g)$, consider the augmentation $\mu_\lambda = [\mu;\, \phi, \lambda]$ and the factorization of the residual polynomial $R_{\mu_\lambda,\phi}(g)$ in $\kappa(\mu_\lambda)[y]$:

$$R_{\mu_\lambda,\phi}(g) = \psi_1^{n_1} \cdots \psi_s^{n_s}, \qquad \psi_1, \ldots, \psi_s \in \operatorname{Irr}(\kappa(\mu_\lambda)). \tag{4.1}$$

Let $\varphi_i = \operatorname{lift}_{\mu_\lambda,\phi}(\psi_i) \in \operatorname{KP}(\mu_\lambda)$ be arbitrary lifts for all $1 \le i \le s$.

Proposition 4.12. $\mathcal{F}_{\mu,\phi}(g)(\lambda) = \bigsqcup_{i=1}^s \mathcal{F}_{\mu_\lambda,\varphi_i}(g)$*.*

Proof. As we saw in Section 2.3, the factorization (4.1) leads to a factorization of $\operatorname{in}_{\mu_\lambda} g$ into a product of pairwise different homogeneous prime elements in $\mathcal{G}_{\mu_\lambda}$, up to units:

$$\operatorname{in}_{\mu_\lambda} g \sim_{\text{unit}} \pi^{n_\lambda} \pi_1^{n_1} \cdots \pi_s^{n_s}, \qquad \pi = \operatorname{in}_{\mu_\lambda} \phi, \quad \pi_i = \operatorname{in}_{\mu_\lambda} \varphi_i,\ 1 \le i \le s.$$

By Theorem 2.11, if $\lambda < \lambda_1$ (so that $n_\lambda > 0$), the irreducible factors of g in the set $\mathcal{F}_{\mu_\lambda}(g)$ determine exactly $s+1$ tangent directions of μ_λ, which are precisely

$$[\phi]_{\mu_\lambda},\ [\varphi_1]_{\mu_\lambda}, \ldots, [\varphi_s]_{\mu_\lambda}.$$

Take any irreducible factor $G \in \mathcal{F}_{\mu_\lambda}(g)$. By Corollary 2.19, $w_G(\phi) > \lambda$ if and only if $\mathbf{t}(\mu_\lambda, w_G) = [\phi]_{\mu_\lambda}$. Therefore, the irreducible factors G with $w_G(\phi) = \lambda$ are distributed among the remaining s tangent directions. The claimed dissection follows. If $\lambda = \lambda_1$, then $n_\lambda = 0$ and we get directly the same dissection. □

Corollary 4.11 and Proposition 4.12 lead to a double-dissection process, as illustrated by Figure 3. Going on, the computation of each principal Newton polygon $N^+_{\mu_\lambda,\varphi_i}(g)$ will lead to further double-dissections.

Definition 4.13. *We say that the type* (μ, ϕ) singles out *an irreducible factor of* g *in* $K^h[x]$ *if*

$$\mathcal{F}_{\mu,\phi}(g) = \{G\} \quad \text{and} \quad \deg(G) = \deg(Q_{\mu,\phi}).$$

If moreover ϕ *is irreducible in* $K^h[x]$ *(that is* $\phi = Q_{\mu,\phi}$*), we say that* ϕ *is an* approximant *of* G*.*

Proposition 4.14. *If in the factorization (4.1) we have* $n_i = 1$*, then the pair* (μ_λ, φ_i) *singles out an irreducible factor of* g *in* $K^h[x]$*.*

Proof. By Lemma 4.7, we know that

$$\ell\left(N^+_{\mu_\lambda,\varphi_i}(g)\right) = n_i, \quad 1 \le i \le s. \tag{4.2}$$

The result then follows from Theorem 4.10. □

Notice that (4.2) is relevant from a computational perspective: *in all required computations of principal Newton polygons, we know a priori the length of the polygon.*

Thus, it suffices to implement a Newton polygon routine

$$\operatorname{NP}(\mu, \phi, \ell)(g)$$

which finds only the first $\ell+1$ coefficients $a_0, \ldots, a_\ell$ of the ϕ-expansion of g, and then computes the lower convex hull of the set $\{(n, \mu(a_n)) \mid 0 \le n \le \ell\}$.

FIGURE 3. Double dissection of $\mathcal{F}_{\mu,\phi}(g)$. The figure represents paths in the tree $\mathcal{T}$, with initial node μ. The first "slope" dissection leads to the horizontal path determined by the nodes $\mu < \mu_{\lambda_t} < \cdots < \mu_{\lambda_1} < w_Q$. For each slope λ_i, the second "residual" dissection gives tangent directions of μ_{λ_i} represented by upwards paths, pointing out to the leaves w_G for all $G \in \mathcal{F}_{\mu_{\lambda_i},\phi}(g)$.

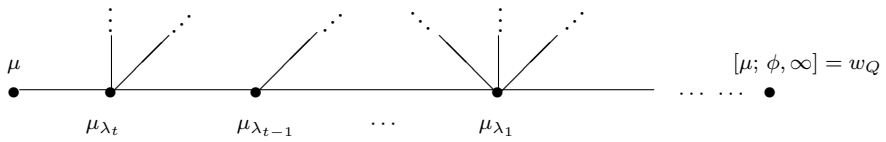
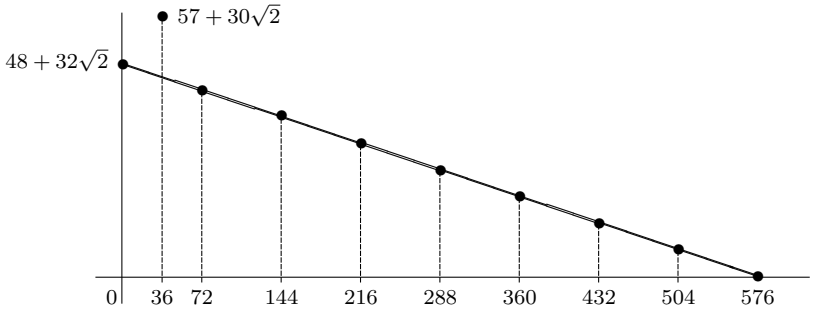


FIGURE 4. Newton polygon $N_{\mu_0,\phi_1}(g)$. The slope is $-\gamma_1$, where $\gamma_1 := \left(3 + 2\sqrt{2}\right)/36$.



Summary. We have shown so far that for any given type (μ, ϕ), we can derive a double-dissection

$$\mathcal{F}_{\mu,\phi}(g) = \bigsqcup_{\lambda} \bigsqcup_{i=1}^{s} \mathcal{F}_{\mu_\lambda,\varphi_i}(g).$$

Theorem 4.10 gives moreover information about the degrees and the number of irreducible factors of g in these sets. This double-dissection process can be continued inductively and whenever we find some $n_i = 1$ in (4.1), an irreducible factor of g is singled out. This sketches the OM algorithm, which will be described in Section 5.

Let us first illustrate the iteration of this double-dissection process in the particular case of Example 1.5.

4.5. **Resolution of Example 1.5.** We saw in Example 4.3 that the first dissection at depth zero detected no reducibility. The second dissection is determined by the factorization of $R_{\mu_0,\phi_0}(g)$ in $k[y] = \kappa(\mu_0)[y]$. Since $g \equiv P^{576} \pmod{\mathcal{M}}$, we get

$$R_{\mu_0,\phi_0}(g) = (y^2 + y + 1)^{576}.$$

Since this polynomial is a power of the irreducible polynomial $\psi_0 = y^2 + y + 1$, the second dissection at depth zero detects no reducibility either.

Let us choose a lift of ψ_0 with respect to (μ_0, ϕ_0). The most natural choice is

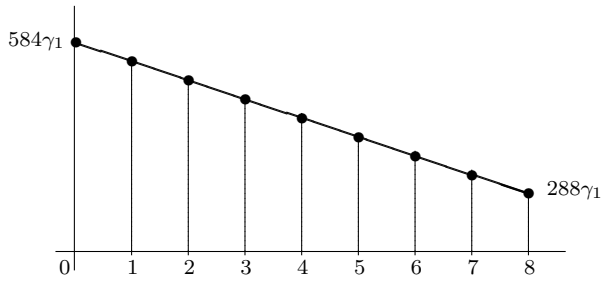
$$\phi_1 = \mathrm{lift}_{\mu_0,\phi_0}(\psi_0) = x^2 + x + 1 = P.$$

All augmentations $\mu = [\mu_0;\, \phi_1, \gamma_1]$, will have $f_0 = 2$ (with the notation of Section 3.3), because $\kappa(\mu) \simeq k[y]/(y^2 + y + 1)$. Let us represent this latter field as

$$\kappa_1 = k(z) \subset \overline{\mathbb{F}}_p, \qquad z^2 + z + 1 = 0.$$

Although we detect no reducibility yet, we obtain some information about the irreducible factors of g: all of them have associated valuations with residual degree multiple of 2.

FIGURE 5. Newton polygon $N^+_{\mu_1,\phi_2}(g)$. The slope is $-\gamma_2$, where $\gamma_2 := 37\gamma_1$.



Depth one. The first dissection at depth one is given by the slopes of the Newton polygon $N_{\mu_0,\phi_1}(g)$. The ϕ_1-expansion of g is immediately deduced from:

$$g = (\phi_1^{72} + 1406\, t_1^6\, t_2^4)^8 + 1410\, t_1^{57}\, t_2^{30}\, \phi_1^{36}.$$

One checks easily that $N_{\mu_0,\phi_1}(g)$ is one-sided of length 576. Its concrete shape is displayed in Figure 4. Therefore, we get a unique augmentation:

$$\mu_1 = [\mu_0, \phi_1, \gamma_1], \quad \gamma_1 = \left(3 + 2\sqrt{2}\right)/36.$$

In particular, $e_1 = (\Gamma_{\mu_1} \colon \Gamma_{\mu_0}) = 36$. Although we detect no reducibility yet, we know that all irreducible factors of g have associated valuations with ramification index multiple of 36.

In order to simplify the computation of $R_{\mu_1,\phi_1}(g)$, we observe that $g \sim_{\mu_1} Q^8$, so that

$$R_{\mu_1,\phi_1}(g) = R_{\mu_1,\phi_1}(Q^8) = R_{\mu_1,\phi_1}(Q)^8 = \left(y^2 + 1406\right)^8$$

in $\kappa_1[y]$. In the notation of Section 2.2, for the computation of $R_{\mu_1,\phi_1}(Q)$ we chose $u := \mathrm{in}_{\mu_1} W$, where $W = t_1^3 t_2^2$. The factorization of $R_{\mu_1,\phi_1}(g)$ detects that g is not irreducible:

$$R_{\mu_1,\phi_1}(g) = (y + 698z + 349)^8 (y - 698z - 349)^8.$$

This implies a factorization $g = F_1 F_2$, where $F_1, F_2 \in K^h[x]$ have both degree 576.

Denote $A_0 = 698x + 349$. Then, the irreducible factors of g in $K^h[x]$ determine two different tangent directions of μ_1, represented by the key polynomials:

$$\phi_2 := \phi_2^{F_1} = \mathrm{lift}_{\mu_1,\phi_1}(y + 698z + 349) = \phi_1^{36} + W A_0,$$

$$\phi_2^{F_2} = \mathrm{lift}_{\mu_1,\phi_1}(y - 698z - 349) = \phi_1^{36} - W A_0.$$

This splits the procedure into two independent tasks, which may be executed in parallel.

From now on, we focus on the factorization of F_1, by analyzing suitable augmentations of the form $\mu = [\mu_1; \phi_2, \gamma_2]$. Since the irreducible factor $\psi_1 := y + 698z + 349$ has degree one, we have $f_1 = 1$, because all these augmentations will have $\kappa(\mu) = \kappa_1[y]/\psi_1 \simeq \kappa_1$.

Depth two. Factors of F_1. The information we are interested in is located in the *principal* Newton polygon $N^+_{\mu_1,\phi_2}(g)$. By Lemma 4.7, the length of $N^+_{\mu_1,\phi_2}(g)$ is equal to $8 = \mathrm{ord}_{\psi_1} R_{\mu_1,\phi_1}(g)$. Thus, we need only to compute the (nine) first coefficients of the ϕ_2-expansion of g, and the desired Newton polygon is the lower convex hull of the corresponding nine points. This turns out to be the polygon displayed in Figure 5: one-sided, of slope $-\gamma_2$, where $\gamma_2 = 37\gamma_1$.

Therefore, we get a unique augmentation:

$$\mu_2 = [\mu_1; \phi_2, \gamma_2], \quad \gamma_2 = 37\gamma_1.$$

Thus, $e_2 = (\Gamma_{\mu_2} \colon \Gamma_{\mu_1}) = 1$. By choosing $u := \mathrm{in}_{\mu_2}(W\phi_1)$, we get:

$$R_{\mu_2,\phi_2}(g) = \frac{1}{702}\big(752 - (602z + 301)y - 298y^2 + (329z - 597)y^3 + 425y^4 + (-433z + 545)y^5 + 179y^6 - (156z + 78)y^7 + 702y^8\big),$$

which factorizes in $\kappa_1[y]$ as: $R_{\mu_2,\phi_2}(g) = \psi_2^8$, for $\psi_2 := y + 973z + 1248$.

So far, we detect no reducibility of F_1. Let $A_1 = 973x + 1248$. A possible lift of ψ_2 is:

$$\phi_3 = \mathrm{lift}_{\mu_2,\phi_2}(\psi_2) = \phi_1^{36} + WA_0 + WA_1\phi_1.$$

Note that $\deg(\phi_3) = \deg(\phi_2)$. This means that we get no new information on ramification indices ($e_2 = 1$) nor residual degrees ($f_2 = \deg \psi_2 = 1$).

On the other hand, for any future augmentation $\mu_3 = [\mu_2; \phi_3, \gamma_3]$, the chain

$$v \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \mu_1 \overset{\phi_2,\gamma_2}{\longrightarrow} \mu_2 \overset{\phi_3,\gamma_3}{\longrightarrow} \mu_3$$

will not be a MLV chain, because of $\deg(\phi_2) = \deg(\phi_3)$. MacLane showed that, in this situation, ϕ_3 is a key polynomial for μ_1 and $\mu_3 = [\mu_1; \phi_3, \gamma_3]$. In other words:

We may consider $\phi_3 = \mathrm{lift}_{\mu_1,\phi_1}(\psi)$ as a better choice than ϕ_2 as a lift of ψ_1 with respect to the type (μ_1, ϕ_1), and obtain μ_3 as a direct augmentation of μ_1.

A double-dissection that detects no reducibility and the degree of the key polynomial does not grow is said to be a **refinement step**. In this case, the most efficient procedure is to go back to μ_1 and consider the augmentations based on the type pair (μ_1, ϕ_3) instead of (μ_1, ϕ_2).

In order to keep a coherent notation, we rename ϕ_3 again as ϕ_2. That is, we take

$$\phi_2 := \phi_1^{36} + W\left(A_0 + A_1\phi_1\right).$$

Depth two, again. Consider the following family of linear polynomials:

$$\begin{array}{llll} A_1 = 973x + 1248, & A_2 = A_1, & A_3 = 235x + 879, & A_4 = 528x + 264, \\ A_5 = 329x + 926, & A_6 = 1079x + 1301, & A_7 = 103x + 813, & A_8 = 1271x + 1397, \end{array}$$

together with $A_9 = A_0 = 698x + 349$.

By iteration of the double-dissection loops, we fall in a series of nine consecutive refinement steps, leading to the following successive improved candidates for ϕ_2:

$$\phi_2^{(i)} = \phi_1^{36} + W\sum_{j=0}^{i} A_j\phi_1^j, \qquad 1 \le i \le 9.$$

Let us perform the double-dissection based on the type (μ_1, ϕ_2), for $\phi_2 = \phi_2^{(9)}$. Let $a_0, \dots, a_8 \in K[x]$ be the first nine coefficients of the ϕ_2-expansion of g. We have:

$$a_0 \sim_{\mu_1} -(322x + 161)W^{16}t_1^{12}, \qquad a_8 \sim_{\mu_1} 702\,W^8.$$

The polygon $N^+_{\mu_1,\phi_2}(g)$ is the line joining $(0, \mu_1(a_0))$ with $(8, \mu_1(a_8))$. Thus, it is a one-sided polygon of slope $-\gamma_2$, where

$$\gamma_2 := \frac{\mu_1(a_0) - \mu_1(a_8)}{8} = \frac{3}{2} + 36\gamma_1.$$

Moreover, all points $(i, \mu_1(a_i))$, for $1 \le i \le 7$, lie strictly above this line. Consider the augmentation

$$\mu_2 = [\mu_1; \phi_2, \gamma_2].$$

Clearly, $e_2 = (\Gamma_{\mu_2} \colon \Gamma_{\mu_1}) = 2$, so that the associated valuations of all irreducible factors of F_1 have ramification index multiple of 72. Also, the residual polynomial $R_{\mu_2,\phi_2}(g)$ will have degree 4.

Since $\mu_2(\phi_2^2) = 3 + 72\gamma_1$, we may choose $u := \mathrm{in}_{\mu_2}(W^2t_1^3)$. We obtain the residual polynomial:

$$R_{\mu_2,\phi_2}(g) = y^4 - (322z + 161)/702 = \left(y^2 - (35z - 419)\right)\left(y^2 + (35z - 419)\right),$$

where the two quadratic factors are irreducible.

By Proposition 4.14, we conclude that $F_1 \in K^h[x]$ is the product of two different irreducible polynomials of degree 288. They have both ramification index 72 and residual degree 4.

A concrete approximant to each irreducible factor can be obtained as a lift of the quadratic factors of $R_{\mu_2,\phi_2}(g)$ with respect to (μ_2, ϕ_2). For instance,

$$\phi_2^4 - (35x - 419)W^4t_1^6, \qquad \phi_2^4 + (35x - 419)W^4t_1^6.$$

The second branch. The analysis of the second branch, based on the type $(\mu_1, \phi_2^{F_2})$, leads to a completely analogous result. The polynomial $F_2 \in K^h[x]$ splits as the product of two irreducible factors of degree 288, with exactly the same arithmetic behaviour as above. Actually, by taking

$$\phi_2' = \phi_1^{36} - W\sum_{j=0}^{9} A_j \phi_1^j, \qquad \mu_2' = [\mu_1;\, \phi_2', \gamma_2],$$

we obtain completely analogous computations, leading to

$$R_{\mu_2',\phi_2'}(g) = y^4 + (322z + 161)/702 = \left(y^2 - (35z + 454)\right)\left(y^2 + (35z + 454)\right).$$

The corresponding approximants are:

$$\phi_2'^{\,4} - (35x + 454)W^4 t_1^6, \qquad \phi_2'^{\,4} + (35x + 454)W^4 t_1^6.$$

4.6. **Newton polygons and Henselization (proof of Theorem 4.10).** There is an addition law for Newton polygons. Consider two polygons N, N' with sides $S_1, \dots, S_r$, $S_1', \dots, S_s'$, 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', whereas the sides of $N + N'$ are obtained by joining to this endpoint all sides in the multiset $\{S_1, \dots, S_r, S_1', \dots, S_s'\}$, ordered by increasing slopes.

Theorem 4.15. [30, Thm. 4.1] *For all $\phi \in \mathrm{KP}(\mu)$ and nonzero $g, h \in K[x]$, we have*

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

This follows mainly from the fact that the sum of Newton polygons is simply the lower convex hull of the Minkowski sum.

4.6.1. *Newton polygons with respect to Henselian valuations.* We assume in this section that the valued field (K, v) is Henselian. The following result is crucial for our purpose.

Theorem 4.16. [30, Thm. 4.4] *For a Henselian (K, v), let $Q \in \mathrm{KP}(\nu)$ for some extension ν of v to $K[x]$. Then, for all $F \in \mathrm{Irr}(K)$ we have*

$$Q \mid_\nu F \iff \nu < v_F \ \text{ and } \ \mathbf{t}(\nu, v_F) = [Q]_\nu.$$

Moreover, if these conditions hold, then:

(i) *Either $F = Q$, or the Newton polygon $N_{\nu,Q}(F)$ is one-sided of slope $-v_F(Q)$.*
(ii) *$F \sim_\nu Q^\ell$ with $\ell = \ell(N_{\nu,Q}(F)) = \deg(F)/\deg(Q)$.*

Let us rewrite Theorem 4.10 in the Henselian case and show that it follows easily from Theorem 4.16.

Theorem 4.17. *For a Henselian (K, v), let ν be an extension of v to $K[x]$, $Q \in \mathrm{KP}(\nu)$, $g \in K[x]$ monic and $N = N^+_{\nu,Q}(g)$. Then,*

(i) *For all $G \in \mathcal{F}_{\nu,Q}(g)$, $\deg(G)$ is a multiple of $\deg(Q)$.*
(ii) *For all $\epsilon \in \Gamma_{\mathbb{Q}}$, we have*

$$\sum\nolimits_{G \in \mathcal{F}_{\nu,Q}(g)(\epsilon)} \deg(G) = \ell\left(S_\epsilon(N)\right)\deg(Q).$$

Proof. Let $\mathcal{F}(g)$ be the multiset of irreducible factors of g. By Theorem 4.16,

$$\mathcal{F}_{\nu,Q}(g) = \{G \in \mathcal{F}(g) \mid \ \nu < v_G,\ \mathbf{t}(\nu, v_G) = [Q]_\nu\} = \{G \in \mathcal{F}(g) \mid \ Q \mid_\nu G\},$$

and all polynomials in this set have degree a multiple of $\deg(Q)$. This proves (i). Recall that

$$\mathcal{F}_{\nu,Q}(g)(\epsilon) = \{G \in \mathcal{F}_{\nu,Q}(g) \mid \ v_G(Q) = \epsilon\}$$

for all $\epsilon \in \Gamma_{\mathbb{Q}}$. We claim that $\ell\left(S_\epsilon(N^+_{\nu,Q}(G))\right) = 0$ for all $G \in \mathcal{F}(g)$ such that $G \notin \mathcal{F}_{\nu,Q}(g)(\epsilon)$. Indeed, if $G \notin \mathcal{F}_{\nu,Q}(g)$, then $Q \nmid_\nu G$ and Lemma 4.7 shows that $\ell\left(N^+_{\nu,Q}(G)\right) = 0$. If $G = Q$, then $N_{\nu,Q}(G) = \{(1, 0)\}$. Thus, $S_\epsilon(N^+_{\nu,Q}(G))$ has length zero too. If $G \in \mathcal{F}_{\nu,Q}(g)$ and $G \neq Q$, then Theorem 4.16 shows that $N_{\nu,Q}(G)$ is one-sided of slope $-v_G(Q)$. Thus, if $v_G(Q) \neq \epsilon$, then necessarily $\ell\left(S_\epsilon(N^+_{\nu,Q}(G))\right) = 0$. This ends the proof of our claim.

By Theorem 4.15,

$$\ell\left(S_\epsilon(N))\right) = \sum\nolimits_{G\in\mathcal{F}(g)} \ell\left(S_\epsilon(N^+_{\nu,Q}(G))\right) = \sum\nolimits_{G\in\mathcal{F}_{\nu,Q}(g)(\epsilon)} \ell\left(S_\epsilon(N^+_{\nu,Q}(G))\right).$$

Finally, for all $G \in \mathcal{F}_{\nu,Q}(g)(\epsilon)$, we have $\ell\left(S_\epsilon(N^+_{\nu,Q}(G))\right) = \deg(G)/\deg(Q)$, by Theorem 4.16. This ends the proof of (ii). □

4.6.2. *Newton polygons with respect to non-Henselian valuations.* Let us go back to our arbitrary valued field (K, v) and its Henselization (K^h, v^h).

Consider the unique extension μ^h of μ to $K^h[x]$ whose restriction to K^h is v^h (Theorem 1.1). The strategy to prove Theorem 4.10 is to deduce it from Theorem 4.17 after a suitable comparison of the sets $\mathcal{F}_{\mu,\phi}(g)$, $\mathcal{F}_{\mu,\phi}(g)(\lambda)$ with the analogous objects $\mathcal{F}_{\nu,Q}(g)$, $\mathcal{F}_{\nu,Q}(g)(\epsilon)$, with respect to $\nu = \mu^h$ and $Q = Q_{\mu,\phi}$. To this end, we need a relevant consequence of Theorem 3.6.

Proposition 4.18. [30, Prop. 5.6] *For $\phi \in \mathrm{KP}(\mu)$, let $Q \in \mathrm{Irr}(K^h)$ be the irreducible factor of ϕ determined by μ. Then, $Q \in \mathrm{KP}(\mu^h)$ and $\mathrm{in}_{\mu^h}(\phi/Q)$ is a unit in $\mathcal{G}_{\mu^h}$.*

With the above notation, from now on we denote

$$P := \phi/Q \in K^h[x], \qquad \alpha := \mu^h(P).$$

The first thing to observe is that the types (μ, ϕ) and (μ^h, Q) "point out" to the same irreducible factors of g in $K^h[x]$.

Lemma 4.19. $\mathcal{F}_{\mu,\phi}(g) = \mathcal{F}_{\mu^h,Q}(g)$.

Proof. By Theorem 1.1, for all $G \in \mathcal{F}(g)$, we have

$$\mu < w_G \iff \mu^h < (w_G)^h = v_G.$$

Thus, in order to prove the lemma, we need only to check that

$$\mathbf{t}(\mu, w_G) = [\phi]_\mu \iff \mathbf{t}(\mu^h, v_G) = [Q]_{\mu^h}.$$

By Corollary 2.19, this is equivalent to:

$$\mu(\phi) < w_G(\phi) \iff \mu^h(Q) < v_G(Q). \tag{4.3}$$

By Proposition 4.18, $\mathrm{in}_{\mu^h} P$ is a unit in $\mathcal{G}_{\mu^h}$. Hence, $Q \nmid_{\mu^h} P$. Since $\mathbf{t}(\mu^h, v_G) = [Q]_{\mu^h}$, this implies $\mu^h(P) = v_G(P)$ by Lemma 2.8. Hence,

$$\mu^h(\phi) - \mu^h(Q) = \mu^h(P) = v_G(P) = v_G(\phi) - v_G(Q). \tag{4.4}$$

Since, $\mu^h(\phi) = \mu(\phi)$ and $v_G(\phi) = w_G(\phi)$, this proves (4.3). □

Corollary 4.20. *Item (i) of Theorem 4.10 follows from item (i) of Theorem 4.17.*

Corollary 4.21. *For all $\lambda \in \Gamma_{\mathbb{Q}}$, $\mathcal{F}_{\mu,\phi}(g)(\lambda) = \mathcal{F}_{\mu^h,Q}(g)(\lambda - \alpha)$.*

Proof. By Lemma 4.19, we may rewrite these subsets as:

$$\mathcal{F}_{\mu,\phi}(g)(\lambda) = \{G \in \mathcal{F}_{\mu,\phi}(g) \mid w_G(\phi) = \lambda\},$$
$$\mathcal{F}_{\mu^h,Q}(g)(\lambda - \alpha) = \{G \in \mathcal{F}_{\mu,\phi}(g) \mid v_G(Q) = \lambda - \alpha\}.$$

These sets coincide by (4.4). □

In order to finish the proof of Theorem 4.10, we must compare the Newton polygons $N^+_{\mu,\phi}(g)$ and $N^+_{\mu^h,Q}(g)$. Instead of comparing these polygons directly, we compare each one with an auxiliary polygon. Consider the canonical ϕ-expansion of g:

$$g = \sum\nolimits_{n\geq 0} a_n \phi^n, \quad a_n \in K[x], \quad \deg(a_n) < \deg(\phi).$$

We may deduce a trivial Q-expansion of g in $K^h[x]$:

$$g = \sum\nolimits_{n\geq 0} b_n Q^n, \quad b_n = a_n P^n.$$

This Q-expansion is far from being the canonical one, but it leads to a Newton polygon which is easily comparable with $N_{\mu,\phi}(g)$.

Notation. Let us denote by $\mathcal{N}(g)$ the convex hull of the cloud of points

$$\{(n, \mu^h(b_n)) \mid n \geq 0\}.$$

Let $\mathcal{N}^+(g)$ be the polygon formed by the sides of $\mathcal{N}(g)$ of slope smaller than $-\nu(Q)$.

Lemma 4.22. *The linear automorphism*

$$\mathbb{Q} \times \Gamma_{\mathbb{Q}} \longrightarrow \mathbb{Q} \times \Gamma_{\mathbb{Q}}, \qquad (x, y) \longmapsto (x, y + \alpha x)$$

maps $N_{\mu,\phi}(g)$ to $\mathcal{N}(g)$. Moreover, it maps $S_\lambda(N_{\mu,\phi}(g))$ to $S_{\lambda-\alpha}(\mathcal{N}(g))$ and it preserves the lengths of these components. In particular, it maps $N^+_{\mu,\phi}(g)$ to $\mathcal{N}^+(g)$.

Proof. Since $\mu^h(b_n) = \mu(a_n) + n\alpha$, this linear automorphism maps:

$$\{(n, \mu(a_n)) \mid n \geq 0\} \longmapsto \left\{(n, \mu^h(b_n)) \mid n \geq 0\right\}.$$

Since linear mappings preserve convex subsets, $N_{\mu,\phi}(g)$ is mapped to $\mathcal{N}(g)$. The points lying on $S_\lambda(N_{\mu,\phi}(g))$ correspond to monomials $a_n\phi^n$ satisfying:

$$\mu(a_n) + n\lambda \leq \mu(a_m) + m\lambda \quad \text{for all } m \geq 0.$$

This is equivalent to

$$\mu^h(b_n) + n(\lambda - \alpha) \leq \mu^h(b_m) + m(\lambda - \alpha) \quad \text{for all } m \geq 0.$$

Thus, the linear automorphism maps $S_\lambda(N_{\mu,\phi}(g))$ to $S_{\lambda-\alpha}(\mathcal{N}(g))$, and it preserves the lengths of these segments. □

Therefore, the proof of Theorem 4.10 follows immediately from Theorem 4.17, once we prove the next result.

Lemma 4.23. $\mathcal{N}^+(g) = N^+_{\mu^h,Q}(g)$.

Proof. It suffices to show that $S_\epsilon(\mathcal{N}^+(g)) = S_\epsilon\left(N^+_{\mu^h,Q}(g)\right)$, for all $\epsilon \in \Gamma_{\mathbb{Q}}$ such that $\epsilon > \mu^h(Q)$. Consider the augmented valuation $\nu_\epsilon = [\mu^h; Q, \epsilon]$. Recall that Q becomes a key polynomial of minimal degree for ν_ϵ. The monomials b_nQ^n such that $\nu_\epsilon(b_nQ^n) = \nu_\epsilon(g)$ correspond to points lying on $S_\epsilon(\mathcal{N}^+(g))$. Imagine that these monomials are:

$$b_sQ^s + \cdots + b_tQ^t.$$

Then, if we denote for simplicity $\overline{b}_n = \mathrm{in}_{\nu_\epsilon} b_n$ and $\pi = \mathrm{in}_{\nu_\epsilon} Q$, we have:

$$\mathrm{in}_{\nu_\epsilon}(g) = \overline{b}_s\pi^s + \cdots + \overline{b}_t\pi^t \in \mathcal{G}^0_{\nu_\epsilon}[\pi] = \mathcal{G}_{\nu_\epsilon}.$$

Indeed, by Proposition 4.18, $\mathrm{in}_{\mu^h} b_n = \mathrm{in}_{\mu^h}(a_nP^n)$ is a unit in $\mathcal{G}_{\mu^h}$ for all n. Hence, $Q \nmid_{\mu^h} b_n$, so that $\nu_\epsilon(b_n) = \mu^h(b_n)$. Hence, the homomorphism $\mathcal{G}_{\mu^h} \to \mathcal{G}_{\nu_\epsilon}$ maps $\mathrm{in}_{\mu^h} b_n$ to $\overline{b}_n$, and the latter is a unit in $\mathcal{G}_{\nu_\epsilon}$.

Now, let $g = \sum_{n\geq 0} c_nQ^n$ be the canonical Q-expansion of g. We can argue as above. The monomials c_nQ^n such that $\nu_\epsilon(c_nQ^n) = \nu_\epsilon(g)$ correspond to points lying on $S_\epsilon\left(N^+_{\mu^h,Q}(g)\right)$. If these monomials are $c_kQ^k + \cdots + c_\ell Q^\ell$, we deduce as above:

$$\mathrm{in}_{\nu_\epsilon}(g) = \overline{c}_k\pi^k + \cdots + \overline{c}_\ell\pi^\ell \in \mathcal{G}^0_{\nu_\epsilon}[\pi] = \mathcal{G}_{\nu_\epsilon}.$$

By Theorem 2.5, we deduce that

$$s = k, \quad t = \ell, \quad \overline{b}_n = \overline{c}_n$$

for all $s \leq n \leq t$ such that $\nu_\epsilon(b_nQ^n) = \nu_\epsilon(g)$, which must be the same indices for which $\nu_\epsilon(c_nQ^n) = \nu_\epsilon(g)$. This proves the lemma. □

5. The OM-algorithm

5.1. **A formal OM-algorithm.** Results of Section 4 lead to the following algorithm, where NP stands for the Newton polygon routine described in Section 4.4. Executability of the involved subroutines is elaborated upon in Section 5.4.

Algorithm 1: OM-algorithm

Input : $g \in \mathrm{Irr}(K)$, v a valuation on K
Output: A list of types singling out the irreducible factors of g in $K^h[x]$

```
Stack ← [(v, x, deg(g))]; Types ← [ ];
while #Stack > 0 do
    pick any (μ, φ, ℓ) ∈ Stack and delete it from Stack;
    for −λ slope of NP(μ, φ, ℓ)(g) do
        μ_λ ← [μ; φ, λ];
        compute and factorize R_{μ_λ,φ}(g) = ψ_1^{n_1} ··· ψ_s^{n_s} in κ(μ_λ)[y];
        for 1 ≤ i ≤ s do
            φ ← lift_{μ_λ,φ}(ψ_i);
            if deg(φ) > deg(φ) then
                μ ← μ_λ
            if n_i = 1 then
                append (μ_λ, φ) to Types
            else
                append (μ, φ, n_i) to Stack
return Types
```

Theorem 5.1. *If the OM-algorithm terminates then it provides:*

- *An approximant in $K[x]$ to each irreducible factor of g in $K^h[x]$.*
- *All extensions of v to the field $L = K[x]/(g)$, plus a computation of their ramification indices and residual degrees.*

Proof. Assuming termination, each irreducible factor $G \in K^h[x]$ of g is singled out by some output type (μ, ϕ) thanks to Corollary 4.11, Proposition 4.12 and Proposition 4.14. We thus have

$$\mathcal{F}_{\mu,\phi}(g) = \{G\}\,, \quad \mathbf{t}(\mu, w_G) = [\phi]_\mu, \quad \deg(G) = \deg(Q_{\mu,\phi}).$$

Each augmented valuation being ordinary, μ is inductive and Lemma 3.7 shows that $\phi \in \mathrm{KP}(\mu) \subset \mathrm{KP}(\mu^h)$ is irreducible over $K^h[x]$. Thus, $\phi = Q_{\mu,\phi}$ and ϕ is an approximant of G (Definition 4.13). The second point follows from Theorem 5.2 below. □

5.2. **Extensions of v to the field $L = K[x]/(g)$.** Let (μ, ϕ) be an output type. By storing all pairs (μ_n, ϕ_{n+1}) and slopes γ_{n+1} considered along the procedure, we get a MLV chain of ordinary augmentations:

$$v \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \longrightarrow \mu_{r-1} \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu \tag{5.1}$$

satisfying moreover $\deg(\phi_r) < \deg(\phi)$.

Theorem 5.2. *Let $G \in \mathrm{Irr}(K^h[x])$ be the irreducible factor of g singled out by (μ, ϕ). Then,*

$$e(\overline{w}_G/v) = e_0 \cdots e_r, \qquad f(\overline{w}_G/v) = f_0 \cdots f_{r-1} \deg(R_{\mu,\phi_r}(\phi)),$$

where, e_i, f_j are the numerical data of the MLV chain of μ.

Proof. By Lemma 3.7, $\phi \in \mathrm{KP}(\mu^h)$. Since $\mathbf{t}(\mu, w_G) = [\phi]_\mu$, we have

$$\mu^h(\phi) = \mu(\phi) < w_G(\phi) = v_G(\phi).$$

Hence, $\mathbf{t}(\mu^h, v_G) = [\phi]_{\mu^h}$, by Corollary 2.19. Now, since $\mu^h(G) < v_G(G) = \infty$, we deduce that $\phi \mid_{\mu^h} G$. Since $\deg(G) = \deg(\phi)$, this implies that G is a key polynomial for μ^h and $G \sim_{\mu^h} \phi$ [27, Lem 2.5].

Therefore, it makes sense to consider the ordinary augmentation $[\mu^h; G, \infty]$. Since this valuation has support $GK^h[x]$, we have $[\mu^h; G, \infty] = v_G$, by Proposition 1.2. By Lemma 3.7, we obtain the following MLV chain of v_G:

$$v^h \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0^h \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r^h = \mu^h \overset{G,\infty}{\longrightarrow} v_G,$$

whose numerical data $e_0, \dots, e_r$; $f_0, \dots, f_{r-1}$ coincide with those determined by the MLV chain (5.1) of μ. By Proposition 3.3,

$$e(\bar{v}_G/v^h) = e_0 \cdots e_r, \qquad f(\bar{v}_G/v^h) = f_0 \cdots f_{r-1} \deg(R_{\mu^h,\phi_r}(G)).$$

Since $G \sim_{\mu^h} \phi$, [27, Cor. 5.5] shows that $R_{\mu^h,\phi_r}(G) = R_{\mu^h,\phi_r}(\phi)$. Also, let $u \in \mathcal{G}_\mu$ be a homogeneous unit such that $\mathrm{gr}_\mu(u) = \mu(\phi_r^{e_r})$. Let $u^h \in \mathcal{G}_{\mu^h}$ be the image of u under the isomorphism $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_{\mu^h}$. Then, it is easy to check that the following diagram commutes

$$\begin{array}{ccc} K[x] & \subset & K^h[x] \\ {\scriptstyle R_{\mu,\phi,u}}\downarrow & & \downarrow{\scriptstyle R_{\mu^h,\phi,u^h}} \\ \kappa(\mu)[y] & \hookrightarrow & \kappa(\mu^h)[y] \end{array}$$

where the lower horizontal map is the isomorphism induced by $\mathcal{G}_\mu \hookrightarrow \mathcal{G}_{\mu^h}$. We deduce that $\deg\left(R_{\mu^h,\phi_r}(\phi)\right) = \deg\left(R_{\mu,\phi_r}(\phi)\right)$. Therefore, the theorem will be proved if we check that

$$e(\overline{w}_G/v) = e(\bar{v}_G/v^h), \qquad f(\overline{w}_G/v) = f(\bar{v}_G/v^h). \tag{5.2}$$

Now, the extension $L^h = L \cdot K^h = K^h[x]/(G)$ is a Henselization of $(L, \overline{w}_G)$. Hence, the commutative diagram of extensions of valuations:

$$\begin{array}{ccc} (K^h, v^h) & \longrightarrow & (L^h, \bar{v}_G) \\ \uparrow & & \uparrow \\ (K, v) & \longrightarrow & (L, \overline{w}_G) \end{array}$$

implies (5.2), because $e(v^h/v) = 1 = f(v^h/v)$ and $e(\bar{v}_G/\overline{w}_G) = 1 = f(\bar{v}_G/\overline{w}_G)$. □

5.3. **Towards better approximants of the irreducible factors.** We may consider the whole class $[\phi]_\mu \subset \mathrm{KP}(\mu)$ as a set of approximants to G provided by the OM-algorithm. The measure of the quality of any $Q \in [\phi]_\mu$ as an approximant to G is indicated by the value $w_G(Q - G) = w_G(Q)$.

If v has rank one, then K is dense in K^h and the set $w_G\left([\phi]_\mu\right)$ is unbounded in $\Gamma_\mathbb{Q}$. In this case, there are approximants with arbitrarily large precision. For larger rank, this is unfortunately not always possible as shown by the following example, for which this set is bounded.

Example 5.3. *Take a prime number $p \equiv 1 \pmod 4$ and let ord_p be the p-adic valuation. Denote by $\bar{a}$ the reduction modulo p of an integer $a \in \mathbb{Z}$. Choose a p-adic root $i \in \mathbb{Z}_p$ of the polynomial $g = x^2 + 1$:*

$$i = i_0 + i_1 p^{\ell_1} + \cdots + i_n p^{\ell_n} + \cdots,$$

with $0 < i_n < p$ for all n. Denote the truncations of i by

$$a_n := i_0 + i_1 p^{\ell_1} + \cdots + i_{n-1} p^{\ell_{n-1}} \in \mathbb{Z}.$$

Consider the field $K = \mathbb{Q}(t)$ equipped with the ord_t valuation. Every $u \in K^*$ has an initial coefficient $\mathrm{in}(u) = \left(u\, t^{-\mathrm{ord}_t(u)}\right)(0) \in \mathbb{Q}^*$, with respect to ord_t. Consider the following discrete rank-two valuation on K:

$$v\colon K^* \longrightarrow \mathbb{Z}^2_{\mathrm{lex}}, \qquad v(u) := \left(\mathrm{ord}_t(u), \mathrm{ord}_p(\mathrm{in}(u))\right),$$

with values in $\mathbb{Z}^2$ equipped with the lexicographical order. The residue field is $k = \mathbb{F}_p$.

The OM-algorithm applied to the polynomial $g = x^2 + 1$ terminates after a single double-dissection. Indeed, the Newton polygon $N_{v,x}(g)$ is one-sided of slope $(0, 0)$ and for $\mu_0 = [v; x, (0, 0)]$, we have $R_{\mu_0,x}(g) = y^2 + 1 = (y - \bar{i}_0)(y + \bar{i}_0)$. Hence, the algorithm detects the irreducible factors $x - i$, $x + i \in$

$K^h[x]$, singled out by the output types $(\mu_0, x - i_0)$, $(\mu_0, x + i_0)$, respectively. However, the quality of the approximants is bounded:

$$w_G\left([x - i_0]_{\mu_0}\right) = \{\bar{v}(a_n - i) \mid n \geq 0\} \subset \{0\} \times \mathbb{Z}.$$

The MLV chains of w_{x-i} and w_{x+i} require here a limit augmentation*, namely*

$$v \overset{x,(0,0)}{\longrightarrow} \mu_0 \longrightarrow w_{x-i} = [\mathcal{C},\, g, \infty], \qquad v \overset{x,(0,0)}{\longrightarrow} \mu_0 \longrightarrow w_{x+i} = [\mathcal{C}',\, g, \infty],$$

where $\mathcal{C} = ([v;\, x - a_n, (0, \ell_n)])_{n\geq 0}$ and $\mathcal{C}' = ([v;\, x + a_n, (0, \ell_n)])_{n\geq 0}$.

In general, the enlargement of the chain (5.1) into a MLV chain of w_G is not easy to describe. It may be necessary to consider several limit augmentations [30, Ex. 8.6].

5.4. **Executability of the OM-algorithm.**

Proposition 5.4. *Suppose that v has a finite rational rank ($\dim_{\mathbb{Q}}(\Gamma_{\mathbb{Q}}) < \infty$) and we have algorithms performing the following tasks.*

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

Then, there are algorithms performing all subroutines of the formal OM-algorithm.

Proof. Indeed, we use only three subroutines:

$$\mathrm{NP}(\mu, \phi, \ell)(-), \qquad R_{\mu_\lambda,\phi}(-), \qquad \mathrm{lift}_{\mu_\lambda,\phi}(-).$$

The subroutine $\mathrm{NP}(\mu, \phi, \ell)(-)$, described in Section 4.4, requires only:

(i) A quotient-with-remainder routine in $K[x]$ to compute truncated ϕ-expansions.

(ii) A routine to compute μ.

By Lemma 4.8, the computation of $\mu(a)$ for any $a \in K[x]$ follows easily from the computation of the Newton polygon

$$\mathrm{NP}\left(\mu_{r-1}, \phi_{r-1}, \lfloor \deg(a)/\deg(\phi_{r-1}) \rfloor\right)(a).$$

Thus, a recursive descending procedure along the MLV chain (5.1), enables the computation of μ, based in the end on the routine computing the valuation v.

The routines $R_{\mu_\lambda,\phi}(-)$ and $\mathrm{lift}_{\mu_\lambda,\phi}(-)$ can be obtained by a similar descending recursive procedure, described in [26, Sec. 5]. □

5.5. **Refinement steps and termination of the OM-algorithm.** The only obstacle for the termination of the OM-algorithm would be the existence of an infinite sequence of double-dissections (double **for** loops).

Since $\mathcal{F}(g)$ is a finite set, it admits only a finite number of non-trivial dissections of any of its subsets. Also, since $\deg(\phi) \leq \deg(g)$ for all key polynomials ϕ constructed along the process, the condition $\deg(\phi) < \deg(\varphi)$ inside the second **for** loop may occur only a finite number of times. Thus, the OM-algorithm does not terminate if and only if there is an infinite sequence of *refinement steps*, defined as follows.

Definition 5.5. *A refinement step for a type (μ, ϕ, ℓ) is a step of the **while** loop which yields a unique new type $(\mu_\lambda, \varphi, n)$, with moreover $\deg(\varphi) = \deg(\phi)$.*

By Theorem 2.18, $\deg(\varphi) = e_{\mathrm{rel}}(\mu_\lambda)\deg(\psi)\deg(\phi)$. Hence, a refinement step is characterized by the following two conditions:

- $N^+_{\mu,\phi}(g)$ is one-sided and its slope $-\lambda$ satisfies $e_{\mathrm{rel}}(\mu_\lambda) = 1$.
- $R_{\mu_\lambda,\phi}(g) = (y - \zeta)^\ell$, for some $\zeta \in \kappa(\mu_\lambda)^*$.

In this case, we just replace (μ, ϕ, ℓ) with (μ, φ, ℓ) in the *Stack*, where φ is the lift of $y - \zeta$.

Montes proved that infinite sequences of refinement steps cannot occur in the discrete rank-one case [24].

Theorem 5.6. *If v is discrete of rank-one, then the OM-algorithm terminates.*

Let us write $L = K(\theta)$, where $\theta \in L$ is the class of x modulo the ideal $gK[x]$. The proof of this theorem is based on the finiteness of the local index

$$\operatorname{ind}(g) := v\left((\mathcal{O}_g \colon \mathcal{O}_v[\theta])\right) \in \Gamma,$$

where $\mathcal{O}_g$ is the integral closure of $\mathcal{O}_v$ in the finite extension L/K. Through an ordered isomorphism between Γ and $\mathbb{Z}$, this index is identified with a non-negative integer. The theorem follows from the fact that in all intermediate steps of the algorithm, including the refinement steps, there is a positive integer contributing to the total value of $\operatorname{ind}(g)$ [14, Thm. 4.8].

If v is not discrete of rank one, we can identify three kinds of infinite refinements steps. As we saw in Section 5.1, the OM-algorithm aims to construct an MLV chain

$$v \overset{\phi_0,\gamma_0}{\longrightarrow} \mu_0 \overset{\phi_1,\gamma_1}{\longrightarrow} \cdots \overset{\phi_r,\gamma_r}{\longrightarrow} \mu_r = \mu$$

of a valuation μ which is sufficiently close to the valuation w_G, for some irreducible factor G of g in $K^h[x]$. Denote $m_n := \deg(\mu_n) = \deg(\phi_n)$ for all $0 \le n \le r$. For a field $K \subset \mathbb{K} \subset K^h$, let

$$V_{m_n}(\mathbb{K}) := \{w_G(f) \mid f \in \mathbb{K}[x] \text{ monic, } \deg(f) = m_n\} \subset \Gamma_{\mathbb{Q}}.$$

For each $n > 0$, the analysis of the augmentation step $\mu_{n-1} \to \mu_n$ leads to three different infinite refinement situations:

(IR1) There exists $\max\left(V_{m_n}(K)\right)$,
(IR2) $\max\left(V_{m_n}(K)\right)$ does not exist, but there exists $\max\left(V_{m_n}(K^h)\right)$,
(IR3) $\max\left(V_{m_n}(K^h)\right)$ does not exist,

By [28, Thm. 4.7], the augmentation $\mu_{n-1} \to \mu_n$ is ordinary in the case (IR1) and a limit augmentation in cases (IR2) and (IR3).

Vaquié showed that limit augmentations in the Henselian case occur only when G has defect [45], [28, Sec. 6]. Thus, we say that $\mu_{n-1} \to \mu_n$ is a *defectless* limit augmentation in the (IR2) case, and a *defect* limit augmentation in the (IR3) case. Defect limit augmentations occur only when $\operatorname{char}(k) = p > 0$; also, $\deg(\mu_n)/\deg(\mu_{n-1})$ is necessarily a power of p.

Let us detail some examples of each type of infinite refinement steps.

Example 5.7 ((IR2) case)**.** *Let $(K, v) = (\mathbb{Q}(t), \operatorname{ord}_t)$ be the valued field considered in Example 5.3. Let us apply the OM-algorithm to the polynomial*

$$g := x^4 + (t+2)x^2 + 1 \in K[x].$$

The double-dissection applied to the triple $(v, x, 4)$ yields a one-sided Newton polygon of slope $(0, 0)$. For $\mu_0 = [v, x, (0, 0)]$, the residual polynomial factorizes

$$R_{\mu_0,x}(g) = 1 + 2y^2 + y^4 = (y^2+1)^2 = (y - \bar{a}_1)^2(y + \bar{a}_1)^2 \in k[y].$$

As lifts of the irreducible factors we may take $x - a_1$, $x + a_1$, respectively. We get $\mathrm{Stack} = [(v, x - a_1, 2), (v, x + a_1, 2)]$. By Theorem 4.10, we detect a splitting of g into a product of two (unknown) polynomials in $K^h[x]$ of degree two.

The application of the double-dissection to the triple $(v, x - a_1, 2)$ leads to an infinite sequence of refinements:

$$(v, x - a_1, 2) \rightsquigarrow (v, x - a_2, 2) \rightsquigarrow \cdots \rightsquigarrow (v, x - a_n, 2) \rightsquigarrow \cdots \tag{5.3}$$

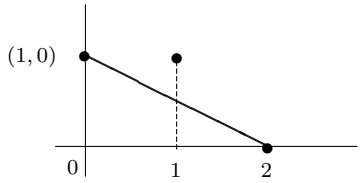
and a similar situation occurs for the triple $(v, x + a_1, 2)$. Indeed, the truncated $(x - a_n)$-expansion of g is $b_0 + b_1(x - a_n) + b_2(x - a_n)^2$, with

$$b_0 := g(a_n) = c_n^2 + ta_n^2, \quad b_1 := g'(a_n) = 4a_nc_n + 2ta_n, \quad b_2 := \frac{1}{2}\,g''(a_n) = 6c_n + t - 4,$$

where $c_n := a_n^2 + 1$. One checks easily that $\lambda_n := v(c_n) = (0, \ell_n)$ and $\overline{c_n/p^{\ell_n}} = -2\,\overline{i_0 i_n}$.

Hence, $N^+_{v,x-a_n}(g)$ is one-sided of slope $-\lambda_n$ and contains the three points $(0, 2\lambda_n)$, $(1, \lambda_n)$, $(2, (0, 0))$. Denote $\rho_n := [v, x - a_n, \lambda_n]$. We may identify $\kappa(\rho_n) = k$ and take $u_n := \operatorname{in}_{\rho_n}(p^{\ell_n})$ as a unit of grade λ_n. We get $R_{\rho_n,x-a_n}(g) = (y - \bar{i}_n)^2$ and a natural lift of $y - \bar{i}_n$ is $(x - a_n) - i_n p^{\ell_n} = x - a_{n+1} \in \mathrm{KP}(\rho_n)$.

FIGURE 6. Newton polygon $N_{\mathcal{C},x^2+1}(g)$ (or $N^+_{\mu_0,x-i}(g)$).



The totally ordered family of valuations $\mathcal{C} = (\rho_n)_n \geq 0$ is an essential continuous family of augmentations of $\rho_0 = \mu_0$. It can be easily shown that all polynomials of degree one are $\mathcal{C}$-stable, but $\phi := x^2 + 1$ is $\mathcal{C}$-unstable; indeed, for all n we have

$$\phi = (x - a_n)^2 + 2a_n(x - a_n) + c_n \implies \rho_n(\phi) = \min\{2\lambda_n, \lambda_n, \lambda_n\} = \lambda_n.$$

Thus, ϕ is a limit key polynomial for $\mathcal{C}$ and the right triple to append to the Stack *would be $(\mathcal{C}, \phi, 2)$.*

The double-dissection loop can be applied to this triple, to continue the OM-algorithm. The truncated ϕ-expansion of degree two is the whole ϕ-expansion:

$$g = -t + t\phi + \phi^2.$$

The Newton polygon, displayed in Figure 6, is one-sided of slope $-\lambda = -(1, 0)/2$. The limit augmentation $\mu = [\mathcal{C}; \phi, \lambda]$ has $e_{\rm rel}(\mu) = 2$. We may still identify $\kappa(\mu) = k$ and take $u = \mathrm{in}_\mu\, t$ as a unit of grade 2λ. We get $R_{\mu,\phi}(g) = y - 1$. Thus, g is a lift of $y - 1$ and the algorithm appends the type (μ, g) to the output list Types.

We may proceed in a analogous way with the triple $(\mathcal{C}', \phi, \lambda)$, where $\mathcal{C}' = (\rho'_n)_{n\geq 0}$ is the essential continuous family of the valuations $\rho'_n = [v, x + a_n, \lambda_n]$.

The OM-algorithm would output two types (μ, g), (μ', g) which single out two irreducible factors G, G' of degree two of g in $K^h[x]$, with MLV chains:

$$v \overset{x,(0,0)}{\longrightarrow} \mu_0 \overset{\phi,\lambda}{\longrightarrow} \mu \overset{g,\infty}{\longrightarrow} w_G, \qquad v \overset{x,(0,0)}{\longrightarrow} \mu_0 \overset{\phi,\lambda}{\longrightarrow} \mu' \overset{g,\infty}{\longrightarrow} w_{G'},$$

where $\mu_0 \to \mu$, $\mu_0 \to \mu'$ are limit augmentations and $\mu \to w_G$, $\mu' \to w_{G'}$ are ordinary augmentations. Since μ and μ' are not inductive, we do not get approximants to the irreducible factors G, G'. However, we know the ramification indices and residual degrees of their associated valuations. Indeed, by Proposition 3.3,

$$e(\overline{w}_G/v) = e(\overline{w}_{G'}/v) = 2, \qquad f(\overline{w}_G/v) = f(\overline{w}_{G'}/v) = 1 \tag{5.4}$$

Example 5.8 ((IR1) case)**.** *Take p, i as in the preceding example and consider the base field $K = \mathbb{Q}_p(t)$, equipped with the analogous discrete rank-two valuation*

$$v\colon K^* \longrightarrow \mathbb{Z}^2_{\rm lex}, \qquad v(u) := (\mathrm{ord}_t(u), \mathrm{ord}_p(\mathrm{in}(u)))\,.$$

Let us apply the OM-algorithm to the same polynomial $g = x^4 + (2 + t)x^2 + 1$.

The double-dissection applied to the triple $(v, x, 4)$ yields two triples $(v, x - a_1, 2)$, $(v, x + a_1, 2)$, each one leading to infinite sequences of refinements as in (5.3). However, imagine that our lifting routine chooses $\mathrm{lift}_{\mu_0,x}(y - \bar{a}_1) = x - i$ and $\mathrm{lift}_{\mu_0,x}(y + \bar{a}_1) = x + i$.

Then, the double-dissection applied to the triple $(v, x - i, 2)$ is no more a refinement step. The truncated $(x - i)$-expansion of g is $b_0 + b_1(x - i) + b_2(x - i)^2$, with

$$b_0 := g(i) = -t, \quad b_1 := g'(i) = 2ti, \quad b_2 := g''(i)/2 = t - 4.$$

Thus, $N^+_{\mu_0,x-i}(g)$ is the polygon displayed in Figure 6. It is one-sided of slope $-\lambda = -(1, 0)/2$. The ordinary augmentation $\mu := [\mu_0; x - i, \lambda]$ has $e_{\rm rel}(\mu) = 2$. We may still identify $\kappa(\mu) = k$ and take $u := \mathrm{in}_\mu\, t$ as a unit of grade 2λ. We get

$$\mathrm{in}_\mu\, g = \mathrm{in}_\mu(-t - 4(x - i)^2) = -4u\left(\frac{1}{4} + \frac{(x - i)^2}{u}\right),$$

so that $R_{\mu,x-i}(g) = y + (1/4)$, admitting $\phi = (x - i)^2 + (t/4)$ as a lift. The algorithm appends the type (μ, ϕ) to the output list Types.

We may proceed in a analogous way with the triple $(v, x+i, 2)$ to obtain the augmentation $\mu' = [\mu_0;\, x+i, \lambda]$ and a key polynomial $\phi' = (x+i)^2 + (t/4)$. The output of the OM-algorithm is a list of two types (μ, ϕ), (μ', ϕ') which single out two irreducible factors G, G' of degree two of g in $K^h[x]$.

The MLV chains of μ and μ' contain only ordinary augmentations:

$$v \overset{x,(0,0)}{\longrightarrow} \mu_0 \overset{x-i,\lambda}{\longrightarrow} \mu, \qquad v \overset{x,(0,0)}{\longrightarrow} \mu_0 \overset{x+i,\lambda}{\longrightarrow} \mu'$$

Hence, the key polynomials $\phi = (x-i)^2 + (t/4)$, $\phi = (x+i)^2 + (t/4)$ are approximants to the true factors G, G', respectively. We have

$$w_G(x-i) = \lambda = (1/2, 0) = \max\left(V_1(K)\right).$$

The ramification indices and residual degrees of their associated valuations are given by (5.4).

Example 5.9 ((IR3) case)**.** *Let $\mathbb{F}$ be an algebraic closure of the prime field $\mathbb{F}_p$, for some prime number p. For an indeterminate t, consider the fields of Newton-Puiseux series and Hahn series in t, respectively:*

$$K := \bigcup_{N\in\mathbb{N}} \mathbb{F}((t^{1/N})) \subset \mathbb{F}((t^{\mathbb{Q}}))_{\rm lex}.$$

The Hahn field $\mathbb{F}((t^{\mathbb{Q}}))_{\rm lex}$ consists of all power series with rational exponents and well-ordered support. As remarked by Abhyankar [1]*,*

$$s := \sum\nolimits_{n\geq 1} t^{-1/p^n} \in \mathbb{F}((t^{\mathbb{Q}}))_{\rm lex}$$

is a root of the Artin-Schreier irreducible polynomial $g = x^p - x - t^{-1} \in K[x]$. The truncations of s belong to K:

$$s_n = t^{-1/p} + \cdots + t^{-1/p^n} \in K, \quad n \geq 1.$$

Consider the valuation $v := \mathrm{ord}_p$ on K, with value group $\Gamma = \mathbb{Q}$ and residue field $k = \mathbb{F}$. The valued field (K, v) is Henselian.

Let us apply the OM-algorithm to test the irreducibility of g. The double-dissection applied to the triple (v, x, p) yields a one-sided Newton polygon of slope $1/p$. For $\mu_0 := [v, x, -1/p]$, and $u_0 := \mathrm{in}_{\mu_0}\, t^{-1/p}$ as a chosen unit of grade $-1/p$, the residual polynomial is $R_{\mu_0,x}(g) = (y-1)^p \in k[y]$. Take $x - s_1$ as a lift of $y - 1$. The iterative application of the double-dissection leads to an infinite sequence of refinements:

$$(v, x-s_1, p) \rightsquigarrow (v, x-s_2, p) \rightsquigarrow \quad \cdots \quad \rightsquigarrow (v, x-s_n, p) \rightsquigarrow \quad \cdots$$

Consider the essential continuous family $\mathcal{C} := (\rho_n)_{n\geq 0}$, where $\rho_n := [v;\ x - s_n, 1/p^{n+1}]$. All polygons $N_{v,x-s_n}(g)$ are one-sided of slope $1/p^{n+1}$ and $R_{\rho_n,x-s_n}(g) = (y-1)^p$, if we choose $u_n := \mathrm{in}_{\mu_n}\, t^{-1/p^{n+1}}$ as a unit of grade $-1/p^{n+1}$.

The polynomial g is a limit key polynomial, and $w_g = [\mathcal{C};\, g, \infty]$. The unique extension of v to $L = K[x]/(g)$ is the valuation $\bar{w}$ naturally induced by w_g. It has

$$e(\bar{w}/v) = f(\bar{w}/v) = 1, \qquad d(\bar{w}/v) = p,$$

where $d(\bar{w}/v)$ is the defect of the extension.

Summary. We developed an executable OM-algorithm over general valued fields, whose termination depends only of the non-existence of an infinite sequence of refinement steps.

• In order to overcome the existence of infinite sequence of refinements of type (IR1), the lifting routine $\mathrm{lift}_{\mu_{n-1},\phi_{n-1}}(-)$ should be clever enough to compute $\max(V_{m_n}(K))$ in a finite number of steps, for all n.

• In order to overcome the existence of an infinite sequence of refinements of types (IR2) or (IR3), the OM-algorithm should be modified in order to be able to detect limit augmentations and compute limit key polynomials.

In the next section, we will see that termination can be guaranteed in some new situations which go beyond the usual discrete rank-one case.

6. Irreducibility and Factorization : proof of Theorem 0.1 and Theorem 0.2

In this section, we extend the OM-based algorithms of Poteaux-Weimann [41] (irreducibility test and polynomial factorization) from the discrete rank-one case to the more general settings of Theorems 0.1 and 0.2 stated in the introduction.

A crucial feature of our algorithms is that, *under some restrictions on the residual characteristic*, we can show that :

• Infinite refinements of type (IR1) can be avoided by considering *approximate roots* as "optimal" key polynomials. This is the main point.

• Infinite refinements of type (IR3) do not occur as there are no defect limit augmentations.

• If g is irreducible, or if v has rank one, there are no infinite refinements of type (IR2) since defectless limit augmentations do not appear (this is independent of the residual characteristic).

We obtain in this way an irreducibility test for an arbitrary valued field (K, v) and a factorization algorithm for an arbitrary rank one valued field (possibly non discrete), under some restrictions on the residual characteristic.

In order to improve the approximations of the irreducible factors, we develop a valuated Hensel lifting, valid for any augmented valuation and any residual characteristic.

We illustrate our algorithms on Example 1.5 in Section 6.2.6.

6.1. Irreducibility test.

Let $g \in K[x]$ be a monic polynomial. Let n be a divisor of $\deg(g)$ such that $\mathrm{char}(K) \nmid n$.

Definition 6.1. *The* approximate root $Q = \sqrt[n]{g}$ *is a monic polynomial in* $K[x]$*, of degree* $\deg(g)/n$*, such that the canonical* Q*-expansion of* g*:*

$$g = Q^n + a_{n-1}Q^{n-1} + \cdots + a_1 Q + a_0, \quad \deg(a_i) < \deg(Q),$$

satisfies $a_{n-1} = 0$.

Approximate roots were introduced by Abhyankar and Moh in [3] as a tool to prove the embedding line theorem (see [38] for a survey). In [2], Abhyankar used approximate roots for an irreducibility test in $\mathbb{C}[[x]][y]$, then generalized in [40, 41] over a complete discrete valuation ring.

It is obvious that the approximate root is unique, if it exists. The existence follows from the following result, which gives moreover a concrete algorithm to compute it.

Lemma 6.2. [38, proof of Proposition 6.3] *Let* $g \in K[x]$ *be a monic polynomial. Let* n *be a divisor of* $\deg(g)$ *such that* $\mathrm{char}(K) \nmid n$*. Take any monic polynomial* $\phi \in K[x]$ *of degree* $\deg(g)/n$*, and consider the* ϕ*-expansion*

$$g = \phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0, \quad \deg(a_i) < \deg(\phi).$$

Take $\phi^* = \phi + (a_{n-1}/n)$ *and let* a^*_{n-1} *be the* $(n-1)$*-th coefficient of the* ϕ^**-expansion of* g*. Then, if* $a_{n-1} \neq 0$*, we have* $\deg(a^*_{n-1}) < \deg(a_{n-1})$.

The next result establishes a link between approximate roots and key polynomials.

Proposition 6.3. *Let* μ *be a valuation on* $K[x]$ *and* φ *a key polynomial for* μ*. Let* $g \in K[x]$ *be a monic polynomial such that* $\deg(\varphi) \mid \deg(g)$*,* $\mathrm{char}(k_\mu) \nmid \deg(g)$ *and moreover:*

(i) $N_{\mu,\varphi}(g)$ *is one-sided of slope* $-\lambda$.
(ii) *For* $\mu_\lambda = [\mu;\, \varphi, \lambda]$*, we have* $R_{\mu_\lambda,\varphi}(g) = \psi^n$*, for some* $\psi \in \mathrm{Irr}(\kappa(\mu_\lambda))$.

Then, the following holds:

(a) *The approximate root* $Q = \sqrt[n]{g}$ *is a key polynomial for* μ_λ *and* $R_{\mu_\lambda,\varphi}(Q) = \psi$.
(b) *If* $N_{\mu_\lambda,Q}(g)$ *is one-sided of slope* $-\lambda_*$ *and for* $\nu = [\mu_\lambda;\, Q, \lambda_*]$ *we have* $R_{\nu,Q}(g) = \psi_*^{n_*}$ *for some* $\psi_* \in \mathrm{Irr}(\kappa(\nu))$*, then* $n_* < n$.

Proof. By (i) and (ii), $\deg(g) = ef n \deg(\varphi)$, where $e = e_{\mathrm{rel}}(\mu_\lambda)$ and $f = \deg(\psi)$. Take any monic $\phi \in K[x]$ of degree $ef\deg(\varphi) = \deg(Q)$ such that $R_{\mu_\lambda,\varphi}(\phi) = \psi$. By Theorem 2.18, ϕ is a key polynomial for μ_λ. By Lemma 6.2, we may obtain Q from ϕ by a finite number of transformations of the form $\phi \mapsto \phi^* = \phi + (a_{n-1}/n)$, where a_{n-1} is the $(n-1)$-th coefficient of the ϕ-expansion of g. Hence, in order to prove (a), it suffices to show that $\phi^* \in \mathrm{KP}(\mu_\lambda)$ and $R_{\mu_\lambda,\varphi}(\phi^*) = \psi$.

By Lemma 4.7, the Newton polygon $N^+_{\mu_\lambda,\phi}(g)$ has length n. Since

$$n = \deg(g)/\deg(\phi) = \ell\left(N_{\mu_\lambda,\phi}(g)\right),$$

we deduce that $N_{\mu_\lambda,\phi}(g) = N^+_{\mu_\lambda,\phi}(g)$. Thus, all slopes $-\epsilon$ of $N_{\mu_\lambda,\phi}(g)$ satisfy $\epsilon > \mu_\lambda(\phi)$. Now, the point of abscissa $n-1$ lying on $N_{\mu_\lambda,\phi}(g)$ is $(n-1,\epsilon)$, where $-\epsilon$ is the largest slope of this polygon. Since the point $(n-1,\mu_\lambda(a_{n-1}))$ lies on or above the polygon, we have $\mu_\lambda(a_{n-1}) \geq \epsilon$. Since $\mathrm{char}(k_\mu) \nmid \deg(g)$, we have $\mu_\lambda(n) = 0$, so that

$$\mu_\lambda(a_{n-1}/n) = \mu_\lambda(a_{n-1}) \geq \epsilon > \mu_\lambda(\phi).$$

Thus, $\phi \sim_{\mu_\lambda} \phi^*$. Since $\deg(\phi) = \deg(\phi^*)$, we deduce that ϕ^* is a key polynomial for μ_λ and $R_{\mu_\lambda,\varphi}(\phi^*) = R_{\mu_\lambda,\varphi}(\phi) = \psi$ [27, Lem. 2.5, Cor. 5.5]. This proves (a).

Let $g = \sum_{i\geq 0} b_i Q^i$ be the Q-expansion of g. By the definition of the approximate root, $b_{n-1} = 0$. Under the hypotheses of (b), we have

$$n\deg(Q) = \deg(g) = e_* f_* n_* \deg(Q),$$

where $e_* = e_{\mathrm{rel}}(\nu)$ and $f_* = \deg(\psi_*)$. Hence, $n = e_* f_* n_*$ and the equality $n = n_*$ holds only when $e_* = f_* = 1$. This is incompatible with the assumptions in (b). Indeed, $e_* = f_* = 1$ implies that $R_{\nu,Q}(g) = (y+\zeta)^n$ for some $\zeta \in \kappa(\nu)^*$. Since $\mathrm{char}(\mu_\lambda) \nmid n$, the $(n-1)$-th coefficient of this polynomial is $n\zeta^{n-1} \neq 0$. By the definition of the residual coefficients (Section 2.3), the point $(n-1, b_{n-1})$ lies on the Newton polygon. This is a contradiction because $b_{n-1} = 0$. This proves (b). □

We obtain Algorithm 2 below as an irreducibility test for arbitrary valued fields (K, v).

Algorithm 2: Irreducibility Test

Input : (K, v) valued field, $g \in K[x]$ monic, square-free such that $\mathrm{char}(k) \nmid \deg(g)$
Output: True if g is irreducible over $K^h[x]$ and False otherwise

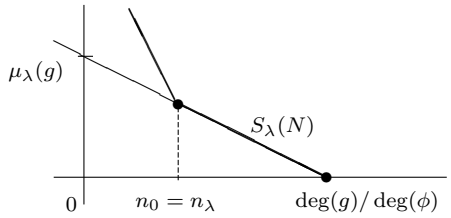
```
μ ← v;  φ ← x;  n ← deg(g) ;
while n > 1 do
    if N_{μ,φ}(g) is one-sided (of slope −λ) then
        μ ← [μ; φ, λ]
    else
        return False
    if R_{μ,φ}(g) = ψ^m for some ψ ∈ Irr(κ(μ)) then
        φ ← ᵐ√g
    else
        return False
    n ← m
return True
```

Proposition 6.4. *Algorithm 2 returns a correct answer and terminates in* $\log(\deg(g))$ *steps. If* g *is irreducible over* $K^h[x]$*, the algorithm computes as byproduct a MLV chain of the valuation* w_g *together with its residual degree and ramification index.*

Proof. The condition $\deg(\phi) \mid \deg(g)$ holds initially for $\phi = x$ and it is preserved along the execution of the algorithm as long as no factorization of g is detected.

Now, in the very first step, $N_{v,x}(g)$ could be one-sided of slope $-\lambda \in \Gamma$ and $R_{\mu,x}(g)$ be the n-th power of a polynomial of degree one. Thus, $e = f = 1$, with the notation of the proof of Proposition 6.3. However, as long as we do not detect a factorization of g over $K^h[x]$, Proposition 6.3 shows that in all further steps we will have $e_* f_* > 1$. Therefore, no refinement steps occur and the algorithm terminates in $\log(\deg(g))$ steps. As we did for the OM-algorithm, if g is irreducible over $K^h[x]$, then by storing all types (μ, ϕ) obtained along the process, we obtain a MLV chain of its associated valuation w_g. The last statement follows from Theorem 5.2. □

FIGURE 7. Right end-side of $N = N_{\mu,\phi}(g)$, defined by a splitting pair.



6.2. **Polynomial factorization.** Consider a monic, square-free $g \in K[x]$ such that $\mathrm{char}(k) \nmid \deg(g)$.

A *splitting pair* of g is any pair (μ, ϕ) considered in the last call of the **while** loop of Algorithm 2. Note that, either $(\mu, \phi) = (v, x)$, or (μ, ϕ) is a type. A splitting pair has the following properties.

Lemma 6.5. *Let $g \in K[x]$ be monic, square-free with splitting pair (μ, ϕ).*

(i) *If $(\mu, \phi) \neq (v, x)$, then $\mathcal{F}_{\mu,\phi}(g) = \mathcal{F}(g)$.*
(ii) *$N_{\mu,\phi}(g) = N^+_{\mu,\phi}(g)$ has length $\ell(N_{\mu,\phi}(g)) = \deg(g)/\deg(\phi)$.*
(iii) *ϕ is irreducible over $K^h[x]$.*

Proof. Items (i), (ii) follow immediately from the design of the Irreducibility test. Item (iii) follows from Lemma 3.7, because μ is an inductive valuation. □

6.2.1. *Right end-slope factorization.* Let $-\lambda$ be the *right end-slope* of $N = N_{\mu,\phi}(g)$. That is, the slopes $-\epsilon$ of N satisfy $-\epsilon \leq -\lambda$, or equivalently, $\epsilon \geq \lambda$. Let n_λ be the abscissa of the left end-point of $S_\lambda(N)$ (cf. Figure 7).

From now on, we assume g reducible in $K^h[x]$ and denote $\mu_\lambda = [\mu, \phi, \lambda]$. Although a splitting pair of g is not unique, the valuation μ_λ is intrinsically associated to g. Indeed, Figure 3 (where $\lambda = \lambda_t$) shows that μ_λ is the greatest common lower node of the finite set of leaves $\{w_G \mid G \in \mathcal{F}(g)\}$ in the tree $\mathcal{T}$. The existence of greatest common lower nodes in $\mathcal{T}$ is guaranteed by [4, Prop. 5.2].

By definition of a splitting pair, at least one of the following situations occurs:

- $N_{\mu,\phi}(g)$ is not one-sided.
- $R_{\mu_\lambda,\phi}(g)$ has at least two coprime factors.

The first point is equivalent to $n_\lambda > 0$. The second point is equivalent to

$$R_{\mu_\lambda,\phi}(g) = \psi_1^{n_1} \cdots \psi_s^{n_s}, \quad \psi_i \in \mathrm{Irr}(\kappa(\mu_\lambda)) \quad s \geq 2.$$

Let $\varphi_i := \mathrm{lift}_{\mu_\lambda,\phi}(\psi_i) \in \mathrm{KP}(\mu_\lambda)$ be monic lifts of ψ_i for $i = 1, \ldots, s$. We denote $n_0 := n_\lambda$ and $\varphi_0 := \phi$ for convenience. So, either $n_0 > 0$, or $s \geq 2$.

Lemma 6.6. *$g \sim_{\mu_\lambda} \prod_{i=0}^s \varphi_i^{n_i}$ and $\deg(g) = \sum_{i=0}^s \deg(\varphi_i^{n_i})$.*

Proof. By (2.5) in Section 2.3, we know that $\mathrm{in}_{\mu_\lambda} g \sim_{\mathrm{unit}} \mathrm{in}_{\mu_\lambda}(\prod_{i=0}^s \varphi_i^{n_i})$. By Lemma 6.5,(ii) and our choice of λ, we get $\mathrm{lc}_{\mu_\lambda}(g) = 1$. Since $\phi \in \mathrm{KP}(\mu_\lambda)$ has minimal degree and $\varphi_i \in \mathrm{KP}(\mu_\lambda)$, Theorem 2.18 implies that $\mathrm{lc}_{\mu_\lambda}(\varphi_i) = 1$ for all $i \geq 0$. By Theorem 2.5, $\mathrm{in}_{\mu_\lambda} g = \mathrm{in}_{\mu_\lambda}(\prod_{i=0}^s \varphi_i^{n_i})$ (which proves the first claim) and $\deg_{\mu_\lambda}(g) = \sum_{i=0}^s \deg_{\mu_\lambda}(\varphi_i^{n_i})$.

As mentioned after Definition 2.6, $\deg_{\mu_\lambda}(g) = \max(S_{\mu_\lambda,\phi}(g)) = \deg(g)/\deg(\phi)$. On the other hand, Theorem 2.18 shows that $\deg_{\mu_\lambda}(\varphi_i) = \deg(\varphi_i)/\deg(\phi)$ for all $0 \leq i \leq s$. This proves the second claim. □

Let μ^h_λ be the unique common extension of μ_λ and v^h to $K^h[x]$ (Theorem 1.1).

Proposition 6.7. *There exist unique monic $G_0, \ldots, G_s \in K^h[x]$ such that $g = \prod_{i=0}^s G_i$, $G_i \sim_{\mu^h_\lambda} \varphi_i^{n_i}$ and $\deg(G_i) = \deg(\varphi_i^{n_i})$ for all i. If $n_i = 1$, then G_i is irreducible.*

Proof. Since the augmentation $\mu \to \mu_\lambda$ is ordinary, the valuation μ_λ is inductive. Thus, $\varphi_0, \ldots, \varphi_s \in \mathrm{KP}(\mu^h_\lambda)$, by Lemma 3.7. For all $0 \leq i \leq s$, let G_i be the product of all irreducible factors G of g in $K^h[x]$ satisfying $\varphi_i \mid_{\mu^h_\lambda} G$. Then, the result follows from Lemma 6.6 and Theorem 4.16. □

6.2.2. *Hensel lifting.* The next result is a generalization of the multifactor Hensel lifting [10, Algorithm 15.17] to an arbitrary valuation. We keep the notation of the previous paragraph.

Proposition 6.8. *Let $\gamma = \mu_\lambda(g - \varphi_0^{n_0} \cdots \varphi_s^{n_s}) - \mu_\lambda(g)$. For all $n \in \mathbb{N}$ we can compute monic polynomials $G_0^{(n)}, \dots, G_s^{(n)} \in K[x]$ such that $\mu_\lambda^h(G_i - G_i^{(n)}) > \mu_\lambda^h(G_i) + 2^n\gamma$.*

Proof. Note that $\gamma > 0$ by Lemma 6.6. Such a valuated Hensel lifting is detailed in [41, Section 4.3] in the discrete rank-one case. Since $\varphi_i^{n_i}$ is strongly monic in ϕ with respect to μ_λ ([41, Definition 5]), then [41, Lemma 7] remains true in our context and [41, Algorithm `HenselStep`] extends straightforwardly to the valuation μ_λ. □

This Hensel-like algorithm has quadratic convergence in the sense that the precision is doubled at each Hensel step. We refer the reader to Subsection 6.2.6 for an illustrating example with more details. The following corollary is immediate.

Corollary 6.9. *If the sequence $(2^n\gamma)_{n\in\mathbb{N}}$ is unbounded, then the sequence $(G_i^{(n)})_{n\in\mathbb{N}}$ converges to G_i for all $0 \le i \le s$. In particular, this holds whenever v has rank one.*

If v has rank one, any choice of lifts φ_i will allow to approximate the G_i's with an arbitrary precision. If v has rank > 1, this is not always possible, as illustrated by Example 5.7.

6.2.3. *Gauss valuation and Okutsu bound.* Let v_0 be Gauss' valuation on $K[x]$. In order to factorize recursively each approximant $G_i^{(n)}$ of Proposition 6.8, we will measure the quality of the approximation with Gauss' valuation on $K^h[x]$:

$$v_0^h : K^h[x] \to \Gamma_{\mathbb{Q}}\infty, \qquad v_0^h\left(\sum\nolimits_i c_i x^i\right) := \min v^h(c_i),$$

which offers the advantage of being independent of the current splitting pair (μ, ϕ). The valuation v_0^h is asymptotically equivalent to the valuation μ_λ^h in the following sense :

Lemma 6.10. *Suppose $g \in \mathcal{O}[x]$ monic, and let μ, ϕ, λ as above. Then, for all $F \in K^h[x]$, we have*

$$v_0^h(F) \le \mu^h(F) \le \mu_\lambda^h(F) \le v_0^h(F) + \lambda\frac{\deg(F)}{\deg(\phi)}.$$

Proof. The assumption $g \in \mathcal{O}[x]$ ensures that the right end-slope $-\lambda_0$ of $N_{v,x}(g)$ satisfies $\lambda_0 \ge 0$. Hence, the first extended valuation $\mu_0 := [v, x, \lambda_0]$ computed by the irreducibility test of g satisfies $\mu_0^h \ge v_0^h$. Since $\mu_\lambda^h \ge \mu_0^h$, this proves the left inequality of the lemma. Let us prove the right inequality. Since μ_λ^h and v_0^h coincide on K^h, we may suppose $F \in \mathcal{O}^h[x]$ up to multiplying F by a suitable constant $c \in K^h$. Also, it is enough to consider the case F irreducible in $\mathcal{O}^h[x]$. In such a case, $v_0^h(F) = 0$ and the claim follows from [27, Theorem 3.9], having in mind that $\lambda = \mu_\lambda(\phi)$. □

In what follows, splitting pairs of polynomials in $K^h[x]$ are defined as for $K[x]$.

Definition 6.11. *Let $F \in K^h[x]$ be monic square-free, with splitting pair (μ^h, ϕ^h) and right end-slope $-\lambda$. The* Okutsu bound *of F is $\delta_0(F) := \mu_\lambda^h(F)$.*

Note that $\delta_0(F)$ does not depend on the choice of the splitting pair. The notation and terminology for $\delta_0(F)$ is justified by the fact that Definition 6.11 coincides with [25, Definition 5.9] when F is irreducible.

Proposition 6.12. *Let $f, g \in \mathcal{O}[x]$ be monic, square-free such that $v_0(f - g) > \delta_0(g)$ and $char(k) \nmid \deg(f)\deg(g)$. Then, g and f have the same right end-slope and the same right end residual polynomial. In particular, g is irreducible in $K^h[x]$ if and only if f is irreducible in $K^h[x]$.*

Proof. Let (μ, ϕ) be a splitting pair of g with right end-slope λ. Since $f, g \in \mathcal{O}[x]$, Lemma 6.10 shows that

$$\mu_\lambda(f - g) \ge v_0(f - g) > \delta_0(g) = \mu_\lambda(g) \ge v_0(g) \ge 0. \tag{6.1}$$

Hence, $\deg(g) = \deg(f)$ and $g \sim_{\mu_\lambda} f$. This implies $N_{\mu,\phi}(g) = N_{\mu,\phi}(f)$ and $R_{\mu_\lambda,\phi}(g) = R_{\mu_\lambda,\phi}(f)$ [27, Cor. 5.5]. The statement follows easily from these properties. □

Corollary 6.13. *Let $g \in \mathcal{O}[x]$ be monic square-free such that $char(k) \nmid \deg(g)$. Running algorithm* Irreducibility*(g) with Gauss precision $\sigma > \delta_0(g)$ returns a correct answer and allows to compute a splitting pair (μ, ϕ) of g. If g is reducible, the precision σ is also sufficient to compute the right end-slope λ and $R_{\mu_\lambda,\phi}(g)$.*

Remark 6.14. *In the discrete rank one case, one has* a priori *an upper bound for $\delta_0(g)$ in terms of the valuation of the discriminant of g, namely*

$$\delta_0(g) \leq 2v(\mathrm{disc(g)})/\deg(\mathrm{g}) \tag{6.2}$$

by [7, Lemma 2.2]. *This bound can be computed efficiently, although it's not interesting from a complexity perspective. In practice, we rather start with a small precision and check if it is sufficient to detect the right end-slope of the current Newton polygon (see* [40, Rem.5.4] *for more details in an analoguous discrete rank one situation). If not, we double the precision and restart all computations. This is the approach we implicitly follow here.*

6.2.4. *A factorization algorithm.* For $g \in K^h[x]$ monic square-free, we define

$$\delta_{\max}(g) := \max\{\delta_0(G),\ G \in \mathcal{F}(g)\}.$$

The previous results lead to Algorithm 3 below.

Algorithm 3: Factorization

Input : $g \in \mathcal{O}[x]$ monic, square-free with $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > \deg(g)$ and a precision $\sigma \in \Gamma$ such that $\sigma > \delta_{\max}(g)$.

Output: The irreducible factors of g in $K^h[x]$ computed with Gauss precision $\geq \sigma$.

```
Run Algorithm 2 with input g and with precision δ_0(g);
if g is irreducible then
    return [g]
else
    (μ, φ) ← splitting pair of g;
    −λ ← right end-slope of N_{μ,φ}(g);
    μ_λ ← [μ; φ, λ];
    compute and factorize R_{μ_λ,φ}(g) = ψ_1^{n_1} ··· ψ_s^{n_s} in κ(μ_λ)[y];
    compute some φ_i ← lift_{μ_λ,φ}(ψ_i) for 1 ≤ i ≤ s and let (φ_0, n_0) ← (φ, n_λ);
    γ ← μ_λ(g − φ_0^{n_0} ··· φ_s^{n_s}) − μ_λ(g);
    compute n ∈ ℕ such that 2^n γ ≥ σ + λ deg(g)/deg(φ);
    compute G_0^(n), ..., G_s^(n) ∈ O[x] as in Proposition 6.8;
    Res ← [ ];
    for i = 0, ..., s do
        if n_i = 1 then
            append G_i^(n) to Res
        else
            call recursively Algorithm 3 on G_i^(n) and append the output to Res
    return Res
```

Theorem 6.15. *If v has rank one, then Algorithm 3 terminates and returns a correct answer. Moreover, the approximant factors converge to the irreducible factors of g when we let $\sigma \to \infty$.*

Proof. Since Γ has rank one and $\gamma > 0$, there exists $n \in \mathbb{N}$ such that

$$2^n\gamma \geq \sigma + \lambda \deg(g)/\deg(\phi).$$

By Proposition 6.8 and Lemma 6.10, $v_0^h(G_i - G_i^{(n)}) > \sigma$, where G_i is given by Proposition 6.7. Since $\sigma > \delta_{\max}(g) \geq \delta_0(G_i^{(n)})$, we deduce by induction from Corollary 6.13 that the algorithm will

recursively detect and compute all irreducible factors of g with the suitable precision. The last statement is obvious. □

Remark 6.16. *Again, the bound $\delta_{\max}(g)$ is unknown before running Algorihm 3. One checks easily that* (6.2) *gives again an* a priori *computable upper bound $\delta_{\max}(g) \leq v(\mathrm{disc(g)})$ in the discrete rank one case. However, we rather follow in practice the analoguous strategy described in Remark 6.14.*

For v of arbitrary rank, the algorithm will return a correct answer as soon as all involved γ's satisfy

$$\delta_{\max}(g) \leq \sup(m\gamma, m \in \mathbb{N})$$

since we can then compute a suitable integer $n \in \mathbb{N}$ at each call. This might be a weaker condition than that of Corollary 6.9. However, it is not clear that the approximants $G^{(n)}$ of $G \in \mathcal{F}(g)$ converge to G.

The following corollary is immediate:

Corollary 6.17. *Suppose that v has rank one. Let $g \in \mathcal{O}[x]$ be monic square-free with* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) > \deg(g)$*. If $f \in \mathcal{O}[x]$ is monic and satisfies $v_0(g - f) > \delta_{\max}(g)$, then g and f have the same OM-factorization.*

6.2.5. *Proof of Theorems 0.1 and 0.2.* The first result is a consequence of Theorem 6.15 while the second result follows from Corollary 6.13. In both cases, we compute the involved indices of ramification and residual degrees thanks to Theorem 5.2.

6.2.6. *Coming back to Example 1.5.* Besides factorization, Algorithm 3 gives an alternative way to solve Problem 1.4, where Hensel lifting and approximate roots replace the refinement steps inherent to Algorithm 1. This is particularily relevant from a complexity point of view, as shown in [41] in the discrete rank one case.

Let us illustrate this fact on our Example 1.5 solved in Subsection 4.5. At the end of the depth one step, one has computed a factorization of the current residual polynomial

$$R_{\mu_1,\phi_1}(g) = (y + 698z + 349)^8 (y - 698z - 349)^8 =: \psi_1^8 \psi_2^8 \in \kappa_1[y]$$

which implies a factorization $g = F_1 F_2$ in $K^h[x]$. In order to find the next augmented valuations of the MLV chains of g, we need to compute a key polynomial of degree 72 for each induced tangent direction, *not leading to a refinement step* (such as $\phi_2^{(9)}$ in the notation of Subsection 4.5). As explained above, this can be achieved as follows :

(1) Compute approximants $\tilde{G}_1, \tilde{G}_2$ of F_1, F_2 with a high enough precision (Proposition 6.8).
(2) Compute the 8^{th}-approximate roots of $\tilde{G}_1$ and $\tilde{G}_2$ (Proposition 6.3).

Let us detail step (1), based on the generalized Hensel lifting of [41]. The initialisation requires to compute $G_1, G_2 \in K[x]$ with G_1, G_2 monic of degrees $\deg(G_i) = \deg(F_i)$ and their "Bézout cofactors" $U_1, U_2 \in K[x]$ such that $\mu_1(U_i) = -\mu_1(G_i)$ and such that

$$\mu_1(g - G_1 G_2) > \mu_1(g) \quad \text{and} \quad \mu_1(U_1 G_1 + U_2 G_2 - 1) > 0.$$

For G_1 and G_2, this is equivalent to take an arbitrary monic lift of ψ_1^8 and ψ_2^8. Following Subsection 4.5, we can take

$$G_1 = (\phi_1^{36} + W\,(698x + 349))^8 \quad \text{and} \quad G_2 = (\phi_1^{36} - W\,(698x + 349))^8$$

where $W = t_1^3\, t_2^2$. We check indeed that $\mu_1(g - G_1 G_2) = \mu_1(g) + \gamma_1 > \mu_1(g)$ as required (where γ_1 is the current slope). To compute U_1, U_2, we first compute a residual Bezout relation

$$u_1\, \psi_1^8 + u_2\, \psi_2^8 = 1 \in \kappa_1[y].$$

We find $u_1(y) = u_2(-y)$, with

$$u_1 = (538 - 447z)\, y^7 - 269y^6 + (104 + 208z)\, y^5 - 101y^4 - (365 + 730z)\, y^3 - 584y^2 + (244 + 488z)\, y + 369.$$

Then we lift u_1, u_2 in $K[x]$, imposing the conditions $\mu_1(U_i) = -\mu_1(G_i)$. We can take :

$$\begin{aligned} U_1 \;=\; & (538 - 447x)\, W^{-15} \phi_1^{252} - 269 W^{-14} \phi_1^{216} + (104 + 208x)\, W^{-13} \phi_1^{180} - 101 W^{-12} \phi_1^{144} \\ & - (365 + 730x)\, W^{-11} \phi_1^{108} - 584 W^{-10} \phi_1^{36} + (244 + 488x)\, W^{-9} \phi_1^{36} + 369 W^{-8}, \end{aligned}$$

and U_2 given by the same formula but replacing W with $-W$. We can indeed check that $\mu_1(U_i) = -\mu_1(G_i)$ and $\mu_1(U_1G_1 + U_2G_2 - 1) = \gamma_1 > 0$, as required. Applying several times the classical Hensel's step (adapted to the valuation μ_1, see [41, Prop.8]) allows to lift this factorization up to a higher precision. After n steps, we get $\tilde{G}_1, \tilde{G}_2 \in K[x]$ monic of degrees $\deg(\tilde{G}_i) = \deg(F_i)$, which satisfy

$$\mu_1(g - \tilde{G}_1\tilde{G}_2) > \mu_1(g) + 2^n\gamma_1$$

which in turns forces $\mu_1^h(F_i - \tilde{G}_i) > \mu_1^h(F_i) + 2^n\gamma_1$. By Lemma 6.10, we get

$$v_0^h(F_i - \tilde{G}_i) > \mu_1(F_i) + \left(2^n - \frac{\deg(F_i)}{\deg(\phi_1)}\right)\gamma_1$$

As we are in the rank one case, one can take n such that the right hand side is greater than $\delta_{\max}(F_i)$ (see Remark 6.14 about how to reach in practice a sufficient precision). Then, calling recursively Algorithm 3 on each factor $\tilde{G}_i$ will allow to compute the MLV-chains of all irreducible factors of g (Corollary 6.13).

Notice that $\deg(\tilde{G}_1) < \mathrm{char}(k)$, so Proposition 6.3 ensures that the 8^{th}-approximate root ϕ of $\tilde{G}_1$ leads immediately to a splitting pair (μ_1^h, ϕ) of $\tilde{G}_1$, hence of F_1 by Proposition 6.12. In other words, we may have chosen ϕ instead of $\phi_2^{(9)}$ as a "splitting" key polynomial for F_1 in Subsection 4.5. In the discrete rank one case, it is shown that this approach is less onerous than refinement steps inherent to Algorithm 1. One reason is that we might need $O(\delta_{\max})$ refinement steps to compute a splitting pair, while Algorithm 3 uses only $O(\log(\delta_{\max}))$ Hensel steps due to quadratic convergence. Moreover, it is shown in [41] that we can modify Algorithm 3 to an even more efficient algorithm using a divide and conquer strategy for the precision.

References

[1] S.S. Abhyankar, Coverings of algebraic curves, Amer. J. Math. **79** (1957), 825–856.

[2] S.S. Abhyankar, Irreducibility criterion for germs of analytic functions of two complex variables, Adv. Math. **35** (1989), 190–257.

[3] S.S. Abhyankar, T. Moh, Newton-Puiseux Expansion and Generalized Tschirnhausen Transformation, J. Reine Angew. Math. **260** (1973), 47–83.

[4] M. Alberich-Carramiñana, J. Guàrdia, E. Nart, J. Roé, Valuative trees of valued fields, J. Algebra **614** (2023), 71–114.

[5] M. dos Santos Barnabé, J. Novacoski, Valuations on $K[x]$ approaching a fixed irreducible polynomial, J. Algebra **592** (2022), 100–117.

[6] J.-D. Bauch, Computation of integral bases, J. Number Theory **165** (2016), 382—407.

[7] J.-D. Bauch, E. Nart, H. Stainsby, Complexity of the OM factorizations of polynomials over local fields, LMS J. of Comp. and Math. **16** (2013), 139–171.

[8] D. Duval, Rational Puiseux expansions, Compositio Math. **70** (1989), no.2, 119–154.

[9] O. Endler, Valuation Theory, Universitex, Springer-Verlag, Berlin Heidelberg, 1972.

[10] J.v.z. Gathen, G. Jürgen, Modern Computer Algebra, Cambridge University Press, 2013.

[11] A. Jakhar, S. K. Khanduja, N. Sangwan, On factorization of polynomials in Henselian valued fields, Comm. Alg. **46-7** (2018), 3205–3221.

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

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

[14] J. Guàrdia, J. Montes, E. Nart, Newton polygons of higher order in algebraic number theory, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

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

[16] J. Guàrdia, J. Montes, E. Nart, Higher Newton polygons and integral bases, J. Number Theory **147** (2015), 549-–589.

[17] J. Guàrdia, E. Nart, Genetics of polynomials over local fields, in *Arithmetic, geometry, and coding theory*, Contemp. Math. vol. 637 (2015), 207-241.

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

[19] F.J. Herrera Govantes, W. Mahboub, M.A. Olalla Acosta, M. Spivakovsky, Key polynomials for simple extensions of valued fields, J. Singul. **25** (2022), 197–267.

[20] F.-V. Kuhlmann, Value groups, residue fields, and bad places of rational function fields, Trans. Amer. Math. Soc. **356** (2004), no. 11, 4559–4660.

[21] J. Mac Donald, Fiber polytopes and fractional power series, J. of Pure and App. Alg. **104** (1995), no. 2, 213–233.

[22] S. Mac Lane, A construction for absolute values in polynomial rings, Trans. Amer. Math. Soc. **40** (1936), 363–395.
[23] S. Mac Lane, A construction for prime ideals as absolute values of an algebraic field, Duke Math. J. **2** (1936), 492–510.
[24] J. Montes, Polígonos de Newton de orden superior y aplicaciones aritméticas, PhD Thesis, Universitat de Barcelona, 1999.
[25] N. Moraes de Oliveira, E. Nart, Defectless polynomials over Henselian fields and inductive valuations, J. Algebra, **541** (2020), 270–307.
[26] N. Moraes de Oliveira, E. Nart, Computation of residual polynomial operators of inductive valuations, J. Pure Appl. Algebra **225-9** (2021), 106668.
[27] E. Nart, Key polynomials over valued fields, Publ. Mat. **64** (2020), 195–232.
[28] E. Nart, Mac Lane-Vaquié chains of valuations on a polynomial ring, Pacific J. Math. **311-1** (2021), 165–195.
[29] E. Nart, Rigidity of valuative trees under Henselization, Pacific J. Math. **319** (2022), 189–211.
[30] E. Nart, J. Novacoski, The defect formula, Adv. Math. **428** (2023), 109153.
[31] J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg 1992.
[32] J. Novacoski, On Mac Lane–Vaquié key polynomials, J. Pure Appl. Algebra **225** (2021), 106644.
[33] J. Novacoski and M. Spivakovsky, Reduction of local uniformization to the rank one case, Valuation Theory in Interaction, EMS Series of Congress Reports, Eur. Math. Soc. (2014) 404–431.
[34] J. Novacoski, M. Spivakovsky, On the local uniformization problem, Banach Center Publ. **108** (2016), 231–238.
[35] K. Okutsu, Construction of integral basis I, II, Proc. Japan Acad. Ser. A **58** (1982), 47–49, 87–89.
[36] Ø. Ore, Zur Theorie der algebraischen Körper, Acta Math. **44** (1923), 219–314.
[37] Ø. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, Math. Ann. **99** (1928), 84–117.
[38] P. Popescu-Pampu, Approximate roots, Fields Inst. Comm. **33** (2002), 1–37.
[39] A. Poteaux and M. Weimann, Computing Puiseux series : a fast divide and conquer algorithm, Ann. Henri Leb. **4** (2021), 1061–1102.
[40] A. Poteaux, M. Weimann, A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, Comput. Complexity **31** (2022), no. 6, 1–52.
[41] A. Poteaux, M. Weimann, Local polynomial factorisation: improving the Montes algorithm, Proceedings of the 2022 ACM on International Symposium on Symbolic and Algebraic Computation ISSAC'22 (2022), 149–158.
[42] H. D. Stainsby, Triangular bases of integral closures, J. Symb. Comp. **87** (2018) 140–175.
[43] M. Vaquié, Famille admisse associée à une valuation de $K[x]$, Singularités Franco-Japonaises, Séminaires et Congrés 10, SMF, Paris (2005), Actes du colloque franco-japonais, juillet 2002, édité par Jean-Paul Brasselet et Tatsuo Suwa, 391–428.
[44] M. Vaquié, Extension d'une valuation, Trans. Amer. Math. Soc. **359** (2007), no. 7, 3439–3481.
[45] M. Vaquié, Famille essential de valuations et défaut d'une extension, J. Algebra **311** (2007), no. 2, 859–876.

Institut de Robòtica i Informàtica Industrial (IRI, CSIC-UPC), Institut de Matemàtiques de la UPC-BarcelonaTech (IMTech) and Departament de Matemàtiques, Universitat Politècnica de Catalunya · BarcelonaTech, Av. Diagonal, 647, E-08028 Barcelona, Catalonia
Email address: Maria.Alberich@upc.edu

Departament de Matemàtiques, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú, Catalonia
Email address: jordi.guardia-rubies@upc.edu

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia
Email address: nart@mat.uab.cat, jroe@mat.uab.cat

Université de Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL. F-59000 Lille, France
Email address: adrien.poteaux@univ-lille.fr

LMNO, UMR 6139, Université de Caen-Normandie, F-14032 Caen, France
Email address: martin.weimann@unicaen.fr