COMPUTATION OF INTEGRAL BASES

JENS-DIETRICH BAUCH

ABSTRACT. Let $A$ be a Dedekind domain, $K$ the fraction field of $A$, and $f \in A[x]$ a monic irreducible separable polynomial. For a given non-zero prime ideal $p$ of $A$ we present in this paper a new method to compute a $p$-integral basis of the extension of $K$ determined by $f$. Our method is based on the use of simple multipliers that can be constructed with the data that occurs along the flow of the Montes Algorithm. Our construction of a $p$-integral basis is significantly faster than the similar approach from [7] and provides in many cases a priori a triangular basis.

INTRODUCTION

Let $A$ be a Dedekind domain, $K$ the fraction field of $A$, and $p$ a non-zero prime ideal of $A$. By $A_p$ we denote the localization of $A$ at $p$. Let $\pi \in p$ be a prime element of $p$.

Denote by $\theta \in K_{\text{sep}}$ a root of a monic irreducible separable polynomial $f \in A[x]$ of degree $n$ and let $L = K(\theta)$ be the finite separable extension of $K$ generated by $\theta$. We denote by $\mathcal{O}$ the integral closure of $A$ in $L$ and by $\mathcal{O}_p$ the integral closure of $A_p$ in $L$. A $p$-integral basis of $\mathcal{O}$ is an $A_p$-basis of $\mathcal{O}_p$ (cf. Definition 3.1).

If $A$ is a PID, then $\mathcal{O}$ is a free $A$-module of rank $n$, and its easy to construct an $A$-basis of $\mathcal{O}$ from the different $p$-integral bases, for prime ideals $p$ of $A$ that divide the discriminant of $f$.

In this work we follow the the approach from [10] and [7] to compute $p$-integral bases. That is, we construct for any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ lying over $p$ a local set $B_{\mathfrak{p}} \subset A[x]$ and a multiplier $z_{\mathfrak{p}} \in L$ such that $\cup_{\mathfrak{p}|p} z_{\mathfrak{p}} B_{\mathfrak{p}}$ is a $p$-integral basis of $\mathcal{O}$, where $z_{\mathfrak{p}} B_{\mathfrak{p}}$ denotes the set we obtain by multiplying all elements in $B_{\mathfrak{p}}$ by $z_{\mathfrak{p}}$. The construction of these local sets and the multipliers is based on the Okutsu-Montes (OM) representations of the prime ideals of $\mathcal{O}$ lying over $p$, provided by the Montes algorithm. In comparison with the existing methods from [10] and [7] our construction of the multipliers is much simpler (and faster) and results in many cases directly in a triangular $p$-integral basis $B$ of $\mathcal{O}$, that is, $B = \{b_0, \ldots, b_{n-1}\}$, where $b_i = g_i(\theta) / \pi^{m_i}$ with $g_i \in A[x]$, monic of degree $i$ and $m_i \in \mathbb{Z}$. Hence the transformation into a basis in HNF becomes especially efficient.

The article is divided in the following sections. In section 1 we summaries the Montes algorithm briefly and introduce the basic ingredients of our algorithm for the computation of a $p$-integral basis. That is, we define types, Okutsu invariants, and a local set $B_{\mathfrak{p}} \subset A[x]$ (cf. Definition 1.7), for a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ lying over $p$. In section 2 we introduce the notion of (semi)-reduced bases, which provides a new criterion of being a $p$-integral bases (Theorem 3.2) and a new method

Key words and phrases. $p$-integral bases, maximal order, Montes algorithm, Dedekind domain.

This research was supported by MTM2009-10359 from the Spanish MEC and by the Netherlands Organisation for Scientific Research (NWO) under grant 613.001.011.
of constructing multipliers \( z_p \), for any prime ideal \( P \) of \( \mathcal{O} \) over \( p \), such that the union of the sets \( \{ z_p \cdot b(\theta)/\pi^{m_b} \mid b \in B_P \} \), for \( P|p \) and certain integers \( m_b \), is a \( p \)-integral basis. If we assume that \( A/p \) is finite with \( q \) elements and \( R \) is a set of representatives of \( A/p \) then we will see that the complexity of the method is dominated by \( O(n^{1+r}\delta \log q + n^{1+r}\delta^{2+r} + n^{2+r}\delta^{1+r}) \) operation in \( R \) (Lemma 3.9), where \( \delta := v_p(\text{Disc} f) \). In section 2 we consider the practical performance of our method in the context of algebraic function fields. We have implemented the method for the case \( A = k[t] \), where \( k \) is a finite field or \( k = \mathbb{Q} \). The package can be downloaded from \url{https://github.com/JensBauch/Integral_Basis}

1. Montes algorithm

We consider the monic separable and irreducible polynomial \( f \in A[x] \). For a non-zero prime ideal \( p \) of \( A \) we denote the induced discrete valuation by \( v_p : A \to \mathbb{Z} \cup \{ \infty \} \) and the completion of \( K \) at \( p \) by \( K_p \). The valuation \( v_p \) extends in an obvious way to \( K_p \). Denote by \( \hat{A}_p \) the valuation ring of \( v_p \) and by \( m_p = p\hat{A}_p \) its maximal ideal.

By the classical theorem of Hensel \([12]\) the prime ideals of \( \mathcal{O} \) lying over \( p \) are in one-to-one correspondence with the monic irreducible factors of \( f \) in \( \hat{A}_p[x] \).

In this section we describe the Montes algorithm, which determines for the input of \( f \) and \( \pi \) a parametrization of the irreducible factors of \( f \) in \( \hat{A}_p[x] \). Let \( \mathfrak{P} \) be a prime ideal of \( \mathcal{O} \) lying over \( p \) and denote by \( f_{\mathfrak{P}} \in \hat{A}_p[x] \) the corresponding irreducible factor of \( f \). Then, the Montes algorithm produces a list of data, a so-called type,

\[ t = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})) \]

which is a representation of the irreducible factor \( f_{\mathfrak{P}} \) and therefore a representation the prime ideal \( \mathfrak{P} \). We call this representation an OM-representation of \( \mathfrak{P} \) (cf. Definition 1.2).

The Montes algorithm can be seen as a factorization algorithm, which detects the factorization of \( f \in \hat{A}_p[x] \), but never computes it. To this purpose, a kind of Hensel’s lemma of higher order is applied \([12]\) Theorem 3.7]. At any level \( i \geq 1 \), besides the fundamental data \( \phi_i \in A[x] \), \( \lambda_i \in \mathbb{Q}_{>0} \), \( \psi_i \in F_i[y] \), where \( F_i \) is a finite extension of \( K_p := A/p \), the type supports:

- \( N_i : \hat{A}_p[x] \to 2^{\mathbb{R}_{\geq 0}} \) a Newton polygon operator,
- \( R_i : \hat{A}_p[x] \to F_i[y] \) a residual polynomial operator,
- \( v_{i-1} : K_p(x) \to \mathbb{Z} \cup \{ \infty \} \) a discrete valuation.

Below we give a brief overview of the Montes algorithm, the OM-representation of prime ideals, and certain applications, which will be useful for further considerations. The results are mainly extracted from \([9]\) and \([10]\). A comprehensive explanation of the Montes algorithm can be found in \([8]\).

1.1. Types. We consider \( v_p : K_p \to \mathbb{Q} \) the by \( p \) induced valuation on \( K_p \) and extend it to a discrete valuation \( v_0 \) on \( K_p(x) \), determined by

\[ (1) \quad v_0 : K_p[x] \to \mathbb{Z} \cup \{ \infty \}, \quad v_0(c_0 + \cdots + c_r x^r) := \min\{v_p(c_i) \mid 0 \leq j \leq r\} \]

Types of order zero

We denote by \( F_0 := k_p = A/p \) and define the 0-th residual polynomial operator

\[ R_0 : \hat{A}_p[x] \to F_0[y], \quad g(x) \mapsto g(y)/\pi^{v_0(g)} \]
where \( \mathbf{a} : \hat{A}_p[y] \to \bar{F}_0[y] \) is the natural reduction map and \( \pi \in \mathfrak{p} \) a uniformizer. A \textit{type of order zero} 

\[ t = (\psi_0), \]

is determined by \( \psi_0(y) \in \bar{F}_0[y] \), a monic irreducible polynomial. A \textit{representative} of \( t \) is any monic polynomial \( \phi_1(x) \in \mathbb{A}[x] \) such that \( R_0(\phi_1) = \psi_0 \).

We consider the polynomial \( f \) in \( \mathbb{A}[x] \). From a factorization of \( R_0(f)(y) = \psi_{1,0}^{n_1} \cdots \psi_{s,0}^{n_s} \) into the product of irreducible monic polynomials \( \psi_{i,0}(y) \in \bar{F}_0[y] \) we deduce types of order zero. Each irreducible factor \( \psi_{i,0}(y) \) singles out one type of order zero. For convenience, we consider one fixed factor, denote it by \( \psi_0 \), and consider a representative \( \phi_1 \in \mathbb{A}[x] \). Let \( m_1 := \deg \phi_1 \).

\textit{Types of order one}:

\textbf{Newton polygon operator.} The Newton polygon of a polynomial \( g(x) \in K_p[x] \) is determined by the pair \((v_0, \phi_1)\). If \( \sum_{s \geq 0} a_s(x)\phi_1(x)^s \) is the \( \phi_1 \)-adic development of \( g(x) \), then

\[ N_1(g) := N_{v_0, \phi_1}(g) \]

is defined to be the lower convex hull of the set of points of the plane with coordinates \((s, v_0(a_s)(x)\phi_1(x)^s)\). However, we only consider the principal part of this polygon, \( N_1^-(g) = N_{v_0, \phi_1}^-(g) \), formed by the sides of negative slopes of \( N_1(g) \). The length \( l(N_1^-(g)) \) of the polygon \( N_1^-(g) \) is, by definition, the abscissa of its right end point. The typical shape of \( N_1^-(g) \) for a monic polynomial \( g \) is as shown below.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig1}
\caption{Newton polygon of \( g \).}
\end{figure}

\textbf{Residual polynomial operator.} We fix \( \mathbb{F}_1 := \bar{F}_0(y)/(\psi_0(y)) \) and we set \( z_0 \) to be the class of \( y \) in \( \mathbb{F}_1 \), so that \( \mathbb{F}_1 = \bar{F}_0[z_0] \). The polygon \( N := N^-_1(g) \) has a residual coefficient \( c_s \) at each integer abscissa, \( \ord_{\phi_1} g \leq s \leq l(N) \), defined as follows:

\[ c_s := \begin{cases} 0, & \text{if } (s, v_0(a_s)) \text{ lies above } N, \\ R_0(a_s)(z_0) \in \mathbb{F}_1, & \text{if } (s, v_0(a_s)) \text{ lies on } N. \end{cases} \]

Denote by \( \text{Slopes}(N) \) the set of slopes of \( N \). Given any \( \lambda \in \mathbb{Q}_{>0} \), we define:

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

The picture below illustrates both possibilities. In this picture \( L_\lambda \) is the line of slope \(-\lambda\) having first contact with \( N \) from below.
In any case, $S_{\lambda}(N)$ is a segment of $\mathbb{R}^2$ with end points having integer coordinates. Any such segment has a degree. If $\lambda = h/e$ with $h$, $e$ positive coprime integers, the degree of $S_{\lambda}(N)$ is defined as:

$$d := d(S_{\lambda}(N)) := l(S_{\lambda}(N))/e,$$

where $l(S_{\lambda}(N))$ is the length of the projection of $S_{\lambda}(N)$ to the horizontal axis. Note that $S_{\lambda}$ splits into $d$ minimal subsegments, whose end points have integer coordinates. Denote $s_0$ and $s_1$ the abscissas of the endpoints of $S_{\lambda}$. Then, the abscissas of the points on $S_{\lambda}$ with integer coordinates are given by $s_0, s_0 + e, \ldots, s_1 = s_0 + de$. We define the residual polynomial of first order of $f(x)$, with respect to $v_0, \phi_1, \lambda$, as:

$$R_{v_0,\phi_1,\lambda}(g)(y) := c_{s_0} + c_{s_0 + e}y + \cdots + c_{s_1}y^d \in \mathbb{F}_1[y].$$

Note that $c_{s_0}c_{s_1} \neq 0$; thus, the degree of $R_{v_0,\phi_1,\lambda}(g)$ is always equal to $d$. Let $h_1, e_1$ be coprime positive integers and consider the positive rational number $\lambda_1 = h_1/e_1$. Let $\psi_1(y) \in \mathbb{F}_1[y]$ be a monic irreducible polynomial with $\psi_1(y) \neq y$. Then,

$$t = (\psi_0; (\phi_1, \lambda_1, \psi_1)),$$

called a type of order one. Such a type supports a residual polynomial operator of the first order $R_1 := R_{v_0,\phi_1,\lambda_1}$. Given any such type, one can compute a representative of $t$; that is, any monic polynomial $\phi_2(x) \in A[x]$ of degree $e_1 \deg \psi_1 \deg \phi_1$, satisfying $R_1(\phi_2)(y) = \psi_1(y)$. This polynomial is necessarily irreducible in $A_p[x]$.

**Discrete valuation.** The triple $(v_0, \phi_1, \lambda_1)$ also determines a discrete valuation on $K_p(x)$ as follows. For $g \in K_p[x]$ nonzero, we consider the intersection point $(0, H)$ of the vertical axis with the line of slope $-\lambda_1$ containing $S_{\lambda_1}(N_1^{-}(g))$. Then, we set $v_1(g(x)) := e_1H$.

**Types of order $r$:**

Now we may start over again with the pair $(v_1, \phi_2)$ and repeat all constructions in order two. The iteration of this procedure leads to the concept of a type of order $r$.

A type of order $r \geq 1$ is a chain:

$$t = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r)),$$

where $\phi_1(x), \ldots, \phi_r(x) \in A[x]$ are monic and irreducible in $A_p[x]$, $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}_{>0}$, and $\psi_0(y) \in \mathbb{F}_0[y], \ldots, \psi_r(y) \in \mathbb{F}_r[y]$ are monic irreducible polynomials over certain fields $\mathbb{F}_0 \subset \cdots \subset \mathbb{F}_r$ 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 $1 \leq i < r$,
• \( \deg \phi_i \mid \deg \phi_{i+1} \).
• \( N_i(\phi_{i+1}) := N_{v_{i-1}}(\phi_{i+1}) \) is one-sided of slope \(-\lambda_i\), and
• \( R_i(\phi_{i+1})(y) := R_{v_{i-1}}(\phi_{i+1})(y) = \psi_i(y) \).

We define \( F_{i+1} := \hat{F}_{i}[\psi_i(y)] \).

(3) \( \psi_r(y) \neq y \). We define \( F_{r+1} := \hat{F}_{r}[\psi_r(y)] \).

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:

- \( \phi_i(x) \), monic polynomial in \( A[x] \), irreducible in \( \hat{A}_p[x] \),
- \( m_i \), \( \deg \phi_i(x) \),
- \( V_i := v_{i-1}(\phi_i) \), nonnegative integer,
- \( \lambda_i = h_i/e_i \), \( h_i, e_i \) positive coprime integers
- \( \psi_i(y) \), monic irreducible polynomial in \( \hat{F}_i[y] \),
- \( f_i \), \( \deg \psi_i(y) \),
- \( z_i \), the class of \( y \) in \( \hat{F}_{i+1} \), so that \( \psi_i(z_i) = 0 \) and \( \hat{F}_{i+1} = \hat{F}_i[z_i] \).

Take \( f_0 := \deg \psi_0 \). Note that

(3) \( m_i = (f_0 f_1 \cdots f_{i-1})(e_1 \cdots e_{i-1}) = e_{i-1} f_{i-1} m_{i-1} \), \( \dim_{\hat{F}_0} \hat{F}_{i+1} = f_0 f_1 \cdots f_i \).

The discrete valuations \( v_0, \ldots, v_r \) on the field \( K_p(x) \) are essential invariants of the type.

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

1. We say that \( t \) divides \( g(x) \), if \( \psi_r(y) \) divides \( R_r(g)(y) \) in \( \hat{F}_r[y] \). We denote \( \ord_t(g) := \ord_{\psi_r}(R_r(g)) \)
2. We say that \( t \) is \( g \)-complete if \( \ord_{\psi_r}(R_r(g)) = 1 \). In this case, \( t \) singles out a monic irreducible factor \( g_t(x) \in \hat{A}_p[x] \) of \( g(x) \), uniquely determined by the property \( R_r(g_t)(y) = \psi_r(y) \). If \( K_t \) is the extension field of \( K_p \) determined by \( g_t(x) \), then

\[
e(K_t/K_p) = e_1 \cdots e_r, \quad f(K_t/K_p) = f_0 f_1 \cdots f_r.
\]

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

\[
\text{Trunc}_i(t) := (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_i, \lambda_i, \psi_i)).
\]

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

A type \( t \) of order 0 is by definition optimal.

1.2. The Montes algorithm. For given \( f(x) \) and an uniformizer \( \pi \) of \( p \), the Montes algorithm determines a family \( t_1, \ldots, t_\kappa \) of \( f \)-complete and optimal types, which correspond uniquely to the irreducible factors of \( f_{t_1}, \ldots, f_{t_\kappa} \) of \( f \) in \( \hat{A}_p[x] \). This correspondence is determined by

1. For all \( 1 \leq i \leq \kappa \), the type \( t_i \) is \( f_{t_i} \)-complete.
2. For all \( j \neq i \), the type \( t_j \) does not divide \( f_{t_i} \).
Initially the algorithm computes the order zero types determined by the irreducible factors of \(f(x)\) modulo \(\mathfrak{p}\), and then enlarges them successively in an adequate way until the whole list of \(f\)-complete optimal types is obtained. We overview the enlargement process along the Montes algorithm. Therefor we consider a type of order \(i-1\) dividing \(f(x)\),

\[
\mathbf{t} := (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}))
\]

and construct a representative \(\phi_i(x)\). The type \(\mathbf{t}\) branches in principle into as many types as pairs \((\lambda, \psi(y))\), where \(-\lambda\) runs on the slopes of \(N_{-i}(f)\) and \(\psi(y)\) runs on the different monic irreducible factors of \(R_{u,-1,\phi,-\lambda}(f)(y) \in F[y]\).

Every output \(\mathbf{t}\) of the Montes algorithm is a type of order \(r+1\), where \(r\) is called the Okutsu depth of the corresponding irreducible factor \(f_k(x)\). The sequence \([\phi_1, \ldots, \phi_r]\) is an Okutsu frame of \(f_k(x)\). Details can be found in \([12]\).

The invariants \(v_i, h_i, e_i, f_i\) at each level \(0 \leq i \leq r\) are canonical (depend only on \(f(x)\)). The \((r+1)\)-level \(\mathbf{t}\) carries only the invariants:

\[
\phi_{r+1}, m_{r+1}, V_{r+1}, \lambda_{r+1} = -h_{r+1}, e_{r+1} = 1, \psi_{r+1}, f_{r+1} = 1.
\]

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

\[
f_{\mathfrak{p}}(x) := f_k(x) \in \hat{A}_\mathfrak{p}[x], \quad \phi_{\mathfrak{p}}(x) := \phi_{r+1}(x) \in A[x], \quad F_{\mathfrak{p}} := F_{r+1},
\]

\[
\psi_{\mathfrak{p}}(y) := \psi_{r+1}(y) \in F_{\mathfrak{p}}[y], \quad n_{\mathfrak{p}} := m_{r+1} = \deg f_{\mathfrak{p}} = \deg \phi_{\mathfrak{p}},
\]

\[
\mathbf{t}_{\mathfrak{p}} := \mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})).
\]

**Definition 1.2.** We say that \(\mathbf{t}_{\mathfrak{p}}\) is an OM representation of \(\mathfrak{p}\).

---

**Algorithm 1 : Montes algorithm**

**Input:** A monic irreducible separable polynomial \(f \in A[x]\) and a uniformizer \(\pi\) of a prime ideal \(\mathfrak{p}\) of \(A\).

**Output:** A family \(\mathbf{t}_1, \ldots, \mathbf{t}_s\) of \(f\)-complete and optimal types, parameterizing the monic irreducible factors \(f_{\mathfrak{p}_1}(x), \ldots, f_{\mathfrak{p}_s}(x)\) of \(f\) in \(\hat{A}_\mathfrak{p}[x]\).

---

1.3. Okutsu approximations. Denote \(\mathfrak{p}\) a prime ideal of \(\mathcal{O}\) over \(\mathfrak{p}\) and let

\[
\mathbf{t}_{\mathfrak{p}} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1}))
\]

be an OM representation of \(\mathfrak{p}\). The polynomial \(\phi_{\mathfrak{p}}(x)\) is an Okutsu approximation to the irreducible factor \(f_{\mathfrak{p}}(x) := f_{\mathfrak{t}_{\mathfrak{p}}}(x)\) [12] Sect. 4.1. The value \(\lambda_{r+1} = h_{r+1}\) is not a canonical invariant of \(f_{\mathfrak{p}}\). It measures how close is \(\phi_{\mathfrak{p}}\) to \(f_{\mathfrak{p}}\); we have \(\phi_{\mathfrak{p}} = f_{\mathfrak{p}}\) if and only if \(h_{r+1} = \infty\).

In order to determine a \(\mathfrak{p}\)-integral basis our algorithm (cf. Algorithm 3) requires the computation of an Okutsu approximation \(\phi_{\mathfrak{p}}\) with sufficiently large value \(\lambda_{r+1} = h_{r+1}\). This can be achieved by applying the single-factor lifting algorithm of [11], which improves the Okutsu approximation to \(f_{\mathfrak{p}}\) with quadratic convergence; that is, doubling the value of \(h_{r+1}\) at each iteration. By [10] p. 744 it holds

\[
\nu_{\mathfrak{p}}(\phi_{\mathfrak{p}}(\theta)) = V_{r+1} + \lambda_{r+1},
\]

where \(V_{r+1} = e_r f_r (e_r V_r + h_r)\) (cf. [1] p. 141) is an invariant of the type \(\mathbf{t}_{\mathfrak{p}}\). By [10] Proposition 4.7 the value \(\nu_{\mathfrak{p}}(\phi_{\mathfrak{p}}(\theta))\) is given by a closed formula in terms of the data attached to the types \(\mathbf{t}_{\mathfrak{p}}, \mathbf{t}_{\mathfrak{p}'}\), for any prime ideal \(\mathfrak{p}'\) of \(\mathcal{O}\) lying over \(\mathfrak{p}\).
different from \( \mathfrak{P} \). Hence, the single-factor lifting algorithm can produce an element \( \phi_{\mathfrak{P}}(\theta) \) in \( L \) with arbitrary large valuation at \( \mathfrak{P} \) and constant value \( v_{\mathfrak{P}'}(\phi_{\mathfrak{P}}(\theta)) \), for \( \mathfrak{P}' \mid \mathfrak{P} \) with \( \mathfrak{P}' \neq \mathfrak{P} \).

**Proposition 1.3.** For any integer \( 0 \leq m < n_{\mathfrak{P}} \), there exist a monic polynomial \( g_m(x) \in \hat{A}_p[x] \) of degree \( m \) such that
\[
\hat{v}(g_m(\theta_{\mathfrak{P}})) \geq \hat{v}(g(\theta_{\mathfrak{P}})) - v_0(g(x)),
\]
for all polynomials \( g(x) \in \hat{A}_p[x] \) having degree \( m \).

Note that the valuation condition from the last proposition do not depend on the choice of the root \( \theta_{\mathfrak{P}} \) of \( f_\mathfrak{P} \).

**Definition 1.4.** We call \( g_m(x) \) a divisor polynomial of degree \( m \) of \( f_\mathfrak{P} \).

**Lemma 1.5.** Let \( 0 \leq i < j < n_{\mathfrak{P}} \) and \( g_i(x), g_j(x) \) two divisor polynomials of \( f_\mathfrak{P} \). Then,
\[
\hat{v}(g_j(\theta_{\mathfrak{P}})) \geq \hat{v}(g_i(\theta_{\mathfrak{P}})).
\]

**Proof.** Since \( x^{j-i}g_i(x) \in \hat{A}_p[x] \) is monic and has degree equal \( j \), the last proposition shows that \( \hat{v}(g_j(\theta_{\mathfrak{P}})) \geq \hat{v}(x^{j-i}g_i(\theta_{\mathfrak{P}})) \geq \hat{v}(g_i(\theta_{\mathfrak{P}})) \). \( \square \)

Let \( t_\mathfrak{P} \) be an OM representation of the prime ideal \( \mathfrak{P} \) lying over \( p \), with \( p \)-polynomials \( \phi_1, \ldots, \phi_r \). We fix \( \phi_0 := x \). Recall that \( m_i = \deg \phi_i \), for \( 0 \leq i \leq r \).

**Theorem 1.6.** For \( 0 < m < n_{\mathfrak{P}} \), we write uniquely
\[
m = \sum_{i=0}^{r} c_i m_i, \quad 0 \leq c_i < \frac{m_i+1}{m_i}.
\]
Then, \( g_m(x) := \prod_{i=0}^{r} \phi_i(x)^{c_i} \) is a divisor polynomial of degree \( m \) of \( f_\mathfrak{P} \).
Definition 1.7. For a prime ideal \( \mathfrak{P} \) of \( \mathcal{O} \) we define
\[
\mathcal{B}_\mathfrak{P} := \{ g_0(x), g_1(x), \ldots, g_{n_\mathfrak{P} - 1}(x) \}
\]
with \( g_0(x) = 1 \).

Note that, for a prime ideal \( \mathfrak{P} \), the set \( \mathcal{B}_\mathfrak{P} \) is a subset of \( A[x] \). The set of all \( g_m(\theta_\mathfrak{P})/\pi^{v(g_m(\theta_\mathfrak{P}))} \), for \( 0 \leq m < n_\mathfrak{P} \), is an \( \hat{A}_p \)-basis of the integral closure of \( \hat{A}_p \) in the finite extension \( K_p(\theta_\mathfrak{P}) \). This basis is called the Okutsu basis of \( \mathfrak{P} \).

2. Reduced bases

In order to describe our algorithm for the computation of a \( p \)-integral basis we use the notion of reduced bases which was introduced by W.M.Schmidt [16] in the context of algebraic function field.

By weaken the concept of reduceness we obtain the notion of semi-reduceness and deduce a new description of being a \( p \)-integral basis (cf. Theorem 3.2). Recall that \( L = K(\theta) \) is the finite extension of \( K \) determined by the monic separable and irreducible polynomial \( f \).

Let \( v_p \) be the discrete valuation determined by the non-zero prime ideal \( p \) and \( \pi \in p \) a uniformizer. We define a \( v_p \)-compatible norm.

Definition 2.1. A \( p \)-norm on \( L \) is a mapping \( w : \rightarrow \mathbb{Q} \cup \{ \infty \} \) that satisfies:

1. \( w(x + y) \geq \min\{w(x), w(y)\} \), for all \( x, y \in L \),
2. \( w(ax) = v(a) + w(x) \), for all \( a \in K \) and \( x \in L \), and
3. \( w(x) = \infty \) if and only if \( x = 0 \).

In other words, a \( p \)-norm is an extension of the valuation \( v_p \) to the finite extension \( L \) having all properties of a valuation except for the good behavior with respect to multiplication.

Definition 2.2. Let \( w \) be a \( p \)-norm. The set \( \mathcal{B} \subset L \) is called \( w \)-reduced if
\[
w\left( \sum_{b \in \mathcal{B}} \lambda_b b \right) = \min_{\mathcal{B}} \{w(\lambda_b b)\}
\]
for all \( \lambda_b \in K \). Or equivalently, \([4]\) holds for all \( \lambda_b \in A \). If we have additionally \( 0 \leq w(b) < 1 \), for all \( b \in \mathcal{B} \), then we call \( \mathcal{B} \) \( w \)-orthonormal.

If we weaken condition \([4]\) to
\[
\left\lfloor w\left( \sum_{b \in \mathcal{B}} \lambda_b b \right) \right\rfloor = \min_{\mathcal{B}} \{\lfloor w(\lambda_b b)\rfloor\},
\]
we call \( \mathcal{B} \) \( w \)-semi-reduced or \( w \)-semi-orthonormal, respectively.

If the \( p \)-norm \( w \) is fixed we just say (semi-) reduced or (semi-) orthonormal, respectively.

Let \( \mathcal{B} = \{b_1, \ldots, b_m\} \) be a \( w \)-reduced set. Then, for any \( a_1, \ldots, a_m \in K^* \), the set \( \{a_1 b_1, \ldots, a_m b_m\} \) is \( w \)-reduced.

Clearly, any (semi-) reduced set \( \mathcal{B} \subset L \) can be normalized to a (semi-) orthonormal set \( \{\pi^m b \mid b \in \mathcal{B}\} \), where \( m_b := -\lfloor w(b) \rfloor \).
2.1. \( \mathfrak{P} \)-reduceness. In this section we introduce the notion of \( \mathfrak{P} \)-reduceness, which can be seen as a “local” concept of reduceness. Let \( \mathfrak{P} \) be a prime ideal of \( \mathcal{O} \) lying over \( \mathfrak{p} \) with ramification index \( e := e(\mathfrak{P}/\mathfrak{p}) \). We denote by \( v_\mathfrak{p} \) the discrete valuation which is induced by \( \mathfrak{P} \). Then, the discrete valuation

\[
w_\mathfrak{p} : L \to \mathbb{Q} \cup \{ \infty \}, \quad w_\mathfrak{p} := \frac{v_\mathfrak{p}(z)}{e}
\]

becomes a \( p \)-norm on \( L \).

Clearly, \( w_\mathfrak{p} \) has a better behavior with respect to multiplications. In fact, we have \( w_\mathfrak{p}(ab) = w_\mathfrak{p}(a) + w_\mathfrak{p}(b) \), for all \( a, b \in L \). Hence, we obtain the following statement.

**Lemma 2.3.** Let \( \mathcal{B} \subset L \) be a \( w_\mathfrak{p} \)-reduced set and \( c \in L^* \). Then, \( c\mathcal{B} \) is \( w_\mathfrak{p} \)-reduced.

In order to derive an adequate reduceness criterion for the concept of “local” reduceness, we are going to consider local fields. Therefore, we consider the completion of \( L \) at the prime ideal \( \mathfrak{P} \) (details can be found in [14]).

Denote by \( L_\mathfrak{P} \) the completion of \( L \) at the prime ideal \( \mathfrak{P} \). Regarding the notation from Subsection 1.4 for \( \mathfrak{P}|\mathfrak{p} \), we can realize the completion \( L_\mathfrak{P} \) by

\[
L_\mathfrak{P} = K_\mathfrak{p}(\theta_\mathfrak{P}),
\]

where \( K_\mathfrak{p} \) is the completion of \( K \) at \( \mathfrak{p} \), and \( \theta_\mathfrak{P} \) denotes a root of \( f_\mathfrak{P} \), the irreducible factor of \( f \) in \( A_0[x] \) corresponding to \( \mathfrak{P} \).

The valuation \( v_\mathfrak{P} \) extends in a unique way to a non-discrete valuation

\[
\hat{v} : K_\mathfrak{p} \to \mathbb{Q}.
\]

Note that \( \hat{v}(\mathfrak{P}(z)) = w_\mathfrak{p}(z) \), for \( z \in L \), where \( \mathfrak{P}(z) \) denotes the injection of \( L \) into \( L_\mathfrak{P} \) determined by \( \theta \mapsto \theta_\mathfrak{P} \). In particular, it holds

\[
\hat{v}(g(\mathfrak{P})) = w_\mathfrak{p}(g(\theta)), \quad \text{for all } g(x) \in A[x].
\]

We denote by \( \hat{\mathcal{O}}_\mathfrak{P} \subset L_\mathfrak{P} \) the valuation ring of the restriction of \( \hat{v} \) to \( L_\mathfrak{P} \) and set \( m_\mathfrak{P} := \{ z \in \hat{\mathcal{O}}_\mathfrak{P} \mid \hat{v}(z) > 0 \} \) the maximal ideal of \( \hat{\mathcal{O}}_\mathfrak{P} \).

The next lemma will play a fundamental role in the subsequent description of the computation of \( \mathfrak{p} \)-integral bases. Any nonzero prime ideal \( \mathfrak{P} \) of \( \mathcal{O} \) determines a set \( \mathcal{B}_\mathfrak{P} \) of divisor polynomials (cf. Definition 1.7). For a subset \( \mathcal{B} \) of \( A[x] \) denote

\[
\mathcal{B}(\theta) := \{ g(\theta) \mid g \in \mathcal{B} \}.
\]

**Lemma 2.4.** The set \( \mathcal{B}_\mathfrak{P}(\theta) \) is \( w_\mathfrak{P} \)-reduced.

**Proof.** Clearly, \( w := w_\mathfrak{p} = e^{-1}v_\mathfrak{p} \) is a discrete valuation, and \( w(g(\theta)) = \hat{v}(g(\mathfrak{P})) \) for all \( g \in A[x] \) by (6). Suppose that \( \mathcal{B}_\mathfrak{P}(\theta) = \{ 1, g_1(\theta), \ldots, g_{n_\mathfrak{P}-1}(\theta) \} \) is not \( w \)-reduced. Let \( \lambda_0, \ldots, \lambda_{n_\mathfrak{P}-1} \in A \) with

\[
w \left( \sum_{i=0}^{n_\mathfrak{P}-1} \lambda_ig_i(\theta) \right) > \min_{0 \leq i < n_\mathfrak{P}} \{ w(\lambda_ig_i(\theta)) \}.
\]

By the strict triangle inequality we only have to consider all summands on the left hand side of (7), which have the same (minimal) \( w \)-value. In other words, we can assume that all summands on the left hand side of (7) have the same norm. According to Lemma 1.5 it holds \( w(g_j(\theta)) \geq w(g_j(\theta)) \), for all \( 0 \leq j < i < n_\mathfrak{P} \). Since all summands in (7) have the same norm, we have \( v_\mathfrak{p}(\lambda_j) \geq v_\mathfrak{p}(\lambda_i) \), for all
0 \leq j < i < n_q. Hence, $g(x) := \lambda_{n_q-1}^{-1} \sum_{i=0}^{n_q-1} \lambda_i g_i(\theta)$ is a monic polynomial of degree $n_q - 1$ with coefficients in $A_q$ satisfying:

$$w(g(\theta)) > \min_{0 \leq i < n_q} \{w(\lambda_{n_q-1}^{-1} \lambda_i g_i(\theta))\} = w(g_{n_q-1}(\theta)),$$

which is a contradiction, as $g_{n_q-1}$ is a divisor polynomial of $f_q$ (cf. Proposition 1.3).

Henceforth we consider the $p$-norm $w := w_p$. We are interested in a criterion to check whether a set $B \subset L$ is $w$-reduced or not. To this end, we consider $\mathfrak{P}$-adic expansions of elements in $L_q$.

Let $\pi_q$ be a prime element of the prime ideal $\mathfrak{P}$ (i.e. $v_p(\pi_q) = 1$), denote by $\mathcal{O}_q$ the valuation ring of $v_p$ and fix a system of representatives $R$ of the residue class field $k_p := \mathcal{O}_q/\mathfrak{P} = \mathcal{O}_q/\mathfrak{m}_q$ of $\mathfrak{P}$. By [14, Satz 4.4] any nonzero element $z$ in $L_q$ has a unique representation $z = \pi_q^n(\lambda_0 + \lambda_1 \pi_q + \lambda_2 \pi_q^2 + \cdots)$, where $\lambda_i \in R$ and $m = v_q(z) \in \mathbb{Z}$. In particular, for any $z \in L^*$ we can write

$$v_p(z) = \sum_{j=v_p(z)}^{\infty} \lambda_j \pi_q^j, \quad \lambda_j \in R.$$

We are interested in a kind of reduction map, which provides a reduceness-criterion. For any $r \in \mathbb{R}$ the sets

$$L_{\geq r} := \{ z \in L \mid w(z) \geq r \} \supset L_{> r} := \{ z \in L \mid w(z) > r \}$$

are $A_p$-submodules of $L$. Their quotient is a $k_p$-vector space $V_r := L_{> r}/L_{\geq r}$, where $k_p := A/p$ is the residue field of $p$. For $r \notin w(L)$ it holds $V_r = 0$, whereas for $r \in w(L)$ there is a non-canonical isomorphism $V_r \cong k_p$, which we are going to describe. Suppose that $r \in w(L)$; that is, $er \in \mathbb{Z}$. Consider the division with remainder

$$er = qe + m, \quad 0 \leq m < e.$$ 

For $z \in L$ with $w(z) \geq r$, a reduction map is given by

$$\text{red}_q(z) : L_{\geq r} \to k_p, \quad z \mapsto z\pi^{-q} \pi^{-m} + \mathfrak{P}.$$ 

Clearly, $\text{red}_q$ is $k_p$-linear and it vanishes on $L_{> r}$. Thus, it induces a concrete isomorphism between $V_r$ and $k_p$.

**Theorem 2.5.** A set $B \subset L$ is $w$-reduced if and only if for any $\rho \in \mathcal{R} := \{ w(b) + \mathbb{Z} \mid b \in B \}$ the vectors in

$$\{ \text{red}_q^w(b) \mid b \in B \text{ with } w(b) + \mathbb{Z} = \rho \}$$

are $k_p$-linearly independent.

**Proof.** For $\rho \in \mathcal{R}$, we set $B_\rho := \{ b \in B \mid w(b) + \mathbb{Z} = \rho \}$. We use the following claim in order to prove the statement.

**Claim:**

The set $B$ is $w$-reduced if and only if $B_\rho$ is $w$-reduced, for all $\rho \in \mathcal{R}$.

By the claim we can assume that all vectors $b \in B$ have the same length $\rho$ modulo $\mathbb{Z}$. Moreover, we may assume that all vectors $b \in B$ have the same norm,
by replacing each \( b \in \mathcal{B} \) by \( \pi^m b \) for an adequate choice of \( m \in \mathbb{Z} \). Let us denote by \( r := w(b) \) this common norm.

Let \( \mathcal{B} = \{b_1, \ldots, b_n\} \). We take \( h_1, \ldots, h_n \in K \) and consider \( z := \sum_{i=1}^n h_i b_i \). Let \( m := \min_{1 \leq i \leq n} \{v_p(h_i)\} \) and denote by \( I \) the set of all indices \( i \) for which \( v_p(h_i) = m \). For \( i \in I \), we write \( h_i = \lambda_i \pi^m + h'_i \) with \( \lambda_i \in k_p \) and \( v_p(h'_i) > v_p(h_i) \). Denote \( z' := \sum_{i \in I} \lambda_i b_i \). Since \( w(a + b) = \min\{w(a), w(b)\} \), for all \( a, b \in L \) with \( w(a) \neq w(b) \), we obtain:

\[
 w(z) = w\left( \sum_{i \in I} h_i b_i \right) = w\left( \sum_{i \in I} \lambda_i \pi^m b_i \right) = m + w(z').
\]

On the other hand,

\[
 \min_{1 \leq i \leq n} \{w(h_i b_i)\} = \min_{i \in I} \{w(h_i b_i)\} = w(h_i b_i) = w(\lambda_i \pi^m b_i) = m + r.
\]

Thus, \( w(z') = r \) is equivalent to

\[
 0 \neq \text{red}_p^{\mathcal{B}}(z') = \sum_{i \in I} \lambda_i \text{red}_p(\mathcal{B}_i).
\]

Hence, \( w(\sum_{i=1}^n h_i b_i) = \min\{w(h_i b_i)\} \), for any \( h_1, \ldots, h_n \in K \) is equivalent to the fact that

\[
 \text{red}_p(\mathcal{B}_1), \ldots, \text{red}_p(\mathcal{B}_n)
\]

are \( k_p \)-linearly independent.

We proof the claim. Since any subset of a reduced family is reduced, we only need to show that \( \mathcal{B} \) is reduced if all \( \mathcal{B}_p \) are reduced.

Let \( I := \{\rho \in \mathbb{R}/\mathbb{Z} \mid \mathcal{B}_p \neq \emptyset\} \). We have \( E := (\mathcal{B})_K = \bigoplus_{\rho \in I} E_\rho \), where \( E_\rho \) is the subspace of \( E \) generated by \( \mathcal{B}_p \). Take \( a_1, \ldots, a_n \in K \) and let \( x = \sum_{i=1}^n a_i b_i \). This element splits as \( x = \sum_{\rho \in I} x_\rho \), where \( x_\rho = \sum_{b_i \in \mathcal{B}_p} a_i b_i \). Since all values \( w(x_\rho) \) are different (because \( w(a_i b_i) \equiv w(b_i) \mod \mathbb{Z} \)), we have \( w(x) = \min_{\rho \in I} \{w(x_\rho)\} \). On the other hand, since all \( \mathcal{B}_p \) are reduced, we have \( w(x_\rho) = \min_{b_i \in \mathcal{B}_p} \{w(a_i b_i)\} \). Thus, \( \mathcal{B} \) is reduced.

\[\square\]

In order to obtain an analogous criterion to test if a subset of \( L \) is \( w \)-semi-reduced we introduce another kind of reduction map.

**Definition 2.6.** For \( r \in \mathbb{R} \) and \( z \in L_{\geq |r|} \), we have \( v_p(z \pi^{-|r|}) = v_p(z) - e |r| \geq 0 \). We write \( v_p(z \pi^{-|r|}) = \lambda_0 + \lambda_1 \pi + \cdots + \lambda_{e-1} \pi^{e-1} + \cdots \), and define

\[
 \text{sred}_p^r(z) := (\lambda_0 \ldots \lambda_{e-1}) \in k_p^e.
\]

Clearly, \( \text{sred}_p^r \) is \( k \)-linear.

**Theorem 2.7.** A set \( \mathcal{B} \subset L \) is \( w \)-semi-reduced if and only if the vectors in

\[
 \{\text{sred}_p^w(b) \mid b \in \mathcal{B}\}
\]

are \( k \)-linearly independent.

**Proof.** The statement can be proven by considering the proof of Theorem 2.5 and replacing \( w \) by \( [w] \) and \( \text{red}_p^{\mathcal{B}} \) by \( \text{sred}_p^{\mathcal{B}} \), respectively. \[\square\]
2.2. \textit{p}-reduceness. The concept of \(\mathfrak{P}\)-reduceness can be generalized to several prime ideals \(\mathfrak{P}_1, \ldots, \mathfrak{P}_s\). Henceforth denote by \(S = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}\) the set of all prime ideals lying over \(p\). The set \(S\) induces a mapping
\[
(8) \quad w_S : L \to \mathbb{Q} \cup \{\infty\}, \quad w_S(z) := \min_{1 \leq i \leq s} \{w_{\mathfrak{P}_i}(z)\}
\]
An immediate consequence of this definition is the following observation.

\textbf{Lemma 2.8.} The map \(w_S\) is a \(p\)-norm on \(F\).

As in the last subsection we define “reduction maps” \(\text{red}\) and \(\text{sred}\) in order to generalize the reduceness-criterion from Theorem 2.5 and the semi-reduceness-criterion of Theorem 2.7 to this situation. Denote for \(1 \leq i \leq s\) the ramification index of \(\mathfrak{P}_i\) and set \(w := w_S\).

\textbf{Definition 2.9.} For \(r \in \mathbb{R}\) and \(z \in L\), we define
\[
\text{red}_S^r(z) := (\text{red}_{\mathfrak{P}_i}^r(z))_{1 \leq i \leq s} \in k_{\mathfrak{P}_1} \times \cdots \times k_{\mathfrak{P}_s}, \quad \text{and}
\]
\[
\text{sred}_S^r(z) := (\text{sred}_{\mathfrak{P}_i}^r(z))_{1 \leq i \leq s} \in k_{\mathfrak{P}_1}^e \times \cdots \times k_{\mathfrak{P}_s}^e.
\]
The following properties are transmitted by the properties of the local mappings \(\text{red}_{\mathfrak{P}_i}\) and \(\text{sred}_{\mathfrak{P}_i}\), for \(1 \leq i \leq s\), respectively.

\textbf{Lemma 2.10.} The mappings \(\text{red}_S^r\) and \(\text{sred}_S^r\) are \(k_p\)-linear and vanish on \(L_{\geq r}\) and \(L_{\geq |r|+1}\), respectively.

Analogously to Theorem 2.5 and Theorem 2.7 one can prove the following statements.

\textbf{Theorem 2.11.} A set \(B \subset L\) is \(w\)-reduced if and only if for any \(\rho \in \mathcal{R} := \{w(b) + \mathbb{Z} | b \in B\}\) the vectors in
\[
\{\text{red}_S^{w(b)}(b) | b \in B \text{ with } w(b) + \mathbb{Z} = \rho\}
\]
are \(k_p\)-linearly independent.

\textbf{Theorem 2.12.} A set \(B \subset L\) is \(w\)-semi-reduced if and only if the vectors in
\[
\{\text{sred}_S^{w_p(b)}(b) | b \in B\}
\]
are \(k_p\)-linearly independent.

We are interested in the relation between \(\mathfrak{P}\)-reduced and \(S\)-reduced. Recall that \(\pi\) is a fixed uniformizer of \(p\).

\textbf{Theorem 2.13.} For \(1 \leq i \leq s\), let \(B_i \subset L\) be \(w_{\mathfrak{P}_i}\)-reduced and \(z_i \in L\) such that, for all \(b \in B_i\),
\[
(9) \quad w_{\mathfrak{P}_i}(z_i b) < w_{\mathfrak{P}_j}(z_i b), \text{ for } j \in \{1, \ldots, s\} \setminus \{i\}.
\]
Then, \(\bigcup_{i=1}^s z_i B_i\) is \(w\)-reduced.

\textit{Proof.} We set \(\text{red}_i^r := \text{red}_{\mathfrak{P}_i}^r\), and \(w_i := w_{\mathfrak{P}_i}\), for \(1 \leq i \leq s\) and \(r \in \mathbb{Q}\). By (9), for \(1 \leq i \leq s\) and \(b \in B_i\), it holds \(w(z_i b) = w_i(z_i b)\) and \(w(z_i b) < w_j(z_i b), \text{ for } j \neq i\). Then, we obtain \(\text{red}_j^{w(z_i b)}(z_i b) = 0 \in k_{\mathfrak{P}_j}\), for all \(j \neq i\), by the definition of \(\text{red}_j^r\). Hence, \(\text{red}_S^{w(z_i b)}(z_i b)\) is given by
\[
(0, \ldots, 0, \text{red}_i^{w(z_i b)}(z_i b), 0, \ldots, 0).
\]
By Lemma 2.3, the sets $z_i B_i$ are $w_i$-reduced, for $1 \leq i \leq s$, and therefore $\{ \text{red}^w_{S}(z_i, b) \mid b \in B_i \}$ are $k_p$-linearly independent by Theorem 2.5. Hence, the set $\bigcup_{i=1}^{s} z_i B_i$ is $w$-reduced by Theorem 2.11.

**Theorem 2.14.** For $1 \leq i \leq s$, let $B_i \subset L$ be $w_p$-reduced and $z_i \in L$ such that for all $b \in B_i$

$$
(1) \quad [w_p(z_i, b)] \leq [w_p(z_j, b)] \quad \text{for} \quad 1 \leq i < j \leq s
$$

$$
(2) \quad [w_p(z_i, b)] < [w_p(z_i, b)] \quad \text{for} \quad 1 \leq l < i \leq s.
$$

Then, $\bigcup_{i=1}^{s} z_i B_i$ is $w$-semi-reduced.

**Proof.** We set $w_i := w_p$ and $\text{red}_i := \text{red}_p^{w_i}$, for $1 \leq i \leq s$ and $r \in \mathbb{Q}$. By the hypothesis, for $1 \leq l < i \leq s$ and $b \in B_i$, we have $[w(z_i, b)] = [w_i(z_i, b)] < [w_i(z_i, b)]$; hence, $\text{red}^w_{S}(z_i, b) = 0 \in k_p^{e_i}$. In particular, with $r_i := w_i(z_i, b)$ we deduce, for $1 \leq i \leq s$

$$(10) \quad \text{red}_i^{w_i}(z_i, b) = (0, \ldots, 0, \text{red}_i^{w_i}(z_i, b), \ast, \ldots, \ast),$$

with some vectors $* \in k_p^{e_i}$, for $j > i$. Since $[w(z_i, b)] = [w_i(z_i, b)]$, we have $\text{red}_i^w(z_i, b) = \text{red}_i^w(z_i, b)$, for $b \in B_i$. According to Lemma 2.3, the sets $z_i B_i$ are $w_i$-reduced, and particularly $w_i$-semi-reduced. Then, by Theorem 2.7, the family $\{ \text{red}_i^w(z_i, b) \mid b \in B_i \}$ is $k_p$-linearly independent. By (10), the family $\bigcup_{1 \leq i \leq s} \{ \text{red}_i^w(z_i, b) \mid b \in B_i \}$ is $k_p$-linearly independent. Thus, by Theorem 2.12, $\bigcup_{1 \leq i \leq s} z_i B_i$ is $w$-semi-reduced.

$$\square$$

3. Computation of $p$-integral bases

Let $\theta$ be a root of a monic irreducible separable polynomial $f \in A[x]$ of degree $n$ and let $L = K(\theta)$ be the finite separable extension of $K$ generated by $\theta$. We fix a non-zero prime ideal $p$ of $A$ and denote by $A_p$ the localization of $A$ at $p$ and set $k_p = A/p$. We denote by $O$ the integral closure of $A$ in $L$. The goal of this section is to describe an algorithm, which computes a (reduced) $p$-integral basis of $O$.

**Lemma-Definition 3.1.** Let $b_1, \ldots, b_n \in O$ be $A$-linearly independent elements and denote by $M = \langle b_1, \ldots, b_n \rangle$ the $A$-submodule of $O$ that they generate. The following conditions are equivalent:

1. $b_1 \otimes 1, \ldots, b_n \otimes 1$ are an $A_p$-basis of $O \otimes_A A_p$.
2. $b_1 \otimes 1, \ldots, b_n \otimes 1$ are a $k_p$-basis of $O \otimes_A k_p$.

If these conditions are satisfied we call $(b_1, \ldots, b_n)$ a $p$-integral basis of $O$.

**Proof.** The three conditions are equivalent by Nakayama’s lemma. \(\square\)

Denote by $S$ the set of all prime ideals of $O$ lying over $p$ and consider the $p$-norm $w_S$ defined in (8). In [7] it was shown that a $w_S$-orthonormal set of $n$ elements in $L$ determines a $p$-integral basis. The next theorem is an improvement of this result and a new description of being a $p$-integral basis.

**Theorem 3.2.** Let $B$ be subset of $L$ with $n$ elements. Then, $B$ is a $p$-integral basis of $O$ if and only if $B$ is $w_S$-semi-orthonormal.
Proof: We set \( w := w_\mathcal{O} \). Suppose that \( \mathcal{B} \) is \( w \)-semi-orthonormal. An easy computation shows that \( w(z) \geq 0 \) if and only if \( z \in \mathcal{O} \); hence, the set \( \mathcal{B} \) is a subset of \( \mathcal{O} \). According to Lemma-Definition 3.1, it is sufficient to show that \( \mathcal{B} \) is a set of \( k_p \)-linearly independent vectors in order to show that \( \mathcal{B} \) is a \( p \)-integral basis of \( \mathcal{O} \).

Assume \( \sum_{b \in B} \lambda_b b \in \mathcal{O} \otimes_A A_p \) with \( \lambda_b \in A_p \). Then, \( w(\sum_{b \in B} \lambda_b b) \geq 1 \). Since \( \mathcal{B} \) is \( w \)-semi-orthonormal, we deduce \( w(\lambda_b b) \geq 1 \), for all \( b \in \mathcal{B} \), and therefore \( v_p(\lambda_b) \geq 1 \), for all \( b \in \mathcal{B} \). That is, \( \lambda_b \in pA_p \), for \( b \in \mathcal{B} \).

For the other direction we use the following claim.

Claim: Let \( \mathcal{B}' = (b'_1, \ldots, b'_n) \) be a \( w \)-semi-orthonormal basis, \( T \in \text{GL}_n(A_p) \), and \( \mathcal{B} = (b_1, \ldots, b_n) \) determined by \( T(b'_1, \ldots, b'_n)^{\text{tr}} = (b_1, \ldots, b_n)^{\text{tr}} \). Then, \( \mathcal{B} \) is a \( w \)-semi-orthonormal basis.

After the claim, the statement of the theorem yields immediately. Let \( \mathcal{B} \) be any \( p \)-integral basis of \( \mathcal{O} \) and \( \mathcal{B}' \) a \( w \)-semi-orthonormal subset of \( \mathcal{O} \) with \( n \) elements. As shown above, the family \( \mathcal{B}' \) is also a \( p \)-integral basis of \( \mathcal{O} \); hence, the transition matrix from \( \mathcal{B} \) to \( \mathcal{B}' \) belongs to \( \text{GL}_n(A_p) \). Thus, the claim states that \( \mathcal{B} \) is \( w \)-semi-orthonormal too.

In order to prove the claim we consider [2] Lemma 2.8.8. Analogously to its proof one can show that a matrix \( T = (t_{i,j}) \in K^{n \times n} \) belongs to \( \text{GL}_n(A_p) \) if and only if

\[
\min_{1 \leq i \leq n} \left\{ v_p \left( \sum_{j=1}^n t_{j,i} a_j \right) \right\} = \min_{1 \leq i \leq n} \left\{ v_p(a_i) \right\},
\]

for all \( a_1, \ldots, a_n \in K \). Let \( a_1, \ldots, a_n \in K \) and set \( a'_i := \sum_{j=1}^n t_{j,i} a_j \), for \( 1 \leq i \leq n \). Since \( \mathcal{B}' \) is \( w \)-semi-orthonormal and by (11) we obtain

\[
\left\lfloor w \left( \sum_{i=1}^n a_i b_i \right) \right\rfloor = \left\lfloor w \left( \sum_{i=1}^n a'_i b'_i \right) \right\rfloor = \min_{1 \leq i \leq n} \left\{ v_p(a'_i) \right\} = \min_{1 \leq i \leq n} \left\{ v_p(a_i) \right\}.
\]

Thus, \( \mathcal{B} \) is \( w \)-semi-orthonormal.

\[\square\]

3.1. The algorithm. Let \( \mathcal{S} = \{ \mathcal{P}_1, \ldots, \mathcal{P}_s \} \) be the set of all prime ideals of \( \mathcal{O} \) lying over \( \mathfrak{p} \). For \( 1 \leq j \leq s \), we denote by \( \Phi_j := \phi_{\mathcal{P}_j} \) an Okutsu approximation of the \( p \)-adic irreducible factor \( f_{\mathcal{P}_j} \) of \( f \) in \( A_\mathfrak{p}[[x]] \) (cf. subsection 1.3) and let \( \mathcal{B}_j := \mathcal{B}_{\mathcal{P}_j}(\theta) \), where \( \mathcal{B}_{\mathcal{P}_j} \) is defined in Definition 1.7.

In [10] are given closed formulas for the values \( v_{\mathcal{P}_j}(\Phi_i(\theta)) \) for \( j \neq i \) in terms of data collected by the Montes algorithm. We recall that when we improve \( \Phi_i \), the value \( v_{\mathcal{P}_j}(\Phi_i(\theta)) \) increases, but the values \( v_{\mathcal{P}_j}(\Phi_i(\theta)) \) for \( j \neq i \) remain constant.

We set \( n_{\mathcal{P}_j} = \deg f_{\mathcal{P}_j} \), for \( 1 \leq j \leq s \). Note that \( n_{\mathcal{P}_j} = e(\mathcal{P}_j/p)f(\mathcal{P}_j/p) \), where \( f(\mathcal{P}_j/p) \) denotes the residue degree of \( \mathcal{P}_j \) over \( \mathfrak{p} \). By Lemma 2.4 the set \( \mathcal{B}_j \) is \( w_{\mathcal{P}_j} \)-reduced. By definition it holds \( \# \mathcal{B}_j = \deg f_{\mathcal{P}_j} \), for \( 1 \leq j \leq s \); hence, \( \# \bigcup_{\mathcal{P}_j} \mathcal{B}_j = \sum_{\mathcal{P}_j} \deg f_{\mathcal{P}_j} = \deg f = n \). Denote by \( \pi \) a uniformizer of \( \mathfrak{p} \).

By applying Theorems 2.13, 2.14 and 3.2 we obtain the next two statements.
Theorem 3.3. For $1 \leq \kappa \leq s$, we set

$$z_\kappa := \prod_{j=1, j \neq \kappa}^s \Phi_j^\epsilon_j(\theta),$$

where $\epsilon_j \in \{0, 1\}$ and the Okutsu approximation $\Phi_j$ are chosen in such a way that, for all $b \in \mathcal{B}_\kappa$,

1. $|w_{\mathcal{B}_\kappa}(z_\kappa b)| \leq |w_{\mathcal{B}_\kappa}(z_\kappa)|$, for $1 \leq \kappa < i \leq s$,
2. $|w_{\mathcal{B}_\kappa}(z_\kappa b)| < |w_{\mathcal{B}_\kappa}(z_\kappa)|$, for $1 \leq i < \kappa \leq s$.

Then, $\{b_1, \ldots, b_n\} := \bigcup_{\kappa=1}^s z_\kappa \mathcal{B}_\kappa$ is $w_S$-semi-reduced. In particular, the family

$$\frac{b_i}{\pi^{\lfloor w_S(b_i) \rfloor}}, \quad 1 \leq i \leq n,$

is a $p$-integral basis of $\mathcal{O}$.

Theorem 3.4. If we replace in Theorem 3.3 item 1 and 2 by the condition $w_{\mathcal{B}_\kappa}(z_\kappa b) < w_{\mathcal{B}_\kappa}(z_\kappa)$, for $i \in \{1, \ldots, s\} \setminus \{\kappa\}$,

then $(b_i/\pi^{\lfloor w_S(b_i) \rfloor})_{1 \leq i \leq n}$ is a $w_S$-orthonormal basis of $\mathcal{O}$.

The idea of using multipliers to construct integral bases goes back to Ore (1925). In [7] a similar way of determining adequate multipliers is presented. An advantage of our choice is that in practice the multipliers $z_\kappa$ are simple. That is, many exponents $\epsilon_j$ in (12) can be chosen to be zero. Often we may take

$$z_\kappa = \prod_{j<\kappa} \Phi_j(\theta), \quad 1 \leq \kappa \leq s.$$

Since $\deg \Phi_j = n_{\mathcal{B}_j}$ and $\mathcal{B}_{\mathcal{B}_j} = \{g_0(\theta), \ldots, g_{n_{\mathcal{B}_j}}(\theta)\}$ with $g_m \in A[x]$ monic of degree $m$ for $1 \leq j \leq s$, the degree of $\prod_{j<\kappa} \Phi_j(x)g_m$ is equal $\sum_{j<\kappa} n_{\mathcal{B}_j} + m$, and the basis $\mathcal{B}$ is in that particular case triangular. Even though, the multipliers $z_\kappa$ are not always that simple, our choice leads in many cases to a partly triangular basis $\mathcal{B}$. Hence, the resulting $p$-integral basis $(b_i/\pi^{\lfloor w_S(b_i) \rfloor})_{1 \leq i \leq n}$ can be transformed quickly into a triangular or Hermite basis.

Algorithm 3: Computation of a $p$-integral basis

Input: Monic separable and irreducible polynomial $f \in A[x]$, an uniformizer $\pi$ of a non-zero prime ideal $p$ of $A$, and a boolean variable red.

Output: A $p$-integral basis of $\mathcal{O}$, which is additionally $w_S$-orthonormal if $\text{red} = \text{TRUE}$.

1. Algorithm 1($f, \pi$)
2. for $\mathcal{B} || p$ do
3. Determine $\mathcal{B}_i = \mathcal{B}_{\mathcal{B}_i}(\theta)$ with $\mathcal{B}_{\mathcal{B}_i}$ as in Definition 1.7
4. Determine $\Phi_i$ by Algorithm 2 satisfying, if $\text{red} = \text{FALSE}$, the conditions of Theorem 3.3 and else the conditions of Theorem 3.4
5. end for
6. $\{b_1, \ldots, b_n\} \leftarrow \bigcup_{\kappa=1}^s z_\kappa \mathcal{B}_\kappa$
7. return $(b_i/\pi^{\lfloor w_S(b_i) \rfloor})_{1 \leq i \leq n}$

In order to determine the exponents $\epsilon_j$ and the precision of the approximations $\Phi_j$ so that $z_\kappa$ satisfies the conditions of Theorem 3.3 or Theorem 3.4, we have to
compute the values $w_{\Phi_i}(z_i b)$, for all $1 \leq \kappa, j \leq s$ and $b \in B_\kappa$. That is, we need to determine the values $v_{\Phi_i}((\Phi_j(\theta)))$ and $v_{\Phi_i}(b)$, for $1 \leq \kappa, j \leq s$ and all $b \in B_\kappa$. In [10 Proposition 4.7] concrete formulas can be found, which only depend on the data computed along Algorithm 1. Hence, these values can be computed as a by-product at cost zero. Thus, the cost of the determination of the integers $c_j$ and the precision of the approximations $\Phi_j$ can be neglected.

In order to determine an integral basis of $O$ (i.e., an $A$-basis), we may compute $p$-integral bases $B_p$ of $O$ for any prime ideal $p$ with $v_p(Disc f) > 1$ and transform it into a triangular basis. Then by an easy application of the CRT one can combine the "local" bases $B_p$ to a global one.

3.2. Complexity. For the subsequent complexity analysis we define $\delta := v_p(Disc f)$ the $p$-valuation of the discriminant of $f$. The following steps dominate the runtime of Algorithm 3:

(1) Montes algorithm
(2) Computation of local sets $B_i = B_{\Phi_i}(\theta)$, for $1 \leq i \leq s$
(3) Computation of multiplier $z_i$, for $1 \leq i \leq s$:
   (a) Determining $\Phi_i$ with necessary precision
   (b) Computing $z_p := \prod_{1 \leq i \leq s} \Phi_i^{c_i}$
(4) Computing $\bigcup_{1 \leq i \leq s} z_i B_i$

We admit fast multiplication techniques of Schönhage-Strassen [7]. Let $R$ be a ring and let $g_1, g_2 \in R[x]$ be two polynomials, whose degrees are bounded by $d_1$ and $d_2$, respectively. Then, the multiplication $g_1 \cdot g_2$ needs at most $O(max\{d_1, d_2\})^{1+\epsilon}$ operations in $R$. We may consider the elements in $A$ to be finite $p$-adic developments whose length is at most $\delta + 1$ by [11 Thm. 3.14]. We fix a system of representatives $R$ of $A/p$ and call an operation in $A$ $p$-small if it involves two elements belonging to $R$. Hence, any multiplication in $A$ can be realized with at most $O(\delta^{1+\epsilon})$ $p$-small operations. We assume that the residue field $A/p$ is finite with $q$ elements.

1. Montes algorithm:
   The Montes algorithm has a cost of $O\left( n^{2+\epsilon} + n^{1+\epsilon} \delta \log q + n^{1+\epsilon} \delta^{2+\epsilon} \right)$ $p$-small operations [11 Thm. 5.15].

2. Local sets:
   We begin with analyzing the cost of determining $B_i = B_{\Phi_i}(\theta)$ for one $i \in \{1, \ldots, s\}$ as defined in Definition 3.7. We fix $\Psi = \Psi_i$ and consider $\Psi_m(x) := \prod_{i=0}^{r-1} \phi_i(x)^{c_i}$ with $m = \sum_{i=0}^{r} c_i m_i$, $0 \leq c_i < m_{i+1}/m_i$ for $0 < m < n_p$. Let $d_i := m_{i+1}/m_i - 1$ and define $g(x) := \prod_{i=0}^{r} \phi_i(x)^{d_i}$. Then, $g_m(x) g(x)$ for $0 < m < n_p$. Thus, the cost of computing $g$ by brute force is dominating the complexity of the computation of $g_0, \ldots, g_{n_p-1}$. We count for any power $\phi_i^k$ in $g_1$ multiplications in $A[x]$. Since $g$ is the product of $r$ powers we can determine $g$ by $\sum_{i=0}^{r} d_i + r + 1 < \sum_{i=0}^{r} m_{i+1}/m_i$ multiplications in $A[x]$. Since $t$ is optimal, it holds $2m_i \leq m_{i+1}$, for $1 \leq i < r$ (cf. Definition 3.7 and (3)) and we get

$$\sum_{i=0}^{r} \frac{m_{i+1}}{m_i} = 1 + \sum_{i=1}^{r-1} \frac{m_{i+1}}{m_i} + \frac{m_{r+1}}{m_r} \leq 1 + \frac{m_r}{2^{r-1}} + \frac{m_r}{2^{r-2}} + \cdots + \frac{m_r}{2} + m_{r+1} = O(m_{r+1}).$$
Since \( m_r + 1 = n_{p_I} \), we can determine \( B_{p_I} \) with at most \( O(n_{p_I}) \) multiplications in \( A[\theta] \). Then, the cost of the computation of \( B_{p_I} \), for \( 1 \leq j \leq s \), is \( O(\sum_{i=1}^{s} n_{p_I}) = O(n) \) multiplications in \( A[\theta] \). Since each multiplication in \( A[\theta] \) has a cost of \( O(n^{1+\varepsilon}) \) multiplications in \( A \), the total cost of these \( O(n) \) multiplications in \( A[\theta] \) is \( O \left( n^{2+\varepsilon} \delta^{1+\varepsilon} \right) \) \( p \)-small operations.

**Okutsu approximation:**

In order to compute the multipliers \( z_\kappa \), defined in \( (12) \), we have to improve the Okutsu approximations \( \Phi_i \) to an adequate precision. According to [1, Theorem 5.16], the cost of the computation of an Okutsu approximation \( \Phi_i \) with precision \( \nu \) at \( \mathcal{P}_i \) (that is, \( w_{\mathcal{P}_i}(\Phi_i(\theta)) \geq \nu \)) is given by

\[
O(n_{\mathcal{P}_i} n^{1+\varepsilon} + n\delta^{1+\varepsilon})
\]

\( p \)-small operations.

The following technical lemmas provide concrete bounds for the precision \( \nu \) of the Okutsu approximation \( \Phi_i \), for \( 1 \leq i \leq s \), which is sufficient in order to determine a \( p \)-integral basis with Algorithm [3].

In the following observation we assume that the multipliers \( z_\kappa \) are given by

\[
z_\kappa = \prod_{j=1}^{s} \Phi_j^\epsilon_j(\theta), \quad \text{all } \epsilon_j = 1.
\]

Although in practice many of the exponents \( \epsilon_j \) can be chosen to be zero, for the complexity estimation we consider the worst case \( \epsilon_j = 1 \), for \( j \neq \kappa \).

**Lemma 3.5.** For \( 1 \leq i \leq s \), let \( \mathcal{B}_i = \{b_{i,j} \mid 0 \leq j \leq n_{\mathcal{P}_i} - 1\} \) and \( \Phi_i \) such that

\[
w_{\mathcal{P}_i}(\Phi_i(\theta)) \geq \max \left\{ \max_{1 \leq \kappa < i < s} \{H_{i,\kappa}\}, \max_{1 \leq \kappa < s} \{H_{i,\kappa}\} + 1 \right\},
\]

where

\[
H_{i,\kappa} := \max_{0 \leq l < n_{\mathcal{P}_i}} \left\{ w_{\mathcal{P}_i} \left( b_{\kappa,l} \prod_{j \neq \kappa}^{s} \Phi_j^\epsilon_j(\theta) \right) - w_{\mathcal{P}_i} \left( b_{\kappa,l} \prod_{j \neq \kappa}^{s} \Phi_j(\theta) \right) \right\}.
\]

Then, \( \{b_1, \ldots, b_n\} = \bigcup_{\kappa=1}^{s} z_\kappa \mathcal{B}_\kappa \), with \( z_\kappa := \Phi_1(\theta) \cdots \Phi_{\kappa-1}(\theta) \cdot \Phi_{\kappa+1}(\theta) \cdots \Phi_s(\theta) \) is \( w_{\mathcal{P}} \)-semi-reduced. In particular, the family

\[
\frac{b_i}{\pi[\mathcal{P}(b_i)]}, \quad 1 \leq i \leq n
\]

is a \( p \)-integral basis of \( I \).

**Proof.** We show that the conditions on the \( \Phi_i \) can be translated to the following statement: For \( 1 \leq \kappa \leq s \) and for \( 0 \leq l < n_{\mathcal{P}_\kappa} \) it holds

1. \( w_{\mathcal{P}_\kappa}(z_{\kappa} b_{\kappa,l}) \leq w_{\mathcal{P}_\kappa}(z_{\kappa} b_{\kappa,l}) \) for \( 1 \leq \kappa < i \leq s \) and
2. \( w_{\mathcal{P}_\kappa}(z_{\kappa} b_{\kappa,l}) \leq w_{\mathcal{P}_\kappa}(z_{\kappa} b_{\kappa,l}) \) for \( 1 \leq i < \kappa \leq s \).

Then, the statement of the lemma follows from Theorem [3,3].
The inequality \( w_{\Phi_i}(\Phi_i(\theta)) \geq H_{i,\kappa} \), for \( \kappa < i \), implies that, for \( 0 \leq l < n_{\Phi_\kappa} \),
\[
  w_{\Phi_i}(\Phi_i(\theta)) \geq w_{\Phi_\kappa}\left(b_{\kappa, l} \prod_{j=1, j \neq \kappa}^s \Phi_j(\theta)\right) - w_{\Phi_i}\left(b_{\kappa, l} \prod_{j=1, j \neq \kappa}^s \Phi_j(\theta)\right) \\
\Longleftrightarrow w_{\Phi_i}\left(b_{\kappa, l} \prod_{j=1, j \neq \kappa}^s \Phi_j(\theta)\right) \geq w_{\Phi_\kappa}\left(b_{\kappa, l} \prod_{j=1, j \neq \kappa}^s \Phi_j(\theta)\right),
\]
which proves the first item. Analogously, the inequality \( w_{\Phi_i}(\Phi_i(\theta)) \geq H_{i,\kappa} + 1 \), for \( \kappa > i \), implies the second item. \( \square \)

Analogously to the last proof one can show with Theorem 3.4 the following statement.

**Corollary 3.6.** If we require
\[
w_{\Phi_i}(\Phi_i(\theta)) > \max_{1 \leq \kappa \leq s} \{H_{i,\kappa} \mid \kappa \neq i\},
\]
for \( 1 \leq i \leq s \), instead of \( [13] \), then the \( p \)-integral basis from the last lemma is \( w_S \)-orthonormal.

By Lemma 3.5, we deduce a lower bound for the precision of the approximations \( \Phi_i \), for \( 1 \leq i \leq s \).

**Lemma 3.7.** For \( i \neq \kappa \) and \( 1 \leq i, \kappa \leq s \) we have
\[
H_{i,\kappa} = O(\delta).
\]

**Proof.** We keep the notation from Lemma 3.5. For \( 1 \leq \kappa, j \leq s \) and \( 0 \leq l < n_{\Phi_\kappa} \) it holds
\[
  w_{\Phi_\kappa}(b_{\kappa, l} z_\kappa) - w_{\Phi_i}(b_{\kappa, l} \prod_{j=1, j \neq \kappa}^s \Phi_j(\theta)) \leq w_{\Phi_\kappa}(b_{\kappa, l} z_\kappa),
\]
since \( b_{\kappa, l}, \Phi_i(\theta) \in O \). We estimate \( w_{\Phi_\kappa}(b_{\kappa, l} z_\kappa) \) in order to determine a bound for \( H_{i,\kappa} \). By definition, the elements \( b_{\kappa, l} \in B_\kappa \) are given by \( b_{\kappa, l} = g_{\kappa, l}(\theta) \) with \( g_{\kappa, l}(x) \in A[x] \) monic of degree \( m < n_{\Phi_\kappa} \). In [1] Proposition 1.3 it is shown that all monic polynomials \( g \in A[x] \) of degree less than \( n_{\Phi_\kappa} \) satisfy \( v_{\Phi_\kappa}(g(\theta))/e(\Phi_\kappa/p) \leq \mu \) for a certain constant \( \mu \) which satisfies \( \mu \leq \delta/n_{\Phi_\kappa} \). Hence, \( w_{\Phi_\kappa}(b_{\kappa, l}) \leq \delta/n_{\Phi_\kappa} \), for all \( 0 \leq l < n_{\Phi_\kappa} \).

We consider \( w_{\Phi_\kappa}(z_\kappa) = \sum_{j=1, j \neq \kappa}^s v_{\Phi_\kappa}(\Phi_j(\theta))/e(\Phi_\kappa/p) \). Let \( f_1, \ldots, f_s \) be the irreducible factors of the polynomial \( f \) in \( \hat{A}_p[x] \). As in [3], we identify the completion of \( L \) at the prime ideal \( \Phi_\kappa \) with \( K_p(\theta_{\Phi_\kappa}) \), for \( 1 \leq \kappa \leq s \), where \( \theta_{\Phi_\kappa} \) denotes a root of the irreducible factor \( f_\kappa \). Let \( \hat{v} \) be the extension of \( v_p \) to the algebraic closure of \( K_p \).

**Claim:** It holds \( w_{\Phi_\kappa}(\Phi_j(\theta)) = \hat{v}(\Phi_j(\theta_{\Phi_\kappa})) = \hat{v}(\text{Res}(f_{\Phi_j}, f_{\Phi_\kappa}))/\deg f_{\Phi_\kappa} \).

After the claim, the statement of the lemma follows immediately. In fact, since
\[
\delta = \sum_{i=1}^s v_p(\text{Disc}(f_{\Phi_i})) + 2\sum_{1 \leq j < \kappa \leq s} v_p(\text{Res}(f_{\Phi_j}, f_{\Phi_\kappa}))
\]
we deduce $w_{\Phi_{s}}(z_{s}) \leq \delta$. Together with the previous estimations, we obtain $H_{i,\kappa} = O(\delta)$.

In order to prove the claim we consider $Z$ the set of roots of $f_{\Phi_{s}}$. Since $f_{\Phi_{s}}, f_{\Phi_{j}} \in \hat{A}[x]$ are irreducible, $\hat{v}$ is constant on $f_{\Phi_{s}}(Z)$. As

$$\hat{v}(\text{Res}(f_{\Phi_{j}}, f_{\Phi_{s}})) = \hat{v}\left(\prod_{\alpha \in Z} f_{\Phi_{j}}(\alpha)\right),$$

we obtain $\hat{v}(\text{Res}(f_{\Phi_{j}}, f_{\Phi_{s}})) = \deg f_{\Phi_{j}} \cdot \hat{v}(f_{\Phi_{s}}(\theta_{\Phi_{s}}))$. In [10] Prop. 7.4 there is a closed formula for $\hat{v}(\Phi_{j}(\theta_{\Phi_{s}}))$ which is valid for any Okutsu approximation $\Phi_{j}$ of $f_{\Phi_{j}}$; in particular, $\hat{v}(\Phi_{j}(\theta_{\Phi_{s}})) = \hat{v}(f_{\Phi_{j}}(\theta_{\Phi_{s}}))$. This ends the proof of the claim.

According to the last lemma, we compute in Algorithm 3 approximations $\Phi_{i}$ with a precision $\nu = O(\delta)$ at cost of

$$O(nn_{b} \delta^{1+\epsilon})$$
p-small operations. In the worst case we have to determine all approximations $\Phi_{i}$ with that precision. As $\sum_{i=1}^{s} n_{\Phi_{i}} = n$, the cost of computing the adequate approximations can be estimated by $O(n^{2}\delta^{1+\epsilon})$ p-small operations.

**3b Multiplier:**

We analyze the cost of the computation of the multipliers $z_{\kappa}$, for $1 \leq \kappa \leq s$. As mentioned before, the worst case occurs if any multiplier $z_{\kappa}$ is given by

$$z_{\kappa} = \prod_{j=1}^{s} \Phi_{j}(\theta).$$

**Lemma 3.8.** Let $s \geq 2$. The multipliers $z_{1}, \ldots, z_{s}$ can be determined by $2(s-3)+s$ multiplications in $A[\theta]$.

**Proof.** Initially we compute the products

$$\Phi_{1}\Phi_{2},\Phi_{1}\Phi_{2}\Phi_{3}, \ldots, \Phi_{1}\cdots\Phi_{s-2} \quad \text{and}$$

$$\Phi_{s-1}\Phi_{s},\Phi_{s-2}\Phi_{s-1}\Phi_{s}, \ldots, \Phi_{3}\cdots\Phi_{s}.$$ 

This can be realized by $2(s-3)$ multiplications. Every $z_{i}$ can be written as a product of two factors, where each of them belongs to list (14), list (15), or is one of the $\Phi_{i}$. Hence, to determine the multipliers $z_{1}, \ldots, z_{s}$ we have to apply exactly $s$ additional multiplications. 

The complexity of any multiplication in the realization of the multipliers can be estimated by $O(n^{1+\epsilon})$ operations in $A$, since the degree of any product of approximations in (14) and (15) is less than $n$, for $1 \leq i \leq s$. As $s \leq n$, the complexity of the computation of $z_{1}, \ldots, z_{s}$ is equal to $O(sn^{1+\epsilon}) = O(n^{2+\epsilon})$ operations in $A$; that is, $O(n^{2+\epsilon})$ p-small operations.

**4 Basis multiplication:**

We determine the products $z_{\kappa}b_{\kappa,j}$, for $1 \leq \kappa \leq s$ and $0 \leq j < n_{\Phi_{s}}$. Any $b_{\kappa,j}$ is given by $b_{\kappa,j} = g_{\kappa,j}(\theta)$, where $g_{\kappa,j}(x)$ is a monic polynomial in $A[x]$ of degree $j < n_{\Phi_{s}}$. For $1 \leq \kappa \leq s$, the multiplier $z_{\kappa}$ is given by a polynomial in $A[x]$ of degree less than $n - n_{\Phi_{s}}$ evaluated in $\theta$. As $\sum_{i=1}^{s} n_{\Phi_{i}} = n$, the computation of $z_{\kappa}b_{\kappa,j}$ can be realized at cost of $O(n^{1+\epsilon})$ operations in $A$. In particular, we can compute
all sets $z_{p}B_{\kappa}$ at the cost of $O(n^{2+\epsilon})$ operations in $A$ which equates $O\left(n^{2+\epsilon}\delta^{1+\epsilon}\right)$
p-small operations.

We summarize the results in the following lemma.

**Lemma 3.9.** A $p$-integral basis of $O$ can be determined by at most

$$O\left(n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon} + n^{2+\epsilon}\delta^{1+\epsilon}\right)$$
p-small operations.

### 4. Experimental results

We have implemented the $p$-integral basis algorithm 3 from Section 3 in *Magma* [3] for an algebraic function field $F$ determined by a monic separable and irreducible polynomial $f \in A[x]$ with $A := k[t]$ for a field $k$ as specified. Furthermore we have extended this algorithm to an integral basis algorithm; that is, we determine an integral basis of $O_{F} := \text{Cl}(A, F)$ by computing a triangular $p$-integral basis of $O_{p}$ for all $p \in \text{Spec}(A)$ with $v_{p}(\text{Disc} f) > 1$ and merge those by an application of the CRT.

We will compare the runtime of our algorithm with the implementation of the variant of the Round 2 algorithm [5] and with the implementation of the Quotient method presented in [7] both in *Magma*. All timings are in seconds and taken on a Linux server, with an Intel Xeon processor, running at 2.27 GHz, with 12 GB of RAM memory. For the first examples we use families of global function fields, which cover all the computational difficulties of the Montes algorithm [11]. Later, we use function fields over the rationals. Note that we assume that all prime polynomials in $A$, which are divisible by the ramified prime ideals of $O_{F}$, are precomputed.

#### 4.1. Global function fields.** At first we consider global function fields; that is, $f(t, x) \in \mathbb{F}_{q}[t, x]$ is defined over a finite field $\mathbb{F}_{q}$ with $q$ elements.

**4.1.1. Example 1.** Let $f(t, x) = (x^{6}+4p(t)x^{3}+3p(t)^{2}x^{2}+4p(t)^{2})^{2}+p(t)^{3}+p(t)^{k} \in \mathbb{F}_{7}[t, x]$ with $p(t) = t^{3} + 2$ and $1 \leq k \leq 500$ and denote by $F$ the induced function field. Those prime ideals of $O_{F}$ which divide $p$ are among the ramified prime ideals of $O_{F}$. For $k \geq 17$ the ideal $p \cdot O_{F}$ splits into 6 prime ideals.
4.1.2. **Example 2.** We consider the function field from Example 4.1.1 for prime polynomials $p \in A$ with $1 \leq \deg(p) \leq 220$ for $k = 23$.

4.1.3. **Example 3.** For $1 \leq l \leq 7$ and $p := t^2 + 4$ we take the family of polynomials $f_l \in \mathbb{F}_7[t, x]$ as defined below and denote by $F_l$ the induced function fields. For $l > 1$ we have $p \cdot \mathcal{O}_{F_l} = \mathfrak{p}^\deg f_l$. 
<table>
<thead>
<tr>
<th>Multiplier</th>
<th>Quotients</th>
<th>Magma</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>486</td>
<td>−a</td>
</tr>
</tbody>
</table>

4.1.4. Example 4. We consider \( f(t, x) := x^{4330} - (t^2 + 1)(x^2 - 1) - (t^8 + 2t^6 + 1)x \) in \( \mathbb{F}_3[t, x] \) and denote by \( F/\mathbb{F}_3 \) the induced function field. It holds \( t \cdot \mathcal{O}_F = \prod_{i=1}^{14} \mathfrak{P}_i \).

4.2. Function fields over \( \mathbb{Q} \). The following examples are taken from [4]. For \( 1 \leq l \leq 6 \) we take the polynomials \( g_l \in \mathbb{Q}[t, x] \) as below and denote by \( F_l \) the induced function fields.

<table>
<thead>
<tr>
<th>( l )</th>
<th>( \text{deg } g_l )</th>
<th>Multiplier</th>
<th>Quotients</th>
<th>Ramification</th>
<th>Magma</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>( t \cdot \mathcal{O}_{F_1} = \mathfrak{P}_1^{-1} \mathfrak{P}_2^{-1} \mathfrak{P}_3^{-1} \mathfrak{P}_4^{-1} \mathfrak{P}_5^{-1} \mathfrak{P}_6^{-1} )</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>22</td>
<td>35</td>
<td>53</td>
<td>( t \cdot \mathcal{O}_{F_2} = \mathfrak{P}_1^{-1} \mathfrak{P}_2^{-1} \mathfrak{P}_3^{-1} \mathfrak{P}_4^{-1} \mathfrak{P}_5^{-1} \mathfrak{P}_6^{-1} )</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>200</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>401</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>500</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References


[17] A. Schönhage, V. Strassen,

Department of Mathematics and Computer Science Technische Universiteit Eindhoven P.O. Box 513, 5600 MB Eindhoven, The Netherlands
E-mail address: j.bauch@tue.nl