SQUARE-FREE OM COMPUTATION OF GLOBAL INTEGRAL BASES

JORDI GUÀRDIA AND ENRIC NART

ABSTRACT. For a prime p, the OM algorithm finds the p-adic factorization of an irreducible polynomial $f \in \mathbb{Z}[x]$ in polynomial time. This may be applied to construct p-integral bases in the number field K defined by f. In this paper, we adapt the OM techniques to work with a positive integer N instead of p. As an application, we obtain an algorithm to compute global integral bases in K, which does not require a previous factorization of the discriminant of f.

INTRODUCTION

The OM algorithm is a p-adic polynomial factorization method developed by Montes [10], based on ideas of Ore and MacLane [8, 9, 12]. For a number field K with defining polynomial $f \in \mathbb{Z}[x]$, the OM algorithm may be applied to compute p-integral bases for the different prime factors p of the discriminant $\operatorname{disc}(f)$ of f [5, 6, 7]. Hence, it facilitates the computation of a global integral basis, as long as a factorization of $\operatorname{disc}(f)$ is available. Since integer factorization is a heavy task, this approach is unfeasible in practice if f has a large degree or large coefficients.

It is well-known that the determination of the ring of integers of a number field is a computationally hard problem. Indeed, it is polynomial-time equivalent to the square-free factorization of integers ([2],[3],[1]). Chistov described in ([2], [3]) a polynomial time algorithm to determine integral bases of number fields given an oracle to find square-free factorizations. It is based upon a previous algorithm of factorization of polynomials over complete fields, where Newton polygons of first order are crulcial.

Buchmann and Lenstra, inspired in a normalization criterion by Grauert-Remmert and Zassenhaus, introduced an algorithm which constructs successive augmentations of a given order in K [1]. Along this process, some splittings of $\operatorname{disc}(f)$ are obtained as a by-product. At a certain stage, one knows that the maximal order has been reached if certain factors of $\operatorname{disc}(f)$ are squarefree. Therefore, combined with an integer squarefree decomposition routine, this algorithm computes global integral bases of K. T he algorithm is efficient in cases where the splitting of $\operatorname{disc}(f)$, caused by the

order augmentation steps, yields factors which are sufficiently small to admit a feasible squarefree decomposition.

In this paper, we adapt the OM techniques to work with a positive integer N instead of a prime p. This provides a method to compute a global integral basis of K which behaves as the Buchmann-Lenstra algorithm.

For a given prime p, the classical OM algorithm computes a tree of *types* whose leaves are in 1-1 correspondence with the p-adic irreducible factors of f. These types support valuations on $\mathbb{Q}(x)$ extending the p-adic valuation, which encode intrinsic data of the p-adic irreducible factors.

The tree of types is computed by a branching process based essentially on two tasks: construction of higher order Newton polygons of f with respect to the supported valuations, and polynomial factorization, over certain finite fields, of the *residual polynomials* of f with respect to certain sides of the Newton polygons.

For an integer $N > 1$, we consider similar *squarefree (SF) types* supporting pseudo-valuations on $\mathbb{Q}(x)$ extending the N-adic pseudo-valuation.

Newton polygons with respect to pseudo-valuations are easy to define, but the residual polynomials of f, with respect to the sides of these polygons, have coefficients in certain finite $(\mathbb{Z}/N\mathbb{Z})$-algebras. Hence, instead of polynomial factorization, we must use a polynomial squarefree decomposition, which makes sense for these artinian algebras.

The new *SF-OM* algorithm computes a tree of SF-types containing intrinsic data of the p-adic irreducible factors of f, simultaneously for all prime factors p of N. When these data cannot be coherently integrated in one single tree of SF-types, the method yields a splitting of N as a by-product.

This leads to a computation of a global integral basis of K, similar in spirit to the Buchmann-Lenstra algorithm. Along the branching process of SF-types, a splitting of $\mathrm{disc}(f)$ is obtained, and at a certain stage, the accumulated data yield a global integral basis if certain factors are squarefree.

This method speeds up the computations with respect to the classical OM algorithm, because the number of types to be considered is much smaller in general. For a double reason: a squarefree integer may have many prime factors, and a squarefree factor of a residual polynomial may have many irreducible factors too.

As a consequence, the amount of integer linear algebra necessary to glue the local bases to build up a global basis is drastically reduced.

We made an implementation in `Magma` of the SF-OM algorithm, which is available on request to the authors. The implementation includes a library to work with towers of artinian algebras. Even if this part is much slower than the internal pre-compiled routines of `Magma` for towers of finite fields, the new program is faster, in many cases, than our implementation of the classical Montes algorithm.

The content of the paper is as follows. Section 1 contains basic algorithms for polynomials over artinian $(\mathbb{Z}/N\mathbb{Z})$-algebras. Section 2 introduces SF-types and their basic properties. Section 3 describes the SF-OM algorithm.

In section 4, we show that for any prime factor p of N, an SF-type determines a tree of classical p-types. This connection is used in section 5 to analyze arithmetic properties of K encoded by SF-types. Section 6, inspired in [6], describes how to use the SF-OM algorithm to compute a global integral basis of K. In section 7, we discuss a few concrete examples.

Acknowledgements. Claus Fieker suggested to us that an adequate development of Montes' methods modulo N, based on polynomial squarefree decomposition over $(\mathbb{Z}/N\mathbb{Z})$-algebras, could lead to this kind of results. We are indebted to him for his fine intuition.

1. Polynomial squarefree decomposition over $(\mathbb{Z}/N\mathbb{Z})$-algebras

1.1. **Inductive artinian algebras.** For an integer $N > 1$, let $A_0 = \mathbb{Z}/N\mathbb{Z}$.

Let A be an artinian A_0-algebra. That is, $\operatorname{Spec}(A) = \operatorname{Max}(A)$ is finite and discrete. Then, A is isomorphic to a product of local A_0-algebras:

$$(1.1) \qquad A \simeq \prod\nolimits_{\mathfrak{m}\in\operatorname{Max}(A)} A_{\mathfrak{m}}.$$

Since each $A_{\mathfrak{m}}$ has a finite length as an A_0-module, A is a finite set.

The isomorphism (1.1) induces an analogous decomposition of the polynomial ring $A[y]$ in one indeterminate y:

$$A[y] \simeq \prod\nolimits_{\mathfrak{m}\in\operatorname{Max}(A)} A_{\mathfrak{m}}[y].$$

Irreducible polynomials are easily characterized in terms of their components. Also, non-unique factorization pathologies in $A[y]$ are easily explained by this decomposition.

For each $\mathfrak{m} \in \operatorname{Max}(A)$, let $\mathbb{F}_{\mathfrak{m}} = A/\mathfrak{m}$ be the residue field and

$$\operatorname{red}_{\mathfrak{m}}\colon A \longrightarrow \mathbb{F}_{\mathfrak{m}}, \qquad \operatorname{red}_{\mathfrak{m}}\colon A[y] \longrightarrow \mathbb{F}_{\mathfrak{m}}[y]$$

the reduction modulo $\mathfrak{m}$ homomorphisms for the rings A and $A[y]$.

Definition 1.1. *Let $t \in A[y]$ and denote by $\operatorname{lc}(t) \in A$ its leading coefficient.*
We say that $t \in A[y]$ is unitary *if $\operatorname{lc}(t)$ is a unit in A.*
We say that t is strongly unitary *if all its non-zero coefficients are units.*
We say that t is squarefree *if it is unitary and $\operatorname{red}_{\mathfrak{m}}(t) \in \mathbb{F}_{\mathfrak{m}}[y]$ is squarefree for all $\mathfrak{m} \in \operatorname{Max}(A)$.*

If $s, t \in A[y]$ and t is unitary, the natural routine $q, r = \operatorname{Quotrem}(s, t)$ computes $q, r \in A[y]$ such that $s = tq + r$ and $\deg r < \deg t$. Clearly,

$$(1.2) \qquad sA[y] + tA[y] = rA[y] + tA[y].$$

Also, a unitary t is a *minimal* polynomial:

$$(1.3) \qquad \deg t = \operatorname{Min}\{\deg s \mid s \in tA[y], s \neq 0\}.$$

In particular, for a unitary t of positive degree, the chain of ideals generated by the powers of t is strictly decreasing:

$$A[y] \supsetneq tA[y] \supsetneq t^2 A[y] \supsetneq \cdots$$

Hence, for all nonzero $s \in A[y]$ we may define

$$\operatorname{ord}_t(s) = k \quad \text{if} \quad s \in t^k A[y] \setminus t^{k+1} A[y].$$

We agree that $\operatorname{ord}_t(0) = \infty$.

Lemma 1.2. *Let $t \in A[y]$ be a unitary polynomial of degree $n > 0$. Let $B = A[y]/(t)$ and denote by $z \in B$ the class of y. Then, $1, z, \ldots, z^{n-1}$ is an A-basis of B, and the natural map $A \to B$ is injective.*

Proof. Let $M \subset B$ be the sub-A-module generated by $1, z, \ldots, z^{n-1}$. Since $z^n \in M$, we have $M = B$. On the other hand, (1.3) shows that $1, z, \ldots, z^{n-1}$ are A-linearly independent and the map $A \to B$ is injective. $\square$

Definition 1.3. *An* inductive A_0-*algebra of length $r \geq 0$ is an artinian algebra A which may be obtained by a chain of augmentations:*

$$(1.4) \qquad A_0 \subset A_1 \subset \cdots \subset A_r = A, \qquad A_{i+1} = A_i[y]/(t_i), \quad 0 \leq i < r,$$

for some squarefree, strongly unitary $t_i \in A_i[y]$ such that $t_i(0) \neq 0$ for $i > 0$.

The moduli sequence *of A is the list $[t_{-1}, t_0, \ldots, t_{r-1}]$ of the different "moduli", starting formally with $t_{-1} := N$.*

1.2. Polynomial squarefree decomposition over inductive algebras.

Let A be an inductive algebra of length r as in (1.4). In this section, we describe a squarefree decomposition routine (SFD) for polynomials with coefficients in A. We start with a gcd_A routine in $A[y]$. Given $s, t \in A[y]$, the idea is to mimic Euclid's algorithm to compute a monic polynomial $d = \gcd_A(s, t)$ in $A[y]$ such that

$$sA[y] + tA[y] = dA[y].$$

This is not always possible, but when the method crashes it outputs a factorization in $A[y]$ of one of the moduli of A.

The $\gcd_A$ routine is defined recursively, assuming that $\gcd_{A_{r-1}}$ is well-defined. At the bottom of the recursion, for $a \in A_0$ it makes sense to define $\gcd_{A_{-1}}(a, N) \in \mathbb{Z}_{>0}$ as the usual $\gcd(\tilde{a}, N)$, for any lifting $\tilde{a} \in \mathbb{Z}$ of a.

Algorithm 1.4 $(\gcd_A(s, t))$**.**

   Input: $s, t \in A[y]$, $t \neq 0$, where A is an inductive A_0-algebra of length
              $r \geq 0$ with moduli sequence $[t_{-1}, t_0, \ldots, t_{r-1}]$
  Output: Either a proper factor of a modulus of A, or a monic $d \in A[y]$
              such that $sA[y] + tA[y] = dA[y]$.

  (1)   while $t \neq 0$ do
  (2) $a \leftarrow \operatorname{lc}(t), \;\; b \leftarrow \gcd_{A_{r-1}}(a, t_{r-1})$
  (3)   if $b \neq 1$ then return $[r-1, b]$ else $t \leftarrow a^{-1}t$
  (4) $q, r = \operatorname{Quotrem}(s, t)$
  (5) $s \leftarrow t, \;\; t \leftarrow r$
  (6)   return s

Convention. *Throughout the paper, we shall simply write* $\gcd_A(s,t) = d$ *to indicate that the routine* $\gcd_A(s,t)$ *does not crash and outputs* d.

In step 2, we identify $a \in A$ with a polynomial in $A_{r-1}[y]$. For the routine to be consistent, the condition $\gcd_{A_{r-1}}(a, t_{r-1}) = 1$ should imply that a is a unit in A. This fact, and the fundamental properties of $\gcd_A$ are contained in the following result.

Lemma 1.5. *For* $a \in A$, *if* $\gcd_{A_{r-1}}(a, t_{r-1}) = 1$, *then* a *is a unit in* A.
  Moreover, if $\gcd_A(s,t) = d$ *for certain* $s,t \in A[y]$, *then*
  (a) $sA[y] + tA[y] = dA[y]$,
  (b) *For all* $\mathfrak{m} \in \mathrm{Max}(A)$, $\mathrm{red}_\mathfrak{m}(d) = \gcd\left(\mathrm{red}_\mathfrak{m}(s), \mathrm{red}_\mathfrak{m}(t)\right)$ *in* $\mathbb{F}_\mathfrak{m}[y]$.

Proof. We prove these properties for the algebras $A_0, A_1, \ldots, A_r = A$ in a recursive way. For $r = 0$, the condition $\gcd_{A_{-1}}(a, N) = 1$ implies trivially that a is a unit in A_0. Hence, the routine $\gcd_{A_0}$ is consistent.

Once a routine $\gcd_{A_i}$ is consistent, the equality (a) is a consequence of (1.2) applied to each division with remainder in step (4). Then, (b) follows from (a) by the compatibility of all operations with reduction modulo $\mathfrak{m}$.

Finally, suppose $\gcd_{A_i}(a, t_i) = 1$. From $aA_i[y] + t_i A_i[y] = A_i[y]$, we deduce a Bézout identity $au + t_i v = 1$, proving that a is a unit in A_{i+1}. $\square$

With this $\gcd_A$ routine in hand, we can mimic the standard squarefree decomposition routine for polynomials with coefficients in a field of characteristic zero [14, §20.3]. If our polynomial in $A[y]$ has a not too large degree, the output will be correct.

Algorithm 1.6 (SFD)**.**
  Input: A unitary $f \in A[y]$ with $\deg f < p$ for all prime factors p of N.
  Output: A proper factor of a modulus of A, or pairs $(s_1, \ell_1), \ldots, (s_k, \ell_k)$,
            where $s_1, \ldots, s_k \in A[y]$ are monic squarefree pairwise coprime
            polynomials, and $f = \mathrm{lc}(f)\, s_1^{\ell_1} \cdots s_k^{\ell_k}$ with $1 \le \ell_1 < \cdots < \ell_k$.
  (1) $f \leftarrow f/\mathrm{lc}(f)$, $g \leftarrow f/\gcd_A(f, f')$
  (2) $\ell \leftarrow 1$, $L \leftarrow [\,]$
  (3)   while $f \neq 1$ do
  (4) $f \leftarrow f/g$, $h \leftarrow \gcd_A(f, g)$, $s \leftarrow g/h$
  (5)   if $s \neq 1$ then append (s, ℓ) to L
  (6) $g \leftarrow h$, $\ell \leftarrow \ell + 1$
  (7)   return L

Of course, although not specifically indicated, after every call to $\gcd_A$ the routine ends if we find a proper factor of a modulus of A.

The next result is an immediate consequence of Lemma 1.5.

Lemma 1.7. *Suppose the SFD routine does not crash and outputs a list of pairs* $(s_1, \ell_1), \ldots, (s_k, \ell_k)$. *Then, for any* $\mathfrak{m} \in \mathrm{Max}(A)$, *the list*

$$(\mathrm{red}_\mathfrak{m}(s_1), \ell_1), \ldots, (\mathrm{red}_\mathfrak{m}(s_k), \ell_k)$$

is the canonical squarefree decomposition of $\mathrm{red}_\mathfrak{m}(f)$ *in* $\mathbb{F}_\mathfrak{m}[y]$.

This result justifies that the output polynomials $s_1, \ldots, s_k \in A[y]$ are squarefree and pairwise coprime.

Remark 1.8. The condition $\deg f < p$ for all $p \mid N$ fits well with our purpose of constructing a global integral basis in a number field of degree n. In this context, $\deg f \leq n$ and N will be a positive divisor of the discriminant from which all prime factors $p \leq n$ have been removed (cf. section 6.4).

2. TYPES WITH RESPECT TO PSEUDO-VALUATIONS

Let $v \colon \mathcal{O} \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation on an integral domain $\mathcal{O}$, and let $\mathcal{O}_v$ be the completion of $\mathcal{O}$ at v.

A *type* over $(\mathcal{O}, v)$ is a discrete object parameterizing a certain equivalence class of monic irreducible polynomials in $\mathcal{O}_v[x]$ [7]. Types were introduced by Montes [10] as a tool to perform "higher dissections", a procedure foreseen by Ore aiming at a polynomial factorization algorithm in $\mathcal{O}_v[x]$.

The papers [4, 7] contain variant definitions of a type, with slight changes in the normalization of certain data.

Let $N > 1$ be an integer. This section introduces SF-types over $(\mathbb{Z}, \mathrm{ord}_N)$, where ord_N is the *N-adic pseudo-valuation* introduced in section 2.1.

For $N = p$ prime, ord_p is a valuation. However, SF-types over $(\mathbb{Z}, \mathrm{ord}_p)$ do not coincide with those introduced by Montes, which become *irreducible* types in our terminology (see Definition 4.1).

2.1. **Pseudo-valuations.**

Definition 2.1. *A* pseudo-valuation *on $\mathcal{O}$ is a mapping $v \colon \mathcal{O} \to \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions for all $a, b \in \mathcal{O}$:*

(1) $v(a) = \infty$ *if and only if $a = 0$.*
(2) $v(-1) = 0$.
(3) $v(ab) \geq v(a) + v(b)$.
(4) $v(a + b) \geq \mathrm{Min}\{v(a), v(b)\}$.

These axioms imply that $v(-a) = v(a)$ for all $a \in \mathcal{O}$, and equality holds in (4) when $v(a) \neq v(b)$ [13, §1].

Definition 2.2. *We say that $a, b \in \mathcal{O}$ are v-equivalent if either $a = b = 0$, or $v(a - b) > v(a)$. We then write $a \sim_v b$. Note that this implies $v(a) = v(b)$.*

A pseudo-valuation may be extended to the ring of fractions $\mathcal{S}_v^{-1}\mathcal{O}$, where $\mathcal{S}_v$ is the multiplicatively closed subset of all non-zero *stable* elements:

$$\mathcal{S}_v = \{a \in \mathcal{O} \setminus \{0\} \mid v(ab) = v(a) + v(b) \text{ for all } b \in \mathcal{O}\}.$$

Also, v determines a pseudo-valuation on the polynomial ring $\mathcal{O}[x]$ by:

$$v(a_0 + a_1 x + \cdots + a_s x^s + \cdots) = \mathrm{Min}\{v(a_s) \mid 0 \leq s\}.$$

We fix an integer $N > 1$, and let $\mathcal{O}$ be either $\mathbb{Z}$ or the p-adic ring $\mathbb{Z}_p$, the latter case only when $N = p$ is a prime number.

Let $A_0 = \mathbb{Z}/N\mathbb{Z}$ and denote reduction modulo N by $\mathrm{red}_N \colon \mathcal{O} \to A_0$. Denote still by $\mathrm{red}_N \colon \mathcal{O}[x] \to A_0[y]$ the mapping that reduces modulo N the coefficients of a polynomial and changes the variable x to y.

We define the N-adic pseudo-valuation

$$\mathrm{ord}_N \colon \mathcal{O} \to \mathbb{Z} \cup \{\infty\}, \qquad \mathrm{ord}_N(a) = k \ \text{ if } \ a \in N^k\mathcal{O} \setminus N^{k+1}\mathcal{O}.$$

Consider the *residual polynomial operator*

$$(2.1) \qquad R_0 \colon \mathcal{O}[x] \to A_0[y], \quad f \mapsto \mathrm{red}_N\left(f/N^{\mathrm{ord}_N(f)}\right).$$

We agree that $R_0(0) = 0$. Clearly,

$$\mathcal{S}_{\mathrm{ord}_N} = \{a \in \mathcal{O} \mid R_0(a) \text{ is a unit in } A_0\},$$

Definition 2.3. *A non-zero polynomial $f \in \mathcal{O}[x]$ is said to be N-robust if all its non-zero coefficients are stable.*

The next results follow easily from the definitions.

Lemma 2.4. *Two polynomials $f, h \in \mathcal{O}[x]$ are ord_N-equivalent if and only if $\mathrm{ord}_N(f) = \mathrm{ord}_N(h)$ and $R_0(f) = R_0(h)$.*

Lemma 2.5. *Let $f, h \in \mathcal{O}[x]$ and suppose that f is N-robust.*
  (1) $\mathrm{ord}_p(f) = \mathrm{ord}_p(N)\,\mathrm{ord}_N(f)$ *for all prime factors p of N.*
  (2) $\mathrm{ord}_N(fh) = \mathrm{ord}_N(f) + \mathrm{ord}_N(h)$ *and $R_0(fh) = R_0(f)R_0(h)$.*

Thus, robust polynomials are stable for the extension of ord_N to $\mathcal{O}[x]$. However, they do not form a multiplicatively closed set.

2.2. **Types over $(\mathcal{O}, \mathrm{ord}_N)$, also called SF-types.** An *SF-type* $\mathbf{t} = (t_0)$ of *order zero* over $(\mathcal{O}, \mathrm{ord}_N)$ is determined by the choice of a monic squarefree, strongly unitary $t_0 \in A_0[y]$.

Consider $A_1 = A_0[y]/(t_0)$, and let $z_0 \in A_1$ be the class of y.

A *representative* of $\mathbf{t}$ is a monic N-robust $g \in \mathcal{O}[x]$ such that $R_0(g) = t_0$.

An *SF-type of order $r > 0$* over $(\mathcal{O}, \mathrm{ord}_N)$ is a collection of data:

$$\mathbf{t} = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r))$$

distributed into levels $0, 1, \ldots, r$, such that
  • $\mathbf{t}' = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_{r-1}, \lambda_{r-1}, t_{r-1}))$ is an SF-type of order $r-1$
  • $g_r \in \mathcal{O}[x]$ is a representative of $\mathbf{t}'$
  • λ_r is a positive rational number
  • $t_r \in A_r[y]$ is monic squarefree, strongly unitary, with $t_r(0) \neq 0$.

By the very definition, from a type of order r we may deduce types of order $0 \leq i \leq r$, by an adequate truncation:

$$\mathbf{t}_i := \mathrm{Trunc}_i(\mathbf{t}) := (t_0; (g_1, \lambda_1, t_1); \ldots; (g_i, \lambda_i, t_i)).$$

For the definition of a type to be complete we must define representatives of types of positive order, and describe the artinian inductive algebra A_{r+1} attached to $\mathbf{t}$. To this end, we discuss some data and operators that $\mathbf{t}$

carries at the r-th level. Note that $\mathbf{t}$ supports analogous objects at the levels $0, 1, \ldots, r-1$, associated with the truncated types $\mathbf{t}_0, \ldots, \mathbf{t}_{r-1}$.

Numerical data

$e_0 = m_0 = 1$, $h_0 = \lambda_0 = 0$, $f_0 = \deg t_0$, $V_0 = 0$.

$m_r = \deg g_r = e_{r-1} f_{r-1} m_{r-1} = (e_0 \cdots e_{r-1})(f_0 \cdots f_{r-1})$,

$\lambda_r = h_r / e_r$, with h_r, e_r positive coprime integers,

$\ell_r h_r + \ell_r' e_r = 1$, Bézout identity determined by $0 \le \ell_r < e_r$,

$f_r = \deg t_r$,

$V_r = v_{r-1}(g_r) = e_{r-1} f_{r-1} (e_{r-1} V_{r-1} + h_{r-1})$.

From the latter recurrence it is easy to deduce the following identity:

$$(2.2) \qquad \frac{V_r}{e_1 \cdots e_{r-1}} = \sum_{1 \le j < r} \frac{m_r}{m_j} \frac{h_j}{e_1 \cdots e_j}.$$

Inductive artinian algebra

$$A_0 \subset A_1 \subset \cdots \subset A_r \subset A_{r+1}, \qquad A_{r+1} = A_r[y]/(t_r).$$

Let $z_r \in A_{r+1}$ be the class of y in A_{r+1}; thus, $A_{r+1} = A_r[z_r] = A_0[z_0, \ldots, z_r]$. By Lemma 1.2, A_{r+1} is a free A_r-algebra with basis $1, z_r, \ldots, z_r^{f_r - 1}$.

Since $t_r(0)$ is a unit in A_r, z_r is a unit in A_{r+1}.

Newton polygon operator of order r

Let $v_0 := \mathrm{ord}_N$ be the N-adic pseudo-valuation, and let $2^{\mathbb{R}^2}$ be the set of subsets of $\mathbb{R}^2$. For $r > 0$ the type $\mathbf{t}$ determines an operator:

$$N_r := N_{v_{r-1}, g_r} : \mathcal{O}[x] \to 2^{\mathbb{R}^2}.$$

The Newton polygon of the zero polynomial is the empty set. For a non-zero $f \in \mathcal{O}[x]$ we consider its canonical g_r-expansion:

$$(2.3) \qquad f = \sum_{0 \le s} a_s g_r^s, \quad a_s \in \mathcal{O}[x], \ \deg a_s < m_r.$$

For each $s \in \mathbb{Z}_{\ge 0}$ we compute $u_s = v_{r-1}(a_s g_r^s) \in \mathbb{Z}_{\ge 0}$, and we define $N_r(f)$ as the lower convex hull of the set of points $\{(s, u_s) \in \mathbb{R}^2 \mid s \ge 0, a_s \ne 0\}$.

The Newton polygon $N_r(f)$ is the union of different adjacent *sides*, whose endpoints are called *vertices* of the polygon. The typical shape of this polygon is shown in Figure 1.

The *length* of $N_r(f)$ is by definition the abscissa of the last vertex. We denote it by $\ell(N_r(f)) = \lfloor \deg(f)/m_r \rfloor$.

Definition 2.6. *The polygon $N_r^-(f)$ determined by the sides of negative slope of $N_r(f)$ is called the* principal Newton polygon *of f.*

If $N_r(f)$ has no sides of negative slope, then $N_r^-(f)$ is the one-point set formed by the left endpoint of $N_r(f)$.

For any $\lambda \in \mathbb{Q}_{>0}$, the λ-component of $N := N_r^-(f)$ is the segment

$$S_\lambda(N) = \{(x, y) \in N \mid y + \lambda x \text{ is minimal}\} = N \cap L,$$

where L is the line of slope $-\lambda$ which first touches N from below.

FIGURE 1. Newton polygon of a polynomial $f \in \mathcal{O}[x]$
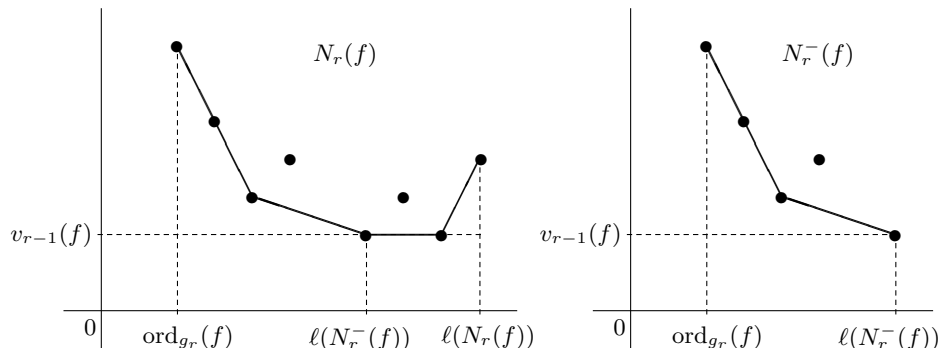
We denote by $(s_r(f), u_r(f)) \in N_r^-(f)$ the coordinates of the left endpoint of the segment $S_r(f) := S_{\lambda_r}(N_r(f))$ (see Figure 2).

If $N_r(f)$ has a side S of slope $-\lambda_r$, then $S_r(f) = S$; otherwise, $S_r(f) = \{(s_r(f), u_r(f))\}$ is a vertex of $N_r(f)$.

Pseudo-valuation of order r

This is a pseudo-valuation $v_r \colon \mathcal{O}[x] \to \mathbb{Z} \cup \{\infty\}$. For a non-zero $f \in \mathcal{O}[x]$ having a g_r-expansion as in (2.3), we define

$$(2.4) \qquad v_r(f) = e_r \operatorname{Min} \{u_s + s\lambda_r \mid s \ge 0\} = \operatorname{Min} \{v_r(a_s g_r^s) \mid s \ge 0\}.$$

Assuming that v_{r-1} is a pseudo-valuation, it is easy to check that v_r is a pseudo-valuation too.

Note that $v_r(f)/e_r$ can be reinterpreted as the ordinate where the line L in Figure 2 cuts the vertical axis.

Residual polynomial operator of order r

$$R_r := R_{v_{r-1}, g_r, \lambda_r} \colon \mathcal{O}[x] \to A_r[y].$$

The operator R_r maps 0 to 0. For a non-zero $f \in \mathcal{O}[x]$ with g_r-expansion as in (2.3), we take the following residual coefficients $c_s \in A_r$, for $s \in \mathbb{Z}_{\ge 0}$:

$$c_s = \begin{cases} 0, & \text{if } (s, u_s) \text{ lies above } N_r^-(f), \text{ or } u_s = \infty, \\ z_{r-1}^{\nu_{r-1}(a_s)} R_{r-1}(a_s)(z_{r-1}), & \text{if } (s, u_s) \text{ lies on } N_r^-(f). \end{cases}$$

For $r = 1$, we agree that $z_0^{\nu_0(a)} = 1$ for all $a \in \mathcal{O}[x]$, even when $z_0 = 0$.

For $r > 1$ and a nonzero $a \in \mathcal{O}[x]$, we define:

$$(2.5) \qquad \nu_{r-1}(a) = \ell'_{r-1} s_{r-1}(a) - \ell_{r-1} u_{r-1}(a) \in \mathbb{Z},$$

where $s_{r-1}(a)$, $u_{r-1}(a)$ were introduced in Definition 2.6.

Since z_{r-1} is a unit in A_r, the element $z_{r-1}^{\nu_{r-1}(a_s)} \in A_r$ is well defined regardless of the sign of the integer exponent.

FIGURE 2. Residual polynomial $R_r(f)$. The line L has slope $-\lambda_r$.
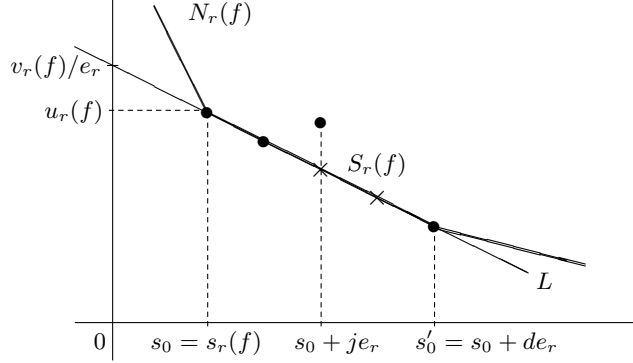
Take $\lambda = h/e$, with h, e positive coprime integers. Let S be the λ-component of $N_r(f)$ (Definition 2.6), with endpoints having abscissas $s_0 \le s_0'$. We define the residual polynomial attached to $\mathbf{t}$ and λ as:

$$R_{v_{r-1}, g_r, \lambda}(f) = c_{s_0} + c_{s_0+e}\, y + \cdots + c_{s_0+de}\, y^d \in A_r[y],$$

where $d = (s_0' - s_0)/e$. Note that $s_0, s_0+e, \ldots, s_0' = s_0+de$ are the abscissas of the points in $S \cap \mathbb{Z}^2$.

Since $\deg a_s < m_r = e_{r-1}f_{r-1}m_{r-1}$, we have $\ell(N_{r-1}^-(a_s)) < e_{r-1}f_{r-1}$, so that $\deg R_{r-1}(a_s) < f_{r-1} = \deg t_{r-1}$. Hence, the residual coefficient attached to a point lying on $N_r^-(f)$ is always nonzero. In particular, $c_{s_0} \ne 0$ and $c_{s_0'} \ne 0$. Thus, $\deg R_{v_{r-1}, g_r, \lambda}(f) = d$.

Definition 2.7. *Let $\mathbf{t}_0$ be a type of order zero. A polynomial $f \in \mathcal{O}[x]$ is said to be $\mathbf{t}_0$-robust if it is N-robust (Definition 2.3).*

For our type $\mathbf{t}$ of order $r > 0$, we say that $f \in \mathcal{O}[x]$ is $\mathbf{t}$-robust if all coefficients $a_s \in \mathcal{O}[x]$ of the canonical g_r-expansion of f are $\mathbf{t}_{r-1}$-robust and satisfy $\gcd_{A_{r-1}}(R_{r-1}(a_s), t_{r-1}) = 1$.

If f is $\mathbf{t}$-robust, then $R_{r-1}(a_s)(z_{r-1})$ is a unit in A_r for all s, by Lemma 1.5. In particular, the polynomial $R_{v_{r-1}, g_r, \lambda}(f)$ is strongly unitary for all slopes $-\lambda$ of $N_r^-(f)$.

Note that, for $r > 0$, $\mathbf{t}$-robustness does not depend on λ_r nor t_r.

Definition 2.8. *A representative of $\mathbf{t}$ is a $\mathbf{t}$-robust monic $g \in \mathcal{O}[x]$ of degree $m_{r+1} := e_r f_r m_r$, such that $R_r(g) = t_r$.*

We denote by $\operatorname{Rep}(\mathbf{t}) \subset \mathcal{O}[x]$ the set of all representatives of $\mathbf{t}$.

The condition $R_r(g) = t_r$ implies that $N_r(g)$ contains a side of slope $-\lambda_r$ whose projection to the horizontal axis has length $e_r f_r$. Thus, m_{r+1} is the minimal possible degree of a polynomial $g \in \mathcal{O}[x]$ satisfying this condition.

Hence, if g is a representative of $\mathbf{t}$, the principal monomial of the g_r-expansion of g is $g_r^{e_r f_r}$, and $N_r(g)$ must be one-sided of slope $-\lambda_r$ with endpoints $(0, e_r f_r (V_r + \lambda_r))$, $(f_r, e_r f_r V_r)$. In particular,

$$v_r(g) = V_{r+1} := e_r^2 f_r (V_r + \lambda_r) = e_r f_r (e_r V_r + h_r).$$

In order to enlarge $\mathbf{t}$ to a type of order $r + 1$, a crucial step is the construction of a representative. The construction for classical types (based on [7, Prop. 3.4]) applies without changes to SF-types.

The condition of g being $\mathbf{t}$-robust is not guaranteed by this routine. In any case, by introducing adequate hooks, we guarantee either a robust output or a non-trivial splitting of some modulus in the sequence $[t_{-1}, t_0, \ldots, t_r]$.

2.3. **Tree structure on the set of types.** Let us introduce a tree structure on the set $\mathcal{T} = \mathcal{T}(\mathcal{O}, \mathrm{ord}_N)$ of all SF-types over $(\mathcal{O}, \mathrm{ord}_N)$.

The root nodes are the types of order zero, and the previous node of a type $\mathbf{t} \in \mathcal{T}$ of order $r > 0$ is $\mathrm{Trunc}_{r-1}(\mathbf{t})$. Thus, there is a unique path of length r joining $\mathbf{t}$ with its root node:

$$\underset{\mathrm{Trunc}_0(\mathbf{t})}{\bullet} \xrightarrow{\mathrm{Trunc}_1(\mathbf{t})} \bullet \quad \cdots \cdots \quad \overset{\mathrm{Trunc}_{r-1}(\mathbf{t})}{\bullet} \xrightarrow{\qquad} \underset{\mathbf{t}}{\bullet}$$

The connected components of $\mathcal{T}$ are the subtrees $\mathcal{T}_\varphi$ of all types $\mathbf{t}$ with $\mathrm{Trunc}_0(\mathbf{t}) = (\varphi)$, for a monic squarefree strongly unitary $\varphi \in A_0[y]$.

The branches of a type $\mathbf{t}$ of order r are types of the form $\mathbf{t}^* = (\mathbf{t}; (g, \lambda, t))$, obtained by enlarging $\mathbf{t}$ with data (g, λ, t) at the $(r+1)$-th level.

2.4. **Basic properties of types.** For the definition of the sum of plane segments see [4, Sec. 1.1].

Theorem 2.9. *Let* $\mathbf{t} = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r))$ *be an SF-type of order* $r \geq 1$, *and let* $f, h \in \mathcal{O}[x]$, $f \neq 0$.

(A) $f \sim_{v_r} h$ *if and only if* $S_r(f) = S_r(h)$ *and* $R_r(f) = R_r(h)$.

(B) *Suppose* $v_r(f) = v_r(h)$, *and let* $H = f + h$. *Then,*

$$y^{\nu_r(f)} R_r(f) + y^{\nu_r(h)} R_r(h) = \begin{cases} 0, & \text{if } v_r(H) > v_r(f), \\ y^{\nu_r(H)} R_r(H), & \text{if } v_r(H) = v_r(f). \end{cases}$$

(C) *If* f *is* $\mathbf{t}$-*robust, then* $v_r(fh) = v_r(f) + v_r(h)$ *and*

$$S_r(fh) = S_r(f) + S_r(h), \quad R_r(fh) = R_r(f)R_r(h).$$

(D) *Let* $g \in \mathcal{O}[x]$ *be a representative of* $\mathbf{t}$, *and let* $f = \sum_{0 \leq s} b_s g^s$ *be the canonical g-expansion of* f.

(i) $f \sim_{v_r} gh \implies R_r(f) \in t_r A_r[y] \implies \deg(f) \geq \deg(g)$.
(ii) $v_r(f) = \mathrm{Min}\{v_r(b_s g^s) \mid 0 \leq s\}$.

Proof. We prove the four statements simultaneously by induction on the order r of $\mathbf{t}$. The analogous statements for types of order zero follow immediately from the definitions (cf. Lemmas 2.4 and 2.5).

For each statement (X) of the theorem, we assume that the analogous statement (X_{r-1}) for the truncated type $\mathbf{t}_{r-1} = \mathrm{Trunc}_{r-1}(\mathbf{t})$ is true.

For any $q \in \mathcal{O}[x]$ and any $s \in \mathbb{Z}_{\geq 0}$, let $(s, u_s(q))$ be the point attached to the s-th term of the canonical g_r-expansion of q and let $c_s(q) \in A_r$ be the corresponding residual coefficient determined by $N_r(q)$.

We denote $g = g_r$, $u_s = u_s(f)$, $u'_s = u_s(h)$ for simplicity. Let

$$f = \sum_{0 \leq s} a_s g^s, \quad h = \sum_{0 \leq s} a'_s g^s, \quad f - h = \sum_{0 \leq s} (a_s - a'_s) g^s$$

be the canonical g-expansions of f, h and $f - h$.

Since g is $\mathbf{t}_{r-1}$-robust, (C_{r-1}) shows that

$$(2.6) \qquad u_s = v_{r-1}(a_s g^s) = v_{r-1}(a_s) + s v_{r-1}(g) = v_{r-1}(a_s) + s V_r.$$

By (2.4) and the definition of v_r, we get

$$(2.7) \qquad v_r(f) \leq v_r(a_s g^s) = e_r(u_s + s\lambda_r), \;\; \forall s \geq 0,$$

and equality holds if and only if $(s, u_s) \in S_r(f)$.

Let us prove (A). Suppose $f \sim_{v_r} h$; that is, $v_r(f - h) > v_r(f)$. Take a point $(s, u_s) \in S_r(f)$ for which equality holds in (2.7). By (2.7) applied to h and $f - h$, we get $v_r(h) \leq v_r(a'_s g^s) = e_r(u'_s + s\lambda_r)$, and

$$(2.8) \qquad v_r(a_s g^s) = v_r(f) < v_r(f - h) \leq v_r\left((a_s - a'_s)g^s\right).$$

This proves $v_r(a_s g^s) = v_r(a'_s g^s)$, leading to $u_s = u'_s$. Thus, $S_r(f) \subset S_r(h)$ and the symmetry of the argument implies $S_r(f) = S_r(h)$.

Also, (2.6), (2.7) and (2.8) imply $a_s \sim_{v_{r-1}} a'_s$. By (A_{r-1}), we deduce that $S_{r-1}(a_s) = S_{r-1}(a'_s)$ (if $r > 1$) and $R_{r-1}(a_s) = R_{r-1}(a'_s)$. This implies in any case $c_s(f) = c_s(h)$. Since this works for any abscissa s for which (s, u_s) lies on $S_r(f) = S_r(h)$, the polynomials $R_r(f)$ and $R_r(h)$ coincide.

The reciprocal implication follows from (B). In fact, $S_r(f) = S_r(h)$ implies $v_r(f) = v_r(h)$ and $\nu_r(f) = \nu_r(h) = \nu_r(-h)$. If moreover $R_r(f) = R_r(h)$, then $R_r(f) + R_r(-h) = 0$, and this implies $v_r(f - h) > v_r(f)$ by (B). Therefore, the proof of (B) will complete the proof of (A) as well.

Let us prove (B). If $v_r(f + h) > v_r(f)$, then $f \sim_{v_r} -h$ and we have seen above that this implies $\nu_r(f) = \nu_r(-h) = \nu_r(h)$ and $R_r(f) = R_r(-h) = -R_r(h)$. Hence, $R_r(f) + R_r(h) = 0$, as predicted by (B).

Suppose $v_r(f) = v_r(h) = v_r(f + h)$, and let L be the line of slope $-\lambda_r$ cutting the vertical axis at the point $(0, v_r(f)/e_r)$. As Figure 2 shows, this line L contains the segments $S_r(f)$, $S_r(h)$ and $S_r(f + h)$.

Suppose $s_0 := s_r(f) \leq s_r(h)$. We then have $s_0 \leq s_r(f + h)$ too. The points in $L \cap \mathbb{Z}^2$ have abscissa $s_j := s_0 + j e_r$, for some $j \in \mathbb{Z}$. Let $q = f, h$, or $f + h$. The left endpoint of $S_r(q)$ lies on L, so that

$$s_r(q) = s_0 + m_q e_r, \quad u_r(q) = u_r(f) - m_q h_r,$$

for some non-negative integer m_q. The formula (2.5) for the function ν_r yields $\nu_r(q) = \nu_r(f) + m_q$.

Consider the following residual coefficients:

$$\tilde{c}_s(q) = \begin{cases} c_s(q), & \text{if } (s, u_s(q)) \text{ lies on } L, \\ 0, & \text{if } (s, u_s(q)) \text{ lies above } L. \end{cases}$$

These residual coefficients satisfy:
$$y^{\nu_r(q)}R_r(q) = y^{\nu_r(f)}y^{m_q}R_r(q) = y^{\nu_r(f)}\sum_{0 \le j}\tilde{c}_{s_j}(q)y^j.$$

Hence, the identity predicted by (B) in this case amounts to:

(2.9) $$\tilde{c}_s(f) + \tilde{c}_s(h) = \tilde{c}_s(f+h), \quad \forall s \ge 0.$$

Suppose $\tilde{c}_s(f) = 0$, so that (s, u_s) lies above L. If (s, u_s') lies above L, then $(s, u_s(f+h))$ lies above L too and $\tilde{c}_s(h) = \tilde{c}_s(f+h) = 0$. If (s, u_s') lies on L, then $a_s + a_s' \sim_{v_{r-1}} a_s'$ and $\tilde{c}_s(h) = c_s(h) = c_s(f+h) = \tilde{c}_s(f+h)$, by (A_{r-1}). The same arguments prove (2.9) when $\tilde{c}_s(h) = 0$.

Suppose $\tilde{c}_s(f) \ne 0$ and $\tilde{c}_s(h) \ne 0$, so that $(s, u_s) = (s, u_s')$ lies on L. By (2.6), we have $v_{r-1}(a_s) = v_{r-1}(a_s')$. By (B_{r-1}),

$$y^{\nu_{r-1}(a_s)}R_{r-1}(a_s) + y^{\nu_{r-1}(a_s')}R_{r-1}(a_s')$$
$$= \begin{cases} 0, & \text{if } v_{r-1}(a_s + a_s') > v_{r-1}(a_s), \\ y^{\nu_{r-1}(a_s+a_s')}R_r(a_s + a_s'), & \text{if } v_{r-1}(a_s + a_s') = v_{r-1}(a_s). \end{cases}$$

Since $z_0^{\nu_0(a)} = 1$ for all $a \in \mathcal{O}[x]$, and z_{r-1} is a unit in A_r for $r > 1$, we may replace $y = z_{r-1}$ to derive the identity (2.9). This ends the proof of (B).

Let us prove (C). Assume that f is **t**-robust (Definition 2.7).

Let $s_0 = s_r(f)$, $\ell_0 = s_r(h)$ be the abscissas of the left endpoints of $S_r(f)$, $S_r(h)$, respectively. Let $d = \deg R_r(f)$, $d' = \deg R_r(h)$, and denote

$$s_j = s_0 + je_r, \ 0 \le j \le d; \qquad \ell_i = \ell_0 + ie_r, \ 0 \le i \le d'.$$

For an abscissa $s \notin \{s_j \mid 0 \le j \le d\}$ the point (s, u_s) does not lie on $S_r(f)$ and (2.7) shows that $v_r(a_sg^s) > v_r(f)$. Analogously, $v_r(a_s'g^s) > v_r(h)$ for the abscissas $s \notin \{\ell_i \mid 0 \le i \le d'\}$. Therefore, the polynomials $f_0 = \sum_{j=0}^{d} a_{s_j}g^{s_j}$, $h_0 = \sum_{i=0}^{d'} a_{\ell_i}'g^{\ell_i}$ satisfy:

(2.10) $$f \sim_{v_r} f_0, \quad h \sim_{v_r} h_0, \quad v_r(fh - f_0h_0) > v_r(f) + v_r(h).$$

Claim 1. $v_r(f_0h_0) = v_r(f) + v_r(h)$.

Denote $\mathfrak{s}_k = s_0 + \ell_0 + ke_r$, $0 \le k \le d + d'$. Consider the product

$$f_0h_0 = \sum_{0 \le k \le d+d'} b_k g^{\mathfrak{s}_k}, \qquad b_k = \sum_{i+j=k} a_{s_j}a_{\ell_i}',$$

and let the canonical g-expansion of each b_k be:

$$b_k = b_{k,0} + b_{k,1}g, \quad 0 \le k \le d + d'.$$

The lowest degree term of the canonical g-expansion of f_0h_0 is $b_{0,0}\,g^{s_0+\ell_0}$. By (2.10), $v_r(f_0h_0) \ge v_r(f) + v_r(h)$. By (2.4), equality holds if we show that

(2.11) $$v_r\left(b_{0,0}g^{s_0+\ell_0}\right) = v_r(f) + v_r(h).$$

By (2.6) and (2.7), this amounts to

(2.12) $$v_{r-1}(b_{0,0}) = v_{r-1}(a_{s_0}) + v_{r-1}(a_{\ell_0}'),$$

which is equal to $v_{r-1}(a_{s_0}a'_{\ell_0})$ by (C_{r-1}), because a_{s_0} is $\mathbf{t}_{r-1}$-robust. Since

$$a_{s_0}a'_{\ell_0} = b_0 = b_{0,0} + b_{0,1}g$$

(D_{r-1}) shows that $v_{r-1}(b_{0,0}) \geq v_{r-1}(a_{s_0}a'_{\ell_0})$. This inequality cannot be strict because $a_{s_0}a'_{\ell_0} \sim_{v_{r-1}} b_{0,1}g$ implies, by (D_{r-1}):

$$R_{r-1}(a_{s_0})R_{r-1}(a'_{\ell_0}) = R_{r-1}(a_{s_0}a'_{\ell_0}) \in t_{r-1}A_{r-1}[y].$$

Since f is $\mathbf{t}$-robust, $\gcd_{A_{r-1}}(R_{r-1}(a_{s_0}), t_{r-1}) = 1$. Hence, $R_{r-1}(a'_{\ell_0})$ belongs to $t_{r-1}A_{r-1}[y]$, contradicting (D_{r-1}). This ends the proof of Claim 1.

Claim 1 and (2.10), imply $fh \sim_{v_r} f_0 h_0$ and $v_r(fh) = v_r(f) + v_r(h)$.

Therefore, by using (A), we may assume $f = f_0$, $h = h_0$ for the proof of the two last statements of (C) concerning the operators S_r and R_r.

The segment $S_r(f) + S_r(h)$ has as left (resp. right) endpoint the vector sum of the two left (resp. right) endpoints of $S_r(f)$ and $S_r(h)$.

By (2.11) and (2.12), $(s_0 + \ell_0, u_{s_0} + u'_{\ell_0})$ is the left endpoint of $S_r(fh)$. Hence, in order to show that $S_r(fh) = S_r(f) + S_r(h)$ we need only to check that $(s_d + \ell_{d'}, u_{s_d} + u'_{\ell_{d'}})$ is the right endpoint of $S_r(fh)$.

For any term ag^s of the canonical g-expansion of fh, (2.6) and (2.7) yield:

$$v_{r-1}(a) \geq y_s := (v_r(fh)/e_r) - s(V_r + \lambda_r),$$

and equality holds if and only if $(s, v_{r-1}(ag^s)) \in S_r(fh)$.

For $0 \leq k \leq d + d'$, the summand $b_k g^{\mathfrak{s}_k}$ contributes to the canonical g-expansion of fh with two terms: $b_{k,0}g^{\mathfrak{s}_k}$ and $b_{k,1}g^{\mathfrak{s}_k+1}$. By (D_{r-1}),

$$v_{r-1}(b_{k,1}g) \geq v_{r-1}(b_k) \geq v_{r-1}(a_{s_j}a'_{\ell_i}) = v_{r-1}(a_{s_j}) + v_{r-1}(a'_{\ell_i})$$
$$\geq (v_r(f)/e_r) - s_j(V_r + \lambda_r) + (v_r(h)/e_r) - \ell_i(V_r + \lambda_r) = y_{\mathfrak{s}_k},$$

for some pair (i, j) with $i + j = k$. By (2.6), $v_{r-1}(b_{k,1}) \geq y_{\mathfrak{s}_k} - V_r > y_{\mathfrak{s}_k+1}$. Thus, the contribution of the terms $b_{k,1}g^{\mathfrak{s}_k+1}$ is irrelevant in order to detect points $(s, v_{r-1}(ag^s))$ lying on $S_r(fh)$. More precisely, for any $s \in \mathbb{Z}_{\geq 0}$,

$$(2.13) \qquad (s, v_{r-1}(ag^s)) \in S_r(fh) \iff s = \mathfrak{s}_k \text{ and } v_{r-1}(b_{k,0}) = y_s,$$

for some $0 \leq k \leq d + d'$.

Analogous arguments as those used in the proof of Claim 1 show that

$$v_{r-1}(b_{d+d',0}) = v_{r-1}(a_{s_d}a'_{\ell_{d'}}) = v_{r-1}(a_{s_d}) + v_{r-1}(a'_{\ell_{d'}}) = y_{\mathfrak{s}_{d+d'}}.$$

Hence, (2.13) shows that $(s_d + \ell_{d'}, u_{s_d} + u'_{\ell_{d'}})$ is the right endpoint of $S_r(fh)$. This proves $S_r(fh) = S_r(f) + S_r(h)$ and, moreover:

$$(2.14) \qquad c_{\mathfrak{s}_k}(fh) = c_{\mathfrak{s}_k}(b_{k,0}g^{\mathfrak{s}_k}), \quad 0 \leq k \leq d + d'.$$

Claim 2. For each $0 \leq k \leq d + d'$ we have

$$c_{\mathfrak{s}_k}(fh) = \begin{cases} 0, & \text{if } v_{r-1}(b_k) > y_{\mathfrak{s}_k}, \\ z_{r-1}^{\nu_{r-1}(b_k)}R_{r-1}(b_k)(z_{r-1}), & \text{if } v_{r-1}(b_k) = y_{\mathfrak{s}_k}. \end{cases}$$

By (D_{r-1}), $v_{r-1}(b_{k,0}) \geq v_{r-1}(b_k) \geq y_{\mathfrak{s}_k}$. If either $v_{r-1}(b_k) > y_{\mathfrak{s}_k}$ or $v_{r-1}(b_{k,0}) > v_{r-1}(b_k)$, then $c_{\mathfrak{s}_k}(b_{k,0}g^{\mathfrak{s}_k}) = 0$. In the latter case, $b_k \sim_{v_{r-1}} b_{k,1}g$

and (D_{r-1}) shows that $R_{r-1}(b_k) \in t_{r-1}A_{r-1}[y]$, so that $R_{r-1}(b_k)(z_{r-1}) = 0$. Thus, Claim 2 is correct in both cases, by (2.14).

Finally, suppose $v_{r-1}(b_k) = v_{r-1}(b_{k,0}) = y_{\mathfrak{s}_k}$. By (B_{r-1}),

$$y^{\nu_{r-1}(b_k)}R_{r-1}(b_k) - y^{\nu_{r-1}(b_{k,0})}R_{r-1}(b_{k,0})$$

is either zero or equal to $y^{\nu_{r-1}(b_{k,1}g)}R_{r-1}(b_{k,1}g)$. In both cases, the polynomial vanishes when we replace $y = z_{r-1}$. Thus,

$$c_{\mathfrak{s}_k}(b_{k,0}g^{\mathfrak{s}_k}) = z_{r-1}^{\nu_{r-1}(b_{k,0})}R_{r-1}(b_{k,0})(z_{r-1}) = z_{r-1}^{\nu_{r-1}(b_k)}R_{r-1}(b_k)(z_{r-1}).$$

By (2.14), this ends the proof of Claim 2.

We are ready to prove $R_r(fh) = R_r(f)R_r(h)$, which amounts to

$$(2.15) \qquad \sum\nolimits_{i+j=k} c_{s_j}(f)c_{\ell_i}(h) = c_{\mathfrak{s}_k}(fh), \quad 0 \le k \le d + d'.$$

For any pair (i,j) with $i+j=k$, we have $v_{r-1}(a_{s_j}a'_{\ell_i}) \ge y_{\mathfrak{s}_k}$, and equality holds if and only if $(s_j, u_{s_j}) \in S_r(f)$ and $(\ell_i, u'_{\ell_i}) \in S_r(h)$; or equivalently, $c_{s_j}(f) \ne 0$ and $c_{\ell_i}(h) \ne 0$. Hence, in the left-hand side of the equality (2.15) we need only to consider pairs (i,j) in the set:

$$I = \{(i,j) \mid i+j = k \text{ and } v_{r-1}(a_{s_j}a'_{\ell_i}) = y_{\mathfrak{s}_k}\}.$$

If I is the empty set, then both sides of (2.15) vanish. The right-hand side vanishes by Claim 2, because $v_{r-1}(b_k) > y_{\mathfrak{s}_k}$.

Suppose $I \ne \emptyset$ and let $B_k = \sum_{(i,j)\in I} a_{s_j}a'_{\ell_i}$. Clearly, $v_{r-1}(B_k) \ge y_{\mathfrak{s}_k}$ and

$$v_{r-1}(B_k) > y_{\mathfrak{s}_k} \iff v_{r-1}(b_k) > y_{\mathfrak{s}_k}.$$

If $v_{r-1}(B_k) = v_{r-1}(b_k) = y_{\mathfrak{s}_k}$, then $B_k \sim_{v_{r-1}} b_k$, and by (C_{r-1}):

$$S_{r-1}(B_k) = S_{r-1}(b_k), \quad R_{r-1}(B_k) = R_{r-1}(b_k).$$

From the first equality we deduce $\nu_{r-1}(B_k) = \nu_{r-1}(b_k)$. Thus, by (B_{r-1}):

$$\sum_{(i,j)\in I} y^{\nu_{r-1}(a_{s_j}a'_{\ell_i})}R_{r-1}(a_{s_j}a'_{\ell_i}) = \begin{cases} 0, & \text{if } v_{r-1}(b_k) > y_{\mathfrak{s}_k}, \\ y^{\nu_{r-1}(b_k)}R_{r-1}(b_k), & \text{if } v_{r-1}(b_k) = y_{\mathfrak{s}_k}. \end{cases}$$

By taking $y = z_{r-1}$, we get a similar identity in A_r. The right-hand side of this identity is equal to $c_{\mathfrak{s}_k}(fh)$ by Claim 2. Thus, we need only to show that the left-hand side is equal to $\sum_{(i,j)\in I} c_{s_j}(f)c_{\ell_i}(h)$.

Since a_{s_j} is $\mathbf{t}_{r-1}$-robust, (C_{r-1}) shows that

$$S_{r-1}(a_{s_j}a'_{\ell_i}) = S_{r-1}(a_{s_j}) + S_{r-1}(a'_{\ell_i}), \quad R_{r-1}(a_{s_j}a'_{\ell_i}) = R_{r-1}(a_{s_j})R_{r-1}(a'_{\ell_i}).$$

Since the function $\nu_{r-1}(a)$ depends only on the left endpoint of $S_{r-1}(a)$, from the first equality we deduce $\nu_{r-1}(a_{s_j}a'_{\ell_i}) = \nu_{r-1}(a_{s_j}) + \nu_{r-1}(a'_{\ell_i})$. Hence,

$$z_{r-1}^{\nu_{r-1}(a_{s_j}a'_{\ell_i})}R_{r-1}(a_{s_j}a'_{\ell_i})(z_{r-1}) = c_{s_j}(f)c_{\ell_i}(h).$$

This ends the proof of (C).

Let us prove (D). By (A) and (C), from $f \sim_{v_r} gh$ we deduce:

$$R_r(f) = R_r(gh) = R_r(g)R_r(h) = t_r R_r(h) \in t_r A_r[y].$$

This implies $f_r = \deg(t_r) \le \deg R_r(f) \le \deg(f)/m_r e_r$, the last inequality by the definition of the operator R_r. This proves (i).

Write $f = b_0 + gq$. By (i), $b_0 \not\sim_{v_r} -gq$, so that

$$v_r(f) = \mathrm{Min}\{v_r(b_0), v_r(gq)\}.$$

By (C), $v_r(gq) = v_r(g) + v_r(q)$. A recursive argument proves (ii). $\qquad\square$

Corollary 2.10. *Let* $\mathbf{t}$ *be a type of order* $r \ge 1$. *Let* $f, h \in \mathcal{O}[x]$ *with* f $\mathbf{t}$-*robust. Then,* $N_r^-(fh) = N_r^-(f) + N_r^-(h)$.

Proof. The polygon $N_r^-(f) + N_r^-(h)$ is uniquely determined by the property

$$S_\lambda(N_r^-(f) + N_r^-(h)) = S_\lambda(N_r^-(f)) + S_\lambda(N_r^-(h)),$$

for $-\lambda$ running on the slopes of $N_r^-(f)$ and $N_r^-(h)$ [4, Sec. 1.1]. This is satisfied by $N_r^-(fh)$, by (C) of Theorem 2.9 applied to the type obtained by replacing λ_r with λ in the data of the last level. $\qquad\square$

Definition 2.11. *Let* $\mathbf{t}$ *be a type of order* $r \ge 0$. *For any* $f \in \mathcal{O}[x]$ *we define* $\mathrm{ord}_{\mathbf{t}}(f) = \mathrm{ord}_{t_r}(R_r(f))$ *in* $A_r[y]$ *(see section 1.1).*

If $\mathrm{ord}_{\mathbf{t}}(f) > 0$ *we say that* $\mathbf{t}$ *divides* f, *and we write* $\mathbf{t} \mid f$.

Corollary 2.12. *Let* $\mathbf{t}$ *be a type of order* $r \ge 1$ *and let* $\mathbf{t}_{r-1} = \mathrm{Trunc}_{r-1}(\mathbf{t})$.
  (1) *For any* $f \in \mathcal{O}[x]$ *we have* $\ell(N_r^-(f)) = \mathrm{ord}_{\mathbf{t}_{r-1}}(f)$.
  (2) *If* $f \in \mathcal{O}[x]$ *is* $\mathbf{t}$-*robust, then*

$$\mathrm{ord}_{\mathbf{t}_{r-1}}(fh) = \mathrm{ord}_{\mathbf{t}_{r-1}}(f) + \mathrm{ord}_{\mathbf{t}_{r-1}}(h), \quad \forall h \in \mathcal{O}[x].$$

Proof. Denote $g = g_r$ and let $f = \sum_{0 \le s} a_s g^s$ be the canonical g-expansion of f. Let $I = \{s \in \mathbb{Z}_{\ge 0} \mid v_{r-1}(a_s g^s) = v_{r-1}(f)\}$, and take

$$s_0 = \mathrm{Min}(I), \quad f_0 = \sum_{s \in I} a_s g^s = g^{s_0} h.$$

By (D) of Theorem 2.9, $I \ne \emptyset$, $s_0 = \ell(N_r^-(f))$, and $f \sim_{v_{r-1}} f_0$.

Since g is $\mathbf{t}_{r-1}$-robust, (A) and (C) of Theorem 2.9 show that

$$R_{r-1}(f) = R_{r-1}(f_0) = R_{r-1}(g)^{s_0} R_{r-1}(h) = t_{r-1}^{s_0} R_{r-1}(h).$$

Hence, the corollary will be proven if we show that $t_{r-1} \nmid R_{r-1}(h)$.

To this end, write $h = a_{s_0} + gq$. By (D) and (C) of Theorem 2.9:

$$v_{r-1}(h) = v_{r-1}(a_{s_0}) = v_{r-1}(gq).$$

Hence, (B) of Theorem 2.9 shows that:

$$(2.16) \qquad y^{\nu_{r-1}(a_{s_0})} R_{r-1}(a_{s_0}) + y^{\nu_{r-1}(gq)} R_{r-1}(gq) = y^{\nu_{r-1}(h)} R_{r-1}(h).$$

Now, $R_{r-1}(gq) = R_{r-1}(g) R_{r-1}(q) = t_{r-1} R_{r-1}(q)$. Suppose that t_{r-1} divides $R_{r-1}(h)$. Since $z_0^{\nu_0(a)} = 1$ for all $a \in \mathcal{O}[x]$, and z_{r-1} is a unit in A_r for $r > 1$, we may replace $y = z_{r-1}$ in (2.16), leading to $R_{r-1}(a_{s_0})(z_{r-1}) = 0$. This is impossible, because $\deg R_{r-1}(a_{s_0}) < f_{r-1} = \deg t_{r-1}$. This proves (1).

Item (2) follows immediately from (1) and Corollary 2.10. $\qquad\square$

3. THE SF-OM ALGORITHM

Given N and a monic irreducible $f \in \mathbb{Z}[x]$, the SF-OM algorithm either finds a proper factor of N, or constructs an *SF-OM representation of f with respect to N*.

That is, a finite tree $\mathcal{T}(f)$ of SF-types with the following properties:

(1) The root nodes are the types of order zero attached to the squarefree factors of $\mathrm{red}_N(f)$ in $A_0[y]$.

(2) The leaves $\mathbf{t}_1, \ldots, \mathbf{t}_m$ satisfy $\mathrm{ord}_{\mathbf{t}_i}(f) = 1$ and $\mathrm{Rep}(\mathbf{t}_i) \cap \mathrm{Rep}(\mathbf{t}_j) = \emptyset$ for all $1 \le i \ne j \le m$.

Initially, we compute a squarefree decomposition of $\mathrm{red}_N(f)$ in $A_0[y]$:

$$\mathrm{red}_N(f) = T_1^{\ell_1} \cdots T_k^{\ell_k}, \qquad 1 \le \ell_1 < \cdots < \ell_k.$$

For each squarefree factor T the type of order zero $\mathbf{t}_0 = (T)$ is taken as one of the root nodes of the tree. Let $\ell := \mathrm{ord}_{\mathbf{t}_0}(f) = \mathrm{ord}_T(\mathrm{red}_N(f))$.

If $\ell = 1$, then $\mathbf{t}_0$ is a leaf too. If $\ell > 1$, then $\mathbf{t}_0$ sprouts several branches $\mathbf{t}_{\lambda,t} = (T; (g, \lambda, t))$, where g is a representative of $\mathbf{t}_0$, $-\lambda$ runs on the slopes of $N_{v_0,g}^-(f)$ and t runs on the squarefree factors of $R_{v_0,g,\lambda}(f) \in A_1[y]$, provided by the SFD algorithm.

All types $\mathbf{t}$ obtained along the process branch in a similar way, as long as $\mathrm{ord}_{\mathbf{t}}(f) > 1$. Let us briefly review the relevant subroutines which are used.

`SFD(A, φ)`
Algorithm 1.6 applied to $\varphi \in A[y]$, plus a test to check if the squarefree factors are strongly unitary.

`Newton(t, ℓ, f)`
The type $\mathbf{t}$ of order i is equipped with a representative g. The routine computes the first $\ell + 1$ coefficients $a_0, \ldots, a_\ell$ of the canonical g-expansion $f = \sum_{0 \le s} a_s g^s$, and the Newton polygon of the cloud of points $(s, v_i(a_s g^s))$ for $0 \le s \le \ell$. Then, it tests if $\gcd_{A_i}(R_i(a_s), t_i) = 1$, and certificates that the input polynomial f is $\mathbf{t}$-robust.

`ResidualPolynomial(t, λ, f)`
The type $\mathbf{t}$ of order i is equipped with a representative g. The routine computes the residual polynomial $R_{v_i,g,\lambda}(f) \in A_{i+1}[y]$.

`Representative(t)`
Computation of a representative of $\mathbf{t}$ based on [7, Prop. 3.4].

We now describe the SF-OM algorithm in pseudocode. We emphasize the type to which a certain level data belongs as a superindex: $g_i^{\mathbf{t}}$, $\lambda_i^{\mathbf{t}}$, $t_i^{\mathbf{t}}$, etc.

SF-OM ALGORITHM

INPUT:
- A monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $n > 1$.
- An integer $N > 1$ whose prime factors p satisfy $p > n$.

1 Call $\mathtt{SFD}(A_0, \mathrm{red}_N(f))$, with output $L = [(T_1, \ell_1), \ldots, (T_k, \ell_k)]$

2 If $\ell_1 = 1$ THEN build the type $\mathbf{t} = (T_1)$, set `Leaves` $\leftarrow [\mathbf{t}]$ and delete (T_1, ℓ_1) from the list L ELSE   `Leaves` $\leftarrow [\,]$

3 FOR each (T, ℓ) in L DO

4   Take a robust monic lifting $g \in \mathbb{Z}[x]$ of T and create a type $\mathbf{t}$ with
$$t_0^{\mathbf{t}} \leftarrow T, \quad \omega_1^{\mathbf{t}} \leftarrow \ell, \quad g_1^{\mathbf{t}} \leftarrow g, \quad A_1^{\mathbf{t}} \leftarrow A_0[y]/(T)$$
Initialize a stack `BranchNodes` $\leftarrow [\mathbf{t}]$

WHILE #`BranchNodes` > 0 **DO**

5   Extract a type $\mathbf{t}_0$ from `BranchNodes`. Let $i - 1$ be its order

6   FOR every slope $-\lambda$ of `Newton`$(\mathbf{t}_0, \omega_i^{\mathbf{t}_0}, f)$ DO

7 $\lambda_i^{\mathbf{t}_0} \leftarrow \lambda, \ R_i(f) \leftarrow$ `ResidualPolynomial`$(\mathbf{t}_0, \lambda, f)$

8   Call `SFD`$(A_i^{\mathbf{t}_0}, R_i(f))$, with output $L' = [(T_1', \ell_1'), \ldots, (T_j', \ell_j')]$

9   FOR each (T', ℓ') in L' DO

10 $\mathbf{t} \leftarrow \mathbf{t}_0 \quad t_i^{\mathbf{t}} \leftarrow T', \quad A_{i+1}^{\mathbf{t}} \leftarrow A_i^{\mathbf{t}}[y]/(T'), \quad \omega_{i+1}^{\mathbf{t}} \leftarrow \ell'$

11   IF $\ell' = 1$ THEN add $\mathbf{t}$ to `Leaves` and go to step **5**

12 $g_{i+1}^{\mathbf{t}} \leftarrow$ `Representative`$(\mathbf{t})$ and add $\mathbf{t}$ to `BranchNodes`

END WHILE

OUTPUT:

If no proper factor of N is detected along the process, the types in `Leaves` are the leaves of an SF-OM representation of f with respect to N.

This description of the SF-OM algorithm omits implementation details which are not relevant for the purposes of this paper, like an acceleration of the routine based on the use of *optimal SF-types*.

Also, we omitted all hooks. All subroutines crash if a proper factor of N, or of some modulus $t_i \in A_i[y]$, is detected. In the former case, the routine outputs the factor of N and ends. In the latter case, the algorithm modifies some accumulated data and continues.

More precisely, if a factorization $t_i = \varphi\psi$ in $A_i[y]$ is detected, then all types $\mathbf{t}$ in the stack `BranchNodes` whose truncation at the i-th level is

$$\mathrm{Trunc}_i(\mathbf{t}) = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_i, \lambda_i, t_i))$$

are replaced with two types of order i:

$$\mathbf{t}' = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_i, \lambda_i, \varphi)), \quad \mathbf{t}'' = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_i, \lambda_i, \psi)).$$

4. Tree of irreducible types associated with an SF-type

We fix an SF-type $\mathbf{t} = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r))$. Let A be the inductive artinian algebra attached to $\mathbf{t}$ in section 2.2.

Definition 4.1. *We say that $\mathbf{t}$ is* unramified *if $e_0 = \cdots = e_r = 1$. We say that $\mathbf{t}$ is* irreducible *if N is a prime and all $t_i \in A_i[y]$ are irreducible.*

Irreducible types coincide with the types introduced by Montes [10, 4], except for a different normalization of the data and operators they support, which has been taken from [7].

We fix a prime factor p of N, and denote by $\mathrm{Max}_p(A)$ the set of maximal ideals containing p. For instance, $\mathrm{Max}_p(A_0) = \{\mathfrak{m}_0\}$, with $\mathfrak{m}_0 = pA_0$.

4.1. **Tree of maximal ideals of an inductive artinian algebra.** Consider the formal disjoint union of all the sets $\mathrm{Max}_p(A_i)$:

$$\mathcal{M}_p = \coprod_{i=0}^{r+1} \mathrm{Max}_p(A_i)$$

Note that $\mathrm{Max}_p(A_i)$ and $\mathrm{Max}_p(A_{i+1})$ are disjoint subsets of $\mathcal{M}_p$ even if $A_i = A_{i+1}$, which may occur for several indices $0 \leq i \leq r$.

The set $\mathcal{M}_p$ may be given the structure of a finite connected tree with root node $\mathfrak{m}_0$, by defining the previous node of any $\mathfrak{n} \in \mathrm{Max}_p(A_i)$, with $i > 0$, as the prime ideal $\mathfrak{n} \cap A_{i-1}$. The leaves are the elements in $\mathrm{Max}_p(A)$.

The path joining any $\mathfrak{m} \in \mathrm{Max}_p(A)$ with the root node is:

$$\mathfrak{m}_0 \mapsto \mathfrak{m}_1 \mapsto \cdots \mapsto \mathfrak{m}_r \mapsto \mathfrak{m}_{r+1} = \mathfrak{m}, \qquad \mathfrak{m}_i := \mathfrak{m} \cap A_i,\ 0 \leq i \leq r+1.$$

The finite field $\mathbb{F}_{\mathfrak{m}} = A/\mathfrak{m}$ is an inductive artinian algebra with intermediate fields $\mathbb{F}_{\mathfrak{m}_i} = A_i/\mathfrak{m}_i$, for $0 \leq i \leq r+1$. The canonical mapping $\mathrm{red}_{\mathfrak{m}} \colon A \to \mathbb{F}_{\mathfrak{m}}$ respects the inductive structures:

$$(4.1) \quad \begin{array}{ccccccccc} A_0 & \subset & A_1 & \subset & \cdots & \subset & A_r & \subset & A \\ \downarrow & & \downarrow & & & & \downarrow & & \downarrow \mathrm{red}_{\mathfrak{m}} \\ \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_{\mathfrak{m}_0} & \subset & \mathbb{F}_{\mathfrak{m}_1} & \subset & \cdots & \subset & \mathbb{F}_{\mathfrak{m}_r} & \subset & \mathbb{F}_{\mathfrak{m}}. \end{array}$$

The branches of any node $\mathfrak{n} \in \mathrm{Max}_p(A_i)$ are parameterized by the irreducible factors of $\mathrm{red}_{\mathfrak{n}}(t_i)$ in $\mathbb{F}_{\mathfrak{n}}[y]$. Choose monic polynomials $\psi \in A_i[y]$ such that $\mathrm{red}_{\mathfrak{n}}(\psi)$ are these irreducible factors. Each pair $(\mathfrak{n}, \psi)$ determines a maximal ideal of $A_i[y]$, and the class modulo $t_i A_i[y]$ of this ideal is a maximal ideal of $A_{i+1} = A_i[y]/(t_i)$ whose intersection with A_i is $\mathfrak{n}$.

4.2. **Admissible ϕ-expansions with respect to irreducible types.** Consider an irreducible type of order $r \geq 0$ over $(\mathbb{Z}_p, \mathrm{ord}_p)$:

$$\mathbf{t}^{\star} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r)).$$

The inductive Artin algebra $\mathbb{F}$ associated with $\mathbf{t}^{\star}$ is a chain of finite fields:

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r \subset \mathbb{F}_{r+1} = \mathbb{F}.$$

All polynomials in $\mathbb{Z}_p[x]$ are $\mathbf{t}^{\star}$-robust. Also, a representative of $\mathbf{t}^{\star}$ is necessarily irreducible in $\mathbb{Z}_p[x]$ [4, Thm. 2.11].

Denote by $N_i^{\star}$, $v_i^{\star}$, $R_i^{\star}$ the Newton polygon operators, valuations and residual polynomial operators associated with $\mathbf{t}^{\star}$, respectively.

Denote $\phi = \phi_r$ and consider an arbitrary ϕ-expansion of a non-zero polynomial $f \in \mathbb{Z}_p[x]$, not necessarily the canonical one:

$$(4.2) \qquad f = b_0 + b_1\phi + \cdots + b_s\phi^s + \cdots, \quad b_s \in \mathbb{Z}_p[x].$$

Take $u'_s = v^\star_{r-1}(b_s \phi^s)$ for all $s \geq 0$, and let M be the Newton polygon obtained as the lower convex hull of the set of points (s, u'_s) with $b_s \neq 0$.

To any integer abscissa $0 \leq s$ we attach a residual coefficient as usual:

$$c'_s = \begin{cases} 0, & \text{if } (s, u'_s) \text{ lies above } M, \text{ or } u'_s = \infty, \\ (z^\star_{r-1})^{\nu^\star_{r-1}(b_s)} R^\star_{r-1}(b_s)(z^\star_{r-1}), & \text{if } (s, u'_s) \text{ lies on } M. \end{cases}$$

For the points (s, u'_s) lying on M we now can have $c'_s = 0$, because $R^\star_{r-1}(b_s)$ could be divisible by ψ_{r-1} in $\mathbb{F}_{r-1}[y]$.

Let S be the λ_r-component of M (Definition 2.6), with endpoints having abscissas $s_0 \leq s'_0 = s_0 + de_r$. We can define the residual polynomial

$$R'_r(f) = c'_{s_0} + c'_{s_0+e_r}\, y + \cdots + c'_{s_0+de_r}\, y^d \in \mathbb{F}_r[y].$$

Definition 4.2. *We say that the ϕ-expansion (4.2) is* admissible *if $c'_s \neq 0$ for each abscissa s of a vertex of M^-.*

Admissible ϕ-expansions yield the same principal Newton polygon and the same residual polynomials as the canonical ϕ-expansion.

Definition 4.3. *Let $N \subset \mathbb{R}_{\geq 0} \times \mathbb{R}$ be a Newton polygon, and let i_0 be the abscissa of the left endpoint of N. For any $i_0 \leq s \leq \ell(N)$, let $(s, y_s(N))$ be the unique point on N of abscissa s. For $0 \leq s < i_0$ we take $y_s(N) = \infty$.*

We say that N lies on or above a Newton polygon M, and we write $N \geq M$, if $y_s(N) \geq y_s(M)$ for all $0 \leq s \leq \mathrm{Min}\{\ell(N), \ell(M)\}$.

Lemma 4.4. [4, Lem. 1.12] *For any ϕ-expansion one has $(N^\star_r)^-(f) \geq M^-$. If the ϕ-expansion is admissible, then $(N^\star_r)^-(f) = M^-$ and $R^\star_r(f) = R'_r(f)$.*

4.3. **Tree of irreducible p-types attached to an SF-type.** Recall that $\mathbf{t}_{r-1} = \mathrm{Trunc}_{r-1}(\mathbf{t})$. From now on, we make the following

Assumption: Either $\rho := \mathrm{ord}_p(N) = 1$ or $\mathbf{t}_{r-1}$ is unramified.

The next result reveals, under certain conditions, some arithmetic information about the prime p encoded by the SF-type $\mathbf{t}$.

Theorem 4.5. *For each $\mathfrak{m} \in \mathrm{Max}_p(A)$ there exists an irreducible type*

$$\mathbf{t}_\mathfrak{m} = (\psi_{\mathfrak{m},0}; (\phi_{\mathfrak{m},1}, \lambda_{\mathfrak{m},1}, \psi_{\mathfrak{m},1}); \ldots; (\phi_{\mathfrak{m},r}, \lambda_{\mathfrak{m},r}, \psi_{\mathfrak{m},r}))$$

over $(\mathbb{Z}_p, \mathrm{ord}_p)$, uniquely determined by the following conditions, where all data and operators of $\mathbf{t}_\mathfrak{m}$ are marked with a subscript $\mathfrak{m}$:

(A) *Each $\phi_{\mathfrak{m},i} \in \mathbb{Z}_p[x]$ is a p-adic irreducible factor of g_i, and $\lambda_{\mathfrak{m},i} = \rho\lambda_i$, for $1 \leq i \leq r$. In particular, $e_{\mathfrak{m},i} = e_i$ for $i < r$, and $e_{\mathfrak{m},r} = e_r/\gcd(\rho, e_r)$.*

(B) *Denote $G_{\mathfrak{m},i} = g_i/\phi_{\mathfrak{m},i} \in \mathbb{Z}_p[x]$ for $1 \leq i \leq r$. The following constants, which depend only on $\mathbf{t}$ and $\mathfrak{m}$, are non-zero:*

$$\xi_i = z_{\mathfrak{m},i-1}^{\nu_{\mathfrak{m},i-1}(G_{\mathfrak{m},i})} R_{\mathfrak{m},i-1}(G_{\mathfrak{m},i})(z_{\mathfrak{m},i-1}) \in \mathbb{F}^*_{\mathfrak{m},i}.$$

Hence, starting with the initial values $\chi_0 = \mathrm{red}_p(N/p^\rho)$, $\sigma_0 = 1$, *we may consider non-zero constants in* $\mathbb{F}_{\mathfrak{m},i}$ *defined by the recurrent formulas:*

$$\chi_i = (\chi_{i-1})^{\ell'_i - \ell_i V_i} \, \xi_i^{\ell_i}, \quad \sigma_i = (\chi_{i-1})^{-(e_i V_i + h_i)} \, \xi_i^{e_i}, \quad 1 \le i \le r.$$

(C) *There is a commutative diagram of vertical isomorphisms*

$$
\begin{array}{ccccccccc}
\mathbb{F}_{\mathfrak{m}_0} & \subset & \mathbb{F}_{\mathfrak{m}_1} & \subset & \cdots & \subset & \mathbb{F}_{\mathfrak{m}_r} & \subset & \mathbb{F}_{\mathfrak{m}_{r+1}} = \mathbb{F}_{\mathfrak{m}} \\
\| \iota_0 & & \downarrow \iota_1 & & \cdots & & \downarrow \iota_r & & \downarrow \iota_{r+1} \\
\mathbb{F}_{\mathfrak{m},0} & \subset & \mathbb{F}_{\mathfrak{m},1} & \subset & \cdots & \subset & \mathbb{F}_{\mathfrak{m},r} & \subset & \mathbb{F}_{\mathfrak{m},r+1}
\end{array}
$$

determined by $\iota_{i+1}\left(\mathrm{red}_{\mathfrak{m}}(z_i)\right) = \sigma_i z_{\mathfrak{m},i}$, *for* $0 \le i \le r$.

We shall consider these isomorphisms as identities. Thus, the mapping $\mathrm{red}_{\mathfrak{m}}$ *in (4.1) may be considered as a homomorphism between the inductive Artin algebras of* $\mathbf{t}$ *and* $\mathbf{t}_{\mathfrak{m}}$. *Under these identifications, we have*

$$\mathrm{red}_{\mathfrak{m}}(z_i) = \sigma_i z_{\mathfrak{m},i}, \quad \psi_{\mathfrak{m},i}(y) = \sigma_i^{-\deg(\psi)} \mathrm{red}_{\mathfrak{m}}(\psi)(\sigma_i y), \quad 0 \le i \le r,$$

where $\mathfrak{m}_{i+1} = (\mathfrak{m}_i, \psi)$ *is the parameterization described in section 4.1.*

(D) *The assignment* $\mathfrak{n} \mapsto \mathbf{t}_{\mathfrak{n}}$ *yields a tree isomorphism between the subtree* $\mathcal{M}_p^0 \subset \mathcal{M}_p$ *obtained by deleting the root node* $\mathfrak{m}_0$, *and the full finite subtree of* $\mathcal{T}(\mathbb{Z}_p, \mathrm{ord}_p)$ *having as leaves the types* $\mathbf{t}_{\mathfrak{m}}$ *for all* $\mathfrak{m} \in \mathrm{Max}_p(A)$.

(E) *The sets* $\mathrm{Rep}(\mathbf{t}_{\mathfrak{m}})$, *for* $\mathfrak{m}$ *running on* $\mathrm{Max}_p(A)$, *are pairwise disjoint. Moreover,* $\sum_{\mathfrak{m} \in \mathrm{Max}_p(A)} m_{\mathfrak{m},r+1} = m_{r+1}/\gcd(\rho, e_r)$.

(F) *Let* $f \in \mathcal{O}[x]$ *be a* $\mathbf{t}$-*robust polynomial.*
  (i) *If* $r > 0$, *we have* $N_{\mathfrak{m},r}^-(f) = E_\rho(N_r^-(f))$, *where* $E_\rho \colon \mathbb{R}^2 \to \mathbb{R}^2$ *is the affinity* $E_\rho(x,y) = (x, \rho y)$.
  (ii) $R_{\mathfrak{m},r}(f)(y) = \tau_r(f) \, \mathrm{red}_{\mathfrak{m}}\left(R_r(f)\right)(\sigma_r y^{\gcd(\rho, e_r)})$, *where* $\tau_0(f) = \chi_0^{v_0(f)}$, *and* $\tau_r(f) = (\chi_{r-1})^{u_r(f) - s_r(f) V_r} \, \xi_r^{s_r(f)}$ *for* $r > 0$.

(G) *For any* $f \in \mathcal{O}[x]$, $v_{\mathfrak{m},r}(f) \ge (\rho/\gcd(\rho, e_r)) \, v_r(f)$. *If* f *is* $\mathbf{t}$-*robust, then equality holds.*

(H) *Suppose that* $\gcd(\rho, e_r) = 1$. *Every* $g \in \mathrm{Rep}(\mathbf{t})$ *factors in* $\mathbb{Z}_p[x]$ *as a product of monic irreducible polynomials:*

$$g = \prod_{\mathfrak{m} \in \mathrm{Max}_p(A)} \phi_{\mathfrak{m}}, \qquad \phi_{\mathfrak{m}} \in \mathrm{Rep}(\mathbf{t}_{\mathfrak{m}}),$$

such that $\mathbf{t}_{\mathfrak{m}} \nmid \phi_{\mathfrak{n}}$ *for all* $\mathfrak{m}, \mathfrak{n} \in \mathrm{Max}_p(A)$, $\mathfrak{m} \ne \mathfrak{n}$.

Proof. With the notation of section 4.1, let $\mathfrak{m} = (\mathfrak{m}_r, \psi)$, for some monic $\psi \in A_r[y]$ such that $\mathrm{red}_{\mathfrak{m}}(\psi)$ is an irreducible factor of $\mathrm{red}_{\mathfrak{m}}(t_r)$ in $\mathbb{F}_{\mathfrak{m}_r}[y]$.

We proceed by induction on the order r of $\mathbf{t}$. First, suppose $r = 0$.

We take $\mathbf{t}_{\mathfrak{m}} = (\psi_{\mathfrak{m},0})$, for $\psi_{\mathfrak{m},0} = \mathrm{red}_{\mathfrak{m}}(\psi)$. Thus, $\mathbb{F}_{\mathfrak{m}_0} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_{\mathfrak{m},0}$ and

$$\mathbb{F}_{\mathfrak{m}} = A_1/\mathfrak{m} \simeq \mathbb{F}_{\mathfrak{m}_0}[y]/(\psi_{\mathfrak{m},0}) = \mathbb{F}_{\mathfrak{m},1}.$$

This isomorphism sends $\mathrm{red}_{\mathfrak{m}}(z_0)$ to $z_{\mathfrak{m},0}$. Since t_0 is squarefree, the factors $\psi_{\mathfrak{m},0}$ are pairwise different. This proves (C) and (D).

Clearly, $v_{\mathfrak{m},0} = \mathrm{ord}_p \geq \rho\, v_0$. Equality holds for $\mathbf{t}$-robust polynomials by Lemma 2.5. This proves (G).

For a non-zero $f \in \mathcal{O}[x]$, $R_{\mathfrak{m},0}(f) = \mathrm{red}_p\left(f/p^{v_{\mathfrak{m},0}(f)}\right)$ and $R_0(f) = \mathrm{red}_N\left(f/N^{v_0(f)}\right)$. Since $\mathrm{red}_p = \mathrm{red}_\mathfrak{m} \circ \mathrm{red}_N$, for a robust f we get by (G):

$$(4.3) \qquad R_{\mathfrak{m},0}(f) = \mathrm{red}_p\,(N/p^\rho)^{v_0(f)}\,\mathrm{red}_\mathfrak{m}\left(R_0(f)\right) = \tau_0(f)\,\mathrm{red}_\mathfrak{m}\left(R_0(f)\right).$$

This proves (F).

Let $g \in \mathrm{Rep}(\mathbf{t})$. Since $v_0(g) = 0$, we have $\tau_0(g) = 1$ and (4.3) shows that

$$\mathrm{red}_p(g) = R_{\mathfrak{m},0}(g) = \mathrm{red}_\mathfrak{m}\left(R_0(g)\right) = \mathrm{red}_\mathfrak{m}(t_0) = \prod\nolimits_{\mathfrak{m} \in \mathrm{Max}_p(A)} \psi_{\mathfrak{m},0}.$$

By Hensels' lemma, $g = \prod_{\mathfrak{m} \in \mathrm{Max}_p(A)} \phi_\mathfrak{m}$, for monic irreducible $\phi_\mathfrak{m} \in \mathbb{Z}_p[x]$ with $\mathrm{red}_p(\phi_\mathfrak{m}) = \psi_{\mathfrak{m},0}$. Each $\phi_\mathfrak{m}$ is a representative of $\mathbf{t}_\mathfrak{m}$ and the sets $\mathrm{Rep}(\mathbf{t}_\mathfrak{m})$ are clearly pairwise disjoint. Also,

$$\sum\nolimits_\mathfrak{m} m_{\mathfrak{m},1} = \sum\nolimits_\mathfrak{m} \deg\phi_\mathfrak{m} = \deg g = m_1.$$

This proves (E) and (H). The proof for types of order zero is complete.

We now assume $r > 0$ and the existence of an irreducible p-type

$$\mathbf{t}_{\mathfrak{m}_r} = \left(\psi_{\mathfrak{m},0}; (\phi_{\mathfrak{m},1}, \lambda_{\mathfrak{m},1}, \psi_{\mathfrak{m},1}); \ldots; (\phi_{\mathfrak{m},r-1}, \lambda_{\mathfrak{m},r-1}, \psi_{\mathfrak{m},r-1})\right),$$

such that for each statement (X) of the theorem, the analogous statement (X_{r-1}) concerning $\mathbf{t}_{r-1}$ is true.

By condition (H_{r-1}), the p-adic factorization of g_r takes the form:

$$g_r = \prod\nolimits_{\mathfrak{n} \in \mathrm{Max}_p(A_r)} \phi_\mathfrak{n}.$$

Take $\phi_{\mathfrak{m},r} = \phi_{\mathfrak{m}_r} \in \mathrm{Rep}(\mathbf{t}_{\mathfrak{m}_r})$. Consider the irreducible p-type of order r:

$$\mathbf{t}_\mathfrak{m} := \left(\mathbf{t}_{\mathfrak{m}_r}; (\phi_{\mathfrak{m},r}, \lambda_{\mathfrak{m},r}, \psi_{\mathfrak{m},r})\right),$$

where $\lambda_{\mathfrak{m},r} \in \mathbb{Q}_{>0}$ and $\psi_{\mathfrak{m},r} \in \mathbb{F}_{\mathfrak{m},r}[y]$ monic irreducible, with $\psi_{\mathfrak{m},r}(0) \neq 0$, are uniquely determined by (A), (B) and (C):

$$\lambda_{\mathfrak{m},r} = \rho\lambda_r, \quad \psi_{\mathfrak{m},r}(y) = \sigma_r^{-\deg(\psi)}\,\mathrm{red}_\mathfrak{m}(\psi)(\sigma_r y).$$

Since $t_r(0)$ is a unit in A_r, we have $\mathrm{red}_\mathfrak{m}(\psi)(0) \neq 0$. Hence, we need only to prove (B); that is, $\xi_r \neq 0$, to ensure that $\sigma_r \neq 0$ and $\psi_{\mathfrak{m},r}$ is well defined.

By Theorem 2.9, the operator $R_{\mathfrak{m},r-1}$ is multiplicative; hence,

$$(4.4) \qquad \delta := R_{\mathfrak{m},r-1}(g_r/\phi_{\mathfrak{m},r})(z_{\mathfrak{m},r-1}) = \prod\nolimits_{\mathfrak{n} \neq \mathfrak{m}_r} R_{\mathfrak{m},r-1}(\phi_\mathfrak{n})(z_{\mathfrak{m},r-1}).$$

For every $\mathfrak{n} \in \mathrm{Max}_p(A_r)$, $\mathfrak{n} \neq \mathfrak{m}_r$, we have $\mathbf{t}_{\mathfrak{m}_r} \nmid \phi_\mathfrak{n}$ by (H_{r-1}). Hence, $\psi_{\mathfrak{m},r-1} \nmid R_{\mathfrak{m},r-1}(\phi_\mathfrak{n})$, and $R_{\mathfrak{m},r-1}(\phi_\mathfrak{n})(z_{\mathfrak{m},r-1}) \neq 0$. Thus, the constant δ of (4.4) is nonzero, and this implies $\xi_r \neq 0$. In fact, $\xi_1 = \delta$ for $r = 1$, whereas for $r > 1$, ξ_r is equal to δ times a power of the unit $z_{\mathfrak{m},r-1}$.

Therefore, our type $\mathbf{t}_\mathfrak{m}$ is well defined and satisfies (A), (B) and (C).

By construction, $\mathfrak{n}$ is the previous node of $\mathfrak{m}$ in $\mathcal{M}_p^0$ if and only if $\mathbf{t}_\mathfrak{n}$ is the previous node of $\mathbf{t}_\mathfrak{m}$ in $\mathcal{T}$. This proves (D).

Let us prove (E). Since any $g \in \mathrm{Rep}(\mathbf{t_m})$ is irreducible in $\mathbb{Z}_p[x]$, [4, Lem. 2.4] shows that $R_{\mathfrak{m},i}(g)$ is a power of the irreducible polynomial $\psi_{\mathfrak{m},i}$ in $\mathbb{F}_{\mathfrak{m},i}[y]$, for all $0 \le i \le r$. Now, for $\mathfrak{n} \in \mathrm{Max}_p(A)$, $\mathfrak{n} \ne \mathfrak{m}$, let $\mathfrak{m}_i = \mathfrak{m} \cap A_i$ be the greatest common node in the paths joining $\mathfrak{m}$ and $\mathfrak{n}$ with $\mathfrak{m}_0$. By the construction of $\mathbf{t_m}$ and $\mathbf{t_n}$, we have $\psi_{\mathfrak{m},i} \ne \psi_{\mathfrak{n},i}$, so that g cannot be a representative of $\mathbf{t_n}$. Thus, the sets $\mathrm{Rep}(\mathbf{t_m})$ and $\mathrm{Rep}(\mathbf{t_n})$ are disjoint.

The branches $\mathfrak{m} = \mathfrak{n}_1, \ldots, \mathfrak{n}_k$ of $\mathfrak{m}_r$ are determined by monic liftings $\psi = \psi_1, \ldots, \psi_k \in A_r[y]$ of the irreducible factors of the squarefree polynomial $\mathrm{red}_{\mathfrak{m}}(t_r)$ in $\mathbb{F}_{\mathfrak{m},r}[y]$. Thus,

$$(4.5) \qquad \sum\nolimits_{j=1}^{k} f_{\mathfrak{n}_j,r} = \deg t_r = f_r.$$

Let $d = \gcd(\rho, e_r)$. By (A), $e_{\mathfrak{m},r} = e_r/d$ for all $\mathfrak{m} \in \mathrm{Max}_p(A)$. By (4.5),

$$\sum\nolimits_{j=1}^{k} m_{\mathfrak{n}_j,r+1} = \sum\nolimits_{j=1}^{k} e_{\mathfrak{n}_j,r} f_{\mathfrak{n}_j,r} m_{\mathfrak{n}_j,r}$$
$$= \sum\nolimits_{j=1}^{k} (e_r/d) f_{\mathfrak{n}_j,r} m_{\mathfrak{m}_r,r} = e_r f_r m_{\mathfrak{m}_r,r}/d.$$

By our assumptions, $\gcd(\rho, e_i) = 1$ for all $i < r$. Thus, by (E_{r-1}):

$$\sum\nolimits_{\mathfrak{m} \in \mathrm{Max}_p(A)} m_{\mathfrak{m},r+1} = \sum\nolimits_{\mathfrak{n} \in \mathrm{Max}_p(A_r)} e_r f_r m_{\mathfrak{n},r}/d = e_r f_r m_r/d = m_{r+1}/d.$$

This ends the proof of (E).

Let us prove (F). Assume that $f \in \mathcal{O}[x]$ is $\mathbf{t}$-robust. Denote $g = g_r$, $\phi = \phi_{\mathfrak{m},r}$ and $G = g/\phi$. The canonical g-expansion of f induces in a natural way a ϕ-expansion:

$$(4.6) \qquad f = \sum\nolimits_{0 \le s} a_s g^s = \sum\nolimits_{0 \le s} b_s \phi^s, \quad b_s = a_s G^s.$$

Let $u_s = v_{r-1}(a_s g^s)$, $u'_s = v_{\mathfrak{m},r-1}(b_s \phi^s) = v_{\mathfrak{m},r-1}(a_s g^s)$. Let M be the Newton polygon determined by the ϕ-expansion (4.6); that is, M is the lower convex hull of the set of points $\{(s, u'_s) \mid s \ge 0\}$.

Since a_s and g are $\mathbf{t}_{r-1}$-robust, (G_{r-1}) and Theorem 2.9,(C) show that

$$(4.7) \qquad u'_s = v_{\mathfrak{m},r-1}(a_s) + s\, v_{\mathfrak{m},r-1}(g) = \rho\,(v_{r-1}(a_s) + s\, v_{r-1}(g)) = \rho\, u_s,$$

for all $s \ge 0$. Hence, $M = E_\rho(N_r(f))$.

We now proceed to compare M^- with $N^-_{\mathfrak{m},r}(f)$ by using Lemma 4.4.

By item (C) of Theorem 2.9, the functions $s_{\mathfrak{m},r-1}$ and $u_{\mathfrak{m},r-1}$ convert a product of polynomials into a sum of integers. Therefore, the function $\nu_{\mathfrak{m},r-1} = \ell'_{\mathfrak{m},r-1} s_{\mathfrak{m},r-1} - \ell_{\mathfrak{m},r-1} u_{\mathfrak{m},r-1}$ has the same property.

Hence, by using (F_{r-1}),(ii) and (C_{r-1}), for any abscissa s such that (s, u'_s) lies on M, the residual coefficient c'_s may be expressed as:

$$
\begin{aligned}
c'_s &= z_{\mathfrak{m},r-1}^{\nu_{\mathfrak{m},r-1}(b_s)} R_{\mathfrak{m},r-1}(b_s)(z_{\mathfrak{m},r-1}) \\
&= z_{\mathfrak{m},r-1}^{\nu_{\mathfrak{m},r-1}(a_s)+s\nu_{\mathfrak{m},r-1}(G)} R_{\mathfrak{m},r-1}(a_s)(z_{\mathfrak{m},r-1}) R_{\mathfrak{m},r-1}(G)^s(z_{\mathfrak{m},r-1}) \\
\text{(4.8)} \qquad &= \xi_r^s\, z_{\mathfrak{m},r-1}^{\nu_{\mathfrak{m},r-1}(a_s)} R_{\mathfrak{m},r-1}(a_s)(z_{\mathfrak{m},r-1}) \\
&= \xi_r^s\, z_{\mathfrak{m},r-1}^{\nu_{\mathfrak{m},r-1}(a_s)} \tau_{r-1}(a_s)\,\mathrm{red}_{\mathfrak{m}}\left(R_{r-1}(a_s)\right)(\sigma_{r-1}z_{r-1}), \\
&= \xi_r^s\, z_{\mathfrak{m},r-1}^{\nu_{\mathfrak{m},r-1}(a_s)} \tau_{r-1}(a_s)\,\mathrm{red}_{\mathfrak{m}}\left(R_{r-1}(a_s)(z_{r-1})\right) \neq 0,
\end{aligned}
$$

because, being f **t**-robust, $R_{r-1}(a_s)(z_{r-1})$ is a unit in A_r by Lemma 1.5.

Therefore, the ϕ-expansion (4.6) is admissible with respect to $\mathbf{t}_{\mathfrak{m}}$, and Lemma 4.4 shows that $M^- = N_{\mathfrak{m},r}^-(f)$ and $R'_r(f) = R_{\mathfrak{m},r}(f)$.

The equality between Newton polygons implies $N_{\mathfrak{m},r}^-(f) = E_\rho(N_r^-(f))$.

For the proof of item (ii) we need the following fact.

Claim. $\nu_{\mathfrak{m},r-1}(a_s) = \nu_{r-1}(a_s)$ for all $s \geq 0$.

By (F_{r-1}), $N_{\mathfrak{m},r-1}^-(a_s) = E_\rho(N_{r-1}^-(a_s))$. The affinity E_ρ maps the λ_{r-1}-component of $N_{r-1}^-(a_s)$ into the $\rho\lambda_{r-1}$-component of $N_{\mathfrak{m},r-1}(a_s)$; thus,

$$
\text{(4.9)} \qquad s_{\mathfrak{m},r-1}(a_s) = s_{r-1}(a_s), \quad u_{\mathfrak{m},r-1} = \rho\, u_{r-1}(a_s).
$$

By (A), $e_{\mathfrak{m},r-1} = e_{r-1}$. By our assumptions, either $e_{r-1} = 1$ or $\rho = 1$.

If $e_{r-1} = e_{\mathfrak{m},r-1} = 1$, then $\ell_{\mathfrak{m},r-1} = \ell_{r-1} = 0$ and $\ell'_{\mathfrak{m},r-1} = \ell'_{r-1} = 1$.

If $\rho = 1$, then $\lambda_{\mathfrak{m},r-1} = \lambda_{r-1}$, so that $h_{\mathfrak{m},r-1} = h_{r-1}$. Hence, $\ell_{\mathfrak{m},r-1} = \ell_{r-1}$ and $\ell'_{\mathfrak{m},r-1} = \ell'_{r-1}$. The Claim follows in both cases from (4.9).

We now compare $R_r(f)$ with $R'_r(f) = R_{\mathfrak{m},r}(f)$. Let $s_0 = s_r(f) \leq s'_0$ be the abscissas of the endpoints of the λ_r-component S of $N_r^-(f)$. The affinity E_ρ maps S into the $\rho\lambda_r$-component of M; thus, the latter component has endpoints with the same abscissas $s_0 \leq s'_0$.

For any integer $s_0 \leq s \leq s'_0$ we have $u'_s = \rho u_s$ by (4.7). Hence, the point (s, u_s) lies above $N_r^-(f)$ if and only if the point (s, u'_s) lies above $M^- = E_\rho(N_r^-(f))$. In this situation, we have $c_s = 0 = c'_s$.

Let now $s = s_j = s_0 + je_r$ be such that (s, u_s) lies on S. The identity

$$
\text{(4.10)} \qquad \xi_r^{s_j}\, \sigma_{r-1}^{-\nu_{r-1}(a_{s_j})}\, \tau_{r-1}(a_{s_j}) = \tau_r(f)\,\sigma_r^j,
$$

is straightforward to deduce from the definition of each constant. We need only to have in mind two identities:

$$
\begin{aligned}
u_{r-1}(a_{s_j}) + s_{r-1}(a_{s_j})\lambda_{r-1} &= v_{r-1}(a_{s_j})/e_{r-1}, \\
v_{r-1}(a_{s_j}) + s_j V_r + jh_r &= u_{s_j} + (je_r)\lambda_r = u_r(f),
\end{aligned}
$$

which follow from the definition of v_{r-1} and the fact that (s_j, u_{s_j}) lies on S.

By (4.8), the Claim, (C_{r-1}) and (4.10), we have:

$$
\begin{aligned}
c'_{s_j} &= \xi_r^{s_j}\, z_{\mathfrak{m},r-1}^{\nu_{r-1}(a_{s_j})}\, \tau_{r-1}(a_{s_j})\,\mathrm{red}_{\mathfrak{m}}\left(R_{r-1}(a_{s_j})(z_{r-1})\right) \\
&= \xi_r^{s_j}\, \sigma_{r-1}^{-\nu_{r-1}(a_{s_j})}\, \tau_{r-1}(a_{s_j})\,\mathrm{red}_{\mathfrak{m}}\left(c_{s_j}\right) = \tau_r(f)\sigma_r^j\,\mathrm{red}_{\mathfrak{m}}(c_{s_j}).
\end{aligned}
$$

Item (ii) follows from this identity. In fact, c_{s_j} is the coefficient of y^j in $R_r(f)$, whereas c'_{s_j} is the coefficient of y^{jd} in $R'_r(f)$, where $d = \gcd(\rho, e_r)$, because $s_j = s_0 + je_r = s_0 + jde_{\mathfrak{m},r}$. This ends the proof of (F).

Let us prove (G). By Lemma 4.4, $N^-_{\mathfrak{m},r}(f) \geq M^-$. Also, $u'_s \geq \rho\, u_s$ for all s, by (G$_{r-1}$). Thus, $M \geq E_\rho(N_r(f))$, leading to $N^-_{\mathfrak{m},r}(f) \geq E_\rho(N^-_r(f))$.

By definition, $v_{\mathfrak{m},r}(f)/e_{\mathfrak{m},r}$ is the ordinate where the line of slope $-\rho\lambda_r$ first touching $N^-_{\mathfrak{m},r}(f)$ from below cuts the vertical axis. Since $v_r(f)/e_r$ admits the same interpretation with respect to the polygon $N^-_r(f)$ and the similar line of slope $-\lambda_r$, we deduce that $v_{\mathfrak{m},r}(f)/e_{\mathfrak{m},r} \geq \rho\, v_r(f)/e_r$. By (A), this implies $v_{\mathfrak{m},r}(f) \geq (\rho/\gcd(\rho, e_r))\, v_r(f)$.

Also, this argument shows that equality holds if $N^-_{\mathfrak{m},r}(f) = E_\rho(N_r(f))$, which follows from item (i) of (F) for a $\mathbf{t}$-robust f.

Finally, let us prove (H). Let g be a representative of $\mathbf{t}$, so that $R_r(g) = t_r$. Since g is $\mathbf{t}$-robust, item (ii) of (F) shows that

$$R_{\mathfrak{m},r}(g)(y) = \tau_r(g)\,\mathrm{red}_{\mathfrak{m}}(R_r(g))(\sigma_r y) = \tau_r(g)\,\mathrm{red}_{\mathfrak{m}}(t_r)(\sigma_r y).$$

Since t_r is squarefree, the irreducible factor $\psi_{\mathfrak{m},r}$ of $\mathrm{red}_{\mathfrak{m}}(t_r)(\sigma_r y)$ divides $R_{\mathfrak{m},r}(g)$ only once; in other words, $\mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}}(g) = 1$.

Let $g = \phi_1 \cdots \phi_k$ the factorization of g into a product of monic irreducible polynomials in $\mathbb{Z}_p[x]$. Since $\mathbf{t}_{\mathfrak{m}}$ is irreducible,

$$1 = \mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} g = \mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} \phi_1 + \cdots + \mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} \phi_k.$$

Hence, there exists an index $1 \leq i \leq k$ such that $\mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} \phi_i = 1$ and $\mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} \phi_j = 0$ for all $j \neq i$. Let us denote $\phi_{\mathfrak{m}} = \phi_i$.

An irreducible $\phi_{\mathfrak{m}} \in \mathbb{Z}_p[x]$ with $\mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} \phi_{\mathfrak{m}} = 1$ satisfies $R_{\mathfrak{m},r}(\phi_{\mathfrak{m}}) = \psi_{\mathfrak{m},r}$ and has degree $m_{\mathfrak{m},r+1}$ [4, Lem. 2.4]. Hence, $\phi_{\mathfrak{m}}$ is a representative of $\mathbf{t}_{\mathfrak{m}}$.

By (E), these factors $\phi_{\mathfrak{m}}$ are pairwise different, and:

$$\deg g = m_{r+1} = \sum\nolimits_{\mathfrak{m}\in \mathrm{Max}_p(A)} m_{\mathfrak{m},r+1} = \sum\nolimits_{\mathfrak{m}\in \mathrm{Max}_p(A)} \deg \phi_{\mathfrak{m}}.$$

Hence, $g = \prod_{\mathfrak{m}\in \mathrm{Max}_p(A)} \phi_{\mathfrak{m}}$. $\hfill \square$

Corollary 4.6. *For $r > 1$ and any $\mathfrak{m} \in \mathrm{Max}_p(A)$ we have:*

$$s_{\mathfrak{m},r-1}(G_{\mathfrak{m},r}) = 0, \quad u_{\mathfrak{m},r-1}(G_{\mathfrak{m},r}) = (\rho V_r - V_{\mathfrak{m},r})/e_{r-1}.$$

Proof. As mentioned after Definition 2.8, $N_{r-1}(g_r)$ is one-sided of slope $-\lambda_{r-1}$ and has left endpoint $(0, V_r/e_{r-1})$, whereas $N_{\mathfrak{m},r-1}(\phi_{\mathfrak{m},r})$ is one-sided of slope $-\rho\lambda_{r-1}$ and has left endpoint $(0, V_{\mathfrak{m},r}/e_{r-1})$. Hence,

$$s_{r-1}(g_r) = 0, \qquad u_{r-1}(g_r) = V_r/e_{r-1},$$
$$s_{\mathfrak{m},r-1}(\phi_{\mathfrak{m},r}) = 0, \quad u_{\mathfrak{m},r-1}(\phi_{\mathfrak{m},r}) = V_{\mathfrak{m},r}/e_{r-1}.$$

On the other hand, (F) of Theorem 4.5 shows that

$$s_{\mathfrak{m},r-1}(g_r) = s_{r-1}(g_r) = 0, \quad u_{\mathfrak{m},r-1}(g_r) = \rho\, u_{r-1}(g_r) = \rho\, V_r/e_{r-1}.$$

By Corollary 2.10, $s_{\mathfrak{m},r-1}(G_{\mathfrak{m},r}) = s_{\mathfrak{m},r-1}(g_r) - s_{\mathfrak{m},r-1}(\phi_{\mathfrak{m},r}) = 0$, and $u_{\mathfrak{m},r-1}(G_{\mathfrak{m},r}) = u_{\mathfrak{m},r-1}(g_r) - u_{\mathfrak{m},r-1}(\phi_{\mathfrak{m},r}) = (\rho V_r - V_{\mathfrak{m},r})/e_{r-1}$. $\hfill \square$

Corollary 4.7. *Let $f \in \mathcal{O}[x]$ be a $\mathbf{t}$-robust polynomial and let $\mathfrak{m} \in \mathrm{Max}_p(A)$.*

    (1) *If $r \geq 1$, then $\mathrm{ord}_{\mathbf{t}_{r-1}}(f) = \mathrm{ord}_{\mathbf{t}_{\mathfrak{m},r-1}}(f)$.*

    (2) *If $\gcd(\rho, e_r) = 1$, then $\mathrm{ord}_{\mathbf{t}}(f) \leq \mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}}(f)$. Equality holds if moreover $R_r(f) = t_r^{\mathrm{ord}_{\mathbf{t}}(f)} q$ in $A_r[y]$, with $\gcd_{A_r}(q, t_r) = 1$.*

Proof. Item (1) follows from Theorem 4.5,(F) and Corollary 2.12.

Let $\mathrm{red}_{\mathfrak{m}}(\psi)$ be the irreducible factor of $\mathrm{red}_{\mathfrak{m}}(t_r)$ corresponding to $\mathfrak{m}$, for some $\psi \in A_r[y]$. By (C) and (F) of Theorem 4.5,

$$
\begin{aligned}
\mathrm{ord}_{\mathbf{t}} f &= \mathrm{ord}_{t_r} R_r(f) \leq \mathrm{ord}_{\mathrm{red}_{\mathfrak{m}}(t_r)} \mathrm{red}_{\mathfrak{m}}(R_r(f)) \leq \mathrm{ord}_{\mathrm{red}_{\mathfrak{m}}(\psi)} \mathrm{red}_{\mathfrak{m}}(R_r(f)) \\
&= \mathrm{ord}_{\mathrm{red}_{\mathfrak{m}}(\psi)(\sigma_r y)} \mathrm{red}_{\mathfrak{m}}(R_r(f))(\sigma_r y) = \mathrm{ord}_{\psi_{\mathfrak{m},r}} R_{\mathfrak{m},r}(f) = \mathrm{ord}_{\mathbf{t}_{\mathfrak{m}}} f.
\end{aligned}
$$

If $R_r(f) = t_r^{\mathrm{ord}_{\mathbf{t}}(f)} q$, with $\gcd_{A_r}(q, t_r) = 1$, the two inequalities in this chain become equalities, by Lemma 1.5. $\qquad\square$

5. ARITHMETIC PROPERTIES OF NUMBER FIELDS ENCODED BY SF-TYPES

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 1$. Consider the number field $K = \mathbb{Q}(\theta)$ generated by some root $\theta \in \overline{\mathbb{Q}}$ of f. Let $\mathbb{Z}_K$ be the ring of integers of K.

For a given prime number p, let $\mathrm{ord}_p \colon \overline{\mathbb{Q}}_p^* \longrightarrow \mathbb{Q}$ be the canonical extension of the p-adic valuation to an algebraic closure of $\mathbb{Q}_p$.

Let $\mathcal{P}$ be the set of prime ideals in $\mathbb{Z}_K$ lying above p. For any $\mathfrak{p} \in \mathcal{P}$, denote $\mathbb{F}_{\mathfrak{p}} = \mathbb{Z}_K/\mathfrak{p}$. Let $e_{\mathfrak{p}}$ be the ramification index of $\mathfrak{p}$, and $f_{\mathfrak{p}} = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathbb{F}_{\mathfrak{p}}$ its residual degree. Let $v_{\mathfrak{p}}$ be the discrete valuation on K induced by $\mathfrak{p}$ and let $\mathbb{Z}_{\mathfrak{p}} \subset K$ be its valuation ring. The canonical isomorphism $\mathbb{F}_{\mathfrak{p}} \simeq \mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{\mathfrak{p}}$ will be considered as an identity.

Consider the normalized valuation:

$$
w_{\mathfrak{p}} \colon K \longrightarrow \mathbb{Q} \cup \{\infty\}, \quad w_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha)/e_{\mathfrak{p}},
$$

which extends ord_p to K. Endow K with the $\mathfrak{p}$-adic topology and fix a topological embedding $\iota_{\mathfrak{p}} \colon K \hookrightarrow \overline{\mathbb{Q}}_p$. Then,

$$
w_{\mathfrak{p}}(\alpha) = \mathrm{ord}_p(\iota_{\mathfrak{p}}(\alpha)), \quad \forall\, \alpha \in K.
$$

Notation. For any $h \in \mathbb{Z}_p[x]$ we abuse of language and write $w_{\mathfrak{p}}(h(\theta))$ instead of $\mathrm{ord}_p(h(\iota_{\mathfrak{p}}(\theta)))$.

The polynomial f factorizes in $\mathbb{Z}_p[x]$ as $f = \prod_{\mathfrak{p} \in \mathcal{P}} F_{\mathfrak{p}}$, where $F_{\mathfrak{p}}$ is the minimal polynomial of $\iota_{\mathfrak{p}}(\theta)$ over $\mathbb{Q}_p$.

Consider an integer $N > 1$ and an SF-type over $(\mathbb{Z}, \mathrm{ord}_N)$ of order $r > 0$,

$$
\mathbf{t} = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r)),
$$

with truncates $\mathbf{t}_i = \mathrm{Trunc}_i(\mathbf{t})$ for $0 \leq i \leq r$. Suppose that $\rho := \mathrm{ord}_p(N) > 0$.

Throughout this section we make the following

Assumptions: (1) f is $\mathbf{t}_i$-robust for all $0 \leq i \leq r$,

    (2) Either $\rho = 1$, or $\mathbf{t}$ is unramified.

5.1. **Prime ideals attached to an SF-type.** Let A be the artinian algebra attached to $\mathbf{t}$, and let $\{\mathbf{t}_\mathfrak{m} \mid \mathfrak{m} \in \mathrm{Max}_p(A)\}$ be the tree of irreducible p-types associated with $\mathbf{t}$ in Theorem 4.5. We define

$$\mathcal{P}_\mathbf{t} = \bigcup\nolimits_{\mathfrak{m} \in \mathrm{Max}_p(A)} \mathcal{P}_{\mathbf{t}_\mathfrak{m}}, \qquad \mathcal{P}_{\mathbf{t}_\mathfrak{m}} := \{\mathfrak{p} \in \mathcal{P} \mid \mathbf{t}_\mathfrak{m} \mid F_\mathfrak{p}\}.$$

As we saw in the proof of item (E) of Theorem 4.5, an irreducible polynomial in $\mathbb{Z}_p[x]$ cannot be divided by two different $\mathbf{t}_\mathfrak{m}$'s; hence, these sets $\mathcal{P}_{\mathbf{t}_\mathfrak{m}}$ are pairwise disjoint.

If $\mathbf{t} \mid f$, then $\mathbf{t}_\mathfrak{m} \mid f$ for all $\mathfrak{m}$, by Corollary 4.7. Since

$$0 < \mathrm{ord}_{\mathbf{t}_\mathfrak{m}}(f) = \sum\nolimits_{\mathfrak{p} \in \mathcal{P}} \mathrm{ord}_{\mathbf{t}_\mathfrak{m}}(F_\mathfrak{p}),$$

the sets $\mathcal{P}_{\mathbf{t}_\mathfrak{m}}$ are all non-empty in this case.

Let us fix $g \in \mathrm{Rep}(\mathbf{t})$ and denote $N_{r+1} = N_{v_r,g}$. For each $\mathfrak{m} \in \mathrm{Max}_p(A)$, let $\phi_\mathfrak{m} \in \mathbb{Z}_p[x]$ be the irreducible factor of g attached to $\mathfrak{m}$ in Theorem 4.5.

Lemma 5.1. *Let $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_\mathfrak{m}}$ for some $\mathfrak{m} \in \mathrm{Max}_p(A)$. Then, there is a unique slope $-\mu$ of $N_{r+1}^-(f)$ and a unique monic irreducible factor ψ of $R_{v_\mathfrak{m},r,\phi_\mathfrak{m},\rho\mu}(f)$ such that the irreducible type $(\mathbf{t}_\mathfrak{m}; (\phi_\mathfrak{m}, \rho\mu, \psi))$ divides $F_\mathfrak{p}$.*

Proof. By Theorem 4.5, $N_{v_\mathfrak{m},r,\phi_\mathfrak{m}}(f) = E_\rho(N_{r+1}(f))$, so that the slopes of this polygon are $-\rho\lambda$, for $-\lambda$ running on the slopes of $N_{r+1}(f)$.

The result follows from [4, Thms. 3.1, 3.7]. $\square$

Proposition 5.2. *Suppose that $\mathbf{t} \mid f$ and for each slope $-\lambda$ of $N_{r+1}^-(f)$ Algorithm 1.6 outputs a squarefree decomposition of $R_{v_r,g,\lambda}(f)$ in $A[y]$ with strongly unitary squarefree factors. Consider the types $\mathbf{t}_{\lambda,t} = (\mathbf{t}; (g, \lambda, t))$ for $-\lambda$ a slope of $N_{r+1}^-(f)$ and $t \in A[y]$ a squarefree factor of $R_{v_r,g,\lambda}(f)$.*

If the least positive denominator e_λ of every slope $-\lambda$ satisfies $\gcd(\rho, e_\lambda) = 1$, then we have a splitting of $\mathcal{P}_\mathbf{t}$ into a union of pairwise disjoint subsets:

$$\mathcal{P}_\mathbf{t} = \bigcup\nolimits_{(\lambda,t)} \mathcal{P}_{\mathbf{t}_{\lambda,t}}$$

Proof. It is easy to check that these $\mathcal{P}_{\mathbf{t}_{\lambda,t}}$ are pairwise disjoint subsets of $\mathcal{P}_\mathbf{t}$. Let us show that they cover $\mathcal{P}_\mathbf{t}$.

Take $\mathfrak{p} \in \mathcal{P}_\mathbf{t}$. There is a unique $\mathfrak{m} \in \mathrm{Max}_p(A)$ such that $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_\mathfrak{m}}$. By Lemma 5.1, there is a type $\mathbf{t}'_\mathfrak{m} = (\mathbf{t}_\mathfrak{m}; (\phi_\mathfrak{m}, \rho\mu, \psi))$ dividing $F_\mathfrak{p}$, for a certain slope $-\mu$ of $N_{r+1}^-(f)$.

By Theorem 4.5,(F) applied to the type $\mathbf{t}_{\mu,t}$ (for any choice of t), we have

$$R_{v_\mathfrak{m},r,\phi_\mathfrak{m},\rho\mu}(f) = \tau_{r+1}(f)\,\mathrm{red}_\mathfrak{m}(R_{v_r,g,\mu}(f))(\sigma_{r+1}y),$$

for some non-zero constants $\tau_{r+1}(f), \sigma_{r+1} \in \mathbb{F}_\mathfrak{m}$. Take any monic $\varphi \in A[y]$ such that $\psi(y) = \sigma_{r+1}^{-\deg\varphi}\,\mathrm{red}_\mathfrak{m}(\varphi)(\sigma_{r+1}y)$. Clearly, there is a unique squarefree factor t of $R_{v_r,g,\mu}(f)$ such that $\mathrm{red}_\mathfrak{m}(t)$ is divisible by the irreducible factor $\mathrm{red}_\mathfrak{m}(\varphi)$ of $\mathrm{red}_\mathfrak{m}(R_{v_r,g,\mu}(f))$ in $\mathbb{F}_\mathfrak{m}[y]$. For this choice of t, let $A' = A[t]/(t)$ be the artinian inductive algebra associated with the type $\mathbf{t}_{\mu,t}$. Clearly, $\mathfrak{m}' = (\mathfrak{m}, \varphi)$ determines a maximal ideal of A' for which $\mathbf{t}'_\mathfrak{m} = (\mathbf{t}_{\mu,t})_{\mathfrak{m}'}$. Since, $\mathbf{t}'_\mathfrak{m} \mid F_\mathfrak{p}$, the prime ideal $\mathfrak{p}$ belongs to $\mathcal{P}_{\mathbf{t}_{\mu,t}}$. $\square$

5.2. Computation of $w_{\mathfrak{p}}$ in terms of data of the SF-type.

Proposition 5.3. *For any $h \in \mathbb{Z}_p[x]$ we have*

$$(5.1) \qquad\qquad w_{\mathfrak{p}}(h(\theta)) \geq \rho\, v_r(h)/e_1 \cdots e_r, \quad \forall\, \mathfrak{p} \in \mathcal{P}_{\mathbf{t}}.$$

If h is $\mathbf{t}$-robust and $\gcd_{A_r}(R_r(h), t_r) = 1$, then equality holds.

Proof. Take $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ for some $\mathfrak{m} \in \operatorname{Max}_p(A)$. By [4, Prop. 2.9],

$$(5.2) \qquad\qquad w_{\mathfrak{p}}(h(\theta)) \geq v_{\mathfrak{m},r}(h)/e_{\mathfrak{m},1} \cdots e_{\mathfrak{m},r},$$

and equality holds if and only if $\mathbf{t}_{\mathfrak{m}} \nmid h$. By Theorem 4.5, $e_{\mathfrak{m},i} = e_i$ for all $1 \leq i \leq r$, and $v_{\mathfrak{m},r}(h) \geq \rho\, v_r(h)$. This proves (5.1).

If h is $\mathbf{t}$-robust, then $v_{\mathfrak{m},r}(h) = \rho\, v_r(h)$, by Theorem 4.5. If moreover $\gcd_{A_r}(R_r(h), t_r) = 1$, then $\mathbf{t} \nmid h$. By Corollary 4.7, $\mathbf{t}_{\mathfrak{m}} \nmid h$, so that equality holds in (5.2). Thus, equality holds in (5.1). $\square$

Corollary 5.4. *For all $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$, $w_{\mathfrak{p}}(g_r(\theta)) = \rho(V_r + \lambda_r)/(e_1 \cdots e_{r-1})$.*

Proof. The Newton polygon $N_r(g_r)$ contains a single point $(1, V_r)$, so that $v_r(g_r) = e_r(V_r + \lambda_r)$ and $R_r(g_r) = 1$. The desired equality follows from Proposition 5.3, since g_r is $\mathbf{t}$-robust. $\square$

The next result completes the computation of $w_{\mathfrak{p}}(g_r(\theta))$ for all $\mathfrak{p} \in \mathcal{P}$.

Lemma 5.5. *Let $\mathfrak{p} \in \mathcal{P}$ such that $\mathfrak{p} \notin \mathcal{P}_{\mathbf{t}_\ell}$ for some minimal $0 \leq \ell \leq r$. If $\ell > 0$, let $-\mu$ be the slope of $N_\ell^-(f)$ attached to $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\ell-1}}$, as explained in Lemma 5.1. If $\ell = 0$ take $\mu = 0$. Then,*

$$w_{\mathfrak{p}}(g_r(\theta)) = \rho\,(m_r/m_\ell)\,(V_\ell + \delta)/(e_1 \cdots e_{\ell-1}),$$

where $\delta = \mu$ if $\ell = r$, and $\delta = \operatorname{Min}\{\lambda_\ell, \mu\}$ if $\ell < r$.

Proof. By Theorem 4.5, $g_r = \prod_{\mathfrak{n} \in \operatorname{Max}_p(A_r)} \phi_{\mathfrak{n}}$, so that

$$(5.3) \qquad\qquad w_{\mathfrak{p}}(g_r(\theta)) = \sum_{\mathfrak{n} \in \operatorname{Max}_p(A_r)} w_{\mathfrak{p}}(\phi_{\mathfrak{n}}(\theta)).$$

If $\ell = 0$, then $\phi_{\mathfrak{n}}$ and $F_{\mathfrak{p}}$ are congruent modulo p to a power of two different monic irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}$; hence $w_{\mathfrak{p}}(\phi_{\mathfrak{n}}(\theta)) = 0$ for all $\mathfrak{n}$, so that $w_{\mathfrak{p}}(g_r(\theta)) = 0$.

Suppose $\ell > 0$. Choose any $\mathfrak{m} \in \operatorname{Max}_p(A_r)$ such that $\mathfrak{m}_\ell = \mathfrak{m} \cap A_\ell$ is the unique ideal in $\operatorname{Max}_p(A_\ell)$ such that $\mathfrak{p} \in \mathcal{P}_{(\mathbf{t}_{\ell-1})_{\mathfrak{m}_\ell}}$. The computation of $w_{\mathfrak{p}}(\phi_{\mathfrak{n}}(\theta))$ for $\mathfrak{n} \in \operatorname{Max}_p(A_r)$ depends on the relative position of $(\mathbf{t}_{r-1})_{\mathfrak{n}}$ and $(\mathbf{t}_{\ell-1})_{\mathfrak{m}_\ell}$ in the tree of irreducible p-types attached to $\mathbf{t}$. By (D) of Theorem 4.5, we may use instead the tree $\mathcal{M}_p(A_r)$ of maximal ideals of the inductive artinian algebra A_r containing p, which is easier to handle.

For any $\mathfrak{n} \in \operatorname{Max}_p(A_r)$ we define the intersection index $i := i(\mathfrak{m}, \mathfrak{n})$ as the maximal index $0 \leq i \leq r$ with $\mathfrak{m}_i = \mathfrak{n}_i$. Then, [5, Prop. 4.7] shows that

$$w_{\mathfrak{p}}(\phi_{\mathfrak{n}}(\theta)) = \begin{cases} 0, & \text{if } i = 0, \\ (m_{\mathfrak{n},r}/m_{\mathfrak{m},i})(V_{\mathfrak{m},i} + \rho\lambda_i)/(e_1 \cdots e_{i-1}), & \text{if } 0 < i < \ell, \\ (m_{\mathfrak{n},r}/m_{\mathfrak{m},\ell})(V_{\mathfrak{m},\ell} + \rho\,\delta)/(e_1 \cdots e_{\ell-1}), & \text{if } i \geq \ell. \end{cases}$$

For $0 \le j \le k \le r$, denote:

$$\mathcal{L}_{j,k}(\mathfrak{m}) = \{\mathfrak{n} \in \mathrm{Max}_p(A_k) \mid i(\mathfrak{m}, \mathfrak{n}) = j\},$$
$$\mathcal{M}_{j,k}(\mathfrak{m}) = \{\mathfrak{n} \in \mathrm{Max}_p(A_k) \mid \mathfrak{m}_j = \mathfrak{n}_j\} = \bigcup_{i=j}^{k} \mathcal{L}_{i,k}(\mathfrak{m}).$$

We claim that

(5.4) $$\sum_{\mathfrak{n} \in \mathcal{M}_{j,k}(\mathfrak{m})} m_{\mathfrak{n},k}/m_{\mathfrak{m},j} = m_k/m_j.$$

In fact, if we sum $m_{\mathfrak{n},k}/m_{\mathfrak{m},j}$ over all $\mathfrak{n} \in \mathrm{Max}_p(A_k)$ having the same previous node $\mathfrak{n}' \in \mathrm{Max}_p(A_{k-1})$, we get $e_{k-1}f_{k-1}m_{\mathfrak{n}',k-1}$ by (4.5). Hence,

$$\sum_{\mathfrak{n} \in \mathcal{M}_{j,k}(\mathfrak{m})} m_{\mathfrak{n},k}/m_{\mathfrak{m},j} = e_{k-1}f_{k-1} \sum_{\mathfrak{n}' \in \mathcal{M}_{j,k-1}(\mathfrak{m})} m_{\mathfrak{n}',k-1}/m_{\mathfrak{m},j}.$$

An iteration of this argument proves (5.4), since $\mathcal{M}_{j,j}(\mathfrak{m}) = \{\mathfrak{m}_j\}$.

By (5.3) and the explicit formulas for $w_{\mathfrak{p}}(\phi_{\mathfrak{n}}(\theta))$, we have:

$$w_{\mathfrak{p}}(g_r(\theta)) = \sum_{k=1}^{\ell-1} \sum_{\mathfrak{n} \in \mathcal{L}_{k,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}(V_{\mathfrak{m},k} + \rho\lambda_k)}{m_{\mathfrak{m},k}\, e_1 \cdots e_{k-1}} + \sum_{k=\ell}^{r} \sum_{\mathfrak{n} \in \mathcal{L}_{k,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}(V_{\mathfrak{m},\ell} + \rho\delta)}{m_{\mathfrak{m},\ell}\, e_1 \cdots e_{\ell-1}}.$$

By using $h_{\mathfrak{m},k} = \rho h_k$ and the identity (2.2) for $V_{\mathfrak{m},k}/e_1 \cdots e_{k-1}$, we get

$$w_{\mathfrak{p}}(g_r(\theta)) = \sum_{k=1}^{\ell-1} \left(\sum_{\mathfrak{n} \in \mathcal{L}_{k,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}}{m_{\mathfrak{m},k}} \right) \sum_{1 \le j \le k} \frac{m_{\mathfrak{m},k}}{m_{\mathfrak{m},j}} \frac{\rho\, h_j}{e_1 \cdots e_j}$$

$$+ \sum_{k=\ell}^{r} \left(\sum_{\mathfrak{n} \in \mathcal{L}_{k,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}}{m_{\mathfrak{m},\ell}} \right) \left(\sum_{1 \le j < \ell} \frac{m_{\mathfrak{m},\ell}}{m_{\mathfrak{m},j}} \frac{\rho\, h_j}{e_1 \cdots e_j} + \frac{\rho\delta}{e_1 \cdots e_{\ell-1}} \right).$$

If we group all terms involving $(\rho\, h_j)/(e_1 \cdots e_j)$ for each $1 \le j < \ell$, and we use (5.4), we see that $w_{\mathfrak{p}}(g_r(\theta))$ is equal to

$$\sum_{1 \le j < \ell} \left(\sum_{\mathfrak{n} \in \mathcal{M}_{j,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}}{m_{\mathfrak{m},j}} \right) \frac{\rho\, h_j}{e_1 \cdots e_j} + \left(\sum_{\mathfrak{n} \in \mathcal{M}_{\ell,r}(\mathfrak{m})} \frac{m_{\mathfrak{n},r}}{m_{\mathfrak{m},\ell}} \right) \frac{\rho\, \delta}{e_1 \cdots e_{\ell-1}}$$

$$= \sum_{1 \le j < \ell} \frac{m_r}{m_j} \frac{\rho\, h_j}{e_1 \cdots e_j} + \frac{m_r}{m_\ell} \frac{\rho\, \delta}{e_1 \cdots e_{\ell-1}} = \frac{\rho\, m_r}{m_\ell} \frac{V_\ell + \delta}{e_1 \cdots e_{\ell-1}},$$

the last equality again by (2.2). $\qquad\square$

5.3. Computation of the residue fields attached to prime ideals.
Let $A = A_0[z_0, \ldots, z_r]$ be the artinian algebra associated with $\mathbf{t}$, and denote by $\mathrm{red}_p \colon A \to A/pA$ the homomorphism of reduction modulo p.

The isomorphism (1.1) induces an isomorphism of $(\mathbb{Z}/p\mathbb{Z})$-algebras:

$$\mathrm{red}_p(A) = A/pA \simeq \prod_{\mathfrak{m} \in \mathrm{Max}_p(A)} \mathbb{F}_{\mathfrak{m}}.$$

In this section, we relate this algebra $\mathrm{red}_p(A)$ with the residue fields $\mathbb{F}_{\mathfrak{p}}$ of the prime ideals $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$. To this end, we introduce some rational functions in $\mathbb{Q}(x)$. We agree that $g_0 = x$, $\pi_0 = N$, and we define

$$(5.5) \qquad \phi_i = g_i\, \pi_i^{-V_i}, \quad \gamma_i = \phi_i^{e_i} \pi_i^{-h_i}, \quad \pi_{i+1} = \phi_i^{\ell_i} \pi_i^{\ell_i'}, \quad 0 \le i \le r.$$

For $i > 0$, let $h = \phi_i, \gamma_i$, or π_{i+1}. We may express $h = N^{n_0} g_1^{n_1} \ldots g_i^{n_i} \in \mathcal{S}(v_r)^{-1} \mathcal{O}[x]$, for certain exponents $n_0, \ldots, n_r \in \mathbb{Z}$. In particular,

$$(5.6) \qquad v_r(h) = e_{i+1} \cdots e_r\, v_i(h), \quad w_{\mathfrak{p}}(h(\theta)) = \rho\, v_r(h)/(e_1 \cdots e_r),$$

since this holds for the $\mathbf{t}$-robust polynomials $N, g_1, \ldots, g_i$. The second identity follows from Proposition 5.3, because $R_r(g_j)$ is a unit in A_r for $j \le r$.

Lemma 5.6. (1) $v_r(\phi_r) = h_r$, $v_r(\gamma_r) = 0$, $v_r(\pi_{r+1}) = 1$.
(2) For all $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$ we have

$$w_{\mathfrak{p}}(\phi_r(\theta)) = \rho\, h_r/e_1 \cdots e_r, \quad w_{\mathfrak{p}}(\gamma_r(\theta)) = 0, \quad w_{\mathfrak{p}}(\pi_{r+1}(\theta)) = \rho/e_1 \cdots e_r.$$

Proof. Let us prove the equalities of (1) simultaneously by induction on r. For $r = 0$ they amount to $v_0(x) = 0$ and $v_0(N) = 1$, because $\phi_0 = \gamma_0 = x$ and $\pi_1 = N$. Suppose that (1) holds for all $i < r$. Then by (5.6), we have

$$(5.7) \qquad\qquad v_r(\pi_r) = e_r\, v_{r-1}(\pi_r) = e_r.$$

Hence, by the recurrent definition of the functions,

$$
\begin{aligned}
v_r(\phi_r) &= v_r(g_r) - V_r v_r(\pi_r) = e_r(V_r + \lambda_r) - V_r e_r = e_r \lambda_r = h_r, \\
v_r(\gamma_r) &= e_r v_r(\phi_r) - h_r v_r(\pi_r) = 0, \\
v_r(\pi_{r+1}) &= \ell_r v_r(\phi_r) + \ell_r' v_r(\pi_r) = \ell_r h_r + \ell_r' e_r = 1.
\end{aligned}
$$

Item (2) follows from (5.6) and item (1). $\square$

Lemma 5.7. Consider a rational function $h = N^{n_0} g_1^{n_1} \cdots g_r^{n_r} \in \mathbb{Q}(x)$ with $v_r(h) = 0$. Then, there exist integers $a_1, \ldots, a_r$ such that $h = \gamma_1^{a_1} \cdots \gamma_r^{a_r}$.

Proof. By induction on r. For $r = 0$ the statement is obvious because necessarily $h = 1$. For $r > 0$, we have

$$v_r\left(N^{n_0} g_1^{n_1} \cdots g_{r-1}^{n_{r-1}}\right) \equiv 0 \pmod{e_r}, \qquad v_r(g_r) \equiv h_r \pmod{e_r}.$$

Hence, the condition $v_r(h) = 0$ implies $n_r = e_r m$ for some $m \in \mathbb{Z}$. Now, $h' = h \gamma_r^{-m} = N^{n_0} g_1^{n_1} \cdots g_{r-1}^{n_{r-1}} \pi_r^{m(e_r V_r + h_r)}$ satisfies $h' = N^{\nu_0} g_1^{\nu_1} \cdots g_{r-1}^{\nu_{r-1}}$ for some integers $\nu_0, \ldots, \nu_{r-1}$, and $v_r(h') = v_r(h) - m v_r(\gamma_r) = 0$, by Lemma 5.6. Hence, $h' = \gamma_1^{a_1} \cdots \gamma_{r-1}^{a_{r-1}}$, by the induction hypothesis. $\square$

Theorem 5.8.
  (A) There is an injective homomorphism of $(\mathbb{Z}/p\mathbb{Z})$-algebras:

$$\gamma_{\mathbf{t}} \colon \mathrm{red}_p(A) \hookrightarrow \prod_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}} \mathbb{F}_{\mathfrak{p}}, \quad x \mapsto \gamma_{\mathbf{t}}(x) = (\gamma_{\mathbf{t},\mathfrak{p}}(x))_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}}$$

determined by $\gamma_{\mathbf{t},\mathfrak{p}}(\mathrm{red}_p(z_i)) = \gamma_i(\theta) + \mathfrak{p}$ for all $0 \le i \le r$.

  (B) For all $\mathfrak{m} \in \mathrm{Max}_p(A)$, $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ we have $\gamma_{\mathbf{t},\mathfrak{p}} \circ \mathrm{red}_p = \gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}} \circ \mathrm{red}_{\mathfrak{m}}$.

Moreover, if $\phi_{\mathfrak{m},r}$, $\gamma_{\mathfrak{m},r}$, $\pi_{\mathfrak{m},r+1} \in \mathbb{Q}_p(x)$ are the rational functions associated with $\mathbf{t}_{\mathfrak{m}}$ by the recurrent formulas of (5.5), we have

$$(5.8) \quad \begin{array}{rcl} (\phi_r/\phi_{\mathfrak{m},r})(\theta) + \mathfrak{p} & = & \gamma_{\mathbf{t},\mathfrak{p}}\left(\xi_r \chi_{r-1}^{-V_r}\right), \\ (\gamma_r/\gamma_{\mathfrak{m},r})(\theta) + \mathfrak{p} & = & \gamma_{\mathbf{t},\mathfrak{p}}\left(\sigma_r\right), \\ (\pi_{r+1}/\pi_{\mathfrak{m},r+1}^{\rho})(\theta) + \mathfrak{p} & = & \gamma_{\mathbf{t},\mathfrak{p}}\left(\chi_r\right), \end{array}$$

where $\xi_i, \chi_i, \sigma_i \in \mathbb{F}_{\mathfrak{m},i} \subset \mathbb{F}_{\mathfrak{m}} \subset \mathrm{red}_p(A)$ are defined in Theorem 4.5.

(C) *Let $h \in \mathbb{Z}[x]$. If $r = 0$, take $s_0 = 0$, $u_0 = v_0(h)$. If $r > 0$, take $(s_0, u_0) = (s_r(h), u_r(h))$, the left endpoint of $S_r(h)$. Then, for each $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$,*

$$(5.9) \qquad h(\theta)\phi_r(\theta)^{-s_0}\pi_r(\theta)^{-u_0} + \mathfrak{p} = \gamma_{\mathbf{t},\mathfrak{p}}\left(\mathrm{red}_p(R_r(h)(z_r))\right).$$

Proof. For an irreducible type, statement (B) is trivial and statements (A), (C) were proved in [4, Sec. 3.1].

Thus, for $r \geq 1$, $\mathfrak{m} \in \mathrm{Max}_p(A)$ and $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$, we may apply (C) to the polynomial $G_{\mathfrak{m},r} = g_r/\phi_{\mathfrak{m},r} \in \mathbb{Z}_p[x]$ and the type $\mathbf{t}_{\mathfrak{m},r-1} := (\mathbf{t}_{\mathfrak{m}})_{r-1}$.

Denote $u = (\rho V_r - V_{\mathfrak{m},r})/e_{r-1}$. For $r > 1$, Corollary 4.6 shows that $s_{r-1}(G_{\mathfrak{m},r}) = 0$ and $u_{r-1}(G_{\mathfrak{m},r}) = u$. For the artinian algebra associated with a p-type, the mapping red_p is the identity and (C) yields:

$$(5.10) \quad \begin{array}{rcl} G_{\mathfrak{m},r}(\theta)\pi_{\mathfrak{m},r-1}(\theta)^{-u} + \mathfrak{p} & = & \gamma_{\mathbf{t}_{\mathfrak{m},r-1},\mathfrak{p}}\left(R_{\mathfrak{m},r-1}(G_{\mathfrak{m},r})(z_{\mathfrak{m},r-1})\right) \\ & = & \gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}}\left(\xi_r z_{\mathfrak{m},r-1}^{\ell_{\mathfrak{m},r-1}u}\right), \end{array}$$

the last equality following from $\gamma_{\mathbf{t}_{\mathfrak{m},r-1}} = (\gamma_{\mathbf{t}_{\mathfrak{m}}})_{|\mathbb{F}_{\mathfrak{m},r}}$ and the definition of the constant $\xi_r \in \mathbb{F}_{\mathfrak{m},r}^*$ in Theorem 4.5.

Note that (5.10) holds for $r = 1$ too, because $u = 0 = v_0(G_{\mathfrak{m},1})$.

Let us prove the theorem by induction on r.

For $r = 0$ we have $\mathbf{t} = (t_0)$ and $A = A_0[y]/(t_0) = A_0[z_0]$. Each monic irreducible factor ψ of $\mathrm{red}_p(t_0)$ in $(\mathbb{Z}/p\mathbb{Z})[y]$ determines a maximal ideal $\mathfrak{m} = (\mathfrak{m}_0, \psi) \in \mathrm{Max}_p(A)$ with $\mathbb{F}_{\mathfrak{m}} = (\mathbb{Z}/p\mathbb{Z})[y]/(\psi)$ and $\mathbf{t}_{\mathfrak{m}} = (\psi)$.

For every $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ the polynomial $F_{\mathfrak{p}}$ is congruent to a power of ψ modulo p. Hence, the field $\mathbb{F}_{\mathfrak{m}}$ is embedded into $\mathbb{F}_{\mathfrak{p}}$ by sending the class of y modulo ψ to $\theta + \mathfrak{p} = \gamma_0(\theta) + \mathfrak{p}$. Since $\mathrm{red}_p(A) \simeq \prod_{\mathfrak{m} \in \mathrm{Max}_p(A)} \mathbb{F}_{\mathfrak{m}}$ and the sets $\mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ are pairwise disjoint, this proves (A).

Since $\phi_0 = \phi_{\mathfrak{m},0} = \gamma_0 = \gamma_{\mathfrak{m},0} = x$ and $\pi_1 = N$, $\pi_{\mathfrak{m},1} = p$, statement (B) follows immediately. Although χ_{-1} is not defined, we agree that $\chi_{-1}^0 = 1$.

Finally, the two sides of (5.9) coincide with the element in $\mathbb{F}_{\mathfrak{p}}$ obtained by reducing modulo p the polynomial $h(x)/N^{v_0(h)} \in \mathbb{Z}[x]$ and then replacing x with $\theta + \mathfrak{p}$. This ends the proof of the theorem in the case $r = 0$.

Suppose that $r > 0$ and the theorem holds for types of order less than r. As a consequence of Theorem 4.5 and our general assumptions:

$$e_{\mathfrak{m},i} = e_i, \quad h_{\mathfrak{m},i} = \rho h_i, \quad \ell_{\mathfrak{m},i} = \ell_i, \quad \ell'_{\mathfrak{m},i} = \ell'_i, \quad 1 \leq i \leq r.$$

Let us first prove (B), whose first statement contains an independent definition of $\gamma_{\mathbf{t}}$. For any $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$ and any $a \in A$, let us *define* $\gamma_{\mathbf{t},\mathfrak{p}}(\mathrm{red}_p(a))$ to be $\gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}}(\mathrm{red}_{\mathfrak{m}}(a))$ for the unique $\mathfrak{m} \in \mathrm{Max}_p(A)$ for which $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$.

For the proof of (5.8), we abuse of language and omit evaluation at θ and classes modulo $\mathfrak{p}$. From $\phi_r = g_r \pi_r^{-V_r}$ and $\phi_{\mathfrak{m},r} = \phi_{\mathfrak{m},r} \pi_{\mathfrak{m},r}^{-V_{\mathfrak{m},r}}$, we deduce

$$\phi_r/\phi_{\mathfrak{m},r} = G_{\mathfrak{m},r} \left(\pi_r/\pi_{\mathfrak{m},r}^\rho\right)^{-V_r} \pi_{\mathfrak{m},r}^{V_{\mathfrak{m},r}-\rho V_r}.$$

If $r = 1$, then $u = 0 = V_1$, and (5.10) yields $\phi_r/\phi_{\mathfrak{m},r} = \gamma_{\mathbf{t},\mathfrak{p}}(\xi_1)$, as desired.

If $r > 1$, then (5.10) and the induction hypothesis lead to

$$\phi_r/\phi_{\mathfrak{m},r} = G_{\mathfrak{m},r} \gamma_{\mathbf{t},\mathfrak{p}} \left(\chi_{r-1}^{-V_r}\right) \pi_{\mathfrak{m},r}^{V_{\mathfrak{m},r}-\rho V_r}$$

$$= \gamma_{\mathbf{t},\mathfrak{p}} \left(\xi_r z_{\mathfrak{m},r-1}^{\ell_{r-1}u}\right) \gamma_{\mathbf{t},\mathfrak{p}} \left(\chi_{r-1}^{-V_r}\right) \pi_{\mathfrak{m},r-1}^u \pi_{\mathfrak{m},r}^{-e_{r-1}u}$$

$$= \gamma_{\mathbf{t},\mathfrak{p}} \left(\xi_r \chi_{r-1}^{-V_r}\right) \left(\gamma_{\mathfrak{m},r-1}^{\ell_{r-1}} \pi_{\mathfrak{m},r-1} \pi_{\mathfrak{m},r}^{-e_{r-1}}\right)^u = \gamma_{\mathbf{t},\mathfrak{p}} \left(\xi_r \chi_{r-1}^{-V_r}\right),$$

because $\gamma_{\mathfrak{m},r-1}^{\ell_{r-1}} \pi_{\mathfrak{m},r-1} \pi_{\mathfrak{m},r}^{-e_{r-1}} = 1$ in $\mathbb{Q}_p(x)$ by a direct application of (5.5).

This ends the proof of the first identity in (5.8). The other two identities follow easily from the first one and the induction hypothesis.

Let us prove (A). Since $\gamma_{\mathbf{t}_{\mathfrak{m}}}(z_{\mathfrak{m},i}) = \gamma_{\mathfrak{m},i}(\theta) + \mathfrak{p}$, for all $0 \leq i \leq r$, the homomorphism $\gamma_{\mathbf{t}}$ defined in (B) satisfies:

$$\gamma_{\mathbf{t},\mathfrak{p}}(\mathrm{red}_p(z_i)) = \gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}}(\mathrm{red}_{\mathfrak{m}}(z_i)) = \gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}}(\sigma_i z_{\mathfrak{m},i})$$

$$= \gamma_{\mathbf{t}_{\mathfrak{m}},\mathfrak{p}}(\sigma_i) \left[\gamma_{\mathfrak{m},i}(\theta) + \mathfrak{p}\right] = \gamma_i(\theta) + \mathfrak{p} = \gamma_i(\theta) + \mathfrak{p},$$

by Theorem 4.5 and the second identity in (5.8). Hence, the mapping $\gamma_{\mathbf{t}}$ defined in (A) is well defined and coincides with the mapping $\gamma_{\mathbf{t}}$ defined in (B). Finally, for any $\mathfrak{m} \in \mathrm{Max}_p(A)$, the homomorphism $\gamma_{\mathbf{t}}$ embeds the field $\mathbb{F}_{\mathfrak{m}}$ diagonally into $\prod_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}} \mathbb{F}_{\mathfrak{p}}$. Since the sets $\mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ are pairwise disjoint, $\gamma_{\mathbf{t}}$ is injective. This ends the proof of (A).

Let us prove (C). By Lemma 5.6 and (5.7), for any $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$ we have

$$v_r \left(\phi_r^{s_0} \pi_r^{u_0}\right) = s_0 h_r + u_0 e_r = v_r(h), \quad w_{\mathfrak{p}} \left(\phi_r^{s_0}(\theta) \pi_r^{u_0}(\theta)\right) = \rho\, v_r(h)/(e_1 \cdots e_r).$$

Let $d = \deg R_r(h)$ and denote $s_j = s_0 + je_r$ for $0 \leq j \leq d$. Let $h = \sum_{0 \leq s} a_s g_r^s$ be the canonical g_r-expansion of h and consider $h_0 = \sum_{j=0}^d a_{s_j} g_r^{s_j}$. For any integer abscissa $s \neq s_j$ we have $v_r(a_s g_r^s) > v_r(h)$; hence,

$$w_{\mathfrak{p}}(a_s(\theta) g_r(\theta)^s) > \rho\, v_r(h)(e_1 \cdots e_r) = w_{\mathfrak{p}} \left(\phi_r^{s_0}(\theta) \pi_r^{u_0}(\theta)\right)$$

by Proposition 5.3. Therefore,

$$(5.11) \qquad h(\theta)\phi_r(\theta)^{-s_0} \pi_r(\theta)^{-u_0} + \mathfrak{p} = h_0(\theta)\phi_r(\theta)^{-s_0} \pi_r(\theta)^{-u_0} + \mathfrak{p}.$$

Now, for any $0 \leq j \leq d$, we have the following identity in $\mathbb{Q}(x)$, which is easy to deduce from the recurrent formulas of (5.5) (cf. [4, Lem. 3.4]):

$$a_{s_j}\, g_r^{s_j} \phi_r^{-s_0} \pi_r^{-u_0} = \gamma_{r-1}^{\nu_{r-1}(a_{s_j})} a_{s_j}\, \phi_{r-1}^{-s_{r-1}(a_{s_j})} \pi_{r-1}^{-u_{r-1}(a_{s_j})} \gamma_r^j,$$

If we evaluate the left-hand side at θ, take classes modulo $\mathfrak{p}$ and sum over $0 \leq j \leq d$, we get the left-hand side of (5.9), thanks to (5.11). If we do the same operation with the right-hand side, we get the right-hand side of (5.9), thanks to the induction hypothesis and the definition of $R_r(h)$. $\square$

Corollary 5.9. *If* $\operatorname{ord}_{\mathbf{t}}(f) = 1$ *and* $R_r(f) = t_r q$ *with* $\gcd_{A_r}(q, t_r) = 1$*, then:*
  (1) $e_{\mathfrak{p}} = e_1 \cdots e_r$ *for all* $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}$*, and* $\quad \sum_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}} f_{\mathfrak{p}} = f_0 f_1 \cdots f_r$.
  (2) $\gamma_{\mathbf{t}}$ *is an isomorphism.*

Proof. By Corollary 4.7, $\operatorname{ord}_{\mathbf{t}_{\mathfrak{m}}}(f) = 1$ for all $\mathfrak{m} \in \operatorname{Max}_p(A)$. This implies that every $\mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$ is a one-element set, say $\mathcal{P}_{\mathbf{t}_{\mathfrak{m}}} = \{\mathfrak{p}_{\mathfrak{m}}\}$. By [4, Cor. 3.8],

$$e_{\mathfrak{p}_{\mathfrak{m}}} = e_{\mathfrak{m},1} \cdots e_{\mathfrak{m},r} = e_1 \cdots e_r, \quad f_{\mathfrak{p}_{\mathfrak{m}}} = f_{\mathfrak{m},0} f_{\mathfrak{m},1} \cdots f_{\mathfrak{m},r}.$$

By a recurrent application of (4.5),

$$\sum_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}} f_{\mathfrak{p}} = \sum_{\mathfrak{m} \in \operatorname{Max}_p(A)} f_{\mathfrak{m},0} \cdots f_{\mathfrak{m},r} = f_r \sum_{\mathfrak{n} \in \operatorname{Max}_p(A_r)} f_{\mathfrak{n},0} \cdots f_{\mathfrak{n},r-1} = f_r \cdots f_0.$$

In particular, $\dim_{\mathbb{Z}/p\mathbb{Z}}(\operatorname{red}_p(A)) = f_0 \cdots f_r = \dim_{\mathbb{Z}/p\mathbb{Z}}(\oplus_{\mathfrak{p} \in \mathcal{P}_{\mathbf{t}}} \mathbb{F}_{\mathfrak{p}})$. Since $\gamma_{\mathbf{t}}$ is injective, it is an isomorphism. $\qquad\square$

6. Computation of integral bases

We keep the notation and assumptions from the last section.

6.1. **Reduced p-integral bases.** Let $\mathbb{Z}_{(p)}$ be the local ring of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. Let $\mathbb{Z}_{K,p} \subset K$ be the integral closure of $\mathbb{Z}_{(p)}$ in the number field K. This ring is a free $\mathbb{Z}_{(p)}$-module of rank n. A $\mathbb{Z}_{(p)}$-basis of $\mathbb{Z}_{K,p}$ is called a *p-integral basis* of K.

Consider the following pseudo-valuation extending ord_p to K:

$$w := w_p \colon K \longrightarrow e^{-1}\mathbb{Z} \cup \{\infty\}, \quad w(\alpha) = \operatorname{Min}_{\mathfrak{p} \in \mathcal{P}}\{w_{\mathfrak{p}}(\alpha)\},$$

where $e = \operatorname{lcm}\{e_{\mathfrak{p}} \mid \mathfrak{p} \in \mathcal{P}\}$. The p-integral elements $\alpha \in \mathbb{Z}_{K,p}$ are characterized by the condition $w(\alpha) \geq 0$. Clearly $\mathbb{Q}^* \subset \mathcal{S}_w$ (cf. Definition 2.1).

Definition 6.1. *A subset* $\mathcal{B} = \{\alpha_1, \ldots, \alpha_m\} \subset K$ *is called* p-reduced *if for all families* $a_1, \ldots, a_m \in \mathbb{Z}_{(p)}$*, one has:*

$$(6.1) \qquad w\left(\sum_{1 \leq i \leq m} a_i \alpha_i\right) = \operatorname{Min}\{w(a_i \alpha_i) \mid 1 \leq i \leq m\}.$$

Lemma 6.2. [6, Lem. 5.6] *A* p-reduced *set* $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\} \subset K$ *such that* $w(\mathcal{B}) \subset [0, 1)$ *is a* p-integral basis *of* K.

The reduceness criterion of Theorem 6.4 below plays an essential role.

Definition 6.3. *For each* $\mathfrak{p} \in \mathcal{P}$ *let us fix some* $\pi_{\mathfrak{p}} \in \mathbb{Z}_{\mathfrak{p}}$ *with* $w_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1/e_{\mathfrak{p}}$. *For any value* $\delta \in w(K)$*, consider the* $\mathbb{Z}_{(p)}$-modules:

$$K_\delta = \{\alpha \in K \mid w(\alpha) \geq \delta\} \supset K_\delta^+ = \{\alpha \in K \mid w(\alpha) > \delta\},$$

and the following homomorphism of $\mathbb{Z}_{(p)}$-modules with kernel K_δ^+:

$$\operatorname{red}_\delta \colon K_\delta \longrightarrow V = \prod_{\mathfrak{p} \in \mathcal{P}} \mathbb{F}_{\mathfrak{p}}, \quad \operatorname{red}_\delta(\alpha) = \left(\alpha \pi_{\mathfrak{p}}^{-\lfloor e_{\mathfrak{p}} \delta \rfloor} + \mathfrak{p}\mathbb{Z}_{\mathfrak{p}}\right)_{\mathfrak{p} \in \mathcal{P}}.$$

Theorem 6.4. [6, Lem. 5.7] *Let* $\mathcal{B} \subset K$ *with* $w(\mathcal{B}) \subset [0, 1)$*. Then,* $\mathcal{B}$ *is* p-reduced if and only if $\operatorname{red}_\delta(\mathcal{B}_\delta) \subset V$ *is a* $(\mathbb{Z}/p\mathbb{Z})$-linearly independent family *for all* $\delta \in w(\mathcal{B})$*, where* $\mathcal{B}_\delta = \{\alpha \in \mathcal{B} \mid w(\alpha) = \delta\}$.

FIGURE 3. Newton polygons of f, $q_s g_r^s$ and $r_s = f - q_s g_r^s$
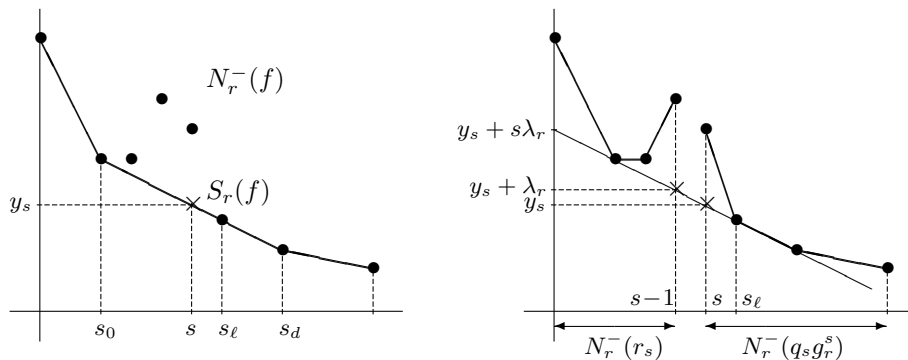
Clearly, the following diagram commutes:

$$
\begin{array}{ccc}
K_\delta \times K_\epsilon & \xrightarrow{\mathrm{red}_\delta \times \mathrm{red}_\epsilon} & V \times V \\
\downarrow & & \downarrow \\
K_{\delta+\epsilon} & \xrightarrow{\mathrm{red}_{\delta+\epsilon}} & V
\end{array}
$$

where the vertical mappings are ordinary multiplication.

6.2. Quotients of g_r-expansions.

Definition 6.5. Let $f = a_0 + a_1 g_r + \cdots + a_m g_r^m$ be the canonical g_r-expansion of f. The g_r-quotients of f are the quotients $q_1, \ldots, q_m \in \mathbb{Z}[x]$ of the divisions with remainder involved in the computation of the coefficients a_s:

$$f = g_r\, q_1 + a_0, \quad q_1 = g_r\, q_2 + a_1, \quad \cdots, \quad q_m = g_r \cdot 0 + a_m = a_m.$$

Clearly, for any $1 \le s \le m$, the canonical g_r-expansion of q_s is:

(6.2) $q_s = a_s + a_{s+1} g_r + \cdots + a_m g_r^{m-s}.$

In particular, if f is **t**-robust, all its g_r-quotients are **t**-robust.

Lemma 6.6. Let $R_r(f) = c_{s_0} + c_{s_1} y + \cdots + c_{s_d} y^d \in A_r[y]$, where $s_0 \le s_d$ are the abscissas of the endpoints of $S_r(f)$ and $s_j = s_0 + j e_r$ for $0 \le j \le d$.
  Take $\ell = \mathrm{Min}\{ j \mid s_j \ge s, \ c_{s_j} \ne 0 \}$. Then,

$$R_r(q_s) = c_{s_\ell} + c_{s_{\ell+1}} y + \cdots + c_{s_d} y^{d-\ell}.$$

Proof. By (6.2), the g_r-expansions of $q_s g_r^s$ and f coincide except for the first s coefficients. Hence, in the region $[s, \infty) \times \mathbb{R}$ both polynomials provide the same cloud of points $(s, v_{r-1}(a_s g_r^s))$. Thus, the Newton polygons $N_r(f)$ and $N_r(q_s g_r^s)$ coincide in the region $[s_\ell, \infty) \times \mathbb{R}$ (cf. Figure 3).

  In particular, the λ_r-component $S_r(q_s g_r^s)$ is contained in $S_r(f)$ and has endpoints with abscissas $s_\ell \le s_d$. Also, the residual coefficients of f and $q_s g_r^s$ coincide for all integer abscissas $s_j \ge s_\ell$. Since $R_r(q_s) = R_r(q_s g_r^s)$, this ends the proof of the lemma. $\square$

Theorem 6.7. *Suppose that $\mathbf{t}_{r-1} \mid f$ and for each slope $-\lambda$ of $N_r^-(f)$ the least positive denominator e_λ of λ satisfies $\gcd(\rho, e_\lambda) = 1$. Also, suppose that Algorithm 1.6 outputs a squarefree decomposition of $R_{v_{r-1}, g_r, \lambda}(f)$ in $A_r[y]$ with strongly unitary squarefree factors.*

Suppose that $-\lambda_r$ is one of the slopes of $N_r^-(f)$, and let $s_0 < s_d$ be the abscissas of the endpoints of $S_r(f)$. For any integer $s_0 < s \leq s_d$, let q_s be the s-th g_r-quotient of f, and denote $H_s = (y_s - sV_r)/(e_0 \cdots e_{r-1})$, where $y_s \in \mathbb{Q}$ is determined by the condition $(s, y_s) \in S_r(f)$. Then,

$$w(q_s(\theta)) \geq \rho\, v_r(q_s)/(e_0 \cdots e_r) = \rho\, H_s.$$

Proof. From $S_r(q_s g_r^s) \subset S_r(f)$ we deduce $v_r(q_s g_r^s) = v_r(f) = e_r(y_s + s\lambda_r)$, as Figure 3 shows. Since $v_r(g_r) = e_r(V_r + \lambda_r)$, we get

$$v_r(q_s) = e_r(y_s - sV_r) = e_0 \cdots e_r\, H_s.$$

We want to check that $w_\mathfrak{p}(q_s(\theta)) \geq \rho\, H_s$ for all $\mathfrak{p} \in \mathcal{P}$. The proof mimics that of [6, Thm. 3.3]. Denote $e = e_0 \cdots e_{r-1}$.

Case $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{r-1}}$. By Proposition 5.2, $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mu,t}}$ for some slope $-\mu$ of $N_r(f)$ and squarefree factor t of $R_{v_{r-1}, g_r, \mu}(f)$.

Let $v_{\mu,r}$ be the r-th pseudo-valuation of $\mathbf{t}_{\mu,t}$. For any polynomial $h \in \mathbb{Z}[x]$, $v_{\mu,r}(h)/e_\mu$ is the ordinate of the intersection point of the vertical axis with the line of slope $-\mu$ first touching $N_r(h)$ from below. Hence, a look at Figure 3 justifies the following arguments.

If $\mu \geq \lambda_r$, Proposition 5.3 applied to $q_s g_r^s$ yields:

$$w_\mathfrak{p}(q_s(\theta) g_r(\theta)^s) \geq \rho\, v_{\mu,r}(q_s g_r^s)/(e e_\mu) \geq \rho(y_s + s\mu)/e,$$

so that $w_\mathfrak{p}(q_s(\theta)) \geq (\rho(y_s + s\mu)/e) - s w_\mathfrak{p}(g_r(\theta)) = \rho\, H_s$, by Corollary 5.4.

If $\mu < \lambda_r$, Proposition 5.3 applied to $r_s = f - q_s g_r^s$ yields:

$$w_\mathfrak{p}(r_s(\theta)) \geq \rho\, v_{\mu,r}(r_s)/(e e_\mu) \geq \rho\,(y_s + \lambda_r + (s-1)\mu)/e > \rho\,(y_s + s\mu)/e.$$

Since $q_s(\theta) g_r(\theta)^s = -r_s(\theta)$, we deduce $w_\mathfrak{p}(q_s(\theta)) > \rho H_s$ in this case.

Case $\mathfrak{p} \notin \mathcal{P}_{\mathbf{t}_{r-1}}$. Take the minimal index $0 \leq \ell < r$ for which $\mathfrak{p} \notin \mathcal{P}_{\mathbf{t}_\ell}$.

Since $-q_s(\theta) = r_s(\theta) g_r(\theta)^{-s} = \sum_{0 \leq i < s} a_i(\theta) g_r(\theta)^{i-s}$, it suffices to show:

$$(6.3) \qquad w_\mathfrak{p}(a_i(\theta)) - w_\mathfrak{p}\left(g_r(\theta)^{s-i}\right) > \rho\, H_s, \quad 0 \leq i < s.$$

Take $g_0 = x$. For any $0 \leq i < s$, consider the multiadic expansion in $\mathbb{Z}[x]$:

$$a_i = \sum_{\mathbf{j} \in J} b_\mathbf{j}\, G^\mathbf{j}, \quad \deg(b_\mathbf{j}) < \deg(g_\ell), \quad G^\mathbf{j} = g_\ell^{j_\ell} \cdots g_{r-1}^{j_{r-1}},$$

where $J = \{(j_\ell, \ldots, j_{r-1}) \mid 0 \leq j_k < e_k f_k \text{ for all } \ell \leq k < r\}$. An iterative application of (2.4) yields $v_{r-1}(a_i) = \mathrm{Min}\{v_{r-1}\left(b_\mathbf{j}\, G^\mathbf{j}\right) \mid \mathbf{j} \in J\}$.

There is an index $\mathbf{j} \in J$ such that $w_\mathfrak{p}(a_i(\theta) \geq w_\mathfrak{p}(b_\mathbf{j}(\theta) G(\theta)^\mathbf{j})$. If $\ell > 0$, we have $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\ell-1}}$, and Proposition 5.3 shows that

$$w_\mathfrak{p}(b_\mathbf{j}(\theta)) \geq \rho\, v_{\ell-1}(b_\mathbf{j})/(e_0 \cdots e_{\ell-1}) = \rho\, v_{r-1}(b_\mathbf{j})/e$$
$$= \rho(v_{r-1}(b_\mathbf{j}\, G^\mathbf{j}) - \rho\, v_{r-1}(G^\mathbf{j}))/e \geq \rho\, v_{r-1}(a_i)/e - \rho\, v_{r-1}(G^\mathbf{j})/e.$$

If $\ell = 0$, $w_\mathfrak{p}(b_\mathbf{j}(\theta)) \geq \rho\, v_0(b_\mathbf{j}) = \rho\, v_{r-1}(b_\mathbf{j})/e$, and the same inequalities hold.

Finally, by the convexity of the Newton polygon:

$$v_{r-1}(a_i g_r^i) \geq y_i \geq y_s + (s-i)\lambda_r.$$

Hence, $v_{r-1}(a_i) \geq y_s - sV_r + (s-i)(V_r + \lambda_r) = y_s - sV_r + v_r(g_r^{s-i})/e_r$.

For any polynomial $h \in \mathbb{Z}[x]$ and any integer $k \geq 0$, denote

$$\epsilon_k(h) := \rho\, v_k(h)/(e_0 \cdots e_k) - w_{\mathfrak{p}}(h(\theta)).$$

The above inequalities yield:

$$(6.4) \qquad w_{\mathfrak{p}}(a_i) - w_{\mathfrak{p}}(g_r(\theta)^{s-i}) \geq \rho\, H_s - \epsilon_{r-1}(G^{\mathbf{j}}) + \epsilon_r(g_r^{s-i}).$$

For any $\ell \leq k < r$, we have $v_{r-1}(g_k)/e = (V_k + \lambda_k)/(e_0 \cdots e_{k-1})$. Take $\delta = \mu$ if $\ell < k$, and $\delta = \mathrm{Min}\,\{\lambda_\ell, \mu\}$ if $\ell = k$. By using (2.2) and the explicit formulas of Lemma 5.5, we obtain:

$$\rho^{-1}\epsilon_{r-1}(g_k) = \frac{m_k}{m_\ell}\frac{\lambda_\ell - \delta}{e_0 \cdots e_{\ell-1}} + \sum_{\ell < u \leq k} \frac{m_k}{m_u}\frac{h_u}{e_0 \cdots e_u}$$

$$\leq \frac{m_k}{m_\ell}\frac{\lambda_\ell - \mathrm{Min}\,\{\lambda_\ell, \mu\}}{e_0 \cdots e_{\ell-1}} + \sum_{\ell < u \leq k} \frac{m_k}{m_u}\frac{h_u}{e_0 \cdots e_u}.$$

$$\rho^{-1}\epsilon_r(g_r) = \frac{m_r}{m_\ell}\frac{\lambda_\ell - \mathrm{Min}\,\{\lambda_\ell, \mu\}}{e_0 \cdots e_{\ell-1}} + \sum_{\ell < u \leq r} \frac{m_r}{m_u}\frac{h_u}{e_0 \cdots e_u} > 0.$$

We may deduce $\epsilon_{r-1}(G^{\mathbf{j}}) < \epsilon_r(g_r)$ from the obvious inequality:

$$j_u m_u + j_{u+1} m_{u+1} + \cdots + j_{r-1} m_{r-1} < m_r, \quad \ell \leq u < r.$$

This proves (6.3), having in mind (6.4) and $\epsilon_r(g_r) > 0$. $\square$

6.3. **Computation of reduced local integral bases.**

Suppose that, for the input (N, f), the SF-OM algorithm of section 3 does not detect a proper factor of N and outputs a tree $\mathcal{T}(f)$ of SF-types.

Definition 6.8. *Let S be a side of a Newton polygon derived, along the execution of the SF-OM algorithm, from a type $\mathbf{t}_{r-1}$ of order $r-1$, with representative g_r. Let $-\lambda_S$ be the slope of S and let $R_{v_{r-1}, g_r, \lambda_S}(f) = c\, T_1^{\ell_1} \cdots T_k^{\ell_k}$ be the squarefree factorization of the residual polynomial attached to S.*

We say that S is a terminal side of order r *if $\ell_1 = 1$. In this case, S determines a leaf of the tree $\mathcal{T}(f)$:*

$$\mathbf{t}_S = (\mathbf{t}_{r-1}; (g_r, \lambda_r, t_r)), \qquad \lambda_r := \lambda_S, \quad t_r := T_1.$$

Let $\mathcal{S}_{\mathrm{trm}}$ be the set of all terminal sides provided by the OM algorithm.

Let $S \in \mathcal{S}_{\mathrm{trm}}$ be a terminal side of order r. For each $1 \leq i \leq r$, let $d_i = \deg R_i(f)$ and denote by s_{d_i} the abscissa of the right endpoint of $S_i(f)$. Moreover, for each $0 \leq j < s_{d_i}$ we introduce the following notation:

$$q_{i,j} = (s_{d_i} - j)\text{-th } g_i\text{-quotient of } f, \qquad H_{i,j} = v_i(q_{i,j})/e_0 \cdots e_i.$$

Let $J_S = \left\{ (j_0, \ldots, j_r) \in \mathbb{N}^{r+1} \mid 0 \leq j_i < e_i f_i,\ 0 \leq i \leq r \right\}$, and define:

$$\mathcal{B}_S = \{ q_{\mathbf{j}} \mid \mathbf{j} \in J_S \}, \qquad q_{\mathbf{j}} = \theta^{j_0} q_{1,j_1}(\theta) \cdots q_{r,j_r}(\theta) N^{-\lfloor H_{1,j_1} + \cdots + H_{r,j_r} \rfloor}.$$

Also, we consider some more integral elements derived from the eventual leaf of $\mathcal{T}(f)$ of order zero. If there is a squarefree factor $t \in A_0[y]$ dividing $\mathrm{red}_N(f)$ with exponent one, the type of order zero $\mathbf{t}^0 = (t)$ is both a root node and a leaf of $\mathcal{T}(f)$. Choose a monic $g \in \mathbb{Z}[x]$ lifting t, and consider the division with remainder $f = q\,g + a$, $\deg(a) < \deg(g)$. Consider the set:

$$\mathcal{B}^0 = \{q(\theta), \theta\,q(\theta), \ldots, \theta^{\deg(t)-1}q(\theta)\}.$$

Definition 6.9. *A set $\mathcal{B} \subset \mathbb{Z}_K$ is a (reduced) N-integral basis of K if it is a (reduced) p-integral basis simultaneously for all prime factors p of N.*

The next theorem is the main result of the paper.

Theorem 6.10. *Suppose that either N is squarefree or all types in $\mathcal{T}(f)$ are unramified. Then, the following set is a reduced N-integral basis of K:*

$$\mathcal{B} = \mathcal{B}^0 \cup \left(\bigcup\nolimits_{S \in \mathcal{S}_{\mathrm{trm}}} \mathcal{B}_S\right).$$

The proof of this theorem requires some auxiliary results.

By a recurrent application of Proposition 5.2, $\mathcal{P}$ splits into the disjoint union of the subsets $\mathcal{P}_\mathbf{t}$, for $\mathbf{t}$ running on the leaves of $\mathcal{T}(f)$. In other words,

$$\mathcal{P} = \mathcal{P}^0 \cup \left(\bigcup\nolimits_{S \in \mathcal{S}_{\mathrm{trm}}} \mathcal{P}_S\right), \qquad \mathcal{P}^0 := \mathcal{P}_{\mathbf{t}^0}, \quad \mathcal{P}_S := \mathcal{P}_{\mathbf{t}_S}.$$

Lemma 6.11. *Let S be a terminal side. For any $\mathbf{j} = (j_0, \ldots, j_r) \in J_S$, there exists $\mathfrak{p} \in \mathcal{P}_S$ such that*

$$(6.5) \qquad w_\mathfrak{p}(\theta^{j_0}) = 0; \qquad w_\mathfrak{p}(q_{i,j_i}(\theta)) = \rho\,H_{i,j_i}, \quad 1 \le i \le r.$$

Proof. Let $\mathbf{t} = \mathbf{t}_S = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r))$.

For any $\mathfrak{p} \in \mathcal{P}_S$, let $\mathfrak{m} \in \mathrm{Max}_p(A)$ such that $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_\mathfrak{m}}$. Then,

$$w_\mathfrak{p}(\theta) > 0 \iff y \mid t_0 \text{ and } \mathfrak{m} \cap A_1 = (\mathfrak{m}_0, y).$$

Hence, there exists $\mathfrak{m}' \in \mathrm{Max}_p(A_1)$ such that $w_\mathfrak{p}(\theta^{j_0}) = 0$ for all $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_\mathfrak{m}}$, for all $\mathfrak{m} \in \mathrm{Max}_p(A)$ with $\mathfrak{m} \cap A_1 = \mathfrak{m}'$. In fact, if $t_0 = y$, then $j_0 = 0$, and any $\mathfrak{m}' \in \mathrm{Max}_p(A_1)$ does the job. If $t_0 \ne y$, there are irreducible factors in $\mathrm{red}_p(t_0)$ leading to maximal ideals in $\mathrm{Max}_p(A_1)$ different from $(\mathfrak{m}_0, y)$.

Now starting with this $\mathfrak{m}' \in \mathrm{Max}_p(A_1)$, we use a recurrent argument to show the existence of $\mathfrak{m} \in \mathrm{Max}_p(A)$ such that $\mathfrak{m} \cap A_1 = \mathfrak{m}'$ and

$$w_\mathfrak{p}(q_{i,j_i}(\theta)) = \rho\,H_{i,j_i}, \quad 1 \le i \le r, \qquad \forall\,\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_\mathfrak{m}}.$$

Suppose $\mathfrak{m}' \in \mathrm{Max}_p(A_r)$ satisfies this condition for all $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}'}}$ and all $i < r$. Denote $q = q_{r,j_r}$. By Theorem 4.5, there is a unique p-adic irreducible factor $\phi_{\mathfrak{m}'}$ of g_r which is a representative of $\mathbf{t}_{\mathfrak{m}'}$, and satisfies

$$R_{\mathfrak{m}',r}(q)(y) = \tau_r(q)\,\mathrm{red}_\mathfrak{m}(R_r(q))(\sigma_r y),$$

for some non-zero constants $\tau_r(q), \sigma_r \in \mathbb{F}_{\mathfrak{m}'}$. By Lemma 6.6,

$$\deg R_r(q) \le (s_{d_r} - (s_{d_r} - j_r))/e_r \le j_r/e_r < f_r.$$

Since $\mathrm{red}_\mathfrak{m}(t_r)$ is squarefree, it has a monic irreducible factor not dividing $\mathrm{red}_\mathfrak{m}(R_r(q))$. If we write this irreducible factor as $\mathrm{red}_\mathfrak{m}(\varphi)$ for some

monic $\varphi \in A_r[y]$, we see that $\psi(y) := \sigma_r^{-\deg \varphi} \mathrm{red}_{\mathfrak{m}}(\varphi)(\sigma_r y)$ does not divide $R_{\mathfrak{m}',r}(q)$. Hence, for the maximal ideal $\mathfrak{m} = (\mathfrak{m}', \varphi)$ in $\mathrm{Max}_p(A_{r+1})$, the type $\mathbf{t}_{\mathfrak{m}} = (\mathbf{t}_{\mathfrak{m}'}; (\phi_{\mathfrak{m}}, \rho \lambda_r, \psi))$ divides f and it does not divide q. Hence,

$$w_{\mathfrak{p}}(q(\theta)) = v_{\mathfrak{m},r}(q)/(e_0 \cdots e_r) = \rho \, v_r(q)/(e_0 \cdots e_r) = \rho \, H_s.$$

for every $\mathfrak{p} \in \mathcal{P}_{\mathbf{t}_{\mathfrak{m}}}$, by [4, Prop. 2.9]. $\square$

Lemma 6.12. *We have* $\#\mathcal{B} = n$ *and* $0 \leq w(\alpha) < 1$, *for all* $\alpha \in \mathcal{B}$.

Proof. By Corollary 5.9, $\#\mathcal{B}^0 = \sum_{\mathfrak{p} \in \mathcal{P}^0} e_{\mathfrak{p}} f_{\mathfrak{p}}$ and

$$\#\mathcal{B}_S = (e_0 f_0) \cdots (e_r f_r) = \sum_{\mathfrak{p} \in \mathcal{P}_S} e_{\mathfrak{p}} f_{\mathfrak{p}}, \quad \forall S \in \mathcal{S}_{\mathrm{trm}}.$$

Hence, $\#\mathcal{B} = \sum_{\mathfrak{p} \in \mathcal{P}} e_{\mathfrak{p}} f_{\mathfrak{p}} = n$.

For any terminal side S and any $\alpha \in \mathcal{B}_S$, we have $0 \leq w(\alpha) < 1$ by Lemma 6.11. Let us show that $w(\alpha) = 0$ for all $\alpha \in \mathcal{B}^0$.

Let $\mathbf{t}^0 = (t)$ be the leaf of order zero of $\mathcal{T}(f)$. Let $g \in \mathbb{Z}[x]$ be a monic lifting of t, and consider the division with remainder $f = qg + a$. We have $\mathrm{red}_N(a) = 0$, and $\mathrm{red}_N(f) = \mathrm{red}_N(q) \, \mathrm{red}_N(g) = \mathrm{red}_N(q) t$, so that $\mathrm{red}_N(q)$ is coprime with t. Hence, $\mathrm{red}_p(q)$ is coprime with $\mathrm{red}_p(t)$, and this implies $w_{\mathfrak{p}}(q(\theta)) = 0$ for all $\mathfrak{p} \in \mathcal{P}^0$.

If $t = y$, then $\mathcal{B}^0 = \{q(\theta)\}$ and the lemma is proven. If $t \neq y$, then $\mathrm{red}_p(t)$ has irreducible factors different from y and there are prime ideals $\mathfrak{p} \in \mathcal{P}^0$ such that $w_{\mathfrak{p}}(\theta) = 0$. For them, we have $w_{\mathfrak{p}}(\theta^j q(\theta)) = 0$ for all j. $\square$

Definition 6.13. *With the notation of Definition 6.8, let S be a terminal side and consider the splitting* $\mathcal{P}_{\mathbf{t}_{r-1}} = \bigcup_{\lambda,t} \mathcal{P}_{\mathbf{t}_{\lambda,t}}$ *of Proposition 5.2:*

A terminal side T is said to dominate *S if there exists a pair (λ, t) with $\lambda \geq \lambda_S$, such that $\mathbf{t}_{\lambda,t}$ is a truncation of the leaf $\mathbf{t}_T$ of $\mathcal{T}(f)$ (or equivalently, $\mathcal{P}_T \subset \mathcal{P}_{\mathbf{t}_{\lambda,t}}$). In this case, we write $T \geq S$.*

Lemma 6.14.   (1) *Domination is a partial ordering on $\mathcal{S}_{\mathrm{trm}}$.*
      (2) *For any $S, T \in \mathcal{S}_{\mathrm{trm}}$ such that $T \not\geq S$, we have*

$$\alpha \in \mathcal{B}_S, \quad \mathfrak{p} \in \mathcal{P}_T \implies w_{\mathfrak{p}}(\alpha) > w(\alpha).$$

Proof. Let $S \in \mathcal{S}_{\mathrm{trm}}$, and let (λ_S, t_S) be the unique pair such that $\mathbf{t}_S = \mathbf{t}_{\lambda_S, t_S}$. The reflexive property $S \geq S$ is obvious.

Let $T \in \mathcal{S}_{\mathrm{trm}}$ such that $T \geq S$. Let (λ, t) be the unique pair such that $\lambda \geq \lambda_S$ and $\mathbf{t}_{\lambda,t}$ is a truncation of $\mathbf{t}_T$.

If $T \neq S$, then $(\lambda_S, t_S) \neq (\lambda, t)$ and $\mathbf{t}_S = \mathbf{t}_{\lambda_S, t_S}$ cannot have $\mathbf{t}_{\lambda,t}$ as one of its truncations. This shows that domination is antisymmetric.

Now, suppose $R \geq T$. If $\mathbf{t}_T = \mathbf{t}_{\lambda,t}$, then there is a pair (λ', t') with $\lambda' \geq \lambda$ such that $\mathbf{t}_{\lambda',t'}$ is a truncation of $\mathbf{t}_R$. If $\mathbf{t}_T \neq \mathbf{t}_{\lambda,t}$, then the previous node of $\mathbf{t}_T$ is a truncation of $\mathbf{t}_R$. In both cases, $R \geq S$. This shows that domination is transitive and ends the proof of item (1).

Let $\alpha = q_{\mathbf{j}} \in \mathcal{B}_S$ for some $\mathbf{j} = (j_0, \ldots, j_r) \in J_S$. If $T \not\geq S$, then a prime ideal $\mathfrak{p} \in \mathcal{P}_T$ satisfies either $\mathfrak{p} \notin \mathcal{P}_{\mathbf{t}_{r-1}}$, or $\mathfrak{p} \in \mathcal{P}_{\mu,t}$ with $\mu < \lambda_S$. In both

FIGURE 4. Newton polygon of q_{r,j_r}. The line L has slope $-\lambda_r$.
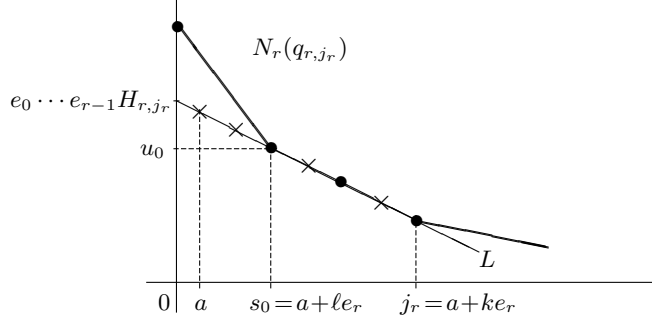
cases, we saw along the proof of Theorem 6.7 that $w_{\mathfrak{p}}(q_{r,j_r}) > \rho\, H_{r,j_r}$. Since $w_{\mathfrak{p}}(q_{i,j_i}) \geq \rho\, H_{i,j_i}$ for all $1 \leq i < r$, again by Theorem 6.7, we deduce

$$w_{\mathfrak{p}}(\alpha) > \rho\,(H_{1,j_1} + \cdots + H_{r,j_r}) = w(\alpha),$$

the last equality by Lemma 6.11. $\qquad\square$

Lemma 6.15. *Let $S \in \mathcal{S}_{\mathrm{trm}}$. For $0 \leq i \leq r$ and any $\epsilon \in \mathbb{Q}$ we denote*

$$\mathcal{B}_{S,\epsilon}^{(i)} = \left\{ \frac{\theta^{j_0} q_{1,j_1}(\theta) \cdots q_{i,j_i}(\theta)}{N^{\lfloor H_{1,j_1} + \cdots + H_{i,j_i} \rfloor}} \;\middle|\; 0 \leq j_\ell < e_\ell f_\ell,\ 0 \leq \ell \leq i \right\} \cap \mathcal{B}_\epsilon.$$

For any $\delta \in w(\mathcal{B}_S)$, there exists a unique integer $0 \leq a < e_r$ such that

$$(6.6) \qquad \mathcal{B}_{S,\delta} := \mathcal{B}_S \cap \mathcal{B}_\delta = \bigcup_{0 \leq k < f_r} q_{r,ke_r+a}(\theta) N^{-m_k} \mathcal{B}_{S,\delta_k}^{(r-1)},$$

where $m_k \in \mathbb{Z}$ and $\delta_k \in \mathbb{Q}$ depend only on S, δ and k.

Proof. Let $\mathbf{t}_S = (t_0; (g_1, \lambda_1, t_1); \ldots; (g_r, \lambda_r, t_r))$. By Corollary 5.9, all $\mathfrak{p} \in \mathcal{P}_S$ have ramification index $e_{\mathfrak{p}} = e_0 \cdots e_r$. Thus, there is an integer b for which

$$\delta = b/e_0 \cdots e_r, \qquad 0 \leq b < e_0 \cdots e_r.$$

Take $\alpha = q_{\mathbf{j}} \in \mathcal{B}_{S,\delta}$ for $\mathbf{j} = (j_0 \ldots, j_r) \in J_S$. Write $\alpha = q_{r,j_r}(\theta) N^{-m_k} \beta$ with

$$\begin{aligned} \beta &= \theta^{j_0} q_{1,j_1}(\theta) \cdots q_{r-1,j_{r-1}}(\theta) N^{-\lfloor H_{1,j_1} + \cdots + H_{r-1,j_{r-1}} \rfloor}, \\ m_k &= \lfloor H_{1,j_1} + \cdots + H_{r,j_r} \rfloor - \lfloor H_{1,j_1} + \cdots + H_{r-1,j_{r-1}} \rfloor. \end{aligned}$$

Denote $s = s_{d_r} - j_r$, $q_s = q_{r,j_r}$, and let $j_r = ke_r + a$, $0 \leq a < e_r$.

The Newton polygon $N_r(q_s)$, displayed in Figure 4, is easy to deduce from $N_r(q_s g_r^s)$, which was described in Figure 3.

We denote by (s_0, u_0) the left endpoint of $S_r(q_s)$, and write $s_0 = \ell e_r + a$ for some integer $0 \leq \ell \leq k$. A look at Figure 4 shows that

$$(6.7) \qquad H_{r,j_r} = (u_0 + s_0 \lambda_r))/e_0 \cdots e_{r-1} = ((u_0 + \ell h_r)e_r + ah_r)/e_0 \cdots e_r.$$

Take $\mathfrak{p} \in \mathcal{P}_S$ satisfying (6.5). By Theorem 6.7,

$$\begin{aligned} w(\alpha) &= w_{\mathfrak{p}}(\alpha) = \rho\,(H_{r,j_r} - m_k) + w_{\mathfrak{p}}(\beta), \\ w(\beta) &= w_{\mathfrak{p}}(\beta) = \rho\,\big(H_{1,j_1} + \cdots + H_{r-1,j_{r-1}} - \lfloor H_{1,j_1} + \cdots + H_{r-1,j_{r-1}} \rfloor\big). \end{aligned}$$

Recall that $e_0 \cdots e_i H_{i,j_i} = v_i(q_{i,j_i}) \in \mathbb{Z}$ for all i. By our general assumptions, $\rho > 1$ occurs only if $e_0 = \cdots = e_r = 1$, in which case all H_{i,j_i} are integers and $w(\alpha) = w(\beta) = 0$. Hence, we may take $\rho = 1$ in the above equations. From these equalities and (6.7) we deduce the existence of $b_k \in \mathbb{Z}$ such that

$$(6.8) \qquad \begin{aligned} w(\beta) &= w_{\mathfrak{p}}(\beta) = b_k/e_0 \cdots e_{r-1}, \qquad 0 \leq b_k < e_0 \cdots e_{r-1}, \\ b/e_0 \cdots e_r &= w(\alpha) = -m_k + ((u_0 + \ell h_r + b_k)e_r + ah_r)/(e_0 \cdots e_r). \end{aligned}$$

Hence, the integer a depends only on S and δ, because it is uniquely determined by the conditions:

$$ah_r \equiv b \pmod{e_r}, \qquad 0 \leq a < e_r.$$

In particular, there are only f_r possible values of $j_r = ke_r + a$, determined by the choice of $0 \leq k < f_r$. Also, the integers m_k, b_k depend only on S, δ and k. In fact, the integers u_0 and ℓ depend only on S and k, and b_k is uniquely determined by the conditions:

$$b_k \equiv \frac{b - ah_r}{e_r} - u_0 - \ell h_r \pmod{(e_0 \cdots e_{r-1})}, \qquad 0 \leq b_k < e_0 \cdots e_{r-1}.$$

The integer m_k is then determined by (6.8). Thus, the proof of (6.6) is complete, by taking $\delta_k = w(\beta) = b_k/e_0 \cdots e_{r-1}$. $\square$

Lemma 6.16. *For $S \in \mathcal{S}_{\mathrm{trm}}$ let $V_S = \prod_{\mathfrak{p} \in \mathcal{P}_S} \mathbb{F}_{\mathfrak{p}}$, and denote $\mathrm{pr}_S \colon V \to V_S$ the canonical projection. Then, $\mathrm{pr}_S(\mathrm{red}_\delta(\mathcal{B}_{S,\delta}))$ is a $(\mathbb{Z}/p\mathbb{Z})$-basis of V_S for all $\delta \in w(\mathcal{B}_S)$.*

Proof. Take $0 \leq i \leq r$ and $\epsilon = c/e_0 \cdots e_i$, for some integer $0 \leq c < e_0 \cdots e_i$. Consider the mapping

$$\mathrm{red}_{S,\epsilon}^{(i)} \colon \mathcal{B}_{S,\epsilon}^{(i)} \longrightarrow V_S, \qquad \alpha \mapsto (\alpha/\pi_{i+1}(\theta)^c + \mathfrak{p}\mathbb{Z}_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}_S}$$

By Lemma 5.6, $w_{\mathfrak{p}}(\pi_{i+1}(\theta)) = \rho/e_0 \cdots e_i$ for all $\mathfrak{p} \in \mathcal{P}_S$. By our general assumptions, $\rho > 1$ implies $e_0 = \cdots = e_i = 1$, in which case $c = 0$. Thus, $w_{\mathfrak{p}}(\pi_{i+1}(\theta)^c) = c/e_0 \cdots e_i = \epsilon$ for all $\mathfrak{p} \in \mathcal{P}_S$, and $\mathrm{red}_{S,\epsilon}^{(i)}$ is well defined.

Let A be the artinian algebra attached to the type $\mathbf{t}_S$. By Corollary 5.9, the mapping $\gamma_{\mathbf{t}_S} \colon \mathrm{red}_p(A) \to V_S$ is an isomorphism. Since $\mathcal{B}_{S,\delta}^{(r)} = \mathcal{B}_{S,\delta}$ and $\mathrm{red}_{S,\delta}^{(r)} = \mathrm{pr}_S \circ \mathrm{red}_\delta$, the lemma is a consequence of the following:

Claim. The set $\gamma_{\mathbf{t}_S}^{-1}\left(\mathrm{red}_{S,\epsilon}^{(i)}\left(\mathcal{B}_{S,\epsilon}^{(i)}\right)\right)$ is a $(\mathbb{Z}/p\mathbb{Z})$-basis of $\mathrm{red}_p(A_{i+1})$.

If $i = 0$, then $\epsilon = 0$ and $\mathcal{B}_{S,0}^{(0)} = \{1, \theta, \ldots, \theta^{f_0-1}\}$. The image of this set under $\gamma_{\mathbf{t}_S}^{-1}$ is $\{1, \mathrm{red}_p(z_0), \ldots, \mathrm{red}_p(z_0)^{f_0-1}\}$, which is a $(\mathbb{Z}/p\mathbb{Z})$-basis of $\mathrm{red}_p(A_1)$ by Lemma 1.2.

Assuming the Claim for some $0 \leq i < r$ and all $\epsilon \in (e_0 \cdots e_i)^{-1}\mathbb{Z} \cap [0, 1)$, let us show that it holds for $i + 1$ and all $\epsilon \in (e_0 \cdots e_{i+1})^{-1}\mathbb{Z} \cap [0, 1)$.

For commodity we work out the case $i = r - 1$.

Let $\delta = b/e_0 \cdots e_r$, with $0 \le b < e_0 \cdots e_r$. By Lemma 6.15, the elements in the set $\mathcal{B}_{S,\delta}^{(r)} = \mathcal{B}_{S,\delta}$ may be parameterized as:

$$\alpha = q_{r,ke_r+a}(\theta) N^{-m_k} \beta, \qquad 0 \le k < f_r, \ \beta \in \mathcal{B}_{S,\delta_k}^{(r-1)}.$$

With the notation of Lemma 6.15, for each $\mathfrak{p} \in \mathcal{P}_S$ we may express $\alpha/\pi_{r+1}(\theta)^b + \mathfrak{p}$ as the product $(\alpha_1 + \mathfrak{p})(\alpha_2 + \mathfrak{p})(\alpha_3 + \mathfrak{p})$, with:

$$\alpha_1 = \frac{q_{r,j_r}(\theta)}{\phi_r(\theta)^{s_0} \pi_r(\theta)^{u_0}}, \qquad \alpha_2 = \frac{\phi_r(\theta)^{s_0} \pi_r(\theta)^{u_0} \pi_r(\theta)^{b_k}}{N^{m_k} \pi_{r+1}(\theta)^b}, \qquad \alpha_3 = \frac{\beta}{\pi_r(\theta)^{b_k}},$$

where (s_0, u_0) are taken from Theorem 5.8. If $R_r(f) = c_0 + c_1 y + \cdots + c_d y^d$, Lemma 6.6 and Theorem 5.8,(C) show that (see Figure 4)

$$\gamma_{\mathbf{t}_S}^{-1} (\alpha_1 + \mathfrak{p})_{\mathfrak{p} \in \mathcal{P}_S} = \operatorname{red}_p(R_r(q_{r,j_r})(z_r)) = \operatorname{red}_p(c_{d-k+\ell} + \cdots + c_d z_r^{k-\ell}).$$

From the identities $b = a h_r - \nu e_r$ (for some integer ν), $s_0 = \ell e_r + a$, and $\ell_r h_r + \ell_r' e_r = 1$, we deduce:

$$(6.9) \quad s_0 - \ell_r b = \ell e_r + a - \ell_r(a h_r - \nu e_r) = (\ell + \ell_r' a + \ell_r \nu) e_r = (\ell + c) e_r,$$

where the integer $c := \ell_r' a + \ell_r \nu$ depends only on S and δ.

Let $h \in \mathbb{Q}(x)$ such that $\alpha_2 = h(\theta)$. By (6.9) and (5.5), we can write

$$h = \phi_r^{s_0} \pi_r^{u_0 + b_k} N^{-m_k} \pi_{r+1}^{-b} = \phi_r^{s_0 - \ell_r b} \pi_r^{u_0 + b_k - \ell_r' b} N^{-m_k}$$
$$= \gamma_r^{\ell+c} \pi_r^{u_0 + b_k - \ell_r' b + (\ell+c) h_r} N^{-m_k} = \gamma_r^{\ell+c} N^{n_0} g_1^{n_1} \cdots g_{r-1}^{n_{r-1}},$$

for some integers $n_0, \ldots, n_{r-1}$. By Lemmas 5.6 and 5.7, $v_r(h) = 0$ and $h = \gamma_r^{\ell+c} \gamma_1^{a_1} \cdots \gamma_{r-1}^{a_{r-1}}$, for some integers $a_1, \ldots, a_{r-1}$. Hence,

$$\gamma_{\mathbf{t}_S}^{-1} (\alpha_2 + \mathfrak{p})_{\mathfrak{p} \in \mathcal{P}_S} = \operatorname{red}_p(z_r)^{\ell+c} \tau_k,$$

where $\tau_k = \operatorname{red}_p(z_1)^{a_1} \cdots \operatorname{red}_p(z_{r-1})^{a_{r-1}}$ is a unit in $\operatorname{red}_p(A_r)$ which depends only on S, δ and k.

Finally, for β running on $\mathcal{B}_{S,\delta_k}^{(r-1)}$, the elements

$$u_\beta := \gamma_{\mathbf{t}_S}^{-1} (\alpha_3 + \mathfrak{p})_{\mathfrak{p} \in \mathcal{P}_S} \in \operatorname{red}_p(A_r)$$

form a $(\mathbb{Z}/p\mathbb{Z})$-basis of $\operatorname{red}_p(A_r)$ by hypothesis. Summing up, we get

$$\gamma_{\mathbf{t}_S}^{-1} \left(\alpha/\pi_{r+1}(\theta)^b + \mathfrak{p} \right)_{\mathfrak{p} \in \mathcal{P}_S} = \operatorname{red}_p(z_r)^c \tau_k \operatorname{red}_p(c_{d-k+\ell} z_r^\ell + \cdots + c_d z_r^k) u_\beta.$$

Since $\operatorname{red}_p(z_r)$ is a unit, the absolute constant $\operatorname{red}_p(z_r)^c$ (depending only on S and δ) may be dropped from all these elements. Denote

$$\zeta_{k,\beta} = \tau_k \operatorname{red}_p(c_{d-k+\ell} z_r^\ell + \cdots + c_d z_r^k) u_\beta.$$

Since the pairs (k, β) take $f_0 f_1 \cdots f_r = \dim_{\mathbb{Z}/p\mathbb{Z}} \operatorname{red}_p(A)$ values, we need only to show that these elements $\zeta_{k,\beta}$ are linearly independent.

Suppose that for some family of elements $a_{k,\beta} \in \mathbb{Z}/p\mathbb{Z}$, we have

$$(6.10) \qquad\qquad \sum_{k,\beta} a_{k,\beta} \zeta_{k,\beta} = 0.$$

Consider $w_0, \ldots, w_{f_r-1} \in \mathrm{red}_p(A_r)$ such that

$$0 = \sum_{k,\beta} a_{k,\beta}\, \zeta_{k,\beta} = w_0 + w_1\, \mathrm{red}_p(z_r) + \cdots + w_{f_r-1}\, \mathrm{red}_p(z_r)^{f_r-1}.$$

Lemma 1.2 shows that all these coefficients are equal to zero. On the other hand, our explicit formulas show that

$$0 = w_{f_r-1} = \tau_{f_r-1}\, \mathrm{red}_p(c_d) \sum_\beta a_{f_r-1,\beta}\, u_\beta.$$

Since τ_{f_r-1} and $\mathrm{red}_p(c_d)$ are units, we deduce $0 = \sum_\beta a_{f_r-1,\beta}\, u_\beta$, leading to $a_{f_r-1,\beta} = 0$ for all $\beta \in \mathcal{B}^{(r-1)}_{S,\delta_{f_r-1}}$, by our hypothesis. Hence, we obtain an identity like (6.10) for $0 \le k \le f_r - 2$. An iteration of this argument shows that $a_{k,\beta} = 0$ for all k, β, so that our family $\zeta_{k,\beta}$ is linearly independent. $\quad\square$

Proof of Theorem 6.10. Let p be a prime factor of N. By Lemmas 6.2 and 6.12, it suffices to show that $\mathcal{B}$ is a p-reduced set. By Theorem 6.4 we must prove that $\mathrm{red}_\delta(\mathcal{B}_\delta)$ is $(\mathbb{Z}/p\mathbb{Z})$-linearly independent for all $\delta \in w(\mathcal{B})$.

Denote $\mathcal{B}_{\mathrm{trm},\delta} = \bigcup_{S \in \mathcal{S}_{\mathrm{trm}}} \mathcal{B}_{S,\delta}$. Let us first discuss the case $\delta = 0$. We saw along the proof of Lemma 6.12 that $\mathcal{B}^0 \subset \mathcal{B}_0$. Consider the splitting:

$$V = V^0 \times V_{\mathrm{trm}}, \quad V^0 = \prod_{\mathfrak{p} \in \mathcal{P}^0} \mathbb{F}_\mathfrak{p}, \quad V_{\mathrm{trm}} = \prod_{\mathfrak{p} \notin \mathcal{P}^0} \mathbb{F}_\mathfrak{p}.$$

By the proof of Theorem 6.7 applied to the types of order zero given by the root nodes of $\mathcal{T}(f)$, we have

$$w_\mathfrak{p}(q(\theta)) > 0, \ \forall \mathfrak{p} \notin \mathcal{P}^0; \qquad w_\mathfrak{p}(\alpha) > 0, \ \forall \mathfrak{p} \in \mathcal{P}^0, \ \forall \alpha \in \mathcal{B}_{\mathrm{trm},0}.$$

Hence, $\mathrm{red}_0(\mathcal{B}^0) \subset V^0 \times \{0\}$ and $\mathrm{red}_0(\mathcal{B}_{\mathrm{trm},0}) \subset \{0\} \times V_{\mathrm{trm}}$.

It is obvious that $\mathrm{red}_0(\mathcal{B}^0)$ is linearly independent. Thus, $\mathrm{red}_0(\mathcal{B}_0)$ is linearly independent if and only if $\mathrm{red}_0(\mathcal{B}_{\mathrm{trm},0})$ is linearly independent.

Since for $\delta > 0$ we have $\mathcal{B}_\delta = \mathcal{B}_{\mathrm{trm},\delta}$, the proof of the theorem will be complete if we show that $\mathrm{red}_\delta(\mathcal{B}_{\mathrm{trm},\delta})$ is linearly independent for all $\delta \ge 0$.

For any given $\delta \in w(\mathcal{B})$, let $\mathcal{S}_\delta := \{S \in \mathcal{S}_{\mathrm{trm}} \mid \mathcal{B}_{S,\delta} \ne \emptyset\}$. For any $S \in \mathcal{S}_\delta$ write $\mathrm{red}_\delta(\mathcal{B}_{S,\delta}) = \{\zeta_{S,m} \mid 1 \le m \le \#\mathcal{B}_{S,\delta}\} \subset V$.

Suppose that for some family of elements $a_{S,m} \in \mathbb{Z}/p\mathbb{Z}$, we have

$$(6.11) \qquad\qquad \sum_{S,m} a_{S,m}\, \zeta_{S,m} = 0,$$

the sum running on $S \in \mathcal{S}_\delta$ and $1 \le m \le \#\mathcal{B}_{S,\delta}$. Take $T \in \mathcal{S}_\delta$ minimal with respect to the partial ordering of domination. By Lemma 6.14,

$$w_\mathfrak{p}(\alpha) > \delta, \quad \forall \mathfrak{p} \in \mathcal{P}_T, \ \forall \alpha \in \mathcal{B}_{S,\delta}, \ \forall S \in \mathcal{S}_\delta, \ S \ne T.$$

Hence, $\mathrm{pr}_T(\zeta_{S,m}) = 0$ for all $S \in \mathcal{S}_\delta$, $S \ne T$, and all m. Thus, if we apply pr_T to both sides of (6.11), we get

$$\sum_m a_{T,m}\, \mathrm{pr}_T(\zeta_{T,m}) = 0.$$

By Lemma 6.16, $a_{T,m} = 0$, for all m. Hence, we get again an equation like (6.11) for S running on $\mathcal{S}_\delta \setminus \{T\}$. An iteration of this argument shows that $a_{S,m} = 0$ for all S, m. Thus, $\mathrm{red}_\delta(\mathcal{B}_{\mathrm{trm},\delta})$ is $(\mathbb{Z}/p\mathbb{Z})$-linearly independent. $\quad\square$

6.4. **Computation of global integral bases.** Let P be the product of all prime factors p of $\mathrm{disc}(f)$ with $\mathrm{ord}_p(\mathrm{disc}(f)) > 1$. It is well-known that a P-integral basis of K is necessarily a global integral basis of K.

Our algorithm finds a splitting $P = N_1 \cdots N_k$ for which we are able to compute N_i-integral bases $\mathcal{B}_{N_1}, \ldots, \mathcal{B}_{N_k}$ of K. This is sufficient for our purpose, because there are standard procedures to patch these bases into a P-integral basis. Along the algorithm we use the following subroutines:

CoprimeSplitting(d, N)
By an iterative application of gcd routines, a proper divisor d of N determines a factorization $N = c_1^{a_1} \cdots c_k^{a_k}$ with pairwise coprime bases $c_1, \ldots, c_k$. The routine expresses then each $c_i = d_i^{e_i}$ as a perfect power (with $e_i \geq 1$) and outputs the list $[d_1, \ldots, d_k]$.

SFD(N)
Computes the squarefree decomposition $N = d_1^{\ell_1} \cdots d_k^{\ell_k}$, $\ell_1 < \cdots < \ell_k$, and outputs the list of coprime squarefree factors $[d_1, \ldots, d_k]$.

GLOBAL BASIS ALGORITHM
INPUT:
  − A monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degre $n > 1$.

  − An integer D.

1 NBases $\leftarrow [\,]$

2 FOR each prime number $p \leq n$ such that $\mathrm{ord}_p(D) > 1$ DO
  Apply the classical OM algorithm to compute a p-integral basis $\mathcal{B}_p$
  Add the pair $[p, \mathcal{B}_p]$ to NBases
  $D \leftarrow D\, p^{-\mathrm{ord}_p(N)}$

3 Moduli $\leftarrow \{D\}$.
  WHILE #Moduli > 0 **DO**

4   Extract a modulus N from Moduli and call SF-OM(N, f)

5   IF a proper factor d of N is detected THEN join the output of
    CoprimeSplitting(d, N) to Moduli and go to step **4**

6   IF the output tree $\mathcal{T}(f)$ has some ramified leaf THEN
      SFD(N). Let $d_1, \ldots, d_k$ be the squarefree factors
      IF $k > 1$ THEN add $d_1, \ldots, d_k$ to Moduli and go to step **4**.

7   Compute the basis $\mathcal{B}_N$ of Theorem 6.10 and add $[N, \mathcal{B}_N]$ to NBases
  END WHILE

OUTPUT: A list of pairs $[N, \mathcal{B}_N]$, where $\mathcal{B}_N$ is a reduced N-integral basis of K.

Remarks

• The input integer D will be in general the discriminant of f. However, since the computation of this discriminant may be unfeasible, we admit the possibility of working with a partial factorization of it.

• The pairs $[N, \mathcal{B}_N]$ of `NBases` may be patched to obtain a D- integral basis of K. For instance, we can apply the triangulation algorithm given in [11] to all reduced N-integral bases, and then glue them together by means of the Chinese remainder theorem. When D is the discriminant of f or has the same prime factors, this leads to a global integral basis of K.

• The routine `SFD(N)` is the bottleneck of the algorithm. However, in some cases the method is efficient because the successive splittings of the discriminant, caused by the SF-OM routine in step **4**, lead to factors of N which are sufficiently small to admit a feasible performance of `SFD(N)`.

7. Examples

We illustrate the flow of the `Global Basis` algorithm with some examples, which prove its power and efficiency. There are two obvious gains with respect to other existing algorithms: the factorization of the discriminant is not necessary, and square-free decomposition of residual polynomials is used instead of the complete factorization. Thus, finding an SF-OM representation of a polynomial for a given integer N is cheaper than finding its OM representations for all the primes dividing N.

A single SF-type may encode many irreducible types. This compactness of SF-OM representations has a direct impact in the computation of integral bases, because it reduces drastically the amount of $\mathbb{Z}$-linear algebra needed to glue the local bases, which is a time and space expensive task.

The first example we present exhibits the capability of the `Global Basis` algorithm to detect some factors of the discriminant along the computation of an integral basis. We explain it to a certain detail for a better comprehension of the algorithm. The second example makes apparent the benefits of allowing non-irreducible residual polynomials. Finally, we introduce an example that illustrates the compactness of the SF-OM representations.

The three examples are parametrical, the parameters representing integer numbers. Most of the discussions are theoretical, but we include some particular cases which show a number of phenomena occurring along the flow of the algorithm. For these particular cases, we have used our own implementation of the algorithm in *Magma*.

Our experimentation suggests that our program is competitive to other routines for computation of integral bases, with the advantage that it can handle a broader range of number fields.

7.1. **Example 1.** Let us consider the polynomial
$$f = x^4 + 2Nx^2 + N^3(N-1)x + N^2,$$

with $N > 4$ an odd squarefree integer. Its discriminant is

$$\text{disc}(f) = -N^9(N-1)^2 \left(27N^5 - 54N^4 + 27N^3 - 256\right).$$

We first apply the SF-OM algorithm to the pair f, N. We assume that N is not divisible by 3 just for simplicity.

Since $\text{red}_N(f) = y^4$, we take $g_1 = x$, and obtain a Newton polygon $N_1(f)$ with a unique side of slope -1/2. The residual polynomial of this side is $R_1(f) = y^2 + 2y + 1 = (y+1)^2$. We lift the irreducible factor of $R_1(f)$ to $g_2 = x^2 + N$. The second order Newton polygon $N_2(f)$ has a unique side of slope $-3/2$ joining the points $(0,7)$ and $(2,4)$. The residual polynomial $R_2(f) = y + 1$ is squarefree. Hence, the SF-OM-representation of f with respect to N has a unique type:

$$\mathbf{t}_N = (y; (x, -1/2, y+1); (x^2 + N, -3/2, y+1)).$$

In particular, f is irreducible over $\mathbb{Q}_p$ for every prime $p \mid N$.

After theorem 6.10, we know that

$$\mathcal{B}_N = \left\{1, \theta, \frac{\theta^2}{N}, \frac{\theta^3 + N\theta}{N^2}\right\}$$

is an N-basis of the number field $K = \mathbb{Q}(\theta)$ defined by f.

Thus, no matter how many prime factors the integer N has, the SF-OM algorithm finds an N-basis in one hit. This is a significant improvement with respect to the classical OM algorithm, which has to work with every prime factor of N, and patch all local prime bases to find an N-basis.

Let us now see what happens when we apply the `Global Basis` algorithm to the pair f, $D := \text{disc}(f)$. In a realistic situation, we cannot take profit of the factorization of D given above.

We must work out the small primes 2 and 3 apart. Thus, we start by applying the SF-OM algorithm to the pair f, D_1 where $D_1 = |D|/2^{v_2(D)}3^{v_3(D)}$.

In the very beginning, the square-free factorization of f (mod D_1) requires the computation of the GCD of f and its derivative. Along this calculation, when we try to divide f' out by

$$f - \frac{1}{4}xf' = Nx^2 + \frac{3}{4}N^3(N-1)x + N^2,$$

we detect the factor N of D_1, and then its coprime cofactor $D_2 = D_1/N^9$.

We start the main loop again with `Moduli`=$\{N, D_2\}$. We discussed already how the algorithm computes an N-basis. We set `Moduli`=$\{D_2\}$ and apply the SF-OM algorithm to the pair f, D_2.

We compute the squarefree decomposition of f (mod D_2). Thanks to the coefficient $N^3(N-1)$ in f, the computation of $\gcd(f, f')$ detects the factors coming from $\gcd(N-1, D_2)$. We set `Moduli`=$\{N_1, D_3\}$, where N_1, D_3 are the output of `CoprimeSplitting`$(N-1, D_2)$.

For the modulus N_1 we have $f \equiv (x^2 + 1)^2 \pmod{N_1}$, and the SF-OM-representation of f with respect to N_1 has a unique type of order 1:

$$\mathbf{t}_{N_1} = (y^2 + 1; (x^2 + 1, -1/2, y + z_0)), \quad z_0 = y + (y^2 + 1)(\mathbb{Z}/N_1\mathbb{Z})[y].$$

The power basis $\{1, \theta, \theta^2, \theta^3\}$ is an N_1-integral basis.

We have seen so far that, for general N, we will find three divisors of $\mathrm{disc}(f)$, and for two of them the local bases have an specific form. For the remaining factor D_3, a bunch of phenomena can occur, including the chance to find new factors.

For instance, for $N = 10007 \cdot 10009$, we have $N_1 = 50080031 = (N-1)/2$ and $D_3 = 68041943397686978810459285162708530849445$. When we apply the SF-OM algorithm to the pair f, D_3 the obvious 5 dividing D_3 is detected in a valuation computation. For both factors 5 and $D_3/5$ the power basis is a local basis. The classical Montes algorithm shows that the power basis is a 6-integral basis. Hence, in this case, $\mathcal{B}_N$ is a global integral basis.

7.2. Example 2.
Let p be a prime number and take positive integers r, m such that $r < p/2$ and $r < m$. Consider the polynomial

$$f_{p,r,m} = (x^2 + p)(x^2 + 2p) \cdots (x^2 + rp) + p^m = x^{2r} + b_2 x^{2r-2} + \cdots + b_{2r}.$$

We assume that $f := f_{p,r,m}$ is irreducible. The SF-OM-algorithm applied to f and p yields a unique type of order 1:

$$\mathbf{t}_N = (y; (x, -1/2, (y+1)(y+2) \cdots (y+r))),$$

and the following p-basis of the number $K = \mathbb{Q}(\theta)$ field determined by f:

$$\mathcal{B}_p = \left\{ 1, \theta, \frac{\theta^2 + b_2}{p}, \frac{\theta(\theta^2 + b_2)}{p}, \dots, \right.$$

$$\left. \frac{\theta^{2r-2} + b_2\theta^{2r-4} + \cdots + b_{2r-2}}{p^{r-1}}, \frac{\theta(\theta^{2r-2} + b_2\theta^{2r-4} + \cdots + b_{2r-2})}{p^{r-1}} \right\}.$$

We see once more the gain of the SF-OM-algorithm with respect to the classical Montes algorithm, which in this case finds r different types.

Eventually, we might find new factors of the discriminant in the triangulation process of the local bases. For instance, consider the case $f = f_{101,7,11}$. The discriminant $\mathrm{disc}(f)$ has 362 decimal figures. The initial square-free factorizations detect the factors $p = 101$, and $D = \mathrm{disc}(f)/(2^{14}101^{91})$. The `Global Basis` routine finds $D_1 = 104065441$,

$$D_2 = 1045681081654964908367435426796223594285104202271660887,$$

and no further splittings.

However, along the triangulation process of the reduced local D_2-basis introduced in [11], certain valuation computations detect the factors 17 and 37. After all these splittings, in order to compute a global integral basis for f, we need to compute local bases for the moduli:

$$2, 17, 37, 101, 104065441,$$
$$1662450050325858359884635018753932582329259463071003.$$

Checking the squarefreeness of these moduli is almost immediate. Observe that the last two moduli are not prime, but we have no need to factor them in order to compute a global integral basis.

7.3. **Example 3.** For an odd positive integer r, let

$$(x - 1)(x - 2) \cdots (x - r) = x^r + a_{r-1}x^{r-1} + \cdots + a_0.$$

Take a squarefree integer $N > \text{Max}\{|a_0|, \ldots, |a_r|\}$. Consider the polynomials:

$$\phi = x^4 + N^2(N - 1),$$
$$f = \phi^{3r} + a_{r-1}N^6x^2\phi^{3(r-1)} + a_{r-2}N^{14}\phi^{3(r-2)} + a_{r-3}N^{20}x^2\phi^{3(r-3)} + \cdots$$
$$\cdots + a_1N^{7(r-1)}\phi^3 + a_0N^{7r-1}x^2.$$

The SF-OM algorithm applied to the pair f, N generates a unique type of order 2:

$$\mathbf{t}_N = (y; (x, -1/2, (y + 1)(y - 1)); (\phi, -2/3, (y - 1) \cdots (y - r)).$$

If s is the number of primes dividing N, the type $\mathbf{t}_N$ has $2rs$ irreducible types attached. We see again that the use of the SF-OM algorithm can be much faster than the classical Montes algorithm, and that it saves a lot of memory space.

References

[1] J. A. Buchmann, H. W. Lenstra, Jr, *Approximating rings of integers in number fields*, Journal de Théorie des Nombres de Bordeaux **6** (1994), 221–260.

[2] A. L. Chistov, *Polynomial-time factoring polynomials over local fields*, J. Math. Sci., **70:4** (1994), 1912-1933.

[3] A. L. Chistov, *Efficient factoring polynomials over local fields and its applications*, *Proceedings of ICM 1990.* pp. 1509-1519. Berlin, Springer-V.

[4] 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.

[5] J. Guàrdia, J. Montes, E. Nart, A new computational approach to ideal theory in number fields, Found. Comput. Math. **13** (2013), no. 5, 729–762.

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

[7] J. Guàrdia, E. Nart, *Genetics of polynomials over local fields*, Proceedings of AGCT14, Contemporary Mathematics **637** (2015), 207–241.

[8] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40** (1936), pp. 363–395.

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

[10] J. Montes, Polígonos de Newton de orden superior y aplicaciones aritméticas, Tesi Doctoral, Universitat de Barcelona 1999.

[11] N. Moraes d'Oliveira, E. Nart *R*educed normal form of local integral bases, Acta Arithmetica **178** (2017), pp. 181–200.

[12] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84–117.

[13] S. Sarussi, *Quasi-valuations extending a valuation*, Journal of Algebra **372** (2012), 318–364.

[14] V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, 2009.

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT POLITCNICA DE CATALUNYA, ESCOLA POLITÈCNICA SUPERIOR D'ENGINYERIA DE VILANOVA I LA GELTRÚ, AV. VÍCTOR BALAGUER S/N. E-08800 VILANOVA I LA GELTRÚ, CATALONIA, SPAIN
  Email address: jordi.guardia-rubies@upc.edu

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT AUTÒNOMA DE BARCELONA, EDIFICI C, E-08193 BELLATERRA, BARCELONA, CATALONIA, SPAIN
  Email address: nart@mat.uab.cat