A NEW COMPUTATIONAL APPROACH TO IDEAL THEORY IN NUMBER FIELDS

JORDI GUÀRDIA, JESÚS MONTES, AND ENRIC NART

ABSTRACT. Let K be the number field determined by a monic irreducible polynomial $f(x)$ with integer coefficients. In previous papers we parameterized the prime ideals of K in terms of certain invariants attached to Newton polygons of higher order of $f(x)$. In this paper we show how to carry out the basic operations on fractional ideals of K in terms of these constructive representations of the prime ideals. From a computational perspective, these results facilitate the manipulation of fractional ideals of K avoiding two heavy tasks: the construction of the maximal order of K and the factorization of the discriminant of $f(x)$. The main computational ingredient is Montes algorithm, which is an extremely fast procedure to construct the prime ideals.

INTRODUCTION

Let K be a number field of degree n and $\mathbb{Z}_K$ its ring of integers. An essential task in Algorithmic Number Theory is to construct the prime ideals of K in terms of a defining equation of K, usually given by a monic and irreducible polynomial $f(x) \in \mathbb{Z}[x]$. The standard approach to do this, followed by most of the algebraic manipulators like `Kant`, `Pari`, `Magma` or `Sage`, is based on the previous computation of an integral basis of $\mathbb{Z}_K$. This approach has a drawback: one needs to factorize the discriminant, $\mathrm{disc}(f)$, of $f(x)$, which can be a heavy task, even in number fields of low degree, if $f(x)$ has large coefficients.

In this paper we present a direct construction of the prime ideals, that avoids the computation of the maximal order of K and the factorization of $\mathrm{disc}(f)$. The following tasks concerning fractional ideals can be carried out using this construction:

(1) Compute the $\mathfrak{p}$-adic valuation, $v_{\mathfrak{p}}\colon K^* \to \mathbb{Z}$, for any prime ideal $\mathfrak{p}$ of K.
(2) Obtain the prime ideal decomposition of a fractional ideal.
(3) Compute a two-elements representation of a fractional ideal.
(4) Add, multiply and intersect fractional ideals.
(5) Compute the reduction maps, $\mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{p}$.
(6) Solve Chinese remainders problems.

Moreover, along the construction of a prime ideal $\mathfrak{p}$, lying over a prime number p, a $\mathbb{Z}_p$-basis of the ring of integers of the local field $K_{\mathfrak{p}}$ is obtained as a by-product. Hence, from the prime ideal decomposition of the ideal $p\mathbb{Z}_K$ we are also able to derive the resolution of another task:

(7) Compute a p-integral basis of K.

For a given prime number p, the prime ideals of K lying above p are in one-to-one correspondence with the irreducible factors of $f(x)$ in $\mathbb{Z}_p[x]$ [Hen08]. In the paper [HN12] we proved a series of recurrent generalizations of Hensel lemma, leading to a constructive procedure to obtain a family of f-*complete types*, that parameterize the irreducible factors of $f(x)$ in $\mathbb{Z}_p[x]$. A type is an object that gathers combinatorial and arithmetic data attached to Newton polygons of $f(x)$ of higher order, and an f-complete type contains enough information to single out a p-adic irreducible factor of $f(x)$. In [GMN11] we described Montes algorithm, which optimizes the construction of the f-complete types; it outputs a list of f-complete and optimal types that parameterize the prime ideals of K lying above p, and contain valuable arithmetic information on each prime ideal. All these results were based on the PhD thesis of the second author [Mon99]. The algorithm is extremely fast in practice. Its complexity has been recently estimated in [FV10] and [Pau10]. Assuming ordinary arithmetic, it requires $O\left(n^3 \log(\mathrm{disc}(f))^3\right)$ operations in integers less than p.

In [GMN10] we reinterpreted the invariants stored by the optimal types in terms of the Okutsu polynomials attached to the p-adic irreducible factors of $f(x)$ [Oku82]. Suppose $\mathbf{t}$ is the f-complete and optimal type attached to a prime ideal $\mathfrak{p}$, corresponding to a monic irreducible factor $f_\mathfrak{p}(x) \in \mathbb{Z}_p[x]$; then, the arithmetic information stored in $\mathbf{t}$ is synthesized by two invariants of $f_\mathfrak{p}(x)$: an *Okutsu frame* $[\phi_1(x), \ldots, \phi_r(x)]$ and an *Okutsu approximation* $\phi_\mathfrak{p}(x)$ (cf. loc.cit.). The monic polynomials $\phi_1, \ldots, \phi_r, \phi_\mathfrak{p}$ have integer coefficients and they are all irreducible over $\mathbb{Z}_p[x]$; the polynomial $\phi_\mathfrak{p}(x)$ is "sufficiently close" to $f_\mathfrak{p}(x)$. We say that

$$\mathfrak{p} = [p; \phi_1, \ldots, \phi_r, \phi_\mathfrak{p}],$$

is an *Okutsu-Montes representation* of the prime ideal $\mathfrak{p}$. Thus, from the computational point of view, $\mathfrak{p}$ is structured in $r + 1$ levels and at each level one needs to compute (and store) several Okutsu invariants that are omitted in this notation. This computational representation of $\mathfrak{p}$ is essentially canonical: the Okutsu invariants of $\mathfrak{p}$, distributed along the different levels, depend only on the defining equation $f(x)$. These invariants provide a rich and exhaustive source of information about the arithmetic properties of $\mathfrak{p}$, which is crucial in the computational treatment of $\mathfrak{p}$.

From a historical perspective, the sake for a constructive representation of ideals goes back to the very foundation of algebraic number theory. Kummer had the insight that the prime numbers factorize in number fields into the product of prime "ideal numbers", and he tried to construct them as symbols $[p; \phi]$, where $\phi(x)$ is a monic lift to $\mathbb{Z}[x]$ of an irreducible factor of $f(x)$ modulo p. Dedekind showed that these ideas led to a coherent theory only in the case that p does not divide the index $i(f) := (\mathbb{Z}_K : \mathbb{Z}[x]/(f(x)))$. This constructive approach could not be universally used because there are number fields in which p divides the index of all defining equations [Ded78]. Fortunately, this obstacle led Dedekind to invent ideal theory as the only way to perform a decent arithmetic in number fields. Ore, in his Phd thesis [Ore23], tried to regain the constructive approach to ideal theory. He generalized and improved the classical tool of Newton polygons and showed that under the assumption that the defining equation is p-*regular* (a much weaker condition than Dedekind's condition $p \nmid i(f)$), the prime ideals dividing p can be parameterized as $\mathfrak{p} = [p; \phi, \phi_\mathfrak{p}]$ (in our notation), where $\phi_\mathfrak{p}(x) \in \mathbb{Z}[x]$ is certain polynomial whose

ϕ-Newton polygon is one-sided and the residual polynomial attached to this side is irreducible (cf. section 1). The contribution of [Mon99] was to extend Ore's ideas in order to obtain a similar construction of the prime ideals in the general case.

The aim of this paper is to show how to use this constructive representation of the prime ideals to carry out the above mentioned tasks (1)-(6) on fractional ideals and to compute p-integral bases. The outline of the paper is as follows. In section 1 we recall the structure of types, we describe their invariants, and we review the process of construction of the Okutsu-Montes representations of the prime ideals. In section 2 we show how to compute the $\mathfrak{p}$-adic valuation of K with respect to a prime ideal $\mathfrak{p}$; this is the key ingredient to obtain the factorization of a fractional ideal as a product of prime ideals (with integer exponents). The operations of sum, multiplication and intersection of fractional ideals are trivially based on these tasks. In section 3 we show how to find integral elements $\alpha_{\mathfrak{p}} \in \mathbb{Z}_K$ such that $\mathfrak{p}$ is the ideal of $\mathbb{Z}_K$ generated by p and $\alpha_{\mathfrak{p}}$; this leads to the computation of a two-elements representation of any fractional ideal. In section 4, we show how to compute residue classes modulo prime ideals and we design a chinese remainder theorem routine. Section 5 is devoted to the construction of a p-integral basis.

We have implemented a package in `Magma` that performs all the above mentioned tasks; in section 6 we present several examples showing the excellent performance of the package in cases that the standard packages cannot deal with. Our routines work extremely fast as long as we deal only with fractional ideals whose norm may be factorized. Even in cases where $\mathrm{disc}(f)$ may be factorized and an integral basis of $\mathbb{Z}_K$ is available, our methods work faster than the standard ones if the degree of K is not too small. Mainly, this is due to the fact that we avoid the use of linear algebra routines (computation of $\mathbb{Z}$-bases of ideals, Hermite and Smith normal forms of $n \times n$ matrices, etc.), that dominate the complexity when the degree n grows. Finally, in section 7 we make some comments on the apparent limits of these Montes' techniques: they are not yet able to test if a fractional ideal is principal. Also, we briefly mention that the results of this paper may be extended to the function field case, and the similar challenges that arise in this geometric context.

Notations.   Throughout the paper we fix a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n, and a root $\theta \in \overline{\mathbb{Q}}$ of $f(x)$. We let $K = \mathbb{Q}(\theta)$ be the number field generated by θ, and $\mathbb{Z}_K$ its ring of integers.

1. OKUTSU-MONTES REPRESENTATIONS OF PRIME IDEALS

Let p be a prime number. In this section we recall Montes algorithm and we describe the structure of the f-complete and optimal types that parameterize the prime ideals of K lying over p. The results are mainly extracted from [HN12] (HN standing for "Higher Newton") and [GMN11].

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

1.1. **Types and their invariants.** Let $v \colon \overline{\mathbb{Q}}_p^* \to \mathbb{Q}$ be the canonical extension of the p-adic valuation of $\mathbb{Q}_p$ to a fixed algebraic closure. We extend v to the discrete valuation v_1 on the field $\mathbb{Q}_p(x)$, determined by:

$$v_1 \colon \mathbb{Q}_p[x] \longrightarrow \mathbb{Z} \cup \{\infty\}, \quad v_1(b_0 + \cdots + b_r x^r) := \min\{v(b_j), 0 \le j \le r\}.$$

Denote by $\mathbb{F}_0 := \mathrm{GF}(p)$ the prime field of characteristic p, and consider the 0-th *residual polynomial* operator

$$R_0 \colon \mathbb{Z}_p[x] \longrightarrow \mathbb{F}_0[y], \quad g(x) \mapsto \overline{g(y)/p^{v_1(g)}},$$

where, $\overline{}\colon \mathbb{Z}_p[y] \to \mathbb{F}_0[y]$, is the natural reduction map. A *type of order zero*,

$$\mathbf{t} = \psi_0(y),$$

is just a monic irreducible polynomial $\psi_0(y) \in \mathbb{F}_0[y]$. A *representative* of $\mathbf{t}$ is any monic polynomial $\phi_1(x) \in \mathbb{Z}[x]$ 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 $g(x) \in \mathbb{Q}_p[x]$. If $g(x) = \sum_{s \geq 0} a_s(x)\phi_1(x)^s$ 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 $(s, v_1(a_s(x)\phi_1(x)^s))$ [HN12, 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 $\mathbb{Q}_p(x)$, constructed as follows: for any nonzero polynomial $g(x) \in \mathbb{Z}_p[x]$, take a line of slope λ_1 far below $N_1(g)$ and let it shift upwards till it touches the polygon for the first time; if $(0, H)$ is the intersection point of this line with the vertical axis, then $v_2(g(x)) = e_1 H$, by definition. Also, the triple (ϕ_1, v_1, λ_1) determines a residual polynomial operator

$$R_1 := R_{\phi_1, v_1, \lambda_1} \colon \mathbb{Z}_p[x] \longrightarrow \mathbb{F}_1[y], \quad \mathbb{F}_1 := \mathbb{F}_0[y]/(\psi_0(y)),$$

which is a kind of reduction of first order of $g(x)$ [HN12, Def. 1.9].

Let $\psi_1(y) \in \mathbb{F}_1[y]$ be a monic irreducible polynomial, $\psi_1(y) \neq y$. The triple

$$\mathbf{t} = (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)))$$

is called a *type of order one*. Given any such type, one can compute a representative of $\mathbf{t}$; that is, a monic polynomial $\phi_2(x) \in \mathbb{Z}[x]$ of degree $e_1 \deg \psi_1 \deg \phi_1$, satisfying $R_1(\phi_2)(y) \sim \psi_1(y)$. Now we may start over with the pair (ϕ_2, v_2) and repeat all constructions in order two.

The iteration of this procedure leads to the concept of *type of order r* [HN12, Sec. 2]. A type of order $r \geq 1$ is a chain:

$$\mathbf{t} = (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots ; (\phi_r(x), \lambda_r, \psi_r(y))),$$

where $\phi_1(x), \ldots, \phi_r(x)$ are monic polynomials in $\mathbb{Z}[x]$ that are irreducible in $\mathbb{Z}_p[x]$, $\lambda_1, \ldots, \lambda_r$ are negative rational numbers, and $\psi_0(y) \in \mathbb{F}_0[y], \ldots, \psi_r(y) \in \mathbb{F}_r[y]$ are monic irreducible polynomials over certain finite fields $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r$ (to be specified below), that satisfy the following recursive properties:

(1) $R_0(\phi_1)(y) = \psi_0(y)$. We define $\mathbb{F}_1 = \mathbb{F}_0[y]/(\psi_0(y))$.
(2) For all $1 \leq i < r$,
- $\deg \phi_i | \deg \phi_{i+1}$,
- $N_i(\phi_{i+1}) := N_{\phi_i, v_i}(\phi_{i+1})$ is one-sided of slope λ_i, and
- $R_i(\phi_{i+1})(y) := R_{\phi_i, v_i, \lambda_i}(\phi_{i+1})(y) \sim \psi_i(y)$.
We define $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_i(y))$.
(3) $\psi_r(y) \neq y$. We define $\mathbb{F}_{r+1} = \mathbb{F}_r[y]/(\psi_r(y))$.

Thus, a type of order r is an object structured in r levels. In the computational representation of a type, several invariants are stored at each level, $1 \leq i \leq r$. The

most important ones are:

$$\begin{array}{ll}
\phi_i(x), & \text{monic polynomial in } \mathbb{Z}[x], \text{ irreducible over } \mathbb{Z}_p[x] \\
m_i, & \deg \phi_i(x), \\
V_i := v_i(\phi_i) & \text{non-negative integer,} \\
\lambda_i = -h_i/e_i, & h_i, e_i \text{ positive coprime integers,} \\
\ell_i, \ell'_i, & \text{a pair of integers satisfying } \ell_i h_i - \ell'_i e_i = 1, \\
\psi_i(y), & \text{monic irreducible polynomial in } \mathbb{F}_i[y], \\
f_i & \deg \psi_i(y), \\
z_i & \text{the class of } y \text{ in } \mathbb{F}_{i+1}, \text{ so that } \psi_i(z_i) = 0.
\end{array}$$

Take $f_0 := \deg \psi_0$, and let $z_0 \in \mathbb{F}_1$ be the class of y, so that $\psi_0(z_0) = 0$. Note that $m_i = (f_0 f_1 \cdots f_{i-1})(e_1 \cdots e_{i-1})$, $\mathbb{F}_{i+1} = \mathbb{F}_i[z_i]$, and $\dim_{\mathbb{F}_0} \mathbb{F}_{i+1} = f_0 f_1 \cdots f_i$. The discrete valuations $v_1, \ldots, v_{r+1}$ on the field $\mathbb{Q}_p(x)$ are essential invariants of the type.

Definition 1.1. *Let $g(x) \in \mathbb{Z}_p[x]$ be a monic separable polynomial, and $\mathbf{t}$ a type of order $r \geq 1$.*

(1) We say that $\mathbf{t}$ divides $g(x)$ (and we write $\mathbf{t} \mid g(x)$), if $\psi_r(y)$ divides $R_r(g)(y)$ in $\mathbb{F}_r[y]$.

(2) We say that $\mathbf{t}$ is g-complete if $\mathrm{ord}_{\psi_r}(R_r(g)) = 1$. In this case, $\mathbf{t}$ singles out a monic irreducible factor $g_{\mathbf{t}}(x) \in \mathbb{Z}_p[x]$ of $g(x)$, uniquely determined by the property $R_r(g_{\mathbf{t}})(y) \sim \psi_r(y)$. If $K_{\mathbf{t}}$ is the extension of $\mathbb{Q}_p$ determined by $g_{\mathbf{t}}(x)$, then

$$e(K_{\mathbf{t}}/\mathbb{Q}_p) = e_1 \cdots e_r, \qquad f(K_{\mathbf{t}}/\mathbb{Q}_p) = f_0 f_1 \cdots f_r.$$

(3) A representative of $\mathbf{t}$ is a monic polynomial $\phi_{r+1}(x) \in \mathbb{Z}[x]$, of degree $m_{r+1} = e_r f_r m_r$ such that $R_r(\phi_{r+1})(y) \sim \psi_r(y)$. This polynomial is necessarily irreducible in $\mathbb{Z}_p[x]$. By the definition of a type, each $\phi_{i+1}(x)$ is a representative of the truncated type of order i

$$\mathrm{Trunc}_i(\mathbf{t}) := (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots ; (\phi_i(x), \lambda_i, \psi_i(y))).$$

(4) We say that $\mathbf{t}$ is optimal if $m_1 < \cdots < m_r$, or equivalently, if $e_i f_i > 1$, for all $1 \leq i < r$.

Lemma 1.2. *Let $\mathbf{t}$ be a type of order r. Then, $v_j(\phi_i) = (m_i/m_j)V_j$, for all $j < i \leq r$.*

Proof. Let $\phi_i(x) = \sum_{s \geq 0} a_s(x)\phi_j(x)^s$ be the ϕ_j-adic development of ϕ_i. By [HN12, Lem. 2.17], $v_j(\phi_i) = \min_{s \geq 0}\{v_j(a_s \phi_j^s)\}$. Now, $N_j(\phi_i)$ is one-sided of slope λ_j, because ϕ_i is a polynomial of type $\mathrm{Trunc}_j(\mathbf{t})$ [HN12, Def. 2.1+Lem. 2.4(1)]. Since the principal term of the development is $\phi_j^{m_i/m_j}$, we get $v_j(\phi_i) = v_j(\phi_j^{m_i/m_j}) = (m_i/m_j)v_j(\phi_j) = (m_i/m_j)V_j$. $\square$

1.2. **Certain rational functions.** Let $\mathbf{t}$ be a type of order r. We attach to $\mathbf{t}$ several rational functions in $\mathbb{Q}(x)$ [HN12, Sec. 2.4]. Note that V_i is always divisible by e_{i-1} [HN12, Thm. 2.11].

Definition 1.3. *Let $\pi_0(x) = 1$, $\pi_1(x) = p$. We define recursively for all $1 \leq i \leq r$:*

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

These rational functions can be written as a product of powers of $p, \phi_1(x), \ldots, \phi_r(x)$, with integer exponents.

Notation. Let $\Psi(x) = p^{n_0}\phi_1(x)^{n_1}\cdots\phi_s(x)^{n_s} \in \mathbb{Q}(x)$ be a rational function which is a product of powers of $p, \phi_1, \ldots, \phi_s$, with integer exponents. We denote:

$$\log_{\mathbf{t},s}\Psi = (n_0, \ldots, n_s) \in \mathbb{Z}^{s+1}.$$

The next result is inspired by [HN12, Cor. 4.26].

Lemma 1.4. *Let $F(x) \in \mathbb{Z}_p[x]$ be a monic irreducible polynomial divisible by $\mathbf{t}$, and let $\alpha \in \overline{\mathbb{Q}}_p$ be a root of $F(x)$. For some $1 \le s \le r$, let $\Psi(x) = p^{n_0}\phi_1(x)^{n_1}\cdots\phi_s(x)^{n_s}$ be a rational function in $\mathbb{Q}(x)$, such that $v(\Psi(\alpha)) = 0$. Then,*

$$\Psi(x) = \gamma_1(x)^{t_1}\cdots\gamma_s(x)^{t_s},$$

for integer exponents $t_1, \ldots, t_s$, which can be computed by the following algorithm:

1. vec$\leftarrow (n_0, \ldots, n_s)$.
2. *for $i=s$ to 1 by -1 do* $\quad t_i \leftarrow$vec$[i]/e_i,$ $\quad$vec$\leftarrow$vec$-t_i\log_{\mathbf{t},s}\gamma_i,$ $\quad$ *end for.*

Proof. By [HN12, (17)] and [HN12, Cor. 3.2]:

$$\log_{\mathbf{t},s}\Phi_s = (\ldots\ldots,1), \;\; \log_{\mathbf{t},s}\pi_s = (\ldots\ldots,0), \;\; \log_{\mathbf{t},s}\gamma_s = (\ldots\ldots,e_s) \in \mathbb{Z}^{s+1},$$

$$v(\phi_s(\alpha)) = \sum_{i=1}^{s} e_i f_i \cdots e_{s-1} f_{s-1} \frac{h_i}{e_1\cdots e_i}, \qquad v(\gamma_s(\alpha)) = 0.$$

Since $v(\Psi(\alpha)) = 0$, the formula for $v(\phi_s(\alpha))$ shows that $e_s|n_s$. Thus, we can replace $\Psi(x)$ by $\Psi(x)\gamma_s^{-n_s/e_s}$ and iterate the argument. Since $v(\gamma_s(\alpha)) = 0$, the new $\Psi(x)$ satisfies $v(\Psi(\alpha)) = 0$ as well, and the s-th coordinate of $\log_{\mathbf{t},s}\Psi$ is zero. At the last step $(i = 1)$, we get $\Psi(x) = p^{n'_0}\phi_1^{n'_1}$, with $n'_0 + n'_1(h_1/e_1) = 0$. Then, clearly $\Psi(x) = \gamma_1(x)^{n'_1/e_1}$. $\qquad\square$

1.3. **Montes algorithm and the secondary invariants.** At the input of the pair $(f(x), p)$, Montes algorithm computes a family $\mathbf{t}_1, \ldots, \mathbf{t}_g$ of f-complete and optimal types in one-to-one correspondence with the irreducible factors $f_{\mathbf{t}_1}(x), \ldots, f_{\mathbf{t}_g}(x)$ of $f(x)$ in $\mathbb{Z}_p[x]$. This one-to-one correspondence is determined by:

(1) For all $1 \le i \le g$, 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 $f_{\mathbf{t}_i}(x)$.

The algorithm starts by computing the order zero types determined by the irreducible factors of $f(x)$ modulo p, and then proceeds to enlarge them in a convenient way till the whole list of f-complete optimal types is obtained [GMN11].

With regard to the computation of generators of the prime ideals and Chinese remainder multipliers, the algorithm is slightly modified to compute and store some other (secondary) invariants at each level of all types $\mathbf{t}$ considered by the algorithm:

Refinements$_i$,   a list of pairs $[\phi(x), \lambda]$, where ϕ is a representative of
                  Trunc$_{i-1}(\mathbf{t})$ and λ a negative slope,
w_i,   a nonnegative integer called the *height*,
Quot$_i$,   a list of e_i polynomials in $\mathbb{Z}[x]$,
$(\log \Phi)_i$,   the vector $\log_{\mathbf{t},i}\Phi_i \in \mathbb{Z}^{i+1}$,
$(\log \pi)_i$,   the vector $\log_{\mathbf{t},i}\pi_i \in \mathbb{Z}^{i+1}$,
$(\log \gamma)_i$,   the vector $\log_{\mathbf{t},i}\gamma_i \in \mathbb{Z}^{i+1}$.

Let us briefly explain the flow of the algorithm and the computation of these invariants. Suppose a type of order $i - 1$ dividing $f(x)$ is considered,

$$\mathbf{t} = (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots ; (\phi_{i-1}(x), \lambda_{i-1}, \psi_{i-1}(y))).$$

A representative $\phi_i(x)$ is constructed. Suppose that either $i = 1$ or $m_1 < \cdots < m_i$. Let $\ell = \operatorname{ord}_{\psi_{i-1}} R_{i-1}(f)$. If $\mathbf{t}$ is not f-complete ($\ell > 1$), it may ramify to produce new types, that will be germs of distinct f-complete types. To carry out this ramification process we compute simultaneously the first $\ell + 1$ coefficients of the ϕ_i-adic development of $f(x)$ and the corresponding quotients:

$$
\begin{array}{rcl}
f(x) & = & \phi_i(x)q_1(x) + a_0(x), \\
q_1(x) & = & \phi_i(x)q_2(x) + a_1(x), \\
\cdots & & \cdots \\
q_\ell(x) & = & \phi_i(x)q_{\ell+1}(x) + a_\ell(x).
\end{array}
$$

(1)

The Newton polygon of i-th order of $f(x)$, $N_i(f)$, is the lower convex envelope of the set of points $(s, v_i(a_s\phi_i^s))$ of the plane, for all $s \geq 0$. However, we need to build up only the *principal part* of this polygon, $N_i^-(f) = N_{\phi_i,v_i}^-(f)$, formed by the sides of negative slope of $N_i(f)$. By [HN12, Lem. 2.17], this latter polygon is the lower convex envelope of the set of points $(s, v_i(a_s\phi_i^s))$ of the plane, for $0 \leq s \leq \ell$. For each side of slope (say) λ of $N_i^-(f)$, the residual polynomial of i-th order, $R_{\lambda,i}(f)(y) := R_{\phi_i,v_i,\lambda}(f)(y) \in \mathbb{F}_i[y]$, is computed and factorized into a product of irreducible factors. The type $\mathbf{t}$ branches in principle into as many types as pairs $(\lambda, \psi(y))$, where λ runs on the slopes of $N_i^-(f)$ and $\psi(y)$ runs on the different irreducible factors of $R_{\lambda,i}(f)(y)$. If one of these branches

$$
\mathbf{t}_{\lambda,\psi} := (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots ; (\phi_{i-1}(x), \lambda_{i-1}, \psi_{i-1}(y)); (\phi_i(x), \lambda, \psi(y))),
$$

is f-complete, we store this type in an specific list and we go on with the analysis of other branches. Otherwise, we compute a representative $\phi_{\lambda,\psi}(x)$ of $\mathbf{t}_{\lambda,\psi}$. Let e be the least non-negative denominator of λ and $f = \deg \psi$. Then we proceed in a different way according to $ef = 1$ or $ef > 1$.

If $ef > 1$, then $\deg \phi_{\lambda,\psi} > m_i$, so that $\phi_{i+1} := \phi_{\lambda,\psi}$ may be used to enlarge $\mathbf{t}_{\lambda,\psi}$ into several optimal types of order $i + 1$. We store the invariants

ϕ_i, $m_i = \deg \phi_i$, $V_i = v_i(\phi_i)$, $\lambda_i = \lambda$, h_i, $e_i = e$, ℓ_i, ℓ_i', $\psi_i = \psi$, $f_i = f$, z_i, w_i, Quot_i, $(\log \Phi)_i$, $(\log \pi)_i$, $(\log \gamma)_i$

at the i-th level of $\mathbf{t}_{\lambda,\psi}$, and then we proceed to enlarge the type. The invariant V_i is recursively computed by using [HN12, Prop. 2.7+Thm. 2.11]:

$$
V_i = \begin{cases} 0, & \text{if } i = 1, \\ e_{i-1}f_{i-1}\left(e_{i-1}V_{i-1} + h_{i-1}\right), & \text{if } i > 1. \end{cases}
$$

Let s_i be the abscissa of the right end point of the side of $N_i^-(f)$ of slope λ; the secondary invariants are computed as:

$w_i = v_i(a_{s_i})$,
$\operatorname{Quot}_i = [1, q_{s_i-1}(x), \ldots, q_{s_i-e+1}(x)]$,
$(\log \Phi)_i = (l_0, \ldots, l_{i-1}, 1)$, where $(l_0, \ldots, l_{i-1}) := -(V_i/e_{i-1})(\log \pi)_{i-1}$,
$(\log \pi)_i = (l_0, \ldots, l_{i-1}, 0)$, where $(l_0, \ldots, l_{i-1}) := \ell_{i-1}(\log \Phi)_{i-1} - \ell_{i-1}'(\log \pi)_{i-1}$,
$(\log \gamma)_i = e_i(\log \Phi)_i - h_i(\log \pi)_i$.

For $i = 1$ we take $(\log \Phi)_1 = (0, 1)$ and $(\log \pi)_1 = (1, 0)$. Note that all these secondary invariants depend only on λ and not on ψ. They are computed only once for each side of $N_i^-(f)$ and then stored in the different optimal branches that share the same slope. The type $\mathbf{t}_{\lambda,\psi}$ of order i is then ready for further analysis.

If $ef = 1$ then $\deg \phi_{\lambda,\psi} = m_i$, so that the enlargements of $\mathbf{t}_{\lambda,\psi}$ that would result from building up an $(i+1)$-th level from $\phi_{\lambda,\psi}$ would not be optimal. In this case, we replace $\mathbf{t}_{\lambda,\psi}$ by all types

$$\mathbf{t}'_{\lambda',\psi'} := (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots; (\phi_{i-1}(x), \lambda_{i-1}, \psi_{i-1}(y)); (\phi'_i(x), \lambda', \psi'(y))),$$

obtained by enlarging $\mathbf{t}$ with i-th levels deduced from the consideration of $\phi'_i(x) := \phi_{\lambda,\psi}(x)$ as a new (and better) representative of $\mathbf{t}$, but taking into account only the slopes λ' of $N_{\phi'_i, v_i}(f)$ satisfying $\lambda' < \lambda$; this is called a *refinement step* [GMN11, Sect. 3.2]. If the total number of pairs (λ, ψ) is greater than one, we append to the list Refinements$_i$ of all types $\mathbf{t}'_{\lambda',\psi'}$ the pair $[\phi_i(x), \lambda]$. Some of these new branches $\mathbf{t}'_{\lambda',\psi'}$ of order i may be f-complete, some may lead to optimal enlargements and some may lead to further refinement at the i-th level. Thus, in general, the list Refinements$_i$ of a type $\mathbf{t}$ is an ordered sequence of pairs:

$$\text{Refinements}_i = [[\phi_i^{(1)}, \lambda_i^{(1)}], \cdots, [\phi_i^{(s)}, \lambda_i^{(s)}]],$$

reflecting the fact that along the construction of $\mathbf{t}$, s or more successive refinement steps occurred at the i-th level. All polynomials $\phi_i^{(k)}$ are representatives of Trunc$_{i-1}(\mathbf{t})$, and the slopes $\lambda_i^{(k)}$ are negative integers that grow strictly in absolute size: $|\lambda_i^{(1)}| < \cdots < |\lambda_i^{(s)}|$. We emphasize that we store only the pairs $[\phi_i^{(k)}, \lambda_i^{(k)}]$ corresponding to a refinement step that occurred simultaneously with some branching. Thus, the total number of pairs $[\phi, \lambda]$ that are stored in all lists Refinements$_i$ of all optimal types considered by the algorithm is less than the number of p-adic irreducible factors of $f(x)$.

After a finite number of branching, enlargement and/or refinement steps, all types become f-complete and optimal. If $\mathbf{t}$ is an f-complete and optimal type of order r, then the *Okutsu depth* of $f_{\mathbf{t}}(x)$ is [GMN10, Thm. 4.2]:

$$(2) \qquad R = \begin{cases} r, & \text{if } e_r f_r > 1, \text{ or } r = 0 \\ r - 1, & \text{if } e_r f_r = 1, \text{ and } r > 0. \end{cases}$$

The invariants v_{i+1}, h_i, e_i, f_i at each level $1 \le i \le R$ are canonical (depend only on $f(x)$) [GMN10, Cor. 3.7]. On the other hand, the polynomials $\phi_i(x), \psi_i(y)$ depend on several choices, some of them caused by the lifting of elements of a finite field to rings of characteristic zero. However, the sequence $[\phi_1, \ldots, \phi_R]$ is an *Okutsu frame* of $f_{\mathbf{t}}(x)$ [GMN10, Sec. 2]; in the original terminology of Okutsu, the polynomials $\phi_1, \ldots, \phi_R$ are *primitive divisor polynomials* of $f_{\mathbf{t}}(x)$ [Oku82].

1.4. **Okutsu approximations to the irreducible p-adic factors.** Once an f-complete and optimal type $\mathbf{t}$ of order r is computed, Montes algorithm attaches to it an $(r+1)$-level that carries only the invariants:

$$(3) \qquad \begin{aligned} &\phi_{r+1}, \ m_{r+1}, \ v_{r+1}(\phi_{r+1}), \ \lambda_{r+1} = -h_{r+1}, \ e_{r+1} = 1, \ \psi_{r+1}, \ f_{r+1} = 1, \\ &z_{r+1}, \ (\log \Phi)_{r+1}, \ (\log \pi)_{r+1}, \ (\log \gamma)_{r+1}. \end{aligned}$$

The polynomial $\phi_{r+1}(x)$ is a representative of $\mathbf{t}$. The invariants $\lambda_{r+1}, \psi_{r+1}$ are deduced from the computation of the principal part of the Newton polygon of $(r+1)$-th order of $f(x)$ (which is a single side of length one) and the corresponding residual polynomial $R_{r+1}(f)(y) \in \mathbb{F}_{r+1}[y]$ (which has degree one).

If $\mathfrak{p}$ is the prime ideal corresponding to $\mathbf{t}$, we denote

$$f_\mathfrak{p}(x) := f_\mathbf{t}(x) \in \mathbb{Z}_p[x], \quad \phi_\mathfrak{p}(x) := \phi_{r+1}(x) \in \mathbb{Z}[x], \quad \mathbb{F}_\mathfrak{p} := \mathbb{F}_{r+1},$$
$$n_\mathfrak{p} := m_{r+1} = \deg f_\mathfrak{p} = \deg \phi_\mathfrak{p},$$
$$\mathbf{t}_\mathfrak{p} := (\psi_0(y); (\phi_1(x), \lambda_1, \psi_1(y)); \cdots ; (\phi_r(x), \lambda_r, \psi_r(y)); (\phi_\mathfrak{p}(x), \lambda_{r+1}, \psi_{r+1}(y))),$$

and we say that $\mathfrak{p} = [p; \phi_1, \ldots, \phi_r, \phi_\mathfrak{p}]$ is an *Okutsu-Montes representation* of $\mathfrak{p}$. We shall commonly use *OM representation* as an abridged form.

Note that $\mathbf{t}_\mathfrak{p}$ is still an f-complete type of order $r + 1$, but it may eventually be non-optimal because $m_{r+1} = m_r$, if $e_r f_r = 1$.

The polynomial $\phi_\mathfrak{p}(x)$ is an *Okutsu approximation* to the p-adic irreducible factor $f_\mathfrak{p}(x)$ [GMN10, Sec. 4.1]. Several arithmetic tasks involving prime ideals (tasks (1), (3), (5), (6) and (7) from the list given in the Introduction) require the computation of an Okutsu approximation with a sufficiently large value of the last slope $|\lambda_{r+1}| = h_{r+1}$. This can be achieved by applying the *single-factor lifting* algorithm of [GNP11], which is able to improve the Okutsu approximations to $f_\mathfrak{p}(x)$ with quadratic convergence; that is, doubling the value of h_{r+1} at each iteration. Assuming ordinary arithmetic, this procedure requires $O\left(nn_\mathfrak{p}[(h/e(\mathfrak{p}/p))^2 + \log(\mathrm{disc}(f_\mathfrak{p}))^2]\right)$ operations of integers less than p, where h is the value of h_{r+1} to be attained [GNP11, Lem. 6.5].

2. $\mathfrak{p}$-ADIC VALUATION AND FACTORIZATION

In section 2.1 we compute the $\mathfrak{p}$-adic valuation, $v_\mathfrak{p} \colon K^* \to \mathbb{Z}$, determined by a prime ideal $\mathfrak{p}$, in terms of the data contained in the Okutsu-Montes representation of $\mathfrak{p}$. In section 2.2 we describe a procedure to find the prime ideal decomposition of any fractional ideal of K. From the computational point of view, this procedure is based on three ingredients:

(1) The factorization of integers.
(2) Montes algorithm to find the prime ideal decomposition of a prime number.
(3) The computation of $v_\mathfrak{p}$ for some prime ideals $\mathfrak{p}$.

The routines (2) and (3) run extremely fast in practice (see section 6).

It is well-known how to add, multiply and intersect fractional ideals once their prime ideal factorization is available. We omit the description of the routines that carry out these tasks.

From now on, to any prime ideal $\mathfrak{p}$ of K we attach the data $\mathbf{t}_\mathfrak{p}$, $f_\mathfrak{p}(x)$, $\phi_\mathfrak{p}(x)$, $\mathbb{F}_\mathfrak{p}$, described in section 1.4. Also, we choose a root $\theta_\mathfrak{p} \in \overline{\mathbb{Q}}_p$ of $f_\mathfrak{p}(x)$, we consider the local field $K_\mathfrak{p} = \mathbb{Q}_p(\theta_\mathfrak{p})$, and we denote by $\mathbb{Z}_{K_\mathfrak{p}}$ the ring of integers of $K_\mathfrak{p}$.

2.1. **Computation of the $\mathfrak{p}$-adic valuation.** Let p be a prime number and $v \colon \overline{\mathbb{Q}}_p^* \to \mathbb{Q}$, the canonical p-adic valuation. Let $\mathfrak{p}$ be a prime ideal of K lying above p, corresponding to an f-complete type $\mathbf{t}_\mathfrak{p}$ with an added $(r + 1)$-th level, as indicated in section 1.4. We shall freely use all invariants of $\mathbf{t}_\mathfrak{p}$ described in section 1. By item 2 of Definition 1.1 we know that

$$e(\mathfrak{p}/p) = e_1 \cdots e_r, \qquad f(\mathfrak{p}/p) = f_0 f_1 \cdots f_r.$$

The residue field $\mathbb{Z}_{K_\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{K_\mathfrak{p}}$ can be identified to the finite field

$$\mathbb{F}_\mathfrak{p} := \mathbb{F}_{r+1} = \mathbb{F}_0[z_0, z_1, \ldots, z_r].$$

More precisely, in [HN12, (27)] we construct an explicit isomorphism

$$(4) \qquad \gamma \colon \mathbb{F}_{\mathfrak{p}} \xrightarrow{\sim} \mathbb{Z}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathbb{Z}_{K_{\mathfrak{p}}}, \qquad z_0 \mapsto \overline{\theta_{\mathfrak{p}}},\ z_1 \mapsto \overline{\gamma_1(\theta_{\mathfrak{p}})},\ \ldots,\ z_r \mapsto \overline{\gamma_r(\theta_{\mathfrak{p}})},$$

where we indicate by a bar the canonical reduction map, $\mathbb{Z}_{K_{\mathfrak{p}}} \longrightarrow \mathbb{Z}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathbb{Z}_{K_{\mathfrak{p}}}$. We denote by $\mathrm{lred}_{\mathfrak{p}} \colon \mathbb{Z}_{K_{\mathfrak{p}}} \longrightarrow \mathbb{F}_{\mathfrak{p}}$, the reduction map obtained by composition of the canonical reduction map with the inverse of the isomorphism (4).

$$(5) \qquad\qquad\qquad \mathrm{lred}_{\mathfrak{p}} \colon \mathbb{Z}_{K_{\mathfrak{p}}} \longrightarrow \mathbb{Z}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathbb{Z}_{K_{\mathfrak{p}}} \xrightarrow{\gamma^{-1}} \mathbb{F}_{\mathfrak{p}}.$$

Consider the topological embedding $\iota_{\mathfrak{p}} \colon K \hookrightarrow K_{\mathfrak{p}}$ determined by sending θ to $\theta_{\mathfrak{p}}$. We have: $v_{\mathfrak{p}}(\alpha) = e(\mathfrak{p}/p)v(\iota_{\mathfrak{p}}(\alpha))$, for all $\alpha \in K$. In particular, for any polynomial $g(x) \in \mathbb{Z}[x]$,

$$(6) \qquad\qquad\qquad v_{\mathfrak{p}}(g(\theta)) = e(\mathfrak{p}/p)v(g(\theta_{\mathfrak{p}})).$$

Any $\alpha \in K^*$ can be expressed as $\alpha = (a/b)g(\theta)$, for some coprime positive integers a, b and some primitive polynomial $g(x) \in \mathbb{Z}[x]$. By (6),

$$v_{\mathfrak{p}}(\alpha) = e(\mathfrak{p}/p)(v(g(\theta_{\mathfrak{p}})) + v(a/b)).$$

Thus, it is sufficient to learn to compute $v(g(\theta_{\mathfrak{p}}))$. The condition $v(g(\theta_{\mathfrak{p}})) = 0$ is easy to check [GMN10, Lem. 2.2]:

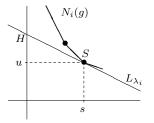$$(7) \qquad\qquad\qquad v(g(\theta_{\mathfrak{p}})) = 0 \iff \psi_0 \nmid R_0(g).$$

If $\psi_0 \mid R_0(g)$, the computation of $v(g(\theta_{\mathfrak{p}}))$ can be based on the following proposition, which is easily deduced from [HN12, Prop. 3.5] and [HN12, Cor. 3.2].

Proposition 2.1. *Let $\mathfrak{p}$, $f_{\mathfrak{p}}(x)$, $\theta_{\mathfrak{p}}$ be as above. Let $\mathbf{t}$ be a type of order R dividing $f_{\mathfrak{p}}(x)$, and let $g(x) \in \mathbb{Z}[x]$ be a nonzero polynomial. For any $1 \leq i \leq R$, take a line L_{λ_i} of slope λ_i far below $N_i(g)$, and let it shift upwards till it touches the polygon for the first time. Let S be the intersection of this line with $N_i(g)$, let (s, u) be the coordinates of the left end point of S, and let $H = u + s|\lambda_i|$ be the ordinate of the point of intersection of L_{λ_i} with the vertical axis. Then,*

(1) *$v(g(\theta_{\mathfrak{p}})) \geq H/e_1 \cdots e_{i-1}$, and equality holds if and only if $\mathrm{Trunc}_i(\mathbf{t}) \nmid g(x)$.*
(2) *If equality holds, then $v(g(\theta_{\mathfrak{p}})) = v(\Phi_i(\theta_{\mathfrak{p}})^s \pi_i(\theta_{\mathfrak{p}})^u)$ and*

$$\mathrm{lred}_{\mathfrak{p}} \left(\frac{g(\theta_{\mathfrak{p}})}{\Phi_i(\theta_{\mathfrak{p}})^s \pi_i(\theta_{\mathfrak{p}})^u} \right) = R_i(g)(z_i) \neq 0.$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Figure 1 shows that the segment S may eventually be a single point. In this case, the residual polynomial of i-th order $R_i(g)(y)$ is a constant [HN12, Def. 2.21], so that $\mathrm{Trunc}_i(\mathbf{t}) \nmid g(x)$ automatically holds.
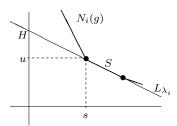

Figure 1

We may compute $v_{\mathfrak{p}}(g(\theta)) = e(\mathfrak{p}/p)v(g(\theta_{\mathfrak{p}}))$ by applying Proposition 2.1 to the type $\mathbf{t}_{\mathfrak{p}}$. If for some $1 \leq i \leq r+1$, the truncated type $\text{Trunc}_i(\mathbf{t}_{\mathfrak{p}})$ does not divide $g(x)$, we compute $v(g(\theta_{\mathfrak{p}}))$ as indicated in item 1 of this proposition. Nevertheless, it may occur that $\text{Trunc}_i(\mathbf{t}_{\mathfrak{p}})$ divides $g(x)$ for all $1 \leq i \leq r+1$ (for instance, if $g(x)$ is a multiple of $\phi_{\mathfrak{p}}(x) = \phi_{r+1}(x)$). In this case, we compute an improvement of the Okutsu approximation $\phi_{\mathfrak{p}}(x)$ by applying the single-factor lifting routine [GNP11]; then, we replace the $(r+1)$-th level of $\mathbf{t}_{\mathfrak{p}}$ by the invariants (3) determined by the new choice of $\phi_{r+1}(x) = \phi_{\mathfrak{p}}(x)$, and we test again if $\mathbf{t}_{\mathfrak{p}} = \text{Trunc}_{r+1}(\mathbf{t}_{\mathfrak{p}})$ divides $g(x)$.

If $\mathbf{t}_{\mathfrak{p}}$ divides $g(x)$, then $\phi_{\mathfrak{p}}(x)$ is simultaneously close to a p-adic irreducible factor of $f(x)$ and to a p-adic irreducible factor of $g(x)$; hence, if $f(x)$ and $g(x)$ do not have a common p-adic irreducible factor, after a finite number of steps the renewed type $\mathbf{t}_{\mathfrak{p}}$ will not divide $g(x)$. On the other hand, if $f(x)$ and $g(x)$ have a common p-adic irreducible factor, they must have a common irreducible factor in $\mathbb{Z}[x]$ too; since $f(x)$ is irreducible, necessarily $f(x)$ divides $g(x)$ and $g(\theta) = 0$.

We may summarize the routine to compute $v_{\mathfrak{p}}(\alpha)$ as follows.

Input: $\alpha \in K^*$ and a prime ideal $\mathfrak{p}$ determined by a type $\mathbf{t}_{\mathfrak{p}}$ of order $r+1$.
Output: $v_{\mathfrak{p}}(\alpha)$.

1. Write $\alpha = \frac{a}{b}g(\theta)$, with a, b coprime integers and $g(x) \in \mathbb{Z}[x]$ primitive.
2. Compute $\nu = e(\mathfrak{p}/p)v(a/b)$.
3. if $\psi_0 \nmid R_0(g)$ then return $v_{\mathfrak{p}}(\alpha) = \nu$.
4. for $i = 1$ to $r+1$ do
    compute $N_i^-(g)$, $R_i(g)$, and the ordinate H of Proposition 2.1.
    if $\psi_i \nmid R_i(g)$ then return $v_{\mathfrak{p}}(\alpha) = e(\mathfrak{p}/p)(H/e_1 \cdots e_{i-1}) + \nu$.
   end for.
5. while $\psi_{r+1} \mid R_{r+1}(g)$ do
    improve $\phi_{\mathfrak{p}}$ and compute the new values λ_{r+1}, ψ_{r+1}.
    compute $N_{r+1}^-(g)$, $R_{r+1}(g)$, and the ordinate H of Proposition 2.1.
   end while.
6. return $v_{\mathfrak{p}}(\alpha) = H + \nu$.

2.2. **Factorization of fractional ideals.** For any $\alpha \in K^*$, the factorization of the principal ideal generated by α is

$$\alpha \mathbb{Z}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}.$$

Let $\alpha = (a/b)g(\theta)$, for some positive coprime integers a, b and some primitive polynomial $g(x) \in \mathbb{Z}[x]$. Then, $v_{\mathfrak{p}}(\alpha) = 0$ for all prime ideals $\mathfrak{p}$ whose underlying prime number p does not divide the product $ab \, \text{N}_{K/\mathbb{Q}}(g(\theta)) = ab \, \text{Resultant}(f, g)$.

Also, if $\mathfrak{p}$ is a prime ideal of K and $\mathfrak{a}$, $\mathfrak{b}$ are fractional ideals, we have

$$v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}.$$

Thus, the $\mathfrak{p}$-adic valuation of the fractional ideal $\mathfrak{a}$ generated by $\alpha_1, \ldots, \alpha_m \in K^*$ is: $v_{\mathfrak{p}}(\mathfrak{a}) = \min_{1 \leq i \leq m}\{v_{\mathfrak{p}}(\alpha_i)\}$.

After these considerations, it is straightforward to deduce a factorization routine of fractional ideals from the routines computing prime ideal decompositions of prime numbers and $\mathfrak{p}$-valuations of elements of K^* with respect to prime ideals $\mathfrak{p}$.

Input: a family $\alpha_1, \ldots, \alpha_m \in K^*$ generating a fractional ideal $\mathfrak{a}$.
Output: the prime ideal decomposition $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$.

1. For each $1 \leq i \leq m$, write $\alpha_i = (a_i/b_i)g_i(\theta)$, with a_i, b_i coprime integers and $g_i(x) \in \mathbb{Z}[x]$ primitive; then compute $N_i = \mathrm{N}_{K/\mathbb{Q}}(g_i(\theta))$.
2. Compute $N = \gcd(a_1 N_1, \ldots, a_m N_m)$ and $M = \mathrm{lcm}(b_1, \ldots, b_m)$.
3. Factorize N and M and store all their prime factors in a list $\mathcal{P}$.
4. For each $p \in \mathcal{P}$ apply Montes algorithm to obtain the prime ideal decomposition of p, and for each $\mathfrak{p}|p$, take $a_\mathfrak{p} = \min_{1 \leq i \leq m}\{v_\mathfrak{p}(\alpha_i)\}$.
5. Return the list of pairs $[\mathfrak{p}, a_\mathfrak{p}]$ for all $\mathfrak{p}$ with $a_\mathfrak{p} \neq 0$.

The bottleneck of this routine is step 3. We get a fast factorization routine in the number field K, as long as the integers N, M attached to the ideal $\mathfrak{a}$ may be easily factorized.

3. Computation of generators

In [GMN11, Sec. 4] we gave an algorithm to compute generators of the prime ideals as certain rational functions of the ϕ-polynomials of the corresponding types. Some inversions in K, one for each prime ideal, were needed. These inversions dominated the complexity of the algorithm, and they were a bottleneck that prevented the computation of generators for number fields of large degree.

In sections 3.1 and 3.2 we construct a two-elements representation of prime ideals, which does not need any inversion in K. This construction works extremely fast in practice even for number fields of large degree (see section 6). In section 3.3 we easily derive two-elements representations of fractional ideals.

For any prime ideal $\mathfrak{p}$ of K we keep the notation for $\mathbf{t}_\mathfrak{p}$, $f_\mathfrak{p}(x)$, $\phi_\mathfrak{p}(x)$, $\mathbb{F}_\mathfrak{p}$, $\theta_\mathfrak{p}$, $K_\mathfrak{p}$, $\mathbb{Z}_{K_\mathfrak{p}}$, as introduced in section 1.4.

3.1. Local generators of the prime ideals.

Definition 3.1. *A local generator of a prime ideal $\mathfrak{p}$ of K is an integral element $\pi \in \mathbb{Z}_K$ such that $v_\mathfrak{p}(\pi) = 1$.*

Let p be a prime number, and let $\mathfrak{p} = [p; \phi_1, \ldots, \phi_r, \phi_\mathfrak{p}]$ be an OM representation of a prime ideal factor of $p\mathbb{Z}_K$, corresponding to an f-complete type $\mathbf{t}_\mathfrak{p}$ with an added $(r+1)$-th level, as indicated in section 1.4. In this section we show how to compute a local generator of $\mathfrak{p}$ from the secondary invariants w_i, Quot_i, of $\mathbf{t}_\mathfrak{p}$, for $1 \leq i \leq r$, computed along the flow of Montes algorithm as indicated in section 1.3.

For each level $1 \leq i \leq r$, let us denote:

$$\mathrm{Quot}_i = [Q_{i,0}(x), \ldots, Q_{i,e_i-1}(x)].$$

Recall that $Q_{i,0}(x) = 1$, and for $0 < j < e_i$, the polynomial $Q_{i,j}(x) = q_{s_i-j}(x) \in \mathbb{Z}[x]$ is the $(s_i - j)$-th quotient of the ϕ_i-adic development of $f(x)$ (cf. (1)), where s_i is the abscissa of the right end point of the side of slope λ_i of $N_i^-(f)$. Also, let us define
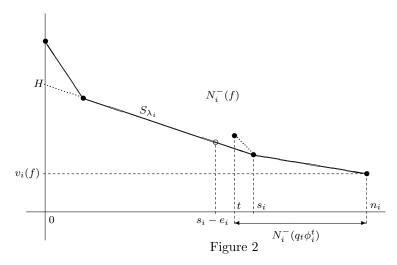
$$H_{i,0} = 0, \qquad H_{i,j} = \frac{w_i + j(|\lambda_i| + V_i)}{e_1 \cdots e_{i-1}}, \quad \forall 0 < j < e_i.$$

Proposition 3.2. *For each level $1 \leq i \leq r$ and subindex $0 \leq j < e_i$:*

(1) $v_\mathfrak{q}(Q_{i,j}(\theta)) \geq e(\mathfrak{q}/p)H_{i,j}$, *for all prime ideals $\mathfrak{q} \mid p$.*
(2) $v_\mathfrak{p}(Q_{i,j}(\theta)) = e(\mathfrak{p}/p)H_{i,j}$.

Proof. Item 1 being proved in [GMN09, Thm. 4.3], let us prove item 2. Fix a level $1 \leq i \leq r$ and a subindex $0 \leq j < e_i$. Let $n_i = \mathrm{ord}_{\psi_{i-1}} R_{i-1}(f)$, and let $f(x) = \sum_{s \geq 0} a_s \phi_i^s$ be the ϕ_i-adic development of $f(x)$. The Newton polygon of i-th

order of $f(x)$, $N_i(f)$, is the lower convex envelope of the cloud of points $(s, v_i(a_s\phi_i^s))$, for all $s \geq 0$. The principal part $N_i^-(f)$ is equal to $N_i(f) \cap ([0, n_i] \times \mathbb{R})$; the typical shape of this polygon is illustrated in Figure 2. Let S_{λ_i} be the side of slope λ_i of this polygon, and s_i the abscissa of the right end point of S_{λ_i}.

Figure 2

For any $0 \leq t \leq n_i$, let $q_t(x)$ be the t-th quotient of the ϕ_i-adic development (see (1)). We have $f(x) = q_t(x)\phi_i(x)^t + r_t(x)$, with

$$r_t(x) = \sum_{0 \leq s < t} a_s(x)\phi_i(x)^s, \qquad q_t(x)\phi_i(x)^t = \sum_{t \leq s} a_s(x)\phi_i(x)^s.$$

Hence, if t_0 is the smallest abscissa of a vertex of $N_i(f)$, such that $t_0 \geq t$, we have

$$N_i(q_t\phi_i^t) \cap ([t_0, \infty) \times \mathbb{R}) = N_i(f) \cap ([t_0, \infty) \times \mathbb{R}).$$

Recall that $Q_{i,j}(x) = q_t(x)$, for $t = s_i - j$; for this value of t we have $t_0 = s_i$ (see Figure 2). On the other hand, all points in the cloud $(s, v_i(a_s\phi_i^s))$, for $s_i - e_i < s < s_i$ lie strictly above S_{λ_i}, because the point on S_{λ_i} with integer coordinates and closest to the right end point has abscissa $s_i - e_i$. Hence, the line of slope λ_i that first touches $N_i(q_{s_i-j}\phi_i^{s_i-j})$ from below is the line containing S_{λ_i}. This line intersects the vertical axis at the point $(0, H)$, with (see Figure 2):

$$H = v_i\left(a_{s_i}\phi_i^{s_i}\right) + s_i|\lambda_i| = w_i + s_i(V_i + |\lambda_i|).$$

On the other hand, this line touches $N_i(q_{s_i-j}\phi_i^{s_i-j})$ only at the point $(s_i, v_i(a_{s_i}\phi_i^{s_i}))$, so that $R_i(q_{s_i-j}\phi_i^{s_i-j})(y)$ is a constant and $\mathrm{Trunc}_i(\mathbf{t_p})$ does not divide $q_{s_i-j}\phi_i^{s_i-j}$. Therefore, Proposition 2.1 shows that

$$v(q_{s_i-j}(\theta_{\mathfrak{p}})\phi_i(\theta_{\mathfrak{p}})^{s_i-j}) = \frac{w_i + s_i(V_i + |\lambda_i|)}{e_1 \cdots e_{i-1}}.$$

By the Theorem of the polygon [HN12, Thm. 3.1],

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

so that

$$v(q_{s_i-j}(\theta_{\mathfrak{p}})) = \frac{w_i + j(V_i + |\lambda_i|)}{e_1 \cdots e_{i-1}} = H_{i,j}.$$

By (6), $v_{\mathfrak{p}}(q_{s_i-j}(\theta)) = e(\mathfrak{p}/p)H_{i,j}$.   □

If $e(\mathfrak{p}/p) = 1$, then $\pi_\mathfrak{p} := p$ is a local generator of $\mathfrak{p}$. If $e(\mathfrak{p}/p) > 1$, we can always find a local generator of $\mathfrak{p}$ by computing a suitable product of quotients in the lists Quot_i, divided by a suitable power of p.

Corollary 3.3.

(1) *Let $j_1, \ldots, j_r$ be subindices satisfying, $0 \le j_i < e_i$, for all $1 \le i \le r$. Then, the following element belongs to $\mathbb{Z}_K$:*

$$\pi_{j_1,\ldots,j_r} := Q_{1,j_1}(\theta) \cdots Q_{r,j_r}(\theta)/p^{\lfloor H_{1,j_1} + \cdots + H_{r,j_r} \rfloor}.$$

(2) *If $e(\mathfrak{p}/p) > 1$, there is a unique family $j_1, \ldots, j_r$ as above, for which $v_\mathfrak{p}(\pi_{j_1,\ldots,j_r}) = 1$. This family may be recursively computed as follows:*

$$j_r \equiv h_r^{-1} \pmod{e_r},$$
$$\mathrm{res}_r := (j_r h_r - 1)/e_r,$$
$$j_{r-1} \equiv -h_{r-1}^{-1}(w_r + j_r V_r + \mathrm{res}_r) \pmod{e_{r-1}},$$
$$\mathrm{res}_{r-1} := (j_{r-1} h_{r-1} + w_r + j_r V_r + \mathrm{res}_r)/e_{r-1},$$
$$\cdots \qquad \cdots$$
$$j_1 \equiv -h_1^{-1}(w_2 + j_2 V_2 + \mathrm{res}_2) \pmod{e_1}.$$

Proof. Item 1 is an immediate consequence of item 1 of Proposition 3.2.

Also, by Proposition 3.2,

$$v_\mathfrak{p}(\pi_{j_1,\ldots,j_r}) = e(\mathfrak{p}/p)\left(H_{1,j_1} + \cdots + H_{r,j_r} - \lfloor H_{1,j_1} + \cdots + H_{r,j_r} \rfloor\right).$$

Thus, item 2 states that there is a unique family $j_1, \ldots, j_r$ such that

$$H_{1,j_1} + \cdots + H_{r,j_r} \equiv \frac{1}{e(\mathfrak{p}/p)} \pmod{\mathbb{Z}}.$$

Since $e(\mathfrak{p}/p) = e_1 \cdots e_r$ and $|\lambda_i| = h_i/e_i$, this is equivalent to:

$$w_1 + j_1 V_1 + \frac{j_1 h_1 + w_2 + j_2 V_2}{e_1} + \cdots$$
$$\cdots + \frac{j_{r-1} h_{r-1} + w_r + j_r V_r}{e_1 \cdots e_{r-1}} + \frac{j_r h_r}{e_1 \cdots e_r} \equiv \frac{1}{e_1 \cdots e_r} \pmod{\mathbb{Z}}.$$

Clearly this congruence has a unique solution $j_1, \ldots, j_r$ satisfying $0 \le j_i < e_i$, for all $1 \le i \le r$, and this solution may be recursively obtained by the procedure described in item 2. $\square$

The identity $e_1 \cdots e_r = e(\mathfrak{p}/p)$ is the only property of $\mathbf{t}_\mathfrak{p}$ that we used in Corollary 3.3. Thus, we don't need to use all levels of $\mathbf{t}_\mathfrak{p}$ to compute a local generator of $\mathfrak{p}$; in practice we may replace r by the minimum level r_0 such that $e_1 \cdots e_{r_0} = e(\mathfrak{p}/p)$.

3.2. Generators of the prime ideals. Let p be a prime number, and $\mathcal{P}$ the set of prime ideals of K lying over p. Once we have local generators $\pi_\mathfrak{p} \in \mathfrak{p}$ of all $\mathfrak{p} \in \mathcal{P}$, in order to find generators we need only to compute a family of integral elements, $\{b_\mathfrak{p} \in \mathbb{Z}_K\}_{\mathfrak{p} \in \mathcal{P}}$, satisfying:

(9) $v_\mathfrak{p}(b_\mathfrak{p}) = 0, \ \forall \mathfrak{p} \in \mathcal{P}, \qquad v_\mathfrak{q}(b_\mathfrak{p}) > 1, \ \forall \mathfrak{q}, \mathfrak{p} \in \mathcal{P}, \ \mathfrak{q} \ne \mathfrak{p}.$

Then, for each $\mathfrak{p} \in \mathcal{P}$, the integral element:

$$\alpha_\mathfrak{p} := b_\mathfrak{p} \pi_\mathfrak{p} + \sum_{\mathfrak{q} \in \mathcal{P}, \mathfrak{q} \ne \mathfrak{p}} b_\mathfrak{q} \in \mathbb{Z}_K$$

clearly satisfies: $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 1$, $v_{\mathfrak{q}}(\alpha_{\mathfrak{p}}) = 0$, for all $\mathfrak{q} \neq \mathfrak{p}$. Therefore, $\mathfrak{p}$ is the ideal generated by p and $\alpha_{\mathfrak{p}}$. The rest of this section is devoted to the construction of these multipliers $\{b_{\mathfrak{p}}\}$.

Let $(\mathbf{t}_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}}$ be the parameterization of the set $\mathcal{P}$ by a family of f-complete types obtained by an application of Montes algorithm. As usual, we suppose that each $\mathbf{t}_{\mathfrak{p}}$ has been conveniently enlarged with an $(r_{\mathfrak{p}} + 1)$-th level, as indicated in section 1.4. From now on we provide the invariants of $\mathbf{t}_{\mathfrak{p}}$ with a subscript $\mathfrak{p}$ to distinguish the prime ideal they belong to: $r_{\mathfrak{p}}, \phi_{i,\mathfrak{p}}, m_{i,\mathfrak{p}}, \lambda_{i,\mathfrak{p}}$, etc.

The integral elements $b_{\mathfrak{p}}$ will be constructed as suitable products of ϕ-polynomials divided by suitable powers of p. The crucial ingredient is Proposition 3.8, that computes $v_{\mathfrak{p}}(\phi_{i,\mathfrak{q}}(\theta))$ for all $\mathfrak{p} \neq \mathfrak{q}$ in $\mathcal{P}$, and all $1 \leq i \leq r_{\mathfrak{q}} + 1$.

Definition 3.4. *For any pair* $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$, $\mathfrak{p} \neq \mathfrak{q}$, *we define the* index of coincidence *between the types* $\mathbf{t}_{\mathfrak{p}}$ *and* $\mathbf{t}_{\mathfrak{q}}$ *as:*

$$i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}}) = \begin{cases} 0, & \text{if } \psi_{0,\mathfrak{p}} \neq \psi_{0,\mathfrak{q}}, \\ \min \{j \in \mathbb{Z}_{>0} \mid (\phi_{j,\mathfrak{p}}, \lambda_{j,\mathfrak{p}}, \psi_{j,\mathfrak{p}}) \neq (\phi_{j,\mathfrak{q}}, \lambda_{j,\mathfrak{q}}, \psi_{j,\mathfrak{q}})\}, & \text{if } \psi_{0,\mathfrak{p}} = \psi_{0,\mathfrak{q}}. \end{cases}$$

Alternatively, $i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})$ *is the least subindex* j *for which* $\mathrm{Trunc}_j(\mathbf{t}_{\mathfrak{p}}) \neq \mathrm{Trunc}_j(\mathbf{t}_{\mathfrak{q}})$.

Remark 3.5. *By definition,*

$$\phi_{i,\mathfrak{p}} = \phi_{i,\mathfrak{q}}, \quad \lambda_{i,\mathfrak{p}} = \lambda_{i,\mathfrak{q}}, \quad \psi_{i,\mathfrak{p}} = \psi_{i,\mathfrak{q}}, \quad \forall i < i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}}).$$

Hence, by the definition of the p-adic valuations $v_{i,\mathfrak{p}}$, $v_{i,\mathfrak{q}}$, *and by* [HN12, Thm. 2.11]*, we get:*

$$v_{i,\mathfrak{p}} = v_{i,\mathfrak{q}}, \quad m_{i,\mathfrak{p}} = m_{i,\mathfrak{q}}, \quad V_{i,\mathfrak{p}} = V_{i,\mathfrak{q}}, \quad \forall i \leq i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}}).$$

Lemma 3.6. *If* $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$, *and* $\mathfrak{p} \neq \mathfrak{q}$, *then* $i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}}) \leq \min\{r_{\mathfrak{p}}, r_{\mathfrak{q}}\}$.

Proof. Suppose $r_{\mathfrak{p}} \leq r_{\mathfrak{q}}$ and $i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}}) = r_{\mathfrak{p}} + 1$. Then, $\mathrm{Trunc}_{r_{\mathfrak{p}}}(\mathbf{t}_{\mathfrak{p}}) = \mathrm{Trunc}_{r_{\mathfrak{p}}}(\mathbf{t}_{\mathfrak{q}})$. Since the type $\mathrm{Trunc}_{r_{\mathfrak{p}}}(\mathbf{t}_{\mathfrak{p}})$ is f-complete, it singles out a unique p-adic irreducible factor of $f(x)$ (item 2 of Definition 1.1). Hence, $\mathrm{Trunc}_{r_{\mathfrak{p}}}(\mathbf{t}_{\mathfrak{q}})$ is also f-complete and it singles out the same p-adic irreducible factor of $f(x)$. This implies that $\mathfrak{p} = \mathfrak{q}$. $\square$

By (6) and (8), for all $1 \leq i \leq r_{\mathfrak{p}} + 1$ we have

$$(10) \qquad v_{\mathfrak{p}}(\phi_{i,\mathfrak{p}}(\theta)) = e(\mathfrak{p}/p) \frac{V_{i,\mathfrak{p}} + |\lambda_{i,\mathfrak{p}}|}{e_{1,\mathfrak{p}} \cdots e_{i-1,\mathfrak{p}}}.$$

In order to compute the values of $v_{\mathfrak{p}}(\phi_{i,\mathfrak{q}}(\theta))$, for $\mathfrak{p} \neq \mathfrak{q}$, we need still another definition.

Definition 3.7. *Let* $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$, $\mathfrak{q} \neq \mathfrak{p}$, *and* $j = i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})$. *Let* $s_{\mathfrak{p}} = \# \mathrm{Refinements}_{j,\mathfrak{p}}$, *and consider the list* $\mathrm{Ref}_{\mathfrak{p}}$ *obtained by extending the list* $\mathrm{Refinements}_{j,\mathfrak{p}}$ *by adding the pair* $[\phi_{j,\mathfrak{p}}, \lambda_{j,\mathfrak{p}}]$ *at the last position:*

$$\mathrm{Ref}_{\mathfrak{p}} = \left[\left[\phi_{j,\mathfrak{p}}^{(1)}, \lambda_{j,\mathfrak{p}}^{(1)}\right], \cdots, \left[\phi_{j,\mathfrak{p}}^{(s_{\mathfrak{p}})}, \lambda_{j,\mathfrak{p}}^{(s_{\mathfrak{p}})}\right], \left[\phi_{j,\mathfrak{p}}^{(s_{\mathfrak{p}}+1)}, \lambda_{j,\mathfrak{p}}^{(s_{\mathfrak{p}}+1)}\right] := [\phi_{j,\mathfrak{p}}, \lambda_{j,\mathfrak{p}}] \right].$$

Let $\mathrm{Ref}_{\mathfrak{q}}$ *be the analogous list for the prime ideal* $\mathfrak{q}$.

We define the greatest common ϕ-polynomial *of the pair* $(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})$ *to be the more advanced common ϕ-polynomial in the two lists* $\mathrm{Ref}_{\mathfrak{p}}$, $\mathrm{Ref}_{\mathfrak{q}}$. *We denote it by:*

$$\phi(\mathfrak{p}, \mathfrak{q}) := \phi_{j,\mathfrak{p}}^{(k)} = \phi_{j,\mathfrak{q}}^{(k)},$$

for the maximum index k such that $\phi_{j,\mathfrak{p}}^{(k)} = \phi_{j,\mathfrak{q}}^{(k)}$.

We define the hidden slopes *of the pair* $(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})$ *to be:* $\lambda_{\mathfrak{p}}^{\mathfrak{q}} := \lambda_{j,\mathfrak{p}}^{(k)}$, $\lambda_{\mathfrak{q}}^{\mathfrak{p}} := \lambda_{j,\mathfrak{q}}^{(k)}$.

Remarks.

(1) By the concrete way the processes of branching, enlarging and/or refining were defined, this polynomial $\phi(\mathfrak{p}, \mathfrak{q})$ always exists. In other words, the lists $\mathrm{Ref}_\mathfrak{p}$, $\mathrm{Ref}_\mathfrak{q}$ have always $\phi_{j,\mathfrak{p}}^{(1)} = \phi_{j,\mathfrak{q}}^{(1)}$. In fact, since $\mathrm{Trunc}_{j-1}(\mathbf{t}_\mathfrak{p}) = \mathrm{Trunc}_{j-1}(\mathbf{t}_\mathfrak{q})$, this type of order $j-1$ had some original representative (say) ϕ_j. By considering $N_{\phi_j, v_j}^-(f)$ and the irreducible factors of all residual polynomials of all sides, we had different branches (λ, ψ) to analyze; if there was only one branch, the algorithm necessarily performed a refinement step, because otherwise we would have $i(\mathbf{t}_\mathfrak{p}, \mathbf{t}_\mathfrak{q}) > j$. After eventually a finite number of these unibranch refinement steps (that were not stored in the list $\mathrm{Refinements}_j$), we considered some representative, let us call it ϕ_j again, leading to several branches. One of these branches led later to the type $\mathbf{t}_\mathfrak{p}$ and one of them (maybe still the same) to the type $\mathbf{t}_\mathfrak{q}$. If the $\mathfrak{p}$-branch was refined, the list $\mathrm{Refinements}_{j,\mathfrak{p}}$ had $\phi_{j,\mathfrak{p}}^{(1)} = \phi_j$ as its initial ϕ-polynomial; if the $\mathfrak{p}$-branch was f-complete or had to be enlarged, then the list $\mathrm{Refinements}_{j,\mathfrak{p}}$ remained empty and we had $\phi_{j,\mathfrak{p}} = \phi_j$. In any case, ϕ_j is the first ϕ-polynomial of the list $\mathrm{Ref}_\mathfrak{p}$. And the same argument works for the list $\mathrm{Ref}_\mathfrak{q}$.

(2) All $\phi_{j,\mathfrak{p}}^{(\ell)}$, $\phi_{j,\mathfrak{q}}^{(\ell)}$ are representatives of $\mathbf{t}_{j-1} := \mathrm{Trunc}_{j-1}(\mathbf{t}_\mathfrak{p}) = \mathrm{Trunc}_{j-1}(\mathbf{t}_\mathfrak{q})$; in particular, all these polynomials have degree m_j. With the obvious meaning for $\psi_{j,\mathfrak{p}}^{(\ell)}$, we have necessarily:

$$\left[\phi_{j,\mathfrak{p}}^{(k)}, \lambda_{j,\mathfrak{p}}^{(k)}, \psi_{j,\mathfrak{p}}^{(k)}\right] \neq \left[\phi_{j,\mathfrak{q}}^{(k)}, \lambda_{j,\mathfrak{q}}^{(k)}, \psi_{j,\mathfrak{q}}^{(k)}\right], \quad \left[\phi_{j,\mathfrak{p}}^{(\ell)}, \lambda_{j,\mathfrak{p}}^{(\ell)}, \psi_{j,\mathfrak{p}}^{(\ell)}\right] = \left[\phi_{j,\mathfrak{q}}^{(\ell)}, \lambda_{j,\mathfrak{q}}^{(\ell)}, \psi_{j,\mathfrak{q}}^{(\ell)}\right],$$

for all $1 \leq \ell < k$. Thus, $\phi(\mathfrak{p}, \mathfrak{q})$ is the first representative of $\mathbf{t}_{j-1}$ for which the branches of $\mathbf{t}_\mathfrak{p}$ and $\mathbf{t}_\mathfrak{q}$ are different.

(3) Caution: we may have $\mathrm{Ref}_\mathfrak{p} = \mathrm{Ref}_\mathfrak{q}$. In this case $\phi(\mathfrak{p}, \mathfrak{q}) = \phi_{j,\mathfrak{p}} = \phi_{j,\mathfrak{q}}$ and $\lambda_\mathfrak{p}^\mathfrak{q} = \lambda_{j,\mathfrak{p}} = \lambda_{j,\mathfrak{q}} = \lambda_\mathfrak{q}^\mathfrak{p}$. The branches of $\mathbf{t}_\mathfrak{p}$ and $\mathbf{t}_\mathfrak{q}$ are distinguished by $\psi_{j,\mathfrak{p}} \neq \psi_{j,\mathfrak{q}}$.

Proposition 3.8. *Let $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$, $\mathfrak{p} \neq \mathfrak{q}$, and $j = i(\mathbf{t}_\mathfrak{p}, \mathbf{t}_\mathfrak{q})$. Let $\phi(\mathfrak{p}, \mathfrak{q})$ be the greatest common ϕ-polynomial of the pair $(\mathbf{t}_\mathfrak{p}, \mathbf{t}_\mathfrak{q})$ and $\lambda_\mathfrak{p}^\mathfrak{q}$, $\lambda_\mathfrak{q}^\mathfrak{p}$ the hidden slopes. Then, for any $1 \leq i \leq r_\mathfrak{q} + 1$,*

$$\frac{v_\mathfrak{p}(\phi_{i,\mathfrak{q}}(\theta))}{e(\mathfrak{p}/p)} = \begin{cases} 0, & \text{if } j = 0, \\[2mm] \dfrac{V_i + |\lambda_i|}{e_1 \cdots e_{i-1}}, & \text{if } i < j, \\[2mm] \dfrac{V_j + |\lambda_\mathfrak{p}^\mathfrak{q}|}{e_1 \cdots e_{j-1}}, & \text{if } i = j \text{ and } \phi_{j,\mathfrak{q}} = \phi(\mathfrak{p}, \mathfrak{q}), \\[2mm] \dfrac{V_j + \min\{|\lambda_\mathfrak{p}^\mathfrak{q}|, |\lambda_\mathfrak{q}^\mathfrak{p}|\}}{e_1 \cdots e_{j-1}}, & \text{if } i = j \text{ and } \phi_{j,\mathfrak{q}} \neq \phi(\mathfrak{p}, \mathfrak{q}), \\[2mm] \dfrac{m_{i,\mathfrak{q}}}{m_j} \cdot \dfrac{V_j + \min\{|\lambda_\mathfrak{p}^\mathfrak{q}|, |\lambda_\mathfrak{q}^\mathfrak{p}|\}}{e_1 \cdots e_{j-1}}, & \text{if } i > j > 0. \end{cases}$$

In these formulas we omit the subscripts $\mathfrak{p}$, $\mathfrak{q}$ when the invariants of the two types coincide (cf. Remark 3.5).

Proof. The case $j = 0$ was seen in (7). The cases $i < j$ and $i = j$, $\phi_{j,\mathfrak{q}} = \phi(\mathfrak{p}, \mathfrak{q})$, are a consequence of (10).

Suppose $i > j > 0$ and $\phi_{j,\mathfrak{p}} = \phi_{j,\mathfrak{q}}$; we have then, $\phi(\mathfrak{p},\mathfrak{q}) = \phi_{j,\mathfrak{p}} = \phi_{j,\mathfrak{q}}$ and $\lambda_{\mathfrak{p}}^{\mathfrak{q}} = \lambda_{j,\mathfrak{p}}$, $\lambda_{\mathfrak{q}}^{\mathfrak{p}} = \lambda_{j,\mathfrak{q}}$. We compute $v_{\mathfrak{p}}(\phi_{i,\mathfrak{q}}(\theta))$ by applying Proposition 2.1 to the polynomial $g(x) = \phi_{i,\mathfrak{q}}(x)$ and the type $\mathbf{t}_{\mathfrak{p}}$. Since $v_{j,\mathfrak{p}} = v_{j,\mathfrak{q}}$ and $\phi_{j,\mathfrak{p}} = \phi_{j,\mathfrak{q}}$, we have $N_{j,\mathfrak{p}}(\phi_{i,\mathfrak{q}}) = N_{j,\mathfrak{q}}(\phi_{i,\mathfrak{q}})$. On the other hand, we saw in the proof of Lemma 1.2 that $N_{j,\mathfrak{q}}(\phi_{i,\mathfrak{q}})$ is one-sided of slope $\lambda_{j,\mathfrak{q}}$. Figure 3 shows the three possibilities for the line $L_{\lambda_{j,\mathfrak{p}}}$ of slope $\lambda_{j,\mathfrak{p}}$ that first touches $N_{j,\mathfrak{p}}(\phi_{i,\mathfrak{q}})$ from below.
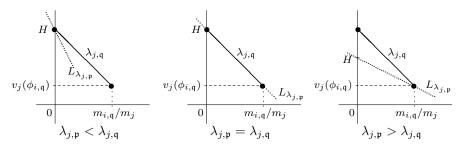

Figure 3

A glance at Figure 3 shows that

$$H = v_j(\phi_{i,\mathfrak{q}}) + \frac{m_{i,\mathfrak{q}}}{m_j}\,\min\{|\lambda_{j,\mathfrak{p}}|,|\lambda_{j,\mathfrak{q}}|\} = \frac{m_{i,\mathfrak{q}}}{m_j}\,(V_j + \min\{|\lambda_{j,\mathfrak{p}}|,|\lambda_{j,\mathfrak{q}}|\}),$$

the last equality by Lemma 1.2. Now, if $\lambda_{j,\mathfrak{p}} \neq \lambda_{j,\mathfrak{q}}$, the line $L_{\lambda_{j,\mathfrak{p}}}$ touches the polygon only at one point, and the residual polynomial $R_{j,\mathfrak{p}}(\phi_{i,\mathfrak{q}})(y)$ is a constant. If $\lambda_{j,\mathfrak{p}} = \lambda_{j,\mathfrak{q}}$, then $L_{\lambda_{j,\mathfrak{p}}}$ contains $N_{j,\mathfrak{p}}(\phi_{i,\mathfrak{q}})$ and $R_{j,\mathfrak{p}}(\phi_{i,\mathfrak{q}}) = R_{j,\mathfrak{q}}(\phi_{i,\mathfrak{q}})$ is a power of $\psi_{j,\mathfrak{q}}$, up to a multiplicative constant. In this case, necessarily $\psi_{j,\mathfrak{q}} \neq \psi_{j,\mathfrak{p}}$, by the definition of $j = i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})$. Therefore, $\mathrm{Trunc}_j(\mathbf{t}_{\mathfrak{p}})$ never divides $\phi_{i,\mathfrak{q}}$, and Proposition 2.1 shows that $v(\phi_{i,\mathfrak{q}}(\theta_{\mathfrak{p}})) = H/(e_1 \cdots e_{j-1})$. By (6), we get the desired expression for $v_{\mathfrak{p}}(\phi_{i,\mathfrak{q}}(\theta))$.

Suppose now $i > j > 0$, $\phi_{j,\mathfrak{p}} \neq \phi_{j,\mathfrak{q}}$, or $i = j$, $\phi_{j,\mathfrak{q}} \neq \phi(\mathfrak{p},\mathfrak{q})$. Consider a new type $\tilde{\mathbf{t}}_{\mathfrak{p}}$, constructed as follows: if $\phi_{j,\mathfrak{p}} = \phi(\mathfrak{p},\mathfrak{q})$, we take $\tilde{\mathbf{t}}_{\mathfrak{p}} = \mathbf{t}_{\mathfrak{p}}$, and if $\phi_{j,\mathfrak{p}} \neq \phi(\mathfrak{p},\mathfrak{q})$, we add an extra level at the j-th position and shift the rest of the levels (with a slight modification of the ψ-polynomials), leading to a type of order $r_{\mathfrak{p}} + 2$:

$$\tilde{\mathbf{t}}_{\mathfrak{p}} = (\psi_0; \cdots ; (\phi_{j-1}, \lambda_{j-1}, \psi_{j-1}); (\phi(\mathfrak{p},\mathfrak{q}), \lambda_{\mathfrak{p}}^{\mathfrak{q}}, \psi); (\phi_{j,\mathfrak{p}}, \lambda_{j,\mathfrak{p}} - \lambda_{\mathfrak{p}}^{\mathfrak{q}}, \psi_{j,\mathfrak{p}}');$$
$$(\phi_{j+1,\mathfrak{p}}, \lambda_{j+1,\mathfrak{p}}, \psi_{j+1,\mathfrak{p}}'); \cdots ; (\phi_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \lambda_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \psi_{r_{\mathfrak{p}}+1,\mathfrak{p}}')).$$

The polynomial $\psi(y) \in \mathbb{F}_j[y]$ is the unique monic irreducible factor of the residual polynomial of j-th order $R_{\phi(\mathfrak{p},\mathfrak{q}),v_j,\lambda_{\mathfrak{p}}^{\mathfrak{q}}}(f_{\mathfrak{p}})$; it has degree one because it belongs to a refined level. For $j \leq k \leq r_{\mathfrak{p}} + 1$, we take $\psi_{k,\mathfrak{p}}'(y) := c_k^{f_{k,\mathfrak{p}}} \psi_{k,\mathfrak{p}}(c_k^{-1} y)$, for certain constants $c_k \in \mathbb{F}_k^*$. By [GMN11, Props. 3.4+3.5], for an adequate choice of these constants c_k, $\tilde{\mathbf{t}}_{\mathfrak{p}}$ is a type dividing $f_{\mathfrak{p}}(x)$, which is still f-complete. This type is not optimal because $\deg \phi(\mathfrak{p},\mathfrak{q}) = \deg \phi_{j,\mathfrak{p}}$, but optimality is not necessary to apply Proposition 2.1.

We consider an analogous construction for $\tilde{\mathbf{t}}_{\mathfrak{q}}$. The new types satisfy $i(\tilde{\mathbf{t}}_{\mathfrak{p}}, \tilde{\mathbf{t}}_{\mathfrak{q}}) = j$ and they have the same j-th ϕ-polynomial; finally, if $i = j$, the polynomial $\phi_{i,\mathfrak{q}}$ is the $(j+1)$-th ϕ-polynomial of $\tilde{\mathbf{t}}_{\mathfrak{q}}$. Therefore, the computation of $v_{\mathfrak{p}}(\phi_{i,\mathfrak{q}})$ is deduced by the same arguments as above. □

We are ready to construct the family $\{b_{\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{P}}$. Consider the following equivalence relation in the set $\mathcal{P}$:

$$\mathfrak{p} \sim \mathfrak{q} \iff \psi_{0,\mathfrak{p}} = \psi_{0,\mathfrak{q}},$$

and denote by $[\mathfrak{p}]$ the class of any $\mathfrak{p} \in \mathcal{P}$.

For any class $[\mathfrak{p}]$ and any $\mathfrak{q} \in [\mathfrak{p}]$, we take (with the notation of Definition 3.7):

$$(\phi_{1,[\mathfrak{p}]}, \lambda^0_{1,\mathfrak{q}}) := \begin{cases} (\phi_{1,\mathfrak{q}}, \lambda_{1,\mathfrak{q}}), & \text{if Refinements}_{1,\mathfrak{q}} \text{ is empty,} \\ \left(\phi^{(1)}_{1,\mathfrak{q}}, \lambda^{(1)}_{1,\mathfrak{q}}\right), & \text{if Refinements}_{1,\mathfrak{q}} \text{ is not empty.} \end{cases}$$

By the first remark following Definition 3.7, the polynomial $\phi_{1,[\mathfrak{p}]}$ does not depend on the choice of $\mathfrak{q} \in [\mathfrak{p}]$. By (7) and (8),

$$(11) \qquad v_{\mathfrak{q}}(\phi_{1,[\mathfrak{p}]}(\theta)) = \begin{cases} 0, & \text{if } \mathfrak{q} \notin [\mathfrak{p}], \\ e(\mathfrak{q}/p)|\lambda^0_{1,\mathfrak{q}}|, & \text{if } \mathfrak{q} \in [\mathfrak{p}]. \end{cases}$$

Consider now, for each class $[\mathfrak{p}]$:

$$B_{[\mathfrak{p}]}(x) := \prod_{[\mathfrak{q}]\neq[\mathfrak{p}]} \phi_{1,[\mathfrak{q}]}(x).$$

Fix a prime ideal $\mathfrak{p} \in \mathcal{P}$. If $\#[\mathfrak{p}] = 1$, the element $b_{\mathfrak{p}} = (B_{[\mathfrak{p}]}(\theta))^2$ satisfies (9) already. Suppose now $\#[\mathfrak{p}] > 1$. For all $\mathfrak{l} \in [\mathfrak{p}]$, $\mathfrak{l} \neq \mathfrak{p}$, let $\phi_{\mathfrak{l}} = \phi_{r_{\mathfrak{l}}+1,\mathfrak{l}}$ be the Okutsu approximation to $f_{\mathfrak{l}}(x)$ contained in $\mathbf{t}_{\mathfrak{l}}$; consider the least positive numerator and denominator of the rational number $v_{\mathfrak{p}}(\phi_{\mathfrak{l}}(\theta))/e(\mathfrak{p}/p)$ (which has been computed in Proposition 3.8):

$$\frac{v_{\mathfrak{p}}(\phi_{\mathfrak{l}}(\theta))}{e(\mathfrak{p}/p)} = \frac{n_{\mathfrak{l}}}{d_{\mathfrak{l}}}, \quad \gcd(n_{\mathfrak{l}}, d_{\mathfrak{l}}) = 1.$$

We look for an integral element of the form:

$$(12) \qquad b_{\mathfrak{p}} = \frac{(B_{[\mathfrak{p}]}(\theta))^m \prod_{\mathfrak{l}\in[\mathfrak{p}], \, \mathfrak{l}\neq\mathfrak{p}} \phi_{\mathfrak{l}}(\theta)^{d_{\mathfrak{l}}}}{p^N},$$

where the exponents N, m are given by

$$N = \sum_{\mathfrak{l}\in[\mathfrak{p}], \, \mathfrak{l}\neq\mathfrak{p}} n_{\mathfrak{l}}, \qquad m = \left\lceil \max_{\mathfrak{q}\in\mathcal{P}, \, \mathfrak{q}\notin[\mathfrak{p}]} \left\{ \frac{Ne(\mathfrak{q}/p)+2}{e(\mathfrak{q}/p)|\lambda^0_{1,\mathfrak{q}}|} \right\} \right\rceil.$$

Take $\mathfrak{q} \notin [\mathfrak{p}]$. By (7) and (11), we have

$$v_{\mathfrak{q}}\left(\prod_{\mathfrak{l}\in[\mathfrak{p}], \, \mathfrak{l}\neq\mathfrak{p}} \phi_{\mathfrak{l}}(\theta)^{d_{\mathfrak{l}}} \right) = 0, \qquad v_{\mathfrak{q}}(B_{[\mathfrak{p}]}(\theta)) = v_{\mathfrak{q}}(\phi_{1,[\mathfrak{q}]}(\theta)) = e(\mathfrak{q}/p)|\lambda^0_{1,\mathfrak{q}}|.$$

Hence, $v_{\mathfrak{q}}(p^N b_{\mathfrak{p}}) = m\, e(\mathfrak{q}/p)|\lambda^0_{1,\mathfrak{q}}| \geq Ne(\mathfrak{q}/p) + 2$, so that $v_{\mathfrak{q}}(b_{\mathfrak{p}}) > 1$, as desired.

For the prime $\mathfrak{p}$ itself, we have $v_{\mathfrak{p}}(B_{[\mathfrak{p}]}(\theta)) = 0$ and, by construction,

$$v_{\mathfrak{p}}(b_{\mathfrak{p}}) = \left(\sum_{\mathfrak{l}\in[\mathfrak{p}], \, \mathfrak{l}\neq\mathfrak{p}} d_{\mathfrak{l}} v_{\mathfrak{p}}(\phi_{\mathfrak{l}}(\theta)) \right) - Ne(\mathfrak{p}/p) = 0.$$

Finally, for a prime $\mathfrak{l} \in [\mathfrak{p}]$, $\mathfrak{l} \neq \mathfrak{p}$, we have $v_{\mathfrak{l}}(B_{[\mathfrak{p}]}(\theta)) = 0$ and

$$v_{\mathfrak{l}}(b_{\mathfrak{p}}) = u_1 + u_2 - Ne(\mathfrak{l}/p), \quad u_1 := \sum_{\mathfrak{l}'\in[\mathfrak{p}], \, \mathfrak{l}'\neq\mathfrak{p},\mathfrak{l}} v_{\mathfrak{l}}(\phi_{\mathfrak{l}'}(\theta)^{d_{\mathfrak{l}'}}), \quad u_2 := v_{\mathfrak{l}}(\phi_{\mathfrak{l}}(\theta)^{d_{\mathfrak{l}}}).$$

Lemma 3.6 and Proposition 3.8 show that u_1 (as all invariants we used so far) depends only on the numerical invariants of the types $\mathbf{t}_\mathfrak{l}, \mathbf{t}_{\mathfrak{l}'}$, of level $1 \leq i \leq i(\mathbf{t}_\mathfrak{l}, \mathbf{t}_{\mathfrak{l}'}) \leq \min\{r_\mathfrak{l}, r_{\mathfrak{l}'}\}$, and not on the quality of the Okutsu approximations $\phi_{\mathfrak{l}'}$. On the other hand, u_2 depends on the choice of $\phi_\mathfrak{l}$ as an Okutsu approximation to $f_\mathfrak{l}(x)$; by (10):

$$u_2 = v_\mathfrak{l}(\phi_\mathfrak{l}(\theta)^{d_\mathfrak{l}}) = d_\mathfrak{l}\, e(\mathfrak{l}/p) \frac{V_{r_\mathfrak{l}+1,\mathfrak{l}} + h_{r_\mathfrak{l}+1,\mathfrak{l}}}{e_{1,\mathfrak{l}} \cdots e_{r_\mathfrak{l},\mathfrak{l}}} = d_\mathfrak{l}(V_{r_\mathfrak{l}+1,\mathfrak{l}} + h_{r_\mathfrak{l}+1,\mathfrak{l}}).$$

Hence, for all $\mathfrak{l} \in [\mathfrak{p}]$, $\mathfrak{l} \neq \mathfrak{p}$, we improve the Okutsu approximation $\phi_\mathfrak{l}$ till we get

$$h_{r_\mathfrak{l}+1,\mathfrak{l}} \geq \frac{2 + Ne(\mathfrak{l}/p) - u_1}{d_\mathfrak{l}} - V_{r_\mathfrak{l}+1,\mathfrak{l}}.$$

This ensures that $v_\mathfrak{l}(b_\mathfrak{p}) > 1$, as desired.

3.3. Two-elements representation of a fractional ideal.

Any fractional ideal $\mathfrak{a}$ of K admits a two-elements representation, $\mathfrak{a} = (\ell, \alpha)$, where $\alpha \in K$ and $\ell = \ell(\mathfrak{a}) \in \mathbb{Q}$ is the least positive rational number contained in $\mathfrak{a}$. It is straightforward to obtain such a representation from the two-elements representation of the prime ideals obtained in the last section. For the sake of completeness we briefly describe the routine. For each prime ideal $\mathfrak{p}$ of K, we have computed an integral element $\alpha_\mathfrak{p} \in \mathbb{Z}_K$ such that

$$v_\mathfrak{p}(\alpha_\mathfrak{p}) = 1, \quad v_\mathfrak{q}(\alpha_\mathfrak{p}) = 0, \ \forall \mathfrak{q}|p, \ \mathfrak{q} \neq \mathfrak{p}.$$

These elements are of the form: $\alpha_\mathfrak{p} = p^{\nu_\mathfrak{p}} g_\mathfrak{p}(\theta)$, where $\nu_\mathfrak{p} \in \mathbb{Z}$ and $g_\mathfrak{p}(x) \in \mathbb{Z}[x]$ is a primitive polynomial. Generically, $\nu_\mathfrak{p} \leq 0$, except for the special case $\mathfrak{p} = p\mathbb{Z}_K$, where $\nu_\mathfrak{p} = 1$, $g_\mathfrak{p}(x) = 1$. Let us write

$$N_{K/\mathbb{Q}}(g_\mathfrak{p}(\theta)) = p^{\mu_\mathfrak{p}} N_\mathfrak{p}, \ \text{with } p \nmid N_\mathfrak{p}.$$

Suppose first that $\mathfrak{a} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{a_\mathfrak{p}}$ has support only in prime ideals dividing p. We take then:

$$\alpha := \prod_{\mathfrak{p}|p} \alpha_\mathfrak{p}^{a_\mathfrak{p}} \prod_{a_\mathfrak{p}<0} N_\mathfrak{p}^{|a_\mathfrak{p}|}, \qquad H := \left\lceil \max_{\mathfrak{p}|p} \left\{ \frac{a_\mathfrak{p}}{e(\mathfrak{p}/p)} \right\} \right\rceil.$$

One checks easily that $\ell(\mathfrak{a}) = p^H$ and $\mathfrak{a} = (p^H, \alpha)$.

In the general case, $\mathfrak{a} = \prod_{p \in S} \mathfrak{a}_p$, where S is a finite set of prime numbers and $\mathfrak{a}_p$ is divided only by prime ideals lying over p. For each $\mathfrak{a}_p$ we find a two-elements representation $\mathfrak{a}_p = (p^{H_p}, \alpha_p)$; then, the two-elements representation of $\mathfrak{a}$ is:

$$\mathfrak{a} = \left(\prod_{p \in S} p^{H_p}, \sum_{p \in S} \left(\prod_{q \in S,\, q \neq p} q^{H_q+1} \right) \alpha_p \right).$$

Note that the second generator α constructed in this way satisfies: $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\mathfrak{a})$, for all $\mathfrak{p}$ with $v_\mathfrak{p}(\mathfrak{a}) \neq 0$, which is slightly stronger than the condition $\mathfrak{a} = (\ell, \alpha)$.

4. RESIDUE CLASSES AND CHINESE REMAINDER THEOREM

In this section we show how to compute residue classes modulo prime ideals, and we design a Chinese remainder theorem routine. As in the previous sections, this will be done without constructing (a basis of) the maximal order of K and without the necessity to invert elements in the number field. Only some inversions in the finite residue fields are required.

For any prime ideal $\mathfrak{p}$ of K we keep the notations for $\mathbf{t}_\mathfrak{p}$, $f_\mathfrak{p}(x)$, $\phi_\mathfrak{p}(x)$, $\mathbb{F}_\mathfrak{p}$, $\theta_\mathfrak{p}$, $K_\mathfrak{p}$, $\mathbb{Z}_{K_\mathfrak{p}}$, as introduced in section 1.4.

4.1. Residue classes modulo a prime ideal. Let $\mathfrak{p}$ be a prime ideal of K, corresponding to an f-complete type $\mathbf{t}_\mathfrak{p}$ with an added $(r+1)$-th level, as indicated in section 1.4.

The finite field $\mathbb{F}_\mathfrak{p} := \mathbb{F}_{r+1}$ is a computational representation of the residue field $\mathbb{Z}_K/\mathfrak{p}$. In fact, fix the topological embedding, $\iota_\mathfrak{p} \colon K \hookrightarrow K_\mathfrak{p}$, determined by sending θ to $\theta_\mathfrak{p}$, and consider the reduction modulo $\mathfrak{p}$ map obtained by composition of the embedding $\mathbb{Z}_K \hookrightarrow \mathbb{Z}_{K_\mathfrak{p}}$ with the local reduction map constructed in (5):

$$\mathrm{red}_\mathfrak{p} \colon \mathbb{Z}_K \hookrightarrow \mathbb{Z}_{K_\mathfrak{p}} \xrightarrow{\mathrm{lred}_\mathfrak{p}} \mathbb{F}_\mathfrak{p}.$$

The commutative diagram:

$$
\begin{array}{ccccc}
\mathbb{Z}_K & \hookrightarrow & \mathbb{Z}_{K_\mathfrak{p}} & \xrightarrow{\mathrm{lred}_\mathfrak{p}} & \mathbb{F}_\mathfrak{p} \\
\downarrow & & \downarrow & & \| \\
\mathbb{Z}_K/\mathfrak{p} & \xrightarrow{\sim} & \mathbb{Z}_{K_\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{K_\mathfrak{p}} & \xrightarrow[\sim]{\gamma^{-1}} & \mathbb{F}_\mathfrak{p}
\end{array}
$$

shows that our reduction map $\mathrm{red}_\mathfrak{p}$ coincides with the canonical reduction map, $\mathbb{Z}_K \longrightarrow \mathbb{Z}_K/\mathfrak{p}$, up to certain isomorphism $\mathbb{Z}_K/\mathfrak{p} \xrightarrow{\sim} \mathbb{F}_\mathfrak{p}$.

The problem has now a computational perspective; we want to find a routine that computes $\mathrm{red}_\mathfrak{p}(\alpha) \in \mathbb{F}_\mathfrak{p}$ for any given integral element $\alpha \in \mathbb{Z}_K$. To this end, it is sufficient to have a routine that computes $\mathrm{lred}_\mathfrak{p}(\alpha) \in \mathbb{F}_\mathfrak{p}$, for any $\mathfrak{p}$-integral $\alpha \in K$. Let us show that this latter routine may be based on item 2 of Proposition 2.1 and Lemma 1.4.

Any $\alpha \in \mathbb{Z}_K$ can be written in a unique way as:

$$\alpha = \frac{a}{b} \frac{g(\theta)}{p^N},$$

where a, b are positive coprime integers not divisible by p and $g(x) \in \mathbb{Z}[x]$ is a primitive polynomial. Clearly,

$$\mathrm{red}_\mathfrak{p}(\alpha) = \mathrm{lred}_\mathfrak{p}(\iota_\mathfrak{p}(\alpha)) = \mathrm{lred}_\mathfrak{p}(a/b)\,\mathrm{lred}_\mathfrak{p}(g(\theta_\mathfrak{p})/p^N),$$

and $\mathrm{lred}_\mathfrak{p}(a/b) \in \mathbb{F}_\mathfrak{p}$ is the element in the prime field determined by the quotient of the classes modulo p of a and b. Thus, we need only to compute $\mathrm{lred}_\mathfrak{p}(g(\theta_\mathfrak{p})/p^N)$.

If $N = 0$, then $\mathrm{lred}_\mathfrak{p}(g(\theta_\mathfrak{p})) = \mathrm{red}_\mathfrak{p}(g(\theta))$ is just the class of $g(x)$ modulo the ideal $(p, \phi_{1,\mathfrak{p}}(x))$. In other words, if $\overline{g}(x) \in \mathbb{F}_0[x]$ is the polynomial obtained by reduction of the coefficients of $g(x)$ modulo p, then $\mathrm{red}_\mathfrak{p}(g(\theta)) = \overline{g}(z_0) \in \mathbb{F}_{1,\mathfrak{p}} \subset \mathbb{F}_\mathfrak{p}$.

If $N > 0$, we look for the first index, $1 \le i \le r+1$, for which the truncation $\mathrm{Trunc}_i(\mathbf{t})$ does not divide $g(x)$. In the paragraph following Proposition 2.1 we showed that this will always occur, eventually (for $i = r+1$) after improving the Okutsu approximation $\phi_\mathfrak{p} = \phi_{r+1}$. By Proposition 2.1, there is a computable point $(s, u) \in N_i(g)$ such that $v(g(\theta_\mathfrak{p})) = (sh_i + ue_i)/(e_1 \cdots e_i) = v(\Phi_i(\theta_\mathfrak{p})^s \pi_i(\theta_\mathfrak{p})^u)$, and

$$\mathrm{lred}_\mathfrak{p}\left(\frac{g(\theta_\mathfrak{p})}{\Phi_i(\theta_\mathfrak{p})^s \pi_i(\theta_\mathfrak{p})^u}\right) = R_i(g)(z_i) \ne 0.$$

Now, if $(sh_i + ue_i)/(e_1 \cdots e_i) > N$, we have $\mathrm{lred}_\mathfrak{p}(g(\theta_\mathfrak{p})/p^N) = 0$; on the other hand, if $(sh_i + ue_i)/(e_1 \cdots e_i) = N$, we have

$$(13) \quad \mathrm{lred}_\mathfrak{p}\left(\frac{g(\theta_\mathfrak{p})}{p^N}\right) = R_i(g)(z_i) \cdot \mathrm{lred}_\mathfrak{p}\left(\frac{\Phi_i(\theta_\mathfrak{p})^s \pi_i(\theta_\mathfrak{p})^u}{p^N}\right) = R_i(g)(z_i)\,z_1^{t_1} \cdots z_i^{t_i},$$

where $p^{-N}\Phi_i(\theta_{\mathfrak{p}})^s \pi_i(\theta_{\mathfrak{p}})^u = \gamma_1^{t_1} \cdots \gamma_i^{t_i}$, and the vector $(t_1, \ldots, t_i) \in \mathbb{Z}^i$ can be found by the procedure of Lemma 1.4, applied to the input vector

$$\log_{\mathbf{t}_{\mathfrak{p}}, i}\left(p^{-N}\Phi_i(x)^s \pi_i(x)^u\right) = (-N, 0, \ldots, 0) + s(\log \Phi)_i + u(\log \pi)_i.$$

Since $(\log \Phi)_i$, $(\log \pi)_i$ have been stored as secondary invariants of $\mathbf{t}_{\mathfrak{p}}$, we get in this way a really fast computation of $\mathrm{lred}_{\mathfrak{p}}(p^{-N}g(\theta_{\mathfrak{p}}))$.

This ends the computation of the reduction modulo $\mathfrak{p}$ map $\mathrm{red}_{\mathfrak{p}}$.

4.2. **Chinese remainder theorem.** It is straightforward to design a Chinese remainder routine once the following problem is solved.

Problem. *Let p be a prime number, $\mathcal{P}$ the set of prime ideals of K lying above p, and $(a_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}}$ a family of non-negative integers. Find a family $(c_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}}$ of integral elements $c_{\mathfrak{p}} \in \mathbb{Z}_K$ such that,*

$$(14) \qquad c_{\mathfrak{p}} \equiv 1 \ (\mathrm{mod}\ \mathfrak{p}^{a_{\mathfrak{p}}}), \quad c_{\mathfrak{p}} \equiv 0 \ (\mathrm{mod}\ \mathfrak{q}^{a_{\mathfrak{q}}}), \ \forall \mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p},$$

for all $\mathfrak{p} \in \mathcal{P}$.

There is an easy solution to this problem: take the element $b_{\mathfrak{p}} \in \mathbb{Z}_K$ satisfying (9), constructed in section 3.2, and consider $c_{\mathfrak{p}} = (b_{\mathfrak{p}})^{p^t(q_{\mathfrak{p}}-1)}$, where $q_{\mathfrak{p}} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = \#\mathbb{F}_{\mathfrak{p}}$, and t is sufficiently large. However, the element $c_{\mathfrak{p}}$ constructed in this way is not useful for practical purposes because it may have a huge norm and a huge height (very large numerators or denominators of the coefficients of its standard representation as a polynomial in θ), if $q_{\mathfrak{p}}$ or t are large. Instead, we shall refine the construction of the element $b_{\mathfrak{p}}$ to get a small size solution $c_{\mathfrak{p}}$ to the above problem.

First we deal with the particular case $a_{\mathfrak{p}} = 1$. The idea is to get an element $b_{\mathfrak{p}} \in \mathbb{Z}_K$ satisfying

$$v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0, \quad v_{\mathfrak{q}}(b_{\mathfrak{p}}) \geq a_{\mathfrak{q}}, \ \forall \mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p},$$

and then find $\beta \in K$ such that $v_{\mathfrak{p}}(\beta) = 0$ and $c_{\mathfrak{p}} := b_{\mathfrak{p}}\beta$ satisfies (14). Since we know the two-elements representation $\mathfrak{q} = (p, \alpha_{\mathfrak{q}})$ of the prime ideals, we could take $b_{\mathfrak{p}} = \prod_{\mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p}}(\alpha_{\mathfrak{q}})^{a_{\mathfrak{q}}}$. Again, this might lead to a $b_{\mathfrak{p}}$ with large size, so that a direct construction of $b_{\mathfrak{p}}$ is preferable in order to keep its size as small as possible.

Thus, we consider an element $b_{\mathfrak{p}} \in \mathbb{Z}_K$ as in (12):

$$b_{\mathfrak{p}} = \frac{(B_{[\mathfrak{p}]}(x))^m \prod_{\mathfrak{l} \in [\mathfrak{p}], \ \mathfrak{l} \neq \mathfrak{p}} \phi_{\mathfrak{l}}(x)^{d_{\mathfrak{l}}}}{p^N},$$

with $N = \sum_{\mathfrak{l} \in [\mathfrak{p}], \ \mathfrak{l} \neq \mathfrak{p}} d_{\mathfrak{l}} v(\phi_{\mathfrak{l}}(\theta_{\mathfrak{p}})) = \sum_{\mathfrak{l} \in [\mathfrak{p}], \ \mathfrak{l} \neq \mathfrak{p}} n_{\mathfrak{l}}$. By construction, $v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0$.

Let $i = \max_{\mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p}}\{i(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{q}})\}$; Lemma 3.6 shows that $i \leq r_{\mathfrak{p}}$. From now on, we use only invariants of the type $\mathbf{t}_{\mathfrak{p}}$ and we drop the subindex $\mathfrak{p}$ in the notation. Let

$$M = \left\lceil \frac{V_{i+1}}{e_1 \cdots e_i} \right\rceil.$$

Arguing as in section 3.2, we can take m sufficiently large, and each $\phi_{\mathfrak{l}}(x)$ sufficiently close to the p-adic irreducible factor $f_{\mathfrak{l}}(x)$, so that

$$(15) \qquad v_{\mathfrak{q}}(b_{\mathfrak{p}}) \geq a_{\mathfrak{q}} + Me(\mathfrak{q}/p), \ \forall \mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p},$$

while keeping fixed the denominator p^N and the condition $v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0$. In particular, $b_{\mathfrak{p}}$ belongs to $\mathbb{Z}_K$. The idea is to multiply $b_{\mathfrak{p}}$ by some element in K that conveniently modifies its residue class modulo $\mathfrak{p}$. We split this task into two parts,

that may be considered as a kind of respective inversion modulo $\mathfrak{p}$ of $(B_{[\mathfrak{p}]}(\theta))^m$ and $p^{-N} \prod_{\mathfrak{l} \in [\mathfrak{p}], \, \mathfrak{l} \neq \mathfrak{p}} \phi_{\mathfrak{l}}(\theta)^{d_{\mathfrak{l}}}$.

Let $h(x) = (B_{[\mathfrak{p}]}(x))^m$. Then, $\zeta := \mathrm{red}_{\mathfrak{p}}(h(\theta)) \in \mathbb{F}_1 \subset \mathbb{F}_{\mathfrak{p}}$ is just the class of $h(x)$ modulo the ideal $(p, \phi_1(x))$. We invert ζ in $\mathbb{F}_1$ and represent the inverse $\zeta^{-1} = \overline{P}(z_0)$, as a polynomial in z_0 of degree less than f_0, with coefficients in the prime field $\mathbb{F}_0$. Take $\beta_0 = P(\theta)$, where $P(x) \in \mathbb{Z}[x]$ is an arbitrary lift of $\overline{P}(x)$; clearly, $h(\theta)\beta_0 \equiv 1 \pmod{\mathfrak{p}}$.

Let now $g(x) = p^{-N} \prod_{\mathfrak{l} \in [\mathfrak{p}], \, \mathfrak{l} \neq \mathfrak{p}} \phi_{\mathfrak{l}}(x)^{d_{\mathfrak{l}}}$. If $[\mathfrak{p}] = \{\mathfrak{p}\}$, then $i = 0$, $N = M = 0$, $g(x) = 1$ and we are done. Suppose $[\mathfrak{p}] \supsetneq \{\mathfrak{p}\}$, so that $1 \leq i \leq r_{\mathfrak{p}}$. By the definition of the index of coincidence, we have $\mathrm{Trunc}_i(\mathbf{t}_{\mathfrak{p}}) \nmid \phi_{\mathfrak{l}}(x)$, for all $\mathfrak{l} \neq \mathfrak{p}$; by the Theorem of the product [HN12, Thm. 2.26], $\mathrm{Trunc}_i(\mathbf{t}_{\mathfrak{p}}) \nmid g(x)$. Therefore, as we saw in the last section,

$$\xi := \mathrm{lred}_{\mathfrak{p}}(p^{-N} g(\theta_{\mathfrak{p}})) = R_i(g)(z_i)\, z_1^{t_1} \cdots z_i^{t_i} \in \mathbb{F}_{i+1},$$

for some easily computable sequence of integers $(t_1, \ldots, t_i)$. Let $V = e_1 \cdots e_i M$; by [HN12, Cor. 3.2], $v\left(\pi_{i+1}(\theta_{\mathfrak{p}})^V\right) = M$. Compute a vector $(t_1', \ldots, t_i') \in \mathbb{Z}^i$ such that $p^{-M} \pi_{i+1}(x)^V = \gamma_1^{t_1'} \cdots \gamma_i^{t_i'}$, as indicated in Lemma 1.4, and take

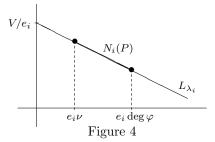$$\xi' := z_1^{t_1'} \cdots z_i^{t_i'} \in \mathbb{F}_{i+1}.$$

Let $\varphi(y) \in \mathbb{F}_i[y]$ be the unique polynomial of degree less than f_i, such that $\varphi(z_i) = z_i^{\ell_i V/e_i}(\xi\xi')^{-1}$. Let $\nu = \mathrm{ord}_y \varphi(y)$. Clearly,

$$V \geq V_{i+1} = e_i f_i v_{i+1}(\phi_i),$$

the last equality by [HN12, Thm. 2.11]. Therefore, we can apply the constructive method described in [HN12, Prop. 2.10] to compute a polynomial $P(x) \in \mathbb{Z}[x]$ satisfying the following properties:

$$\deg P(x) < m_{i+1}, \qquad v_{i+1}(P) = V, \qquad y^\nu R_i(P)(y) = \varphi(y).$$

A look at the proof of [HN12, Prop. 2.10] shows that $N_i(P)$ is one sided of slope λ_i and its end points have abscissa $e_i\nu$ and $e_i \deg \varphi$ (cf. Figure 4).

Figure 4

Claim: $\mathrm{lred}_{\mathfrak{p}}(p^{-M} P(\theta_{\mathfrak{p}})) = \xi^{-1}$.

In fact, since $\deg P(x) < m_{i+1}$ and $v_{i+1}(P) = V$, the Newton polygon $N_{i+1}(P)$ is the single point $(0, V)$; in particular, $\mathrm{Trunc}_{i+1}(\mathbf{t}_{\mathfrak{p}})$ does not divide $P(x)$ and Proposition 2.1 shows that $v(P(\theta_{\mathfrak{p}})) = V/(e_1 \cdots e_i) = M$ and

$$\mathrm{lred}_{\mathfrak{p}}\left(P(\theta_{\mathfrak{p}})/\pi_{i+1}(\theta_{\mathfrak{p}})^V\right) = R_{i+1}(P)(z_{i+1}) \neq 0.$$

Actually, $R_{i+1}(P)(y)$ has degree 0 and it represents a constant in $\mathbb{F}_{i+1}$ that we denote simply by $R_{i+1}(P)$. By (13),

$$\mathrm{lred}_{\mathfrak{p}}\left(p^{-M} P(\theta_{\mathfrak{p}})\right) = R_{i+1}(P)\, \mathrm{lred}_{\mathfrak{p}}(p^{-M} \pi_{i+1}(\theta_{\mathfrak{p}})^V) = R_{i+1}(P)\, \xi'.$$

By the very definition of the residual polynomial [HN12, Defs. 2.20+2.21], we have

$$R_{i+1}(P) = z_i^{(e_i \nu - \ell_i V)/e_i} R_i(P)(z_i) = z_i^{-\ell_i V/e_i} \varphi(z_i) = (\xi \xi')^{-1},$$

and the Claim is proved.

Finally, consider

$$c_{\mathfrak{p}} := b_{\mathfrak{p}} \beta_0 (p^{-M} P(\theta)).$$

The condition (15) ensures that $c_{\mathfrak{p}}$ belongs to $\mathbb{Z}_K$ (although $p^{-M} P(\theta)$ might not be integral) and satisfies $v_{\mathfrak{q}}(c_{\mathfrak{p}}) \geq a_{\mathfrak{q}}$, for all $\mathfrak{q} \in \mathcal{P}$, $\mathfrak{q} \neq \mathfrak{p}$. By construction, $\mathrm{red}_{\mathfrak{p}}(c_{\mathfrak{p}}) = \mathrm{lred}_{\mathfrak{p}}(\iota_{\mathfrak{p}}(c_{\mathfrak{p}})) = 1$.

It remains to solve our Problem when $a_{\mathfrak{p}} > 1$. In this case, we find $c \in \mathbb{Z}_K$ such that

$$c \equiv 1 \ (\mathrm{mod} \ \mathfrak{p}), \qquad c \equiv 0 \ (\mathrm{mod} \ \mathfrak{q}^{a_{\mathfrak{q}}}), \ \forall \mathfrak{q} \in \mathcal{P}, \ \mathfrak{q} \neq \mathfrak{p},$$

and we take $c_{\mathfrak{p}} = (c-1)^m + 1$, where m is the least odd integer that is greater than or equal to $a_{\mathfrak{p}}/v_{\mathfrak{p}}(c-1)$.

5. p-INTEGRAL BASES

Let p be a prime number and let $\mathbb{F} = \mathrm{GF}(p)$ be the prime field of characteristic p. A *p-integral basis of K* is a family of n $\mathbb{Z}$-linearly independent integral elements $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_K$ such that

$$p \nmid \left(\mathbb{Z}_K : \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}} \right),$$

or equivalently, such that the family $\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ is $\mathbb{F}$-linearly independent in the $\mathbb{F}$-algebra $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{F}$.

If the discriminant $\mathrm{disc}(f)$ of $f(x)$ may be factorized, the computation of an integral basis of K (a $\mathbb{Z}$-basis of $\mathbb{Z}_K$) is based on the computation of p-integral bases for the different primes p that divide $\mathrm{disc}(f)$.

Anyhow, even when $\mathrm{disc}(f)$ may not be factorized, the computation of a p-integral basis of K for a given prime p is an interesting task on its own. In this section we show how to carry out this task from the data captured by the OM representations of the prime ideals $\mathfrak{p}$ lying over p. For any such prime ideal we keep the notations for $f_{\mathfrak{p}}(x)$, $\phi_{\mathfrak{p}}(x)$, $n_{\mathfrak{p}}$, $\mathbb{F}_{\mathfrak{p}}$, $\theta_{\mathfrak{p}}$, $K_{\mathfrak{p}}$, $\mathbb{Z}_{K_{\mathfrak{p}}}$, as introduced in section 1.4.

5.1. **Local exponent of a prime ideal.** Let $\mathcal{P}$ be the set of prime ideals lying over p. For any $\mathfrak{p} \in \mathcal{P}$ we fix the topological embedding $K \hookrightarrow K_{\mathfrak{p}}$ determined by sending θ to $\theta_{\mathfrak{p}}$.

Definition 5.1. *We define the local exponent of $\mathfrak{p} \in \mathcal{P}$ to be the least positive integer* $\exp(\mathfrak{p})$ *such that*

$$p^{\exp(\mathfrak{p})} \mathbb{Z}_{K_{\mathfrak{p}}} \subset \mathbb{Z}_p[\theta_{\mathfrak{p}}].$$

Note that $\exp(\mathfrak{p})$ is an invariant of the irreducible polynomial $f_{\mathfrak{p}}(x) \in \mathbb{Z}_p[x]$, but it is not an intrinsic invariant of $\mathfrak{p}$.

The computation of $\exp(\mathfrak{p})$ is easily derived from the results of [GMN10].

Let $\mathfrak{p} = [p; \phi_1, \ldots, \phi_r, \phi_{\mathfrak{p}}]$ be the OM representation of $\mathfrak{p}$, as indicated in section 1.4. By [GMN10, Lem. 4.5]:

$$f_{\mathfrak{p}}(x) \equiv \phi_{\mathfrak{p}}(x) \ (\mathrm{mod} \ \mathfrak{m}^{\lceil \nu \rceil}), \quad \text{where } \nu = \nu_{\mathfrak{p}} + (h_{r+1}/e(\mathfrak{p}/p)),$$

and $\nu_{\mathfrak{p}}$ is the rational number

$$\nu_{\mathfrak{p}} := \frac{h_1}{e_1} + \frac{h_2}{e_1 e_2} + \cdots + \frac{h_r}{e_1 \cdots e_r}.$$

Caution: this number is not always an invariant of $f_{\mathfrak{p}}(x)$. If $e_r f_r = 1$, the Okutsu depth of $f_{\mathfrak{p}}(x)$ is $R = r - 1$ (cf. (2)), and h_r depends on the choice of ϕ_r.

Denote $\phi_0(x) = x$, $m_0 = 1$, $m_{r+1} = n_{\mathfrak{p}}$. Any integer $0 \le m < n_{\mathfrak{p}}$ can be written in a unique way as:

$$m = \sum_{i=0}^{r} a_i m_i, \quad 0 \le a_i < \frac{m_{i+1}}{m_i}.$$

Then, $g_m(x) := \prod_{i=0}^{r} \phi_i(x)^{a_i}$ is a divisor polynomial of degree m of $f_{\mathfrak{p}}(x)$ [GMN10, Thm. 2.15]. Also, if $\nu_m := \lfloor v(g_m(\theta)) \rfloor$, the family

$$(16) \qquad 1, \frac{g_1(\theta_{\mathfrak{p}})}{p^{\nu_1}}, \ldots, \frac{g_{n_{\mathfrak{p}}-1}(\theta_{\mathfrak{p}})}{p^{\nu_{n_{\mathfrak{p}}-1}}}$$

is a $\mathbb{Z}_p$-basis of $\mathbb{Z}_{K_{\mathfrak{p}}}$ [Oku82, I,Thm. 1]. Since the numerators $g_m(x)$ have strictly increasing degree and $\nu_1 \le \cdots \le \nu_{n_{\mathfrak{p}}-1}$, it is clear that $\exp(\mathfrak{p}) = \nu_{n_{\mathfrak{p}}-1}$.

On the other hand, since $m_{i+1}/m_i = e_i f_i$, we have

$$\nu_{n_{\mathfrak{p}}-1} = \left\lfloor \sum_{i=1}^{r} (e_i f_i - 1) v(\phi_i(\theta_{\mathfrak{p}})) \right\rfloor$$

Now, along the proof of [GMN10, Lem. 4.5], it was shown that:

$$(17) \qquad \sum_{i=1}^{r} (e_i f_i - 1) v(\phi_i(\theta_{\mathfrak{p}})) = v(\phi_{r+1}(\theta_{\mathfrak{p}})) - \nu_{\mathfrak{p}} - \frac{h_{r+1}}{e(\mathfrak{p}/p)} = \frac{V_{r+1}}{e(\mathfrak{p}/p)} - \nu_{\mathfrak{p}}.$$

Thus, if we combine (17) with the explicit formula:

$$V_{r+1} = \sum_{i=1}^{r} e_{i+1} \cdots e_r (e_i f_i \cdots e_r f_r) h_i,$$

given in [HN12, Prop. 2.15], we get the following explicit computation of $\exp(\mathfrak{p})$ in terms of the invariants of the OM representation of $\mathfrak{p}$.

Theorem 5.2. *For all $\mathfrak{p} \in \mathcal{P}$, we have $\exp(\mathfrak{p}) = \lfloor \mu_{\mathfrak{p}} \rfloor$, where*

$$\mu_{\mathfrak{p}} := \frac{V_{r+1}}{e(\mathfrak{p}/p)} - \nu_{\mathfrak{p}} = \sum_{i=1}^{r} (e_i f_i \cdots e_r f_r - 1) \frac{h_i}{e_1 \cdots e_i}.$$

Note that $\mu_{\mathfrak{p}}$ is an Okutsu invariant, because it depends only on e_i, f_i, h_i, for $1 \le i \le R$, where R is the Okutsu depth of $f_{\mathfrak{p}}(x)$. If $R = r - 1$, then $e_r f_r = 1$ and the summand of $\mu_{\mathfrak{p}}$ corresponding to $i = r$ vanishes.

5.2. **Computation of a p-integral basis.** Along the computation of the prime ideal decomposition of the ideal $p\mathbb{Z}_K$ (by a single call to the Montes algorithm) we can easily store the local exponents $\exp(\mathfrak{p})$, and the numerators $g_m(x)$ and denominators p^{ν_m} of all $\mathbb{Z}_p$-bases of $\mathbb{Z}_{K_{\mathfrak{p}}}$ given in (16), for all $\mathfrak{p} \in \mathcal{P}$.

It is well-known how to derive a p-integral basis from all these local bases. Let us briefly describe a concrete procedure to do this, taken from [Ore25].

We apply the method described at the end of section 3.2 to compute multipliers $\{b_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{P}}$ satisfying:

$$(18) \qquad v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0, \quad v_{\mathfrak{q}}(b_{\mathfrak{p}}) \ge \exp(\mathfrak{p}) e(\mathfrak{q}/p) + e(\mathfrak{p}/p), \quad \forall \mathfrak{q} \in \mathcal{P}, \mathfrak{q} \ne \mathfrak{p}.$$

Consider the family obtained by multiplying each local basis (16) by its corresponding multiplier:

$$\mathcal{B}_{\mathfrak{p}} := \left[b_{\mathfrak{p}},\, b_{\mathfrak{p}}\, \frac{g_1(\theta)}{p^{\nu_1}},\, \ldots,\, b_{\mathfrak{p}}\, \frac{g_{n_{\mathfrak{p}}-1}(\theta)}{p^{\nu_{n_{\mathfrak{p}}-1}}} \right].$$

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

In fact, although the elements $g_m(\theta)/p^{\nu_m}$ are not (globally) integral, (18) shows that the products $\alpha_{m,\mathfrak{p}} := b_{\mathfrak{p}}\,(g_m(\theta)/p^{\nu_m})$ belong all to $\mathbb{Z}_K$ and satisfy

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

It is easy to deduce from this fact that the family of all $\alpha_{m,\mathfrak{p}}$ determines an $\mathbb{F}$-linearly independent family of the algebra $\mathbb{Z}_K \otimes_{\mathbb{Z}} \mathbb{F}$.

6. Some examples

We have implemented the algorithms described above in a package for Magma. The arithmetic of number fields in any algebraic manipulator has to face two problems: the factorization of the discriminant and the memory requirements for large degrees. Our package allows the user to skip the first problem, while it uses very little memory, expanding Magma's capabilities by far. The package which can be downloaded from its web page (`http:/ma4-upc.edu/ guardia/+Ideals.html`), is described in detail in the accompanying paper [GMN10b]. We include here a few examples which exhibit the power of the package in different situations. Since the bulk of our package is Montes algorithm, we have performed thousands of random tests of different kinds, which confirm the good performance predicted by its theoretical complexity.

[GMN11].

The computations in these examples have been done with Magma v2.15-11 in a Linux server, with two Intel Quad Core processors, running at 3.0 Ghz, with 32Gb of RAM memory.

6.1. **Large degree.** Consider the number field $K = \mathbb{Q}(\theta)$ given by a root $\theta \in \overline{\mathbb{Q}}$ of the polynomial $f(x) = x^{1000} + 2^{50}x^{50} + 2^{60}$. The factorization of the discriminant of f is

$$\mathrm{Disc}(f) = 2^{53940}\, 3^{50}\, 5^{2000}\, 127^{50}\, 313^{50}\, 743^{50}\, 4886229527^{50}\, p^{50},$$

with $p = 337572698551220494882323528404563236947916489629537$. The large degree of f makes impossible to work in this number field using the standard functions of Magma, even after factorizing the discriminant, since the computation of the integral basis is necessary for these functions. But our algorithms avoid this computation, so that we can work with ideals in K. For instance, in the table below we show the local index of the primes dividing $\mathrm{Disc}(f)$ and the time taken

to decompose them in K.

Ideal	Index	Time
$2\mathbb{Z}_K$	26235	$0.36s$
$3\mathbb{Z}_K$	0	$0.61s$
$5\mathbb{Z}_K$	20	$0.63s$
$127\mathbb{Z}_K$	0	$1.29s$
$313\mathbb{Z}_K$	0	$3.69s$
$743\mathbb{Z}_K$	0	$6.47s$
$4886229527\mathbb{Z}_K$	0	$6.96s$
$p\mathbb{Z}_K$	0	$60s$

Thus, we need less than 90 seconds to see that the discriminant of K is

$$\mathrm{Disc}(K) = 2^{1470}3^{50}5^{1960}127^{50}313^{50}743^{50}4886229527^{50}p^{50}.$$

The running times in the table show clearly that the cost of the factorizations increases mainly because of the size of the numbers involved, and that the index has not a serious impact on them. The largest type appearing in these computations has order 3, and it appears along the factorization of the ideal $2\mathbb{Z}_K$, which is

$$2\mathbb{Z}_K = \mathfrak{p}_1^{10}(\mathfrak{p}_1')^{38}\mathfrak{p}_4^{10}(\mathfrak{p}_4')^{38}\mathfrak{p}_{20}^{38},$$

where $\mathfrak{p}_f^e$ stands for a prime ideal with residual degree f and ramification index e. The ideals $I = (\theta^3 + 50)\mathbb{Z}_K$, $J = (\theta + 10)\mathbb{Z}_K$ have a huge norm, so that it is highly improbable to factor them in a reasonable time, but it takes only 0.03 seconds to compute the factorization of its sum:

$$I + J = \mathfrak{p}_1^2(\mathfrak{p}_1')^2\mathfrak{p}_4^2(\mathfrak{p}_4')^2\mathfrak{p}_{20}^2.$$

The decomposition of 5 in the maximal order $\mathbb{Z}_K$ is

$$5\mathbb{Z}_K = \mathfrak{p}_2^5(\mathfrak{p}_2')^5\mathfrak{p}_2^{20}(\mathfrak{p}_2')^{20}\mathfrak{p}_2^{25}\mathfrak{p}_4^{25}\mathfrak{p}_{15}^{25}(\mathfrak{p}_{15}')^{25}.$$

With the residue map computation explained in subsection 4.1, we may check very quickly that $\theta \equiv \zeta \pmod{\mathfrak{p}_4}$, where $\mathbb{Z}_K/\mathfrak{p}_4 \simeq \mathbb{F}_5[\zeta]$, with $\zeta^4 + 2\zeta^2 + 3 = 0$. The Chinese remainder algorithm works also very fast in this number field.

6.2. **Small degree, large coefficients.** The space of modular forms of level 1 and weight 76 has dimension 6. The newforms in this space are defined over the number field $K = \mathbb{Q}(\theta)$, where $\theta \in \overline{\mathbb{Q}}$ is a root of the polynomial:

$$f(x) = x^6 + 57080822040x^5 - 19800791856657142454768x^4$$
$$-11405115067164354385292006554337280x^3$$
$$+9757628454131691442128845013041495838774263808x^2$$
$$+290013995562379500498435975003716024800114593761580810240x$$
$$-92217203874207784163935379997152082331434364841943058919508374716416.$$

The discriminant of $f(x)$ is

$$\mathrm{Disc}(f) = \quad 2^{264}3^{72}5^{16}7^{16}11^213^217^419^243^259 \cdot 193^2\cdot$$
$$293 \cdot 391987^24759427^2137679681521^2M,$$

where M is a composite integer of 135 decimal figures which we have not been able to factorize. J. Rasmussen asked us ([Ras10]) for a test to check certain divisibility conditions on the ring of integers of K, related to his work on congruences satisfied

by the coefficients of certain modular forms. The time to find the decomposition of the primes in the set

$$S := \{2, 3, 5, 7, 11, 13, 17, 19, 43, 59, 193, 293, 391987, 4759427, 137679681521\}$$

is almost negligible, since it involves only types of order at most 1. The table below shows the local indices of these primes.

The discriminant of K is $\mathrm{Disc}(K) = 59{\cdot}293N$, where N is divisible by at least one of the prime factors of M, since M is not a square. The ideal prime decomposition of 3 in $\mathbb{Z}_K$ is

$$3\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''\mathfrak{p}_1'''.$$

Ideal	Index
$2\mathbb{Z}_K$	132
$3\mathbb{Z}_K$	36
$5\mathbb{Z}_K$	8
$7\mathbb{Z}_K$	8
$11\mathbb{Z}_K$	1
$13\mathbb{Z}_K$	1
$17\mathbb{Z}_K$	2
$19\mathbb{Z}_K$	1
$43\mathbb{Z}_K$	1
$59\mathbb{Z}_K$	0
$193\mathbb{Z}_K$	1
$293\mathbb{Z}_K$	0
$391987\mathbb{Z}_K$	1
$4759427\mathbb{Z}_K$	1
$137679681521\mathbb{Z}_K$	1

The algorithm explained in section 3 provides generators for all these ideals:

$\mathfrak{p}_2 = 3\mathbb{Z}_K + 3^{-12}(4\theta^5 + 4311\theta^4 + 1717038\theta^3 + 2900691\theta^2 + 820125\theta + 2834352)\mathbb{Z}_K$
$\mathfrak{p}_1 = 3\mathbb{Z}_K + 3^{-11}(2\theta^5 + 1815\theta^4 + 586980\theta^3 + 732159\theta^2 + 6582870 + 1535274)\mathbb{Z}_K$
$\mathfrak{p}_1' = 3\mathbb{Z}_K + 3^{-11}(2\theta^5 + 2031\theta^4 + 662796\theta^3 + 1123632\theta^2 + 1071630\theta + 295245)\mathbb{Z}_K$
$\mathfrak{p}_1'' = 3\mathbb{Z}_K + 3^{-11}(2\theta^5 + 2307\theta^4 + 910872\theta^3 + 847584\theta^2 + 398034\theta + 1121931)\mathbb{Z}_K$
$\mathfrak{p}_1''' = 3\mathbb{Z}_K + 3^{-11}(2\theta^5 + 2091\theta^4 + 708696\theta^3 + 646380\theta^2 + 634230\theta + 1121931)\mathbb{Z}_K$

Applying the algorithm described in section 4, we can compute without much effort an element $\alpha \in K$ satisfying

$$\alpha \equiv 1\,(\mathrm{mod}\ \mathfrak{p}_2), \qquad \alpha \equiv \theta\,(\mathrm{mod}\ \mathfrak{p}_1),$$
$$\alpha \equiv \theta^2\,\big(\mathrm{mod}\,(\mathfrak{p}_1')^2\big), \qquad \alpha \equiv \theta^3\,\big(\mathrm{mod}\,(\mathfrak{p}_1'')^3\big), \qquad \alpha \equiv \theta^4\,\big(\mathrm{mod}\,(\mathfrak{p}_1''')^4\big).$$

We may take, for instance:

$$\alpha = 3^{-9}(786086\theta^5 + 445989\theta^4 + 196857\theta^3 + 1159353\theta^2 + 649539\theta + 354294).$$

Following the algorithm for p-adic valuations introduced in section 2, we can check this result computing the valuations of the differences $\alpha - \theta^j$ at the prime ideals dividing 3:

$$v_{\mathfrak{p}_2}(\alpha - 1) = 1,\ v_{\mathfrak{p}_1}(\alpha - \theta) = 7,\ v_{\mathfrak{p}_1'}(\alpha - \theta^2) = 4,\ v_{\mathfrak{p}_1''}(\alpha - \theta^3) = 4,\ v_{\mathfrak{p}_1'''}(\alpha - \theta^4) = 4.$$

All these computations are almost immediate. Even the computation of an S-integral basis takes only 0.06 seconds.

6.3. **Medium degree.** Consider the polynomials:

$$\phi_0 = x + 1, \qquad \phi_1 = \phi_0^2 + 2,$$
$$\phi_{21} = \phi_1^2 + 8, \qquad \phi_{22} = \phi_1^4 + 4\phi_0\phi_1^2 + 32,$$
$$\phi_3 = \phi_{22}^2 + 256\phi_1^2, \quad f = \phi_3\phi_{21} + 2^{30}.$$

Let $K = \mathbb{Q}(\theta)$ be the number field of degree 20 determined by a root $\theta \in \overline{\mathbb{Q}}$ of f. For the prime $p = 2$, the polynomial f has two complete types, with associated Okutsu frames $[\phi_1, \phi_{21}]$ and $[\phi_1, \phi_{22}, \phi_3]$, which give rise to the two prime ideals of $\mathbb{Z}_K$ over 2. The concrete decomposition is $2\mathbb{Z}_K = \mathfrak{p}_1^4\mathfrak{p}_2^8$, where $f(\mathfrak{p}_i/2) = i$, $e(\mathfrak{p}_i/2) = 4i$.

The discriminant of f is

$$\mathrm{Disc}(f) = \quad 2^{268} \cdot 3^2 \cdot 19927 \cdot 43691^2 \cdot 211039 \cdot 6059454913 \cdot$$
$$5129209191541557817 \cdot 25506978885046388417449 \cdot$$
$$1491697955430422823875423179482329686789255 71739.$$

In this example we may compare the performance of the standard Magma functions and that of our package, since Magma can determine the ring of integers of K. Once the factorization of $\mathrm{Disc}(f)$ is known, Magma takes 5.8 seconds to determine $\mathbb{Z}_K$, and 0.08 seconds to find the decomposition of the prime 2 in $\mathbb{Z}_K$. Our package takes 0.3 seconds to see that $\mathrm{Disc}(K) = 2^{-234}\,\mathrm{Disc}(f)$, and during this computation already finds the decomposition of all the primes dividing the discriminant. Our program can also compute a 2-integral basis of K, which is already a global integral basis, in 0.02 seconds.

7. CONCLUSIONS

7.1. **Challenges.** We described routines to perform the basic tasks concerning fractional ideals of a number field, based on the Okutsu-Montes representations of the prime ideals. This avoids the factorization of the discriminant of a defining equation and the construction of the maximal order. These routines are very fast in practice, as long as one deals with fractional ideals whose norm may be factorized.

A big challenge arises: is it possible to combine these techniques with some kind of LLL reduction to test if a fractional ideal is principal?

Also, the generators of the prime ideals constructed in this paper have small height as vectors in $\mathbb{Q}^n$ (the coefficients of its standard representation as a polynomial in θ). This may have some advantages, but in many applications it is preferable to have generators of small norm. A solution to the above mentioned challenge would probably lead to a procedure to find generators of small norm too.

7.2. **Comparison with the standard methods.** Suppose the discriminant of the defining equation of the number field may be factorized. Most of the methods to compute a $\mathbb{Z}$-basis of the maximal order are based on variants of the Round 2 and Round 4 algorithms of Zassenhaus. The procedure of section 5 yields a much faster computation of an integral basis and the discriminant of the field.

Once the maximal order is constructed, we can compare our routines for the manipulation of fractional ideals with the standard ones. The routines based on the OM representations of the prime ideals are faster, mainly because they avoid the usual linear algebra techniques (computation of bases of the ideals, Hermite and Smith normal forms, etc.), which become slow if the degree of the number field grows.

7.3. **Curves over finite fields.** The results of these paper are easily extendable to function fields. If C is a curve over a finite field, there is a natural identification of rational prime divisors of C with prime ideals of the integral closures of certain subrings of the function field [Hes02]. Montes algorithm may be applied as well to construct these prime ideals, and the routines of this paper lead to parallel routines to find the divisor of a function, or to construct a function with zeros and poles of a prescribed order, at a finite number of places.

The results of section 5 may be used to efficiently compute bases of the above mentioned integral closures too. However, the challenge of section 7.1 has its parallel in the geometric situation: we hope that the techniques of this paper may be used to find better routines to compute bases of the Riemann-Roch spaces and to deal with reduced divisors. This would open the door to operate in the group $\text{Pic}^0(C)$ of rational points of the Jacobian of C, for curves with plane models of very large degree.

References

[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.

[FV10] D. Ford, O. Veres, *On the Complexity of the Montes Ideal Factorization Algorithm*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, LNCS, Springer Verlag 2010.

[GMN11] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux, to appear, arXiv:0807.4065v3[math.NT].

[GMN09] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, arXiv: 0902.3428v2[math.NT].

[GMN10] J. Guàrdia, J. Montes, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arithmetica **145(1)** (2010), 83–108.

[GMN10b] J. Guàrdia, J. Montes, E. Nart, *Arithmetic in big number fields: The '+Ideals' package*, arXiv: 1005.4596v1[math.NT].

[GNP11] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lift for polynomials over local fields*, arXiv: 1104.3181v1[math.NT].

[Hen08] K. Hensel, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, Berlin, 1908.

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, Journal of Symbolic Computation **33** (2002), 425–445.

[HN12] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Transactions of the American Mathematical Society, to appear, arXiv:0807.2620v2 [math.NT].

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

[Oku82] K. Okutsu, *Construction of integral basis, I, II*, Proceedings of the Japan Academy, **58**, Ser. A (1982), 47–49, 87–89.

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

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

[Pau10] S. Pauli, *Factoring polynomials over local fields, II*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, LNCS, Springer Verlag 2010.

[Ras10] Rasmussen, J., Personal communication.

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

Departament de Ciències Econòmiques i Empresarials, Facultat de Ciències Socials, Universitat Abat Oliba CEU, Bellesguard 30, E-08022 Barcelona, Catalonia, Spain, Departament de Matemàtica Econòmica, Financera i Actuarial, Facultat d'Economia i Empresa, Univ. de Barcelona, Av. Diagonal 690, E-08034 Barcelona, Catalonia, Spain
    E-mail address: montes3@uao.es, jesus.montes@ub.edu

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