ACTA ARITHMETICA
145.1 (2010)

Okutsu invariants and Newton polygons

by

Jordi Guàrdia (Vilanova i la Geltrú), Jesús Montes (Barcelona) and
Enric Nart (Barcelona)

1. Introduction. Let K be a local field with perfect residue class field, $\mathcal{O}$ its ring of integers, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$, and $v\colon \overline{K}^* \to \mathbb{Q}$ the canonical extension of the discrete valuation of K to an algebraic closure of K. Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, $\theta \in \overline{K}$ a root of $F(x)$, and $L = K(\theta)$. Kōsaku Okutsu [Oku] attached to $F(x)$ a family of monic irreducible separable polynomials, $F_1(x), \dots, F_r(x) \in \mathcal{O}[x]$, called the *primitive divisor polynomials* of $F(x)$. Take $F_0(x) = 1$. For each $1 \le i \le r$, $\deg F_i$ is minimal among all monic irreducible polynomials $g(x) \in \mathcal{O}[x]$ satisfying $v(g(\theta))/\deg g > v(F_{i-1}(\theta))/\deg F_{i-1}$, and $v(F_i(\theta))$ is maximal among all polynomials having this minimal degree. Let us call the chain $[F_1, \dots, F_r]$ an *Okutsu frame* of $F(x)$, and let $K_1, \dots, K_r$ be the respective extensions of K determined by these polynomials. The polynomials $F_1, \dots, F_r$ are not uniquely determined, but many of their invariants, like the residual degrees $f(K_i/K)$ and the ramification indices $e(K_i/K)$, depend only on $F(x)$, and they are linked to some arithmetical invariants of the extension L/K and its subextensions (Corollaries 2.8 and 2.9).

In this paper we find a natural characterization of Okutsu frames in terms of Newton polygons of higher order [HN]. More precisely, a family $[F_1, \dots, F_r]$ of monic irreducible separable polynomials in $\mathcal{O}[x]$ is an Okutsu frame of $F(x)$ if and only if (Theorems 3.5 and 3.9):

(1) $F_1(x)$ is irreducible modulo $\mathfrak{m}$ and divides $F(x)$ modulo $\mathfrak{m}$.
(2) $\deg F_1(x) < \cdots < \deg F_r(x) < \deg F(x)$.
(3) For each $1 \le i < r$, the Newton polygons of ith order (with respect to $[F_1, \dots, F_i]$), $N_i(F)$ and $N_i(F_{i+1})$, are one-sided and they have the same negative slope.

2010 *Mathematics Subject Classification*: Primary 11S15; Secondary 11Y05, 11Y40.
Key words and phrases: local factorization, local field, Montes algorithm, Okutsu approximation, Newton polygon, Okutsu frame.

DOI: 10.4064/aa145-1-5

(4) For each $1 \le i < r$, the residual polynomial of ith order, $R_i(F_{i+1})$, is irreducible and, up to a multiplicative constant, $R_i(F)$ is a power of $R_i(F_{i+1})$.
(5) $N_r(F)$ is one-sided of negative slope and $R_r(F)$ is irreducible.

As a consequence, we get closed formulas for the invariants $v(F_i(\theta))$ in terms of combinatorial data attached to these Newton polygons (Corollary 3.6), and we find new Okutsu invariants of $F(x)$ (Corollary 3.7). Newton polygons can also be used to construct *Okutsu approximations* to $F(x)$; these are monic irreducible polynomials sufficiently close to $F(x)$ to share all its Okutsu invariants (Lemma 4.3). In the tamely ramified case any Okutsu approximation to $F(x)$ generates the same extension of K (Proposition 4.4).

Moreover, this characterization of the Okutsu frames provides the following reinterpretation of the Montes algorithm [HN], [GMNa]: at the input of a monic separable polynomial $f(x) \in \mathcal{O}[x]$, the algorithm computes an Okutsu frame and an Okutsu approximation to each irreducible factor of $f(x)$. This widens the scope of applications of this algoritm, as a tool to compute the arithmetic information about the irreducible factors of $f(x)$, contained in their Okutsu invariants. For instance, this perspective yields a measure of the precision of an Okutsu approximation (Lemma 4.5), that makes it possible to slightly modify the algorithm in order to find approximations to the irreducible factors with prescribed precision (Section 4.3).

In another direction, the results of this paper open the door to a new construction of the prime ideals of the number field M determined by a monic irreducible polynomial $f(x)$ with integer coefficients. For any prime number p, the Montes algorithm computes Okutsu frames and Okutsu approximations to the different p-adic irreducible factors of $f(x)$. This can be interpreted as a canonical parameterization of the prime ideals of M dividing p, in terms of Okutsu invariants that depend only on the polynomial $f(x)$. This parameterization is faithful enough to enable one to carry out the basic tasks concerning ideals in number fields, without the necessity of either factorizing the discriminant of $f(x)$ or constructing an integral basis of the ring of integers of the number field. We hope to develop these ideas in a forthcoming paper [GMNb].

In the same vein, the divisors of a curve C over a finite field can be also parameterized in terms of Okutsu invariants that depend only on the defining equation of the curve. This enables one to compute the divisor of a function, or to construct a function with zeros and poles of a prescribed order at a finite number of places, avoiding the computation of integral bases of subrings of the function field of C.

2. Okutsu frames. In this section we review and generalize Okutsu's results [Oku]. The aim of the generalization is to facilitate the application of these results to the situation of Section 4.

Let K be a local field, $\mathcal{O}$ its ring of integers, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$, and $\mathbb{F}$ the residue field, which is supposed to be perfect. Let $\overline{K}$ be a fixed algebraic closure of K, and $v\colon \overline{K}^* \to \mathbb{Q}$ the canonical extension of the discrete valuation of K. We extend the valuation v to the ring $\mathcal{O}[x]$ in a natural way:

$$v\colon \mathcal{O}[x] \to \mathbb{Z}_{\geq 0} \cup \{\infty\}, \qquad v(b_0 + \cdots + b_r x^r) := \min\{v(b_j) \mid 0 \leq j \leq r\}. \tag{2.1}$$

For any finite extension M of K we denote by $\mathcal{O}_M$ the ring of integers of M, and for any $\eta \in \overline{K}$ we define $\deg_M \eta := [M(\eta) : M]$.

We fix throughout the section a monic irreducible polynomial $F(x) \in \mathcal{O}[x]$ of degree n, a root $\theta \in \overline{K}$ of $F(x)$, and the field $L = K(\theta)$.

2.1. Okutsu invariants. Consider the two sequences

$$m_0 := 1 \leq m_1 < \cdots < m_r < m_{r+1} = n,$$
$$\mu_0 := 0 < \mu_1 < \cdots < \mu_r < \mu_{r+1} = \infty,$$

the first one of positive integers, the second one of nonnegative rational numbers (and infinity), defined in the following recurrent way for $i \geq 1$:

$$m_i := \min\{\deg_K \eta \mid \eta \in \overline{K},\, v(\theta - \eta) > \mu_{i-1}\},$$
$$\mu_i := \max\{v(\theta - \eta) \mid \eta \in \overline{K},\, \deg_K \eta = m_i\}.$$

These numbers do not depend on the choice of θ among the roots of $F(x)$.

Definition 2.1. For $1 \leq i \leq r$, choose $\alpha_i \in \overline{K}$, separable over K, such that $\deg_K \alpha_i = m_i$, $v(\theta - \alpha_i) = \mu_i$. Let $F_i(x) \in \mathcal{O}[x]$ be the minimal polynomial of α_i, and denote $K_i = K(\alpha_i)$. The chain $[F_1, \ldots, F_r]$ of monic irreducible separable polynomials in $\mathcal{O}[x]$ is called an *Okutsu frame* of $F(x)$. The length r of an Okutsu frame is called the *depth* of $F(x)$, and it will be denoted $\operatorname{depth}(F)$.

The polynomials $F_1, \ldots, F_r$ that constitute an Okutsu frame of $F(x)$ are not uniquely determined. However, they are canonical in some sense, since many of their invariants (like the sequences $m_1 < \cdots < m_r$ and $\mu_1 < \cdots < \mu_r$) depend only on $F(x)$. More generally, an invariant of the family $F_1, \ldots, F_r, F$ will be called an *Okutsu invariant* if it does not depend on the choice of the Okutsu frame $[F_1, \ldots, F_r]$. Thus, although the frame might be involved in their computation, they are actually invariants of $F(x)$. Corollaries 2.8, 2.14 and 3.7 present more Okutsu invariants of $F(x)$.

Lemma 2.2. *For any $h(x) \in \mathcal{O}[x]$, we have $v(h(\theta)) = 0$ if and only if $h(x)$ is relatively prime to $F(x)$ modulo $\mathfrak{m}$.*

Proof. If there exist $a(x), b(x) \in \mathcal{O}[x]$ such that $a(x)F(x) + b(x)h(x) \in 1 + \mathfrak{m}[x]$, then clearly $v(h(\theta)) = 0$.

By the Hensel lemma, $F(x) \equiv F_1(x)^\ell \pmod{\mathfrak{m}}$ for some $F_1(x) \in \mathcal{O}[x]$ which is irreducible modulo $\mathfrak{m}$. Clearly, $v(F_1(\theta)) > 0$, and if $F_1(x)$ divides $h(x)$ modulo $\mathfrak{m}$, we have $v(h(\theta)) > 0$ too. ∎

COROLLARY 2.3.

(i) *A monic irreducible polynomial $F(x) \in \mathcal{O}[x]$ has depth zero if and only if $F(x)$ is irreducible modulo $\mathfrak{m}$. In this case, the Okutsu frames of $F(x)$ are all empty.*
(ii) *If $[F_1, \dots, F_r]$ is an Okutsu frame of $F(x)$, then $F_1(x)$ is irreducible modulo $\mathfrak{m}$, $m_1 \mid n$, and $F(X) \equiv F_1(x)^{n/m_1} \pmod{\mathfrak{m}}$.* ∎

LEMMA 2.4. *Let $[F_1, \dots, F_r]$ be an Okutsu frame of $F(x)$. For some index, $1 \le i \le r+1$, let $\alpha \in \overline{K}$ be an algebraic integer satisfying $\deg_K \alpha = m_i$, $v(\theta - \alpha) > \mu_{i-1}$, and let $G(x)$ be the minimal polynomial of α over K. Then $[F_1, \dots, F_{i-1}]$ is an Okutsu frame of $G(x)$.*

Proof. Since the sequence $\mu_j = v(\theta - \alpha_j)$ is strictly increasing,

$$v(\alpha - \alpha_j) = \min\{v(\alpha - \theta), v(\theta - \alpha_j)\} = \mu_j, \quad \forall 1 \le j < i.$$

Now, for all $1 \le j < i$ and all $\eta \in \overline{K}$ we have

$$v(\alpha - \eta) > \mu_{j-1} \;\Rightarrow\; v(\theta - \eta) > \mu_{j-1} \;\Rightarrow\; \deg_K \eta \ge m_j,$$
$$\deg_K \eta = m_j \;\Rightarrow\; v(\theta - \eta) \le \mu_j \;\Rightarrow\; v(\alpha - \eta) \le \mu_j. \ \blacksquare$$

COROLLARY 2.5. *Let $[F_1, \dots, F_r]$ be an Okutsu frame of $F(x)$. Then, for all $1 \le i \le r$, $[F_1, \dots, F_{i-1}]$ is an Okutsu frame of $F_i(x)$. In particular,* $\operatorname{depth}(F_i) = i - 1$. ∎

LEMMA 2.6. *For some $1 \le i \le r+1$, let $\alpha, \eta \in \overline{K}$ be algebraic integers satisfying*

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

Then, for any nonzero polynomial $g(x) \in K[x]$ of degree less than m_i, we have $v(g(\eta) - g(\alpha)) > v(g(\alpha))$. In particular, if $\deg_K \alpha = m_i$, then $e(K(\alpha)/K)$ divides $e(K(\eta)/K)$.

Proof. By dividing $g(x)$ by its leading coefficient we can suppose that $g(x)$ is monic. If $g(x)$ has degree zero, the statement is obvious. Suppose $g(x)$ has positive degree $s < m_i$, with roots $\rho_1, \dots, \rho_s$ in $\overline{K}$. By the minimality of m_i, we necessarily have $v(\theta - \rho_j) \le \mu_{i-1}$ for all j. Hence,

$$v(\rho_j - \alpha) = \min\{v(\theta - \rho_j), v(\theta - \alpha)\} \le \mu_{i-1} < v(\eta - \alpha). \tag{2.2}$$

By Taylor's development, there exist $a_1, \dots, a_s \in \overline{K}$ such that

$$g(\eta) - g(\alpha) = a_1(\eta - \alpha) + \dots + a_k(\eta - \alpha)^k + \cdots.$$

Now, (2.2) and the formula

$$a_k = \sum_{\substack{S \subseteq \{1,\dots,s\} \\ \#S=k}} \prod_{j \notin S} (\alpha - \rho_j)$$

show that $v(a_k(\eta-\alpha)^k) > v(g(\alpha))$ for all $k \geq 1$.

If $\deg_K \alpha = m_i$, any $u \in K(\alpha)$ with $v(u) = 1/e(K(\alpha)/K)$ can be expressed as $u = g(\alpha)$ for some $g(x) \in K[x]$ of degree less than m_i. Hence, from $v(g(\eta)) = v(g(\alpha)) = 1/e(K(\alpha)/K)$, we deduce that $e(K(\alpha)/K)$ divides $e(K(\eta)/K)$. ∎

The algebraic integers $\alpha_1, \dots, \alpha_r$ are close to θ with regard to their degree, but the fields $K_1, \dots, K_r$ are not necessarily subfields of L. However, the next proposition, which is a generalization of [Oku, II, Prop. 4], shows that the maximal tamely ramified subextensions of $K_1/K, \dots, K_r/K$ are always included in L.

Proposition 2.7. *For some $1 \leq i \leq r+1$, suppose that $\alpha \in \overline{K}$ satisfies*

$$\deg_K \alpha = m_i, \qquad v(\theta - \alpha) > \mu_{i-1},$$

and let $N = K(\alpha)$. Suppose θ and α are separable over K, let M/K be any finite Galois extension containing L and N, and let $G = \mathrm{Gal}(M/K)$. Consider the subgroups

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

and let $M^{H_i} \subseteq M^{H_i'} \subseteq M$ be the respective fixed fields. Finally, let V be the maximal tamely ramified subextension of N/K. Then $V \subseteq M^{H_i} \subseteq L \cap N$. If moreover $v(\theta - \alpha) = \mu_i$, then $V \subseteq M^{H_i} \subseteq M^{H_i'} \subseteq L \cap N$.

Proof. In order to show that $M^{H_i} \subseteq K(\theta) \cap K(\alpha)$, we need to check that all $\sigma \in G$ that leave θ or α invariant lie in H_i. This is obvious for the automorphisms leaving θ invariant; for the $\sigma \in G$ such that $\sigma(\alpha) = \alpha$, we have $v(\sigma(\theta) - \alpha) = v(\sigma(\theta) - \sigma(\alpha)) > \mu_{i-1}$, so that

$$v(\theta - \sigma(\theta)) \geq \min\{v(\theta - \alpha), v(\alpha - \sigma(\theta))\} > \mu_{i-1}.$$

The same argument shows that $M^{H_i'} \subseteq L \cap N$, if $v(\theta - \alpha) = \mu_i$.

$$\begin{tikzcd}[arrows=dash]
M \arrow[d] \arrow[ddr] & \\
L \arrow[d] & \\
M^{H_i} \arrow[d] \arrow[r] & N \\
V \arrow[d] & \\
K &
\end{tikzcd}$$

By the basic properties of tamely ramified extensions [Nar, Ch. 5, §2], in order to check that $V \subseteq M^{H_i}$, it is sufficient to show that

$$v\left(\frac{\sigma(u)}{u}-1\right)>0, \qquad \forall u\in N^*,\ \forall\sigma\in H_i.$$

Clearly, $v(\theta-\sigma(\alpha)) \ge \min\{v(\theta-\sigma(\theta)), v(\sigma(\theta)-\sigma(\alpha))\} > \mu_{i-1}$ for all $\sigma \in H_i$. Finally, any $u \in N^*$ can be written as $u = g(\alpha)$ for some $g(x) \in K[x]$ of degree less than m_i. By Lemma 2.6 applied to $\eta = \sigma(\alpha)$, we have

$$v(\sigma(u)-u) = v(g(\sigma(\alpha))-g(\alpha)) > v(g(\alpha)) = v(u),$$

as desired. ∎

The following two corollaries generalize [Oku, II, Prop. 6, Cors. 1, 2].

Corollary 2.8. *Let $[F_1,\dots,F_r]$ be an Okutsu frame of $F(x)$. Then the numbers $e(K_i/K)$, $f(K_i/K)$ for $1\le i\le r$ do not depend on the Okutsu frame chosen. Moreover,*

$$e(K_1/K)\,|\,\cdots\,|\,e(K_r/K)\,|\,e(L/K), \qquad f(K_1/K)\,|\,\cdots\,|\,f(K_r/K)\,|\,f(L/K).$$

In particular, $m_1\,|\,\cdots\,|\,m_r\,|\,m_{r+1} = \deg F$.

Proof. For all $1\le i\le r$, suppose that $\eta\in\overline{K}$ satisfies $\deg_K\eta = m_i$ and $v(\theta-\eta)=\mu_i$. By Lemma 2.6, $e(K_i/K) = e(K(\eta)/K)$, because these two numbers divide each other. Hence, $f(K_i/K) = m_i/e(K_i/K) = m_i/e(K(\eta)/K) = f(K(\eta)/K)$.

By Proposition 2.7, we have $f(K_r/K)\,|\,f(L/K)$. By Lemma 2.6, applied to $i=r$, $\alpha=\alpha_r$ and $\eta=\theta$, we get $e(K_r/K)\,|\,e(L/K)$. The rest of the statements follow from Corollary 2.5 by a recurrent argument. ∎

Corollary 2.9. *Suppose L/K is tamely ramified. Let $[F_1,\dots,F_r]$ be an Okutsu frame of $F(x)$, and let $K_{r+1}:=L$. Then*

(i) $K_i = M^{H_i} = M^{H_i'}$ *for all* $1\le i\le r+1$. *Hence,* $K_1\subseteq\cdots\subseteq K_r\subseteq L$.

(ii) $\{v(\theta-\sigma(\theta)) \mid \sigma\in G\} = \begin{cases}\{\mu_1,\dots,\mu_r,\mu_{r+1}\} & \text{if } m_1=1,\\ \{\mu_0,\mu_1,\dots,\mu_r,\mu_{r+1}\} & \text{if } m_1>1.\end{cases}$

In particular, μ_r is the Krasner radius of $F(x)$:

$$\mu_r = \max\{v(\theta-\theta') \mid F(\theta')=0,\ \theta'\ne\theta\}.$$

Proof. Denote $\alpha_{r+1}:=\theta$. By Corollary 2.8, if L/K is tamely ramified, then K_i/K is tamely ramified for all $1\le i\le r+1$. Proposition 2.7, applied to each α_i, shows that $K_i = M^{H_i} = M^{H_i'}$, and hence $H_i = H_i'$ for all $1\le i\le r+1$. Moreover, for all $1\le i\le r$ we have $H_{i+1}\subsetneq H_i = H_i'$, because $[K_{i+1}\colon K_i]>1$; hence, there is some $\sigma\in H_i$ with $v(\theta-\sigma(\theta))=\mu_i$. Finally, there is no $\sigma\in G$ with $v(\theta-\sigma(\theta))=0$ if and only if $H_1=G$, or equivalently, $K_1=K$. ∎

2.2. Okutsu frames and divisor polynomials

PROPOSITION 2.10 ([Oku, I, Prop. 1]). *For any integer $0 \le m < n$ there exists a monic polynomial $g_m(x) \in \mathcal{O}[x]$ of degree m such that*

$$v(g_m(\theta)) \ge v(g(\theta)) - v(g(x)) \tag{2.3}$$

for all polynomials $g(x) \in \mathcal{O}[x]$ of degree m.

Proof. Let $g(x) \in \mathcal{O}[x]$ be a monic polynomial of degree m. Let $\mathcal{O}' \subseteq \mathcal{O}_L$ be the $\mathcal{O}$-module generated by θ and $g(\theta)/\pi^{\lfloor v(g(\theta))\rfloor}$. Clearly,

$$\lfloor v(g(\theta))\rfloor = \ell(\mathcal{O}'/\mathcal{O}[\theta]) \le \ell(\mathcal{O}_L/\mathcal{O}[\theta]) < \infty,$$

where ℓ denotes the length as an $\mathcal{O}$-module. Since v restricted to L is discrete, $v(g(\theta))$ takes only a finite number of values; hence, there exists a monic $g_m(x) \in \mathcal{O}[x]$ of degree m such that $v(g_m(\theta)) \ge v(g(\theta))$ for all monic $g(x) \in \mathcal{O}[x]$ of degree m. In order to check (2.3) it is sufficient to show that $v(g_m(\theta)) \ge v(g(\theta))$ for any $g(x) \in \mathcal{O}[x]$ of degree m such that $v(g(x)) = 0$. Let us prove this by induction on m. For $m = 0$ we have $g_m(x) = 1$ and the statement is obvious. Suppose $m > 0$. If $a \in \mathcal{O}$ is the leading coefficient of $g(x)$, we write

$$g(x) = ag_m(x) + r(x), \qquad m' := \deg r(x) < m.$$

If $v(a) = 0$, then $v(g_m(\theta)) \ge v(a^{-1}g(\theta)) = v(g(\theta))$, by the construction of $g_m(x)$. If $v(a) > 0$, then $v(r(x)) = 0$ and by the induction hypothesis

$$v(g_m(\theta)) \ge v(\theta^{m-m'}g_{m'}(\theta)) \ge v(g_{m'}(\theta)) \ge v(r(\theta)).$$

Thus, $v(r(\theta)) < v(ag_m(\theta))$, so that $v(g(\theta)) = v(r(\theta)) \le v(g_m(\theta))$. ■

DEFINITION 2.11. Clearly, (2.3) does not depend on the choice of θ among the roots of $F(x)$. We call $g_m(x)$ a *divisor polynomial* of degree m of $F(x)$.

LEMMA 2.12. *Let $[F_1, \ldots, F_r]$ be an Okutsu frame of $F(x)$. Let $h(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial of degree m, and let*

$$\delta_F(h) = \max\{v(\theta - \beta) \mid \beta \in \overline{K} \text{ is a root of } h(x)\}.$$

Then, for any $1 \le i \le r$,

(i) $\delta_F(h) < \mu_i \;\Rightarrow\; v(h(\theta)) < (m/m_i)v(F_i(\theta))$,
(ii) $\delta_F(h) = \mu_i \;\Rightarrow\; v(h(\theta)) = (m/m_i)v(F_i(\theta))$,
(iii) $\delta_F(h) > \mu_i \;\Rightarrow\; v(h(\theta)) > (m/m_i)v(F_i(\theta))$.

Proof. We can assume that $F(x)$ and $h(x)$ are separable by considering separable polynomials sufficiently close to them. Take a finite Galois extension M/K containing L, K_i and the roots of $h(x)$. Denote $G := \mathrm{Gal}(M/K)$. Choose a root β of $h(x)$ such that $v(\theta - \beta) = \delta_F(h) \ge v(\theta - \sigma(\beta))$ for all

$\sigma \in G$. This implies

$$v(\theta - \sigma(\theta)) \geq \min\{v(\theta - \sigma(\beta)), v(\sigma(\beta) - \sigma(\theta))\} = v(\theta - \sigma(\beta)) \tag{2.4}$$

for all $\sigma \in G$. Suppose $\delta_F(h) \leq \mu_i$. We claim that

$$v(\theta - \sigma(\beta)) \leq v(\theta - \sigma(\alpha_i)), \quad \forall \sigma \in G. \tag{2.5}$$

In fact, by the maximality of μ_i, we have $v(\theta - \sigma(\alpha_i)) \leq \mu_i$ for all $\sigma \in G$. Now, if $v(\theta - \sigma(\alpha_i)) = \mu_i$, then the inequality (2.5) is obvious; on the other hand, if $v(\theta - \sigma(\alpha_i)) < \mu_i$, by (2.4) we have

$$v(\theta-\sigma(\beta)) \leq v(\theta-\sigma(\theta)) = \min\{v(\theta-\sigma(\alpha_i)), v(\sigma(\alpha_i)-\sigma(\theta))\} = v(\theta-\sigma(\alpha_i)).$$

Therefore, (2.5) shows that

$$\frac{\#G}{m} v(h(\theta)) = \sum_{\sigma \in G} v(\theta - \sigma(\beta)) \leq \sum_{\sigma \in G} v(\theta - \sigma(\alpha_i)) = \frac{\#G}{m_i} v(F_i(\theta)). \tag{2.6}$$

If $\delta_F(h) < \mu_i$, then the inequality in (2.5) is strict, at least for $\sigma = 1$; hence, the inequality in (2.6) is strict too. This proves item (i).

Suppose now $\delta_F(h) \geq \mu_i$. Then $v(\alpha_i - \beta) \geq \min\{v(\alpha_i - \theta), v(\theta - \beta)\} = \mu_i$, and we have directly, for all $\sigma \in G$,

$$v(\theta - \sigma(\beta)) \geq \min\{v(\theta - \sigma(\alpha_i)), v(\sigma(\alpha_i) - \sigma(\beta))\} = v(\theta - \sigma(\alpha_i)). \tag{2.7}$$

Therefore,

$$\frac{\#G}{m} v(h(\theta)) = \sum_{\sigma \in G} v(\theta - \sigma(\beta)) \geq \sum_{\sigma \in G} v(\theta - \sigma(\alpha_i)) = \frac{\#G}{m_i} v(F_i(\theta)). \tag{2.8}$$

The inequalities (2.6) and (2.8) prove item (ii). Finally, if $\delta_F(h) > \mu_i$, the inequality (2.7) is strict at least for $\sigma = 1$, and the inequality in (2.8) is strict too. This proves item (iii). ■

The next result is a generalization of [Oku, II, Prop. 2].

THEOREM 2.13. *Let $m_1 < \cdots < m_r < \deg F$ be the Okutsu degrees of $F(x)$, and let $F_1(x), \ldots, F_r(x) \in \mathcal{O}[x]$ be a family of monic separable polynomials with $\deg F_i(x) = m_i$ for all $1 \leq i \leq r$. Then $[F_1, \ldots, F_r]$ is an Okutsu frame of $F(x)$ if and only if each $F_i(x)$ is a divisor polynomial of $F(x)$ of degree m_i.*

Proof. Suppose that $[F_1, \ldots, F_r]$ is an Okutsu frame of $F(x)$. For any index $1 \leq i \leq r$, let $g(x) \in \mathcal{O}[x]$ be a monic polynomial of degree m_i, and let $g(x) = h_1(x) \cdots h_s(x)$ with $h_j(x) \in \mathcal{O}[x]$ monic and irreducible. By the maximality of μ_i, we have $\delta_F(h_j) \leq \mu_i$ for all j. Lemma 2.12 shows that $v(h_j(\theta)) \leq ((\deg h_j)/m_i) v(F_i(\theta))$ for all j; hence,

$$v(g(\theta)) = \sum_j v(h_j(\theta)) \leq \sum_j ((\deg h_j)/m_i) v(F_i(\theta)) = v(F_i(\theta)).$$

Along the proof of Proposition 2.10 we saw that this property, for all monic $g(x)$ of degree m_i, already implies that $F_i(x)$ is a divisor polynomial of degree m_i.

Conversely, suppose that each $F_i(x)$ is a divisor polynomial of $F(x)$ of degree m_i, and let $[F'_1,\dots,F'_r]$ be an Okutsu frame of $F(x)$. Fix an index $1\le i\le r$; clearly, $v(F_i(\theta))=v(F'_i(\theta))$, since $F_i(x)$ and $F'_i(x)$ are both divisor polynomials of degree m_i. Let us see first that $F_i(x)$ is necessarily irreducible. In fact, suppose $F_i(x)=h_1(x)\cdots h_s(x)$, with all $h_j(x)$ monic irreducible polynomials of degree less than m_i. Then $\delta_F(h_j)\le\mu_{i-1}<\mu_i$ for all j, by the minimality of m_i. By Lemma 2.12, $v(h_j(\theta))<((\deg h_j)/m_i)v(F'_i(\theta))$ for all j, and this implies $v(F_i(\theta))<v(F'_i(\theta))$, in contradiction with our assumption. Once we know that $F_i(x)$ is irreducible, Lemma 2.12 shows that $\delta_F(F_i)=\mu_i$. Thus, $[F_1,\dots,F_r]$ is an Okutsu frame of $F(x)$. ∎

Corollary 2.14. *The rational numbers* $0<v(F_1(\theta))<\cdots<v(F_r(\theta))$ *depend only on* $F(x)$. ∎

In Corollary 3.6 below, we shall show how to compute these invariants solely in terms of the Okutsu frame $[F_1,\dots,F_r]$.

Okutsu refers to $F_1(x),\dots,F_r(x)$ as the *primitive divisor polynomials* of $F(x)$, because by multiplying them in a suitable way one obtains the divisor polynomials of all degrees $0\le m<n$.

Theorem 2.15 ([Oku, II, Thm. 1]). *Let* $[F_1,\dots,F_r]$ *be an Okutsu frame of* $F(x)$. *Take* $F_0(x)=x$. *Let* $0<m<n$, *and write it (in a unique form) as*

$$m=\sum_{i=0}^{r}a_im_i \quad \textit{with} \quad 0\le a_i<m_{i+1}/m_i.$$

Then $g_m(x):=\prod_{i=0}^{r}F_i(x)^{a_i}$ *is a divisor polynomial of degree* m *of* $F(x)$.

Proof. As we saw in the proof of Proposition 2.10, it is sufficient to show that $v(g_m(\theta))\ge v(g(\theta))$ for all $g(x)\in\mathcal{O}[x]$ monic of degree m. Let us prove this by induction on m.

If $m<m_1$, then $g_m(x)=x^m$ and $v(g_m(\theta))=0=v(g(\theta))$ for all $g(x)$ monic of degree m, by Lemma 2.2 and Corollary 2.3. If $m=m_1$ then $g_m(x)=F_1(x)$, which is a divisor polynomial of degree m_1 of $F(x)$ by Theorem 2.13. Thus, the theorem is proven for all $0<m\le m_1$.

Let $m_j\le m<m_{j+1}$ for some $1\le j\le r$, and suppose that the theorem is true for all degrees less than m. We claim that $v(\theta-\eta)\le v(\alpha_j-\eta)$ for any root $\eta\in\overline{K}$ of any monic polynomial $g(x)\in\mathcal{O}[x]$ of degree m. In fact, $v(\theta-\eta)\le\mu_j$, by the minimality of m_{j+1}, and

$$v(\theta-\eta)<\mu_j \;\Rightarrow\; v(\alpha_j-\eta)=\min\{v(\theta-\eta),v(\theta-\alpha_j)\}=v(\theta-\eta),$$
$$v(\theta-\eta)=\mu_j \;\Rightarrow\; v(\alpha_j-\eta)\ge\min\{v(\theta-\eta),v(\theta-\alpha_j)\}=\mu_j.$$

Hence, $v(g(\theta)) \le v(g(\alpha_j))$. Consider now

$$g(x) = F_j(x)q(x) + r(x), \qquad \deg r(x) < m_j.$$

Clearly, $v(g(\theta)) \le v(g(\alpha_j)) = v(r(\alpha_j)) = v(r(\theta))$, the last equality by Lemma 2.6 applied to $\alpha = \alpha_j$, $\eta = \theta$. Since $\deg q(x) = m - m_j$, we have

$$v(q(\theta)) \le v\Big(F_j(\theta)^{a_j-1}\prod_{k=0}^{j-1} F_k(\theta)^{a_k}\Big)$$

by the induction hypothesis; hence

$$v\Big(\prod_{i=0}^{r} F_i(\theta)^{a_i}\Big) \ge v(F_j(\theta)q(\theta)) \ge \min\{v(g(\theta)), v(r(\theta))\} = v(g(\theta)). \blacksquare$$

3. Okutsu frames and Newton polygons of higher order. In this section we study more properties of Okutsu frames in connection with the theory of Newton polygons of higher order. These polygons were introduced in [Mon], and revised in [HN] (HN standing for “higher Newton”).

We keep dealing with a local field K with perfect residue class field, and we keep the notations $\mathcal{O}$, $\mathfrak{m}$, π, $\mathbb{F}$ and v of the previous section. Also, we keep fixing a monic irreducible polynomial $F(x) \in \mathcal{O}[x]$ of degree n, a root $\theta \in \overline{K}$ of $F(x)$, and the field $L = K(\theta)$.

The aim of this section is to characterize when a chain $[F_1, \dots, F_r]$ of monic irreducible separable polynomials is an Okutsu frame of $F(x)$ in terms of invariants linked to certain Newton polygons (Theorems 3.5 and 3.9). As a consequence, we give a closed formula for the invariants $v(F_i(\theta))$ solely in terms of the Okutsu frame (Corollary 3.6), and we find new Okutsu invariants of $F(x)$ (Corollary 3.7).

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 $\varphi(y) = c\psi(y)$.

3.1. Newton polygons of higher order. Let us briefly review Newton polygons of higher order [HN, Secs. 1, 2]. We denote by v_1 the discrete valuation on $K(x)$ determined by the natural extension of v to polynomials, given in (2.1). Consider the 0*th residual polynomial* operator

$$R_0 \colon \mathcal{O}[x] \to \mathbb{F}[y], \qquad g(x) \mapsto \operatorname{red}(g(y)/\pi^{v_1(g)}),$$

where $\operatorname{red}\colon \mathcal{O}[y] \to \mathbb{F}[y]$ is the natural reduction map. A *type of order zero*, $\mathbf{t} = \psi_0(y)$, is just a monic irreducible polynomial $\psi_0(y) \in \mathbb{F}[y]$. A *representative* of $\mathbf{t}$ is any monic polynomial $\phi_1(x) \in \mathcal{O}[x]$ such that $R_0(\phi_1) = \psi_0$. The pair (ϕ_1, v_1) can be used to attach a Newton polygon to any nonzero polynomial $g(x) \in K[x]$. If $g(x) = \sum_{i\ge 0} a_i(x)\phi_1(x)^i$ is the ϕ_1-adic development of $g(x)$, then $N_1(g) := N_{\phi_1,v_1}(g)$ is the lower convex envelope of the set of points of the plane with coordinates $(i, v_1(a_i(x)\phi_1(x)^i))$ [HN, Sec. 1].

Let $\lambda_1 \in \mathbb{Q}^-$ be a negative rational number, $\lambda_1 = -h_1/e_1$, with h_1, e_1 positive coprime integers. The triple (ϕ_1, v_1, λ_1) determines a discrete valuation v_2 on $K(x)$, constructed as follows: for any nonzero polynomial $g(x) \in \mathcal{O}[x]$, take a line of slope λ_1 far below $N_1(g)$ and shift it upwards till it touches the polygon for the first time; if H is the ordinate at the origin of this line, then $v_2(g(x)) = e_1 H$ by definition. Also, the triple (ϕ_1, v_1, λ_1) determines a *residual polynomial* operator

$$R_1 := R_{\phi_1,v_1,\lambda_1} \colon \mathcal{O}[x] \to \mathbb{F}_1[y], \qquad \mathbb{F}_1 := \mathcal{O}[x]/(\mathfrak{m}[x], \phi_1(x)),$$

which is a kind of reduction of first order of $g(x)$ [HN, Def. 1.9].

Let $\psi_1(y) \in \mathbb{F}_1[y]$ be a monic irreducible polynomial with $\psi_1(y) \neq y$. The triple $\mathbf{t} = (\phi_1(x); \lambda_1, \psi_1(y))$ is called a *type of order one*. Given any such type, one can compute a representative of $\mathbf{t}$, that is, a monic separable polynomial $\phi_2(x) \in \mathcal{O}[x]$ of minimum degree satisfying $R_1(\phi_2)(y) \sim \psi_1(y)$.

Now we may start over and repeat all constructions in order two. The pair (ϕ_2, v_2) can be used to attach a Newton polygon $N_2(g) := N_{\phi_2,v_2}(g)$ to any nonzero polynomial $g(x) \in K[x]$. This polygon is constructed from the ϕ_2-adic development $g(x) = \sum_{i\ge 0} b_i(x)\phi_2(x)^i$, as the lower convex envelope of the set of points of the plane with coordinates $(i, v_2(b_i(x)\phi_2(x)^i))$. For any negative rational number λ_2, the triple (ϕ_2, v_2, λ_2) determines a discrete valuation v_3 on $K(x)$ and a *residual polynomial* operator

$$R_2 := R_{\phi_2,v_2,\lambda_2} \colon \mathcal{O}[x] \to \mathbb{F}_2[y], \qquad \mathbb{F}_2 := \mathbb{F}_1[y]/(\psi_1(y)).$$

The iteration of this procedure leads to the concept of *type of order r*. A type of order $r \ge 1$ is a chain

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

where $\phi_1(x), \dots, \phi_r(x)$ are monic irreducible separable polynomials in $\mathcal{O}[x]$, the slopes $\lambda_1, \dots, \lambda_r$ are negative rational numbers, and $\psi_r(y)$ is a polynomial over certain finite extension $\mathbb{F}_r$ of $\mathbb{F}$ (to be specified below), that have the following recursive properties:

(1) $\phi_1(x)$ is irreducible modulo $\mathfrak{m}$. We denote $\psi_0(y) := R_0(\phi_1)(y) \in \mathbb{F}[y]$, and we define $\mathbb{F}_1 := \mathbb{F}[y]/(\psi_0(y))$.

(2) For all $1 \le i < r$, $N_i(\phi_{i+1}) := N_{\phi_i,v_i}(\phi_{i+1})$ is one-sided of slope λ_i, and $R_i(\phi_{i+1})(y) := R_{\phi_i,v_i,\lambda_i}(\phi_{i+1})(y) \sim \psi_i(y)$ for some monic irreducible polynomial $\psi_i(y) \in \mathbb{F}_i[y]$. We define $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_i(y))$.

(3) $\psi_r(y) \in \mathbb{F}_r[y]$ is a monic irreducible polynomial, $\psi_r(y) \neq y$.

We attach to any type $\mathbf{t}$ of order r certain invariants: $e_1, \dots, e_r, h_1, \dots, h_r, f_0, f_1, \dots, f_r$. They are defined as follows: $\lambda_i = -h_i/e_i$, with e_i, h_i positive coprime integers, and $f_i = \deg \psi_i(y)$. Below we shall extensively use these numerical invariants without any mention of the underlying type $\mathbf{t}$, which will be usually implicit in the context.

For any nonzero $g(x) \in K[x]$, we denote by $N_i^-(g)$ the union of the sides of negative slope of $N_i(g)$. We say that $N_i^-(g)$ is the *principal part* of $N_i(g)$. The *length* of either of these two polygons is by definition the length of its projection to the horizontal axis.

At each order $1, \dots, r$, three fundamental theorems provide a far-reaching generalization of the Hensel lemma, that had been worked out by Ore in order one [Ore]: the theorems of the product [HN, Thm. 2.26], of the polygon [HN, Thm. 3.1], and of the residual polynomial [HN, Thm. 3.7]. Let us only mention the following facts, which are an immediate consequence of these results.

PROPOSITION 3.1. *Let $\mathbf{t}$ be a type of order $r \geq 1$, and let $g(x) \in \mathcal{O}[x]$ be a nonzero polynomial. Then, for any $1 \leq i \leq r$:*

(i) *If $N_i^-(g)$ is reduced to a point or it is one-sided of slope $\lambda \neq \lambda_i$, then $R_i(g)(y)$ is a constant in $\mathbb{F}_i$.*

(ii) *If $N_i^-(g)$ is not reduced to a point and $g(x)$ is irreducible, then $N_i(g) = N_i^-(g)$ is one-sided and $N_j(g) = N_j^-(g)$ is one-sided of slope λ_j for all $1 \leq j < i$. Moreover, if $\beta \in \overline{K}$ is a root of $g(x)$, then the theorem of the polygon shows that*

$$v(\phi_i(\beta)) = \frac{|\lambda| + v_i(\phi_i)}{e_1 \cdots e_{i-1}}, \tag{3.1}$$

where λ is the slope of $N_i^-(g)$.

(iii) *If $N_i(g)$ is one-sided of slope λ_i, then* $\deg R_i(g) = (\deg g)/e_i \deg \phi_i$. *If moreover $g(x)$ is irreducible, then $R_i(g)(y)$ is the power of an irreducible polynomial in $\mathbb{F}_i[y]$.*

(iv) *If $i < r$, then $N_{i+1}^-(g)$ has length equal to* $\operatorname{ord}_{\psi_i(y)}(R_i(g)(y))$.

DEFINITION 3.2. Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial, and $\mathbf{t}$ a type of order $r \geq 1$.

(1) We say that $\mathbf{t}$ *divides* $f(x)$ if $\psi_r(y)$ divides $R_r(f)(y)$ in $\mathbb{F}_r[y]$.

(2) We say that $\mathbf{t}$ is *f-complete* if $\operatorname{ord}_{\psi_r}(R_r(f)) = 1$. In this case, $\mathbf{t}$ singles out an irreducible factor of $f(x)$ in $\mathcal{O}[x]$. This factor is denoted $f_{\mathbf{t}}(x)$; it has degree $e_r f_r \deg \phi_r$, and it is uniquely determined by the property $R_r(f_{\mathbf{t}})(y) \sim \psi_r(y)$.

(3) A *representative* of $\mathbf{t}$ is a monic separable polynomial $\phi_{r+1}(x) \in \mathcal{O}[x]$ of minimum degree having the property that $\mathbf{t}$ is ϕ_{r+1}-complete. This polynomial is necessarily irreducible in $\mathcal{O}[x]$. Note that, by the definition of a type, each $\phi_i(x)$ is a representative of the truncated

type of order $i-1$:

$$\mathbf{t}_{i-1} := (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-2}, \phi_{i-1}(x); \lambda_{i-1}, \psi_{i-1}(y)).$$

In [HN, Sec. 2.3] we found an explicit and efficient procedure to compute representatives of arbitrary types.

(4) We say that $\mathbf{t}$ is *optimal* if $\deg \phi_1 < \cdots < \deg \phi_r$, or equivalently, $e_i f_i > 1$ for all $1 \le i < r$. We say that $\mathbf{t}$ is *strongly optimal* if $\mathbf{t}$ is optimal and $e_r f_r > 1$. We convene that all types of order zero are strongly optimal.

We finish this section with a proposition, extracted from [HN, Prop. 3.5], which plays an essential role in what follows, and an auxiliary lemma.

PROPOSITION 3.3. *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, $\theta \in \overline{K}$ a root of $F(x)$, and $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$ a type of order r dividing $F(x)$. Let $g(x) \in \mathcal{O}[x]$ be a nonzero polynomial. Take a line of slope λ_r far below $N_r(g)$, and let it shift upwards till it touches the polygon for the first time. Let H be the ordinate at the origin of this line. Then $v(g(\theta)) \ge H/e_1 \cdots e_{r-1}$, and equality holds if and only if $\mathbf{t}$ does not divide $g(x)$.*

LEMMA 3.4. *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, and let $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$ be a type of order $r \ge 1$ dividing $F(x)$. Let $\phi_{r+1}(x)$ be a representative of $\mathbf{t}$, and let $\lambda_{r+1} = -h_{r+1}/e_{r+1}$ be the slope of $N_{r+1}(F)$, where h_{r+1}, e_{r+1} are positive coprime integers. Then*

$$v(\phi_{r+1}(\theta)) = \frac{\deg \phi_{r+1}}{\deg \phi_r} v(\phi_r(\theta)) + \frac{h_{r+1}}{e_1 \cdots e_{r+1}}.$$

Proof. By [HN, Prop. 2.7], $v_{r+1}(\phi_r) = e_r v_r(\phi_r) + h_r$, and by [HN, Thm. 2.11], $v_{r+1}(\phi_{r+1}) = e_r f_r v_{r+1}(\phi_r)$. These two formulas together show that

$$\frac{v_{r+1}(\phi_{r+1})}{e_1 \cdots e_r} = e_r f_r \frac{|\lambda_r| + v_r(\phi_r)}{e_1 \cdots e_{r-1}}.$$

Therefore, since $\deg \phi_{r+1}/\deg \phi_r = e_r f_r$, the lemma is a consequence of the theorem of the polygon, (3.1):

$$v(\phi_{r+1}(\theta)) = \frac{|\lambda_{r+1}| + v_{r+1}(\phi_{r+1})}{e_1 \cdots e_r}, \qquad v(\phi_r(\theta)) = \frac{|\lambda_r| + v_r(\phi_r)}{e_1 \cdots e_{r-1}}. \ \blacksquare$$

3.2. Okutsu frames and complete types

THEOREM 3.5. *Let $[F_1, \dots, F_r]$ be an Okutsu frame of $F(x)$, and let $K_{r+1} = L$, $F_{r+1}(x) = F(x)$. Then there exist negative rational numbers $\lambda_1, \dots, \lambda_r$, a finite extension $\mathbb{F}_r$ of $\mathbb{F}$ and a monic irreducible polynomial $\psi_r(y) \in \mathbb{F}_r[y]$ such that*

$$(F_1(x); \lambda_1, F_2(x); \dots; \lambda_{r-1}, F_r(x); \lambda_r, \psi_r(y))$$

is an F-complete strongly optimal type of order r. More precisely, F_1 is irreducible modulo $\mathfrak{m}$, the field $\mathbb{F}_1 := \mathcal{O}[x]/(\mathfrak{m}[x], F_1(x))$ is the residue field of K_1, and for all $1 \le i \le r$:

(1) *$N_i(F)$ and $N_i(F_{i+1})$ are one-sided of slope λ_i.*
(2) *If we write $\lambda_i = -h_i/e_i$ with h_i, e_i positive coprime integers, then $e_i = e(K_{i+1}/K)/e(K_i/K)$.*
(3) *$R_i(F)(y) \sim \psi_i(y)^{a_i}$ for some monic irreducible polynomial $\psi_i(y) \in \mathbb{F}_i[y]$, and $R_i(F_{i+1})(y) \sim \psi_i(y)$.*
(4) *$f_i := \deg \psi_i(y) = f(K_{i+1}/K)/f(K_i/K)$.*
(5) *$\mathbb{F}_{i+1} := \mathbb{F}_i[y]/(\psi_i(y))$ has degree $[\mathbb{F}_{i+1} \colon \mathbb{F}] = f(K_{i+1}/K)$.*

Proof. By Corollary 2.3(ii), $F_1(x)$ is irreducible modulo $\mathfrak{m}$ and $F(x) \equiv F_1(x)^{(\deg F)/m_1} \pmod{\mathfrak{m}}$; in particular, $\mathbb{F}_1$ is the residue field of K_1. Let us prove simultaneously all statements (1)–(5) by induction on i. Actually, we argue with an arbitrary $1 \le i \le r$; if $i = 1$ we do not make any assumption and if $i > 1$ we assume that the conditions (1)–(5) are true for the indices $1, \dots, i-1$, for all Okutsu frames of all polynomials of depth less than or equal to r.

If $i = 1$, the Newton polygon $N_1^-(F)$ has length $(\deg F)/m_1$ [HN, Def. 1.8]. If $i > 1$, the induction hypothesis shows that $F_i(x)$ is a representative of the type $(F_1(x); \dots; F_{i-1}(x); \lambda_{i-1}, \psi_{i-1}(y))$, and $\psi_{i-1}(y)$ divides $R_{i-1}(F)(y)$; hence, $N_i^-(F)$ has positive length equal to $\operatorname{ord}_{\psi_{i-1}(y)}(R_{i-1}(F)(y))$, by Proposition 3.1(iv). Therefore, $N_i^-(F)$ is never reduced to a point. By Proposition 3.1(ii), $N_i^-(F) = N_i(F)$ is one-sided and it has a negative slope that we denote by λ_i, and we write it as $\lambda_i = -h_i/e_i$, with h_i, e_i positive coprime integers. Also, by Proposition 3.1(iii), $R_i(F)(y)$ is, up to a multiplicative constant, the power of some monic irreducible polynomial $\psi_i(y) \in \mathbb{F}_i[y]$, whose degree is denoted by f_i.

We want to show that $N_i(F_{i+1})$ is also one-sided of the same slope λ_i, and $R_i(F_{i+1}) \sim \psi_i(y)$. To this end we apply Proposition 3.3 to the polynomial $F_{i+1}(x)$ and the type $\mathbf{t}_i := (F_1(x); \dots; F_i(x); \lambda_i, \psi_i(y))$, in order to estimate $v(F_{i+1}(\theta))$ and compare this estimation with the inequality

$$v(F_{i+1}(\theta)) > \frac{m_{i+1}}{m_i} v(F_i(\theta)) = \frac{m_{i+1}}{m_i} \frac{|\lambda_i| + v_i(F_i)}{e_1 \cdots e_{i-1}}, \tag{3.2}$$

given by Lemma 2.12 and the theorem of the polygon, (3.1). The possible shapes of $N_i^-(F_{i+1})$ and the first point of contact with a line of slope λ_i shifting upwards from below are displayed in Figure 1, where we denote $g(x) := F_{i+1}(x)$ and $m := m_{i+1}/m_i$.

Let $F_{i+1}(x) = \sum_{0 \le j < m_{i+1}/m_i} a_j(x) F_i(x)^j + F_i(x)^{m_{i+1}/m_i}$ be the F_i-adic development of F_{i+1}. Recall that $v_i(F_{i+1}) = \min_{0 \le j \le m_{i+1}/m_i} \{v_i(a_j F_i^j)\}$ [HN, Lem. 2.17(1)]. If $v_i(a_0) = v_i(F_{i+1})$, then $N_i^-(F_{i+1})$ is reduced to the point

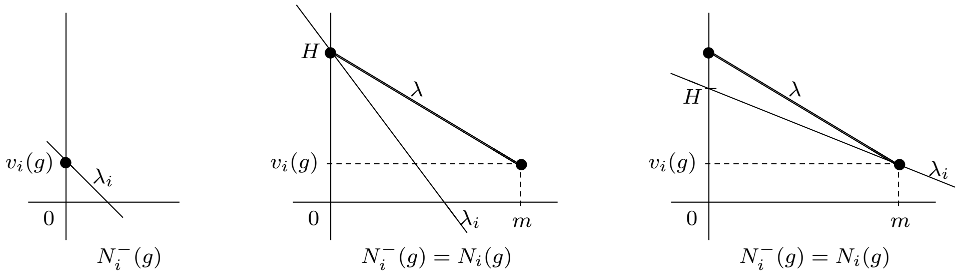

Fig. 1

$(0, v_i(F_{i+1}))$ and Proposition 3.3 shows that

$$v(F_{i+1}(\theta)) = v_i(F_{i+1})/e_1 \cdots e_{i-1} \le v_i(F_i^{m_{i+1}/m_i})/e_1 \cdots e_{i-1},$$

in contradiction with (3.2). Hence, $v_i(a_0) > v_i(F_{i+1})$; this implies that $N_i^-(F_{i+1})$ is not reduced to a point, and by Proposition 3.1(ii), $N_i(F_{i+1}) = N_i^-(F_{i+1})$ is one-sided and has a negative slope, that we denote by λ. In particular, $v_i(F_{i+1}) = (m_{i+1}/m_i)v_i(F_i)$.

The ordinate at the origin of the line of slope λ_i that first touches the polygon from below is equal to

$$H = v_i(F_{i+1}) + \frac{m_{i+1}}{m_i}\min\{|\lambda_i|, |\lambda|\} = \frac{m_{i+1}}{m_i}(v_i(F_i) + \min\{|\lambda_i|, |\lambda|\}).$$

If $\lambda \neq \lambda_i$, item (i) of Proposition 3.1 shows that $R_i(F_{i+1})$ is a constant. Hence, if either $\lambda \neq \lambda_i$ or $\psi_i(y)$ does not divide $R_i(F_{i+1})$, Proposition 3.1 would imply $v(F_{i+1}(\theta)) = H/e_1 \cdots e_{i-1}$, in contradiction with (3.2). Therefore, $\lambda = \lambda_i$ and $R_i(F_{i+1})(y) \sim \psi_i(y)^a$ for some positive exponent a.

Denote $e'_j := e(K_{j+1}/K)/e(K_j/K)$, $f'_j := f(K_{j+1}/K)/f(K_j/K)$ for all $1 \le j \le i$. By the induction hypothesis, $e'_j = e_j$, $f'_j = f_j$ for all $1 \le j < i$. Note that $e(K_1/K) = 1$, $f(K_1/K) = m_1$. By Proposition 3.1(iii) applied to $F_{i+1}(x)$, we have

$$m_i e'_i f'_i = e(K_{i+1}/K) f(K_{i+1}/K) = m_{i+1} = m_i e_i f_i a.$$

By [HN, Cors. 1.16, 1.20] we have

$$e_1 \cdots e_i \,|\, e(K_{i+1}/K) = e_1 \cdots e_{i-1} e'_i,$$
$$[\mathbb{F}_{i+1} \colon \mathbb{F}] = m_1 f_1 \cdots f_i \,|\, f(K_{i+1}/K) = m_1 f_1 \cdots f_{i-1} f'_i.$$

In particular, $e_i \,|\, e'_i$, $f_i \,|\, f'_i$. Thus, if we prove that $a = 1$, then all statements (1)–(5) will be proven. Let $\phi_{i+1}(x) \in \mathcal{O}[x]$ be a representative of the above mentioned type $\mathbf{t}_i$. This monic irreducible polynomial has degree $e_i f_i m_i$ [HN, Thm. 2.11], and by Lemma 3.4, $v(\phi_{i+1}(\theta)) > e_i f_i v(F_i(\theta))$. Now, $a > 1$ implies $\deg \phi_{i+1}(x) < m_{i+1}$, and this leads to $v(\phi_{i+1}(\theta)) \le v(F_i(\theta)^{e_i f_i})$, by Theorem 2.15. Therefore, $a = 1$ and the theorem is proven. ∎

By [HN, Cor. 3.2(1)], Theorem 3.5 has the following immediate consequence.

Corollary 3.6. *The invariants* $v(F_1(\theta)),\dots,v(F_r(\theta))$ *can be computed directly in terms of any Okutsu frame*:

$$v(F_i(\theta))=\sum_{j=1}^{i}(e_jf_j\cdots e_{i-1}f_{i-1})\frac{h_j}{e_1\cdots e_j}.\ \blacksquare$$

Corollary 3.7. *The following invariants depend only on* $F(x)$:

(i) *The slopes* $\lambda_1,\dots,\lambda_r$ *of* $N_1(F),\dots,N_r(F)$, *respectively.*
(ii) *The discrete valuations* $v_1,\dots,v_{r+1}$ *on* $K(x)$.

The slopes $\lambda_1,\dots,\lambda_{r-1}$, *and the discrete valuations* $v_1,\dots,v_r$ *on* $K(x)$, *can be computed from any Okutsu frame of* $F(x)$.

Proof. Suppose that $[F_1',\dots,F_r']$ is another Okutsu frame of $F(x)$, leading to the family of slopes $\lambda_1',\dots,\lambda_r'$, and valuations $v_1,v_2',\dots,v_{r+1}'$ on $K(x)$. By Theorem 3.5, both Okutsu frames determine F-complete types of order r; let h_i,e_i,f_i and h_i',e_i',f_i' be the respective invariants of these types, for all $1\le i\le r$. By Theorem 3.5 and Corollary 2.8,

$$e_i=e(K_{i+1}/K)/e(K_i/K)=e_i',\qquad f_i=f(K_{i+1}/K)/f(K_i/K)=f_i'$$

for all $1\le i\le r$. Let us prove that $\lambda_i=\lambda_i'$ for all $1\le i\le r$, by induction on i. Since $F_1(x)$ and $F_1'(x)$ are both divisor polynomials of degree m_1 of $F(x)$ (Theorem 2.13), we have $\lambda_1=-v(F_1(\theta))=-v(F_1'(\theta))=\lambda_1'$. Suppose $i>1$ and $\lambda_j=\lambda_j'$ (hence $h_j=h_j'$) for all $1\le j<i$. Since $F_i(x)$ and $F_i'(x)$ are both divisor polynomials of degree m_i of $F(x)$, we have $v(F_i(\theta))=v(F_i'(\theta))$, and by the theorem of the polygon (cf. (3.1)),

$$\frac{|\lambda_i|+v_i(F_i)}{e_1\cdots e_{i-1}}=v(F_i(\theta))=v(F_i'(\theta))=\frac{|\lambda_i'|+v_i'(F_i')}{e_1\cdots e_{i-1}}.\tag{3.3}$$

In [HN, Prop. 2.15], we found a closed formula for $v_i(F_i)$ that depends only on $h_1,\dots,h_{i-1}$, $e_1,\dots,e_{i-1}$ and $f_1,\dots,f_{i-1}$; hence, $v_i(F_i)=v_i'(F_i')$, and (3.3) shows that $\lambda_i=\lambda_i'$.

Let us prove now that $v_i=v_i'$ for all $1\le i\le r+1$, by induction on i. The valuation v_1 being canonical, we need only prove that $v_{i+1}=v_{i+1}'$, under the assumption $v_i=v_i'$ for some $1\le i\le r$. We claim that $N_i(F_i')$ is one-sided with negative slope $-h$ for some positive integer $h\ge|\lambda_i|$, which may be taken to be $h=\infty$ if $F_i=F_i'$ [HN, Lem. 2.17(3)]. In fact, let $A(x)=F_i(x)-F_i'(x)$, with $v_i(A)=v_i(F_i)+h$; the shape of $N_i(F_i')$ is displayed in Figure 2, and $v(F_i'(\theta))\ge H/e_1\cdots e_{i-1}$, by Proposition 3.3. This implies $h\ge|\lambda_i|$, because $v(F_i'(\theta))=(|\lambda_i|+v_i(F_i))/e_1\cdots e_{i-1}$, by (3.3).

Both discrete valuations v_{i+1}, v_{i+1}' coincide with $e_1\cdots e_iv_1$ when restricted to K [HN, Prop. 2.6]. Hence, in order to show that they are equal

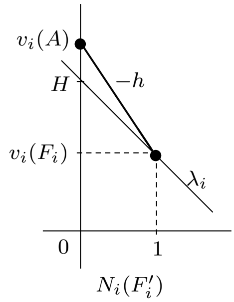

Fig. 2

it is sufficient to show that they coincide on all irreducible polynomials with coefficients in $\mathcal{O}$. Let $g(x) \in \mathcal{O}[x]$ be an irreducible polynomial. Let us recall the definition of v_{i+1} [HN, Def. 2.5]. If we consider a line of slope λ_i far below $N_i(g)$ and we let it shift upwards till it touches the polygon for the first time, then $v_{i+1}(g(x)) = e_i H$, where H is the ordinate at the origin of this line. Let $g(x) = \sum_{0\le j\le m} a_j(x)F_i(x)^j$ be the F_i-adic development of $g(x)$; we recall that $v_i(g) = \min_{0\le j\le m}\{v_i(a_j(x)F_i(x)^j)\}$ [HN, Lem. 2.17(1)]. Note that the 0th coefficient of the F_i'-adic development $g(x) = \sum_{0\le j\le m} a_j'(x)F_i'(x)^j$ is $a_0' = a_0 + a_1A + \cdots + a_mA^m$. We distinguish three cases according to the shape of $N_i^-(g)$, and its first point of contact with the line of slope λ_i under it. These possibilities are reflected in Figure 1 in the proof of Theorem 3.5.

If $v_i(a_0) = v_i(g)$, then $N_i^-(g)$ is reduced to the point $(0, v_i(g))$, and $v_{i+1}(g) = e_iv_i(g)$. Since $v_i(A) > v_i(F_i)$, we have $v_i(a_0) \le v_i(a_kF_i^k) < v_i(a_kA^k)$ for all $k > 0$. Thus, $v_i(a_0') = v_i(a_0) = v_i(g)$, so that $(N_i')^-(g)$ is also reduced to the point $(0, v_i(g))$, and $v_{i+1}'(g) = e_iv_i(g)$ too.

If $v_i(a_0) > v_i(g)$, then $N_i^-(g)$ is not reduced to a point, and $N_i^-(g) = N_i(g)$ is one-sided of negative slope λ, by Proposition 3.1(ii). In the special case $g(x) = F_i(x)$ we take $\lambda = \infty$ [HN, Lem. 2.17(3)]. As Figure 1 shows, $v_{i+1}(g) = e_iH$, where $H = v_i(g) + m\min\{|\lambda_i|, |\lambda|\}$. Now,

$$(3.4) \qquad v_i(a_kA^k) = v_i(a_kF_i^k) + kh \ge v_i(g) + (m-k)|\lambda| + kh$$

for all $k \ge 0$. Suppose $|\lambda| < |\lambda_i|$. Then $h > |\lambda|$, and $v_i(a_kA^k) > v_i(g) + m|\lambda| = v_i(a_0)$ for all $k > 0$. Hence, $v_i(a_0') = v_i(a_0) > v_i(g)$. This implies $N_i^-(g) = (N_i')^-(g)$, because both polygons are one-sided with the same end points: $(0, v_i(a_0))$ and $(m, v_i(g))$. In particular, $v_{i+1}(g) = v_{i+1}'(g) = e_iv_i(a_0)$.

Suppose now $|\lambda| \ge |\lambda_i|$. By (3.4), we have now $v_i(a_kA^k) \ge v_i(g) + m|\lambda_i|$ for all $k \ge 0$. Hence, $v_i(a_0') \ge v_i(g) + m|\lambda_i| > v_i(g)$, and $(N_i')^-(g)$ is one-sided of negative slope λ', which is not necessarily equal to λ. Clearly, $|\lambda'| = (v_i(a_0') - v_i(g))/m \ge |\lambda_i|$, and $v_{i+1}(g) = v_{i+1}'(g) = e_i(v_i(g) + m|\lambda_i|)$.

The last statement of the corollary is a consequence of Theorem 3.5: λ_i is the slope of $N_i(F_{i+1})$, and v_{i+1} is determined by $F_i(x)$, v_i and λ_i. ∎

Our next aim is to prove the converse of Theorem 3.5: an F-complete strongly optimal type is an Okutsu frame, plus the data λ_r, $\psi_r(y)$. To this end we recall what kind of optimal behaviour the optimal types have. The following result is extracted from [GMNa, Thm. 3.1], where this optimality was analyzed in a more general situation.

THEOREM 3.8 ([GMNa, Thm. 3.1]). *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, and $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-1}, \phi_i(x); \lambda_i, \psi_i(y))$ a type of order $i \geq 1$ dividing $F(x)$. Let $\phi_i'(x) \in \mathcal{O}[x]$ be another representative of the truncated type*

$$\mathbf{t}_{i-1} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-2}, \phi_{i-1}(x); \lambda_{i-1}, \psi_{i-1}(y)).$$

Let λ_i' be the slope of the one-sided Newton polygon of ith order of $F(x)$, $N_i'(F)$, taken with respect to the pair $(\phi_i'(x), v_i)$. If $e_i f_i > 1$, then $|\lambda_i'| \leq |\lambda_i|$.

THEOREM 3.9. *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial, and let $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$ be an F-complete strongly optimal type of order $r \geq 1$. Then $[\phi_1, \dots, \phi_r]$ is an Okutsu frame of $F(x)$.*

Proof. Let $m_i' = \deg \phi_i$ for all $1 \leq i \leq r$, and $m_{r+1}' := \deg F$. We know that $m_{i+1}' = m_i' e_i f_i$ for all $1 \leq i \leq r$. Let $s = \operatorname{depth}(F)$ and consider the basic Okutsu invariants

$$m_1 < \cdots < m_s < m_{s+1} = \deg F, \qquad \mu_1 < \cdots < \mu_s < \mu_{s+1} = \infty.$$

Since $\phi_1(x)$ is irreducible modulo $\mathfrak{m}$, $F(x) \equiv \phi_1(x)^{(\deg F)/m_1'} \pmod{\mathfrak{m}}$, and $\deg F > m_1'$, Corollary 2.3 shows that $s \geq 1$ and $m_1' = m_1$. Let $F_1(x) \in \mathcal{O}[x]$ be any choice for the first polynomial of an Okutsu frame. The Newton polygons $N_{\phi_1}(F)$, $N_{F_1}(F)$ are both one-sided, of respective slopes $-v(\phi_1(\theta))$, $-v(F_1(\theta))$. Since $F_1(x)$ is a divisor polynomial of degree m_1 of $F(x)$ (Theorem 2.13), we have $v(\phi_1(\theta)) \leq v(F_1(\theta))$. Since $m_2' > m_1'$, Theorem 3.8 shows that the opposite inequality holds, so that $v(\phi_1(\theta)) = v(F_1(\theta))$. Now, by Theorem 2.13, $\phi_1(x)$ can also be taken as the first polynomial of an Okutsu frame of $F(x)$.

Suppose that for some $1 \leq i \leq r$, the polynomials $\phi_1, \dots, \phi_i$ can be taken as the first i polynomials of an Okutsu frame of $F(x)$. Let us show that in this case, $i = r$ if and only if $i = s$. In fact, suppose $i = r < s$, and let F_{r+1} be any $(r+1)$th polynomial in an Okutsu frame. Since $\mathbf{t}$ is F-complete, $N_r(F)$ is one-sided of slope λ_r and $R_r(F) \sim \psi_r(y)$; on the other hand, Theorem 3.5 shows that $N_r(F_{r+1})$ is one-sided of the same slope λ_r, and $R_r(F_{r+1}) \sim \psi_r(y)$ too. By Proposition 3.1(iii), $m_{r+1} = m_r e_r f_r = m_{r+1}' = \deg F$, and this contradicts the assumption $s > r$. Suppose now $i = s < r$. By Lemma 3.4, $v(\phi_{s+1}(\theta)) > (m_{s+1}'/m_s')v(\phi_s(\theta))$, and we get again a contradiction, since

$m'_{s+1} < m'_{r+1} = \deg F$ implies $v(\phi_{s+1}(\theta)) \le v(\phi_s(\theta)^{m'_{s+1}/m'_s})$, by Theorem 2.15.

Finally, suppose that for some $1 \le i < r$, the polynomials $\phi_1, \dots, \phi_i$ can be taken as the first i polynomials of an Okutsu frame of $F(x)$. We have just seen that also $i < s$; thus, there exists $F_{i+1}(x)$ such that $\phi_1, \dots, \phi_i, F_{i+1}$ are the first $i+1$ polynomials of an Okutsu frame of $F(x)$. By Theorem 3.5, $N_i(F_{i+1})$ is one-sided of the same slope λ_i as $N_i(F)$, and $R_i(F_{i+1}) \sim \psi_i(y)$, the monic irreducible factor of $R_i(F)(y)$; hence, $m_{i+1} = m_i e_i f_i = m'_i e_i f_i = m'_{i+1}$. In particular, F_{i+1} is another representative of the truncated type

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

and $v_{i+1}(F_{i+1}) = v_{i+1}(\phi_{i+1})$, since this value depends only on $\lambda_1, \dots, \lambda_i$ and $f_1, \dots, f_i$ [HN, Prop. 2.15]. By Theorem 3.8, $|\lambda'_{i+1}| \le |\lambda_{i+1}|$, where λ'_{i+1} is the slope of $N_{F_{i+1}, v_{i+1}}(F)$, and by the theorem of the polygon, (3.1), we have $v(F_{i+1}(\theta)) \le v(\phi_{i+1}(\theta))$. Now, since F_{i+1} is a divisor polynomial of degree m_{i+1} of $F(x)$ (Theorem 2.13), we have $v(F_{i+1}(\theta)) = v(\phi_{i+1}(\theta))$. Hence, $\phi_{i+1}(x)$ is a divisor polynomial of degree m_{i+1} of $F(x)$, and Theorem 2.13 shows that $\phi_1, \dots, \phi_i, \phi_{i+1}$ are the first $i+1$ polynomials of an Okutsu frame of $F(x)$. ∎

4. Okutsu approximations to an irreducible polynomial. Although Theorems 3.5 and 3.9 seem to indicate that the notion of Okutsu frame is equivalent to that of F-complete strongly optimal type, this is not quite exact. An F-complete strongly optimal type is an Okutsu frame together with extra information on $F(x)$ given by the data λ_r, $\psi_r(y)$.

In this section we introduce the notion of *Okutsu approximation* to $F(x)$: this is a monic irreducible polynomial in $\mathcal{O}[x]$ of the same degree and sufficiently close to $F(x)$. A better way to summarize the content of Theorems 3.5 and 3.9 is to think that an F-complete strongly optimal type is equivalent to an Okutsu frame, together with an Okutsu approximation to $F(x)$. After extending this point of view to the optimal case (Theorem 4.2), the Montes algorithm can be reinterpreted as a fast method to compute an Okutsu frame and an Okutsu approximation to each of the irreducible factors of a monic separable polynomial in $\mathcal{O}[x]$ (Section 4.2). Finally, Newton polygons can also be used to obtain approximations with arbitrary prescribed precision, leading in this way to a factorization algorithm (Section 4.3).

4.1. Okutsu approximations

Lemma-Definition 4.1. *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial of degree n, $\theta \in \overline{K}$ a root of $F(x)$ and $r = \operatorname{depth}(F)$. For any $\phi(x) \in \mathcal{O}[x]$, the following three conditions are equivalent*:

(i) *$\phi(x)$ is a monic irreducible separable polynomial of degree n, and it has a root $\alpha \in \overline{K}$ satisfying $v(\theta - \alpha) > \mu_r$.*

(ii) *$\phi(x)$ is a monic irreducible separable polynomial of degree n, and*

$$v(\phi(\theta)) > (n/m_r)v(F_r(\theta)),$$

where $F_r(x)$ is the rth polynomial of an Okutsu frame of $F(x)$.

(iii) *$\phi(x)$ is a representative of some F-complete strongly optimal type of order r.*

If any of these conditions is satisfied, we say that $\phi(x)$ is an Okutsu approximation *to $F(x)$.*

Proof. Lemma 2.12 shows that (i) and (ii) are equivalent. Let us show that (ii) and (iii) are equivalent too. Let $[F_1, \ldots, F_r]$ be an Okutsu frame of $F(x)$, and suppose that $\phi(x)$ satisfies (ii). By Theorem 3.5, there are negative rational numbers $\lambda_1, \ldots, \lambda_r$ and a monic irreducible polynomial $\psi_r(y)$ over some finite extension of $\mathbb{F}$, such that the type $(F_1(x); \lambda_1, F_2(x); \ldots; \lambda_{r-1}, F_r(x); \lambda_r, \psi_r(y))$ is F-complete and strongly optimal. Arguing as in the proof of Theorem 3.5, we deduce from Proposition 3.3 that $\phi(x)$ is a representative of this type.

Conversely, suppose $\phi(x)$ is a representative of an F-complete strongly optimal type $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \ldots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$. Then $\phi(x)$ is a monic irreducible polynomial of degree n [HN, Prop. 3.12]. By Theorem 3.9, $[\phi_1, \ldots, \phi_r]$ is an Okutsu frame of $F(x)$, and Lemma 3.4 shows that $v(\phi(\theta)) > (n/m_r)v(\phi_r(\theta))$. ∎

This concept leads to a reinterpretation of the arithmetic information contained in an f-complete optimal type, where $f(x) \in \mathcal{O}[x]$ is a monic separable polynomial.

THEOREM 4.2. *Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial, and let $\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \ldots; \lambda_{r-1}, \phi_r(x); \lambda_r, \psi_r(y))$ be an f-complete optimal type of order $r \geq 1$. Let $\phi_{r+1}(x) \in \mathcal{O}[x]$ be a representative of $\mathbf{t}$, and $f_{\mathbf{t}}(x) \in \mathcal{O}[x]$ the irreducible factor of $f(x)$ that corresponds to $\mathbf{t}$.*

- *If $e_r f_r > 1$, then $[\phi_1, \ldots, \phi_r]$ is an Okutsu frame of $f_{\mathbf{t}}(x)$ and $\phi_{r+1}(x)$ is an Okutsu approximation to $f_{\mathbf{t}}(x)$.*
- *If $e_r f_r = 1$, then $[\phi_1, \ldots, \phi_{r-1}]$ is an Okutsu frame of $f_{\mathbf{t}}(x)$ and $\phi_r(x), \phi_{r+1}(x)$ are both Okutsu approximations to $f_{\mathbf{t}}(x)$.*

Proof. If $e_r f_r > 1$, the type $\mathbf{t}$ is $f_{\mathbf{t}}$-complete and strongly optimal, and the statement is a consequence of Theorem 3.9 and Lemma-Definition 4.1.

If $e_r f_r = 1$, let us show first that the truncated type

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

is strongly optimal and $f_{\mathbf{t}}$-complete. Since $\deg\phi_r = e_{r-1}f_{r-1}\deg\phi_{r-1}$, we have $e_{r-1}f_{r-1} > 1$, and $\mathbf{t}_{r-1}$ is strongly optimal. Since $\mathbf{t}$ is f-complete, we have $R_r(f_{\mathbf{t}})(y) \sim \psi_r(y)$. By Proposition 3.1(i)&(ii), $N_r(f_{\mathbf{t}}) = N_r^-(f_{\mathbf{t}})$ is one-sided of slope λ_r; the length of this polygon is $\deg f_{\mathbf{t}}/\deg\phi_r = e_rf_r = 1$. By Proposition 3.1(iv)&(iii), $\mathrm{ord}_{\psi_{r-1}}(R_{r-1}(f_{\mathbf{t}})) = 1$, and $R_{r-1}(f_{\mathbf{t}})(y) \sim \psi_{r-1}(y)$, so that $\mathbf{t}_{r-1}$ is $f_{\mathbf{t}}$-complete.

Therefore, $[\phi_1,\dots,\phi_{r-1}]$ is an Okutsu frame of $f_{\mathbf{t}}(x)$ by Theorem 3.9. Since $\phi_r(x)$ is a representative of $\mathbf{t}_{r-1}$, it is an Okutsu approximation to $f_{\mathbf{t}}(x)$, by Lemma-Definition 4.1. Finally, $\phi_{r+1}(x)$ is also an Okutsu approximation to $f_{\mathbf{t}}(x)$, because $v(\phi_{r+1}(\theta)) > v(\phi_r(\theta))$, by Lemma 3.4. ∎

The following lemma is an immediate consequence of Lemma 2.4.

LEMMA 4.3. *If $\phi(x)$ is an Okutsu approximation to $F(x)$, then any Okutsu frame of $F(x)$ is an Okutsu frame of $\phi(x)$, and vice versa. In particular, the relation "to be an Okutsu approximation to" is an equivalence relation on the set of all monic irreducible polynomials in $\mathcal{O}[x]$.* ∎

This relation is strictly stronger than the equivalence relation "to have the same Okutsu frames". For instance, consider two representatives $\phi(x)$, $\phi'(x)$, of two optimal types $\mathbf{t},\mathbf{t}'$ of order r that differ only on the last data: $(\lambda_r,\psi_r(y)) \ne (\lambda'_r,\psi'_r(y))$, but they satisfy $e_rf_r = e'_rf'_r$; then $\phi(x),\phi'(x)$ are monic irreducible polynomials of the same degree, having the same Okutsu frames, but they are not Okutsu approximations to each other.

Thus, besides sharing with $F(x)$ all Okutsu invariants, an Okutsu approximation to $F(x)$ is close to $F(x)$ in some stronger sense, as the next result shows.

PROPOSITION 4.4. *Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible polynomial of degree n, $\theta \in \overline{K}$ a root of $F(x)$ and $L = K(\theta)$. Let $\phi(x) \in \mathcal{O}[x]$ be an Okutsu approximation to $F(x)$, $\alpha \in \overline{K}$ a root of $\phi(x)$ such that $v(\theta-\alpha) > \mu_r$, and $N = K(\alpha)$. Then*

(i) $e(N/K) = e(L/K)$, $f(N/K) = f(L/K)$.
(ii) *The maximal tamely ramified subextension of N/K is contained in L/K. In particular, if L/K is tamely ramified then $L = N$.*

Proof. By Lemma 2.6, $e(L/K) = e(N/K)$; since $[N:K] = [L:K]$, we have $f(L/K) = f(N/K)$ too. Item (ii) is a consequence of Proposition 2.7. ∎

We end this section with a measure of the precision of these Okutsu approximations. Let $\mathbf{t} = (\phi_1(x);\lambda_1,\phi_2(x);\dots;\lambda_{r-1},\phi_r(x);\lambda_r,\psi_r(y))$ be an F-complete optimal type. Let $h_1,\dots,h_r$, $e_1,\dots,e_r$, $f_0,f_1,\dots,f_r$, be the usual invariants of the type. Theorem 3.5 shows that $e(L/K) = e_1\cdots e_r$,

$f(L/K)=f_0f_1\cdots f_r$. Consider the rational number

$$\nu_{\mathbf{t}}:=\frac{h_1}{e_1}+\frac{h_2}{e_1e_2}+\cdots+\frac{h_r}{e_1\cdots e_r}.$$

By Proposition 3.1(iv), since $R_r(F)(y)\sim\psi_r(y)$, the Newton polygon $N_{r+1}^-(F)$ has length one and slope $\lambda_{r+1}=-h_{r+1}$ for some positive integer h_{r+1}; in particular, the minimal positive denominator of λ_{r+1} is $e_{r+1}=1$.

LEMMA 4.5. *Let $\phi(x)\in\mathcal{O}[x]$ be an Okutsu approximation to $F(x)$, constructed as a representative of an F-complete optimal type $\mathbf{t}$. Then*

$$F(x)\equiv\phi(x)\ (\mathrm{mod}\ \mathfrak{m}^{\lceil\nu\rceil}),\quad \textit{where}\quad \nu=\nu_{\mathbf{t}}+(h_{r+1}/e(L/K)).$$

Proof. Let $g(x)=\phi(x)-F(x)\in\mathcal{O}[x]$. This polynomial has degree less than n. Take $e_0=1$; since

$$n-1=(e_rf_r-1)m_r+\cdots+(e_1f_1-1)m_1+(e_0f_0-1),$$

Theorem 2.15 shows that

$$\begin{aligned}v(g(\theta))-v(g(x))&\le v(\phi_r(\theta)^{e_rf_r-1}\cdots\phi_1(\theta)^{e_1f_1-1}\theta^{e_0f_0-1})\\&=\sum_{i=1}^r(e_if_i-1)v(\phi_i(\theta)).\end{aligned}$$

Now, $g(\theta)=\phi(\theta)$, and by Lemma 3.4, applied to $\phi_{r+1}(x):=\phi(x)$, we get

$$\begin{aligned}v(g(x))&\ge v(\phi_{r+1}(\theta))-\sum_{i=1}^r(e_if_i-1)v(\phi_i(\theta))\\&=v(\phi_{r+1}(\theta))-\sum_{i=1}^r v(\phi_{i+1}(\theta))-v(\phi_i(\theta))-\frac{h_{i+1}}{e_1\cdots e_{i+1}}\\&=v(\phi_1(\theta))+\sum_{i=1}^r\frac{h_{i+1}}{e_1\cdots e_{i+1}}=\nu.\ \blacksquare\end{aligned}$$

4.2. Reinterpretation of the Montes algorithm. Let $f(x)\in\mathcal{O}[x]$ be a monic separable polynomial. The Montes algorithm starts by computing the order zero types determined by the irreducible factors of $f(x)$ modulo $\mathfrak{m}$, and then proceeds to enlarge them in a convenient way till several f-complete optimal types $\mathbf{t}_1,\dots,\mathbf{t}_s$ are obtained, which are in bijective correspondence with the irreducible factors $f_{\mathbf{t}_1}(x),\dots,f_{\mathbf{t}_s}(x)$ of $f(x)$ in $\mathcal{O}[x]$ ([HN], [GMNa]). This one-to-one correspondence is determined by the following properties:

(1) For all $1\le i\le s$, the type $\mathbf{t}_i$ is $f_{\mathbf{t}_i}$-complete.
(2) For all $j\ne i$, the type $\mathbf{t}_j$ does not divide $f_{\mathbf{t}_i}(x)$.

This enlargement process of the types is based on a branching phenomenon, plus a procedure taking care that all types we construct are optimal. Let us briefly explain how this works. Suppose the algorithm considers an optimal type of order i,

$$\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-1}, \phi_i(x); \lambda_i, \psi_i(y)),$$

dividing $f(x)$. If this type is not f-complete, it may ramify to produce new types, that are the germs of different f-complete types (thus, of different irreducible factors). A representative $\phi_{i+1}(x) \in \mathcal{O}[x]$ of $\mathbf{t}$ is constructed (in a noncanonical way); then $N_{i+1}(f) = N_{\phi_{i+1}, v_{i+1}}(f)$ is computed, and for each side of negative slope (say) λ, the residual polynomial $R_\lambda(f)(y) = R_{\phi_{i+1}, v_{i+1}, \lambda}(f)(y) \in \mathbb{F}_{i+1}[y]$ is computed and factorized into a product of irreducible factors. The type $\mathbf{t}$ ramifies in principle into as many types as pairs $(\lambda, \psi(y))$, where λ runs through the negative slopes of $N_{i+1}(f)$ and $\psi(y)$ runs through the different irreducible factors of $R_\lambda(f)(y)$. These branches determine either types of order $i+1$, or types of order i. To decide which is the case, one looks at the pair (e_i, f_i), where e_i is the least positive denominator of λ_i, and $f_i = \deg(\psi_i(y))$; if $e_i f_i > 1$ then $\phi_i(x)$ is an optimal representative of the truncated type $\mathbf{t}_{i-1}$ (in the sense of Theorem 3.8), and the branches lead to new optimal types of order $i+1$,

$$\mathbf{t}' = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-1}, \phi_i(x); \lambda_i, \phi_{i+1}(x); \lambda, \psi(y)),$$

dividing $f(x)$. If $e_i f_i = 1$ then $\phi_i(x)$ is not optimal, and we replace it by $\phi_i'(x) := \phi_{i+1}(x)$ to get a better representative of the truncated type $\mathbf{t}_{i-1}$; this is called a *refinement step* [GMNa, Sec. 3.2]. In this latter case, we consider new optimal types of order i dividing $f(x)$,

$$\mathbf{t}' = (\phi_1(x); \lambda_1, \phi_2(x); \dots; \lambda_{i-1}, \phi_i'(x); \lambda, \psi(y)), \qquad |\lambda| > |\lambda_i|,$$

that will be analyzed and ramified in a similar way.

The final output of the algorithm is a list of f-complete optimal types. Therefore, Theorems 3.9 and 4.2 have the following interpretation.

Corollary 4.6. *The output of the Montes algorithm is a family of Okutsu frames and Okutsu approximations to all the irreducible factors of $f(x)$.*

Corollary 4.6 opens new perspectives in the applications of the Montes algorithm, as a tool to compute the essential arithmetic information about the irreducible factors of $f(x)$, carried by their Okutsu frames and their Okutsu approximations [GMNb].

We finish this section with an example that illustrates when strongly optimal f-complete types may occur.

Example. Let p be an odd prime number, and $\phi(x) \in \mathbb{Z}_p[x]$ a monic polynomial which is irreducible modulo p. Take $c \in \mathbb{Z}_p$ such that $c \equiv 1 \pmod{p}$, and consider the polynomial $f(x) = \phi(x)^2 + p^2 c$. Clearly, $N_\phi(f)$ is one-sided of length 2 and slope -1, whereas $R_{\phi,-1}(f)(y) = y^2 + 1 \in \mathbb{F}_p[y]$.

If $p \equiv 3 \pmod 4$, the Montes algorithm outputs the f-complete and strongly optimal type $\mathbf{t} = (\phi(x); -1, y^2 + 1)$. In this case, $f(x) = f_{\mathbf{t}}(x)$ is irreducible of depth one, $[\phi]$ is an Okutsu frame of $f(x)$, and any representative of $\mathbf{t}$ (e.g., $\phi_2(x) = \phi(x)^2 + p^2$) is an Okutsu approximation to $f(x)$.

If $p \equiv 1 \pmod 4$, there is some $i \in \mathbb{Z}_p$ satisfying $i^2 = -1$. In this case the residual polynomial $R_{\phi,-1}(f)(y)$ factorizes as $y^2 + 1 = (y - \bar{i})(y + \bar{i})$ in $\mathbb{F}_p[y]$, and the Montes algorithm outputs two types:

$$\mathbf{t} = (\phi(x); -1, y - \bar{i}), \qquad \mathbf{t}' = (\phi(x); -1, y + \bar{i}).$$

These types are f-complete and optimal, but not strongly optimal; they correspond to the two irreducible factors of $f(x)$: $f_{\mathbf{t}}(x) = \phi(x) - ip\sqrt{c}$, $f_{\mathbf{t}'}(x) = \phi(x) + ip\sqrt{c}$, both of depth zero. Let $\phi_2(x) = \phi(x) - ip$, $\phi_2'(x) = \phi(x) + ip$ be representatives respectively of $\mathbf{t}$ and $\mathbf{t}'$. The five polynomials $\phi, f_{\mathbf{t}}, f_{\mathbf{t}'}, \phi_2, \phi_2'$ are Okutsu approximations to one another, since

$$f_{\mathbf{t}}(x) \equiv f_{\mathbf{t}'}(x) \equiv \phi_2(x) \equiv \phi_2'(x) \equiv \phi(x) \pmod p.$$

They are all representatives of the type of order zero, $\mathbf{t}_0 = \phi(y) \pmod p$, which is $f_{\mathbf{t}}$-complete and $f_{\mathbf{t}'}$-complete, but not f-complete.

Note that $\phi_2(x)$ (respectively $\phi_2'(x)$) is a better approximation to $f_{\mathbf{t}}(x)$ (respectively $f_{\mathbf{t}'}(x)$) than $\phi(x)$. This is the basic idea behind a method to get approximations of arbitrarily high precision, to be explained in the next section.

4.3. Applications to local factorization. For many purposes, an Okutsu approximation yields sufficient arithmetic information about an irreducible factor $F(x)$ of $f(x)$, the extension L/K that it determines, and its subextensions. However, the setting of the Montes algorithm can also be used to compute an approximation to each irreducible factor of $f(x)$, with an arbitrary prescribed precision, leading in this way to a factorization algorithm. The basic idea is to continue the process of enlarging the f-complete types.

Let us describe this factorization algorithm in detail. The input polynomial is a monic separable polynomial $f(x) \in \mathcal{O}[x]$. First, we compute all f-complete types parameterizing the irreducible factors of $f(x)$, and an Okutsu approximation to each factor, by a single call to the Montes algorithm. Then, for each complete type $\mathbf{t}$, with representative $\phi_{r+1}(x)$, we compute the Newton polygon $N_{r+1}^-(f)$ and the residual polynomial $R_{r+1}(f)(y) \sim \psi_{r+1}(y)$. By Proposition 3.1, this polygon has length one, a negative slope $\lambda_{r+1} = -h_{r+1}$ for some positive integer h_{r+1}, and $\psi_{r+1}(y) \in \mathbb{F}_{r+1}[y]$ is a monic irreducible polynomial of degree one.

In order to get a better approximation to $f_{\mathbf{t}}(x)$, we compute a representative $\phi_{r+2}(x)$ of the following type of order $r+1$:

$$\mathbf{t}' = (\phi_1(x); \lambda_1, \phi_2(x); \ldots; \lambda_{r-1}, \phi_r(x); \lambda_r, \phi_{r+1}(x); -h_{r+1}, \psi_{r+1}(y)).$$

By Lemma 3.4, $v(\phi_{r+2}(\theta)) > v(\phi_{r+1}(\theta))$, so that $\phi_{r+2}(x)$ is another Okutsu approximation to $f_{\mathbf{t}}(x)$, by Lemma-Definition 4.1(ii). The slope of the polygon $N_{r+2}(f)$ determines the precision of the new approximation. However, computations in order $r+2$ have a higher complexity than computations in order $r+1$. Therefore, we consider $\phi_{r+2}(x)$ as a new representative of the type $\mathbf{t}$, say $\phi'_{r+1}(x) := \phi_{r+2}(x)$, and we repeat the procedure with the new representative: we compute the slope $-h'_{r+1}$ of $N'_{r+1}(f) = N'_{\phi'_{r+1},v_{r+1}}(f)$ and the residual polynomial $R'_{-h_{r+1}}(f)(y)$. By Lemma 4.5, the new precision of the approximation is

$$\nu' = \nu_{\mathbf{t}} + \frac{h'_{r+1}}{e(L/\mathbb{Q}_p)}.$$

Since $v(\phi'_{r+1}(\theta)) > v(\phi_{r+1}(\theta))$, we have $h'_{r+1} > h_{r+1}$, and the new approximation is better than the former one. Note that each iteration requires three computations in order $r+1$: a Newton polygon of length one, a residual polynomial of degree one and a representative of the extended type $\mathbf{t}'$. One can perform the necessary number of iterations till a prefixed precision is attained.

The scheme of the factorization algorithm would be the following:

Input. A monic separable polynomial $f(x) \in \mathcal{O}[x]$ and a precision $N \in \mathbb{N}$.

Output. A family of monic irreducible polynomials $f_1(x), \dots, f_s(x)$ in $\mathcal{O}[x]$, satisfying $f_i(x) \equiv f_{\mathbf{t}_i}(x) \pmod{\mathfrak{m}^N}$ for $1 \le i \le s$, where the polynomials $f_{\mathbf{t}_1}(x), \dots, f_{\mathbf{t}_s}(x)$ are the genuine irreducible factors of $f(x)$ in $\mathcal{O}[x]$.

1. Apply the Montes algorithm to compute f-complete types $\mathbf{t}_1, \dots, \mathbf{t}_s$, corresponding to the irreducible factors of $f(x)$ in $\mathcal{O}[x]$.
2. For each f-complete type $\mathbf{t}$, let r be the order of $\mathbf{t}$, and:
   3. Compute $\nu_{\mathbf{t}} = \sum_{i=1}^{r} h_i/e_1 \cdots e_i$, and $e = e_1 \cdots e_r$.
   4. Compute a representative $\phi(x) \in \mathcal{O}[x]$ of $\mathbf{t}$.
   5. Compute $N_{r+1}(f)$, and let the slope of this one-sided polygon be $-h$. If $\lceil \nu_{\mathbf{t}} + (h/e) \rceil \ge N$ output $\phi(x)$ as the final approximation to $f_{\mathbf{t}}(x)$, and consider the next f-complete type. Else:
   6. Compute $R_{r+1}(f)(y) \sim \psi(y)$ for some monic polynomial $\psi(y) \in \mathbb{F}_{r+1}[y]$ of degree one.
   7. Compute a representative $\phi'(x)$ of the type $\mathbf{t}'$ of order $r+1$ obtained by enlarging $\mathbf{t}$ with the triple $(\phi; -h, \psi(y))$.
   8. Replace $\phi(x) \leftarrow \phi'(x)$ and go to step 5.

This algorithm has some advantages: it has very low memory requirements, and it always outputs a family $f_1(x), \dots, f_s(x) \in \mathcal{O}[x]$ of monic irreducible polynomials that satisfy $f(x) \equiv f_1(x) \cdots f_s(x) \pmod{\mathfrak{m}^N}$, regardless of the value of the imposed precision N.

As to the disadvantages: although the algorithm computes each new approximation very fast, it has a slow convergence because at each step the improvement of the precision is rather small.

Probably, an optimal local factorization algorithm would consist in the application of the Montes algorithm as a fast method to get an Okutsu approximation to each irreducible factor, combined with an efficient "Hensel lift" routine able to improve these initial approximations by doubling the precision at each iteration. One may speculate that Newton polygons of higher order might also be used to design a similar acceleration procedure.

Acknowledgements. This research was partially supported by grants MTM2009-13060-C02-02 and MTM2009-10359 from the Spanish MEC.

References

[HN] J. Guàrdia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, arXiv:0807.2620v2[math.NT]; Trans. Amer. Math. Soc., to appear.

[GMNa] —, —, —, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, arXiv:0807.4065v3[math.NT].

[GMNb] —, —, —, *A new computational approach to ideal theory in number fields*, arXiv:1005.1156v1[math.NT].

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

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., PWN, Warszawa, and Springer, Berlin, 1990.

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

[Ore] Ö. Ore, *Zur Theorie der algebraischen Körper*, Acta Math. 44 (1923), 219–314.

Jordi Guàrdia
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: guardia@ma4.upc.edu

Jesús Montes
Departament de Ciències
Econòmiques i Socials
Facultat de Ciències Socials
Universitat Abat Oliba CEU
Bellesguard 30
E-08022 Barcelona, Catalonia, Spain
E-mail: montes3@uao.es

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

Received on 21.11.2009
and in revised form on 15.4.2010 (6222)