Publ. Mat. **55** (2011), 261–294

OKUTSU-MONTES REPRESENTATIONS OF PRIME IDEALS OF ONE-DIMENSIONAL INTEGRAL CLOSURES

Enric Nart

Abstract

This is a survey on Okutsu-Montes representations of prime ideals of certain one-dimensional integral closures. These representations facilitate the computational resolution of several arithmetic tasks concerning prime ideals of global fields.

Introduction

In 1923, Øystein Ore found a method to construct the prime ideals of a number field, dividing a given prime number p, in terms of a defining equation $f(x) \in \mathbb{Z}[x]$, provided that this equation satisfies certain *p-regularity* condition [**Ore23**]. The idea was to detect first a p-adic factorization of $f(x)$ according to the sides of certain Newton polygon $N(f)$, and then, to detect a further factorization of each of these factors according to the different irreducible polynomials that divide certain residual polynomials $R_\lambda(f)$ with coefficients in a finite field, for λ running on the slopes of the different sides of $N(f)$.

He raised then the question of the existence of an iterative procedure to compute the prime ideals in the p-irregular case, based on the consideration of similar Newton polygons $N_i(f)$ and residual polynomials $R_{\lambda,i}(f)$ of *higher order* $i \geq 1$.

Saunders MacLane attacked this problem in 1936 from the point of view of valuations. Given any discrete valuation v on a field k, he parametrized all discrete valuations of the rational function field $k(x)$ that extend v. Then, given an irreducible polynomial $f(x) \in k[x]$, he characterized all valuations of the field $k[x]/(f(x))$ that extend v, as limits of infinite families of valuations of $k[x]$ whose value on $f(x)$ grows to

2010 *Mathematics Subject Classification.* Primary: 11Y40; Secondary: 11Y05, 11R04.
Key words. Montes algorithm, Newton polygon, local field, global field, integral basis, Okutsu-Montes representation.

infinity. Finally, he gave a criterion to decide when a valuation of $k[x]$ was sufficiently close to a valuation of $k[x]/(f(x))$, to uniquely represent it [**McL36**], [**McL36b**].

In 1999, Jesús Montes developed an algorithm that carries out Ore's program [**Mon99**]. The algorithm follows MacLane's pattern, but the introduction of the right concept of residual polynomial of higher order $R_{\lambda,i}(f)$ makes the whole theory constructive and well adapted to computational applications. The algorithm is highly recursive: each computation in order i requires auxiliary computations in all previous orders $1,\dots,i-1$. This led Montes, for purely computational reasons, to optimize the algorithm so that it keeps working at certain order i as long as possible and it does not pass to work at order $i+1$ until this is absolutely unavoidable. It turns out that the optimized algorithm has an output with unexpected canonical properties, linked to invariants of extensions of local fields that had been studied by Kousaku Okutsu in 1982 [**Oku82**].

The algorithm of Montes computes what we call *Okutsu-Montes representations* of prime ideals of one-dimensional integral closures. These computational representations single out the prime ideals and they carry on essential data of the corresponding extensions of local fields. Moreover, these objects have proved to be an efficient and malleable tool for a computational resolution of several arithmetic tasks concerning prime ideals of integral closures of subrings of global fields.

In this survey notes I explain the structure of Montes algorithm and describe some of its applications, with special emphasis on the computation of integral closures. Most of this material is joint work with Jordi Guàrdia and Jesús Montes. This survey grew out from the notes of a seminar delivered at the MSRI in Berkeley, California, as part of the workshop *Computation of integral closures*, that took place during the week of 26th to 30th of July 2010. We thank the organizer, David Eisenbud, for giving us the opportunity to present these results, and the participants for the charming atmosphere and the fruitful exchange of ideas that contributed to a substantial improvement of the final write up.

1. Overview

1.1. Local fields. Let K be a local field with perfect residue class field. Let $\mathcal{O}$ be its ring of integers, $\mathfrak{m}$ the maximal ideal, $\pi\in\mathfrak{m}$ a generator of $\mathfrak{m}$, and $v\colon \overline{K}^*\longrightarrow\mathbb{Q}$, the canonical extension of the discrete valuation

of K to an algebraic closure, normalized by $v(K^*) = \mathbb{Z}$. Let $K^{\mathrm{sep}} \subset \overline{K}$ be the separable closure of K in $\overline{K}$.

Let us sketch the application of Montes algorithm [**HN08**], [**GMN08**] (HN stands for "higher Newton"). The design of the algorithm will be described in more detail in Section 2.

Montes algorithm.

Input: A monic separable polynomial $f(x) \in \mathcal{O}[x]$.

Output: A family $\mathbf{t}_1, \dots, \mathbf{t}_g$ of *f-complete and optimal types*, parameterizing the monic irreducible factors $F_1(x), \dots, F_g(x)$ of $f(x)$ in $\mathcal{O}[x]$.

For K a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, recent estimations for the complexity of this algorithm have been obtained by Veres [**Ver09**], Ford-Veres [**FV10**], and Pauli [**Pau10**]. The finer estimation is $O(n^{2+\epsilon}\delta^{2+\epsilon})$ operations of integers less than p, where $\delta = v(\mathrm{disc}(f))$.

Let $F(x)$ be one of these irreducible factors, $\theta \in K^{\mathrm{sep}}$ a root of F, $L = K(\theta)$ the corresponding finite separable extension of K, and $\mathcal{O}_L$ its ring of integers.

Let $\mathbf{t}$ be the type corresponding to F. For simplicity, we represent

$$\mathbf{t} = [\phi_1, \dots, \phi_{r+1}]$$

as a sequence of monic irreducible separable polynomials in $\mathcal{O}[x]$ satisfying certain recursive conditions. For the moment let us just mention that

- $\deg \phi_1 \mid \cdots \mid \deg \phi_r \mid \deg \phi_{r+1} = \deg F, \quad \deg \phi_1 < \cdots < \deg \phi_r,$
- $\dfrac{v(\phi_1(\theta))}{\deg \phi_1} < \cdots < \dfrac{v(\phi_{r+1}(\theta))}{\deg \phi_{r+1}}.$

It turns out that the polynomial $\phi_{r+1}(x)$ is an *Okutsu approximation* to $F(x)$; this means that it is sufficiently close to $F(x)$ for certain purposes (see Section 3). Thus, Montes algorithm is a kind of polynomial factorization algorithm. Actually, a rather peculiar one, in two senses:

(1) It is based on a series of generalizations of Hensel lemma, so that successive factorizations of $f(x)$ are *detected*, but never carried out. Only certain auxiliary polynomials over finite extensions of the residue class field are factorized.

(2) Besides computing an approximation to each irreducible factor F, the output of the algorithm provides as well a lot of arithmetic information about the finite extension L/K determined by F.

The type $\mathbf{t}$ is structured in $r+1$ *levels*, and r is called the *order* of $\mathbf{t}$. At each level i, $\mathbf{t}$ stores several combinatorial and arithmetic invariants

$$e_i,\ f_i,\ h_i,\ \lambda_i,\ V_i,\ \text{etc.}$$

linked to Newton polygons of higher order of $f(x)$. These invariants contain essential information about $F(x)$ and the extension L/K. For instance,

$$v(\phi_i(\theta)) = \frac{V_i + |\lambda_i|}{e_1 \cdots e_{i-1}},$$

$$e(L/K) = e_1 \cdots e_r, \quad f(L/K) = f_0 f_1 \cdots f_r, \tag{1}$$

$$\exp(F) = \sum_{i=1}^{r} (e_i f_i \cdots e_r f_r - 1)\frac{h_i}{e_1 \cdots e_i},$$

where $\exp(F)$ is the *exponent* of F; that is, the least non-negative integer such that $\pi^{\exp(F)}\mathcal{O}_L \subset \mathcal{O}[\theta]$.

The type $\mathbf{t}$ determines as well an easy computation of the integral closure of $\mathcal{O}$ inside L. In fact, let $n = \deg F = [L : K]$; for each integer $0 \le m < n$, we express m in a unique way as:

$$m = j_0 + j_1 \deg \phi_1 + \cdots + j_r \deg \phi_r, \quad 0 \le j_i < (\deg \phi_{i+1} / \deg \phi_i),$$

where $\phi_0(x) := x$. We consider the following polynomial of degree m:

$$g_m(x) := \phi_0(x)^{j_0} \phi_1(x)^{j_1} \cdots \phi_r(x)^{j_r}.$$

As shown above, the data of $\mathbf{t}$ allow us to compute

$$\nu_m := \lfloor j_1 v(\phi_1(\theta)) + \cdots + j_r v(\phi_r(\theta)) \rfloor.$$

Then, the following family is an $\mathcal{O}$-basis of $\mathcal{O}_L$:

$$1,\ \frac{g_1(\theta)}{\pi^{\nu_1}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\nu_{n-1}}}.$$

Thus, we may say that Montes algorithm provides the computation of all the integral closures of $\mathcal{O}$ in the different extensions determined by the irreducible factors of the input polynomial $f(x)$, almost as a by-product. We need only to include in the algorithm an efficient computation of the polynomials $g_m(x)$.

1.2. Applications to global fields. Let us illustrate the applications to number fields. For function fields of curves the results are completely analogous, but no implementation has been made yet.

Let $K = \mathbb{Q}[x]/(f(x))$ be now the number field defined by a monic irreducible polynomial $f(x)$ with integer coefficients and degree n. Let $\theta \in \overline{\mathbb{Q}}$ be a root of $f(x)$ and $\mathbb{Z}_K$ the ring of integers of K.

For any prime number p, the prime ideals of K dividing p are in one-to-one correspondence with the monic irreducible factors of $f(x)$ over $\mathbb{Z}_p[x]$. In fact, for any such a prime ideal $\mathfrak{p}$ we consider a topological embedding

$$\iota_{\mathfrak{p}} \colon K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbb{Q}}_p,$$

where $K_{\mathfrak{p}}$ is the completion of K with respect to the $\mathfrak{p}$-adic topology. Then, the corresponding irreducible factor of $f(x)$ is the minimal polynomial of $\iota_{\mathfrak{p}}(\theta)$ over $\mathbb{Q}_p$. We denote this monic irreducible factor by $F_{\mathfrak{p}}(x)$.

Hence, by applying Montes algorithm to $f(x)$ over $\mathbb{Z}_p$, one obtains what we call an *Okutsu-Montes representation* (OM representation) of all prime ideals of K dividing p :

$$\mathfrak{p} = [p; \phi_1, \dots, \phi_r; \phi_{\mathfrak{p}}], \quad \phi_{\mathfrak{p}} := \phi_{r+1},$$

where $\mathbf{t}_{\mathfrak{p}} = [\phi_1, \dots, \phi_r, \phi_{r+1}]$ is the type attached to $F_{\mathfrak{p}}(x)$ by the algorithm.

The polynomials ϕ_i have all integer coefficients. It turns out that the invariants contained in the type $\mathbf{t}_{\mathfrak{p}}$ are the essential data that are necessary for a computational treatment of the prime ideal. For instance, the following tasks in the group of fractional ideals can be based on the data (and operators) of the OM representations of the prime ideals:

(1) Compute the $\mathfrak{p}$-adic valuation, $v_{\mathfrak{p}} \colon K^* \longrightarrow \mathbb{Z}$.
(2) Compute the prime ideal factorization of a fractional ideal.
(3) Compute a two-element representation of a fractional ideal.
(4) Add, multiply and invert fractional ideals.
(5) Compute the reduction map, $\mathbb{Z}_K \longrightarrow \mathbb{Z}_K/\mathfrak{p}$, and a section of this map (a lifting map).
(6) Solve Chinese remainder problems.
(7) Compute a p-integral basis of K.

We have implemented a '+Ideals' package in Magma that contains routines for all these tasks [**GMN10**], [**GMN10b**].

Recall that a *p-integral basis* is a $\mathbb{Q}$-basis of K, made of integral elements $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_K$, that satisfy any of the following equivalent conditions:

(a) $\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ are a $\mathbb{Z}_p$-basis of $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

(b) $\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ are an $\mathbb{F}_p$-basis of $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{F}_p$.

(c) p does not divide the index $(\mathbb{Z}_K : \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}})$.

Since $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{F}_p$ has dimension n as an $\mathbb{F}_p$-vector space, in practice it suffices to check that $\alpha_1, \ldots, \alpha_n$ determine $\mathbb{F}_p$-linearly independent elements in this $\mathbb{F}_p$-algebra.

It is well-known how to compute a p-integral basis of K from the local $\mathbb{Z}_p$-bases of all local rings $\mathbb{Z}_{K_\mathfrak{p}}$, for $\mathfrak{p} \mid p$. One needs only to compute multipliers $\beta_\mathfrak{p} \in \mathbb{Z}_K$ satisfying:

$$v_\mathfrak{p}(\beta_\mathfrak{p}) = 0, \quad v_\mathfrak{q}(\beta_\mathfrak{p}) \geq (\exp(F_\mathfrak{p}) + 1)e(\mathfrak{q}/p), \quad \forall,\ \mathfrak{q} \mid p,\ \mathfrak{q} \neq \mathfrak{p}.$$

These multipliers are easily computed from the data of the OM represen tations [**GMN10**, Section 4.2]. If $\{\mathcal{B}_\mathfrak{p}\}_{\mathfrak{p}|p}$ are the local bases, then $\bigcup_{\mathfrak{p}|p} \beta_\mathfrak{p} \mathcal{B}_\mathfrak{p}$ is a p-integral basis of K (cf. Section 4.1).

Finally, an integral basis of K (a $\mathbb{Z}$-basis of $\mathbb{Z}_K$) is computed as follows:

(1) Factorize the discriminant $\mathrm{disc}(f)$ of the polynomial $f(x)$.

(2) For each prime $p \mid \mathrm{disc}(f)$, compute a p-integral basis of K in Hermite Normal Form.

(3) Glue these data into a global basis by a simple application of the Chinese Remainder Theorem.

1.3. Some remarks.

1. The standard packages that manipulate number fields need to compute an integral basis as a preliminary step. This makes them totally useless for many number fields of large degree, or number fields defined by an equation with large coefficients, because of the impossibility to factorize the discriminant.

The routines based on the OM representations of the prime ideals do not require the factorization of $\mathrm{disc}(f)$ and they work very efficiently for "big" number fields [**GMN10b**]. We do not claim too much originality on this fact. Many researchers who need to work with number fields of large degree develop their own routines to deal with concrete problems, avoiding the computation of the maximal order. But we do claim on efficiency: our routines run extremely fast in practice.

Of course, the bottleneck is again integer factorization: we can deal only with fractional ideals whose norm may be factorized.

2. The routines based on the OM representations have a completely different nature than the classical ones. It often occurs, when dealing

with some problem, that once a direct connexion with the data contained in the OM representations is found, the outcoming routine is much faster than the routine that would be inspired in the classical ones.

3. We do not know how to test if an ideal is principal. To this end it would be necessary to combine the OM representations with some kind of LLL reduction routine (preferably not based on the lattice $\mathbb{Z}_K$).

Question. Is there a theoretical reason that makes it hopeless to design such a test without factorizing the discriminant?

4. Suppose the discriminant of the defining equation $f(x)$ may be factorized. Then, how do our routines behave with respect to the classical ones? Let us discuss this comparison at two levels.

(1) The OM routines compute an integral basis much faster than the ordinary routines of Magma or Pari. We saw that the computation of the local bases is almost a by-product of Montes algorithm.
(2) Once the maximal order of K has been computed, the OM routines still run (slightly) faster than the ordinary ones of Magma or Pari, for number fields whose degree is not too small (say $n \geq 16$). One reason for this is that the OM techniques avoid the use of linear algebra. The standard methods compute $\mathbb{Z}$-basis of the prime ideals, expressed in coordinates with respect to the integral basis. We get in this way $n \times n$ matrices, and the linear algebra procedures to manipulate them (like the computation of Hermite Normal Forms) dominate the complexity for n large.

5. Suppose the discriminant of the defining equation $f(x)$ may be factorized. We mentioned already that we also need the HNF routine to patch the different p-integral bases of K, for the primes p dividing $\mathrm{disc}(f)$, into a global integral basis. This HNF routine is the bottleneck for the whole process, if n is large.

2. The algorithm of Ore, MacLane and Montes

The content of this section is mainly extracted from [**HN08**].

Let K be a local field, $\mathcal{O}$ its ring of integers, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$, and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ the residue class field, which is supposed to be perfect. Let $v\colon \overline{K}^* \longrightarrow \mathbb{Q}$ be the canonical extension to $\overline{K}$ of the discrete valuation of K, normalized by $v(K^*) = \mathbb{Z}$. Let $K^{\mathrm{sep}} \subset \overline{K}$ be the separable closure of K in $\overline{K}$.

We extend v to a discrete valuation v_1 of the field $K(x)$, by letting it act on $K[x]$ as follows:

$$v_1\left(\sum\nolimits_{0\le s} a_s x^s\right) := \min\{v(a_s) \mid 0 \le s\}.$$

Also, we denote $\mathbb{F}_0 := \mathbb{F}$, and we consider the 0-th *residual operator*:

$$R_0\colon \mathcal{O}[x] \longrightarrow \mathbb{F}_0[y], \quad g(x) \mapsto R_0(g)(y) := \overline{g(y)/\pi^{v_1(g)}}.$$

Note that for monic polynomials, R_0 is the ordinary reduction map.

Our aim is to describe the monic irreducible factors of a given monic separable polynomial $f(x) \in \mathcal{O}[x]$. The starting point of the algorithm is Hensel lemma. From a factorization of $R_0(f)(y)$ into a product of monic irreducible polynomials in $\mathbb{F}_0[y]$:

$$R_0(f)(y) = \varphi_1(y)^{\ell_1} \cdots \varphi_k(y)^{\ell_k},$$

we detect (but not compute) a factorization of $f(x)$ in $\mathcal{O}[x]$,

$$f(x) = F_1(x) \cdots F_k(x),$$

into a product of monic (not necessarily irreducible) polynomials satisfying $R_0(F_i)(y) = \varphi_i(y)^{\ell_i}$.

We start then to construct a *tree $\mathcal{T}$ of types*. Actually, $\mathcal{T}$ is the disjoint union of k connected trees, one for each irreducible factor of $R_0(f)$. The initial node of each connected tree is a *type of order zero*, which we are going to describe now.

Let us fix one of the irreducible factors of $R_0(f)$, that we denote from now on by $\psi_0(y) \in \mathbb{F}_0[y]$. The subindex 0 emphasizes that we are working at order zero. We choose (non-canonically) a monic lift $\phi_1(x) \in \mathcal{O}[x]$ of ψ_0 and we denote

$$\mathbf{t} := [\phi_1].$$

This object is the type of order zero that corresponds to the initial node of the tree.

Let $F_{\mathbf{t}}(x) \in \mathcal{O}[x]$ be the (unknown) monic factor of $f(x)$ attached by Hensel lemma to ψ_0; recall that $R_0(F_{\mathbf{t}}) = \psi_0^{\ell_0}$, for certain integer $\ell_0 > 0$.

Our initial node, labelled by ψ_0, is supposed to sprout several branches corresponding to *types of order one*, obtained by adding a different polynomial ϕ_2 for each branch, in a process to be explained in Section 2.4 in more detail. Clearly, if $\ell_0 = 1$ then $F_{\mathbf{t}}$ is already irreducible and the initial node is already a leave of the tree $\mathcal{T}$ (an end node that has no further branching).

A type of order zero supports certain invariants of the irreducible factors of $F_{\mathbf{t}}(x)$:

$$\begin{aligned} &\psi_0(y) \in \mathbb{F}_0[y], \\ &f_0 := \deg \psi_0, \\ &\mathbb{F}_1 := \mathbb{F}_0[y]/(\psi_0(y)), \\ &z_0 := \text{class of } y \text{ in } \mathbb{F}_1. \end{aligned} \tag{2}$$

Note that $\psi_0(z_0) = 0$ and $\mathbb{F}_1 = \mathbb{F}_0[z_0]$. This seemingly innocuous object $\mathbf{t}$ has hidden powers. It determines a *Newton polygon operator* of the first order:

$$N_1 := N_{\phi_1,v_1} \colon \mathcal{O}[x] \longrightarrow 2^{\mathbb{R}^2},$$

where $2^{\mathbb{R}^2}$ is the set of subsets of the plane $\mathbb{R}^2$. Also, for every negative rational number $\lambda \in \mathbb{Q}^-$, the type $\mathbf{t}$ determines a *residual polynomial operator* of the first order:

$$R_{\lambda,1} := R_{\phi_1,v_1,\lambda} \colon \mathcal{O}[x] \longrightarrow \mathbb{F}_1[y].$$

Let us describe all these operators in some detail.

2.1. The Newton polygon operator. Let $m_1 := \deg \phi_1 = f_0$. Any polynomial $g(x) \in \mathcal{O}[x]$ has a canonical ϕ_1-expansion:

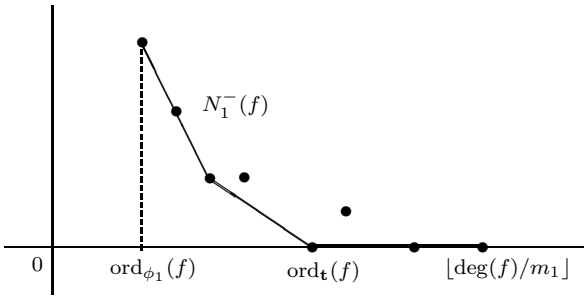
$$g(x) = \sum_{0 \le s} a_s(x)\phi_1(x)^s, \quad \deg a_s < m_1.$$

Then, $N_1(g)$ is the lower convex hull of the set of all points $(s, v_1(a_s))$ in $\mathbb{R}^2$. We are only interested in the *principal part* of this polygon, $N_1^-(g) \subset N_1(g)$, made of all sides with negative slope. The *length* $\ell(N)$ of a polygon N is, by definition, the abscissa of the right end point of N.

We denote:

$$\operatorname{ord}_{\mathbf{t}}(g) := \operatorname{ord}_{\psi_0} R_0(g) = \ell(N_1^-(g)).$$

By construction, the type $\mathbf{t}$ of order zero extracted from the factorization of $f(x)$ modulo $\mathfrak{m}$, had $\operatorname{ord}_{\mathbf{t}}(f) = \ell_0 > 0$. Since our polynomial $f(x)$ is monic, the last point of $N_1(f)$ has ordinate zero. The typical shape of $N_1(f)$ is as shown below.



The polygon $N := N_1^-(f)$ has a *residual coefficient* c_s at each integer abscissa, $\mathrm{ord}_{\phi_1} f \le s \le \mathrm{ord}_{\mathbf{t}}(f)$, defined as follows:

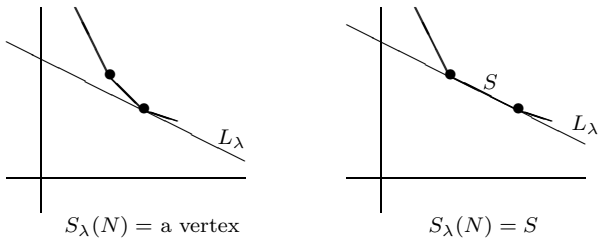
$$c_s := \begin{cases} 0, & \text{if } (s, v_1(a_s)) \text{ lies above } N, \\ R_0(a_s)(z_0) \in \mathbb{F}_1^*, & \text{if } (s, v_1(a_s)) \text{ lies on } N. \end{cases}$$

In the latter case, $c_s \neq 0$ because $\deg a_s < m_1 = f_0$, so that $R_0(a_s)(y)$ cannot be divided by the minimal polynomial $\psi_0(y)$ of z_0 over $\mathbb{F}_0$.

2.2. The residual polynomial operators. We keep the notation $N = N_1^-(f)$. Denote by $\mathrm{Slopes}(N)$ the set of slopes of N. Given any $\lambda \in \mathbb{Q}^-$, we consider:

$$S_\lambda(N) := \{(x,y) \in N \mid y + x|\lambda| \text{ is minimal}\} = \begin{cases} \text{a vertex}, & \text{if } \lambda \notin \mathrm{Slopes}(N), \\ \text{a side}, & \text{if } \lambda \in \mathrm{Slopes}(N). \end{cases}$$

The following picture illustrates both possibilities. In this picture L_λ is the line of slope λ having first contact with N from below.

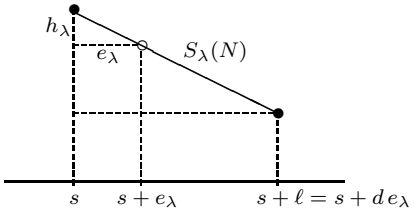


$S_\lambda(N) =$ a vertex $\qquad$ $S_\lambda(N) = S$

In any case, $S_\lambda(N)$ is a segment of $\mathbb{R}^2$ with end points having integer coordinates. Any such segment has a *degree*. If $\lambda = -h_\lambda/e_\lambda$ with h_λ, e_λ positive coprime integers, the degree of $S_\lambda(N)$ is defined as:

$$d := d(S_\lambda(N)) := \ell(S_\lambda(N))/e_\lambda,$$

where $\ell := \ell(S_\lambda(N))$ is the length of the projection of $S_\lambda(N)$ to the horizontal axis.



Note that $S_\lambda(N)$ splits into d minimal subsegments whose end points have integer coordinates.

We define the *residual polynomial* of the first order of $f(x)$, with respect to λ, as:

$$R_{\lambda,1}(f)(y) := R_{\phi_1,v_1,\lambda}(f)(y) := c_s + c_{s+e_\lambda}y + \cdots + c_{s+de_\lambda}y^d \in \mathbb{F}_1[y],$$

where s is the abscissa of the left end point of $S_\lambda(N)$. Since $c_s\, c_{s+de_\lambda} \neq 0$, the degree of $R_{\lambda,1}(f)$ is always equal to d, and the polynomial $R_{\lambda,1}(f)(y)$ is never divisible by y.

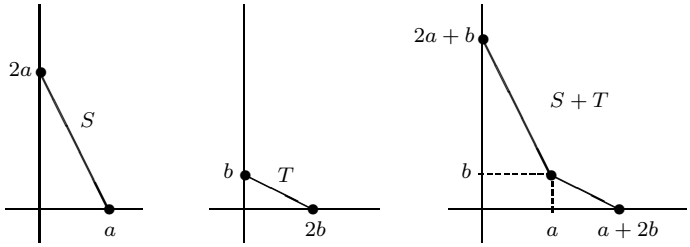
For any polynomial $g(x) \in \mathcal{O}[x]$ the definition of $R_{\lambda,1}(g)$ is completely analogous but taking $N = N_1^-(g)$.

2.3. Fundamental results of Ore.

Theorem of the product [**HN08**, Theorem 1.13]**.** *For any pair of polynomials $g(x), h(x) \in \mathcal{O}[x]$ and any $\lambda \in \mathbb{Q}^-$,*

$$N_1^-(gh) = N_1^-(g) + N_1^-(h), \quad R_{\lambda,1}(gh) = R_{\lambda,1}(g)R_{\lambda,1}(h).$$

The sum of two polygons is the polygon obtained by taking as (left) starting point the vector sum of the two (left) starting points, and then joining to this starting point the sides of both polygons by increasingly ordered slopes. For instance, the next picture shows the sum of two one-sided polygons of respective slope -2 and $-1/2$.



Notation. Given a field $\mathcal{F}$ and two polynomials $\varphi(y), \psi(y) \in \mathcal{F}[y]$, we write $\varphi(y) \sim \psi(y)$ to indicate that there exists a constant $c \in \mathcal{F}^*$ such that $\varphi(y) = c\psi(y)$.

Theorem of the polygon [**HN08**, Theorem 1.15]**.** *Let $f(x)$, ψ_0, ϕ_1, $F_{\mathbf{t}}(x)$, N be as above. Then,*

(1) *The polynomial $F_{\mathbf{t}}(x)$ factorizes in $\mathcal{O}[x]$ as:*

$$F_{\mathbf{t}}(x) = \prod\nolimits_{\lambda \in \mathrm{Slopes}(N)} F_\lambda(x), \quad \deg F_\lambda = \ell(S_\lambda(N))m_1,$$

for some monic polynomials $F_\lambda(x) \in \mathcal{O}[x]$, whose Newton polygon $N_1(F_\lambda)$ is one-sided with slope λ, and $R_{\lambda,1}(F_\lambda) \sim R_{\lambda,1}(f)$ in $\mathbb{F}_1[y]$.

(2) *For any root $\theta \in K^{\mathrm{sep}}$ of F_λ, we have $v(\phi_1(\theta)) = |\lambda|$.*

Theorem of the residual polynomial [**HN08**, Theorem 1.19]**.** *With the same notation, let $\lambda \in \mathrm{Slopes}(N)$ and let*

$$R_{\lambda,1}(f)(y) \sim \prod_{\psi} \psi(y)^{\ell_\psi},$$

be the factorization of $R_{\lambda,1}(f)$ into a product of powers of pairwise different monic irreducible polynomials $\psi \in \mathbb{F}_1[y]$. Denote $f_\psi := \deg \psi$. Then, $F_\lambda(x)$ factorizes in $\mathcal{O}[x]$ as:

$$F_\lambda(x) = \prod\nolimits_{\psi} F_{\lambda,\psi}(x), \quad \deg F_{\lambda,\psi} = \ell_\psi e_\lambda f_\psi m_1,$$

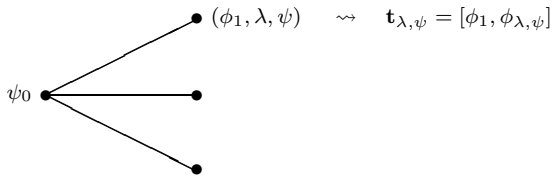
for some monic polynomials $F_{\lambda,\psi}(x) \in \mathcal{O}[x]$ such that $R_{\lambda,1}(F_{\lambda,\psi})(y) \sim \psi(y)^{\ell_\psi}$ in $\mathbb{F}_1[y]$.

This theorem is a kind of *Hensel lemma in order one*.

2.4. Initial branching of types. The theorems of Ore detect a (never computed) factorization of $F_{\mathbf{t}}(x)$ in $\mathcal{O}[x]$:

$$F_{\mathbf{t}}(x) = \prod_{\lambda,\psi} F_{\lambda,\psi}(x).$$

The different (unknown) factors $F_{\lambda,\psi}$ are parameterized by certain *types of order one*. We can think that the root node ψ_0 of our tree, sprouts several branches with end nodes labelled by the different triples $(\phi_1(x), \lambda, \psi(y))$.



Each node determines a type of order one, $\mathbf{t}_{\lambda,\psi} = [\phi_1, \phi_{\lambda,\psi}]$, just by constructing a monic separable polynomial $\phi_{\lambda,\psi}(x) \in \mathcal{O}[x]$ satisfying:

$$\deg \phi_{\lambda,\psi} = e_\lambda f_\psi m_1, \quad R_{\lambda,1}(\phi_{\lambda,\psi}) \sim \psi.$$

At the end of the paragraph we show how to construct $\phi_{\lambda,\psi}$. The positive integer $e_\lambda f_\psi m_1$ is the minimal degree of a polynomial satisfying $R_{\lambda,1}(\phi_{\lambda,\psi}) \sim \psi$; hence, by the Theorem of the product, any such polynomial $\phi_{\lambda,\psi}$ is necessarily irreducible in $\mathcal{O}[x]$.

If $\ell_\psi = 1$, the same argument shows that $F_{\lambda,\psi}$ is irreducible; in this case, the node $\mathbf{t}_{\lambda,\psi}$ becomes a leave of the tree of types, and $\phi_{\lambda,\psi}$ is an approximation to $F_{\lambda,\psi}$.

If $\ell_\psi > 1$ we need to analyze the node $\mathbf{t}_{\lambda,\psi}$ to detect further factorizations of $F_{\lambda,\psi}$, or show that it is irreducible. To this end, it will be necessary to extend the fundamental results of Ore to *order two*. Once we focus our attention on a fixed type $\mathbf{t}_{\lambda,\psi}$, we rename:

$$\lambda_1 := \lambda, \quad \psi_1 := \psi, \quad \phi_2 := \phi_{\lambda,\psi}, \quad R_1 := R_{\lambda_1,1}.$$

The type of order one, $\mathbf{t} := \mathbf{t}_{\lambda,\psi} = [\phi_1, \phi_2]$, keeps the data at level zero described in (2), and supports several data and operators at level one:

$$\begin{aligned}
&\phi_1(x) \in \mathcal{O}[x],\\
&m_1 := \deg \phi_1,\\
&N_1 \colon \mathcal{O}[x] \longrightarrow 2^{\mathbb{R}^2},\\
&\lambda_1 = -h_1/e_1, \quad h_1, e_1 \text{ positive coprime integers},\\
&R_1 \colon \mathcal{O}[x] \longrightarrow \mathbb{F}_1[y],\\
&\psi_1(y) \in \mathbb{F}_1[y],\\
&f_1 := \deg \psi_1,\\
&\mathbb{F}_2 := \mathbb{F}_1[y]/(\psi_1(y)),\\
&z_1 := \text{class of } y \text{ in } \mathbb{F}_2.
\end{aligned}$$

Note that $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2$, and $\mathbb{F}_2 = \mathbb{F}_1[z_1] = \mathbb{F}_0[z_0, z_1]$.

By the Theorem of the product, all irreducible factors F of the new polynomial $F_{\mathbf{t}} := F_{\lambda,\psi}$, satisfy:

$$R_0(F)(y) = \psi_0(y)^{\ell_0(F)} \text{ in } \mathbb{F}_0[y],$$
$$N_1(F) \text{ is one-sided with slope } \lambda_1,$$
$$R_1(F)(y) \sim \psi_1(y)^{\ell_1(F)} \text{ in } \mathbb{F}_1[y],$$

for some positive integers $\ell_0(F)$, $\ell_1(F)$. These properties motivate the use of the term *type*. A type is an object that collects some arithmetic features of irreducible polynomials. The polynomials that have these properties are of a certain "type". The last polynomial of a type is some sort of minimal object having these features; it is also called a *representative* of the type. Let us show how these representatives are constructed.

Construction of the polynomials $\boldsymbol{\phi_{\lambda,\psi}}$. Let us denote for a while:

$$e := e_\lambda, \quad h := h_\lambda, \quad f := f_\psi = \deg \psi.$$

Suppose that $\psi(y) = \epsilon_0 + \epsilon_1 y + \cdots + \epsilon_{f-1} y^{f-1} + y^f \in \mathbb{F}_1[y]$. The polynomial $\phi_{\lambda,\psi}(x)$ we are looking for can be taken of the form:

$$\pi^{hf} a_0(x) + \pi^{h(f-1)} a_e(x)\phi_1(x)^e + \cdots + \pi^{h(f-k)} a_{ek}(x)\phi_1(x)^{ek} + \cdots + \phi_1(x)^{ef},$$

with $R_0(a_{ek})(z_0) = \epsilon_k$, for all $0 \le k < f$.

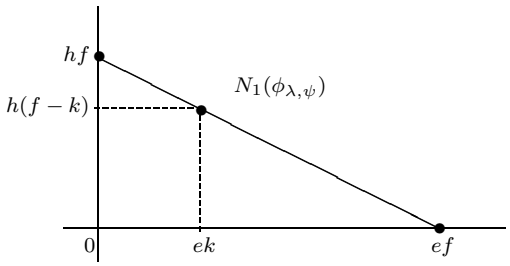
The condition on $a_{ek}(x)$ is easy to fulfill: if $\epsilon_k = 0$ we take $a_{ek}(x) = 0$, whereas for

$$\epsilon_k = u_0 + u_1 z_0 + \cdots + u_{f_0-1} z_0^{f_0-1} \in \mathbb{F}_1^*,$$

with $u_i \in \mathbb{F}_0$, we simply take arbitrary liftings of the u_i to $\mathcal{O}$ (which we denote by the same symbol $u_i \in \mathcal{O}$), and take

$$a_{ek}(x) = u_0 + u_1 x + \cdots + u_{f_0-1} x^{f_0-1} \in \mathcal{O}[x].$$

The Newton polygon of $\phi_{\lambda,\psi}$ is:



Remark. The definition of type, as presented here, is slightly different from the original definition given in [**HN08**], where the types carry exactly the same data and operators but no representative is chosen. Thus, a type in this survey is what in the language of [**HN08**] would be "a type plus the choice of a representative".

2.5. Types of order r.

Definition. A type of order zero is a list $[\phi_1]$ that consists of a single monic polynomial $\phi_1(x) \in \mathcal{O}[x]$, which is irreducible modulo $\mathfrak{m}$.

As we saw in the preceding sections, such an object determines operators N_1, $R_{\lambda,1}$ (for λ a negative rational number) that satisfy three fundamental results, collected in Section 2.3.

Definition. Let $r \geq 1$ be an integer, and $\mathbf{t} = [\phi_1, \dots, \phi_{r+1}]$ a family of monic irreducible separable polynomials in $\mathcal{O}[x]$. We say that $\mathbf{t}$ is a *type of order* r if it satisfies the following properties:

(1) $[\phi_1, \dots, \phi_r]$ is a type of order $r-1$.
(2) $N_r(\phi_{r+1})$ is one-sided with negative slope (say) λ.
(3) $R_{\lambda,r}(\phi_{r+1})(y) \in \mathbb{F}_r[y]$ is an irreducible polynomial.
(4) $\deg \phi_r \mid \deg \phi_{r+1}$.

If $\mathbf{t}$ satisfies these conditions, we add two fundamental invariants at level r:

$$\lambda_r := \text{slope of } N_r(\phi_{r+1}),$$
$$\psi_r(y) \in \mathbb{F}_r[y] \text{ monic such that } R_{\lambda_r,r}(\phi_{r+1}) \sim \psi_r.$$

Altogether, the type supports the following invariants and operators at level r:

$$\phi_r(x) \in \mathcal{O}[x],$$
$$m_r := \deg \phi_r,$$
$$N_r \colon \mathcal{O}[x] \longrightarrow 2^{\mathbb{R}^2},$$
$$\lambda_r = -h_r/e_r, \quad h_r,\ e_r \text{ positive coprime integers},$$
$$R_r := R_{\lambda_r,r} \colon \mathcal{O}[x] \longrightarrow \mathbb{F}_r[y],$$
$$\psi_r(y) \in \mathbb{F}_r[y],$$
$$f_r := \deg \psi_r,$$
$$\mathbb{F}_{r+1} := \mathbb{F}_r[y]/(\psi_r(y)),$$
$$z_r := \text{class of } y \text{ in } \mathbb{F}_{r+1},$$

so that $\psi_r(z_r) = 0$ and $\mathbb{F}_{r+1} = \mathbb{F}_r[z_r] = \mathbb{F}_0[z_0, \dots, z_r]$.

In order to have a coherent definition, it is necessary to show that if $\mathbf{t}$ satisfies these properties, then $\mathbf{t}$ determines a Newton polygon operator of order $r+1$,

$$N_{r+1}\colon \mathcal{O}[x] \longrightarrow 2^{\mathbb{R}^2},$$

and residual polynomial operators of order $r+1$, for each $\lambda \in \mathbb{Q}^-$:

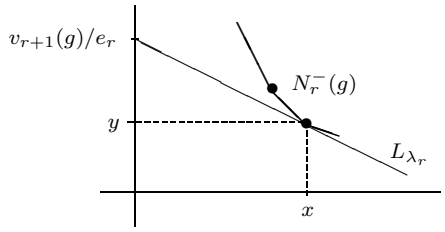
$$R_{\lambda,r+1}\colon \mathcal{O}[x] \longrightarrow \mathbb{F}_{r+1}[y],$$

satisfying analogous results to the three fundamental theorems of Ore.

The first (and essential) step is to construct a discrete valuation v_{r+1} of $K(x)$. Let us describe how it acts on polynomials. Given $g(x) \in K[x] \setminus \{0\}$, we compute $N := N_r^-(g)$ and we take any point $(x,y) \in N$ such that $y + x|\lambda_r|$ is minimal. Then, we define:

$$v_{r+1}(g) := e_r(y + x|\lambda_r|).$$

The following picture illustrates the situation. The line L_{λ_r} is the line of slope λ_r having first contact with N from below.



Note that v_{r+1} depends only on v_r, ϕ_r and λ_r. In MacLane's terminology, ϕ_r is a *key polynomial* over v_r and v_{r+1}/e_r is the *augmented valuation* attached to the pair $(\phi_r, v_r(\phi_r) + |\lambda|)$ [**McL36**, Section 4].

Once we have the discrete valuation v_{r+1}, we can define a Newton polygon operator of order $r+1$ as before. If $g(x) = \sum_{0\le s} a_s(x)\phi_{r+1}(x)^s$ is the ϕ_{r+1}- expansion of a polynomial $g(x)$, then $N_{r+1}(g) := N_{\phi_{r+1},v_{r+1}}(g)$ is defined as the lower convex hull of the set of points (s,u_s), where $u_s := v_{r+1}(a_s\phi_{r+1}^s)$.

Note that the ordinates of the points incorporate $v_{r+1}(\phi_{r+1}^s)$, which is a positive integer. This is necessary to keep the property:

$$\ell(N_{r+1}^-(g)) = \operatorname{ord}_{\psi_r}(R_r(g)).$$

In order one (for $r=0$), we had $v_1(\phi_1) = 0$, because ϕ_1 is monic; thus, the definition of N_1 is coherent with the general definition of the Newton polygons N_r for all $r \ge 1$.

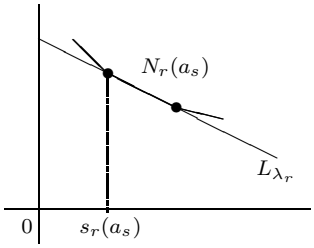
The residual operators of order $r+1$ are defined in a completely analogous way, except for the fact that the residual coefficients of $N := N^-_{r+1}(g)$ need to be twisted by certain powers of z_r. More precisely, for each integer abscissa s in the projection of N over the horizontal axis, we define

$$c_s := \begin{cases} 0, & \text{if } (s, u_s) \text{ lies above } N, \\ z_r^{t_s} R_r(a_s)(z_r) \in \mathbb{F}^*_{r+1}, & \text{if } (s, u_s) \text{ lies on } N. \end{cases}$$

The exponent t_s is defined to be:

$$t_s := \left(s_r(a_s) - h_r^{-1} u_s\right)/e_r,$$

where h_r^{-1} is any integer satisfying: $h_r^{-1} h_r \equiv 1 \pmod{e_r}$, and $s_r(a_s)$ is the abscissa of the left end point of the segment $S_{\lambda_r}(N_r(a_s))$.



With some effort, one is able to prove results completely analogous to the three fundamental results of Ore; that is, Theorems of the product, of the polygon and of the residual polynomial in order r [**HN08**, Sections 2 and 3].

Definition. Let $\mathbf{t}$ be a type of order r. For any $g(x) \in \mathcal{O}[x]$ we define

$$\operatorname{ord}_{\mathbf{t}}(g) := \operatorname{ord}_{\psi_r} R_r(g) = \ell(N^-_{r+1}(g)).$$

Also, we say that $\mathbf{t}$ is *g-complete* if $\operatorname{ord}_{\mathbf{t}}(g) = 1$.

By the Theorem of the product, this operator $\operatorname{ord}_{\mathbf{t}}$ behaves well with respect to products:

$$\operatorname{ord}_{\mathbf{t}}(gh) = \operatorname{ord}_{\mathbf{t}}(g) + \operatorname{ord}_{\mathbf{t}}(h),$$

for any pair of polynomials $g(x), h(x) \in \mathcal{O}[x]$.

2.6. Back to the factorization algorithm. Along the factorization algorithm with input polynomial $f(x) \in \mathcal{O}[x]$, we construct types such that $\operatorname{ord}_{\mathbf{t}}(f)$ is positive. This means that there is some irreducible factor $F(x)$ of $f(x)$ in $\mathcal{O}[x]$, for which $\operatorname{ord}_{\mathbf{t}}(F) > 0$, and this implies that F has the features captured by the type $\mathbf{t}$:

- $N_i(F)$ is one-sided with slope λ_i, $\quad \forall\, 1 \le i \le r$,
- $R_i(F) \sim \psi_i^{\ell_i(F)}$, $\quad \forall\, 0 \le i \le r$.

We denote by $F_{\mathbf{t}}(x) \in \mathcal{O}[x]$ the (unknown) product of all monic irreducible factors F of f such that $\mathrm{ord}_{\mathbf{t}}(F) > 0$; this notation is coherent with the previous way to consider $F_{\mathbf{t}}$ as an (unknown) factor of $f(x)$ detected by Hensel lemma or the results of Ore.

If $\mathbf{t}$ is f-complete, then $F_{\mathbf{t}}$ is already irreducible, and the node corresponding to $\mathbf{t}$ is a leave of the tree of types. If $\mathbf{t}$ is not f-complete, that is, $\mathrm{ord}_{\mathbf{t}}(f) > 1$, it is clear that the extension of Ore's results to order r determines a completely analogous branching of the node of the tree $\mathcal{T}$ that corresponds to $\mathbf{t}$.

As we did in Section 2.4, a node at level r is labelled by the triple $(\phi_r, \lambda_r, \psi_r)$ of fundamental invariants at level r. The type determined by this node is obtained by gathering all levels of all nodes that belong to the unique path joining our node to the root node of the tree.

The polynomial $\phi_{\lambda,\psi}$ that is a representative of the type is constructed by applying in a recursive way the procedure described at the end of Section 2.4. However, at order $r > 1$ one has to care about the powers of z_r that twist the residual coefficients of the polygons [**HN08**, Section 2.3].

2.7. Special features of the Theorem of the polygon in order r.

Proposition. *Suppose* $\mathrm{ord}_{\mathbf{t}}(f) > 0$ *and let* $\theta \in K^{\mathrm{sep}}$ *be a root of* $F_{\mathbf{t}}$. *Then, for any polynomial* $g(x) \in \mathcal{O}[x]$,

$$v_{r+1}(g) \le e_1 \cdots e_r\, v(g(\theta)), \tag{3}$$

and equality holds if and only if $\mathrm{ord}_{\mathbf{t}}(g) = 0$.

Hence, $v_{r+1}/e_1 \cdots e_r$ may be considered an approximation of the valuation v on the finite extension $K(\theta)/K$. The formula for the value of $v(\phi_{r+1}(\theta))$ given by the Theorem of the polygon gives an interpretation of the slopes of $N^-_{r+1}(f)$ as a measure of the inequality of (3), for the polynomial ϕ_{r+1}. More precisely, for any root $\theta \in K^{\mathrm{sep}}$ of the factor F_λ of $F_{\mathbf{t}}$ determined by some $\lambda \in \mathrm{Slopes}(N^-_{r+1}(f))$, the Theorem of the polygon states that:

$$v(\phi_{r+1}(\theta)) = \frac{v_{r+1}(\phi_{r+1}) + |\lambda|}{e_1 \cdots e_r},$$

or equivalently:

$$e_1 \cdots e_r\, v(\phi_{r+1}(\theta)) - v_{r+1}(\phi_{r+1}) = |\lambda|.$$

2.8. Computation of the residue class fields of the extensions determined by the irreducible factors. If the type $\mathbf{t}$ of order r is f-complete, then the field $\mathbb{F}_{r+1}$ is a computational representation of the residue class field of the (unknown) irreducible factor F singled out by $\mathbf{t}$. If $\theta \in K^{\text{sep}}$ is a root of F, $L = K(\theta)$ and $\mathbb{F}_L$ is the residue class field, there is an explicit isomorphism:

$$\gamma\colon \mathbb{F}_{r+1} = \mathbb{F}_0[z_0, \dots, z_r] \longrightarrow \mathbb{F}_L, \quad z_i \mapsto \overline{\gamma_i(\theta)},$$

where $\gamma_i(x) \in K(x)$ are certain rational functions that can be expressed as a product of a power of π and powers of the ϕ polynomials of $\mathbf{t}$ with integer (positive or negative) exponents [**HN08**, Section 2.4 and (36)]:

$$\gamma(x) = \pi^{n_0} \prod_{i=1}^{r} \phi_i(x)^{n_i}, \quad n_i \in \mathbb{Z}.$$

The computation of these rationals functions would be inefficient, so that along the flow of the algorithm only the integer exponents n_i are computed and stored, which is sufficient for all the applications where the residue class field $\mathbb{F}_L$ is involved.

2.9. Higher order indices. Why does this process terminate? Why all types become complete after a finite number of steps? Answer: because each node "swallows" a positive (and big!) integer portion of the absolute index of $f(x)$ [**HN08**, Section 4].

Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial, $L = K(\theta)$, where $\theta \in K^{\text{sep}}$ is a root of F, and $\mathcal{O}_L$ the ring of integers. The *index* $\operatorname{ind}(F)$ is defined as:

$$\operatorname{ind}(F) := \operatorname{length}_{\mathcal{O}}(\mathcal{O}_L/\mathcal{O}[\theta]).$$

Recall the well-known relationship: $v(\operatorname{disc}(F)) = 2\operatorname{ind}(F) + v(\operatorname{disc}(L/K))$.

Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial, and $f = F_1 \cdots F_g$ its factorization into a product of monic irreducible polynomials in $\mathcal{O}[x]$. Let $\mathcal{O}_f := \mathcal{O}[x]/(f(x))$. The index of f is by definition:

$$\operatorname{ind}(f) := \operatorname{length}_{\mathcal{O}}\left((\mathcal{O}_f)^{\sim}/\mathcal{O}_f\right) = \sum_{j=1}^{g} \operatorname{ind}(F_j) + \sum_{1 \le j < k \le g} v(\operatorname{Res}(F_j, F_k)),$$

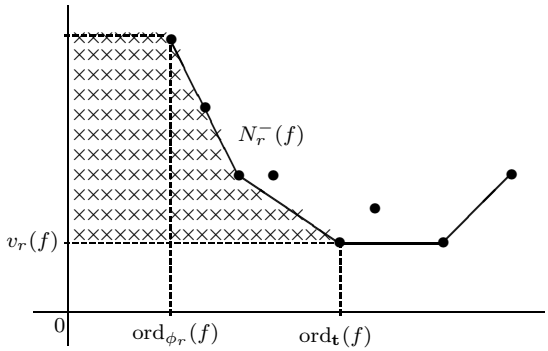
where the superscript $(\ )^{\sim}$ indicates "integral closure".

Now, for each $\mathbf{t} \in \mathcal{T}$, we define:

$$\operatorname{ind}_{\mathbf{t}}(f) := f_0 f_1 \cdots f_r \operatorname{ind}(N^{-}_{r+1}(f)),$$

where r is the order of $\mathbf{t}$ and, for any polygon N, $\operatorname{ind}(N)$ is the number of points of integer coordinates that lie below or on N and the horizontal

line passing through the (left) starting point of N, beyond the vertical axis and above the horizontal line having first contact with N from below.



Theorem. *Let $\mathcal{T}$ be the tree of types considered at any stage of Montes algorithm. Then,*

$$\sum_{\mathbf{t}\in\mathcal{T}} \mathrm{ind}_{\mathbf{t}}(f) \le \mathrm{ind}(f).$$

If all leaves of $\mathcal{T}$ are f-complete, then equality holds.

Corollary.

(1) *The factorization algorithm ends after a finite number of steps.*

(2) *It computes* $\mathrm{ind}(f)$ *as a by-product.*

It is not absolutely true that $\mathrm{ind}_{\mathbf{t}}(f)$ is always positive. However, if for some node $\mathbf{t}$ we have $\mathrm{ind}(N_r^-(f)) = 0$, then this polygon is one-sided and the projection of this side either to the horizontal or to the vertical axis has length one; hence, $\mathbf{t}$ is either complete, or it becomes complete after a unibranch step.

2.10. Optimization of Montes algorithm.

Definition. The type $\mathbf{t} = [\phi_1, \dots, \phi_{r+1}]$ of order r is called *optimal* if either $r = 0$ or $\deg\phi_1 < \cdots < \deg\phi_r$. It is called *strongly optimal* if either $r = 0$ or $\deg\phi_1 < \cdots < \deg\phi_r < \deg\phi_{r+1}$.

Montes algorithm is optimized in such a way that all nodes of the tree of types, except for the leaves, are strongly optimal. Hence, by the very definition, all nodes of the tree, including the leaves, are optimal.

Let us sketch the ideas of the optimization process. Suppose a node of the tree, $\mathbf{t} = [\phi_1, \dots, \phi_r]$ of order $r-1$, is strongly optimal and non-complete. Then, in principle, several branches sprout from $\mathbf{t}$, labelled

by triples (ϕ_r, λ, ψ), where λ is one of the slopes of $N_r^-(f)$ and ψ is one of the irreducible factors of $R_{\lambda,r}(f)$. For each one of these branches let us write,

$$\lambda = -h_\lambda/e_\lambda, \quad f_\psi := \deg \psi, \quad m_{\lambda,\psi} := e_\lambda f_\psi m_r,$$

where e_λ, h_λ are positive coprime integers. Denote by $\phi_{\lambda,\psi}$ the $(r+1)$-th ϕ-polynomial of degree $m_{\lambda,\psi}$ constructed by the general method, as explained in Section 2.6. The type

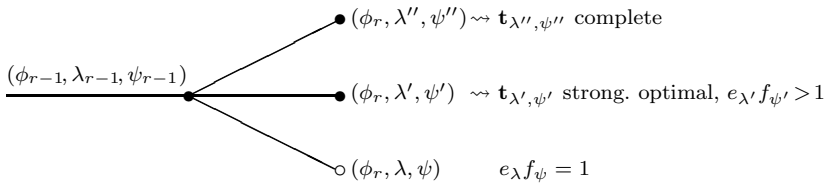
$$\mathbf{t}_{\lambda,\psi} := [\phi_1, \ldots, \phi_r, \phi_{\lambda,\psi}]$$

would correspond to a new node of order r if no optimization were applied. Now there are three different possibilities for each branch:

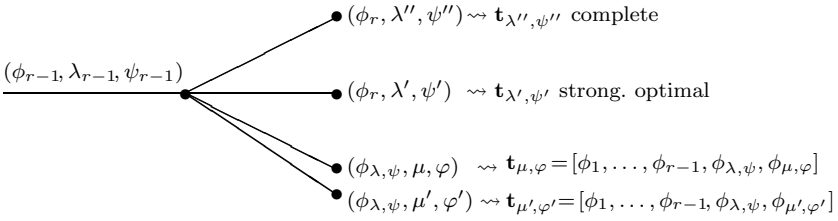
(a) The type $\mathbf{t}_{\lambda,\psi}$ is complete. In this case, $\mathbf{t}_{\lambda,\psi}$ is a leave of the tree.

(b) The type $\mathbf{t}_{\lambda,\psi}$ is not complete, and $e_\lambda f_\psi > 1$. Then, $\mathbf{t}_{\lambda,\psi}$ is strongly optimal and it corresponds to a new node of order r of the tree.

(c) The type $\mathbf{t}_{\lambda,\psi}$ is not complete, and $e_\lambda f_\psi = 1$. In this case, $\mathbf{t}_{\lambda,\psi}$ is not strongly optimal.



Suppose $\mathbf{t}_{\lambda,\psi}$ falls in case (c). Then, the polynomial $\phi_{\lambda,\psi}$ is a better representative of the original type $\mathbf{t}$ than ϕ_r; thus, we consider the order $r-1$ type, $\mathbf{t}' = [\phi_1, \ldots, \phi_{r-1}, \phi_{\lambda,\psi}]$, and we submit it to further branching, but taking into account only slopes strictly less than λ (instead of strictly less than 0) in the Newton polygon $N_{\mathbf{t}',r}(f)$. The branches that arose from $\mathbf{t}'$ are supposed to sprout as well from the initial node labeled with $(\phi_{r-1}, \lambda_{r-1}, \psi_{r-1})$. Each one of these new branches falls in case (a), (b) or (c) and we follow the same procedure accordingly.



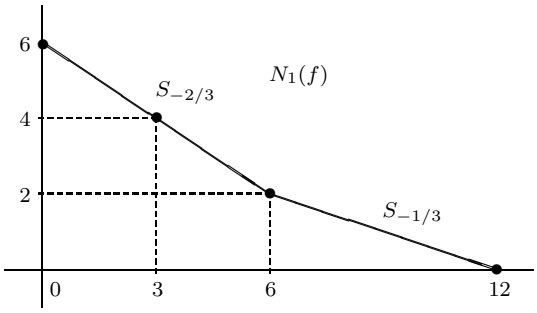
We call this replacement of the order r type $\mathbf{t}_{\lambda,\psi}$ by the order $r-1$ type $\mathbf{t}'$, a *refinement step* [**GMN08**, Section 3]. Since all computations $(v_r,\ N_r,\ R_r,\dots)$ are of a recursive nature, to proceed in order $r-1$ instead of order r causes a considerable improvement of the complexity.

Note that the leaves of the tree, as nodes of complete branches, are not necessarily strongly optimal (in case (a) $e_\lambda f_\psi$ can be indistinctly equal to or greater than one). There will appear non-strongly optimal leaves, for instance, if there are irreducible factors of $f(x)$ that are one an *Okutsu approximation* to the other. In any case, the optimized algorithm always outputs f-complete and optimal types. Curiosly enough, this optimization motivated by pure practical reasons, provides the output of Montes algorithm with unexpected canonical properties.

The concept of Okutsu appoximation and the canonical properties of the output data of Montes algorithm will be discussed in Section 3.

2.11. An example. Let us show how the algorithm works with an example. Take $f(x)=x^{12}+4x^6+16x^3+64\in\mathbb{Z}_2[x]$.

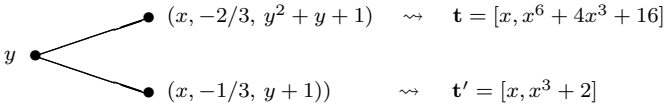
Since $f(x)\equiv x^{12} \pmod 2$, the tree of types will be connected and we can take $\psi_0(y)=y$, $\mathbf{t}_0=[x]$, as the root node. The Newton polygon of first order of $f(x)$ has two sides, with slopes $-2/3$ and $-1/3$, and $\mathrm{ind}_{\mathbf{t}_0}(f)=\mathrm{ind}(N_1(f))=23$.



The residual polynomials of the first order are:

$$R_{-2/3,1}(f)(y)=y^2+y+1,\quad R_{-1/3,1}(f)(y)=(y+1)^2.$$

The type $\mathbf{t}_0$ ramifies into two types of order one, with edges labelled by:

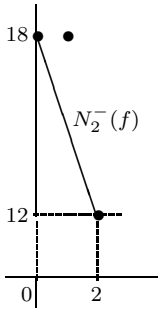


The type $\mathbf{t}$ is complete, and it singles out an (unknown) irreducible factor $F(x) \in \mathbb{Z}_2[x]$; let $L/\mathbb{Q}_2$ be the finite extension determined by F. We can apply (1) to get $e(L/\mathbb{Q}_2) = 3$, $f(L/\mathbb{Q}_2) = 2$. Also, we get an Okutsu approximation $x^6 + 4x^3 + 16$, to F.

The type $\mathbf{t}'$ is not complete: $\mathrm{ord}_{\mathbf{t}'}(f) = \mathrm{ord}_{\psi_1} R_1(f) = 2$, so that some more work in order two is required. Denote $\phi_2(x) = x^3 + 2$. We know that $N_2^-(f)$ will have length 2; hence, in order to compute this polygon we need only to compute the three last terms of the ϕ_2-adic development of $f(x)$:

$$f(x) = \phi_2(x)^4 + \cdots + 28\phi_2(x)^2 - 32\phi_2(x) + 64.$$

We have $v_2(\phi_2) = v_2(2) = 3$, so that $v_2(64) = 18$, $v_2(-32\phi_2(x)) = 18$, and $v_2(28\phi_2(x)^2) = 12$. The Newton polygon of second order has slope $\lambda := -3$ and residual polynomial of second order $R_{\lambda,2}(f)(y) = y^2 + 1 = (y+1)^2$, a power of $\psi(y) := y + 1$. Also, $\mathrm{ind}_{\mathbf{t}'}(f) = 3$.



We want now to construct a polynomial $\phi_{\lambda,\psi}$ of minimal degree satisfying:

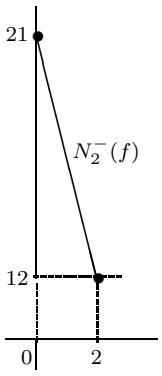
$$N_2(\phi_{\lambda,\psi}) \text{ one-sided with slope } -3, \quad R_{\lambda,2}(\phi_{\lambda,\psi}) \sim \psi.$$

Since $e_\lambda = f_\psi = 1$, this polynomial $\phi_{\lambda,\psi}$ will have again degree 3; we can take $\phi_{\lambda,\psi}(x) = x^3 + 6$. For the sake of optimization, instead of considering the (non-complete, non-strongly optimal) type $[x, x^3+2, x^3+6]$ of order 2, whose further enlargements will require to work in order 3, we replace the type $\mathbf{t}'$ by the type $\mathbf{t}'' = [x, x^3+6]$ of order 1. In this way,

our next work will be done still in order 2. If we now take $\phi_2(x) := x^3+6$, the last three terms of the ϕ_2-adic development of $f(x)$ are:

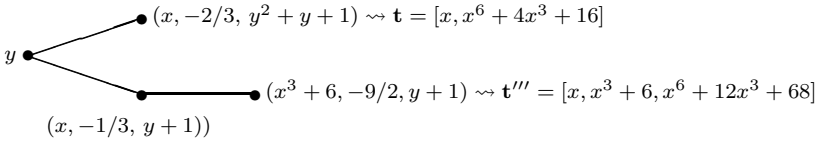
$$f(x) = \phi_2(x)^4 + \cdots + 220\phi_2(x)^2 - 896\phi_2(x) + 1408.$$

We have now $v_2(1408) = 21$, $v_2(896\phi_2) = 24$, $v_2(220\phi_2^2) = 12$, so that $N_2^-(f)$ is one-sided with slope $-9/2$:



and $\mathrm{ind}_{\mathbf{t}''}(f) = \mathrm{ind}(N_2^-(f)) = 4$. The residual polynomial of second order is already irreducible: $R_{-9/2,2}(f)(y) = y+1$. Thus, $\mathbf{t}''$ is extended to a unique type of order two: $\mathbf{t}''' = [x, x^3+6, x^6+12x^3+68]$, which is already complete. It singles out another irreducible factor $G(x) \in \mathbb{Z}_2[x]$; let $M/\mathbb{Q}_2$ be the corresponding extension. By (1) we get $e(M/\mathbb{Q}_2) = 6$, $f(M/\mathbb{Q}_2) = 1$, and we have computed an Okutsu approximation $x^6 + 12x^3 + 68$, to $G(x)$.

The final tree $\mathcal{T}$ of types is:



The total index is equal to: $\mathrm{ind}(f) = \mathrm{ind}_{\mathbf{t}_0}(f) + \mathrm{ind}_{\mathbf{t}''}(f) = 23+4 = 27$.

3. Okutsu frames and optimal types

As in the last section, we fix a local field K with perfect residue field. Let $\mathcal{O}$ be the ring of integers, $\mathfrak{m}$ the maximal ideal, and $\pi \in \mathfrak{m}$ a uniformizer. Let $v\colon \overline{K}^* \longrightarrow \mathbb{Q}$, be the canonical extension of the

discrete valuation of K to an algebraic closure, with the usual normalization $v(K^*) = \mathbb{Z}$. Let $K^{\rm sep} \subset \overline{K}$ be the separable closure of K in $\overline{K}$. For any $\eta \in \overline{K}$ we denote $\deg \eta := [K(\eta)\colon K]$.

All results of this section are extracted from [**GMN09**], which is a revision and extension of the original paper by Okutsu [**Oku82**].

3.1. Okutsu frames. Let us fix a monic irreducible separable polynomial $F(x) \in \mathcal{O}[x]$, of degree n. Let $\theta \in K^{\rm sep}$ be a root of $F(x)$, $L = K(\theta)$, and $\mathcal{O}_L$ the ring of integers.

Denote $\mu_0 := 0$, $m_0 := 1$, and consider sequences, respectively of positive integers and non-negative rational numbers:

$$0 < m_1 < m_2 < \cdots < m_R < m_{R+1} := n,$$
$$0 < \mu_1 < \mu_2 < \cdots < \mu_R < \mu_{R+1} := \infty,$$

defined, for $i \geq 1$, as follows:

$$m_i := \min\left\{\deg \eta \;\middle|\; \eta \in \overline{K} \text{ satisfies } v(\theta - \eta) > \mu_{i-1}\right\},$$

$$\mu_i := \max\left\{v(\theta - \eta) \text{ among all } \eta \in \overline{K} \text{ of degree } m_i\right\}.$$

We can choose separable integral elements $\alpha_i \in K^{\rm sep}$ satisfying

$$\deg \alpha_i = m_i, \quad v(\theta - \alpha_i) = \mu_i, \quad \forall\, 1 \leq i \leq R.$$

Let $F_i(x) \in \mathcal{O}[x]$ be the minimal polynomial of α_i over K, and denote $K_i = K(\alpha_i)$, for all $1 \leq i \leq R$. The fields K_i are not necessarily subfields of L, but we shall see soon that their maximal tamely ramified subextensions over K are always contained in L.

Definition. The sequence $[F_1, \ldots, F_R]$ is called an *Okutsu frame* of F, and R is called the *Okutsu depth* of F.

Although the polynomials F_i are not uniquely determined, we must consider an Okutsu frame as an essentially canonical object attached to F.

Definition. An $\eta \in K^{\rm sep}$ such that $\deg \eta = n$ and $v(\theta - \eta) > \mu_R$ is called an *Okutsu approximation* to θ.

A monic irreducible separable polynomial $G(x) \in \mathcal{O}[x]$ is called an *Okutsu approximation* to F if $\deg G = n$ and $v(G(\theta)) > (n/m_R)v(F_R(\theta))$.

Remarks.

(1) The values $v(F_i(\theta))$, $1 \leq i \leq R$ are independent of the choice of the Okutsu frame [**GMN09**, Corollary 2.14].

(2) $\eta \in K^{\rm sep}$ is an Okutsu approximation to θ if and only if the minimal polynomial of η over K is an Okutsu approximation to $F(x)$ [**GMN09**, Lemma 2.12].

(3) The notion of Okutsu approximation determines an equivalence relation on $\mathcal{O}_{K^{\rm sep}}$, and on the set of monic irreducible separable polynomials in $\mathcal{O}[x]$ [**GMN09**, Lemma 4.3].

Exercises. The following facts are an immediate consequence of the definitions:

(1) $\mathrm{depth}(F) = 0$ if and only if F is irreducible modulo $\mathfrak{m}$.

(2) Suppose that $v(F(0)) = 0$ and let $[F_1, \dots, F_R]$ be an Okutsu frame of F. Let $G(x) := \pi^{nm} F(x/\pi^m)$, for some positive integer m. Then, $[x, F_1(x), \dots, F_R(x)]$ is an Okutsu frame of G, and $\mu_{i,G} = \mu_{i-1} + m$, for all $1 \le i \le R+1$.

(3) Let $E(x)$ be an Eisenstein polynomial. Then $[x]$ is an Okutsu frame of E, and $\mu_1 = 1/n$.

(4) Two Eisenstein polynomials of the same degree, E, E', are Okutsu approximations to each other if and only if $v(E(0) - E'(0)) > 1$.

Suppose that $\mathrm{depth}(F) = 0$ and take $G = \pi^n F(x/\pi)$. Let $E(x)$ be an Eisenstein polynomial of degree n. The polynomial E determines a totally ramified extension and the polynomial G determines an unramified extension. However, the exercises show that G and E have both $[x]$ as Okutsu frame. Hence, it has to be clear that an Okutsu frame is an object attached to an irreducible polynomial and it is by no means an invariant of the finite extension determined by this polynomial.

3.2. Okutsu invariants of finite extensions of K. In spite of what has been said, an Okutsu frame accompanied by an Okutsu approximation do contain a lot of information about the extension L/K and its subextensions.

All results of this section are extracted from [**GMN09**, Section 2.1]. We fix throughout the section an Okutsu frame $[F_1, \dots, F_R]$ of F.

Lemma. *Suppose that $\alpha, \eta \in K^{\rm sep}$ satisfy:*

$$v(\theta - \alpha) > \mu_{i-1}, \quad v(\theta - \eta) > \mu_{i-1},$$

for some $1 \le i \le R+1$. Then, for any polynomial $g(x) \in K[x]$ of degree less than m_i, we have

$$v(g(\eta) - g(\alpha)) > v(g(\alpha)).$$

Moreover, if $\deg \alpha = m_i$, then $e(K(\alpha)/K)$ divides $e(K(\eta)/K)$.

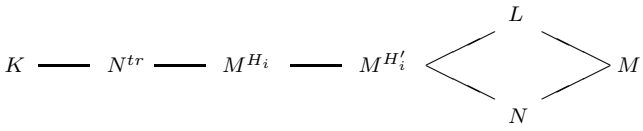
Proposition. *Suppose that* $\alpha \in K^{\mathrm{sep}}$ *satisfies*

$$\deg \alpha = m_i, \quad v(\theta - \alpha) = \mu_i,$$

for some $1 \le i \le R+1$. *Let* $N = K(\alpha)$, M/K *a finite Galois extension containing* L *and* N, *and* $G = \mathrm{Gal}(M/K)$. *Consider the subgroups:*

$$H_i := \{\sigma \in G \mid v(\theta - \sigma(\theta)) > \mu_{i-1}\} \supseteq H_i' := \{\sigma \in G \mid v(\theta - \sigma(\theta)) \ge \mu_i\},$$

and let $M^{H_i} \subset M^{H_i'} \subset M$ *be the respective fixed fields. Finally, let* N^{tr} *be the maximal tamely ramified subextension of* N/K. *Then,* $N^{tr} \subset M^{H_i} \subset M^{H_i'} \subset L \cap N$.



Corollaries. *Let* $K_i = K(\alpha_i)$, *for* $1 \le i \le R$.

(1) *The numbers* $e(K_i/K)$, $f(K_i/K)$, *do not depend on the chosen Okutsu frame.*

(2) $e(K_1/K) | \ldots | e(K_R/K) \mid e(L/K)$, *and* $f(K_1/K) \mid \ldots \mid f(K_R/K) \mid f(L/K)$. *In particular,* $m_1 \mid \cdots \mid m_R \mid n$.

(3) *The extension* K_1/K *is unramified and we have a chain of tamely ramified subfields of* L*:*

(4) *If* $G(x) \in \mathcal{O}[x]$ *is an Okutsu approximation to* F, *it admits a root* $\alpha \in K^{\mathrm{sep}}$ *such that the field* $K_{R+1} := K(\alpha)$ *satisfies:*

$$K_{R+1}^{tr} = L^{tr}, \quad e(K_{R+1}/K) = e(L/K), \quad f(K_{R+1}/K) = f(L/K).$$

(5) *If* L/K *is tamely ramified, then*

$$\{v(\theta - \sigma(\theta)) \mid \sigma \in G\} = \begin{cases} \{\mu_1, \ldots, \mu_R, \infty\}, & \text{if } m_1 = 1, \\ \{0, \mu_1, \ldots, \mu_R, \infty\}, & \text{if } m_1 > 1. \end{cases}$$

In particular, μ_R *is Krasner's radius of* $F(x)$*:*

$$\mu_R = \max\{v(\theta - \theta') \mid \theta, \theta' \in K^{\mathrm{sep}} \text{ roots of } F(x),\ \theta \ne \theta'\}.$$

Moreover, for each $0 \le i \le R$, *there are exactly* $(n/m_i) - (n/m_{i+1})$ *different roots* θ' *of* F *such that* $v(\theta - \theta') = \mu_i$.

One might speculate that the fields K_i in Corollary (3) may not be subfields of L, but they eventually detect the presence of subfields of L with given ramification index and residual degree. Jürgen Klüners provided us with an example showing that is not the case either.

Example (Klüners)**.** Let $F(x) = x^4 + 4x^2 - 4x + 4 \in \mathbb{Z}_2[x]$. This polynomial is separable, irreducible, and it determines a primitive extension L of $\mathbb{Q}_2$. Actually, the roots of F are the squares of the roots of the strongly Eisenstein polynomial $x^4 + 2x + 2$, whose Galois group is well-known. Now, it is easy to check that $[x, x^2 - 2]$ is an Okutsu frame of F, with Okutsu invariants $\mu_1 = 1/2$, $\mu_2 = 5/8$. Thus, the quadratic field $K_2 = \mathbb{Q}_2(\sqrt{2})$ does not correspond to any quadratic subfield of L. Even more, the normal closure of $L/\mathbb{Q}_2$ has a unique quadratic subextension, which is unramified, so that K_2 (which is totally ramified) cannot be connected to any quadratic subfield of this normal closure either.

3.3. Okutsu frames and integral closures. The next theorem shows a relevant property of the polynomials $F_i(x)$ that constitute an Okutsu frame of $F(x)$.

Theorem. *Take $F_0(x) = x$. For any integer $0 \le m < n$, express m in a unique way as:*

$$m = j_0 + j_1 m_1 + \cdots + j_R m_R, \quad 0 \le j_i < (m_{i+1}/m_i),$$

and consider the following polynomial of degree m:

$$g_m(x) := F_0(x)^{j_0} F_1(x)^{j_1} \cdots F_R(x)^{j_R}.$$

Then, for any polynomial $g(x) \in \mathcal{O}[x]$ of degree m we have,

$$v(g_m(\theta)) \ge v(g(\theta)) - v_1(g(x)).$$

Corollary ([**Oku82**, I, Theorem 1])**.** *If $\nu_m := \lfloor v(g_m(\theta)) \rfloor$, then*

$$1, \frac{g_1(\theta)}{\pi^{\nu_1}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\nu_{n-1}}}$$

is an $\mathcal{O}$-basis of $\mathcal{O}_L$.

3.4. Okutsu frames and optimal types.

Theorem. *Let $f(x) \in \mathcal{O}[x]$ be a monic and separable polynomial, $\mathbf{t} = [\phi_1, \ldots, \phi_{r+1}]$ an f-complete optimal type of order $r \ge 0$, and $F(x) \in \mathcal{O}[x]$ the monic irreducible factor of $f(x)$ singled out by $\mathbf{t}$. Then,*

(1) *The Okutsu depth of F is*

$$R = \begin{cases} r, & \text{if } e_r f_r > 1 \text{ or } r = 0, \\ r - 1, & \text{if } e_r f_r = 1 \text{ and } r > 0. \end{cases}$$

In the first case, $[\phi_1, \dots, \phi_r]$ *is an Okutsu frame of* F*, and* ϕ_{r+1} *is an Okutsu approximation to* F*. In the second case,* $[\phi_1, \dots, \phi_{r-1}]$ *is an Okutsu frame of* F*, and* ϕ_r*,* ϕ_{r+1} *are both Okutsu approximations to* F*.*

(2) $F(x) \equiv \phi_{r+1}(x) \pmod{\mathfrak{m}^\nu}$*, where*

$$\nu = \left\lceil \frac{h_1}{e_1} + \frac{h_2}{e_1 e_2} + \cdots + \frac{h_r}{e_1 \cdots e_r} + \frac{h_{r+1}}{e(L/K)} \right\rceil,$$

and $-h_{r+1}$ *is the slope of the one-sided Newton polygon* $N^-_{r+1}(f)$*.*

Remarks.

(1) The optimized Montes algorithm outputs an essentially canonical representation of the irreducible factors.

(2) The two last theorems justify the construction of local bases in terms of the output of Montes algorithm, as presented at the end of Section 1.1.

(3) The numerical invariants h_i, e_i, f_i, λ_i, for $1 \le i \le R$, and the discrete valuations $v_1, \dots, v_{R+1}$ are invariants of $F(x)$.

(4) In spite of the philosophy of Montes algorithm, that detects factorization but never computes it, the last polynomials of the output types are approximations to the irreducible factors, with a controlled precision. Therefore, the algorithm provides a factorization of the input polynomial indeed.

In a recent work with J. Guàrdia and S. Pauli [**GNP10**], we develop a *single-factor lifting* algorithm that improves each one of these approximations up to a prescribed precision. This algorithm has quadratic convergence.

4. Computation of integral closures in global fields

For simplicity, we discuss only the computation of the maximal order of a number field.

Let $K = \mathbb{Q}[x]/(f(x))$ be the number field defined by a monic irreducible polynomial $f(x)$ with integer coefficients and degree n. Let $\theta \in \overline{\mathbb{Q}}$ be a root of $f(x)$ and $\mathbb{Z}_K$ the ring of integers.

We already mentioned in Section 1.2 that an integral basis of K (i.e. a $\mathbb{Z}$-basis of $\mathbb{Z}_K$) can be computed by an standard application of the Chinese remainder theorem, from a family of p-integral bases in Hermite Normal Form, for all prime numbers p dividing $\mathrm{disc}(f)$.

In this section we deal with the computation of a p-integral basis for a given prime number: p. We saw in Section 1.2 that Montes algorithm attaches to each prime ideal $\mathfrak{p}$ of K lying over p an OM representation:

$$\mathfrak{p} = [p; \phi_{1,\mathfrak{p}}, \dots, \phi_{r,\mathfrak{p}}; \phi_{\mathfrak{p}}],$$

where $\phi_{\mathfrak{p}}$ is just the $(r+1)$-th polynomial of the f-complete and optimal type attached to the p-adic irreducible factor of $f(x)$ corresponding to $\mathfrak{p}$. The common feature of the two methods we are about to present is the computation of a p-integral basis in terms of the data encoded by these OM representations.

4.1. Standard OM method. Let $\mathcal{P}$ be the set of prime ideals of K dividing p. For each $\mathfrak{p} \in \mathcal{P}$, we fix a topological embedding

$$\iota_{\mathfrak{p}} \colon K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbb{Q}}_p.$$

Let $F_{\mathfrak{p}}(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial of $\iota_{\mathfrak{p}}(\theta)$ over $\mathbb{Q}_p$, and denote by $n_{\mathfrak{p}} = e(\mathfrak{p}/p)f(\mathfrak{p}/p)$, its degree.

Recall that Montes algorithm can be slightly modified to compute a $\mathbb{Z}_p$-basis of the local ring of integers $\mathbb{Z}_{K_{\mathfrak{p}}}$, for all $\mathfrak{p} \in \mathcal{P}$. Let us denote by:

$$\mathcal{B}_{\mathfrak{p}} = \left\{1, \frac{g_{1,\mathfrak{p}}(\theta)}{p^{\nu_{1,\mathfrak{p}}}}, \dots, \frac{g_{n_{\mathfrak{p}}-1,\mathfrak{p}}(\theta)}{p^{\nu_{n_{\mathfrak{p}}-1,\mathfrak{p}}}}\right\}, \quad \mathfrak{p} \in \mathcal{P},$$

the family of $n_{\mathfrak{p}}$ $\mathfrak{p}$-integral elements constructed as indicated in Section 3.3:

$$g_m(\theta) := \theta^{j_0}\phi_{1,\mathfrak{p}}(\theta)^{j_1} \cdots \phi_{R,\mathfrak{p}}(\theta)^{j_R},$$

so that $\iota_{\mathfrak{p}}(\mathcal{B}_{\mathfrak{p}})$ is an integral basis of the local extension $K_{\mathfrak{p}}/\mathbb{Q}_p$, for all $\mathfrak{p} \in \mathcal{P}$. The Theorem of the polygon provides an explicit computation of the exponents $\nu_{m,\mathfrak{p}} = \lfloor j_1 v(\phi_{1,\mathfrak{p}}(\theta)) + \cdots + j_R v(\phi_{R,\mathfrak{p}}(\theta))\rfloor$, in terms of the data of the OM representation of $\mathfrak{p}$ (see Section 2.7).

We compute then multipliers $\beta_{\mathfrak{p}} \in \mathbb{Z}_K$ satisfying:

$$v_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0, \quad v_{\mathfrak{q}}(\beta_{\mathfrak{p}}) \geq (\exp(F_{\mathfrak{p}}) + 1)e(\mathfrak{q}/p), \quad \forall\, \mathfrak{q} \in \mathcal{P},\, \mathfrak{q} \neq \mathfrak{p}. \tag{4}$$

Proposition ([**Ore25**]). *The family* $\bigcup_{\mathfrak{p}\in\mathcal{P}} \beta_{\mathfrak{p}}\mathcal{B}_{\mathfrak{p}}$ *is a* p*-integral basis of* K.

Proof: Let us denote

$$\alpha_{m,\mathfrak{p}} := \beta_{\mathfrak{p}} \frac{g_{m,\mathfrak{p}}(\theta)}{p^{\nu_{m,\mathfrak{p}}}}, \quad \forall\, 0 \leq m < n_{\mathfrak{p}}.$$

Since $v_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0$, the family of all $\iota_{\mathfrak{p}}(\alpha_{m,\mathfrak{p}})$, for $0 \leq m < n_{\mathfrak{p}}$, is still an integral basis of the local extension $K_{\mathfrak{p}}/\mathbb{Q}_p$. Although $g_{m,\mathfrak{p}}(\theta)/p^{\nu_{m,\mathfrak{p}}}$ is

not necessarily (globally) integral, the element $\alpha_{m,\mathfrak{p}}$ belongs to $\mathbb{Z}_K$ and, even more, it satisfies

$$v_{\mathfrak{q}}(\alpha_{m,\mathfrak{p}}) \geq e(\mathfrak{q}/p), \quad \forall\, \mathfrak{q} \in \mathcal{P},\, \mathfrak{q} \neq \mathfrak{p}. \tag{5}$$

In fact, this is an immediate consequence of (4), because $\nu_{m,\mathfrak{p}} \leq \nu_{n_{\mathfrak{p}}-1,\mathfrak{p}} = \exp(F_{\mathfrak{p}})$, for all m, $\mathfrak{p}$.

Let us check that $\{\alpha_{m,\mathfrak{p}}\}_{m,\mathfrak{p}}$ is an $\mathbb{F}_p$-linearly independent family in $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{F}_p$. Suppose that for certain integers $a_{m,\mathfrak{p}}$ we have

$$\sum_{m,\mathfrak{p}} a_{m,\mathfrak{p}}\alpha_{m,\mathfrak{p}} \in p\mathbb{Z}_K = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

Let us fix one of the primes $\mathfrak{p} \in \mathcal{P}$. By (5),

$$\sum_{m} a_{m,\mathfrak{p}}\alpha_{m,\mathfrak{p}} \in \mathfrak{p}^{e(\mathfrak{p}/p)}, \text{ so that } \sum_{m} a_{m,\mathfrak{p}}\, \iota_{\mathfrak{p}}(\alpha_{m,\mathfrak{p}}) \in (\mathfrak{p}\mathbb{Z}_{K_{\mathfrak{p}}})^{e(\mathfrak{p}/p)} = p\mathbb{Z}_{K_{\mathfrak{p}}}.$$

Since the $\iota_{\mathfrak{p}}(\alpha_{m,\mathfrak{p}})$ are a $\mathbb{Z}_p$-basis of $\mathbb{Z}_{K_{\mathfrak{p}}}$, all $a_{m,\mathfrak{p}}$ are multiples of p. □

The computation of the multipliers $\beta_{\mathfrak{p}}$ in terms of the data of the OM representations of the prime ideals is explained in [**GMN10**, Sections 3.2 and 4.2]. This computation requires to improve the approximations $\phi_{\mathfrak{p}}$ till $v_{\mathfrak{p}}(\phi_{\mathfrak{p}}(\theta))$ has a sufficiently large value. As mentioned at the end of the last section, this can be carried out with the single-factor lifting algorithm [**GNP10**].

4.2. Method of the quotients. This section is extracted from [**GMN09a**]. Let $\mathbf{t} = [\phi_1, \ldots, \phi_i]$ be a type of order $i-1$ corresponding to one of the nodes of the tree $\mathcal{T}$ along the flow of Montes algorithm. Before computing $N_i^-(f)$, we know a priori the length of this polygon:

$$\ell := \ell(N_i^-(f)) = \operatorname{ord}_{\psi_{i-1}} R_{i-1}(f).$$

Hence, we need only to compute the first $\ell+1$ coefficients of the ϕ_i-adic expansion of $f(x)$:

$$\begin{aligned} f(x) &= \phi_i(x)Q_{i,1}(x) + a_0(x),\\ Q_{i,1}(x) &= \phi_i(x)Q_{i,2}(x) + a_1(x),\\ \cdots &\quad \cdots\\ Q_{i,\ell}(x) &= \phi_i(x)Q_{i,\ell+1}(x) + a_\ell(x). \end{aligned}$$

The polynomials $Q_{i,1}(x), \ldots, Q_{i,\ell}(x)$ are called the *quotients of i-th order of $f(x)$ with respect to* $\mathbf{t}$. There are two relevant facts concerning these polynomials:

(1) They are obtained at cost zero along the computation of the coefficients of the ϕ_i-development of $f(x)$ that are necessary to build up the principal polygon $N_i^-(f)$.

(2) The element $Q_{i,j}(\theta)/p^{\lfloor H_{i,j}\rfloor}$ is integral, for an easy computable rational number $H_{i,j}$. More precisely,

$$H_{i,j} = (Y_j - jv_i(\phi_i))/e_1 \cdots e_{i-1},$$

where Y_j is the ordinate of the point of abscissa j lying on $N_i(f)$.

Theorem. *For each prime ideal $\mathfrak{p} = [p; \phi_1, \dots, \phi_r; \phi_\mathfrak{p}] \in \mathcal{P}$, denote by b_i, $1 \le i \le r$, the abscissa of the right end point of the side of slope λ_i of $N_i^-(f)$, and compute the family*

$$\mathcal{B}_\mathfrak{p} := \left\{\beta_\mathfrak{p}, \beta_\mathfrak{p}\frac{g_1(\theta)}{p^{\nu_1}}, \dots, \beta_\mathfrak{p}\frac{g_{n_\mathfrak{p}-1}(\theta)}{p^{\nu_{n_\mathfrak{p}-1}}}\right\}, \quad \beta_\mathfrak{p} := Q_{r+1,1}(\theta),$$

where now, for each $0 \le m < n_\mathfrak{p}$, written in a unique way as:

$$m = j_0 + j_1 m_1 + \cdots + j_r m_r, \quad 0 \le j_i < (m_{i+1}/m_i),$$

we take $g_m(x)$, ν_m to be:

$$g_m(x) := x^{j_0} Q_{1,b_1-j_1}(x) \cdots Q_{r,b_r-j_r}(x),$$
$$\nu_m := \lfloor H_{1,b_1-j_1} + \cdots + H_{1,b_r-j_r} + H_{r+1,1}\rfloor.$$

Then, $\bigcup_{\mathfrak{p}\in\mathcal{P}} \mathcal{B}_\mathfrak{p}$ is a p-integral basis of K.

The advantage of this method with respect to the standard method is twofold:

(1) We replace the computation of the powers $\phi_i(x)^{j_i}$ by a single polynomial $Q_{i,j}(x)$ that was obtained at zero cost.

(2) We replace the whole construction of the multiplier $\beta_\mathfrak{p}$ by the consideration of the polynomial $Q_{r+1,1}$, which is obtained at the cost of only one division with remainder: $f(x) = \phi_\mathfrak{p}(x)Q_{r+1,1}(x) + a_0(x)$.

The disadvantage is that the polynomials $g_m(x)$ considered in the standard method have degree m, while those of the quotients method have, by nature, large degree.

In practice, the method of the quotients has a better average performance, and it is more regular, in the sense that in the examples where the standard method is faster, the difference of the times of execution is very small, while there are peak cases in which the quotients method is extremely faster than the standard one.

In the +Ideals package we compute integral closures by using the method of the quotients.

References

[FV10] D. FORD AND O. VERES, On the complexity of the Montes Ideal Factorization Algorithm, in: *"Algorithmic Number Theory"*, (Hanrot, G., Morain, F., and Thomé, E., eds.), 9th International Symposium, ANTS-IX, Nancy, France, July 19–23, 2010, Lecture Notes in Computer Science **6197**, Springer, 2010, pp. 174–185.

[GMN08] J. GUÀRDIA, J. MONTES, AND E. NART, Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields, *J. Théor. Nombres Bordeaux* (to appear), arXiv:0807. 4065v3[math.NT].

[GMN09a] J. GUÀRDIA, J. MONTES, AND E. NART, Higher Newton polygons and integral bases, arXiv:0902.3428v2[math.NT].

[GMN09] J. GUÀRDIA, J. MONTES, AND E. NART, Okutsu invariants and Newton polygons, *Acta Arith.* **145(1)** (2010), 83–108.

[GMN10] J. GUÀRDIA, J. MONTES, AND E. NART, A new computational approach to ideal theory in number fields, arXiv:1005. 1156v1[math.NT].

[GMN10b] J. GUÀRDIA, J. MONTES, AND E. NART, Arithmetic in big number fields: The '+Ideals' package, arXiv:1005. 4596v1[math.NT].

[HN08] J. GUÀRDIA, J. MONTES, AND E. NART, Newton polygons of higher order in algebraic number theory, *Trans. Amer. Math. Soc.* (to appear), arXiv:0807.2620v2[math.NT].

[GNP10] J. GUÀRDIA, E. NART, AND S. PAULI, Single-factor lifting and factorization of polynomials over local fields, in preparation.

[McL36] S. MACLANE, A construction for absolute values in polynomial rings, *Trans. Amer. Math. Soc.* **40(3)** (1936), 363–395.

[McL36b] S. MACLANE, A construction for prime ideals as absolute values of an algebraic field, *Duke Math. J.* **2(3)** (1936), 492–510.

[Mon99] J. MONTES, Polígonos de Newton de orden superior y aplicaciones aritméticas, Tesi Doctoral, Universitat de Barcelona (1999).

[Oku82] K. OKUTSU, Construction of integral basis. I, *Proc. Japan Acad. Ser. A Math. Sci.* **58(1)** (1982), 47–49; Construction of integral basis. II, *Proc. Japan Acad. Ser. A Math. Sci.* **58(2)** (1982), 87–89.

[Ore23] Ø. ORE, Zur Theorie der algebraischen Körper, *Acta Math.* **44(1)** (1923), 219–314.

[Ore25] Ø. ORE, Bestimmung der Diskriminanten algebraischer Körper, *Acta Math.* **45(1)** (1925), 303–344.

[Pau10] S. PAULI, Factoring polynomials over local fields, II, in: *"Algorithmic Number Theory"*, (Hanrot, G., Morain, F., and Thomé, E., eds.), 9th International Symposium, ANTS-IX, Nancy, France, July 19–23, 2010, Lecture Notes in Computer Science **6197**, Springer, 2010, pp. 301–315.

[Ver09] O. VERES, On the Complexity of Polynomial Factorization Over P-adic Fields, PhD Dissertation, Concordia University (2009).

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

Primera versió rebuda el 23 de setembre de 2010,
darrera versió rebuda el 8 de febrer de 2011.