TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 364, Number 1, January 2012, Pages 361–416
S 0002-9947(2011)05442-5
Article electronically published on May 18, 2011

NEWTON POLYGONS OF HIGHER ORDER IN ALGEBRAIC NUMBER THEORY

JORDI GUÀRDIA, JESÚS MONTES, AND ENRIC NART

Abstract. We develop a theory of arithmetic Newton polygons of higher order that provides the factorization of a separable polynomial over a p-adic field, together with relevant arithmetic information about the fields generated by the irreducible factors. This carries out a program suggested by Ø. Ore. As an application, we obtain fast algorithms to compute discriminants, prime ideal decomposition and integral bases of number fields.

Introduction

R. Dedekind based the foundations of algebraic number theory on ideal theory because the constructive attempts to find a rigorous general definition of the *ideal numbers* introduced by E. Kummer failed. This failure is due to the existence of inessential discriminant divisors; that is, there are number fields K and prime numbers p, such that p divides the index $\mathrm{i}(\theta) := (\mathbb{Z}_K : \mathbb{Z}[\theta])$, for any integral generator θ of K, where $\mathbb{Z}_K$ is the ring of integers. Dedekind gave a criterion to detect when $p \nmid \mathrm{i}(\theta)$, and a procedure to construct the prime ideals of K dividing p in that case, in terms of the factorization of the minimal polynomial of θ modulo p [Ded78].

M. Bauer introduced an arithmetic version of Newton polygons to construct prime ideals in cases where Dedekind's criterion failed [Bau07]. This theory was developed and extended by Ø. Ore in his 1923 thesis and a series of papers that followed [Ore23, Ore24, Ore25, Ore26, Ore28]. Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial that generates K. After K. Hensel's work, the prime ideals of K lying above p are in bijection with the irreducible factors of $f(x)$ over $\mathbb{Z}_p[x]$. Ore's work determines three successive factorizations of $f(x)$ in $\mathbb{Z}_p[x]$, called *dissections* of the set of prime ideals dividing p. The first dissection is determined by Hensel's lemma: $f(x)$ splits into the product of factors that are congruent to the power of an irreducible polynomial modulo p. The second dissection is a further splitting of

Received by the editors October 31, 2008 and, in revised form, June 15, 2010.
2010 *Mathematics Subject Classification.* Primary 11S15; Secondary 11R04, 11R29, 11Y40.
Key words and phrases. Newton polygon, local field, p-adic factorization, number field, prime ideal decomposition, discriminant, integral basis.
This work was partially supported by MTM2009-13060-C02-02 and MTM2009-10359 from the Spanish MEC.

each factor, according to the number of sides of a certain Newton polygon. The third dissection is a further splitting of each of the latter factors, according to the factorization of a certain *residual polynomial* with coefficients in a finite field, attached to each side of the polygon.

Unfortunately, the factors of $f(x)$ obtained after these three dissections are not always irreducible. Ore defined a polynomial to be *p-regular* when it satisfies a technical condition that ensures that the factorization of $f(x)$ is complete after the three dissections. Also, he proved the existence of a p-regular defining equation for every number field, but the proof is not constructive: it uses the Chinese remainder theorem with respect to the different prime ideals that one wants to construct. Ore himself suggested that it should be possible to introduce Newton polygons of higher order that continue the factorization process till all irreducible factors of $f(x)$ are achieved [Ore23, Ch.4, §8], [Ore28, §5].

Ore's program was carried out by the second author in his 1999 thesis [Mon99], under the supervision of the third author. For any natural number $r \geq 1$, Newton polygons of order r were constructed, the case $r = 1$ corresponding to the Newton polygons introduced by Ore. Also, results analogous to Ore's theorems were proved for polygons of order r, providing two more dissections of the factors of $f(x)$, for each order r. The whole process is controlled by an invariant defined in terms of *higher order indices*, which ensures that the process ends after a finite number of steps. Once an irreducible factor of $f(x)$ is detected, the theory determines the ramification index and residual degree of the p-adic field generated by this factor, and a generator of the maximal ideal. These invariants are expressed in terms of combinatorial data attached to the sides of the higher order polygons and the residual polynomials of higher order attached to each side. The process yields as a by-product a computation of $\mathrm{ind}(f) := v_p(\mathrm{i}(\theta))$, where θ is a root of $f(x)$. An implementation in Mathematica of this factorization algorithm was worked out by the first author [Gua97].

We now present these results after a thorough revision and some simplifications. In section 1 we review Ore's results, with proofs, which otherwise can be found only in the original papers by Ore in the language of "höheren Kongruenzen". In section 2 we develop the theory of Newton polygons of higher order, based on the concept of a *type* and its *representative*, which plays the analogous role in order r to that played by an irreducible polynomial modulo p in order one. In section 3 we prove results in order r analogous to Ore's theorems of the polygon and of the residual polynomial (Theorems 3.1 and 3.7), which provide two more dissections for each order. In section 4 we introduce resultants and indices of higher order and we prove the theorem of the index (Theorem 4.18), which relates $\mathrm{ind}(f)$ with the higher order indices constructed from the higher order polygons. This result guarantees that the factorization process finishes at most in $\mathrm{ind}(f)$ steps.

Although the higher order Newton polygons are apparently involved and highly technical objects, they provide fast factorization algorithms because all computations are mainly based on two reasonably fast operations: division with remainder of monic polynomials with *integer* coefficients, and factorization of polynomials over *finite* fields. Thus, from a modern perspective, the main application of these results is the design of fast algorithms to compute discriminants, prime ideal decomposition and integral bases of number fields. However, we present in this paper only the theoretical background of higher order Newton polygons. We shall describe the

concrete design of the algorithms and discuss the relevant computational aspects elsewhere [GMN08, GMN09].

Contents

1. Newton polygons of the first order

1.1. **Principal polygons.** Let $\lambda \in \mathbb{Q}^-$ be a negative rational number, expressed in lower terms as $\lambda = -h/e$, with h, e positive coprime integers. We denote by $\mathcal{S}(\lambda)$ the set of segments of the Euclidean plane with slope λ and end points having nonnegative integer coordinates. The points of $(\mathbb{Z}_{\geq 0})^2$ are also considered to be segments in $\mathcal{S}(\lambda)$, whose initial and final points coincide. The elements of $\mathcal{S}(\lambda)$ will be called *sides of slope* λ. For any side $S \in \mathcal{S}(\lambda)$, we define its *length*, $\ell := \ell(S)$, and *height*, $H := H(S)$, to be the length of the respective projections of S to the horizontal and vertical axes. We define the *degree* of S to be

$$d := d(S) := \ell(S)/e = H(S)/h.$$

Any side S is divided into d segments by the points with integer coordinates that lie on S. A side $S \in \mathcal{S}(\lambda)$ is determined by the initial point (s, u) and the degree d. The final point is $(s+\ell, u-H) = (s+de, u-dh)$. For instance, Figure 1 represents a side of slope $-1/2$, initial point (s, u), and degree three.

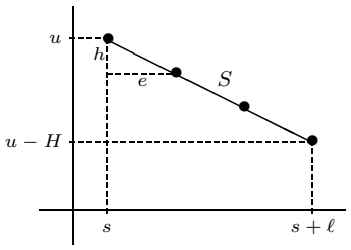


FIGURE 1

The set $\mathcal{S}(\lambda)$ has the structure of an abelian semigroup with the following addition rule: given $S, T \in \mathcal{S}(\lambda)$, the sum $S + T$ is the side of degree $d(S) + d(T)$ of $\mathcal{S}(\lambda)$, whose initial point is the sum of the initial points of S and T. Thus, the addition is geometrically represented by the process of joining the two segments and choosing an appropriate initial point. The addition of a segment S with a point P coincides with the translation $P + S$ of S by the vector determined by P. The neutral element is the point $(0, 0)$. The invariants $\ell(S)$, $H(S)$, $d(S)$ determine semigroup homomorphisms

$$\ell,\, H,\, d : \mathcal{S}(\lambda) \longrightarrow \mathbb{Z}_{\geq 0}.$$

The *set of sides of negative slope* is defined as $\mathcal{S} := \bigcup_{\lambda \in \mathbb{Q}^-} \mathcal{S}(\lambda)$. Since the points of $(\mathbb{Z}_{\geq 0})^2$ belong to $\mathcal{S}(\lambda)$ for all λ, it is not possible (even in a formal sense) to attach a slope to them.

There is a natural geometric representation of a formal sum of sides, as an open convex polygon of the plane. Given a formal sum $S_1 + \cdots + S_t$, of sides of negative slope, we consider the sum P_0 of all initial points of the S_i, and we construct the polygon $N := N(S_1 + \cdots + S_t)$ that starts at P_0 and is obtained by joining all sides of positive length, ordered by increasing slopes. The *length* of N is by definition the largest abscissa $\ell(N)$ of the points of N; the abscissa of P_0 is denoted by $\ell_\infty(N)$. The typical shape of this polygon is shown in Figure 2.

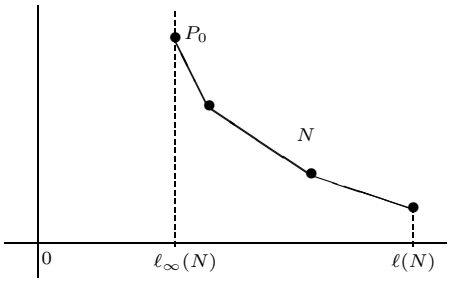


FIGURE 2

Definition 1.1. The semigroup $\mathcal{PP}$ of principal polygons is defined to be the set of all open convex polygons of the plane, attached to finite formal sums of sides of negative slope. The length determines a semigroup homomorphism, $\ell\colon \mathcal{PP} \longrightarrow \mathbb{Z}_{\geq 0}$.

The addition of principal polygons is the operation induced by the formal sum of sides. If $N = N(S_1 + \cdots + S_t)$ and $N' = N(S'_1 + \cdots + S'_s)$, then $N + N'$ is the geometric representation of $S_1 + \cdots + S_t + S'_1 + \cdots + S'_s$. The reader may easily check that this is well-defined and that $\mathcal{PP}$ has a structure of a semigroup with neutral element $\{(0,0)\}$. Clearly, this addition is compatible with the sum operations that we had on all $\mathcal{S}(\lambda)$. The addition of $N \in \mathcal{PP}$ with (the polygon represented by) a point $P \in (\mathbb{Z}_{\geq 0})^2$ is the translation $P + N$.

Note that $N(S) = S$, for all $S \in \mathcal{S}$, but $\ell(N(S)) = \ell_\infty(N(S)) + \ell(S)$. It is quite natural to express a principal polygon directly as a sum of sides: $N = S_1 + \cdots + S_t$. This decomposition is unique in either of the two following situations:

(1) $N = S$, with $S \in (\mathbb{Z}_{\geq 0})^2$,
(2) $N = S_1 + \cdots + S_t$, with all S_i of positive length and slopes $\lambda_1 < \cdots < \lambda_t$.

Any $N \in \mathcal{PP}$ can be expressed in one (and only one) of these canonical forms. The end points of these canonical sides are called the *vertices* of the polygon.

For technical reasons, in the canonical representation of a principal polygon as a sum of sides we (eventually) include a *side of slope* $-\infty$. Informally, it is the side with initial point $(0, \infty)$ and final point P_0, the starting point of the "finite part" of the polygon (cf. Figure 2). In a more formal setting, we define the set of sides of slope $-\infty$ as $\mathcal{S}(-\infty) := \mathbb{Z}_{>0}$, with its natural structure of an abelian monoid. If $S \in \mathcal{S}(-\infty)$ corresponds to the positive integer ℓ, we define $\ell(S) := \ell$, $H(S) := \infty$.

Definition 1.2. If $N \in \mathcal{PP}$ has $\ell_\infty(N) > 0$, then we consider the side of slope $-\infty$ determined by the positive integer $\ell_\infty(N)$ as the "infinite part" of N.

From now on, when we write $N = S_1 + \cdots + S_t$, we implicitly assume that this is the canonical decomposition of the whole of N, the infinite and finite parts, as a sum of sides. Therefore, either $S_1 \in \mathcal{S}$ has a left end point with abscissa zero (and $\ell_\infty(N) = 0$), or $S_1 \in \mathcal{S}(-\infty)$ has length $\ell_\infty(N) > 0$.

We say that N is *one-sided* if either $N = S_1$, with $S_1 \in \mathcal{S}$, $\ell(S_1) > 0$, or $N = S_1 + S_2$, with $S_1 \in \mathcal{S}(-\infty)$, $\ell(S_2) = 0$.

This definition has some advantages. For instance, the projection of a (whole) principal polygon N to the horizontal axis is always the interval $[0, \ell(N)]$. Also, the length of $N = S_1 + \cdots + S_t$ is equal to $\ell(N) = \ell(S_1) + \cdots + \ell(S_t)$.

Clearly, the splitting of $N \in \mathcal{PP}$ into a finite part and an infinite part behaves well with respect to the addition in $\mathcal{PP}$: the sum of the finite (resp. infinite) parts of N and N' are the finite (resp. infinite) parts of $N + N'$.

Let $N \in \mathcal{PP}$. For any integer abscissa, $0 \leq i \leq \ell(N)$, we denote

$$y_i = y_i(N) := \begin{cases} \infty, & \text{if } i < \ell_\infty(N), \\ \text{the ordinate of the point of } N \text{ of abscissa } i, & \text{if } i \geq \ell_\infty(N). \end{cases}$$

For $i \geq \ell_\infty(N)$ these rational numbers form a strictly decreasing sequence.

Definition 1.3. Let $P = (i, y)$ be a "point" of the plane, with integer abscissa $0 \leq i \leq \ell(N)$, and ordinate $y \in \mathbb{R} \cup \{\infty\}$. We say that P *lies on* N if $y = y_i$. We say that P *lies on or above* N if $y \geq y_i$. We say that P *lies above* N if $y > y_i$.

Let $i_0 = \ell_\infty(N)$, and for any $i_0 < i \leq \ell(N)$, let μ_i be the slope of the segment joining $(i-1, y_{i-1})$ and (i, y_i). The sequence $\mu_{i_0+1} \leq \cdots \leq \mu_{\ell(N)}$ is an increasing sequence of negative rational numbers. We call these elements the *unit slopes* of

N. Consider the multisets of unit slopes:

$$U_{i_0}(N) := \emptyset; \quad U_i(N) := \{\mu_{i_0+1}, \dots, \mu_i\}, \quad i_0 < i \le \ell(N).$$

Clearly, $y_i(N) = y_{i_0}(N) + \sum_{\mu \in U_i(N)} \mu$.

Let N' be another principal polygon; denote $j_0 = \ell_\infty(N')$ and consider analogous multisets $U_j(N')$, for all $j_0 \le j \le \ell(N')$. By the definition of the addition law of principal polygons, the multiset $U_k(N+N')$ contains the smallest $k - i_0 - j_0$ unit slopes of the multiset $U_{\ell(N)}(N) \cup U_{\ell(N')}(N')$. Thus,

$$y_i(N) + y_j(N') \ge y_{i+j}(N+N'),$$

and equality holds if and only if $U_i(N) \cup U_j(N') = U_{i+j}(N+N')$.

Lemma 1.4. *Let $N, N' \in \mathcal{PP}$. Let $P = (i,u)$ be a point lying on or above the finite part of N and $P' = (j,u')$ a point lying on or above the finite part of N'. Then $P + P'$ lies on or above the finite part of $N + N'$, and*

$$P + P' \in N + N' \iff P \in N,\ P' \in N',\ \text{and } U_i(N) \cup U_j(N') = U_{i+j}(N+N').$$

Proof. Clearly, $u + u' \ge y_i(N) + y_j(N') \ge y_{i+j}(N+N')$, and $P + P' \in N + N'$ if and only if both inequalities are equalities. □

Definition 1.5. Let $\lambda \in \mathbb{Q}^-$ and $N \in \mathcal{PP}$. We define the *λ-component* of N to be $S_\lambda(N) := \{(x,y) \in N \mid y - \lambda x \text{ is minimal}\}$. In this way we obtain a map:

$$S_\lambda \colon \mathcal{PP} \longrightarrow \mathcal{S}(\lambda).$$

If N has a canonical side S of positive length and slope λ, then $S_\lambda(N) = S$. Otherwise, the λ-component $S_\lambda(N)$ is a single point. Figure 3 illustrates both possibilities; in this figure, L_λ is the line of slope λ having first contact with N from below.

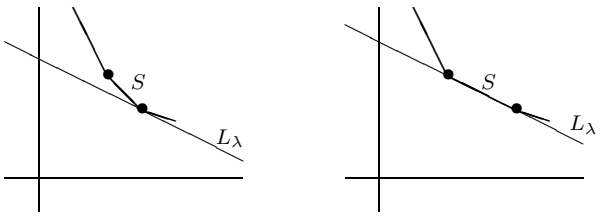


FIGURE 3

Lemma 1.4 shows that S_λ is a semigroup homomorphism:

$$S_\lambda(N+N') = S_\lambda(N) + S_\lambda(N'), \tag{1}$$

for all N, $N' \in \mathcal{PP}$ and all $\lambda \in \mathbb{Q}^-$.

1.2. **ϕ-Newton polygon of a polynomial.** Let p be a prime number and let $\overline{\mathbb{Q}}_p$ be a fixed algebraic closure of the field $\mathbb{Q}_p$ of the p-adic numbers. For any finite subextension, $\mathbb{Q}_p \subseteq L \subseteq \overline{\mathbb{Q}}_p$, we denote by $v_L \colon \overline{\mathbb{Q}}_p \longrightarrow \mathbb{Q} \cup \{\infty\}$ the p-adic valuation normalized by $v_L(L^*) = \mathbb{Z}$. Throughout the paper $\mathcal{O}_L$ will denote the ring of integers of L, $\mathfrak{m}_L$ its maximal ideal, and $\mathbb{F}_L$ the residue field. We usually indicate simply by a bar the canonical reduction map, $\mathrm{red}_L \colon \mathcal{O}_L \longrightarrow \mathbb{F}_L$, and its natural extension to polynomials: $\overline{\alpha} := \mathrm{red}_L(\alpha)$, $\overline{f}(x) := \mathrm{red}_L(f(x))$.

We fix a finite extension K of $\mathbb{Q}_p$ as a base field, and we denote $v := v_K$, $\mathcal{O} := \mathcal{O}_K$, $\mathfrak{m} := \mathfrak{m}_K$, $\mathbb{F} := \mathbb{F}_K$. We also fix a prime element $\pi \in \mathcal{O}$.

We extend the valuation v to $\mathcal{O}[x]$ in a natural way:

$$v\colon \mathcal{O}[x] \longrightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}, \quad v(b_0 + \cdots + b_r x^r) := \min\{v(b_j),\, 0 \leq j \leq r\}.$$

Let $\phi(x) \in \mathcal{O}[x]$ be a monic polynomial of degree m whose reduction modulo $\mathfrak{m}$ is irreducible. We denote by $\mathbb{F}_\phi$ the finite field $\mathcal{O}[x]/(\pi, \phi(x))$, and by

$$\mathrm{red}_\phi\colon \mathcal{O}[x] \longrightarrow \mathbb{F}_\phi$$

the canonical homomorphism.

Any $f(x) \in \mathcal{O}[x]$ admits a unique ϕ-adic development:

$$f(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^n,$$

with $a_i(x) \in \mathcal{O}[x]$, $\deg a_i(x) < m$. For any coefficient $a_i(x)$ we denote $u_i := v(a_i(x)) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

Definition 1.6. The ϕ-Newton polygon of a nonzero polynomial $f(x) \in \mathcal{O}[x]$ is the lower convex envelope of the set of points $P_i = (i, u_i)$, $u_i < \infty$, in the Euclidean plane. We denote this polygon by $N_\phi(f)$.

The length of this polygon is by definition the abscissa of the last vertex. We denote it by $\ell(N_\phi(f)) := n = \lfloor \deg(f)/m \rfloor$. Note that $\deg f(x) = mn + \deg a_n(x)$. The typical shape of this polygon is as shown in Figure 4.

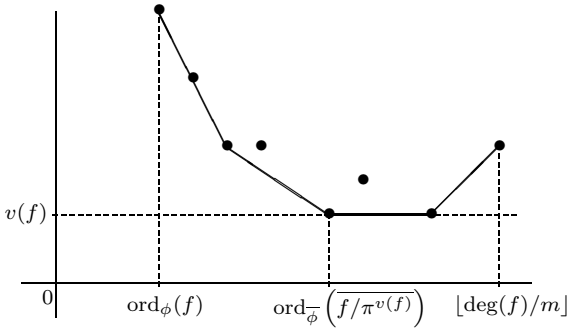


FIGURE 4

Remark 1.7. The ϕ-Newton polygon of $f(x)$ consists of a single point if and only if $f(x) = a(x)\phi(x)^n$, with $\deg(a) < m$.

Definition 1.8. The principal ϕ-polygon of $f(x)$ is the element $N_\phi^-(f) \in \mathcal{PP}$ determined by the sides of negative slope of $N_\phi(f)$, including the side of slope $-\infty$ represented by the length $\mathrm{ord}_\phi(f)$. It has length $\ell(N_\phi^-(f)) = \mathrm{ord}_{\overline{\phi}}\left(\overline{f/\pi^{v(f)}}\right)$.

For any $\lambda \in \mathbb{Q}^-$ we shall denote by $S_\lambda(f) := S_\lambda(N_\phi^-(f))$ the λ-component of this polygon (cf. Definition 1.5).

Let us denote $N = N_\phi^-(f)$ for simplicity. By construction, the points P_i all lie on or above N. The points that lie on N contain the arithmetic information we are

interested in. We attach to any abscissa $\operatorname{ord}_\phi(f) \le i \le \ell(N)$ the following *residual coefficient* $c_i \in \mathbb{F}_\phi$:

$$c_i = \begin{cases} 0, & \text{if } (i,u_i) \text{ lies above } N,\\ \operatorname{red}_\phi\left(a_i(x)/\pi^{u_i}\right), & \text{if } (i,u_i) \text{ lies on } N.\end{cases}$$

Note that c_i is always nonzero in the latter case because $\deg a_i(x) < m$.

Let $\lambda = -h/e$ be a negative rational number, with h, e positive coprime integers. Let $S = S_\lambda(f)$ be the λ-component of N, (s,u) the initial point of S, and $d = d(S)$ the degree of S. The arithmetic information determined by the family of points (i,u_i) that lie on S is synthesized by two polynomials that are built with the coefficients of the ϕ-development of $f(x)$ to which these points are attached.

Definition 1.9. We define the *virtual factor* of $f(x)$ attached to λ (or to S) to be the polynomial

$$f^S(x) := \pi^{-u}\phi(x)^{-s}f^0(x) \in K[x], \quad \text{where} \quad f^0(x) := \sum_{(i,u_i)\in S} a_i(x)\phi(x)^i.$$

We define the *residual polynomial* attached to λ (or to S) to be the polynomial

$$R_\lambda(f)(y) := c_s + c_{s+e}\,y + \cdots + c_{s+(d-1)e}\,y^{d-1} + c_{s+de}\,y^d \in \mathbb{F}_\phi[y].$$

Note that only the points (i,u_i) that lie on S yield a nonzero coefficient of $R_\lambda(f)(y)$. In particular, c_s and c_{s+de} are always nonzero, so that $R_\lambda(f)(y)$ has degree d and it is never divisible by y.

If $\pi' = \rho\pi$ is another prime element of $\mathcal{O}$ and $c = \bar\rho \in \mathbb{F}^*$, the residual coefficients of $N_\phi^-(f)$ with respect to π' satisfy $c_i' = c_i c^{-u_i}$, so that the corresponding residual polynomial $R'_\lambda(f)(y)$ is equal to $c^{-u}R_\lambda(f)(c^h y)$.

We can define in a completely analogous way the residual polynomial of $f(x)$ with respect to a side T, which is not necessarily a λ-component of $N_\phi^-(f)$.

Definition 1.10. Let $T \in \mathcal{S}(\lambda)$ be an arbitrary side of slope λ, with abscissas $s_0 \le s_1$ for the end points, and let $d' = d(T)$. We say that the polynomial $f(x)$ *lies on or above* T if all points of $N_\phi^-(f)$ with integer abscissa $s_0 \le i \le s_1$ lie on or above T; in this case we define

$$R_\lambda(f,T)(y) := \tilde c_{s_0} + \tilde c_{s_0+e}\,y + \cdots + \tilde c_{s_0+(d'-1)e}\,y^{d'-1} + \tilde c_{s_0+d'e}\,y^{d'} \in \mathbb{F}_\phi[y],$$

where $\tilde c_i = c_i$ if (i,u_i) lies on T and $\tilde c_i = 0$ otherwise.

Thus, if all points of $S_\lambda(f)$ lie above T we have $R_\lambda(f,T)(y) = 0$. Note that $\deg R_\lambda(f,T)(y) \le d'$ and equality holds if and only if the final point of T belongs to $S_\lambda(f)$. Usually, T will be an enlargement of $S_\lambda(f)$ and then

$$T \supseteq S_\lambda(f) \implies R_\lambda(f,T)(y) = y^{(s-s_0)/e}R_\lambda(f)(y), \tag{2}$$

where s is the abscissa of the initial point of $S_\lambda(f)$. See Figure 5.

The motivation for this more general definition lies in the bad behaviour of the residual polynomial $R_\lambda(f)(y)$ with respect to sums. Nevertheless, if T is a fixed side and $f(x)$, $g(x)$ lie both on or above T, it is clear that $f(x)+g(x)$ lies on or above T and

$$R_\lambda(f+g,T)(y) = R_\lambda(f,T)(y) + R_\lambda(g,T)(y). \tag{3}$$

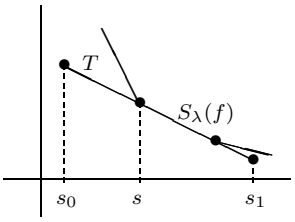


FIGURE 5

1.3. **Admissible ϕ-developments and theorem of the product.** Let

$$f(x) = \sum_{i\geq 0} a'_i(x)\phi(x)^i, \quad a'_i(x) \in \mathcal{O}[x], \tag{4}$$

be a ϕ-development of $f(x)$, not necessarily the ϕ-adic one. Take $u'_i = v(a'_i(x))$, for all $i \geq 0$, and let N' be the principal polygon of the set of points (i, u'_i). Let i_0 be the first abscissa with $a'_{i_0}(x) \neq 0$. To any $i_0 \leq i \leq \ell(N')$ we attach a residual coefficient as before:

$$c'_i = \begin{cases} 0, & \text{if } (i,u'_i) \text{ lies above } N', \\ \operatorname{red}_\phi\left(a'_i(x)/\pi^{u'_i}\right), & \text{if } (i,u'_i) \text{ lies on } N'. \end{cases}$$

For the points (i, u'_i) lying on N' we can now have $c'_i = 0$; for instance, in the case $a'_0(x) = f(x)$, the Newton polygon has only one point $(0, v(f))$ and $c'_0 = 0$ if $f(x)/\pi^{v(f)}$ is divisible by $\phi(x)$ modulo $\mathfrak{m}$.

Finally, for any negative rational number $\lambda = -h/e$ as above, we can define the *residual polynomial* attached to the λ-component $S' = S_\lambda(N')$ to be

$$R'_\lambda(f)(y) := c'_{s'} + c'_{s'+e}\, y + \cdots + c'_{s'+(d'-1)e}\, y^{d'-1} + c'_{s'+d'e}\, y^{d'} \in \mathbb{F}_\phi[y],$$

where $d' = d(S')$ and s' is the abscissa of the initial point of S'.

Definition 1.11. We say that the ϕ-development (4) is *admissible* if $c'_i \neq 0$ for each abscissa i of a vertex of N'.

Lemma 1.12. *If a ϕ-development is admissible, then $N' = N^-_\phi(f)$ and $c'_i = c_i$ for all abscissas i of the finite part of N'. In particular, for any negative rational number λ we have $R'_\lambda(f)(y) = R_\lambda(f)(y)$.*

Proof. Consider the ϕ-adic developments of $f(x)$ and each $a'_i(x)$:

$$f(x) = \sum_{0\leq i} a_i(x)\phi(x)^i, \qquad a'_i(x) = \sum_{0\leq k} b_{i,k}(x)\phi(x)^k.$$

By the uniqueness of the ϕ-adic development we have

$$a_i(x) = \sum_{0\leq k\leq i} b_{i-k,k}(x). \tag{5}$$

Clearly, $w_{i,k} := v(b_{i,k}) \geq u'_i$, for all $0 \leq k$, $0 \leq i \leq \ell(N')$. In particular, all points (i, u_i) lie on or above N'; in fact, for some $0 \leq k_0 \leq i$, we have

$$u_i = v(a_i) \geq \min_{0\leq k\leq i}\{w_{i-k,k}\} = w_{i-k_0,k_0} \geq u'_{i-k_0} \geq y_{i-k_0}(N') \geq y_i(N'). \tag{6}$$

From now on, i will be an integer abscissa of the finite part of N'. Clearly,

$$w_{i-k,k} \geq u'_{i-k} \geq y_{i-k}(N') > y_i(N'), \tag{7}$$

for any $0 < k \leq i$. Also, for the abscissas i with $u'_i = y_i(N')$ we have

$$c'_i = \mathrm{red}_\phi(a'_i(x)/\pi^{u'_i}) = \mathrm{red}_\phi(b_{i,0}(x)/\pi^{u'_i}). \tag{8}$$

Now, if (i, u'_i) is a vertex of N' we have $c'_i \neq 0$ by hypothesis, and from (8) we get $y_i(N') = u'_i = w_{i,0}$. By (7) and (5) we have $u_i = w_{i,0} = u'_i$. This shows that $N' = N^-_\phi(f)$. Let us denote this common polygon by N.

Finally, let us prove the equality of all residual coefficients. If $c_i \neq 0$, then $u_i = y_i(N)$, and from (6) we get $k_0 = 0$ and $u_i = w_{i,0} = u'_i$. By (7), (5) and (8), we get $c_i = \mathrm{red}_\phi(a_i(x)/\pi^{u_i}) = \mathrm{red}_\phi(b_{i,0}(x)/\pi^{u_i}) = c'_i$. If $c_i = 0$, then $u_i > y_i(N)$, and from (5) and (7) we get $w_{i,0} > y_i(N)$ too. By (8) we get $c'_i = 0$. □

The construction of the principal part of the ϕ-Newton polygon of a polynomial can be interpreted as a mapping

$$N^-_\phi \colon \mathcal{O}[x] \setminus \{0\} \longrightarrow \mathcal{PP}, \qquad f(x) \mapsto N^-_\phi(f).$$

Also, for any negative rational number λ, the construction of the residual polynomial attached to λ determines a mapping

$$R_\lambda \colon \mathcal{O}[x] \setminus \{0\} \longrightarrow \mathbb{F}_\phi[y], \qquad f(x) \mapsto R_\lambda(f)(y).$$

The theorem of the product says that both mappings are semigroup homomorphisms.

Theorem 1.13 (Theorem of the product)**.** *For any $f(x), g(x) \in \mathcal{O}[x] \setminus \{0\}$ and any $\lambda \in \mathbb{Q}^-$ we have*

$$N^-_\phi(fg) = N^-_\phi(f) + N^-_\phi(g), \qquad R_\lambda(fg)(y) = R_\lambda(f)(y)R_\lambda(g)(y).$$

Proof. Consider the respective ϕ-adic developments

$$f(x) = \sum_{0 \leq i} a_i(x)\phi(x)^i, \quad g(x) = \sum_{0 \leq j} b_j(x)\phi(x)^j,$$

and denote $u_i = v(a_i(x))$, $v_j = v(b_j(x))$, $N_f = N^-_\phi(f)$, $N_g = N^-_\phi(g)$. Then,

$$f(x)g(x) = \sum_{0 \leq k} A_k(x)\phi(x)^k, \qquad A_k(x) = \sum_{i+j=k} a_i(x)b_j(x). \tag{9}$$

Denote by N' the principal part of the Newton polygon of fg, determined by this ϕ-development. We shall show that $N' = N_f + N_g$, that this ϕ-development is admissible, and that $R'_\lambda(fg) = R_\lambda(f)R_\lambda(g)$ for all λ. The theorem will then be a consequence of Lemma 1.12.

Let $w_k := v(A_k(x))$ for all $0 \leq k$. Lemma 1.4 shows that the point $(i, u_i) + (j, v_j)$ lies on or above $N_f + N_g$ for any $i, j \geq 0$. Since $w_k \geq \min\{u_i + v_j \mid i + j = k\}$, the points (k, w_k) all lie on or above $N_f + N_g$. On the other hand, let $P_k = (k, y_k)$ be a vertex of $N_f + N_g$; that is, P_k is the end point of $S_1 + \cdots + S_r + T_1 + \cdots + T_s$, for certain sides S_i of N_f and T_j of N_g, ordered by increasing slopes among all sides of N_f and N_g. By Lemma 1.4, for all pairs (i, j) such that $i + j = k$, the point $(i, u_i) + (j, v_j)$ lies above $N_f + N_g$ except for the pair $i_0 = \ell(S_1 + \cdots + S_r)$, $j_0 = \ell(T_1 + \cdots + T_s)$ that satisfies $(i_0, u_{i_0}) + (j_0, v_{j_0}) = P_k$. Thus, $(k, w_k) = P_k$ and

$$\mathrm{red}_\phi\left(\frac{A_k(x)}{\pi^{y_k}}\right) = \mathrm{red}_\phi\left(\frac{a_{i_0}(x)b_{j_0}(x)}{\pi^{y_k}}\right) = \mathrm{red}_\phi\left(\frac{a_{i_0}(x)}{\pi^{y_{i_0}(N_f)}}\right)\mathrm{red}_\phi\left(\frac{b_{j_0}(x)}{\pi^{y_{j_0}(N_g)}}\right) \neq 0.$$

This shows that $N' = N_f + N_g$ and that the ϕ-development (9) is admissible.

Finally, by (1), the λ-components $S' := S_\lambda(N')$, $S_f := S_\lambda(N_f)$, $S_g := S_\lambda(N_g)$ are related by $S' = S_f + S_g$. Let $(k, y_k(N'))$ be a point with integer coordinates lying on S' (not necessarily a vertex). Denote by I the set of the pairs (i,j) such that (i,u_i) lies on S_f, (j,v_j) lies on S_g, and $i+j=k$. Take $P(x) = \sum_{(i,j)\in I} a_i(x)b_j(x)$. By Lemma 1.4, for all other pairs (i,j) with $i+j=k$, the point $(i,u_i)+(j,v_j)$ lies above N'. Therefore, $c'_k(fg) = \operatorname{red}_\phi\left(P(x)/\pi^{y_k(N')}\right) = \sum_{(i,j)\in I} c_i(f)c_j(g)$. This shows that $R'_\lambda(fg)(y) = R_\lambda(f)(y)R_\lambda(g)(y)$. □

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

Corollary 1.14. *Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial. Let $\phi_1(x), \dots, \phi_r(x)$ be monic polyomials in $\mathcal{O}[x]$ such that their reductions modulo $\mathfrak{m}$ are pairwise different irreducible polynomials of $\mathbb{F}[x]$ and*

$$f(x) \equiv \phi_1(x)^{n_1} \cdots \phi_r(x)^{n_r} \pmod{\mathfrak{m}}.$$

Let $f(x) = F_1(x)\cdots F_r(x)$ be the factorization into a product of monic polynomials of $\mathcal{O}[x]$ satisfying $F_i(X) \equiv \phi_i(x)^{n_i} \pmod{\mathfrak{m}}$, provided by the Hensel lemma. Then,

$$N_{\phi_i}(F_i) = N^-_{\phi_i}(F_i) = N^-_{\phi_i}(f), \qquad R_\lambda(F_i)(y) \sim R_\lambda(f)(y),$$

for all $1 \le i \le r$ and all $\lambda \in \mathbb{Q}^-$.

Proof. For $1 \le i \le r$, let $G_i(x) = \prod_{j\neq i} F_j(x)$. Since $\phi_i(x)$ does not divide $G_i(x)$ modulo $\mathfrak{m}$, $N^-_{\phi_i}(G_i)$ is the single point $(0,0)$ and $R_\lambda(G_i)(y)$ is a nonzero constant for all $\lambda \in \mathbb{Q}^-$. By the theorem of the product, $N^-_{\phi_i}(f) = N^-_{\phi_i}(F_i) + N^-_{\phi_i}(G_i) = N^-_{\phi_i}(F_i)$, and $R_\lambda(f)(y) = R_\lambda(F_i)(y)R_\lambda(G_i)(y) \sim R_\lambda(F_i)(y)$. On the other hand, $N_{\phi_i}(F_i) = N^-_{\phi_i}(F_i)$ because both polygons have length n_i. □

1.4. **Theorems of the polygon and of the residual polynomial.** Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial divisible by $\phi(x)$ modulo $\mathfrak{m}$. By Hensel's lemma, $f(x) = f_\phi(x)G(x)$ in $\mathcal{O}[x]$, with monic polynomials $f_\phi(x)$, $G(x)$ such that $\operatorname{red}_\phi(G(x)) \neq 0$ and $f_\phi(x) \equiv \phi(x)^n \pmod{\mathfrak{m}}$. The aim of this section is to obtain a further factorization of $f_\phi(x)$ and certain arithmetic data about the factors. Thanks to Corollary 1.14, we shall be able to read this information directly on $f(x)$; more precisely, on the Newton polygon $N^-_\phi(f) = N_\phi(f_\phi)$ and the residual polynomial $R_\lambda(f)(y) \sim R_\lambda(f_\phi)(y)$.

Theorem 1.15 (Theorem of the polygon)**.** *Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial divisible by $\phi(x)$ modulo $\mathfrak{m}$. Suppose that $N^-_\phi(f) = S_1 + \cdots + S_g$ has g sides with slopes $-\infty \le \lambda_1 < \cdots < \lambda_g$. Then, $f_\phi(x)$ admits a factorization in $\mathcal{O}[x]$ into a product of g monic polynomials*

$$f_\phi(x) = F_1(x)\cdots F_g(x),$$

such that, for all $1 \le i \le g$:

1. *$N_\phi(F_i)$ is one-sided and equal to S_i up to a translation.*
2. *If S_i has finite slope λ_i, then $R_{\lambda_i}(F_i)(y) \sim R_{\lambda_i}(f)(y)$.*
3. *For any root $\theta \in \overline{\mathbb{Q}}_p$ of $F_i(x)$, we have $v(\phi(\theta)) = |\lambda_i|$.*

Proof. By the theorem of the product and Corollary 1.14, it is sufficient to show that if $F(x) := f_\phi(x)$ is irreducible, then $N_\phi(F) = S$ is one-sided and the roots $\theta \in \overline{\mathbb{Q}}_p$ all have $v(\phi(\theta))$ equal to minus the slope of S.

For all roots $\theta \in \overline{\mathbb{Q}}_p$ of $F(x)$, $v(\phi(\theta))$ takes the same value because the p-adic valuation is invariant under the Galois action. Since $F(x)$ is congruent to a power of $\phi(x)$ modulo $\mathfrak{m}$, we have $\lambda := -v(\phi(\theta)) < 0$. Clearly, $\lambda = -\infty$ if and only if $F(x) = \phi(x)$, and in this case the theorem is clear. Suppose λ is finite.

Let $x^k + b_{k-1}x^{k-1} + \cdots + b_0 \in \mathcal{O}[x]$ be the minimal polynomial of $\phi(\theta)$ and let $Q(x) = \phi(x)^k + b_{k-1}\phi(x)^{k-1} + \cdots + b_0$. We have $v(b_0) = k|\lambda|$ and $v(b_i) \geq (k-i)|\lambda|$ for all i; this implies that $N_\phi(Q)$ is one-sided with slope λ. Since $Q(\theta) = 0$, our polynomial $F(x)$ is an irreducible factor of $Q(x)$, and by the theorem of the product $N_\phi(F)$ is also one-sided with slope λ. □

If $S_1 \in \mathcal{S}(-\infty)$, the corresponding factor of $f_\phi(x)$ is $F_1(x) = \phi(x)^{\mathrm{ord}_\phi(f)}$.

Let $\lambda = -h/e$, with h, e coprime positive integers, be a negative rational number such that $S := S_\lambda(f)$ has positive length. Let $f_{\phi,\lambda}(x)$ be the factor of $f(x)$, corresponding to the pair ϕ, λ by the theorem of the polygon. Choose a root $\theta \in \overline{\mathbb{Q}}_p$ of $f_{\phi,\lambda}(x)$ and let $L = K(\theta)$. Since $v(\phi(\theta)) > 0$, we can consider an embedding

$$\mathcal{O}[x]/(\pi, \phi(x)) = \mathbb{F}_\phi \hookrightarrow \mathbb{F}_L, \quad \mathrm{red}_\phi(x) \mapsto \overline{\theta}. \tag{10}$$

Thus, a polynomial $P(x) \in \mathcal{O}[x]$ satisfies $v(P(\theta)) > 0$ if and only if $P(x)$ is divisible by $\phi(x)$ modulo $\mathfrak{m}$. This embedding depends on the choice of θ (and not only on L). After this identification of $\mathbb{F}_\phi$ with a subfield of $\mathbb{F}_L$ we can think that all residual polynomials have coefficients in $\mathbb{F}_L$. The theorem of the polygon yields certain arithmetic information on the field L.

Corollary 1.16. *With the notation above, the residual degree $f(L/K)$ is divisible by $m = \deg \phi(x)$, and the ramification index $e(L/K)$ is divisible by e. Moreover, the number of irreducible factors of $f_{\phi,\lambda}(x)$ is at most $d(S)$; in particular, if $d(S) = 1$, then the polynomial $f_{\phi,\lambda}(x)$ is irreducible in $\mathcal{O}[x]$, and $f(L/K) = m$, $e(L/K) = e$.*

Proof. The statement on the residual degree is a consequence of the embedding (10). By the theorem of the polygon, $v_L(\phi(\theta)) = e(L/K)h/e$. Since this is an integer and h, e are coprime, necessarily e divides $e(L/K)$. The upper bound for the number of irreducible factors is a consequence of the theorem of the product. Finally, if $d(S) = 1$, we have $me = \deg(f_{\phi,\lambda}(x)) = f(L/K)e(L/K)$, and necessarily $f(L/K) = m$ and $e(L/K) = e$. □

Let $\gamma(x) := \phi(x)^e/\pi^h \in K[x]$. Note that $v(\gamma(\theta)) = 0$; in particular, $\gamma(\theta) \in \mathcal{O}_L$.

Proposition 1.17 (Computation of $v(P(\theta))$)**.** *We keep the notation above for $f(x)$, $\lambda = -h/e$, θ, L, γ, and the embedding $\mathbb{F}_\phi \subseteq \mathbb{F}_L$ of* (10)*. Let $P(x) \in \mathcal{O}[x]$ be a nonzero polynomial, $S = S_\lambda(P)$, L_λ be the line of slope λ that contains S, and H be the ordinate of the intersection of this line with the vertical axis. Then:*

1. $v(P^S(\theta)) \geq 0, \quad \overline{P^S(\theta)} = R_\lambda(P)(\overline{\gamma(\theta)})$.
2. $v(P(\theta) - P^0(\theta)) > H$.
3. $v(P(\theta)) \geq H$, *and equality holds if and only if* $R_\lambda(P)(\overline{\gamma(\theta)}) \neq 0$.
4. $R_\lambda(f)(\overline{\gamma(\theta)}) = 0$.
5. *If* $R_\lambda(f)(y) \sim \psi(y)^a$ *for an irreducible polynomial* $\psi(y) \in \mathbb{F}_\phi[y]$, *then* $v(P(\theta)) = H$ *if and only if* $\psi(y) \nmid R_\lambda(P)(y)$ *in* $\mathbb{F}_\phi[y]$.

Proof. Let $P(x) = \sum_{0\le i} b_i(x)\phi(x)^i$ be the ϕ-adic development of $P(x)$, and denote $u_i = v(b_i)$, $N = N_\phi^-(P)$. Recall that $P^S(x) = \phi(x)^{-s}\pi^{-u}P^0(x)$, where (s,u) are the coordinates of the initial point of S, and $P^0(x) = \sum_{(i,u_i)\in S} b_i(x)\phi(x)^i$. Hence, for $d = d(S)$ we have

$$\begin{aligned} P^S(x) &= \pi^{-u}\left(b_s(x) + b_{s+e}(x)\phi(x)^e + \cdots + b_{s+de}\phi(x)^{de}\right) \\ &= (b_s(x)/\pi^u) + (b_{s+e}(x)/\pi^{u-h})\gamma(x) + \cdots + (b_{s+de}(x)/\pi^{u-hd})\gamma(x)^d. \end{aligned}$$

Since $v(b_{s+ie}) \ge y_{s+ie}(N) = u - hi$, for all $1 \le i \le d$, the two statements of item (1) are clear.

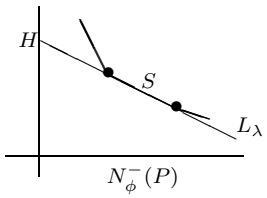


FIGURE 6

All points of N lie on or above the line L_λ; hence, for any integer abscissa i,

$$v(b_i(\theta)\phi(\theta)^i) = u_i + i|\lambda| \ge y_i(N) + i|\lambda| \ge H,$$

and equality holds if and only if $(i,u_i) \in S$. This proves item (2). Also, this shows that $v(P(\theta)) \ge H$. Since $v(\phi(\theta)^s\pi^u) = u + s|\lambda| = H$, we have

$$v(P(\theta)) = H \iff v(P^0(\theta)) = H \iff v(P^S(\theta)) = 0 \iff R_\lambda(P)(\overline{\gamma(\theta)}) \ne 0,$$

the last equivalence by item (1). This proves item (3).

Since $f(\theta) = 0$, item (4) is a consequence of item (3) applied to $P(x) = f(x)$. Finally, if $R_\lambda(f)(y) \sim \psi(y)^a$, then $\psi(y)$ is the minimal polynomial of $\overline{\gamma(\theta)}$ over $\mathbb{F}_\phi$, by item (4). Hence, $R_\lambda(P)(\overline{\gamma(\theta)}) \ne 0$ is equivalent to $\psi(y) \nmid R_\lambda(P)(y)$ in $\mathbb{F}_\phi[y]$. □

We now discuss how Newton polygons and residual polynomials are affected by an extension of the base field by an unramified extension.

Lemma 1.18. *We keep the notation above for $f(x)$, $\lambda = -h/e$, θ, L. Let $K' \subseteq L$ be the unramified extension of K of degree m, and identify $\mathbb{F}_\phi = \mathbb{F}_{K'}$ through the embedding* (10)*. Let $G(x) \in \mathcal{O}_{K'}[x]$ be the minimal polynomial of θ over K'. Let $\phi'(x) = x - \eta$, where $\eta \in K'$ is the unique root of $\phi(x)$ such that $G(x)$ is divisible by $x - \eta$ modulo $\mathfrak{m}_{K'}$. Then, for any nonzero polynomial $P(x) \in \mathcal{O}[x]$:*

$$N_{\phi'}^-(P) = N_\phi^-(P), \quad R'_\lambda(P)(y) = \epsilon^s R_\lambda(P)(\epsilon^e y),$$

where R' denotes the residual polynomial with respect to $\phi'(x)$ over K', $\epsilon \in \mathbb{F}_{K'}^*$ does not depend on $P(x)$, and s is the initial abscissa of $S_\lambda(P)$.

Proof. Consider the ϕ-adic development of $P(x)$:

$$\begin{aligned} P(x) &= \phi(x)^n + a_{n-1}(x)\phi(x)^{n-1} + \cdots + a_0(x) \\ &= \rho(x)^n\phi'(x)^n + a_{n-1}(x)\rho(x)^{n-1}\phi'(x)^{n-1} + \cdots + a_0(x), \end{aligned}$$

where $\rho(x) = \phi(x)/\phi'(x) \in \mathcal{O}_{K'}[x]$. Since $\phi(x)$ is irreducible modulo $\mathfrak{m}$, it is a separable polynomial modulo $\mathfrak{m}_{K'}$, so that $\rho(x)$ is not divisible by $\phi'(x)$ modulo

$\mathfrak{m}_{K'}$, and $v(\rho(\theta))=0$. Therefore, the above $\phi'(x)$-development of $P(x)$ is admissible and $N^-_{\phi'}(P)=N^-_\phi(P)$ by Lemma 1.12. Moreover the residual coefficients of the two polygons are related by $c_i'=c_i\epsilon^i$, where $\epsilon=\overline{\rho(\theta)}\in\mathbb{F}^*_{K'}$. This proves that $R'_\lambda(P)(y)=\epsilon^s R_\lambda(P)(\epsilon^e y)$. □

Theorem 1.19 (Theorem of the residual polynomial)**.** *Let $f(x)\in\mathcal{O}[x]$ be a monic polynomial divisible by $\phi(x)$ modulo $\mathfrak{m}$, S a side of $N^-_\phi(f)$ with finite slope λ, and*

$$R_\lambda(f)(y)\sim\psi_1(y)^{a_1}\cdots\psi_t(y)^{a_t}$$

the factorization of the residual polynomial of $f(x)$ into the product of powers of pairwise different monic irreducible polynomials in $\mathbb{F}_\phi[y]$. Then, the factor $f_{\phi,\lambda}(x)$ of $f(x)$, attached to ϕ,λ by the theorem of the polygon, admits a factorization

$$f_{\phi,\lambda}(x)=G_1(x)\cdots G_t(x)$$

into a product of t monic polynomials in $\mathcal{O}[x]$, such that $N_\phi(G_i)$ is one-sided with slope λ, and $R_\lambda(G_i)(y)\sim\psi_i(y)^{a_i}$ in $\mathbb{F}_\phi[y]$, for all $1\le i\le t$.

Proof. By the theorem of the product, we only need to prove that if $F(x):=f_{\phi,\lambda}(x)$ is irreducible, then $R_\lambda(F)(y)$ is the power of an irreducible polynomial of $\mathbb{F}_\phi[y]$. Let θ, L, K', $G(x)$ be as in Lemma 1.18, so that $F(x)=\prod_{\sigma\in\mathrm{Gal}(K'/K)}G^\sigma(x)$. Under the embedding $\mathbb{F}_\phi\hookrightarrow\mathbb{F}_L$, the field $\mathbb{F}_\phi$ is identified to $\mathbb{F}_{K'}$. By Lemma 1.18, there is a polynomial of degree one, $\phi'(x)\in\mathcal{O}_{K'}[x]$, such that $R'_\lambda(F)(y)\sim R_\lambda(F)(cy)$, for some nonzero constant $c\in\mathbb{F}_{K'}$. For any $\sigma\ne1$, the polynomial $G^\sigma(x)$ is not divisible by $\phi'(x)$ modulo $\mathfrak{m}_{K'}$; thus, $N_{\phi'}(G^\sigma)$ is a single point, and $R'_\lambda(G^\sigma)(y)$ is a constant. Therefore, by the theorem of the product, $R'_\lambda(G)(y)\sim R'_\lambda(F)(y)\sim R_\lambda(F)(cy)$, so that $R_\lambda(F)(y)$ is the power of an irreducible polynomial of $\mathbb{F}_\phi[y]$ if and only if $R'_\lambda(G)(y)$ has the same property over $\mathbb{F}_{K'}$. In conclusion, by extending the base field, we can suppose that $\deg\phi=m=1$.

Now consider the minimal polynomial $P(x)=x^k+b_{k-1}x^{k-1}+\cdots+b_0\in K[x]$ of $\gamma(\theta)=\phi(\theta)^e/\pi^h$ over K. Since $v(\gamma(\theta))=0$, we have $v(b_0)=0$. Thus, the polynomial $Q(x):=\phi(x)^{ek}+\pi^hb_{k-1}\phi(x)^{e(k-1)}+\cdots+\pi^{kh}b_0$ has one-sided $N^-_\phi(Q)$ with slope λ, and $R_\lambda(Q)(y)$ is the reduction of $P(y)$ modulo $\mathfrak{m}$, which is the power of an irreducible polynomial because $P(x)$ is irreducible in $K[x]$. Since $Q(\theta)=0$, $F(x)$ divides $Q(x)$, and it has the same property by the theorem of the product. □

Corollary 1.20. *With the notation above, let $\theta\in\overline{\mathbb{Q}}_p$ be a root of $G_i(x)$, and $L=K(\theta)$. Then, $f(L/K)$ is divisible by $m\deg\psi_i$. Moreover, the number of irreducible factors of $G_i(x)$ is at most a_i; in particular, if $a_i=1$, then $G_i(x)$ is irreducible in $\mathcal{O}[x]$, and $f(L/K)=m\deg\psi_i$, $e(L/K)=e$.*

Proof. The statement about $f(L/K)$ is a consequence of the embedding of the finite field $\mathbb{F}_\phi[y]/(\psi_i(y))$ into $\mathbb{F}_L$ determined by $\mathrm{red}_\phi(x)\mapsto\overline{\theta}$, $y\mapsto\overline{\gamma(\theta)}$. This embedding is well-defined by item (4) of Proposition 1.17. The other statements are a consequence of the theorem of the product and Corollary 1.16. □

1.5. **Types of order one.** Starting with a monic and separable polynomial $f(x)\in\mathcal{O}[x]$, the Newton polygon techniques provide partial information on the factorization of $f(x)$ in $\mathcal{O}[x]$, obtained after three *dissections*. In the first dissection we obtain as many factors of $f(x)$ as pairwise different irreducible factors modulo $\mathfrak{m}$

(Hensel's lemma). In the second dissection, each of these factors splits into the product of as many factors as sides of a certain Newton polygon of $f(x)$ (theorem of the polygon). In the third dissection, the factor that corresponds to a side of finite slope splits into the product of as many factors as irreducible factors of the residual polynomial of $f(x)$ attached to this side (theorem of the residual polynomial).

The final list of factors of $f(x)$ obtained by this procedure can be parameterized by certain data, which we call *types of order zero and of order one*.

Definition 1.21. A type of order zero is a monic irreducible polynomial $\mathbf{t} = \psi_0(y) \in \mathbb{F}[y]$. We attach to any type of order zero the semigroup homomorphism:

$$\omega^{\mathbf{t}}\colon \mathcal{O}[x] \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}, \quad P(x) \mapsto \operatorname{ord}_{\psi_0}(\overline{P(x)/\pi^{v(P)}}).$$

Let $f(x) \in \mathcal{O}[x]$ be a monic and separable polynomial. We say that the type $\mathbf{t}$ is f-complete if $\omega^{\mathbf{t}}(f) = 1$. In this case, we denote by $f_{\mathbf{t}}(x) \in \mathcal{O}[x]$ the monic irreducible factor of $f(x)$ determined by $f_{\mathbf{t}}(y) \equiv \psi_0(y) \pmod{\mathfrak{m}}$.

Definition 1.22. A type of order one is a triple: $\mathbf{t} = (\phi(x); \lambda, \psi(y))$, where:

(1) $\phi(x) \in \mathcal{O}[x]$ is a monic polynomial which is irreducible modulo $\mathfrak{m}$.
(2) $\lambda = -h/e \in \mathbb{Q}^-$, with h, e positive coprime integers.
(3) $\psi(y) \in \mathbb{F}_\phi[y]$ is a monic irreducible polynomial, $\psi(y) \neq y$.

By truncation of $\mathbf{t}$ we obtain the type of order zero: $\operatorname{Trunc}_0(\mathbf{t}) := \phi(y) \pmod{\mathfrak{m}}$.

We denote by $\mathbf{t}_0(f)$ the set of all monic irreducible factors of $f(x)$ modulo $\mathfrak{m}$. We denote by $\mathbf{t}_1(f)$ the set of all types of order one obtained from $f(x)$ along the process of applying the three classical dissections: for any non-f-complete $\psi_0(y) \in \mathbf{t}_0(f)$, we take a monic lift $\phi(x)$ to $\mathcal{O}[x]$; then we consider all finite slopes λ of the sides of positive length of $N_\phi^-(f)$, and finally, for each of them we take the different monic irreducible factors $\psi(y)$ of the residual polynomial $R_\lambda(f)(y) \in \mathbb{F}_\phi[y]$. These types are not intrinsic objects of $f(x)$. There is a noncanonical choice of the lifts $\phi(x) \in \mathcal{O}[x]$, and the data λ, $\psi(y)$ depend on this choice.

Let $\mathbf{T}_1(f)$ be the union of $\mathbf{t}_1(f)$ and the set of all f-complete types of order zero. Let $f_\infty(x)$ be the product of all polynomials $\phi(x)$ of the types $\mathbf{t} \in \mathbf{t}_1(f)$ such that $\phi(x)$ divides $f(x)$ in $\mathcal{O}[x]$. By the previous results, we have a factorization in $\mathcal{O}[x]$:

$$f(x) = f_\infty(x) \prod\nolimits_{\mathbf{t} \in \mathbf{T}_1(f)} f_{\mathbf{t}}(x),$$

where, for any $\mathbf{t} \in \mathbf{t}_1(f)$, $f_{\mathbf{t}}(x)$ is defined to be the unique monic divisor of $f(x)$ in $\mathcal{O}[x]$ satisfying the following properties:

$$\begin{aligned} &f_{\mathbf{t}}(x) \equiv \phi(x)^{ea \deg \psi} \pmod{\mathfrak{m}}, \quad a = \operatorname{ord}_\psi(R_\lambda(f)), \\ &N_\phi(f_{\mathbf{t}}) \text{ is one-sided with slope } \lambda, \\ &R_\lambda(f_{\mathbf{t}})(y) \sim \psi(y)^a \text{ in } \mathbb{F}_\phi[y]. \end{aligned}$$

The factor $f_\infty(x)$ is already expressed as a product of irreducible polynomials in $\mathcal{O}[x]$. Also, if $a = 1$, the theorem of the residual polynomial shows that $f_{\mathbf{t}}(x)$ is irreducible too. Thus, the remaining task is to obtain the further factorization of $f_{\mathbf{t}}(x)$, for the types $\mathbf{t} \in \mathbf{t}_1(f)$ with $a > 1$.

Suppose a type of order one, $\mathbf{t} = (\phi(x); \lambda, \psi(y))$, is fixed. Then, for any nonzero $P(x) \in \mathcal{O}[x]$, any $N \in \mathcal{PP}$, and any $T \in \mathcal{S}(\lambda)$, we shall denote from now on:

$$\begin{aligned} &v_1(P) := v(P), && \omega_1(P) := \omega^{\overline{\phi}}(P) = \mathrm{ord}_{\overline{\phi}}(\overline{P(x)/\pi^{v(P)}}),\\ &N_1(P) := N_\phi(P), && N_1^-(P) := N_\phi^-(P),\\ &S_1(N) := S_\lambda(N), && S_1(P) := S_\lambda(P) = S_\lambda(N_1^-(P)),\\ &R_1(P)(y) := R_\lambda(P)(y), && R_1(P,T)(y) := R_\lambda(P,T)(y). \end{aligned}$$

The subscript "1" emphasizes that these objects are *first order* data.

The aim of the next two sections is to introduce Newton polygons of higher order and prove similar theorems, yielding a further factorization of each $f_{\mathbf{t}}(x)$. As before, we shall obtain arithmetic information about the factors of $f_{\mathbf{t}}(x)$ just by a direct manipulation of $f(x)$, without actually computing a p-adic approximation to these factors. This fact is crucial to ensure that the whole process has a low complexity. However, once an irreducible factor of $f(x)$ is "detected", the theory provides a reasonably good approximation to this factor as a by-product (Proposition 3.12).

2. Newton polygons of higher order

Throughout this section, r is an integer, $r \geq 2$. We shall construct Newton polygons of order r and prove their basic properties and the theorem of the product in order r, under the assumption that analogous results have already been obtained in orders $1, \dots, r-1$. We also assume that the theorems of the polygon and of the residual polynomial have been proved in orders $1, \dots, r-1$ (cf. section 3). For $r = 1$ all these results have been proved in section 1.

2.1. Types of order $r-1$.

A *type of order* $r-1$ is a sequence of data

$$\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \cdots; \lambda_{r-2}, \phi_{r-1}(x); \lambda_{r-1}, \psi_{r-1}(y)),$$

where $\phi_i(x)$ are monic polynomials in $\mathcal{O}[x]$, λ_i are negative rational numbers and $\psi_{r-1}(y)$ is a polynomial over a certain finite field (to be specified below), that satisfy the following recursive properties:

(1) $\phi_1(x)$ is irreducible modulo $\mathfrak{m}$. Let $\psi_0(y) \in \mathbb{F}[y]$ be the polynomial obtained by reduction of $\phi_1(y)$ modulo $\mathfrak{m}$, and define $\mathbb{F}_1 := \mathbb{F}[y]/(\psi_0(y))$.
(2) For all $1 \leq i < r-1$, the Newton polygon of i-th order, $N_i(\phi_{i+1})$, is one-sided with slope λ_i.
(3) For all $1 \leq i < r-1$, the residual polynomial of i-th order, $R_i(\phi_{i+1})(y)$, is an irreducible polynomial in $\mathbb{F}_i[y]$. Let $\psi_i(y) \in \mathbb{F}_i[y]$ be the monic polynomial determined by $R_i(\phi_{i+1})(y) \sim \psi_i(y)$, and define $\mathbb{F}_{i+1} := \mathbb{F}_i[y]/(\psi_i(y))$.
(4) For all $1 \leq i < r-1$, $\phi_{i+1}(x)$ has minimal degree among all monic polynomials in $\mathcal{O}[x]$ satisfying (2) and (3).
(5) $\psi_{r-1}(y) \in \mathbb{F}_{r-1}[y]$ is a monic irreducible polynomial, $\psi_{r-1}(y) \neq y$. We define $\mathbb{F}_r := \mathbb{F}_{r-1}[y]/(\psi_{r-1}(y))$.

The type determines a tower $\mathbb{F} =: \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r$ of finite fields. The field $\mathbb{F}_i$ should not be confused with the finite field with i elements.

By the theorem of the product in orders $1, \dots, r-1$, the polynomials $\phi_i(x)$ are all irreducible over $\mathcal{O}[x]$.

Let us be more precise about the meaning of $N_i(-)$, $R_i(-)$, used in items (2), (3).

Notation. We denote $\mathrm{Trunc}_0(\mathbf{t}) := \psi_0(y)$. For all $1 \le i < r$, we obtain by truncation of $\mathbf{t}$ a type of order i:

$$\mathrm{Trunc}_i(\mathbf{t}) := (\phi_1(x); \lambda_1, \phi_2(x); \cdots; \lambda_{i-1}, \phi_i(x); \lambda_i, \psi_i(y)).$$

We have semigroup homomorphisms:

$$N_i^- \colon \mathcal{O}[x]\backslash\{0\} \to \mathcal{PP}, \quad S_i \colon \mathcal{O}[x]\backslash\{0\} \to \mathcal{S}(\lambda_i), \quad R_i \colon \mathcal{O}[x]\backslash\{0\} \to \mathbb{F}_i[y].$$

For any nonzero polynomial $P(x) \in \mathcal{O}[x]$, $N_i(P)$ is the i-th order Newton polygon with respect to the type $\mathrm{Trunc}_i(\mathbf{t})$, $S_i(P)$ is the λ_i-component of $N_i^-(P)$, and $R_i(P)(y)$ is the residual polynomial of i-th order with respect to λ_i. The polynomial $R_i(P)(y)$ has degree $d(S_i(P))$.

Other data attached to the type $\mathbf{t}$ deserve a specific notation. For all $1 \le i < r$:

- $\lambda_i = -h_i/e_i$, with e_i, h_i positive coprime integers.
- $f_i := \deg \psi_i(y)$.
- $m_i := \deg \phi_i(x)$. Note that $m_{i+1} = m_i e_i f_i = m_1 e_1 f_1 \cdots e_i f_i$.
- ℓ_i, $\ell_i' \in \mathbb{Z}$ are fixed integers such that $\ell_i h_i - \ell_i' e_i = 1$.
- $z_i := y \pmod{\psi_i(y)} \in \mathbb{F}_{i+1}^*$. Note that $\mathbb{F}_{i+1} = \mathbb{F}_i(z_i)$.

We also denote: $f_0 := \deg \psi_0(y) = \deg \phi_1(x)$, $z_0 := y \pmod{\psi_0(y)} \in \mathbb{F}_1^*$, and $m_r := m_{r-1} e_{r-1} f_{r-1}$.

Moreover, for all $0 \le i < r$ we have semigroup homomorphisms

$$\omega_{i+1} \colon \mathcal{O}[x] \setminus \{0\} \longrightarrow \mathbb{Z}_{\ge 0}, \qquad P(x) \mapsto \mathrm{ord}_{\psi_i}(R_i(P)),$$

where, by convention, $R_0(P)(y) = \overline{P(y)/\pi^{v(P)}} \in \mathbb{F}[y]$. By Lemma 2.17 in order $r-1$ (see Definition 1.8 for order one):

$$\ell(N_i(P)) = \lfloor \deg P/m_i \rfloor, \quad \ell(N_i^-(P)) = \omega_i(P), \quad 1 \le i < r, \tag{11}$$

and $N_i^-(P)$ has a side of slope $-\infty$ if and only if $P(x)$ is divisible by $\phi_i(x)$ in $\mathcal{O}[x]$.

Definition 2.1. We say that a monic polynomial $P(x) \in \mathcal{O}[x]$ is of type $\mathbf{t}$ when

(1) $P(x) \equiv \phi_1(x)^{a_0} \pmod{\mathfrak{m}}$, for some positive integer a_0.
(2) For all $1 \le i < r$, the Newton polygon $N_i(P)$ is one-sided with slope λ_i, and $R_i(P)(y) \sim \psi_i(y)^{a_i}$ in $\mathbb{F}_i[y]$, for some positive integer a_i.

Lemma 2.2. *Let $P(x) \in \mathcal{O}[x]$ be a nonzero polynomial. Then,*

(1) $\omega_1(P) \ge e_1 f_1 \omega_2(P) \ge \cdots \ge e_1 f_1 \cdots e_{r-1} f_{r-1} \omega_r(P)$.
(2) $\deg P < m_r \implies \omega_r(P) = 0$.
(3) *If $P(x)$ is of type $\mathbf{t}$, then all inequalities in item (1) are equalities, and*

$$\deg P(x) = m_r \omega_r(P) = m_{r-1} \omega_{r-1}(P) = \cdots = m_1 \omega_1(P).$$

Proof. Item (1) is a consequence of (11); in fact, for all $1 \le i < r$:

$$e_i f_i \omega_{i+1}(P) \le e_i \deg R_i(P) = e_i d(S_i(P)) = \ell(S_i(P)) \le \ell(N_i^-(P)) = \omega_i(P). \tag{12}$$

Item (2) is a consequence of (11) and item (1):

$$m_r > \deg P \ge m_{r-1} \omega_{r-1}(P) \ge m_r \omega_r(P).$$

Finally, if $P(x)$ is of type $\mathbf{t}$ the two inequalities of (12) are equalities, so that $m_i \omega_i(P) = m_{i+1} \omega_{i+1}(P)$; on the other hand, $\deg P = m_1 a_0 = m_1 \omega_1(P)$. □

Definition 2.3. Let $P(x) \in \mathcal{O}[x]$ be a monic polynomial with $\omega_r(P) > 0$. We denote by $P_{\mathbf{t}}(x)$ the monic factor of $P(x)$ of greatest degree among all factors that are of type $\mathbf{t}$. By the theorems of the polygon and of the residual polynomial in orders $1, \dots, r-1$, this factor exists and it satisfies

$$\omega_r(P_{\mathbf{t}}) = \omega_r(P), \quad \deg P_{\mathbf{t}} = m_r \omega_r(P). \tag{13}$$

Lemma 2.4. *Let $P(x), Q(x) \in \mathcal{O}[x]$ be monic polynomials of positive degree.*

1. *If $P(x)$ is irreducible in $\mathcal{O}[x]$, then it is of type $\mathbf{t}$ if and only if $\omega_r(P) > 0$.*
2. *$P(x)$ is of type $\mathbf{t}$ if and only if $\deg P = m_r \omega_r(P) > 0$.*
3. *$P(x)Q(x)$ is of type $\mathbf{t}$ if and only if $P(x)$ and $Q(x)$ are both of type $\mathbf{t}$.*

Proof. The polynomial $P(x)$ is of type $\mathbf{t}$ if and only if $\omega_r(P) > 0$ and $P_{\mathbf{t}}(x) = P(x)$; thus, items (1) and (2) are an immediate consequence of (13). Item (3) follows from the theorem of the product in orders $1, \dots, r-1$. □

We fix a type $\mathbf{t}$ of order $r-1$ for the rest of section 2.

2.2. **The p-adic valuation of r-th order.** In this paragraph we shall attach to $\mathbf{t}$ a discrete valuation $v_r \colon K(x)^* \longrightarrow \mathbb{Z}$, that restricted to K extends v with index $e_1 \cdots e_{r-1}$. We only need to define v_r on $\mathcal{O}[x]$. Consider the mapping

$$H_{r-1} \colon \mathcal{S}(\lambda_{r-1}) \longrightarrow \mathbb{Z}_{\geq 0},$$

that assigns to each side $S \in \mathcal{S}(\lambda_{r-1})$ the ordinate of the point of intersection of the vertical axis with the line $L_{\lambda_{r-1}}$ of slope λ_{r-1} that contains S. If (i, u) is any point with integer coordinates lying on S, then $H_{r-1}(S) = u + |\lambda_{r-1}| i$; thus, H_{r-1} is a semigroup homomorphism.

Definition 2.5. For any nonzero polynomial $P(x) \in \mathcal{O}[x]$, we define

$$v_r(P) := e_{r-1} H_{r-1}(S_{r-1}(P)).$$

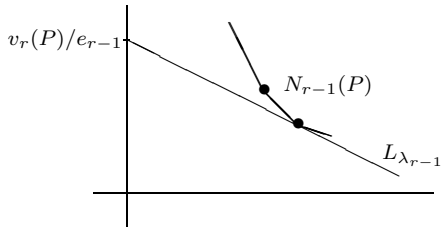


FIGURE 7

Note that v_r depends only on v_{r-1}, ϕ_{r-1} and λ_{r-1}.

Proposition 2.6. *The natural extension of v_r to $K(x)^*$ is a discrete valuation, whose restriction to K^* extends v with index $e_1 \cdots e_{r-1}$.*

Proof. The mapping v_r restricted to $\mathcal{O}[x] \setminus \{0\}$ is a semigroup homomorphism, because it is the composition of three semigroup homomorphisms; in particular, $v_r \colon K(x)^* \longrightarrow \mathbb{Z}$ is a group homomorphism.

Let $P(x), Q(x) \in \mathcal{O}[x]$ be two nonzero polynomials and denote $N_P = N_{r-1}^-(P)$, $N_Q = N_{r-1}^-(Q)$. Let L_P, L_Q be the respective lines of slope λ_{r-1} having first contact with N_P, N_Q from below. All points of N_P lie on or above the line L_P and all points of N_Q lie on or above the line L_Q. If $v_r(P) \leq v_r(Q)$, all points of both

polygons lie on or above the line L_P. Thus, all points of $N_{r-1}^-(P+Q)$ lie on or above this line too, and this shows that $v_r(P+Q) \geq v_r(P)$.

Finally, for any $a \in \mathcal{O}$, we have $v_r(a) = e_{r-1}v_{r-1}(a)$ by definition, since the $(r-1)$-th order Newton polygon of a is the single point $(0, v_{r-1}(a))$. □

This discrete valuation was introduced by S. MacLane in a more abstract setting [McL36, McL36b]. More precisely, items (3) and (4) of Proposition 2.7 below show that v_r/e_{r-1} is an "augmented valuation" of v_{r-1} with respect to the "key polynomial" ϕ_{r-1}, in MacLane's terminology [McL36, Sec.4,(3)].

In [Mon99, Ch.2, §2], explicit generators of the residue field of v_r as a transcendental extension of a finite field were computed. These results lead to a more conceptual and elegant definition of residual polynomials in higher order, as the reductions modulo v_r of the virtual factors (cf. section 2.5). We shall not follow this approach, in order not to burden the paper with more technicalities.

The next proposition gathers the basic properties of this discrete valuation.

Proposition 2.7. *Let $P(x) \in \mathcal{O}[x]$ be a nonzero polynomial.*

(1) *$v_r(P) \geq e_{r-1}v_{r-1}(P)$ and equality holds if and only if $\omega_{r-1}(P) = 0$.*
(2) *$v_r(P) = 0$ if and only if $v_2(P) = 0$ if and only if $\mathrm{red}_{\phi_1}(P) \neq 0$.*
(3) *$v_r(\phi_{r-1}) = e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1}$.*
(4) *If $P(x) = \sum_{0\leq i} a_i(x)\phi_{r-1}(x)^i$ is the ϕ_{r-1}-adic development of $P(x)$, then*

$$v_r(P) = \min_{0\leq i}\{v_r(a_i(x)\phi_{r-1}(x)^i)\} = e_{r-1}\min_{0\leq i}\{v_{r-1}(a_i) + i(v_{r-1}(\phi_{r-1}) + |\lambda_{r-1}|)\}.$$

Proof. We denote $N = N_{r-1}^-(P)$ throughout the proof. By item (1) of Lemma 2.17 in order $r-1$, all points of N lie on or above the horizontal line with ordinate $v_{r-1}(P)$. Hence, $v_r(P) \geq e_{r-1}v_{r-1}(P)$. Equality holds if and only if N is the single point $(0, v_{r-1}(P))$; this is equivalent to $\omega_{r-1}(P) = 0$, by (11). This proves item (1).

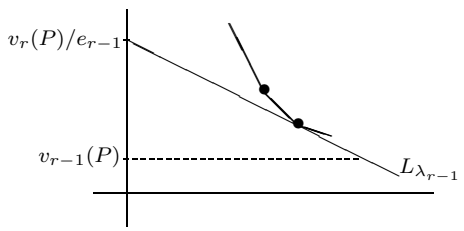


FIGURE 8

By a recurrent application of item (1), $v_r(P) = 0$ is equivalent to $v_1(P) = 0$ and $\omega_1(P) = \cdots = \omega_{r-1}(P) = 0$. By Lemma 2.2 this is equivalent to $v_1(P) = 0$ and $\omega_1(P) = 0$, which is in turn equivalent to $v_2(P) = 0$, and also to $P(x) \notin (\pi, \phi_1(x))$. This proves item (2).

The polygon $N_{r-1}(\phi_{r-1})$ is one-sided with slope $-\infty$, and the finite part is the point $(1, v_{r-1}(\phi_{r-1}))$. This proves item (3).

By definition, $v_r(a_i(x)\phi_{r-1}(x)^i)$ is e_{r-1} times the ordinate at the origin of the line L of slope λ_{r-1} passing through $(i, v_{r-1}(a_i(x)\phi_{r-1}(x)^i))$. Since all points of N lie on or above the line $L_{\lambda_{r-1}}$ of slope λ_{r-1} having first contact with N from below, the line L lies on or above $L_{\lambda_{r-1}}$ too, and $v_r(a_i(x)\phi_{r-1}(x)^i) \geq v_r(P)$. See Figure 9.

Since v_r is a valuation, this proves item (4). □

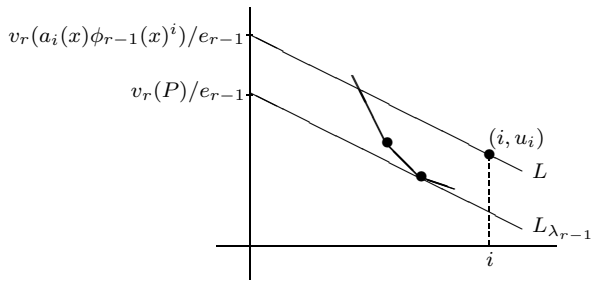


FIGURE 9

In a natural way, ω_r induces a group homomorphism from $K(x)^*$ to $\mathbb{Z}$, but it is not a discrete valuation of this field. For instance, for $K=\mathbb{Q}_p$, $\pi=p$, $\mathbf{t}=(x;-1,y+1)$ and $P(x)=x+p$, $Q(x)=x+p+p^2$, we have

$$\begin{aligned} &R_1(P)=y+1, && R_1(Q)=y+1, && R_1(P-Q)=1,\\ &\omega_2(P)=1, && \omega_2(Q)=1, && \omega_2(P-Q)=0. \end{aligned}$$

However, we shall say that ω_r is a *pseudo-valuation with respect to* v_r; this is justified by the following properties of ω_r.

Proposition 2.8. *Let $P(x), Q(x)\in\mathcal{O}[x]$ be two nonzero polynomials such that $v_r(P)=v_r(Q)$. Then,*

(1) *$v_r(P-Q)>v_r(P)$ if and only if $S_{r-1}(P)=S_{r-1}(Q)$ and $R_{r-1}(P)=R_{r-1}(Q)$. In particular, $\omega_r(P)=\omega_r(Q)$ in this case.*
(2) *If $\omega_r(P)\neq\omega_r(Q)$, then $\omega_r(P-Q)=\min\{\omega_r(P),\omega_r(Q)\}$.*

Proof. Denote $N=N_{r-1}^-(P)$, $N'=N_{r-1}^-(Q)$. Since $v_r(P)=v_r(Q)$, there is a line $L_{\lambda_{r-1}}$ of slope λ_{r-1} having first contact simultaneoulsly with N and N' from below. We consider the shortest segment T of $L_{\lambda_{r-1}}$ that contains $S_{r-1}(P)$ and $S_{r-1}(Q)$. See Figure 10.

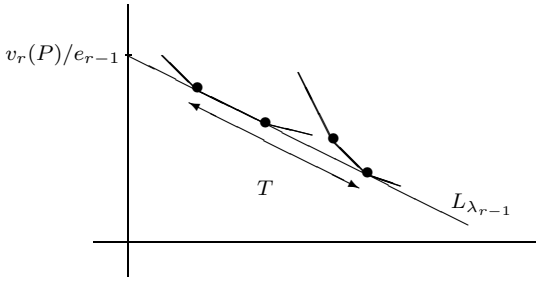


FIGURE 10

By Lemma 2.23 in order $r-1$ (cf. (3) in order one):

$$R_{r-1}(P-Q,T)=R_{r-1}(P,T)-R_{r-1}(Q,T). \tag{14}$$

By (19) in order $r-1$ (cf. (2) in order one), the double condition $S_{r-1}(P)=S_{r-1}(Q)$, $R_{r-1}(P)=R_{r-1}(Q)$, is equivalent to $R_{r-1}(P,T)=R_{r-1}(Q,T)$; that is,

to $R_{r-1}(P-Q,T)=0$. This is equivalent to $N_{r-1}^-(P-Q)$ lying above $L_{\lambda_{r-1}}$, which is equivalent in turn to $v_r(P-Q)>v_r(P)$. This proves item (1).

By (19) and (2), again, the equality (14) translates into

$$y^a R_{r-1}(P-Q)(y)=y^b R_{r-1}(P)(y)-y^c R_{r-1}(Q)(y)$$

for certain nonnegative integers a,b,c. Since the residual polynomials are never divisible by y, and $\psi_{r-1}(y)\neq y$, from $\operatorname{ord}_{\psi_{r-1}}(R_{r-1}(P))<\operatorname{ord}_{\psi_{r-1}}(R_{r-1}(Q))$ we deduce $\operatorname{ord}_{\psi_{r-1}}(R_{r-1}(P-Q))=\operatorname{ord}_{\psi_{r-1}}(R_{r-1}(P))$. This proves item (2). □

We can reinterpret the computation of $v(P(\theta))$ given in item (5) of Proposition 3.5 in order $r-1$ (Proposition 1.17 for $r=2$), in terms of the pair v_r, ω_r.

Proposition 2.9. *Let $\theta\in\overline{\mathbb{Q}}_p$ be a root of a polynomial in $\mathcal{O}[x]$ of type $\mathbf{t}$. Then, for any nonzero polynomial $P(x)\in\mathcal{O}[x]$,*

$$v(P(\theta))\geq v_r(P(x))/e_1\cdots e_{r-1},$$

and equality holds if and only if $\omega_r(P)=0$. □

2.3. **Construction of a representative of t.** By Lemma 2.2, a nonconstant polynomial of type $\mathbf{t}$ has degree at least m_r. In this section we shall show how to construct in an effective (and recursive) way a polynomial $\phi_r(x)$ of type $\mathbf{t}$ and minimal degree m_r.

We first show how to construct a polynomial with prescribed residual polynomial.

Proposition 2.10. *Let V be an integer, $V\geq e_{r-1}f_{r-1}v_r(\phi_{r-1})$. Let $\varphi(y)\in\mathbb{F}_{r-1}[y]$ be a nonzero polynomial of degree less than f_{r-1}, and let $\nu=\operatorname{ord}_y(\varphi)$. Then, we can construct in an effective way a polynomial $P(x)\in\mathcal{O}[x]$ satisfying the following properties:*

$$\deg P(x)<m_r,\qquad v_r(P)=V,\qquad y^\nu R_{r-1}(P)(y)=\varphi(y).$$

Proof. Let L be the line of slope λ_{r-1} with ordinate V/e_{r-1} at the origin. By item (3) of Proposition 2.7, $V/e_{r-1}\geq f_{r-1}v_r(\phi_{r-1})\geq f_{r-1}h_{r-1}$; thus, the line L cuts the horizontal axis at the abscissa $V/h_{r-1}\geq e_{r-1}f_{r-1}$. Let T be the greatest side contained in L, whose end points have nonnegative integer coordinates. Let (s,u) be the initial point of T and denote $u_j:=u-jh_{r-1}$, for all $0\leq j<f_{r-1}$, so that $(s+je_{r-1},u_j)$ lies on L. Clearly, $s<e_{r-1}$ and, for all j,

$$j<f_{r-1},\ s<e_{r-1}\implies s+je_{r-1}<e_{r-1}f_{r-1}. \tag{15}$$

Hence, $(s+je_{r-1},u_j)$ lies on T.

Let $\varphi(y)=\sum_{0\leq j<f_{r-1}}c_jy^j$, with $c_j\in\mathbb{F}_{r-1}$. Select polynomials $c_j(y)\in\mathbb{F}_{r-2}[y]$ of degree less than f_{r-2}, such that c_j is the class of $c_j(y)$ modulo $\psi_{r-2}(y)$, or equivalently, $c_j(z_{r-2})=c_j$.

For any nonzero polynomial $P(x)\in\mathcal{O}[x]$ we denote by $s_i(P)$ the initial abscissa of $S_i(P)$, for all $1\leq i<r$. We want to construct $P(x)$ satisfying:

$$\deg P(x)<m_r,\quad v_r(P)=V,\quad \nu=(s_{r-1}(P)-s)/e_{r-1},\quad y^\nu R_{r-1}(P)(y)=\varphi(y).$$

We proceed by induction on $r\geq 2$. For $r=2$ the polynomials $c_j(y)$ belong to $\mathbb{F}[y]$; we abuse language and denote by $c_j(x)\in\mathcal{O}[x]$ the polynomials obtained by choosing arbitrary lifts to $\mathcal{O}$ of the nonzero coefficients of $c_j(y)$. The polynomial $P(x)=\sum_{0\leq j<f_{r-1}}\pi^{u-jh_1}c_j(x)\phi_1(x)^{s+je_1}$ satisfies the required properties. In fact,

$$\deg(c_j(x)\phi_1(x)^{s+je_1})<m_1+(e_1f_1-1)m_1=m_2,$$

for all j, by (15). For the coefficients $c_j = 0$ we take $c_j(x) = 0$. For the coefficients $c_j \neq 0$, we have $c_j(y) \neq 0$ and $v(c_j(x)) = 0$; hence, $v(\pi^{u-jh_1}c_j(x)) = u - jh_1 = u_j$. Thus, the coefficient $\pi^{u-jh_1}c_j(x)$ determines a point of $N_1^-(P)$ lying on T, and $v_2(P) = V$. Finally, it is clear by construction that $\nu = (s_1(P) - s)/e_1$ and $y^\nu R_1(P)(y) = R_1(P,T)(y) = \varphi(y)$.

Now let $r \geq 3$, and suppose that the proposition has been proved for orders $2, \dots, r-1$. For any $0 \leq j < f_{r-1}$, denote $V_j := u_j - (s + je_{r-1})v_{r-1}(\phi_{r-1})$. Since $u = (V - sh_{r-1})/e_{r-1}$, we get

$$\begin{aligned} V_j &= \frac{1}{e_{r-1}}\,(V - (s+je_{r-1})(e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1}) = \text{(by item (3) of Prop. 2.7)} \\ &= \frac{1}{e_{r-1}}\,(V - (s+je_{r-1})v_r(\phi_{r-1})) \geq \ \text{(by (15))} \\ &\geq \frac{1}{e_{r-1}}\,(V - (e_{r-1}f_{r-1} - 1)v_r(\phi_{r-1})) \geq \ \text{(by hypothesis)} \\ &\geq \frac{1}{e_{r-1}}v_r(\phi_{r-1}) = v_{r-1}(\phi_{r-1}) + \frac{h_{r-1}}{e_{r-1}} > v_{r-1}(\phi_{r-1}) = e_{r-2}f_{r-2}v_{r-1}(\phi_{r-2}), \end{aligned}$$

the last equality by (16) below, in order $r-1$.

Let L_j be the line of slope λ_{r-2} with ordinate at the origin V_j/e_{r-2}. Let $T(j)$ be the greatest side contained in L_j, whose end points have nonnegative integer coordinates. Let $\mathfrak{s}_j$ be the initial abscissa of $T(j)$. Consider the unique polynomial $\varphi_j(y) \in \mathbb{F}_{r-2}[y]$, of degree less than f_{r-2}, such that

$$\varphi_j(y) \equiv y^{(\ell_{r-2}u_j - \mathfrak{s}_j)/e_{r-2}}c_j(y) \ (\mathrm{mod}\ \psi_{r-2}(y)),$$

and let $\nu_j = \mathrm{ord}_y(\varphi_j)$. By the induction hypothesis, we are able to construct a polynomial $P_j(x)$ of degree less than m_{r-1}, with $v_{r-1}(P_j) = V_j$, $\nu_j = (s_{r-2}(P_j) - \mathfrak{s}_j)/e_{r-2}$, and $y^{\nu_j}R_{r-2}(P_j)(y) = \varphi_j(y)$ in $\mathbb{F}_{r-2}[y]$.

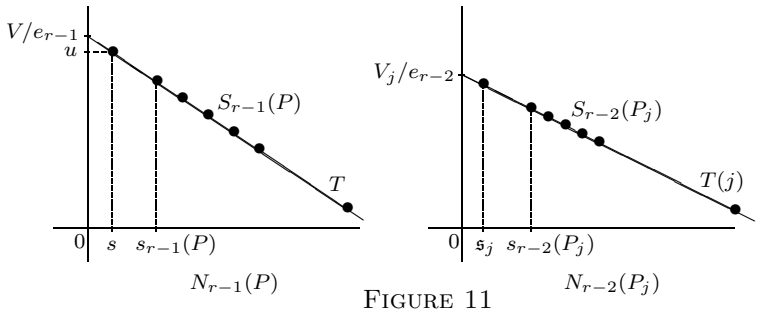


FIGURE 11

The polynomial we are looking for is:

$$P(x) = \sum_{0 \leq j < f_{r-1}} P_j(x)\phi_{r-1}(x)^{s+je_{r-1}} \in \mathcal{O}[x].$$

In fact, by (15), $\deg(P_j(x)\phi_{r-1}(x)^{s+je_{r-1}}) < m_{r-1} + (e_{r-1}f_{r-1} - 1)m_1 = m_r$, for all j. If $P_j(x) \neq 0$, then $v_{r-1}(P_j(x)\phi_{r-1}(x)^{s+je_{r-1}}) = V_j + (s+je_{r-1})v_{r-1}(\phi_{r-1}) = u_j$, so that all of these coefficients determine points of $N_{r-1}^-(P)$ lying on T; this shows that $v_r(P) = V$. For $c_j = 0$ we take $P_j(x) = 0$; hence, $\nu = (s_{r-1}(P) - s)/e_{r-1}$, and

by (19) in order $r-1$:

$$y^{\nu} R_{r-1}(P)(y) = R_{r-1}(P,T)(y) = \sum_{P_j(x)\neq 0} (z_{r-2})^{t(j)} R_{r-2}(P_j)(z_{r-2}) y^j,$$

where $t(j) := t_{r-2}(s + je_{r-1}) = (s_{r-2}(P_j) - \ell_{r-2}u_j)/e_{r-2}$ (cf. Definition 2.19). Finally,

$$\begin{aligned}(z_{r-2})^{t(j)} R_{r-2}(P_j)(z_{r-2}) &= (z_{r-2})^{t(j)-\nu_j} \varphi_j(z_{r-2}) \\ &= (z_{r-2})^{t(j)-\nu_j + \frac{\ell_{r-2}u_j - s_j}{e_{r-2}}} c_j(z_{r-2}) = c_j,\end{aligned}$$

so that $y^{\nu} R_{r-1}(P)(y) = \varphi(y)$. □

Theorem 2.11. *We can effectively construct a monic polynomial $\phi_r(x)$ of type $\mathbf{t}$ such that $R_{r-1}(\phi_r)(y) \sim \psi_{r-1}(y)$. This polynomial is irreducible over $\mathcal{O}[x]$ and it satisfies*

$$\deg \phi_r = m_r, \quad \omega_r(\phi_r) = 1, \quad v_r(\phi_r) = e_{r-1}f_{r-1}v_r(\phi_{r-1}). \tag{16}$$

Proof. The Newton polygon $N_{r-1}(\phi_{r-1})$ is one-sided with slope $-\infty$ and finite part the single point $(1, v_{r-1}(\phi_{r-1}))$. Therefore, $S_{r-1}(\phi_{r-1})$ is a single point and $R_{r-1}(\phi_{r-1})(y) = c_1$, where c_1 is equal to (cf. Definition 2.20):

$$c_1 = \begin{cases} 1, & \text{if } r = 2, \\ (z_{r-2})^{-\ell_{r-2}v_{r-1}(\phi_{r-1})/e_{r-2}}, & \text{if } r > 2. \end{cases}$$

Denote $c := c_1^{e_{r-1}f_{r-1}}$. The polynomial $\varphi(y) := c(\psi_{r-1}(y) - y^{f_{r-1}})$ has degree less than f_{r-1}, and $\nu = \operatorname{ord}_y(\varphi) = 0$. Let $P(x)$ be the polynomial attached by Proposition 2.10 to $\varphi(y)$ and $V = e_{r-1}f_{r-1}v_r(\phi_{r-1})$. Since $\deg(P(x)) < m_r$, the polynomial $\phi_r(x) := \phi_{r-1}(x)^{e_{r-1}f_{r-1}} + P(x)$ is monic and it has degree m_r. Let T be the auxiliary side used in the construction of $P(x)$; we saw along the proof of Proposition 2.10 that $R_{r-1}(P)(y) = \varphi(y) = R_{r-1}(P,T)(y)$. By (19) (and (2) if $r = 2$), $S_{r-1}(P)$ has the same initial point as T and $R_{r-1}(\phi_r, T)(y) = R_{r-1}(\phi_r)(y)$. Also,

$$R_{r-1}(\phi_{r-1}^{e_{r-1}f_{r-1}}, T)(y) = y^{f_{r-1}} R_{r-1}(\phi_{r-1}^{e_{r-1}f_{r-1}})(y) = cy^{f_{r-1}}.$$

Finally, by Lemma 2.23 in order $r-1$ (cf. (3) in order one):

$$\begin{aligned}R_{r-1}(\phi_r, T)(y) &= R_{r-1}(\phi_{r-1}^{e_{r-1}f_{r-1}}, T)(y) + R_{r-1}(P,T)(y) \\ &= cy^{f_{r-1}} + \varphi(y) = c\psi_{r-1}(y),\end{aligned}$$

so that $R_{r-1}(\phi_r)(y) \sim \psi_{r-1}(y)$ and $\omega_r(\phi_r) = 1$. The polynomial $\phi_r(x)$ is irreducible over $\mathcal{O}[x]$ by the theorem of the product in order $r-1$. Finally, it has $v_r(\phi_r) = V$ because all points of $N_{r-1}(\phi_r)$ lie on T. □

Definition 2.12. A *representative* of the type $\mathbf{t}$ is a monic polynomial $\phi_r(x) \in \mathcal{O}[x]$ of type $\mathbf{t}$ such that $R_{r-1}(\phi_r)(y) \sim \psi_{r-1}(y)$. This object plays the analogous role in order $r-1$ to that of an irreducible polynomial modulo $\mathfrak{m}$ in order one.

From now on, we fix a representative $\phi_r(x)$ of $\mathbf{t}$, without necessarily assuming that it has been constructed by the method of Proposition 2.10.

2.4. **Certain rational functions.** We introduce in a recursive way several rational functions in $K(x)$. We let h_r, e_r be arbitrary coprime positive integers, and we fix $\ell_r, \ell'_r \in \mathbb{Z}$ such that $\ell_r h_r - \ell'_r e_r = 1$.

Definition 2.13. We define $\pi_0(x) = 1$, $\pi_1(x) = \pi$, and, for all $1 \le i \le r$,

$$\Phi_i(x) = \frac{\phi_i(x)}{\pi_{i-1}(x)^{f_{i-1}v_i(\phi_{i-1})}}, \qquad \gamma_i(x) = \frac{\Phi_i(x)^{e_i}}{\pi_i(x)^{h_i}}, \qquad \pi_{i+1}(x) = \frac{\Phi_i(x)^{\ell_i}}{\pi_i(x)^{\ell'_i}}.$$

Each of these rational functions can be written as $\pi^{n_0}\phi_1(x)^{n_1}\cdots\phi_r(x)^{n_r}$, for adequate integers $n_i \in \mathbb{Z}$. Also,

$$\Phi_i(x) = \cdots \phi_i(x), \quad \gamma_i(x) = \cdots \phi_i(x)^{e_i}, \quad \pi_{i+1}(x) = \cdots \phi_i(x)^{\ell_i}, \tag{17}$$

where the dots indicate a product of integral powers of π and $\phi_j(x)$, with $1 \le j < i$. We want to compute the value of v_r on all these functions.

Lemma 2.14. *For all $1 \le i < j \le r$, we have $\omega_j(\phi_i) = 0$.*

Proof. Since $N_i(\phi_i)$ is one-sided with slope $-\infty$, we have $\omega_{i+1}(\phi_i) = 0$ because $S_i(\phi_i)$ is a single point. By Lemma 2.2, $\omega_j(\phi_i) = 0$ for all $i < j \le r$. □

Proposition 2.15. *For all $1 \le i < r$ we have*

(1) $v_r(\phi_i) = \sum_{j=1}^{i} (e_{j+1}\cdots e_{r-1})\,(e_j f_j \cdots e_{i-1}f_{i-1})\,h_j$,
(2) $v_r(\Phi_i) = e_{i+1}\cdots e_{r-1}h_i$,
(3) $v_r(\pi_{i+1}) = e_{i+1}\cdots e_{r-1}$,
(4) $v_r(\gamma_i) = 0$,
(5) $\omega_r(\phi_i) = \omega_r(\Phi_i) = \omega_r(\gamma_i) = \omega_r(\pi_{i+1}) = 0$.

Moreover, $v_r(\phi_r) = \sum_{j=1}^{r-1} (e_{j+1}\cdots e_{r-1})\,(e_j f_j \cdots e_{r-1}f_{r-1})\,h_j$ and $v_r(\Phi_r) = 0$.

Proof. We proceed by induction on r. For $r = 2$ all formulas are easily deduced from $v_2(\phi_1) = h_1$, which was proved in Proposition 2.7. Suppose $r \ge 3$ and all statements true for $r - 1$.

Let us start with item (1). By Proposition 2.7 and (16),

$$v_r(\phi_{r-1}) = h_{r-1} + e_{r-1}v_{r-1}(\phi_{r-1}), \qquad v_{r-1}(\phi_{r-1}) = e_{r-2}f_{r-2}v_{r-1}(\phi_{r-2}).$$

Hence, the formula for $i = r - 1$ follows from the induction hypothesis. Suppose from now on that $i < r - 1$. By Lemma 2.14, $\phi_i(x) = \phi_i(x)$ is an admissible ϕ_{r-1}-adic development of $\phi_i(x)$, and by Lemma 2.25 in order $r - 1$ (Lemma 1.12 in order one) we get $N^-_{r-1}(\phi_i) = (0, v_{r-1}(\phi_i))$, so that $v_r(\phi_i) = e_{r-1}v_{r-1}(\phi_i)$ and the formula follows by induction.

Let us now prove items (2) and (3) by induction on i. For $i = 1$, item (1) shows that:

$$v_r(\Phi_1) = v_r(\phi_1) = e_2\cdots e_{r-1}h_1,$$
$$v_r(\pi_2) = \ell_1 v_r(\Phi_1) - \ell'_1 v_r(\pi) = (\ell_1 h_1 - \ell'_1 e_1)e_2\cdots e_{r-1} = e_2\cdots e_{r-1}.$$

Now suppose $i > 1$ and the formulas hold for $1, \dots, i - 1$. We have:

$$v_r(\Phi_i) = v_r(\phi_i) - f_{i-1}v_i(\phi_{i-1})e_{i-1}\cdots e_{r-1} = e_{i+1}\cdots e_{r-1}h_i,$$
$$v_r(\pi_{i+1}) = \ell_i v_r(\Phi_i) - \ell'_i v_r(\pi_i) = (\ell_i h_i - \ell'_i e_i)e_{i+1}\cdots e_{r-1} = e_{i+1}\cdots e_{r-1}.$$

Item (4) is easily deduced from the previous formulas, and item (5) is an immediate consequence of (17) and Lemma 2.14. The last statements follow from (16) and the previous formulas. □

Lemma 2.16. *For $\mathbf{n} = (n_0, \dots, n_{r-1}) \in \mathbb{Z}^r$, consider the rational function $\Phi(\mathbf{n}) = \pi^{n_0}\phi_1(x)^{n_1}\cdots\phi_{r-1}(x)^{n_{r-1}} \in K(x)$. Then, if $v_r(\Phi(\mathbf{n})) = 0$, there exists a unique sequence $i_1, \dots, i_{r-1}$ of integers such that $\Phi(\mathbf{n}) = \gamma_1(x)^{i_1}\cdots\gamma_{r-1}(x)^{i_{r-1}}$. Moreover, i_s depends only on $n_s, \dots, n_{r-1}$, for all $1 \le s < r$.*

Proof. Since the polynomials $\phi_s(x)$ are irreducible and pairwise different, we have $\Phi(\mathbf{n}) = \Phi(\mathbf{n}')$ if and only if $\mathbf{n} = \mathbf{n}'$. By (17), any product $\gamma_1(x)^{i_1}\cdots\gamma_{r-1}(x)^{i_{r-1}}$ can be expressed as $\Phi(\mathbf{j})$, for a suitable $\mathbf{j} = (j_0, \dots, j_{r-2}, e_{r-1}i_{r-1})$. Thus, if $\gamma_1(x)^{i_1}\cdots\gamma_{r-1}(x)^{i_{r-1}} = 1$ we have necessarily $i_{r-1} = 0$, and recursively, $i_1 = \cdots = i_{r-2} = 0$. This proves the uniqueness of the expression of any $\Phi(\mathbf{n})$ as a product of powers of gammas.

Let us prove the existence of such an expression by induction on $r \ge 1$. For $r = 1$, let $\mathbf{n} = (n_0)$; the condition $v_r(\pi^{n_0}) = 0$ implies that $n_0 = 0$ and $\Phi(\mathbf{n}) = 1$. Suppose $r \ge 2$ and that the lemma has been proven for all $\mathbf{n}' \in \mathbb{Z}^{r-1}$. By item (1) of Proposition 2.15, $v_r(\Phi(\mathbf{n})) \equiv n_{r-1}h_{r-1} \pmod{e_{r-1}}$; hence, if $v_r(\Phi(\mathbf{n})) = 0$ we have necessarily $n_{r-1} = e_{r-1}i_{r-1}$ for some integer i_{r-1} that depends only on n_{r-1}. By (17), $\gamma_{r-1}(x)^{i_{r-1}} = \Phi(\mathbf{j})$, for some $\mathbf{j} = (j_0, \dots, j_{r-2}, e_{r-1}i_{r-1})$; hence, $\Phi(\mathbf{n})\gamma_{r-1}(x)^{-i_{r-1}} = \Phi(\mathbf{n}')$, with $\mathbf{n}' = (n'_0, \dots, n'_{r-2}, 0)$, and each n'_s depends only on n_s and n_{r-1}. By item (4) of Proposition 2.15, we still have $v_r(\Phi(\mathbf{n}')) = 0$, and by induction hypothesis we get the desired expression of $\Phi(\mathbf{n})$ as a product of powers of gammas. □

2.5. **Newton polygon and residual polynomials of r-th order.** Let $f(x) \in \mathcal{O}[x]$ be a nonzero polynomial and consider its canonical ϕ_r-adic development

$$f(x) = \sum\nolimits_{0 \le i \le \lfloor \deg(f)/m_r \rfloor} a_i(x)\phi_r(x)^i, \quad \deg a_i(x) < m_r. \tag{18}$$

We define the Newton polygon $N_r(f)$ of $f(x)$, with respect to $\mathbf{t}$ and ϕ_r to be the lower convex envelope of the set of points (i, u_i), $u_i < \infty$, where

$$u_i := v_r\left(a_i(x)\phi_r(x)^i\right) = v_r(a_i(x)) + iv_r(\phi_r(x)).$$

This definition makes sense for $r = 1$, and $N_r(f)$ coincides with the Newton polygon of the first order. In fact, $v_1(a_i(x)\phi_1(x)^i) = v_1(a_i(x))$, because $v_1(\phi_1(x)) = 0$.

The principal part $N_r^-(f)$ is the principal polygon formed by all sides of negative slope, including the side of slope $-\infty$ if $f(x)$ is divisible by $\phi_r(x)$ in $\mathcal{O}[x]$. The typical shape of the polygon is shown in Figure 12.

Lemma 2.17. (1) $\min_{0 \le i \le n}\{u_i\} = v_r(f)$, *where* $n := \ell(N_r(f)) = \lfloor \deg f/m_r \rfloor$.
(2) *The length of $N_r^-(f)$ is $\omega_r(f)$.*
(3) *The side of slope $-\infty$ of $N_r^-(f)$ has length* $\operatorname{ord}_{\phi_r}(f)$.

Proof. The third item is obvious. Let us prove items (1), (2). Let $u := \min_{0 \le i \le n}\{u_i\}$ and consider the polynomial

$$g(x) := \sum_{u_i = u} a_i(x)\phi_r(x)^i.$$

All monomials of $g(x)$ have the same v_r-value and a different ω_r-value:

$$\omega_r(a_i(x)\phi_r(x)^i) = \omega_r(a_i(x)) + \omega_r(\phi_r(x)^i) = i$$

because $\omega_r(a_i) = 0$ by Lemma 2.2. By item (2) of Proposition 2.8, $v_r(g) = u$ and $\omega_r(g) = i_0$, the least abscissa with $u_{i_0} = u$. Since $v_r(f - g) > u$, we have $v_r(f) = v_r(g) = u$, and this proves item (1). On the other hand, item (1) of Proposition 2.8 shows that $\omega_r(f) = \omega_r(g) = i_0$, and this proves item (2). □

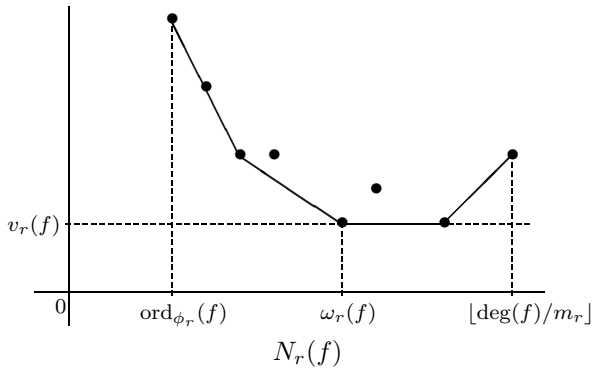


FIGURE 12

The following observation is a consequence of Lemmas 2.2 and 2.17.

Corollary 2.18. *If $f(x)$ has type* **t**, *then $N_r(f) = N_r^-(f)$.* □

From now on let $N = N_r^-(f)$. As we did in order one, we attach to any integer abscissa i of the finite part of N a *residual coefficient* $c_i \in \mathbb{F}_r$. The natural idea is to consider $c_i = R_{r-1}(a_i)(z_{r-1})$ for the points lying on N. However, this does not lead to the right concept of a residual polynomial attached to a side; it is necessary to twist these coefficients by certain powers of z_{r-1}.

Definition 2.19. For any nonzero $P(x) \in \mathcal{O}[x]$ and any index $1 \le j < r$, we denote by $s_j(P)$ the initial abscissa of $S_j(P)$.

For any nonzero $f(x) \in \mathcal{O}[x]$ with ϕ_r-adic development (18), we denote

$$t_{r-1}(i) := t_{r-1}(i, f) := \frac{s_{r-1}(a_i) - \ell_{r-1}u_i}{e_{r-1}}.$$

This number $t_{r-1}(i)$ is always an integer. In fact,

$$u_i = v_r(a_i) + iv_r(\phi_r) \equiv v_r(a_i) \equiv h_{r-1}s_{r-1}(a_i) \pmod{e_{r-1}},$$

the first congruence by (16), and the second congruence being a consequence of $v_r(a_i) = h_{r-1}s_{r-1}(a_i) + e_{r-1}u_{r-1}(a_i)$, where $u_{r-1}(a_i)$ is the ordinate of the initial point of $S_{r-1}(a_i)$. Hence, $\ell_{r-1}u_i \equiv s_{r-1}(a_i) \pmod{e_{r-1}}$.

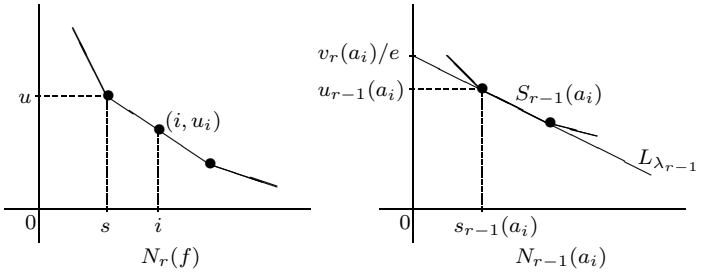


FIGURE 13

Definition 2.20. For any integer abscissa $\operatorname{ord}_{\phi_r}(f) \le i \le \omega_r(f)$, the *residual coefficient* c_i of $N := N_r^-(f)$ is defined to be:

$$c_i := c_i(f) := \begin{cases} 0, & \text{if } (i,u_i) \text{ lies above } N, \\ z_{r-1}^{t_{r-1}(i)} R_{r-1}(a_i)(z_{r-1}) \in \mathbb{F}_r, & \text{if } (i,u_i) \text{ lies on } N. \end{cases}$$

Note that $c_i \neq 0$ if (i,u_i) lies on N because $\omega_r(a_i) = 0$ and $\psi_{r-1}(y)$ is the minimal polynomial of z_{r-1} over $\mathbb{F}_{r-1}$.

Definition 2.21. Let $\lambda_r = -h_r/e_r$ be a negative rational number, with h_r, e_r positive coprime integers. Let $S = S_{\lambda_r}(N)$ be the λ_r-component of N, $d = d(S)$ the degree, and (s,u) the initial point of S.

We define the *virtual factor* of $f(x)$ attached to S (or to λ_r) to be the rational function

$$f^S(x) := \Phi_r(x)^{-s} \pi_r(x)^{-u} f^0(x) \in K(x), \quad f^0(x) := \sum\nolimits_{(i,u_i)\in S} a_i(x) \phi_r(x)^i,$$

where $\Phi_r(x)$, $\pi_r(x)$ are the rational functions introduced in Definition 2.13.

We define the *residual polynomial* attached to S (or to λ_r) to be the polynomial

$$R_{\lambda_r}(f)(y) := c_s + c_{s+e_r}\, y + \cdots + c_{s+(d-1)e_r}\, y^{d-1} + c_{s+de_r}\, y^d \in \mathbb{F}_r[y].$$

Only the points (i,u_i) that lie on S yield a nonzero coefficient of $R_{\lambda_r}(f)(y)$. In particular, c_s and c_{s+de} are always nonzero, so that $R_{\lambda_r}(f)(y)$ has degree d and it is never divisible by y. We emphasize that $R_{\lambda_r}(f)(y)$ does not depend only on λ_r; as for all other objects in section 2, it depends on the type $\mathbf{t}$ too.

We define in an analogous way the residual polynomial of $f(x)$ with respect to a side T that is not necessarily a λ_r-component of N. Let $T \in \mathcal{S}(\lambda_r)$ be an arbitrary side of slope λ_r, with abscissas $s_0 \le s_1$ for the end points. Let $d' = d(T)$. We say that $f(x)$ *lies on or above* T *in order* r if all points of N with abscissa $s_0 \le i \le s_1$ lie on or above T. In this case we define

$$R_{\lambda_r}(f,T)(y) := \tilde{c}_{s_0} + \tilde{c}_{s_0+e_r}\, y + \cdots + \tilde{c}_{s_0+(d'-1)e_r}\, y^{d'-1} + \tilde{c}_{s_0+d'e_r}\, y^{d'} \in \mathbb{F}_r[y],$$

where $\tilde{c}_i := \tilde{c}_i(f) := c_i$ if (i,u_i) lies on T and $\tilde{c}_i = 0$ otherwise.

Note that $\deg R_{\lambda_r}(f,T)(y) \le d'$ and equality holds if and only if the final point of T belongs to $S_{\lambda_r}(f)$. Usually, T will be an enlargement of $S_{\lambda_r}(f)$ and then

$$T \supseteq S_{\lambda_r}(f) \implies R_{\lambda_r}(f,T)(y) = y^{(s-s_0)/e_r} R_{\lambda_r}(f)(y), \tag{19}$$

where s is the abscissa of the initial point of $S_{\lambda_r}(f)$.

For technical reasons, we express c_i in terms of a residual polynomial attached to a certain auxiliary side.

Lemma 2.22. *Let $T \in \mathcal{PP}$ be a principal polygon. Let (i,y_i) be a point lying on T, with integer abscissa i. Let $V = y_i - iv_r(\phi_r)$ and let $L_{\lambda_{r-1}}$ be the line of slope λ_{r-1} that cuts the vertical axis at the point with ordinate V/e_{r-1}. Denote by $T(i)$ the greatest side contained in $L_{\lambda_{r-1}}$, whose end points have nonnegative integer coordinates, and let $\mathfrak{s}_i$ be the abscissa of the initial point of $T(i)$.*

Let $a(x) \in \mathcal{O}[x]$ be a nonzero polynomial such that $u_i := v_r(a\phi_r^i) \ge y_i$. Then,

$$y^{(\mathfrak{s}_i - \ell_{r-1}u_i)/e_{r-1}} R_{r-1}(a, T(i))(y) = y^{(s_{r-1}(a) - \ell_{r-1}u_i)/e_{r-1}} R_{r-1}(a)(y)$$

if $u_i = y_i$, whereas $R_{r-1}(a,T(i))(y) = 0$ if $u_i > y_i$.

In particular, for $T = N_r^-(f)$ *we get* $c_i = z_{r-1}^{(\mathfrak{s}_i - \ell_{r-1}u_i)/e_{r-1}} R_{r-1}(a_i, T(i))(z_{r-1})$.

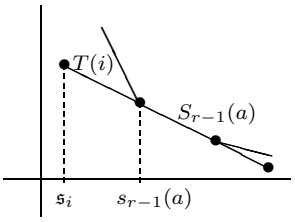


FIGURE 14

Proof. If $v_r(a\phi_r^i) = y_i$, we have $v_r(a) = V$ and $S_{r-1}(a) \subseteq T(i)$. Then, the lemma follows from (19) in order $r-1$. If $v_r(a\phi_r^i) > y_i$, then $S_{r-1}(a)$ lies above $T(i)$ and $R_{r-1}(a_i, T(i))(y) = 0$. See Figure 14. □

Lemma 2.23. *Let* $T \in \mathcal{S}(\lambda_r)$ *be a side of slope* λ_r *and let* $f(x), g(x) \in \mathcal{O}[x]$. *If* $f(x)$ *and* $g(x)$ *lie on or above* T *in order* r, *then* $(f+g)(x)$ *lies on or above* T *in order* r *and*

$$R_{\lambda_r}(f+g, T) = R_{\lambda_r}(f, T) + R_{\lambda_r}(g, T).$$

Proof. Let $s_0 \le s_1$ be the abscissas of the end points of T. We want to check that, for all integers $s_0 \le i \le s_1$,

$$\tilde{c}_i(f+g) = \tilde{c}_i(f) + \tilde{c}_i(g). \tag{20}$$

Let $a_i(x)$, $b_i(x)$, be the respective i-th coefficients of the ϕ_r-adic development of $f(x)$, $g(x)$; then, $a_i(x) + b_i(x)$ is the i-th coefficient of the ϕ_r-adic development of $f(x) + g(x)$. By Lemma 2.22 applied to the point $(i, y_i(T))$ of T,

$$\tilde{c}_i(f) = z_{r-1}^{(\mathfrak{s}_i - \ell_{r-1}u_i)/e_{r-1}} R_{r-1}(a_i, T(i))(z_{r-1}).$$

Analogous equalities hold for $g(x)$ and $(f+g)(x)$, and (20) follows from Lemma 2.23 itself, in order $r-1$ (cf. (3) for $r = 2$). □

2.6. **Admissible ϕ_r-developments and theorem of the product in order r.** Consider an arbitrary ϕ_r-development of $f(x)$, not necessarily the ϕ_r-adic one:

$$f(x) = \sum\nolimits_{i \ge 0} a_i'(x)\phi_r(x)^i, \quad a_i'(x) \in \mathcal{O}[x]. \tag{21}$$

Let N' be the principal polygon of the set of points (i, u_i'), with $u_i' = v_r(a_i'(x)\phi_r(x)^i)$. Let i_0 be the first abscissa with $a_{i_0}'(x) \ne 0$. As we did in order one, to each integer abscissa $i_0 \le i \le \ell(N')$ we attach a residual coefficient

$$c_i' = \begin{cases} 0, & \text{if } (i, u_i') \text{ lies above } N', \\ z_{r-1}^{t_{r-1}'(i)} R_{r-1}(a_i')(z_{r-1}) \in \mathbb{F}_r, & \text{if } (i, u_i') \text{ lies on } N', \end{cases}$$

where $t_{r-1}'(i) = (s_{r-1}(a_i') - \ell_{r-1}u_i')/e_{r-1}$. For the points (i, u_i') lying on N' we may now have $c_i' = 0$; for instance in the case $a_0'(x) = f(x)$ the Newton polygon has only one point $(0, v_r(f))$ and $c_0' = 0$ if $\omega_r(f) > 0$.

Finally, for any negative rational number $\lambda_r = -h_r/e_r$, with h_r, e_r positive coprime integers, we define the residual polynomial attached to the λ_r-component $S' = S_{\lambda_r}(N')$ to be

$$R'_{\lambda_r}(f)(y) := c'_{s'} + c'_{s'+e_r}\, y + \cdots + c'_{s'+(d'-1)e_r}\, y^{d'-1} + c'_{s'+d'e_r}\, y^{d'} \in \mathbb{F}_r[y],$$

where $d' = d(S')$ and s' is the initial abscissa of S'.

Definition 2.24. We say that the ϕ_r-development (21) is admissible if $c'_i \neq 0$ (or equivalently, $\omega_r(a'_i) = 0$) for each abscissa i of a vertex of N'.

Lemma 2.25. *If a ϕ_r-development is admissible, then $N' = N_r^-(f)$ and $c'_i = c_i$ for all abscissas i of the finite part of N'. In particular, for any negative rational number λ_r we have $R'_{\lambda_r}(f)(y) = R_{\lambda_r}(f)(y)$.*

Proof. Consider the ϕ_r-adic developments of $f(x)$ and each $a'_i(x)$:

$$f(x) = \sum\nolimits_{0\le i} a_i(x)\phi_r(x)^i, \qquad a'_i(x) = \sum\nolimits_{0\le k} b_{i,k}(x)\phi_r(x)^k.$$

By the uniqueness of the ϕ_r-adic development we have

$$a_i(x) = \sum\nolimits_{0\le k\le i} b_{i-k,k}(x). \tag{22}$$

Let us denote $w_{i,k} := v_r(b_{i,k})$, $w := v_r(\phi_r)$. By item (1) of Lemma 2.17, $u'_i = v_r(a'_i) + iw = \min_{0\le k}\{w_{i,k} + (k+i)w\}$. Hence, for all $0 \le k$ and all $0 \le i \le \ell(N')$:

$$w_{i,k} + (k+i)w \ge u'_i \ge y_i(N'). \tag{23}$$

Therefore, by (22) and (23), all points (i, u_i) lie on or above N'; in fact,

$$\begin{aligned} u_i = v_r(a_i) + iw \ge \min_{0\le k\le i}\{w_{i-k,k} + iw\} &= w_{i-k_0,k_0} + iw \\ &\ge u'_{i-k_0} \ge y_{i-k_0}(N') \ge y_i(N') \end{aligned} \tag{24}$$

for some $0 \le k_0 \le i$. On the other hand, for any abscissa i of the finite part of N' and for any $0 < k \le i$ we have by (23)

$$w_{i-k,k} \ge u'_{i-k} - iw \ge y_{i-k}(N') - iw > y_i(N') - iw. \tag{25}$$

The following claim ends the proof of the lemma:

Claim. Let i be an abscissa of the finite part of N' such that $(i, u'_i) \in N'$. Then, $u_i = u'_i$ if and only if $c'_i \neq 0$, and in this case, $c'_i = c_i$.

In fact, suppose $c'_i \neq 0$, or equivalently, $\omega_r(a'_i) = 0$. We decompose

$$a'_i(x) = b_{i,0}(x) + B(x), \quad B(x) = \sum_{0<k} b_{i,k}(x)\phi_r(x)^k.$$

Note that $\omega_r(B) > 0$ because $\phi_r(x)|B(x)$. By (23), $v_r(b_{i,0}) = w_{i,0} \ge u'_i - iw = v_r(a'_i)$. Since $\omega_r(a'_i) = 0$ and $\omega_r(B) > 0$, item (1) of Proposition 2.8 shows that $v_r(b_{i,0}) = \min\{v_r(a'_i), v_r(B)\}$; hence, $v_r(b_{i,0}) = v_r(a'_i)$. By (22) and (25) we have $u_i - iw = v_r(a_i) = w_{i,0} = u'_i - iw$, so that $u_i = u'_i$. Let $T(i)$ be the side attached to the point $(i, u'_i) \in N'$ in Lemma 2.22. Since $R_{r-1}(B)(z_{r-1}) = 0$, (19)

shows that $R_{r-1}(B,T(i))(z_{r-1})=0$. By Lemma 2.23, $R_{r-1}(a_i',T(i))(z_{r-1})=R_{r-1}(b_{i,0},T(i))(z_{r-1})$, and Lemma 2.22 shows that

$$\begin{aligned}c_i'&=(z_{r-1})^{(\mathfrak{s}_i-\ell_{r-1}u_i)/e_{r-1}}R_{r-1}(a_i',T(i))(z_{r-1})\\&=(z_{r-1})^{(\mathfrak{s}_i-\ell_{r-1}u_i)/e_{r-1}}R_{r-1}(b_{i,0},T(i))(z_{r-1})\\&=(z_{r-1})^{(s_{r-1}(b_{i,0})-\ell_{r-1}u_i)/e_{r-1}}R_{r-1}(b_{i,0})(z_{r-1})\\&=(z_{r-1})^{(s_{r-1}(a_i)-\ell_{r-1}u_i)/e_{r-1}}R_{r-1}(a_i)(z_{r-1})=c_i,\end{aligned}$$

the next to the last equality because $S_{r-1}(a_i)=S_{r-1}(b_{i,0})$, $R_{r-1}(a_i)=R_{r-1}(b_{i,0})$, by (25) and Proposition 2.8.

Conversely, if $u_i=u_i'=y_i(N')$, we have necessarily $k_0=0$ in (24) and all inequalities of (24) are equalities. Hence, $w_{i,0}+iw=u_i'$, or equivalently, $v_r(a_i')=v_r(b_{i,0})$. Since $\omega_r(b_{i,0})=0$ and $\omega_r(B)>0$, Proposition 2.8 shows that $\omega_r(a_i')=0$. This ends the proof of the claim. □

Theorem 2.26 (Theorem of the product in order r)**.** *For any nonzero $f(x),g(x)\in\mathcal{O}[x]$ and any negative rational number λ_r we have*

$$N_r^-(fg)=N_r^-(f)+N_r^-(g),\qquad R_{\lambda_r}(fg)(y)=R_{\lambda_r}(f)(y)R_{\lambda_r}(g)(y).$$

Proof. Consider the respective ϕ_r-adic developments

$$f(x)=\sum_{0\le i}a_i(x)\phi_r(x)^i,\quad g(x)=\sum_{0\le j}b_j(x)\phi_r(x)^j,$$

and denote $u_i=v_r(a_i\phi_r^i)$, $v_j=v_r(b_j\phi_r^j)$, $N_f=N_r^-(f)$, $N_g=N_r^-(g)$. Take

$$f(x)g(x)=\sum_{0\le k}A_k(x)\phi_r(x)^k,\qquad A_k(x)=\sum_{i+j=k}a_i(x)b_j(x),\tag{26}$$

and denote by N' the principal part of the Newton polygon of order r of fg, determined by this ϕ_r-development.

We shall show that $N'=N_f+N_g$, that this ϕ_r-development is admissible, and that $R'_{\lambda_r}(fg)=R_{\lambda_r}(f)R_{\lambda_r}(g)$ for all negative λ_r. The theorem will then be a consequence of Lemma 2.25.

Let $w_k:=v_r(A_k\phi_r^k)$ for all $0\le k$. Lemma 1.4 shows that the point $(i,u_i)+(j,v_j)$ lies on or above N_f+N_g for all $i,j\ge0$. Since $w_k\ge\min_{i+j=k}\{u_i+v_j\}$, the points (k,w_k) all lie on or above N_f+N_g too. On the other hand, let $P_k=(k,y)$ be a vertex of N_f+N_g; then, P_k is the end point of $S_1+\cdots+S_r+T_1+\cdots+T_s$, for certain sides S_i of N_f and T_j of N_g, ordered by increasing slopes among all sides of N_f and N_g. By Lemma 1.4, for all pairs (i,j) with $i+j=k$, the point $(i,u_i)+(j,v_j)$ lies above N_f+N_g except for the pair $i_0=\ell(S_{r-1}+\cdots+S_r)$, $j_0=\ell(T_{r-1}+\cdots+T_s)$, which satisfies $(i_0,u_{i_0})+(j_0,v_{j_0})=P_k$. Thus, $(k,w_k)=P_k$. This shows that $N'=N_f+N_g$.

Moreover, for all $(i,j)\ne(i_0,j_0)$ we have

$$v_r(A_k\phi_r^k)=v_r(a_{i_0}b_{j_0}\phi_r^k)<v_r(a_ib_j\phi_r^k),$$

so that $v_r(A_k)=v_r(a_{i_0}b_{j_0})<v_r(a_ib_j)$. By Proposition 2.8, $\omega_r(A_k)=\omega_r(a_{i_0}b_{j_0})=\omega_r(a_{i_0})+\omega_r(b_{j_0})=0$, and the ϕ_r-development (26) is admissible.

Finally, by (1), the λ_r-components $S'=S_{\lambda_r}(N')$, $S_f=S_{\lambda_r}(N_f)$, $S_g=S_{\lambda_r}(N_g)$ are related by $S'=S_f+S_g$. Let $(k,y_k(N'))$ be a point with integer coordinates lying on S' (not necessarily a vertex), and let $T(k)$ be the corresponding side of slope λ_{r-1} given in Lemma 2.22, with starting abscissa $\mathfrak{s}_k$. Denote by I the set of

the pairs (i,j) such that (i,u_i) lies on S_f, (j,v_j) lies on S_g, and $i+j=k$. Take $P(x)=\sum_{(i,j)\in I}a_i(x)b_j(x)$. By Lemma 1.4, for all other pairs (i,j) with $i+j=k$, the point $(i,u_i)+(j,v_j)$ lies above N'. By Lemma 2.23,

$$R_{r-1}(A_k,T(k))=R_{r-1}(P,T(k))=\sum\nolimits_{(i,j)\in I}R_{r-1}(a_ib_j,T(k)).$$

Lemma 2.22, (19) and the theorem of the product in order $r-1$ show that

$$\begin{aligned}c'_k(fg)&=(z_{r-1})^{\frac{s_k-\ell_{r-1}w_k}{e_{r-1}}}R_{r-1}(A_k,T(k))(z_{r-1})\\&=(z_{r-1})^{\frac{s_k-\ell_{r-1}w_k}{e_{r-1}}}\sum\nolimits_{(i,j)\in I}R_{r-1}(a_ib_j,T(k))(z_{r-1})\\&=\sum\nolimits_{(i,j)\in I}(z_{r-1})^{\frac{s_{r-1}(a_ib_j)-\ell_{r-1}w_k}{e_{r-1}}}R_{r-1}(a_ib_j)(z_{r-1})\\&=\sum\nolimits_{(i,j)\in I}(z_{r-1})^{t_{r-1}(i,f)+t_{r-1}(j,g)}R_{r-1}(a_i)(z_{r-1})R_{r-1}(b_j)(z_{r-1})\\&=\sum\nolimits_{(i,j)\in I}c_i(f)c_j(g).\end{aligned}$$

This shows that the residual polynomial attached to S' with respect to the ϕ_r-development (26) is equal to $R_{\lambda_r}(f)R_{\lambda_r}(g)$. □

Corollary 2.27. *Let $f(x)\in\mathcal{O}[x]$ be a monic polynomial with $\omega_r(f)>0$, and let $f_{\mathbf{t}}(x)$ be the monic factor of $f(x)$ determined by $\mathbf{t}$ (cf. Definition 2.3). Then $N_r(f_{\mathbf{t}})$ is equal to $N_r^-(f)$ up to a vertical shift, and $R_{\lambda_r}(f)\sim R_{\lambda_r}(f_{\mathbf{t}})$ for any negative rational number λ_r.*

Proof. Let $f(x)=f_{\mathbf{t}}(x)g(x)$. By (13), $\omega_r(g)=0$. By the theorem of the product, $N_r^-(f)=N_r^-(f_{\mathbf{t}})+N_r^-(g)$ and $R_{\lambda_r}(f)=R_{\lambda_r}(f_{\mathbf{t}})R_{\lambda_r}(g)$. Since $N_r^-(g)$ is a single point with abscissa 0 (cf. Lemma 2.17), the polygon $N_r^-(f)$ is a vertical shift of $N_r^-(f_{\mathbf{t}})$ and $R_{\lambda_r}(g)$ is a constant. □

3. Dissections in order r

In this section we extend to order r the theorems of the polygon and of the residual polynomial. We fix throughout a type $\mathbf{t}$ of order $r-1$ and a representative $\phi_r(x)$ of $\mathbf{t}$. We proceed by induction and we assume that all results of this section have been proved already in orders $1,\dots,r-1$. The case $r=1$ was considered in section 1.

3.1. Theorem of the polygon in order r.

Let $f(x)\in\mathcal{O}[x]$ be a monic polynomial such that $\omega_r(f)>0$. The aim of this section is to obtain a factorization of $f_{\mathbf{t}}(x)$ and certain arithmetic data of the factors. Thanks to Corollary 2.27, we shall be able to read this information directly on $N_r^-(f)$ and the different residual polynomials $R_{\lambda_r}(f)(y)$.

Theorem 3.1 (Theorem of the polygon in order r)**.** *Let $f(x)\in\mathcal{O}[x]$ be a monic polynomial such that $\omega_r(f)>0$. Suppose that $N_r^-(f)=S_1+\cdots+S_g$ has g sides with slopes $-\infty\le\lambda_{r,1}<\cdots<\lambda_{r,g}$. Then, $f_{\mathbf{t}}(x)$ admits a factorization*

$$f_{\mathbf{t}}(x)=F_1(x)\cdots F_g(x),$$

as a product of g monic polynomials of $\mathcal{O}[x]$ satisfying the following properties:

(1) *$N_r(F_i)$ is equal to S_i up to a translation.*
(2) *If S_i has finite slope, then $R_{\lambda_{r,i}}(F_i)(y) \sim R_{\lambda_{r,i}}(f)(y)$.*
(3) *For any root $\theta \in \overline{\mathbb{Q}}_p$ of $F_i(x)$, $v(\phi_r(\theta)) = (v_r(\phi_r) + |\lambda_{r,i}|)/e_1 \cdots e_{r-1}$.*

Proof. Let us denote $e = e_1 \cdots e_{r-1}$. We deal first with the case that $f_{\mathbf{t}}(x)$ is irreducible. In this case, $\rho := v(\phi_r(\theta))$ is constant among all roots $\theta \in \overline{\mathbb{Q}}_p$ of $f_{\mathbf{t}}(x)$, and $\rho > 0$, because ϕ_r is congruent to a power of ϕ_1 modulo $\mathfrak{m}$ (cf. Definition 2.1). We have $\rho = \infty$ if and only if $f_{\mathbf{t}}(x) = \phi_r(x)$, and in this case the theorem is clear. Suppose ρ is finite. Lemma 2.2 shows that $\deg f_{\mathbf{t}} = m_r\omega_r(f) > 0$, and we have $N_r(f_{\mathbf{t}}) = N_r^-(f_{\mathbf{t}})$, by Corollary 2.18.

Let $P(x) = \sum_{0\le i\le k} b_i x^i \in \mathcal{O}[x]$ be the minimal polynomial of $\phi_r(\theta)$, and let $Q(x) = P(\phi_r(x)) = \sum_{0\le i\le k} b_i\phi_r(x)^i$. By the theorem of the polygon in order one, the x-polygon of P has only one side and it has slope $-\rho$. The end points of $N_r(Q)$ are $(0, ek\rho)$ and $(k, kv_r(\phi_r))$. Now, for all $0 \le i < k$,

$$\frac{v_r(b_i\phi_r^i) - kv_r(\phi_r)}{k-i} = \frac{ev(b_i) + iv_r(\phi_r) - kv_r(\phi_r)}{k-i} \ge e\rho - v_r(\phi_r).$$

This implies that $N_r(Q)$ has only one side and it has slope $\lambda_r := -(e\rho - v_r(\phi_r))$. Since $Q(\theta) = 0$, $f_{\mathbf{t}}(x)$ divides $Q(x)$ and the theorem of the product shows that $N_r(f_{\mathbf{t}})$ is one-sided with the same slope. By Corollary 2.27, $N_r^-(f)$ is one-sided with the same slope and $R_{\lambda_r}(f_{\mathbf{t}}) \sim R_{\lambda_r}(f)$. This ends the proof of the theorem when $f_{\mathbf{t}}(x)$ is irreducible.

If $f_{\mathbf{t}}(x)$ is reducible, we consider its decomposition $f_{\mathbf{t}}(x) = \prod_j P_j(x)$ into a product of monic irreducible factors in $\mathcal{O}[x]$. By Lemma 2.4, each $P_j(x)$ is of type $\mathbf{t}$ and by the proof in the irreducible case, each $P_j(x)$ has a one-sided $N_r(P_j)$. The theorem of the product shows that the slope of $N_r(P_j)$ is $\lambda_{r,i}$ for some $1 \le i \le s$. If we group these factors according to the slope, we get the desired factorization. By the theorem of the product, $R_{\lambda_{r,i}}(F_i) \sim R_{\lambda_{r,i}}(f_{\mathbf{t}})$, because $R_{\lambda_{r,i}}(F_j)$ is a constant for all $j \ne i$. Finally, $R_{\lambda_{r,i}}(f_{\mathbf{t}}) \sim R_{\lambda_{r,i}}(f)$ by Corollary 2.27. The statement about $v(\phi_r(\theta))$ is obvious because $P_j(\theta) = 0$ for some j, and we have already proved the formula for an irreducible polynomial. □

We recall that if S_1 has slope $-\infty$, the corresponding factor is necessarily $F_1(x) = \phi_r(x)^{\mathrm{ord}_{\phi_r}(f)}$ (cf. Lemma 2.17).

Let $\lambda_r = -h_r/e_r$, with h_r, e_r positive coprime integers, be a negative rational number such that $S := S_{\lambda_r}(f)$ has positive length. Let $f_{\mathbf{t},\lambda_r}(x)$ be the factor of $f(x)$, corresponding to the side S by the theorem of the polygon. Choose a root $\theta \in \overline{\mathbb{Q}}_p$ of $f_{\mathbf{t},\lambda_r}(x)$, and let $L = K(\theta)$. By item (4) of Propositions 1.17 and 3.5, in orders $1, \dots, r-1$, there is a well-defined embedding $\mathbb{F}_r \longrightarrow \mathbb{F}_L$, determined by

$$\mathbb{F}_r \hookrightarrow \mathbb{F}_L,\ z_0 \mapsto \overline{\theta},\ z_1 \mapsto \overline{\gamma_1(\theta)},\ \dots,\ z_{r-1} \mapsto \overline{\gamma_{r-1}(\theta)}. \tag{27}$$

This embedding depends on the choice of θ. After this identification of $\mathbb{F}_r$ with a subfield of $\mathbb{F}_L$ we can think that all residual polynomials of r-th order have coefficients in $\mathbb{F}_L$.

Corollary 3.2. *For the rational functions of Definition* 2.13*:*

(1) $v(\phi_r(\theta)) = \sum_{i=1}^r e_i f_i \cdots e_{r-1} f_{r-1} h_i/(e_1 \cdots e_i)$,
(2) $v(\pi_r(\theta)) = 1/(e_1 \cdots e_{r-1})$,

(3) $v(\Phi_r(\theta)) = h_r/(e_1 \cdots e_r)$,
(4) $v(\gamma_r(\theta)) = 0$.

Proof. Item (1) is a consequence of the theorem of the polygon and the formula for $v_r(\phi_r)$ in Proposition 2.15. Item (2) follows from Proposition 2.9, because $v_r(\pi_r) = 1$, $\omega_r(\pi_r) = 0$ by Proposition 2.15. Item (3) follows from the theorem of the polygon and item (2) in order $r-1$. Item (4) follows from items (2), (3). □

Corollary 3.3. *The residual degree $f(L/K)$ is divisible by $f_0 \cdots f_{r-1}$, and the ramification index $e(L/K)$ is divisible by $e_1 \cdots e_r$. Moreover, the number of irreducible factors of $f_{\mathbf{t},\lambda_r}(x)$ is at most $d(S)$; in particular, if $d(S) = 1$ the polynomial $f_{\mathbf{t},\lambda_r}(x)$ is irreducible in $\mathcal{O}[x]$, and $f(L/K) = f_0 \cdots f_{r-1}$, $e(L/K) = e_1 \cdots e_r$.*

Proof. The statement on the residual degree is a consequence of the embedding (27). Denote $e_L = e(L/K)$, $e = e_1 \cdots e_{r-1}$, $f = f_0 \cdots f_{r-1}$. By the same result in order $r-1$ (cf. Corollary 1.16 for $r = 2$), e_L is divisible by e. Now, by the theorem of the polygon, $v_L(\phi_r(\theta)) = (e_L/e)v_r(\phi_r) + (e_L/e)(h_r/e_r)$. Since this is an integer and h_r, e_r are coprime, necessarily e_r divides e_L/e.

The upper bound for the number of irreducible factors is a consequence of the theorem of the product. Finally, if $d(S) = 1$, we have $efe_r = \deg(f_{\mathbf{t},\lambda_r}) = f(L/K)e(L/K)$, and necessarily $f(L/K) = f$ and $e(L/K) = ee_r$. □

We now prove an identity that plays an essential role in what follows.

Lemma 3.4. *Let $P(x) = \sum_{0\le i} a_i(x)\phi_r(x)^i$ be the ϕ_r-adic development of a nonzero polynomial in $\mathcal{O}[x]$. Let $\lambda_r = -h_r/e_r$ be a negative rational number, with h_r, e_r coprime positive integers. Let $S = S_{\lambda_r}(P)$ be the λ_r-component of $N_r^-(P)$, (s,u) the initial point of S, and (i,u_i) any point lying on S. Let $(s(a_i),u(a_i))$ be the initial point of the side $S_{r-1}(a_i)$. Then, the following identity holds in $K(x)$:*

$$\phi_r(x)^i \frac{\Phi_{r-1}(x)^{s(a_i)}\pi_{r-1}(x)^{u(a_i)}}{\Phi_r(x)^s\pi_r(x)^u} = \gamma_{r-1}(x)^{t_{r-1}(i)}\gamma_r(x)^{\frac{i-s}{e_r}}. \tag{28}$$

Proof. If we substitute $u = u_i + (i-s)\frac{h_r}{e_r}$ and $\gamma_r = \Phi_r^{e_r}/\pi_r^{h_r}$ in (28), we see that the identity is equivalent to

$$\phi_r(x)^i \frac{\Phi_{r-1}(x)^{s(a_i)}\pi_{r-1}(x)^{u(a_i)}}{\pi_r(x)^{u_i}} = \gamma_{r-1}(x)^{t_{r-1}(i)}\Phi_r(x)^i.$$

If we now substitute Φ_r, π_r and γ_{r-1} by their defining values and we use $e_{r-1}t_{r-1}(i) = s(a_i) - \ell_{r-1}u_i$, we get an equation involving only π_{r-1}, which is equivalent to

$$u(a_i) + \ell'_{r-1}u_i + h_{r-1}t_{r-1}(i) + if_{r-1}v_r(\phi_{r-1}) = 0.$$

This equality is easy to check by using $e_{r-1}u(a_i) + s(a_i)h_{r-1} = v_r(a_i) = u_i - iv_r(\phi_r)$, $v_r(\phi_r) = e_{r-1}f_{r-1}v_r(\phi_{r-1})$, and $\ell_{r-1}h_{r-1} - \ell'_{r-1}e_{r-1} = 1$. □

Proposition 3.5 (Computation of $v(P(\theta))$)**.** *We keep the notation above for $f(x)$, $\lambda_r = -h_r/e_r$, θ, L, and the embedding (27). Let $P(x) \in \mathcal{O}[x]$ be a nonzero polynomial, $S = S_{\lambda_r}(P)$, L_{λ_r} be the line of slope λ_r that contains S, and H be the ordinate at the origin of this line. Denote $e = e_1 \cdots e_{r-1}$. Then:*

(1) $v(P^S(\theta)) \ge 0$, $\quad \overline{P^S(\theta)} = R_{\lambda_r}(P)(\overline{\gamma_r(\theta)})$.
(2) $v(P(\theta) - P^0(\theta)) > H/e$.
(3) $v(P(\theta)) \ge H/e$, *and equality holds if and only if* $R_{\lambda_r}(P)(\overline{\gamma_r(\theta)}) \ne 0$.
(4) $R_{\lambda_r}(f)(\overline{\gamma_r(\theta)}) = 0$.

(5) *If* $R_{\lambda_r}(f)(y) \sim \psi_r(y)^a$ *for some irreducible polynomial* $\psi_r(y) \in \mathbb{F}_r[y]$, *then* $v(P(\theta)) = H/e$ *if and only if* $\psi_r(y) \nmid R_{\lambda_r}(P)(y)$ *in* $\mathbb{F}_r[y]$.

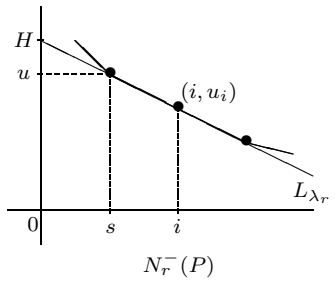


FIGURE 15

Proof. Let $P(x) = \sum_{0\le i} a_i(x)\phi_r(x)^i$ be the ϕ_r-adic development of $P(x)$, and denote $u_i = v_r(a_i\phi_r^i)$, $N = N_r^-(P)$. Recall that

$$P^S(x) = \Phi_r(x)^{-s}\pi_r(x)^{-u}P^0(x), \quad P^0(x) = \sum\nolimits_{(i,u_i)\in S} a_i(x)\phi_r(x)^i,$$

where (s,u) are the coordinates of the initial point of S. By Corollary 3.2,

$$v(\Phi_r(\theta)^s\pi_r(\theta)^u) = \frac{1}{e}\left(s\frac{h_r}{e_r} + u\right) = \frac{H}{e}. \tag{29}$$

On the other hand, by the theorem of the polygon and Proposition 2.9:

$$v(a_i(\theta)\phi_r(\theta)^i) = \frac{v_r(a_i)}{e} + \frac{i}{e}\left(v_r(\phi_r) + \frac{h_r}{e_r}\right) = \frac{1}{e}\left(u_i + i\frac{h_r}{e_r}\right) \ge \frac{H}{e}, \tag{30}$$

for all i, with equality if and only if $(i,u_i) \in S$. This proves item (2).

Also, (29) and (30) show that $v(P^S(\theta)) \ge 0$, so that $P^S(\theta)$ belongs to $\mathcal{O}_L$. Denote for simplicity $z_r = \overline{\gamma_r(\theta)}$. In order to prove the equality $\overline{P^S(\theta)} = R_{\lambda_r}(P)(z_r)$, we need to show that for every $(i,u_i) \in S$:

$$\operatorname{red}_L\left(\frac{a_i(\theta)\phi_r(\theta)^i}{\Phi_r(\theta)^s\pi_r(\theta)^u}\right) = (z_{r-1})^{t_{r-1}(i)}R_{r-1}(a_i)(z_{r-1})(z_r)^{(i-s)/e_r}. \tag{31}$$

Let $(s(a_i), u(a_i))$ be the initial point of $S_{r-1}(a_i)$. By items (1), (2) of the proposition in order $r-1$ (Proposition 1.17 if $r=2$), applied to the polynomial $a_i(x)$,

$$\overline{(a_i)^{S_{r-1}(a_i)}(\theta)} = R_{r-1}(a_i)(z_{r-1}),$$
$$a_i(\theta) \equiv \Phi_{r-1}(\theta)^{s(a_i)}\pi_{r-1}(\theta)^{u(a_i)}(a_i)^{S_{r-1}(a_i)}(\theta) \pmod{\mathfrak{m}_L^{(v_r(a_i)e(L/K)/e)+1}}.$$

Since $v_r(a_i)e(L/K)/e = v_L(a_i(\theta))$, it suffices to check the following identity in L:

$$\phi_r(\theta)^i\frac{\Phi_{r-1}(\theta)^{s(a_i)}\pi_{r-1}(\theta)^{u(a_i)}}{\Phi_r(\theta)^s\pi_r(\theta)^u} = \gamma_{r-1}(\theta)^{t_{r-1}(i)}\gamma_r(\theta)^{\frac{i-s}{e_r}},$$

which is a consequence of Lemma 3.4. This ends the proof of item (1).

Also, (30) shows that $v(P(\theta)) \ge H/e$, and

$$v(P(\theta)) = H/e \iff v(P^0(\theta)) = H/e \overset{(29)}{\iff} v(P^S(\theta)) = 0 \iff R_{\lambda_r}(P)(z_r) \ne 0,$$

the last equivalence by item (1). This proves item (3). The last two items are proved by similar arguments to that of the proof of Proposition 1.17. □

3.2. **Theorem of the residual polynomial in order r.** We now discuss how Newton polygons and residual polynomials are affected by an extension of the base field by an unramified extension. We keep the notation above for $f(x)$, $\lambda_r = -h_r/e_r$, θ, L and the embedding (27).

Proposition 3.6. *Let K' be the unramified extension of K of degree $f_0 \cdots f_{r-1}$. We identify $\mathbb{F}_r = \mathbb{F}_{K'}$ through the embedding (27). Let $G(x) \in \mathcal{O}_{K'}[x]$ be the minimal polynomial of θ over K'. Then, there exist a type of order $r-1$ over K', $\mathbf{t}' = (\phi_1'(x); \lambda_1, \phi_2'(x); \cdots; \lambda_{r-1}, \psi_{r-1}'(y))$, anda representative $\phi_r'(x)$ of $\mathbf{t}'$, with the following properties (where the superscript $'$ indicates that the objects are taken with respect to $\mathbf{t}'$):*

(1) $f_0' = \cdots = f_{r-1}' = 1$.
(2) *$G(x)$ is of type $\mathbf{t}'$.*
(3) *For any nonzero polynomial $P(x) \in \mathcal{O}[x]$,*

$$(N')_r^-(P) = N_r^-(P), \quad R'_{\lambda_r}(P)(y) = \sigma_r^s \tau_r^u R_{\lambda_r}(P)(\mu_r y),$$

where (s,u) is the initial point of $S_{\lambda_r}(P)$ and σ_r, τ_r, $\mu_r \in \mathbb{F}_{K'}^*$ are constants that depend only on $\mathbf{t}$ and θ.

Proof. We proceed by induction on r. The case $r = 1$ is considered in Lemma 1.18; for the constant ϵ defined there, we can take $\sigma_1 = \epsilon$, $\tau_1 = 1$, and $\mu_1 = \epsilon^{e_1}$. Let $r \geq 2$ and suppose we have already constructed $\mathbf{t}'_{r-2}$ and a representative $\phi'_{r-1}(x)$ satisfying these properties. Let $\eta_1, \ldots, \eta_{f_{r-1}} \in \mathbb{F}_{K'}$ be the roots of $\psi_{r-1}(y)$, and denote $F(x) = f_{\mathbf{t},\lambda_r}(x)$. We have

$$R'_{r-1}(\phi_r)(y) \sim R_{r-1}(\phi_r)(\mu_{r-1}y) \sim \psi_{r-1}(\mu_{r-1}y) = \textstyle\prod_{i=1}^{f_{r-1}}(\mu_{r-1}y - \eta_i),$$
$$R'_{r-1}(F)(y) \sim R_{r-1}(F)(\mu_{r-1}y) \sim \psi_{r-1}(\mu_{r-1}y)^{a_{r-1}} = \textstyle\prod_{i=1}^{f_{r-1}}(\mu_{r-1}y - \eta_i)^{a_{r-1}}.$$

Since $G(x)$ is of type $\mathbf{t}'_{r-2}$, Lemma 2.2 shows that $\deg G = m'_{r-1}\omega'_{r-1}(G)$. Since $(N')_{r-1}^-(F) = N_{r-1}^-(F)$, the theorem of the product shows that $(N')_{r-1}^-(G)$ is one-sided, with slope λ_{r-1} and positive length $\omega'_{r-1}(G)$. By the theorem of the residual polynomial, $R'_{r-1}(G)(y) \sim (\mu_{r-1}y - \eta)^a$, for some root $\eta \in \mathbb{F}_{K'}$ of $\psi_{r-1}(y)$ and some positive integer a. We take $\psi'_{r-1}(y) = y - \mu_{r-1}^{-1}\eta$, and

$$\mathbf{t}' = (\phi_1'(x); \lambda_1, \phi_2'(x); \cdots; \lambda_{r-2}, \phi'_{r-1}(y); \lambda_{r-1}, \psi'_{r-1}(y)).$$

Thus, $f'_{r-1} = 1$. We have $a = \omega'_r(G)$ and $\deg G = m'_{r-1}\omega'_{r-1}(G) = m'_{r-1}e_{r-1}a = m'_r a$; therefore, $G(x)$ is of type $\mathbf{t}'$, by Lemma 2.4.

The same argument shows that there is a unique irreducible factor $\phi'_r(x)$ of $\phi_r(x)$ in $\mathcal{O}_{K'}[x]$ such that $R'_{r-1}(\phi'_r)(y) \sim (\mu_{r-1}y - \eta)$. We choose $\phi'_r(x)$ as a representative of $\mathbf{t}'$. Let $\rho_r(x) = \phi_r(x)/\phi'_r(x) \in \mathcal{O}_{K'}[x]$. By construction, $\omega'_r(\rho_r) = 0$, because $R'_{r-1}(\rho_r)(y) \sim \psi_{r-1}(\mu_{r-1}y)/(\mu_{r-1}y - \eta)$.

Let $P(x) \in \mathcal{O}[x]$ be a nonzero polynomial. As an immediate consequence of $(N')_{r-1}^-(P) = N_{r-1}^-(P)$, and $R'_{r-1}(P)(y) \sim R_{r-1}(P)(\mu_{r-1}y)$, we get respectively $v'_r(P) = v_r(P)$, and $\omega'_r(P) = \omega_r(P)$. Consider the ϕ_r-adic development of $P(x)$:

$$\begin{aligned} P(x) &= \phi_r(x)^n + a_{n-1}(x)\phi_r(x)^{n-1} + \cdots + a_0(x) \\ &= \rho_r(x)^n\phi'_r(x)^n + a_{n-1}(x)\rho_r(x)^{n-1}\phi'_r(x)^{n-1} + \cdots + a_0(x). \end{aligned}$$

Since $\omega'_r(\rho_r) = 0$, this ϕ'_r-adic development of $P(x)$ is admissible. On the other hand, the equality $(N')_r^-(P) = N_r^-(P)$ is deduced from the tautology:

$$v_r(a_i(x)\phi_r(x)^i) = v'_r(a_i(x)\phi_r(x)^i) = v'_r(a_i(x)\rho_r(x)^i\phi'_r(x)^i).$$

In order to prove the relationship between $R'_{\lambda_r}(P)(y)$ and $R_{\lambda_r}(P)(y)$, we introduce some elements in $\mathbb{F}^*_{K'}$, constructed in terms of the rational functions of Definition 2.13. By Corollary 3.2, $v(\Phi_r(\theta)) = v(\Phi'_r(\theta))$, $v(\pi_r(\theta)) = (e_1\cdots e_{r-1})^{-1} = v(\pi'_r(\theta))$, and $v(\gamma_r(\theta)) = 0 = v(\gamma'_r(\theta))$. Also, by the theorem of the polygon,

$$v(\rho_r(\theta)) = (v_r(\phi_r) - v'_r(\phi'_r))/(e_1\cdots e_{r-1}) = v(\pi'_{r-1}(\theta))(v_r(\phi_r) - v'_r(\phi'_r))/e_{r-1}.$$

We introduce the following elements of $\mathbb{F}^*_{K'}$:

$$\mu_r := \overline{\gamma_r(\theta)/\gamma'_r(\theta)}, \qquad \tau_r := \overline{\pi_r(\theta)/\pi'_r(\theta)},$$
$$\sigma_r := \overline{\Phi_r(\theta)/\Phi'_r(\theta)}, \qquad \epsilon_r := \overline{\rho_r(\theta)/\pi'_{r-1}(\theta)^{(v_r(\phi_r)-v'_r(\phi'_r))/e_{r-1}}}.$$

Since $f_{r-1}v_r(\phi_{r-1}) = v_r(\phi_r)/e_{r-1}$, the recursive definition of the functions of Definition 2.13 yields the following identities:

$$\sigma_r = \epsilon_r/(\tau_{r-1})^{v_r(\phi_r)/e_{r-1}}, \qquad \tau_r = (\sigma_{r-1})^{\ell_{r-1}}/(\tau_{r-1})^{\ell'_{r-1}}. \tag{32}$$

We need still another interpretation of ϵ_r. Since $(N')^-_{r-1}(\phi_r) = N^-_{r-1}(\phi_r)$, the theorem of the product shows that $(N')^-_{r-1}(\rho_r)$ is one-sided with slope λ_{r-1}; hence, the initial point $(s'_{r-1}(\rho_r), u'_{r-1}(\rho_r))$ of $S := S'_{r-1}(\rho_r)$ is given by $s'_{r-1}(\rho_r) = 0$ and

$$u'_{r-1}(\rho_r) = v'_r(\rho_r)/e_{r-1} = (v'_r(\phi_r) - v'_r(\phi'_r))/e_{r-1} = (v_r(\phi_r) - v'_r(\phi'_r))/e_{r-1}. \tag{33}$$

Recall that the virtual factor $\rho^S_r(x)$ is by definition $\rho_r(x)/\pi'_{r-1}(x)^{u'_{r-1}(\rho_r)}$; therefore, item (1) of Proposition 3.5 shows that, for $r \geq 2$:

$$\epsilon_r = R'_{r-1}(\rho_r)(z'_{r-1}). \tag{34}$$

We have seen above that for each integer abscissa i, the i-th terms of the ϕ_r-adic and ϕ'_r-adic developments of $P(x)$ determine the same point (i, u_i) of the plane. Let $i = s + je_r$ be an abscissa such that (i, u_i) lies on $S_{\lambda_r}(P) = S'_{\lambda_r}(P)$; the corresponding residual coefficients at this abscissa are respectively

$$c_i = (z_{r-1})^{t_{r-1}(i)} R_{r-1}(a_i)(z_{r-1}), \quad c'_i = (z'_{r-1})^{t'_{r-1}(i)} R'_{r-1}(a_i\rho_r^i)(z'_{r-1}),$$

and $R_{\lambda_r}(P)(y) = \sum_{0\leq j\leq d} c_i y^j$, $R'_{\lambda_r}(P)(y) = \sum_{0\leq j\leq d} c'_i y^j$. Hence, the last equality of item (3) is equivalent to $c'_i = c_i\sigma_r^s\tau_r^u\mu_r^j$, for all such i.

Note that $t_{r-1}(i) = (s_{r-1}(a_i) - \ell_{r-1}u_i)/e_{r-1} = t'_{r-1}(i)$, since

$$s'_{r-1}(a_i\rho_r^i) = s'_{r-1}(a_i) + is'_{r-1}(\rho_r) = s'_{r-1}(a_i) = s_{r-1}(a_i),$$

the last equality because $N^-_{r-1}(a_i) = (N')^-_{r-1}(a_i)$. For simplicity we denote by $(s(a_i), u(a_i))$ the initial point of $S_{r-1}(a_i)$. By (33), the initial point of $S'_{r-1}(a_i\rho_r^i)$ is $(s(a_i), u(a_i) + i(v_r(\phi_r) - v'_r(\phi'_r))/e_{r-1})$. Now, by induction, the theorem of the product, and (34), we have

$$\begin{aligned} c'_i &= (z'_{r-1})^{t_{r-1}(i)} R'_{r-1}(a_i)(z'_{r-1})\,\epsilon_r^i \\ &= (z'_{r-1})^{t_{r-1}(i)} (\sigma_{r-1})^{s(a_i)} (\tau_{r-1})^{u(a_i)} R_{r-1}(a_i)(z_{r-1})\,\epsilon_r^i \\ &= c_i(\mu_{r-1})^{-t_{r-1}(i)} (\sigma_{r-1})^{s(a_i)} (\tau_{r-1})^{u(a_i)} \epsilon_r^i \\ &= c_i\mu_r^j \left(\mu_r^{-j}(\mu_{r-1})^{-t_{r-1}(i)}\right) (\sigma_{r-1})^{s(a_i)} (\tau_{r-1})^{u(a_i)} \epsilon_r^i. \end{aligned}$$

By Lemma 3.4,

$$\begin{aligned}\gamma_r(\theta)^j\gamma_{r-1}(\theta)^{t_{r-1}(i)} &= \phi_r(\theta)^i\Phi_{r-1}(\theta)^{s(a_i)}\pi_{r-1}(\theta)^{u(a_i)}\Phi_r(\theta)^{-s}\pi_r(\theta)^{-u}\\ &= \phi_r(\theta)^i\Phi_{r-1}(\theta)^{s(a_i)-\ell_{r-1}u}\pi_{r-1}(\theta)^{u(a_i)+\ell'_{r-1}u}\Phi_r(\theta)^{-s}.\end{aligned}$$

We get an analogous expression for $\gamma'_r(\theta)^j\gamma'_{r-1}(\theta)^{t_{r-1}(i)}$, just by putting $'$ everywhere and by replacing $u(a_i)$ by $u(a_i\rho_r^i) = u(a_i) + i(v_r(\phi_r) - v'_r(\phi'_r))/e_{r-1}$. By taking the quotient of both expressions and taking classes modulo $\mathfrak{m}_{K'}$ we get

$$\mu_r^j(\mu_{r-1})^{t_{r-1}(i)} = \epsilon_r^i(\sigma_{r-1})^{s(a_i)-\ell_{r-1}u}(\tau_{r-1})^{u(a_i)+\ell'_{r-1}u}\sigma_r^{-s}.$$

Therefore, $c'_i = c_i\mu_r^j(\sigma_{r-1})^{\ell_{r-1}u}(\tau_{r-1})^{-\ell'_{r-1}u}\sigma_r^s = c_i\mu_r^j\tau_r^u\sigma_r^s$, by (32). □

Theorem 3.7 (Theorem of the residual polynomial in order r)**.** *Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial with $\omega_r(f) > 0$, and let S be a side of $N_r^-(f)$ with finite slope λ_r. Consider the factorization*

$$R_{\lambda_r}(f)(y) \sim \psi_{r,1}(y)^{a_1}\cdots\psi_{r,t}(y)^{a_t}$$

of the residual polynomial of $f(x)$ into the product of powers of pairwise different monic irreducible polynomials in $\mathbb{F}_r[y]$. Then, the factor $f_{\mathbf{t},\lambda_r}(x)$ of $f_{\mathbf{t}}(x)$, corresponding to S by the theorem of the polygon, admits a factorization in $\mathcal{O}[x]$,

$$f_{\mathbf{t},\lambda_r}(x) = G_1(x)\cdots G_t(x),$$

into a product of t monic polynomials, with all $N_r(G_i)$ one-sided of slope λ_r, and $R_{\lambda_r}(G_i)(y) \sim \psi_{r,i}(y)^{a_i}$ in $\mathbb{F}_r[y]$.

Proof. Let us deal first with the case $F(x) := f_{\mathbf{t},\lambda_r}(x)$ irreducible. We only need to prove that $R_{\lambda_r}(F)(y)$ is the power of an irreducible polynomial of $\mathbb{F}_r[y]$. Let $\theta \in \overline{\mathbb{Q}}_p$ be a root of $F(x)$, take $L = K(\theta)$, and fix the embedding $\mathbb{F}_r \to \mathbb{F}_L$ as in (27). Let K' be the unramified extension of K of degree $f_0\cdots f_{r-1}$, and let $G(x) \in \mathcal{O}_{K'}[x]$ be the minimal polynomial of θ over K', so that $F(x) = \prod_{\sigma\in\mathrm{Gal}(K'/K)} G^\sigma(x)$. Under the embedding $\mathbb{F}_r \to \mathbb{F}_L$, the field $\mathbb{F}_r$ is identified to $\mathbb{F}_{K'}$. By Proposition 3.6, we can construct a type $\mathbf{t}'$ of order $r-1$ over K' such that $R'_{\lambda_r}(F)(y) \sim R_{\lambda_r}(F)(cy)$, for some nonzero constant $c \in \mathbb{F}_{K'}$. By the construction of $\mathbf{t}'$, for any $\sigma \neq 1$, the polynomial $G^\sigma(x)$ is not divisible by $\phi'_1(x)$ modulo $\mathfrak{m}_{K'}$; thus, $\omega'_r(G^\sigma) \le \omega'_1(G^\sigma) = 0$, and $R'_{\lambda_r}(G^\sigma)(y)$ is a constant. Therefore, by the theorem of the product, $R'_{\lambda_r}(G)(y) \sim R'_{\lambda_r}(F)(y) \sim R_{\lambda_r}(F)(cy)$, so that $R_{\lambda_r}(F)(y)$ is the power of an irreducible polynomial of $\mathbb{F}_r[y]$ if and only if $R'_{\lambda_r}(G)(y)$ has the same property over $\mathbb{F}_{K'}$. In conclusion, by extending the base field, we can suppose that $f_0 = \cdots = f_{r-1} = 1$.

Let $P(x) = \sum_{j=0}^k b_j x^j \in \mathcal{O}[x]$ be the minimal polynomial of $\gamma_r(\theta)$ over K. Let

$$\Pi(x) := \gamma_r(x)/\phi_r(x)^{e_r} = \pi_{r-1}(x)^{-e_rf_{r-1}v_r(\phi_{r-1})}\pi_r(x)^{-h_r}.$$

By (17), $\Pi(x)$ admits an expression $\Pi(x) = \pi^{n'_0}\phi_1(x)^{n'_1}\cdots\phi_{r-1}(x)^{n'_{r-1}}$ for some integers $n'_1,\dots,n'_r$. Take $\Phi(x) := \pi^{n_0}\phi_1(x)^{n_1}\cdots\phi_{r-1}(x)^{n_{r-1}}$ with sufficiently large nonnegative integers n_i so that $\Pi(x)^k\Phi(x)$ is a polynomial in $\mathcal{O}[x]$. Then, the following rational function is actually a polynomial in $\mathcal{O}[x]$:

$$Q(x) := \Phi(x)P(\gamma_r(x)) = \sum_{j=0}^k B_{je_r}(x)\phi_r(x)^{je_r}, \quad B_{je_r}(x) = \Phi(x)\Pi(x)^j b_j.$$

Moreover, by item (5) of Proposition 2.15, $\omega_r(B_{je_r}) = 0$ for all j such that $B_{je_r} \neq 0$, so that this ϕ_r-development of $g(x)$ is admissible.

Our aim is to show that $N_r(Q)$ is one-sided with slope λ_r, and $R_{\lambda_r}(Q)(y)$ is equal to $P(y)$ modulo $\mathfrak{m}$, up to a nonzero multiplicative constant. Since $P(x)$ is irreducible, $R_{\lambda_r}(Q)(y)$ will be the power of an irreducible polynomial of $\mathbb{F}[y]$. Since $Q(\theta) = 0$, $F(x)$ is a divisor of $Q(x)$ and the residual polynomial of $F(x)$ will be the power of an irreducible polynomial too, by the theorem of the product. This will end the proof of the theorem in the irreducible case.

Let us find a lower bound to all $v_r(B_{je_r}\phi_r^{je_r})$. Denote $u := v_r(\Phi)$. By Proposition 2.15 and (16), we get $v_r(\pi_{r-1}) = e_{r-1}$, $v_r(\pi_r) = 1$, and $v_r(\Pi) = -e_r v_r(\phi_r) - h_r$. Therefore,

$$u_{je_r} := v_r(B_{je_r}\phi_r^{je_r}) = v_r(b_j) + u - j(e_r v_r(\phi_r) + h_r) + je_r v_r(\phi_r) \geq u - jh_r. \tag{35}$$

For $j = 0, k$ we have $v(b_0) = 0$ (because $v(\gamma_r(\theta)) = 0$) and $v(b_k) = 0$ (because $b_k = 1$). Hence, equality holds in (35) for these two abscissas. This proves that $N_r(g)$ has only one side T, with end points $(0, u)$, $(ke_r, u - kh_r)$, and slope λ_r.

Let $R_{\lambda_r}(g)(y) = \sum_{j=0}^{k} c_{je_r} y^j$. We want to show that $c_{je_r} = c\bar{b}_j$ for a certain constant $c \in \mathbb{F}^*$ independent of j. If $(je_r, u_{je_r}) \notin T$, then $c_{je_r} = 0$, and by (35), this is equivalent to $\bar{b}_j = 0$. Now suppose that $(je_r, u_{je_r}) \in T$; by item (1) of Proposition 3.5 (cf. (31))

$$\operatorname{red}_L\left(\frac{B_{je_r}(\theta)\phi_r(\theta)^{je_r}}{\pi_r(\theta)^u}\right) = c_{je_r}\overline{\gamma_r(\theta)}^j.$$

Hence, we want to check that for all j,

$$\operatorname{red}_L\left(\frac{B_{je_r}(\theta)\phi_r(\theta)^{je_r}}{\pi_r(\theta)^u\gamma_r(\theta)^j}\right) = c\bar{b}_j,$$

for some nonzero constant c. Now, if we substitute $B_{je_r}(x)$ and $\Pi(x)$ by its defining values, the left-hand side is equal to $c\bar{b}_j$, for $c = \operatorname{red}_L(\Phi(\theta)/\pi_r(\theta)^u)$. This ends the proof of the theorem in the irreducible case.

In the general case, consider the decomposition, $F(x) = \prod_j P_j(x)$, into a product of monic irreducible factors in $\mathcal{O}[x]$. By Lemma 2.4, each $P_j(x)$ has type $\mathbf{t}$, so that $\omega_r(P_j) > 0$. By the theorem of the product, $N_r(P_j)$ is one-sided, of positive length and slope λ_r. By the proof in the irreducible case, the residual polynomial $R_{\lambda_r}(P_j)(y)$ is the positive power of an irreducible polynomial, and by the theorem of the product it must be $R_{\lambda_r}(P_j)(y) \sim \psi_{r,i}(y)^{b_j}$ for some $1 \leq i \leq t$. If we group these factors according to the irreducible factor of the residual polynomial, we get the desired factorization. □

Corollary 3.8. *With the notation above, let $\theta \in \overline{\mathbb{Q}}_p$ be a root of $G_i(x)$ and let $L = K(\theta)$. Let $f_r = \deg \psi_{r,i}(y)$. Then, $f(L/K)$ is divisible by $f_0 f_1 \cdots f_r$. Moreover, the number of irreducible factors of $G_i(x)$ is at most a_i; in particular, if $a_i = 1$, then $G_i(x)$ is irreducible in $\mathcal{O}[x]$ and*

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

Proof. The statement about $f(L/K)$ is a consequence of the extension of the embedding (27) to an embedding

$$\mathbb{F}_r[y]/(\psi_{r,i}(y)) \hookrightarrow \mathbb{F}_L, \qquad y \mapsto \overline{\gamma_r(\theta)}, \tag{36}$$

which is well-defined by item (4) of Proposition 3.5. The other statements follow from the theorem of the product. The computation of $f(L/K)$ and $e(L/K)$ follows from

$$f(L/K)e(L/K) = \deg G_i = f_0 f_1 \cdots f_r e_1 \cdots e_{r-1} e_r$$

and the fact that $f(L/K)$ is divisible by $f_0 \cdots f_r$ and $e(L/K)$ is divisible by $e_1 \cdots e_r$ (cf. Corollary 3.3). □

3.3. **Types of order r attached to a separable polynomial.** Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial.

Definition 3.9. Let $\mathbf{t}$ be a type of order $r-1$. We say that $\mathbf{t}$ is *f-complete* if $\omega_r(f) = 1$. In this case, $f_{\mathbf{t}}(x)$ is irreducible and the ramification index and residual degree of the extension of K determined by $f_{\mathbf{t}}(x)$ can be computed in terms of some data of $\mathbf{t}$, by applying Corollary 3.8 in order $r-1$ (Corollary 1.20 if $r = 2$).

The results of section 3 can be interpreted as the addition of *two more dissections*, for each order $2, \dots, r$, to the three classical ones, in the process of factorization of $f(x)$. If $\mathbf{t}$ is a type of order $r-1$ and $\omega_r(f) > 1$, we construct a representative $\phi_r(x)$ of $\mathbf{t}$. The factor $f_{\mathbf{t}}(x)$ then admits to further factorizations at two levels: first $f_{\mathbf{t}}(x)$ factorizes into as many factors as the number of sides of $N_r^-(f)$, and then, the factor corresponding to each finite slope splits into the product of as many factors as the number of pairwise different irreducible factors of the residual polynomial attached to the slope.

Notation. Suppose $\mathbf{t}$ is a type of order $r-1$, $\omega_r(f) > 1$ and $\phi_r(x)$ is a representative of $\mathbf{t}$. We denote by

$$(\mathbf{t}; \lambda_r, \psi_r) = (\phi_1(x); \lambda_1, \phi_2(x); \cdots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$$

the type of order r distinguished by the choice of a finite slope λ_r of a side of $N_r^-(f)$ and a monic irreducible factor $\psi_r(y)$ of $R_{\lambda_r}(f)(y)$ in $\mathbb{F}_r[y]$.

Definition 3.10. In section 1.5, we defined two sets $\mathbf{t}_0(f)$, $\mathbf{t}_1(f)$. We recursively define $\mathbf{t}_r(f)$ to be the set of all types of order r constructed as above, $\mathbf{t}' = (\mathbf{t}; \lambda_r, \psi_r(y))$, from those $\mathbf{t} \in \mathbf{t}_{r-1}(f)$ that are not f-complete. This set is not an intrinsic invariant of $f(x)$ because it depends on the choices of the representatives $\phi_1(x), \dots, \phi_r(x)$ of the truncations of $\mathbf{t}$.

We denote by $\mathbf{t}_s(f)^{\mathrm{compl}}$ the subset of the f-complete types of $\mathbf{t}_s(f)$, and we define

$$\mathbf{T}_r(f) := \mathbf{t}_r(f) \cup \left(\bigcup_{0 \le s < r} \mathbf{t}_s(f)^{\mathrm{compl}} \right).$$

Hensel's lemma and the theorems of the polygon and of the residual polynomial in orders $1, \dots, r$ determine a factorization

$$f(x) = f_{r,\infty}(x) \prod_{\mathbf{t} \in \mathbf{T}_r(f)} f_{\mathbf{t}}(x), \tag{37}$$

where $f_{r,\infty}(x)$ is the product of the different representatives $\phi_i(x)$ (of the different types in $\mathbf{T}_r(f)$) that divide $f(x)$ in $\mathcal{O}[x]$.

The following remark is an immediate consequence of the definitions.

Lemma 3.11. *The following conditions are equivalent:*

(1) $\mathbf{t}_{r+1}(f)=\emptyset$.
(2) $\mathbf{t}_r(f)^{\mathrm{compl}}=\mathbf{t}_r(f)$.
(3) *For all* $\mathbf{t}\in\mathbf{t}_{r-1}(f)$ *and all* $\lambda_r\in\mathbb{Q}^-$, *the residual polynomial of* r*-th order,* $R_{\lambda_r}(f)(y)$, *is separable.* □

If these conditions are satisfied, then (37) is a factorization of $f(x)$ into the product of monic irreducible polynomials in $\mathcal{O}[x]$, and we get arithmetic information about each factor by Corollary 3.8. As long as there is some $\mathbf{t}\in\mathbf{t}_r(f)$ which is not f-complete, we must apply the results of this section in order $r+1$ to get further factorizations of $f_{\mathbf{t}}(x)$, or to detect that it is irreducible. We need some invariant to control the whole process and ensure that after a finite number of steps we shall have $\mathbf{t}_r(f)^{\mathrm{compl}}=\mathbf{t}_r(f)$. This is the aim of the next section.

We end with a remark about p-adic approximations to the irreducible factors of $f(x)$, which is an immediate consequence of Lemma 2.2, the theorem of the polygon and Proposition 2.15.

Proposition 3.12. *Let* $\mathbf{t}$ *be an* f*-complete type of order* r, *with representative* $\phi_{r+1}(x)$. *Let* $\theta\in\overline{\mathbb{Q}}_p$ *be a root of* $f_{\mathbf{t}}(x)$, *and* $L=K(\theta)$. *Then,* $\deg\phi_{r+1}=\deg f_{\mathbf{t}}$, *and* $\phi_{r+1}(x)$ *is an approximation to* $f_{\mathbf{t}}(x)$ *satisfying*

$$v(\phi_{r+1}(\theta))=(v_{r+1}(\phi_{r+1})+h_{r+1})/e(L/K)=\sum_{i=1}^{r+1}e_if_i\cdots e_rf_r\,\frac{h_i}{e_1\dots e_i},$$

where $-h_{r+1}$ *is the slope of the unique side of* $N^-_{r+1}(f)$, *and* $e_{r+1}=1$. □

4. Indices and resultants of higher order

We fix throughout this section a natural number $r\geq 1$.

4.1. Computation of resultants with Newton polygons.

Definition 4.1. Let $\mathbf{t}$ be a type of order $r-1$ and let $\phi_r(x)\in\mathcal{O}[x]$ be a representative of $\mathbf{t}$. For any pair of monic polynomials $P(x),Q(x)\in\mathcal{O}[x]$ we define

$$\mathrm{Res}_{\mathbf{t}}(P,Q):=f_0\cdots f_{r-1}\Big(\sum_{i,j}\min\{E_iH'_j,E'_jH_i\}\Big),$$

where $E_i=\ell(S_i)$, $H_i=H(S_i)$ are the lengths and heights of the sides S_i of $N_r^-(P)$, and $E'_j=\ell(S'_j)$, $H'_j=H(S'_j)$ are the lengths and heights of the sides S'_j of $N_r^-(Q)$.

We recall that for a side S of slope $-\infty$ we took $H(S)=\infty$ by convention. Thus, the part of $\mathrm{Res}_{\mathbf{t}}(P,Q)$ that involves sides of slope $-\infty$ is always

$$f_0\cdots f_{r-1}(\mathrm{ord}_{\phi_r}(P)H(Q)+\mathrm{ord}_{\phi_r}(Q)H(P)), \tag{38}$$

where $H(P)$, $H(Q)$ are the total heights respectively of $N_r^-(P)$, $N_r^-(Q)$.

Lemma 4.2. *Let* $P(x),P'(x),Q(x)\in\mathcal{O}[x]$ *be monic polynomials.*

(1) $\mathrm{Res}_{\mathbf{t}}(P,Q)=0$ *if and only if* $\omega_r(P)\omega_r(Q)=0$.
(2) $\mathrm{Res}_{\mathbf{t}}(P,Q)<\infty$ *if and only if* $\mathrm{ord}_{\phi_r}(P)\,\mathrm{ord}_{\phi_r}(Q)=0$.
(3) $\mathrm{Res}_{\mathbf{t}}(P,Q)=\mathrm{Res}_{\mathbf{t}}(Q,P)$.
(4) $\mathrm{Res}_{\mathbf{t}}(PP',Q)=\mathrm{Res}_{\mathbf{t}}(P,Q)+\mathrm{Res}_{\mathbf{t}}(P',Q)$.

Proof. The first three items are an immediate consequence of the definition. Item (4) follows from $N_r^-(PP')=N_r^-(P)+N_r^-(P')$. □

In the simplest case when $N_r^-(P)$ and $N_r^-(Q)$ are both one-sided, $\mathrm{Res}_{\mathbf{t}}(P,Q)$ represents the area of the rectangle joining the two triangles determined by the sides if they are ordered by increasing slope. The reader may figure out a similar geometrical interpretation of $\mathrm{Res}_{\mathbf{t}}(P,Q)$ in the general case, as the area of a union of rectangles below the Newton polygon $N_r^-(PQ) = N_r^-(P) + N_r^-(Q)$. See Figure 16.

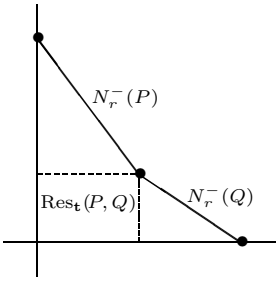


FIGURE 16

Our aim is to compute $v(\mathrm{Res}(P,Q))$ as a sum of several $\mathrm{Res}_{\mathbf{t}}(P,Q)$ for an adequate choice of types $\mathbf{t}$. To this end, we want to compare types attached to P and Q, and this is not easy because in the definition of the sets $\mathbf{t}_r(P)$, $\mathbf{t}_r(Q)$, we had freedom in the choices of the different representatives $\phi_i(x)$. For commodity in the exposition, we assume in this section that these polynomials are universally fixed.

Convention. We fix from now on a monic lift $\phi_1(x) \in \mathcal{O}[x]$ of every monic irreducible polynomial $\psi_0(y) \in \mathbb{F}[y]$. We then proceed recursively: for any type of order i, $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \cdots; \lambda_{i-1}, \phi_i(x); \lambda_i, \psi_i(y))$, with $1 \le i < r$ and $\phi_1(x), \ldots, \phi_i(x)$ belonging to the infinite family of previously chosen polynomials, we fix a representative $\phi_{i+1}(x)$ of $\mathbf{t}$. Also, we assume from now on that all types are made up only with our chosen polynomials $\phi_i(x)$.

Once these choices are made, the set $\mathbf{t}_r(P)$ is uniquely determined by r and $P(x)$. More precisely, $\mathbf{t}_r(P)$ is the set of all types $\mathbf{t}$ of order r such that $\omega_{r+1}^{\mathbf{t}}(P) > 0$ and the truncation $\mathrm{Trunc}_{r-1}(\mathbf{t})$ is not P-complete; in other words,

$$\mathbf{t}_r(P) = \left\{\mathbf{t} \text{ type of order } r \text{ such that } \omega_{r+1}^{\mathbf{t}}(P) > 0,\, \omega_r^{\mathbf{t}}(P) > 1\right\}.$$

However, in view of the computation of resultants, we need a broader concept of "type attached to a polynomial".

Definition 4.3. For any monic polynomial $P(x) \in \mathcal{O}[x]$, we define

$$\hat{\mathbf{t}}_r(P) := \{\mathbf{t} \text{ type of order } r \text{ such that } \omega_{r+1}^{\mathbf{t}}(P) > 0\} \supseteq \mathbf{t}_r(P).$$

The following observation is a consequence of the fact that $\omega_{r+1}^{\mathbf{t}}$ is a semigroup homomorphism for every type $\mathbf{t}$ of order r.

Lemma 4.4. *$\hat{\mathbf{t}}_r(PQ) = \hat{\mathbf{t}}_r(P) \cup \hat{\mathbf{t}}_r(Q)$, for all monic $P(x), Q(x) \in \mathcal{O}[x]$.* □

Note that the analogous statement for the sets $\mathbf{t}_r(P)$ is false. For instance, let $P(x), Q(x)$ be two monic polynomials congruent to the same irreducible polynomial $\psi(y)$ modulo $\mathfrak{m}$. We have $\mathbf{t}_0(P) = \mathbf{t}_0(Q) = \{\psi(y)\} = \mathbf{t}_0(PQ)$, and the type of order zero $\psi(y)$ is P-complete and Q-complete; thus, $\mathbf{t}_1(P) = \emptyset = \mathbf{t}_1(Q)$. However, $\psi(y)$ is not PQ-complete, and $\mathbf{t}_1(PQ) \neq \emptyset$.

We can build the set $\hat{\mathbf{t}}_r(P)$ in a constructive way analogous to that used to construct $\mathbf{t}_r(P)$. To this end, the P-complete types of order $r-1$ must be expanded as well to produce types of order r. Thanks to our convention about fixing a universal family of representatives of the types, these expansions are unique.

Lemma 4.5. *Let $P(x) \in \mathcal{O}[x]$ be a monic polynomial. Let $\mathbf{t}$ be a P-complete type of order $r-1$ with representative $\phi_r(x)$ and suppose that $P(x)$ is not divisible by $\phi_r(x)$ in $\mathcal{O}[x]$. Then, $\mathbf{t}$ can be extended to a unique type $\mathbf{t}' \in \hat{\mathbf{t}}_r(P)$ such that $\mathrm{Trunc}_{r-1}(\mathbf{t}') = \mathbf{t}$. The type $\mathbf{t}'$ is P-complete too.*

Proof. By Lemma 2.17, $N_r^-(P)$ has length one and finite slope $\lambda_r \in \mathbb{Q}^-$; hence, $\deg R_{\lambda_r}(P) = 1$. Let $\psi_r(y)$ be the monic polynomial of degree one determined by $R_{\lambda_r}(P)(y) \sim \psi_r(y)$. The type $\mathbf{t}' = (\mathbf{t}; \lambda_r, \psi_r(y))$ is P-complete and it is the unique type of order r such that $\mathrm{Trunc}_{r-1}(\mathbf{t}') = \mathbf{t}$ and $\omega_{r+1}^{\mathbf{t}'}(P) > 0$. In fact, let us check that $\omega_{r+1}^{\mathbf{t}''}(P) = 0$ for any $\mathbf{t}'' = (\mathbf{t}; \lambda_r', \psi_r'(y)) \neq \mathbf{t}'$. If $\lambda_r' \neq \lambda_r$, then $R_{\lambda_r'}(P)$ is a constant; if $\lambda_r' = \lambda_r$, but $\psi_r(y) \neq \psi_r'(y)$, then $\psi_r'(y)$ cannot divide $R_{\lambda_r}(P)(y)$. □

Lemma 4.6. *Let $P(x) \in \mathcal{O}[x]$ be a monic polynomial. Then, $\hat{\mathbf{t}}_r(P) = \emptyset$ if and only if all irreducible factors of $P(x)$ are the representatives of some type of order $0, 1, \dots, r-1$. Moreover, if $P(x)$ is irreducible and $\hat{\mathbf{t}}_r(P) \neq \emptyset$, then $|\hat{\mathbf{t}}_r(P)| = 1$.*

Proof. By Lemma 4.4, we can assume that $P(x)$ is irreducible. If $P(x) = \phi_s(x)$ is the representative of some type of order $s-1 \leq r-1$, then $N_s(\phi_s)$ is one-sided of slope $-\infty$; hence, $R_{\lambda_s}(\phi_s)$ is a constant for every $\lambda_s \in \mathbb{Q}^-$, and $\omega_{s+1}^{\mathbf{t}'}(\phi_s) = 0$, for every type $\mathbf{t}'$ of order $\geq s$. Thus, $\hat{\mathbf{t}}_r(\phi_s) = \emptyset$, for all $r \geq s$. Otherwise, the theorems of the polygon and of the residual polynomial show that the unique element of $\hat{\mathbf{t}}_0(P)$ can be successively extended to a unique element of $\hat{\mathbf{t}}_1(P), \dots, \hat{\mathbf{t}}_r(P)$. □

Definition 4.7. For any pair of monic polynomials $P(x), Q(x) \in \mathcal{O}[x]$, we define

$$\mathrm{Res}_r(P, Q) := \sum\nolimits_{\mathbf{t} \in \hat{\mathbf{t}}_{r-1}(P) \cap \hat{\mathbf{t}}_{r-1}(Q)} \mathrm{Res}_{\mathbf{t}}(P, Q).$$

The following two lemmas are an immediate consequence of Lemmas 4.2 and 4.4.

Lemma 4.8. *The following conditions are equivalent:*

(1) $\mathrm{Res}_{r+1}(P, Q) = 0$.
(2) $\hat{\mathbf{t}}_r(P) \cap \hat{\mathbf{t}}_r(Q) = \emptyset$.
(3) *For all $\mathbf{t} \in \hat{\mathbf{t}}_{r-1}(P) \cap \hat{\mathbf{t}}_{r-1}(Q)$ and all $\lambda_r \in \mathbb{Q}^-$, the residual polynomials of r-th order, $R_{\lambda_r}(P)(y)$, $R_{\lambda_r}(Q)(y)$, have no common factor in $\mathbb{F}_r[y]$.* □

Lemma 4.9. *For any three monic polynomials $P(x), P'(x), Q(x) \in \mathcal{O}[x]$, we have $\mathrm{Res}_r(PP', Q) = \mathrm{Res}_r(P, Q) + \mathrm{Res}_r(P', Q)$.* □

Theorem 4.10. *Let $P(x), Q(x) \in \mathcal{O}[x]$ be two monic polynomials having no common factors. Then,*

(1) $v(\mathrm{Res}(P, Q)) \geq \mathrm{Res}_1(P, Q) + \cdots + \mathrm{Res}_r(P, Q)$, *and*
(2) *equality holds if and only if* $\mathrm{Res}_{r+1}(P, Q) = 0$.

Proof. Let us deal first with the case where $P(x)$, $Q(x)$ are both irreducible and $\hat{\mathbf{t}}_{r-1}(P) = \hat{\mathbf{t}}_{r-1}(Q) = \{\mathbf{t}\}$, for some type $\mathbf{t}$. Let $\phi_r(x)$ be the representative of $\mathbf{t}$. For $0 \leq i \leq r$, let E_i, H_i be the length and height of the unique side of $N_i(P)$, and E_i', H_i' be the length and height of the unique side of $N_i(Q)$. By Lemma 4.6,

neither P nor Q is equal to $\phi_1, \dots, \phi_{r-1}$, and by Lemma 2.4, P and Q are both of type $\mathbf{t}$; hence, $0 < E_i E_i'$, $0 < H_i H_i' < \infty$, and $H_i/E_i = H_i'/E_i'$, for all $1 \le i < r$.

Suppose that $-\lambda_r := H_r/E_r \le H_r'/E_r' =: -\lambda_r'$. Since P, Q cannot be both equal to $\phi_r(x)$, we have $P(x) \ne \phi_r(x)$ and $H_r < \infty$. Since,

$$\operatorname{Res}(P,Q) = \pm \prod\nolimits_{Q(\theta)=0} P(\theta), \quad v(\operatorname{Res}(P,Q)) = \deg(Q)\, v(P(\theta)),$$

we need to relate $v(P(\theta))$ with the resultants $\operatorname{Res}_i(P,Q)$.

If $Q(x) \ne \phi_r(x)$, the theorem of the residual polynomial shows that $R_{\lambda_r'}(Q)(y) \sim \psi_r'(y)^{a'}$, for some monic irreducible polynomial $\psi_r'(y) \in \mathbb{F}_r[y]$ and some positive a'. By applying Proposition 2.9 to the type of order r, $\mathbf{t}' = (\mathbf{t}; \lambda_r', \psi_r'(y))$, we get

$$v(P(\theta)) \ge v_{r+1}'(P)/e_1 \cdots e_{r-1} e_r' = (v_r(P) + H_r)/e_1 \cdots e_{r-1}, \tag{39}$$

the last equality by the definition of v_{r+1}'. Also, equality holds in (39) if and only if $\omega_{r+1}'(P) = 0$, where ω_{r+1}' is the pseudo-valuation of order $r+1$ attached to $\mathbf{t}'$.

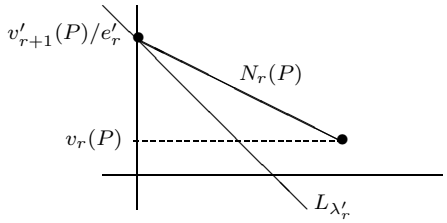


FIGURE 17

If $Q(x) = \phi_r(x)$, then $P(\theta) = a_0(\theta)$, where $a_0(x)$ is the 0-th coefficient of the ϕ_r-adic development of $P(x)$. By Proposition 2.9, $v(a_0(\theta)) = v_r(a_0)/e_1 \cdots e_{r-1}$, and by Lemma 2.17, $v_r(a_0) = v_r(P) + H_r$. Thus,

$$v(P(\theta)) = (v_r(P) + H_r)/e_1 \cdots e_{r-1}.$$

In both cases, $\deg Q = m_r \omega_r(Q) = f_0 e_1 f_1 \cdots e_{r-1} f_{r-1} E_r'$, by Lemma 2.2. If we apply recursively $v_{s+1}(P) = e_s(v_s(P_s) + H_s)$, $E_{s+1}' = (e_s f_s)^{-1} E_s'$, for all $1 \le s < r$, and $v_1(P) = 0$, we get

$$\begin{aligned} v(\operatorname{Res}(P,Q)) &= \deg(Q) v(P(\theta)) \ge \deg Q\, (v_r(P) + H_r)/e_1 \cdots e_{r-1} \\ &= f_0 \cdots f_{r-1} E_r' (v_r(P) + H_r) \\ &= \sum\nolimits_{s=1}^{r} f_0 \cdots f_{s-1} E_s' H_s = \sum\nolimits_{s=1}^{r} \operatorname{Res}_s(P,Q), \end{aligned}$$

and equality holds if and only if either $Q = \phi_r$, or $Q \ne \phi_r$ and $\omega_{r+1}'(P) = 0$. If $Q = \phi_r$, then $\hat{\mathbf{t}}_r(Q) = \emptyset$ and $\operatorname{Res}_{r+1}(P,Q) = 0$. If $Q \ne \phi_r$, the condition $\psi_r' \nmid R_{\lambda_r'}(P)$ is equivalent to item (3) of Lemma 4.8, because $R_{\lambda_r}(P)(y) \sim \psi_r(y)^a$ for some irreducible $\psi_r(y) \in \mathbb{F}_r[y]$, and $R_{\lambda_r''}(P)(y)$ is a constant for any negative rational number $\lambda_r'' \ne \lambda_r$. This ends the proof of the theorem in this case.

Assume now that $P(x)$ and $Q(x)$ are both irreducible, but $\hat{\mathbf{t}}_{r-1}(P) \cap \hat{\mathbf{t}}_{r-1}(Q) = \emptyset$. If $\hat{\mathbf{t}}_0(P) \cap \hat{\mathbf{t}}_0(Q) = \emptyset$, then $\operatorname{Res}_1(P,Q) = \cdots = \operatorname{Res}_{r+1}(P,Q) = 0$, by definition; on the other hand, $v(\operatorname{Res}(P,Q)) = 0$, because $P(x)$ and $Q(x)$ have no common factors modulo $\mathfrak{m}$. Hence, the theorem is proven in this case. If $\hat{\mathbf{t}}_0(P) \cap \hat{\mathbf{t}}_0(Q) \ne \emptyset$, let $1 \le s < r$ be maximal with the property $\hat{\mathbf{t}}_{s-1}(P) \cap \hat{\mathbf{t}}_{s-1}(Q) \ne \emptyset$. Clearly, $\operatorname{Res}_r(P,Q) = 0$

for all $r > s$; thus, we want to show that $v(\mathrm{Res}(P,Q)) = \mathrm{Res}_1(P,Q) + \cdots + \mathrm{Res}_s(P,Q)$, and this follows from the proof of the previous case for $r = s$.

Now let $P(x) = P_1(x)\cdots P_g(x)$, $Q(x) = Q_1(x)\cdots Q_{g'}(x)$ be the factorizations of $P(x)$, $Q(x)$ into a product of monic irreducible polynomials in $\mathcal{O}[x]$. We know that $v(\mathrm{Res}(P_i,Q_j)) \geq \mathrm{Res}_1(P_i,Q_j)+\cdots+\mathrm{Res}_r(P_i,Q_j)$ for all i,j; thus, item (1) follows from Lemma 4.9 and the bilinearity of resultants. Equality in item (1) holds if and only if it holds for each pair P_i, Q_j; that is, if and only if $\mathrm{Res}_{r+1}(P_i,Q_j) = 0$, for all i,j. This is equivalent to $\mathrm{Res}_{r+1}(P,Q) = 0$, again by Lemma 4.9. □

We end this section with an example that illustrates the necessity to introduce the sets $\hat{\mathbf{t}}_r(P)$. Let $\mathcal{O} = \mathbb{Z}_p$, $P(x) = x+p$, $Q(x) = x+p+p^{100}$, and let $\mathbf{t}_0 = y \in \mathbb{F}[y]$. Clearly, $\mathbf{t}_0(P) = \{\mathbf{t}_0\} = \mathbf{t}_0(Q)$, and $\mathbf{t}_0$ is both P-complete and Q-complete, so that $\mathbf{t}_1(P) = \emptyset = \mathbf{t}_1(Q)$. If we take $\phi_1(x) = x$, we get $\mathrm{Res}_1(P,Q) = \mathrm{Res}_{\mathbf{t}_0}(P,Q) = 1$, whereas $v(\mathrm{Res}(P,Q)) = 100$. Thus, we need to consider the expansions of $\mathbf{t}_0$ to types of higher order in order to reach the right value of $v(\mathrm{Res}(P,Q))$. The number of expansions to consider depends on the choices of the representatives $\phi_i(x)$; for instance, if we take $\mathbf{t} = (x;-1,y+1)$, with representative $\phi_2(x) = x+p$, we already have $\mathrm{Res}_2(P,Q) = 99$.

Nevertheless, the sets $\hat{\mathbf{t}}_r(P)$ were introduced only as an auxiliary tool to prove Theorem 4.10. In practice, the factorization algorithm computes only the sets $\mathbf{t}_r(P)$, as we shall show in the next section.

4.2. **Index of a polynomial and index of a polygon.** All representatives of types are still assumed to belong to a universally fixed family, as in the last section.

Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, $\theta \in \overline{\mathbb{Q}}_p$ a root of $F(x)$, and $L = K(\theta)$. It is well known that $(\mathcal{O}_L\colon \mathcal{O}[\theta]) = |\mathbb{F}|^{\mathrm{ind}(F)}$, for some natural number $\mathrm{ind}(F)$ that will be called the *v-index* of $F(x)$. Note that

$$\mathrm{ind}(F) = v(\mathcal{O}_L\colon \mathcal{O}[\theta])/[K\colon \mathbb{Q}_p].$$

Recall the well-known relationship, $v(\mathrm{disc}(F)) = 2\,\mathrm{ind}(F) + v(\mathrm{disc}(L/K))$, linking $\mathrm{ind}(F)$ with the discriminant of $F(x)$ and the discriminant of L/K.

Definition 4.11. Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial and $f(x) = F_1(x)\cdots F_k(x)$ its decomposition into the product of monic irreducible polynomials in $\mathcal{O}[x]$. We define the *index* of $f(x)$ by the formula

$$\mathrm{ind}(f) := \sum_{i=1}^{k} \mathrm{ind}(F_i) + \sum\nolimits_{1\leq i<j\leq k} v(\mathrm{Res}(F_i,F_j)).$$

Definition 4.12. Let S be a one-sided principal polygon, and denote $E = \ell(S)$, $H = H(S)$, $d = d(S)$. We define

$$\mathrm{ind}(S) := \begin{cases} \frac{1}{2}(EH - E - H + d), & \text{if } S \text{ has finite slope,} \\ 0, & \text{otherwise.} \end{cases}$$

Let $N = S_1 + \cdots + S_g$ be a principal polygon, with all sides of positive length, ordered by increasing slopes $-\infty \leq \lambda_1 < \cdots < \lambda_g$. We define

$$\mathrm{ind}(N) := \sum_{i=1}^{g} \mathrm{ind}(S_i) + \sum\nolimits_{1\leq i<j\leq g} E_iH_j.$$

If S_1 has slope $-\infty$, then it contributes $E_1H_{\mathrm{fin}}(N)$ to $\mathrm{ind}(N)$, where $H_{\mathrm{fin}}(N)$ is the total height of the finite part of N.

Remark 4.13. Note that $\operatorname{ind}(N) = 0$ if and only if either N is a single point, or N is one-sided with slope $-\infty$, or N is one-sided with $E = 1$ or $H = 1$.

Remark 4.14. The contribution of the sides of finite slope to $\operatorname{ind}(N)$ is the number of points with integer coordinates that lie on or below the finite part of N, above the horizontal line L that passes through the last point of N, and to the right of the vertical line L' that passes through the initial point of the finite part of N.

For instance, the polygon in Figure 18 has index 25, the infinite side contributes 18 (the area of the rectangle 3×6) and the finite part has index 7, corresponding to the marked seven points with integer coordinates, distributed into $\operatorname{ind}(S_1) = 2$, $\operatorname{ind}(S_2) = 1$, $E_1 H_2 = 4$.

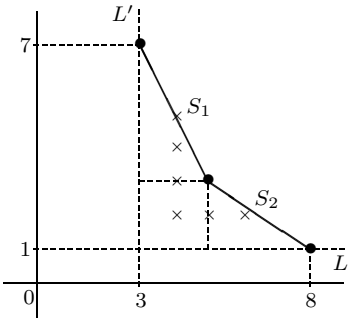


FIGURE 18

Let $i_0 \le i_1$ be the respective abscissas of the starting point and the last point of the finite part N_{fin} of N. For any integer abscissa $i_0 \le i \le i_1$, let y_i be the distance of the point of N of abscissa i to the line L. Clearly, we can count the points with integer coordinates on or below N_{fin}, above L and to the right of L', as the sum of the points with given abscissa:

$$\operatorname{ind}(N_{\text{fin}}) = \lfloor y_{i_0+1} \rfloor + \cdots + \lfloor y_{i_1-1} \rfloor. \tag{40}$$

For instance, in Figure 18 we have $y_4 = 4$, $y_5 = 2$, $y_6 = 1$ and $y_7 = 0$.

Definition 4.15. Let $P(x) \in \mathcal{O}[x]$ be a monic and separable polynomial. Let $\mathbf{t}$ be a type of order $r-1$ and $\phi_r(x)$ a representative of $\mathbf{t}$. We define

$$\operatorname{ind}_{\mathbf{t}}(P) := f_0 \cdots f_{r-1} \operatorname{ind}(N_r^-(P)),$$

where $N_r(P)$ is the Newton polygon of r-th order with respect to $\mathbf{t}$ and $\phi_r(x)$.

For any natural number $r \ge 1$ we define

$$\operatorname{ind}_r(P) := \sum\nolimits_{\mathbf{t} \in \mathbf{t}_{r-1}(P)} \operatorname{ind}_{\mathbf{t}}(P).$$

Since the Newton polygon $N_r^-(P)$ depends on the choice of $\phi_r(x)$, the value of $\operatorname{ind}_{\mathbf{t}}(P)$ depends on this choice too, although this is not reflected in the notation.

Lemma 4.16. *Let $P(x) \in \mathcal{O}[x]$ be a monic and separable polynomial.*

1. *Let $\mathbf{t}$ be a type of order r, and suppose that $\mathbf{t} \notin \mathbf{t}_r(P)$ or $\mathbf{t}$ is P-complete. Then,* $\operatorname{ind}_{\mathbf{t}}(P) = 0$.
2. *If $\mathbf{t}_r(P) = \mathbf{t}_r(P)^{\text{compl}}$, then* $\operatorname{ind}_{r+1}(P) = 0$.
3. *If* $\operatorname{ind}_r(P) = 0$, *then $\mathbf{t}_r(P) = \mathbf{t}_r(P)^{\text{compl}}$.*

Proof. If $\mathbf{t} \notin \mathbf{t}_r(P)$, then either $\omega_{r+1}(P) = 0$ or $\omega_r(P) = 1$. If $\mathbf{t}$ is P-complete, then $\omega_{r+1}(P) = 1$. By Lemmas 2.2 and 2.17, in all cases $\ell(N^-_{r+1}(P)) = \omega_{r+1}(P) \leq 1$, and $\mathrm{ind}_{\mathbf{t}}(P) = 0$ by Remark 4.13. This proves item (1), and item (2) is an immediate consequence.

If $\mathrm{ind}_r(P) = 0$, then $\mathrm{ind}_{\mathbf{t}}(P) = 0$ for all $\mathbf{t} \in \mathbf{t}_{r-1}(P)$. For any such $\mathbf{t}$ we have $\omega_r(P) > 0$, so that $N^-_r(P)$ is not a single point. By Remark 4.13, $N^-_r(P)$ is one-sided with either slope $-\infty$, or length one, or height one. In the first case $P(x)$ is divisible by the representative $\phi_r(x)$ of $\mathbf{t}$ and $\omega_r(P) = \ell(N^-_r(P)) = \mathrm{ord}_{\phi_r}(P) = 1$, because $P(x)$ is separable; thus, $\mathbf{t}$ is P-complete and $\mathbf{t}$ is not extended to any type in $\mathbf{t}_r(P)$. If $N^-_r(P)$ is one-sided with finite slope λ_r and the side has degree one, then the residual polynomial $R_{\lambda_r}(P)(y)$ has degree one. Thus, $\mathbf{t}$ is either P-complete or it can be extended in a unique way to a type $\mathbf{t}' \in \mathbf{t}_r(P)$; in the latter case, necessarily $\omega^{\mathbf{t}'}_{r+1}(P) = 1$ and $\mathbf{t}'$ is P-complete. This proves item (3). □

Lemma 4.17. *Let $P(x), Q(x) \in \mathcal{O}[x]$ be two monic and separable polynomials, without common factors, and let $\mathbf{t}$ be a type of order $r-1$. Then,*

$$\mathrm{ind}_{\mathbf{t}}(PQ) = \mathrm{ind}_{\mathbf{t}}(P) + \mathrm{ind}_{\mathbf{t}}(Q) + \mathrm{Res}_{\mathbf{t}}(P, Q),$$

$$\mathrm{ind}_r(PQ) = \mathrm{ind}_r(P) + \mathrm{ind}_r(Q) + \mathrm{Res}_r(P, Q).$$

Proof. For simplicity, in the discussion we omit the weight $f_0 \cdots f_{r-1}$ that multiplies all terms in the identities.

All terms involved in the first identity are the sum of a finite part and an infinite part. If $P(x)Q(x)$ is not divisible by $\phi_r(x)$, all infinite parts are zero. If $\phi_r(x)$ divides (say) $P(x)$, then the infinite part of $\mathrm{ind}_{\mathbf{t}}(PQ)$ is $\mathrm{ord}_{\phi_r}(P)(H_{\mathrm{fin}}(P)+H_{\mathrm{fin}}(Q))$, the infinite part of $\mathrm{ind}_{\mathbf{t}}(P)$ is $\mathrm{ord}_{\phi_r}(P)H_{\mathrm{fin}}(P)$, the infinite part of $\mathrm{ind}_{\mathbf{t}}(Q)$ is zero, and the infinite part of $\mathrm{Res}_{\mathbf{t}}(P, Q)$ is $\mathrm{ord}_{\phi_r}(P)H(Q)$, by (38). Thus, the first identity is correct, as far as the infinite parts are concerned.

The finite part of the first identity follows from $N^-_r(PQ) = N^-_r(P) + N^-_r(Q)$ and Remark 4.14. Let $N = N^-_r(PQ)$ and let $\mathcal{R}$ be the region of the plane that lies on or below N, above the line L and to the right of the line L', as indicated in Remark 4.14. The number $\mathrm{ind}_{\mathbf{t}}(PQ)$ counts the total number of points with integer coordinates in $\mathcal{R}$, the number $\mathrm{ind}_{\mathbf{t}}(P) + \mathrm{ind}_{\mathbf{t}}(Q)$ counts the number of points with integer cordinates in the regions determined by the right triangles whose hypotenuses are the sides of $N^-_r(P)$ and $N^-_r(Q)$. The region of $\mathcal{R}$ not covered by these triangles is a union of rectangles and $\mathrm{Res}_{\mathbf{t}}(P, Q)$ is precisely the number of points with integer coordinates of this region.

In order to prove the second identity, we note first that for any monic separable polynomial $R(x) \in \mathcal{O}[x]$,

$$\mathrm{ind}_r(R) = \sum\nolimits_{\mathbf{t} \in \hat{\mathbf{t}}_{r-1}(R)} \mathrm{ind}_{\mathbf{t}}(R),$$

by item (1) of Lemma 4.16. Now, if we apply this to $R = P, Q, PQ$, the identity follows from the first one and Lemma 4.4, keeping in mind that $\mathrm{ind}_{\mathbf{t}}(Q) = 0 = \mathrm{Res}_{\mathbf{t}}(P, Q)$ if $\mathbf{t} \notin \hat{\mathbf{t}}_{r-1}(Q)$, because $N^-_r(Q)$ is a single point. □

We are ready to state the theorem of the index, which is a crucial ingredient of the factorization process. It ensures that an algorithm based on the computation of the sets $\mathbf{t}_r(f)$ and the higher indices $\mathrm{ind}_r(f)$ obtains the factorization of $f(x)$, and

relevant arithmetic information on the irreducible factors, after a finite number of steps. Also, this algorithm yields a computation of $\mathrm{ind}(f)$ as a by-product.

Theorem 4.18 (Theorem of the index)**.** *Let $f(x) \in \mathcal{O}[x]$ be a monic and separable polynomial. Then,*

(1) $\mathrm{ind}(f) \geq \mathrm{ind}_1(f) + \cdots + \mathrm{ind}_r(f)$, *and*
(2) *equality holds if and only if* $\mathrm{ind}_{r+1}(f) = 0$.

Note that Lemma 4.16 and this theorem guarantee the equality in (1) whenever all types of $\mathbf{t}_r(f)$ are f-complete. Also, Theorem 4.18 shows that this latter condition will be reached at some order r.

Corollary 4.19. *Let $f(x) \in \mathcal{O}[x]$ be a monic and separable polynomial. There exists $r \geq 0$ such that all types in $\mathbf{t}_r(f)$ are f-complete, or equivalently, such that $\mathbf{t}_{r+1}(f) = \emptyset$.*

Proof. By the theorem of the index, there exists $r \geq 1$ such that $\mathrm{ind}_r(f) = 0$, and by item (3) of Lemma 4.16, this implies $\mathbf{t}_r(f) = \mathbf{t}_r(f)^{\mathrm{compl}}$. □

In the next section we exhibit an example where the factorization is achieved in order three. More examples, and a more accurate discussion of the computational aspects, can be found in [GMN08].

4.3. **An example.** Take $p = 2$, and $f(x) = x^4 + ax^2 + bx + c \in \mathbb{Z}[x]$, with $v(a) \geq 2$, $v(b) = 3$, $v(c) = 2$. This polynomial has $v(\mathrm{disc}(f)) = 12$ for all a, b, c with these restrictions. Since $f(x) \equiv x^4 \pmod 2$, all types we are going to consider will start with $\phi_1(x) = x$. The Newton polygon $N_1(f)$ has slope $\lambda_1 = -1/2$, and the residual polynomial of $f(x)$ with respect to λ_1 is $R_1(f)(y) = y^2 + 1 = (y+1)^2 \in \mathbb{F}$, where $\mathbb{F}$ is the field with two elements. Hence, $\mathbf{t}_1(f) = \{\mathbf{t}\}$, where $\mathbf{t} := (x; -1/2, y+1)$. We have $e_1 = 2, f_0 = f_1 = 1$ and $\omega_2(f) = 2$, so that $\mathbf{t}$ is not f-complete. The partial information we get in order one is $\mathrm{ind}_1(f) = 2$, and the fact that all irreducible factors of $f(x)$ will generate extensions $L/\mathbb{Q}_2$ with even ramification number, because $e_1 = 2$.

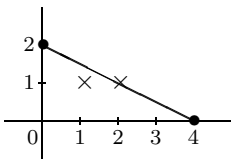


FIGURE 19

Take $\phi_2(x) = x^2 - 2$ as a representative of $\mathbf{t}$. The ϕ_2-development of $f(x)$ is

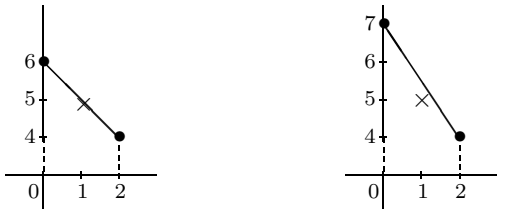
$$f(x) = \phi_2(x)^2 + (a+4)\phi_2(x) + (bx + c + 2a + 4).$$

By Proposition 2.7 and (16), we have

$$v_2(x) = 1,\ v_2(\phi_2) = 2,\ v_2(a+4) \geq 4,\ v_2(bx) = 7,\ v_2(c+2a+4) \geq 6.$$

Hence, according to $v(c+2a+4) = 3$ or $v(c+2a+4) \geq 4$, the Newton polygon of second order, $N_2(f)$, is shown in Figure 20.

If $v(c+2a+4) \geq 4$, $N_2(f)$ is one-sided with slope $\lambda_2 = -3/2$, and $R_2(f)(y) = y + 1$. The type $\mathbf{t}' := (x; -1/2, x^2 - 2; -3/2, y+1)$ is f-complete and $\mathbf{t}_2(f) = \{\mathbf{t}'\}$.



$v(c+2a+4)=3$ $\qquad$ $v(c+2a+4)\geq 4$

FIGURE 20

We have $e_2=2, f_2=1$. Thus, $f(x)$ is irreducible over $\mathbb{Z}_2[x]$, and it generates an extension $L/\mathbb{Q}_2$ with $e(L/\mathbb{Q}_2)=e_1e_2=4$, $f(L/\mathbb{Q}_2)=f_0f_1f_2=1$. Moreover, $\mathrm{ind}_2(f)=1$, so that $\mathrm{ind}(f)=\mathrm{ind}_1(f)+\mathrm{ind}_2(f)=3$.

If $v(c+2a+4)=3$, $N_2(f)$ is one-sided with slope $\lambda_2=-1$, and $R_2(f)(y)=y^2+1=(y+1)^2$. The type $\mathbf{t}':=(x;-1/2,x^2-2;-1,y+1)$ is not f-complete, $\mathbf{t}_2(f)=\{\mathbf{t}'\}$, and we need to pass to order three. We have $h_2=e_2=f_2=1$ and $\mathrm{ind}_2(f)=1$. Take $\phi_3(x)=x^2-2x-2$ as a representative of $\mathbf{t}'$. The ϕ_3-adic development of $f(x)$ is

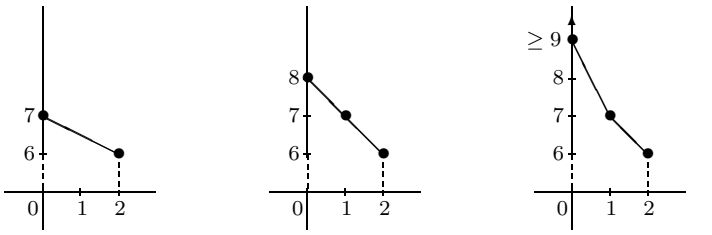
$$f(x)=\phi_3(x)^2+(4x+a+8)\phi_3(x)+(b+2a+16)x+c+2a+12.$$

By Proposition 2.7 and (16), we have

$$v_3(x)=1,\ v_3(\phi_3)=3,\ v_3(4x)=5,\ v_3(c+2a+12)\geq 8,$$

$$v_3(4x+a+8)=\begin{cases}4, & \text{if } v(a)=2,\\ 5, & \text{if } v(a)\geq 3,\end{cases}\quad v_3((b+2a+16)x)=\begin{cases}\geq 9, & \text{if } v(a)=2,\\ 7, & \text{if } v(a)\geq 3.\end{cases}$$

In Figure 21, we show three possibilities for the Newton polygon of third order.



$v(a)\geq 3$ $\qquad$ $v(a)=2$, $v(c+2a+12)=4$ $\qquad$ $v(a)=2$, $v(c+2a+12)\geq 5$

FIGURE 21

If $v(a)\geq 3$, $N_3(f)$ is one-sided with slope $\lambda_3=-1/2$, and $R_3(f)(y)=y+1$. The type $\mathbf{t}'':=(x;-1/2,\phi_2(x);-1,\phi_3(x);-1/2,y+1)$ is f-complete and $\mathbf{t}_3(f)=\{\mathbf{t}''\}$. We have $e_3=2, f_3=1$. Thus, $f(x)$ is irreducible over $\mathbb{Z}_2[x]$, and it generates an extension $L/\mathbb{Q}_2$ with $e(L/\mathbb{Q}_2)=e_1e_2e_3=4$, $f(L/\mathbb{Q}_2)=f_0f_1f_2f_3=1$. Also, $\mathrm{ind}_3(f)=0$, so that $\mathrm{ind}(f)=\mathrm{ind}_1(f)+\mathrm{ind}_2(f)+\mathrm{ind}_3(f)=3$.

If $v(a)=2$ and $v(c+2a+12)=4$, $N_3(f)$ is one-sided with slope $\lambda_3=-1$, and $R_3(f)(y)=y^2+y+1$. The type $\mathbf{t}'':=(x;-1/2,\phi_2(x);-1,\phi_3(x);-1,y^2+y+1)$ is f-complete and $\mathbf{t}_3(f)=\{\mathbf{t}''\}$. We have $e_3=1, f_3=2$. Thus, $f(x)$ is irreducible over $\mathbb{Z}_2[x]$, and it generates an extension $L/\mathbb{Q}_2$ with $e(L/\mathbb{Q}_2)=e_1e_2e_3=2$, $f(L/\mathbb{Q}_2)=f_0f_1f_2f_3=2$. Also, $\mathrm{ind}_3(f)=1$, so that $\mathrm{ind}(f)=\mathrm{ind}_1(f)+\mathrm{ind}_2(f)+\mathrm{ind}_3(f)=4$.

If $v(a) = 2$ and $v(c + 2a + 12) \geq 5$, $N_3(f)$ has two sides with slopes $\lambda_3 \leq -2$, $\lambda_3' = -1$, and $R_{\lambda_3}(f)(y) = R_{\lambda_3'}(f)(y) = y + 1$. There are two types extending $\mathbf{t}'$:

$$\mathbf{t}_1'' := (x; -1/2, \phi_2(x); -1, \phi_3(x); \lambda_3, y + 1),$$
$$\mathbf{t}_2'' := (x; -1/2, \phi_2(x); -1, \phi_3(x); -1, y + 1).$$

Both types have $e_3 = f_3 = 1$, they are both f-complete and $\mathbf{t}_3(f) = \{\mathbf{t}_1'', \mathbf{t}_2''\}$. Thus, $f(x)$ has two irreducible factors of degree two over $\mathbb{Z}_2[x]$, and both generate extensions $L/\mathbb{Q}_2$ with $e(L/\mathbb{Q}_2) = 2$, $f(L/\mathbb{Q}_2) = 1$. Finally, $\mathrm{ind}_3(f) = 1$, so that $\mathrm{ind}(f) = \mathrm{ind}_1(f) + \mathrm{ind}_2(f) + \mathrm{ind}_3(f) = 4$.

In the final design of the Montes algorithm as presented in [GMN08], this polynomial $f(x)$ is factorized already in order two. In the case $v(c + 2a + 4) = 3$ the algorithm considers $\phi_3(x) = x^2 - 2x - 2$ as a different representative of type $\mathbf{t}$, in order to avoid the increase of recursivity caused by the work in a higher order. See [GMN08, Sec.3] for more details on this optimization.

4.4. **Proof of the theorem of the index.** Our first aim is to prove Theorem 4.18 for $f(x) \in \mathcal{O}[x]$ a monic irreducible polynomial of degree n such that $\hat{\mathbf{t}}_r(f)$ is not empty. By Lemma 4.6, $\hat{\mathbf{t}}_r(f) = \{\mathbf{t}\}$ for some $\mathbf{t} = (\phi_1(x); \cdots, \phi_r(x); \lambda_r, \psi_r(y))$, and $f(x) \neq \phi_s(x)$ for $s = 1, \ldots, r$. By Lemma 2.4, $f(x)$ is of type $\mathbf{t}$ and $n = m_{r+1}\omega_{r+1}(f)$.

For $1 \leq s \leq r$, let E_s, H_s, d_s be the length, height and degree of the unique side of $N_s(f)$. Note that $E_s > 0$, because $f(x)$ is of type $\mathbf{t}$, and $0 < H_s < \infty$, because $f(x) \neq \phi_s(x)$. By the theorem of the residual polynomial, $R_{\lambda_r}(f) \sim \psi_r(y)^{a_r}$, for $a_r = \omega_{r+1}(f) > 0$.

Let $\theta \in \overline{\mathbb{Q}}_p$ be a root of $f(x)$, $L = K(\theta)$, and let us fix an embedding $\mathbb{F}_r[y]/\psi_r(y) \hookrightarrow \mathbb{F}_L$, as in (36). We introduce some notation:

$$\nu_s := v(\phi_s(\theta)) = \textstyle\sum_{i=1}^{s} e_i f_i \cdots e_{s-1} f_{s-1} \dfrac{h_i}{e_1 \ldots e_i}, \text{ for all } 1 \leq s \leq r,$$

$$\nu_{\mathbf{j}} := j_1\nu_1 + \cdots + j_r\nu_r \in \mathbb{Q}, \text{ for all } \mathbf{j} = (j_0, \ldots, j_r) \in \mathbb{N}^{r+1},$$

$$\Phi(\mathbf{j}) := \frac{\theta^{j_0}\phi_1(\theta)^{j_1} \ldots \phi_r(\theta)^{j_r}}{\pi^{\lfloor \nu_{\mathbf{j}} \rfloor}} \in \mathcal{O}_L, \text{ for all } \mathbf{j} = (j_0, \ldots, j_r) \in \mathbb{N}^{r+1},$$

$$b_0 := f_0; \quad b_s := e_s f_s, \quad \text{for } 1 \leq s < r; \quad b_r := e_r f_r a_r,$$

$$J := \{\mathbf{j} \in \mathbb{N}^{r+1} \mid 0 \leq j_s < b_s, 0 \leq s \leq r\}.$$

Lemma 4.20. *Let $\mathcal{O}_L' \subseteq \mathcal{O}_L$ be the sub-$\mathcal{O}$-module generated by $\{\Phi(\mathbf{j}) \mid \mathbf{j} \in J\}$, and denote $q = |\mathbb{F}|$. Then,*

(1) *$\mathcal{O}_L'$ is a free $\mathcal{O}$-module of rank n, with basis $\{\Phi(\mathbf{j}) \mid \mathbf{j} \in J\}$,*
(2) *$\mathcal{O}[\theta] \subseteq \mathcal{O}_L'$, and $(\mathcal{O}_L' : \mathcal{O}[\theta]) = q^{\sum_{\mathbf{j} \in J} \lfloor \nu_{\mathbf{j}} \rfloor}$.*

Proof. Clearly, $|J| = n$, and the numerators of $\Phi(\mathbf{j})$, for $\mathbf{j} \in J$, are monic polynomials of degree $0, 1, \ldots, n - 1$. Thus, the family $\{\Phi(\mathbf{j}) \mid \mathbf{j} \in J\}$ is $\mathcal{O}$-linearly independent. This proves item (1) and $\mathcal{O}[\theta] \subseteq \mathcal{O}_L'$. Finally, since the numerators of $\Phi(\mathbf{j})$, for $\mathbf{j} \in J$, are an $\mathcal{O}$-basis of $\mathcal{O}[\theta]$:

$$\mathcal{O}_L'/\mathcal{O}[\theta] \simeq \prod_{\mathbf{j} \in J} \pi^{-\lfloor \nu_{\mathbf{j}} \rfloor}\mathcal{O}/\mathcal{O} \simeq \prod_{\mathbf{j} \in J} \mathcal{O}/\pi^{\lfloor \nu_{\mathbf{j}} \rfloor}\mathcal{O},$$

and since $|\mathcal{O}/\pi^a\mathcal{O}| = q^a$, we get $(\mathcal{O}_L' : \mathcal{O}[\theta]) = q^{\sum_{\mathbf{j} \in J} \lfloor \nu_{\mathbf{j}} \rfloor}$. □

Our next step is to prove that $\mathcal{O}'_L$ is actually an order of $\mathcal{O}_L$. To this end we need a couple of auxiliary results.

Lemma 4.21. *Let* $Q(x) = \sum_{\mathbf{j}=(j_0,\dots,j_{r-1},0)\in J} a_{\mathbf{j}}\, x^{j_0}\phi_1(x)^{j_1}\dots\phi_{r-1}(x)^{j_{r-1}}$, *for some* $a_{\mathbf{j}}\in\mathcal{O}$. *Then,*

$$v(Q(\theta)) = \min\{v(a_{\mathbf{j}}) + \nu_{\mathbf{j}} \mid \mathbf{j} = (j_0,\dots,j_{r-1},0)\in J\}.$$

Proof. Since $\deg Q < m_r$, we have $v(Q(\theta)) = v_r(Q)/e_1\cdots e_{r-1}$, by Lemma 2.2 and Proposition 2.9. Let us prove that $v(a_{\mathbf{j}}) + \nu_{\mathbf{j}} \geq v_r(Q)/e_1\cdots e_{r-1}$, by induction on $r\geq 1$. If $r=1$ this is obvious because $v_1(Q) = \min\{v(a_{\mathbf{j}})\}$. Let $r\geq 2$ and suppose the result is true for $r-1$. For each $0\leq j_{r-1} < b_{r-1}$, consider the polynomial

$$Q_{j_{r-1}}(x) = \sum\nolimits_{(j_0,\dots,j_{r-2},0,0)\in J} a_{\mathbf{j}}\, x^{j_0}\phi_1(x)^{j_1}\dots\phi_{r-2}(x)^{j_{r-2}},$$

where $\mathbf{j} = (j_0,\dots,j_{r-2},j_{r-1},0)$ in each summand. Clearly,

$$Q(x) = \sum\nolimits_{0\leq j_{r-1}<b_{r-1}} Q_{j_{r-1}}(x)\phi_{r-1}(x)^{j_{r-1}}$$

is the ϕ_{r-1}-adic development of $Q(x)$. By item (4) of Proposition 2.7, the theorem of the polygon and the induction hypothesis we get

$$\begin{aligned} v_r(Q)/e_{r-1} &= \min_{0\leq j_{r-1}<b_{r-1}} \{v_{r-1}(Q_{j_{r-1}}) + j_{r-1}(v_{r-1}(\phi_{r-1}) + |\lambda_{r-1}|)\} \\ &= \min_{0\leq j_{r-1}<b_{r-1}} \{v_{r-1}(Q_{j_{r-1}}) + j_{r-1}e_1\cdots e_{r-2}\nu_{r-1}\} \\ &\leq e_1\cdots e_{r-2}\left(v(a_{\mathbf{j}}) + j_1\nu_1 + \cdots + j_{r-2}\nu_{r-2} + j_{r-1}\nu_{r-1}\right). \end{aligned}$$

□

Lemma 4.22. *Let* $\mathbf{j} = (j_0,\dots,j_r)\in\mathbb{N}^{r+1}$.

(1) *For all* $0\leq s<r$,

$$\begin{aligned}\Phi(j_0,\dots,j_{s-1},j_s+b_s,j_{s+1},\dots,j_r) &= \pi^{\delta_{\mathbf{j},s}}\Phi(j_0,\dots,j_s,j_{s+1}+1,j_{s+2},\dots,j_r) \\ &\quad + \sum\nolimits_{\mathbf{j}'=(j'_0,\dots,j'_s,0,\dots,0)\in J} c_{\mathbf{j},\mathbf{j}'}\Phi(\mathbf{j}+\mathbf{j}'),\end{aligned}$$

for some nonnegative integer $\delta_{\mathbf{j},s}$ *and some* $c_{\mathbf{j},\mathbf{j}'}\in\mathcal{O}$.

(2) $\Phi(j_0,\dots,j_{r-1},j_r+b_r) = \sum_{\mathbf{j}'\in J} c_{\mathbf{j},\mathbf{j}'}\Phi(\mathbf{j}+\mathbf{j}')$, *for some* $c_{\mathbf{j},\mathbf{j}'}\in\mathcal{O}$.

Proof. Let $0\leq s<r$, and denote $\phi_0(x) = x$, $\nu_0 = 0$, $e_0 = 1$. The polynomial $Q(x) = \phi_s(x)^{b_s} - \phi_{s+1}(x)$ has degree less than $m_{s+1} = b_s m_s$; hence, it admits a development

$$Q(x) = \sum\nolimits_{\mathbf{j}'=(j'_0,\dots,j'_s,0,\dots,0)\in J} a_{\mathbf{j}'}\, x^{j'_0}\phi_1(x)^{j'_1}\dots\phi_s(x)^{j'_s},$$

for some $a_{\mathbf{j}'}\in\mathcal{O}$. If we substitute $\phi_s(x)^{b_s} = \phi_{s+1}(x) + Q(x)$ in $\Phi(j_0,\dots,j_{s-1},j_s+b_s,j_{s+1},\dots,j_r)$ we get the identity of item (1), with

$$\delta_{\mathbf{j},s} = \lfloor \nu_{\mathbf{j}} + \nu_{s+1}\rfloor - \lfloor \nu_{\mathbf{j}} + b_s\nu_s\rfloor, \qquad c_{\mathbf{j},\mathbf{j}'} = a_{\mathbf{j}'}\,\pi^{\lfloor \nu_{\mathbf{j}}+\nu_{\mathbf{j}'}\rfloor - \lfloor \nu_{\mathbf{j}}+b_s\nu_s\rfloor}.$$

Clearly,

$$\nu_{s+1} = e_s f_s \nu_s + \frac{h_{s+1}}{e_1\cdots e_{s+1}} > b_s\nu_s,$$

so that $\delta_{\mathbf{j},s}\geq 0$. Also, $\nu_{s+1} > b_s\nu_s$ implies that $v(Q(\theta)) = b_s\nu_s$, and by the above lemma we have $v(a_{\mathbf{j}'}) + \nu_{\mathbf{j}'} \geq b_s\nu_s$. This shows that $v(c_{\mathbf{j},\mathbf{j}'})\geq 0$.

Item (2) follows by identical arguments, starting with $Q(x) = \phi_r(x)^{b_r} - f(x)$. □

Proposition 4.23. *The $\mathcal{O}$-module $\mathcal{O}'_L$ is a subring of $\mathcal{O}_L$.*

Proof. For all $\mathbf{j}, \mathbf{j}' \in J$ we have $\Phi(\mathbf{j})\Phi(\mathbf{j}') = \pi^{\delta}\Phi(\mathbf{j}+\mathbf{j}')$, with $\delta = \lfloor \nu_{\mathbf{j}} + \nu_{\mathbf{j}'} \rfloor - \lfloor \nu_{\mathbf{j}} \rfloor - \lfloor \nu_{\mathbf{j}'} \rfloor \in \{0, 1\}$. Thus, it is sufficient to check that $\Phi(\mathbf{j}) \in \mathcal{O}'_L$, for all $\mathbf{j} \in \mathbb{N}^{r+1}$.

For any $0 \leq s \leq r+1$, let $J_s := \{\mathbf{j} = (j_0, \ldots, j_r) \in \mathbb{N}^{r+1} \mid 0 \leq j_t < b_t,\ s \leq t \leq r\}$. Note that $J_0 = J$, $J_{r+1} = \mathbb{N}^{r+1}$. Consider the condition

$$(i_s) \qquad \Phi(\mathbf{j}) \in \mathcal{O}'_L, \text{ for all } \mathbf{j} \in J_s.$$

By the definition of $\mathcal{O}'_L$, the condition (i_0) holds, and our aim is to show that (i_{r+1}) holds. Thus, it is sufficient to show that (i_s) implies (i_{s+1}), for all $0 \leq s \leq r$. Let us prove this implication by induction on j_s. Take $\mathbf{j}_0 = (j_0, \ldots, j_r) \in J_{s+1}$. If $0 \leq j_s < b_s$, condition (i_{s+1}) holds for $\mathbf{j}_0$. Let $j_s \geq b_s$ and suppose that $\Phi(j'_0, \ldots, j'_{s-1}, j, j'_{s+1}, \ldots, j'_r) \in \mathcal{O}'_L$, for all $j'_0, \ldots, j'_{s-1} \in \mathbb{N}$, all $0 \leq j < j_s$, and all $0 \leq j'_t < b_t$, for $t > s$.

By item (2) of the last lemma, applied to $\mathbf{j} = (j_0, \ldots, j_{s-1}, j_s - b_s, 0, \ldots, 0)$:

$$\Phi(j_0, \ldots, j_{s-1}, j_s - b_s, 0, \ldots, 0, b_r) = \sum_{\mathbf{j}' \in J} c_{\mathbf{j},\mathbf{j}'} \Phi(\mathbf{j} + \mathbf{j}') \quad \text{if } s < r, \tag{41}$$

and $\Phi(j_0, \ldots, j_r) = \sum_{\mathbf{j}' \in J} c_{\mathbf{j},\mathbf{j}'} \Phi(\mathbf{j}+\mathbf{j}')$ if $s = r$. In both cases, the terms $\Phi(\mathbf{j}+\mathbf{j}')$ belong to $\mathcal{O}'_L$, because the s-th coordinate of $\mathbf{j}+\mathbf{j}'$ is $j_s - b_s + j'_s < j_s$. In particular, if $s = r$ we are done. If $s < r$ we apply item (1) of the last lemma to $\mathbf{j} = (j_0, \ldots, j_{s-1}, j_s - b_s, j_{s+1}, \ldots, j_r)$ and we get

$$\Phi(\mathbf{j}_0) = \pi^{\delta_{\mathbf{j},s}} \Phi(j_0, \ldots, j_s - b_s, j_{s+1} + 1, j_{s+2}, \ldots, j_r) + \sum\nolimits_{\mathbf{j}' = (j'_0, \ldots, j'_s, 0, \ldots, 0) \in J} c_{\mathbf{j},\mathbf{j}'} \Phi(\mathbf{j} + \mathbf{j}').$$

The last sum belongs to $\mathcal{O}'_L$ by the same argument as above. Thus, we need only to show that the term $\Phi(j_0, \ldots, j_s - b_s, j_{s+1} + 1, j_{s+2}, \ldots, j_r)$ belongs to $\mathcal{O}'_L$ too. If $j_{s+1} + 1 < b_{s+1}$, this follows from the induction hypothesis. If $j_{s+1} + 1 = b_{s+1}$ and $s = r - 1$, this is clear by (41). Finally, if $j_{s+1} + 1 = b_{s+1}$ and $s < r - 1$, we can apply item (1) of the last lemma again to see that it is sufficient to check that $\Phi(j_0, \ldots, j_s - b_s, 0, j_{s+2} + 1, \ldots, j_r)$ belongs to $\mathcal{O}'_L$. In this iterative process we conclude either by (41), or because we find some $j_t + 1 < b_t$. □

We still need some auxiliary lemmas. The first one is an easy remark about integral parts.

Lemma 4.24. *For all $x \in \mathbb{R}$ and $e \in \mathbb{Z}_{>0}$, we have $\sum_{0 \leq k < e} \left\lfloor \dfrac{x+k}{e} \right\rfloor = \lfloor x \rfloor$.*

Proof. The identity is obvious when x is an integer, $0 \leq x < e$, because $\left\lfloor \dfrac{x+k}{e} \right\rfloor = 1$ for the x values of k such that $e - x \leq k < e$, and it is zero otherwise.

Write $x = n + \epsilon$, with $n = \lfloor x \rfloor$ and $0 \leq \epsilon < 1$; clearly, $\lfloor (x+k)/e \rfloor = \lfloor (n+k)/e \rfloor$, because $\epsilon/e < 1/e$. Consider the division with remainder, $n = Qe + r$, with $0 \leq r < e$. Then,

$$\sum_{0 \leq k < e} \left\lfloor \frac{n+k}{e} \right\rfloor = \sum_{0 \leq k < e} \left(Q + \left\lfloor \frac{r+k}{e} \right\rfloor \right) = eQ + r = n.$$

□

Lemma 4.25. *Take $e_0 = 1$, $h_0 = 0$ by convention. Every $\mathbf{j} \in \mathbb{N}^{r+1}$ can be written uniquely as $\mathbf{j} = \mathbf{j}' + \mathbf{j}''$, with $\mathbf{j}'$, $\mathbf{j}''$ belonging respectively to the two sets:*

$$J' := \{\mathbf{j}' = (j'_0, \dots, j'_r) \in \mathbb{N}^{r+1} \mid 0 \le j'_s < e_s, \text{ for all } 0 \le s \le r\} \subseteq J,$$
$$J'' := \{\mathbf{j}'' = (j''_0, \dots, j''_r) \in \mathbb{N}^{r+1} \mid j''_s \equiv 0 \pmod{e_s}, \text{ for all } 0 \le s \le r\}.$$

Then, for any $\mathbf{j}'' = (k_0, e_1k_1, \dots, e_rk_r) \in J''$, there is a unique $\mathbf{j}' = (j'_0, \dots, j'_r) \in J'$ such that $v(\Phi(\mathbf{j}' + \mathbf{j}'')) = 0$. Moreover, $j'_r = 0$, and j'_s depends only on $k_{s+1}, \dots, k_r$, for $0 \le s < r$.

Proof. For any $\mathbf{j} \in \mathbb{N}^{r+1}$ denote by $\lambda_{\mathbf{j}}$ the positive integer

$$\lambda_{\mathbf{j}} := e_1 \cdots e_r\, \nu_{\mathbf{j}} = \sum_{s=1}^{r} j_s \sum_{i=1}^{s} e_i f_i \cdots e_{s-1} f_{s-1} e_{i+1} \cdots e_r h_i$$
$$= \sum_{i=1}^{r} \left(\sum_{t=i}^{r} j_t e_i f_i \cdots e_{t-1} f_{t-1} \right) e_{i+1} \cdots e_r h_i.$$

Clearly,

$$v(\Phi(\mathbf{j})) = \nu_{\mathbf{j}} - \lfloor \nu_{\mathbf{j}} \rfloor = \frac{\lambda_{\mathbf{j}}}{e_1 \cdots e_r} - \Big\lfloor \frac{\lambda_{\mathbf{j}}}{e_1 \cdots e_r} \Big\rfloor. \tag{42}$$

Thus, $v(\Phi(\mathbf{j})) = 0$ if and only if $\lambda_{\mathbf{j}} \equiv 0 \pmod{e_1 \cdots e_r}$. Now define, for each $0 \le s \le r$,

$$\lambda_{\mathbf{j},s} := j_s h_s e_{s+1} \cdots e_r + \sum_{i=s+1}^{r} \left(\sum_{t=i}^{r} j_t e_i f_i \cdots e_{t-1} f_{t-1} \right) e_{i+1} \cdots e_r h_i.$$

Note that $\lambda_{\mathbf{j},s}$ depends only on $j_s, \dots, j_r$, and $\lambda_{\mathbf{j},0} = \lambda_{\mathbf{j}}$, $\lambda_{\mathbf{j},r} = j_r h_r$. Clearly,

$$\lambda_{\mathbf{j},s} - \lambda_{\mathbf{j},s+1} = j_s h_s e_{s+1} \cdots e_r + \left(\sum_{t=s+2}^{r} j_t e_{s+1} f_{s+1} \cdots e_{t-1} f_{t-1} \right) e_{s+2} \cdots e_r h_{s+1},$$

for all $0 \le s < r$. In particular, $\lambda_{\mathbf{j},s} \equiv \lambda_{\mathbf{j},s+1} \pmod{e_{s+1} \cdots e_r}$, and

$$\lambda_{\mathbf{j}} \equiv 0 \pmod{e_1 \cdots e_r} \iff \lambda_{\mathbf{j},s} \equiv 0 \pmod{e_s \cdots e_r}, \text{ for all } 1 \le s \le r.$$

The condition $\lambda_{\mathbf{j},r} \equiv 0 \pmod{e_r}$ is equivalent to $j_r \equiv 0 \pmod{e_r}$. On the other hand, for $1 \le s < r$, the condition $\lambda_{\mathbf{j},s} \equiv 0 \pmod{e_s \cdots e_r}$ is equivalent to

$$\lambda_{\mathbf{j},s+1} \equiv 0 \pmod{e_{s+1} \cdots e_r}, \text{ and}$$
$$j_s h_s + \big(\textstyle\sum_{t=s+2}^{r} j_t (f_{s+1} \cdots f_{t-1})(e_{s+2} \cdots e_{t-1}) \big)\, h_{s+1} + \dfrac{\lambda_{\mathbf{j},s+1}}{e_{s+1} \cdots e_r} \equiv 0 \pmod{e_s}.$$

Thus, the class of j_s modulo e_s is uniquely determined, and it depends only on $j_{s+1}, \dots, j_r$. □

Corollary 4.26. *Let $\kappa = (k_0, \dots, k_r) \in \mathbb{N}^{r+1}$, and let $\mathbf{j} = \mathbf{j}' + (k_0, e_1k_1, \dots, e_rk_r)$, where $\mathbf{j}'$ is the unique element in J' such that $v(\Phi(\mathbf{j})) = 0$. Then,*

$$\Phi(\mathbf{j}) = \theta^{k_0} \gamma_1(\theta)^{k_1} \cdots \gamma_r(\theta)^{k_r} \gamma_1(\theta)^{i_1} \cdots \gamma_{r-1}(\theta)^{i_{r-1}},$$

for some integers $i_1, \dots, i_{r-1}$. Moreover, each i_s depends only on $k_{s+1}, \dots, k_r$.

Proof. By Lemma 4.25, $\mathbf{j} = (k_0, j_1' + e_1k_1, \dots, j_{r-1}' + e_{r-1}k_{r-1}, e_rk_r)$. By (17),

$$\gamma_s(\theta)^{k_s} = \pi^{n_{s,0}}\phi_1(\theta)^{n_{s,1}} \cdots \phi_s(\theta)^{e_sk_s},$$

for all $1 \le s \le r$, with integers $n_{s,i}$ that depend only on k_s. Hence,

$$\Phi(\mathbf{j})\theta^{-k_0}\gamma_1(\theta)^{-k_1} \cdots \gamma_r(\theta)^{-k_r} = \pi^{n_0}\phi_1(\theta)^{n_1} \cdots \phi_{r-1}(\theta)^{n_{r-1}},$$

for integers n_s that depend only on j_s' and $k_{s+1}, \dots, k_r$; hence they depend only on $k_{s+1}, \dots, k_r$. By Corollary 3.2, $v(\pi^{n_0}\phi_1(\theta)^{n_1} \cdots \phi_{r-1}(\theta)^{n_{r-1}}) = 0$, and by Propositions 2.9 and 2.15 we have $v_r(\pi^{n_0}\phi_1(x)^{n_1} \cdots \phi_{r-1}(x)^{n_{r-1}}) = 0$. By Lemma 2.16, this rational function can be expressed as a product $\gamma_1(x)^{i_1} \cdots \gamma_{r-1}(x)^{i_{r-1}}$, with integers $i_1, \dots, i_{r-1}$ such that each i_s depends only on $n_s, \dots, n_{r-1}$, that is, on $k_{s+1}, \dots, k_r$. □

Corollary 4.27. *Let $\mathbf{j}_1 = \mathbf{j}_1' + \mathbf{j}''$, $\mathbf{j}_2 = \mathbf{j}_2' + \mathbf{j}''$, for some $\mathbf{j}_1', \mathbf{j}_2' \in J'$, $\mathbf{j}'' \in J''$. Then, $v(\Phi(\mathbf{j}_1)) = v(\Phi(\mathbf{j}_2))$ if and only if $\mathbf{j}_1 = \mathbf{j}_2$. In particular,*

$$\{v(\Phi(\mathbf{j})) \mid \mathbf{j} \in J'\} = \{k/e_1 \cdots e_r \mid 0 \le k < e_1 \cdots e_r\}.$$

Proof. Let $\mathbf{j}_1 = (j_{1,0}, \dots j_{1,r})$, $\mathbf{j}_2 = (j_{2,0}, \dots j_{2,r})$. With the notation of Lemma 4.25, (42) shows that

$$\begin{aligned} v(\Phi(\mathbf{j}_1)) = v(\Phi(\mathbf{j}_2)) &\iff \lambda_{\mathbf{j}_1} \equiv \lambda_{\mathbf{j}_2} \pmod{e_1 \cdots e_r} \\ &\iff \lambda_{\mathbf{j}_1,s} \equiv \lambda_{\mathbf{j}_2,s} \pmod{e_s \cdots e_r}, \text{ for all } 1 \le s \le r. \end{aligned}$$

For $s = r$ this is equivalent to $j_{1,r} = j_{2,r}$. Also, if $j_{1,t} = j_{2,t}$ for all $t > s$, then $\lambda_{\mathbf{j}_1,s} - \lambda_{\mathbf{j}_2,s} = (j_{1,s} - j_{2,s})h_se_{s+1} \cdots e_r$, so that $\lambda_{\mathbf{j}_1,s} \equiv \lambda_{\mathbf{j}_2,s} \pmod{e_s \cdots e_r}$ is equivalent to $j_{1,s} = j_{2,s}$.

Finally, it is clear that $|J'| = e_1 \cdots e_r$, and we have just shown that the elements $v(\Phi(\mathbf{j}))$, $\mathbf{j} \in J'$, take $e_1 \cdots e_r$ different values, all of them contained in the set $\{k/e_1 \cdots e_r \mid 0 \le k < e_1 \cdots e_r\}$ by (42). □

Proposition 4.28. *If $\mathbf{t}$ is f-complete, then $\mathcal{O}_L' = \mathcal{O}_L$. Moreover, the family of all $\Phi(\mathbf{j})\Phi(\mathbf{j}')$, for $\mathbf{j} \in J_0 := \{\mathbf{j} \in J \mid v(\Phi(\mathbf{j})) = 0\}$ and $\mathbf{j}' \in J'$, is an $\mathcal{O}$-basis of $\mathcal{O}_L$. Finally, if L/K is ramified, there exists $\mathbf{j}' \in J'$ such that $\mathfrak{m}_L = \Phi(\mathbf{j}')\mathcal{O}_L$.*

Proof. Corollary 3.8 shows that $e(L/K) = e_1 \cdots e_r$, $f(L/K) = f_0f_1 \cdots f_r$. By Corollary 4.27, we have $\{v_L(\Phi(\mathbf{j}')) \mid \mathbf{j}' \in J'\} = \{0, 1, \dots, e(L/K)-1\}$; in particular, if $e(L/K) > 1$, there exists $\mathbf{j}' \in J'$ such that $v_L(\Phi(\mathbf{j}')) = 1$. By Lemma 4.25, $|J_0| = f_0f_1 \cdots f_r = \dim_{\mathbb{F}_K} \mathbb{F}_L$, and each $\mathbf{j} \in J_0$ is parameterized by a sequence $(k_0, \dots, k_r)$, with $0 \le k_s < f_s$ for all $0 \le s \le r$. By item (4) of Proposition 3.5, $\mathbb{F}_L = \mathbb{F}_K(\overline{\gamma_0(\theta)}, \dots, \overline{\gamma_r(\theta)})$, where $\gamma_0(x) := x$. Recall that $z_i = \overline{\gamma_i(\theta)}$ for all $0 \le i \le r$, under our identification of $\mathbb{F}_{r+1} := \mathbb{F}_r[y]/\psi_r(y)$ with $\mathbb{F}_L$.

By Corollary 4.26,

$$\overline{\Phi(\mathbf{j})} = z_0^{k_0}z_1^{k_1+i_1} \cdots (z_{r-1})^{k_{r-1}+i_{r-1}}z_r^{k_r} = z_0^{k_0}z_1^{k_1}\Gamma_2(k_2, \dots, k_r) \cdots \Gamma_r(k_r),$$

where $\Gamma_s(k_s, \dots, k_r) := z_s^{k_s}(z_{s-1})^{i_{s-1}}$, for $s \ge 2$. Now, the family of all $\overline{\Phi(\mathbf{j})}$ for $\mathbf{j} \in J_0$ is an $\mathbb{F}_K$-basis of $\mathbb{F}_L$. In fact, the set of all $\Gamma_r(k_r)$ for $0 \le k_r < f_r$ is an $\mathbb{F}_r$-basis of $\mathbb{F}_L = \mathbb{F}_{r+1}$, because they are obtained from the basis $z_r^{k_r}$, just by multiplying every element by the nonzero scalar $z_{r-1}^{i_{r-1}} \in \mathbb{F}_r$, which depends only on k_r. Then, the set of all $\Gamma_{r-1}(k_{r-1}, k_r)\Gamma_r(k_r)$ for $0 \le k_{r-1} < f_{r-1}$, $0 \le k_r < f_r$, is an $\mathbb{F}_{r-1}$-basis of $\mathbb{F}_L$, because they are obtained from the basis $(z_{r-1})^{k_{r-1}}\Gamma_r(k_r)$, just

by multiplying every element by the nonzero scalar $z_{r-2}^{i_{r-2}} \in \mathbb{F}_{r-1}$, which depends only on k_{r-1}, k_r, etc.

Therefore, the $e(L/K)f(L/K)$ elements $\Phi(\mathbf{j})\Phi(\mathbf{j}')$, $\mathbf{j} \in J_0$, $\mathbf{j}' \in J'$, are an $\mathcal{O}$-basis of $\mathcal{O}_L$. By Proposition 4.23, all these elements are contained in $\mathcal{O}'_L$, and we have necessarily $\mathcal{O}'_L = \mathcal{O}_L$. □

Proof of Theorem 4.18. Suppose first that $f(x) \in \mathcal{O}[x]$ is a monic irreducible polynomial, such that $\hat{\mathbf{t}}_r(f) = \{\mathbf{t}\}$. In this case we have built an order $\mathcal{O}[\theta] \subseteq \mathcal{O}'_L \subseteq \mathcal{O}_L$, such that (for $q = |\mathbb{F}|$):

$$(\mathcal{O}_L \colon \mathcal{O}[\theta]) = q^{\mathrm{ind}(f)}, \quad (\mathcal{O}'_L \colon \mathcal{O}[\theta]) = q^{\sum_{\mathbf{j}\in J}\lfloor \nu_{\mathbf{j}}\rfloor}, \tag{43}$$

the last equality by Lemma 4.20. Therefore, in order to prove item (1) of Theorem 4.18, it is sufficient to show that

$$\sum_{\mathbf{j}\in J}\lfloor \nu_{\mathbf{j}}\rfloor = f_0 \sum_{\mathbf{j}=(0,j_1,\dots,j_r)\in J} \lfloor \nu_{\mathbf{j}}\rfloor = \mathrm{ind}_1(f) + \cdots + \mathrm{ind}_r(f). \tag{44}$$

Let us prove this identity by induction on $r \geq 1$. For $r = 1$ we have $\mathrm{ind}_1(f) = f_0 \,\mathrm{ind}(N_1(f))$, and $j\nu_1 = j|\lambda_1| = y_j(N_1(f))$; thus, (44) was proved already in (40). From now on, let $r \geq 2$. Both sides of the identity depend only on a_r, f_0 and the vectors $\mathbf{e} = (e_1, \dots, e_r)$, $\mathbf{f} = (f_1, \dots, f_{r-1})$, $\mathbf{h} = (h_1, \dots, h_r)$. Recall that

$$\nu_s = \nu_s(\mathbf{e}, \mathbf{f}, \mathbf{h}) := \sum_{i=1}^{s} e_i f_i \cdots e_{s-1} f_{s-1} \frac{h_i}{e_1 \dots e_i}.$$

If we denote $\mathbf{e}' = (e_2, \dots, e_r)$, $\mathbf{f}' = (f_2, \dots, f_{r-1})$, $\mathbf{h}' = (h_2, \dots, h_r)$, it is easy to check that, for every $2 \leq s \leq r$:

$$\nu_s(\mathbf{e}, \mathbf{f}, \mathbf{h}) - \frac{m_s}{m_2} f_1 h_1 = \frac{1}{e_1} \nu_{s-1}(\mathbf{e}', \mathbf{f}', \mathbf{h}'). \tag{45}$$

Let us show that the identity

$$f_0 \sum_{\mathbf{j}=(0,j_1,\dots,j_r)\in J} \Big\lfloor \sum_{s=1}^{r} j_s \nu_s(\mathbf{e}, \mathbf{f}, \mathbf{h}) \Big\rfloor = \mathrm{ind}_1(f) + \cdots + \mathrm{ind}_r(f)$$

holds for any choice of a_r, f_0 and $\mathbf{e}, \mathbf{f}, \mathbf{h}$, under the assumption that the same statement is true for $r - 1$. Write $j_1 = je_1 + k$, with $0 \leq j < f_1$, $0 \leq k < e_1$, and let $0 \leq s_k < e_1$ be determined by $kh_1 \equiv s_k \pmod{e_1}$. Then, by (45),

$$\begin{aligned}
\Big\lfloor \sum_{s=1}^{r} j_s \nu_s(\mathbf{e}, \mathbf{f}, \mathbf{h}) \Big\rfloor &= \Big\lfloor jh_1 + k\frac{h_1}{e_1} + \sum_{s=2}^{r} j_s \nu_s(\mathbf{e}, \mathbf{f}, \mathbf{h}) \Big\rfloor \\
&= \sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + jh_1 + \Big\lfloor k\frac{h_1}{e_1} + \frac{1}{e_1} \sum_{s=2}^{r} j_s \nu_{s-1}(\mathbf{e}', \mathbf{f}', \mathbf{h}') \Big\rfloor \\
&= \sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + jh_1 + \Big\lfloor k\frac{h_1}{e_1} \Big\rfloor + \Big\lfloor \frac{s_k}{e_1} + \frac{1}{e_1} \sum_{s=1}^{r-1} j_{s+1} \nu_s(\mathbf{e}', \mathbf{f}', \mathbf{h}') \Big\rfloor.
\end{aligned}$$

Therefore, it is sufficient to check the two identities:

$$f_0 \sum_{\substack{(0,0,j_2,\dots,j_r)\in J \\ 0\le j<f_1,\,0\le k<e_1}} \left(\sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + j h_1 + \left\lfloor k\frac{h_1}{e_1}\right\rfloor\right) = \operatorname{ind}_1(f),$$

$$f_0 \sum_{\substack{(0,0,j_2,\dots,j_r)\in J \\ 0\le j<f_1,\,0\le k<e_1}} \left\lfloor \frac{s_k}{e_1} + \frac{1}{e_1}\sum_{s=1}^{r-1} j_{s+1}\nu_s(\mathbf{e}',\mathbf{f}',\mathbf{h}')\right\rfloor = \operatorname{ind}_2(f)+\cdots+\operatorname{ind}_r(f).$$

The integers $0 \le i < (n/f_0)$ are in 1-1 correspondence with the vectors $(0, j_1, \dots, j_r)$ in J via

$$i = j_1 + j_2(m_2/f_0) + \cdots + j_r(m_r/f_0).$$

Therefore, the left-hand side of the first identity is equal to $f_0 \sum_{0\le i<(n/f_0)} \lfloor i\frac{h_1}{e_1}\rfloor$, which is equal to $\operatorname{ind}_1(f)$ by (40). The second identity follows from the induction hypothesis. In fact, the set $\{s_k \mid 0 \le k < e_1\}$ coincides with $\{0, 1, \dots, e_1 - 1\}$, and by Lemma 4.24 the left-hand side of the identity is equal to

$$f_0 f_1 \sum_{(0,0,j_2,\dots,j_r)\in J} \left\lfloor \sum_{s=1}^{r-1} j_{s+1}\nu_s(\mathbf{e}',\mathbf{f}',\mathbf{h}')\right\rfloor.$$

Let us now prove the second part of the theorem. Suppose that $\operatorname{ind}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_r(f)$. Let $\phi_{r+1}(x)$ be the representative of $\mathbf{t}$; if $f(x) = \phi_{r+1}(x)$, we have directly $\operatorname{ind}_{r+1}(f) = 0$ because $N_{r+1}(f)$ is a side of slope $-\infty$. If $f(x) \ne \phi_{r+1}(x)$, then $\hat{\mathbf{t}}_{r+1}(f) \ne \emptyset$ by Lemma 4.6, and $\operatorname{ind}_{r+1}(f) = 0$ by item (1) of the theorem in order $r + 1$.

Conversely, suppose that $\operatorname{ind}_{r+1}(f) = 0$. Lemma 4.16 shows that all types in $\mathbf{t}_{r+1}(f)$ are f-complete, and Lemma 4.5 shows that all types in $\hat{\mathbf{t}}_{r+1}(f)$ are f-complete too. If $\mathbf{t}$ is f-complete, we have $\mathcal{O}'_L = \mathcal{O}_L$ by Proposition 4.28, and we get $\operatorname{ind}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_r(f)$, by (43) and (44). If $\mathbf{t}$ is not f-complete, we have in particular $f(x) \ne \phi_{r+1}(x)$, and we can extend $\mathbf{t}$ in a unique way to a type $\mathbf{t}' = (\mathbf{t}; \lambda_{r+1}, \psi_{r+1}(y))$ of order $r + 1$, which is f-complete by our assumption. By Proposition 4.28, (43) and (44), applied to $\mathbf{t}'$ in order $r + 1$, we get $\operatorname{ind}(f) = \operatorname{ind}_1(f)+\cdots+\operatorname{ind}_r(f)+\operatorname{ind}_{r+1}(f)$ as above. Since $\operatorname{ind}_{r+1}(f) = 0$, we have $\operatorname{ind}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_r(f)$, as desired. This ends the proof of the theorem in the particular case we were dealing with.

Let us now prove the theorem in the other instances where $f(x)$ is irreducible: $f(x) = \phi_s(x)$ for the representative $\phi_s(x)$ of some type of order $s - 1 \le r - 1$ (cf. Lemma 4.6). In this case, $\operatorname{ind}_s(f) = 0$ because $N_s(f)$ is a side of slope $-\infty$. Also, if $s < r$ we have $\operatorname{ind}_{s+1}(f) = \cdots = \operatorname{ind}_r(f) = 0$ by definition, because $\mathbf{t}_s(f) = \emptyset$ by Lemma 4.6. Since $f(x) \ne \phi_1(x), \dots, \phi_{s-1}(x)$, we have $\hat{\mathbf{t}}_{s-1}(f) \ne \emptyset$ and we can apply the theorem in order $s - 1$:

$$\operatorname{ind}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_{s-1}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_r(f).$$

This proves both statements of the theorem and it ends the proof of the theorem when $f(x)$ is irreducible.

In the general case, if $f(x) = F_1(x) \cdots F_k(x)$ is the factorization of $f(x)$ into a product of monic irreducible polynomials, we have by definition

$$\operatorname{ind}(f) = \sum_{i=1}^{k} \operatorname{ind}(F_i) + \sum_{1 \le i < j \le k} v(\operatorname{Res}(F_i, F_j)).$$

By Lemma 4.17, an analogous relationship holds for every $\operatorname{ind}_s(f)$, $1 \le s \le r$. Hence, item (1) of the theorem holds by the theorem applied to each $\operatorname{ind}(F_i)$, and by Theorem 4.10. Let us now prove item (2). By Lemma 4.17, $\operatorname{ind}_{r+1}(f) = 0$ if and only if $\operatorname{ind}_{r+1}(F_i) = 0$ and $\operatorname{Res}_{r+1}(F_i, F_j) = 0$, for all i and all $j \neq i$. By the theorem in the irreducible case and Theorem 4.10, this is equivalent to $\operatorname{ind}(f) = \operatorname{ind}_1(f) + \cdots + \operatorname{ind}_r(f)$. □

References

[Bau07] M. Bauer, *Zur allgemeinen Theorie der algebraischen Grössen*, Journal für die reine und angewandte Mathematik **132**(1907), pp. 21–32.

[Ded78] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen **23**(1878), pp. 1–23.

[Gua97] J. Guàrdia, *Geometria aritmètica en una família de corbes de gènere tres*, Tesi Doctoral, Universitat de Barcelona 1997.

[GMN08] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, arXiv:0807.4065v2[math.NT].

[GMN09] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, arXiv: 0902.3428v1[math.NT].

[Mon99] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, Tesi Doctoral, Universitat de Barcelona, 1999.

[McL36] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society, **40**(1936), pp. 363–395. MR1501879

[McL36b] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2**(1936), pp. 492–510. MR1545943

[Ore23] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica **44**(1923), pp. 219–314. MR1555187

[Ore24] Ø. Ore, *Weitere Untersuchungen zur Theorie der algebraischen Körper*, Acta Mathematica **45**(1924-25), pp. 145–160.

[Ore25] Ø. Ore, *Bestimmung der Diskriminanten algebraischer Körper*, Acta Mathematica **45**(1925), pp. 303–344. MR1555198

[Ore26] Ø. Ore, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, Mathematische Annalen **96**(1926), pp. 313–352.

[Ore28] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen **99**(1928), pp. 84–117. MR1512440

Departament de Matemàtica Aplicada IV, Escola Politècnica Superior d'Enginyera de Vilanova i la Geltrú, Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú, Catalonia, Spain

E-mail address: guardia@ma4.upc.edu

Departament de Ciències Econòmiques i Socials, Facultat de Ciències Socials, Universitat Abat Oliba CEU, Bellesguard 30, E-08022 Barcelona, Catalonia, Spain

E-mail address: montes3@uao.es

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia, Spain

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