COMPUTING INTEGRAL BASES VIA LOCALIZATION AND HENSEL LIFTING

J. BOEHM, W. DECKER, S. LAPLAGNE, G. PFISTER

Abstract. We present a new algorithm for finding an integral basis (the normalization) of an algebraic function field of one variable in characteristic zero. Our basic strategy is to reduce from global to local and, then, to "very local": Theoretically, this amounts to localization and, then, completion at each singularity. Practically, we work with approximations by suitably truncated Puiseux expansions. In contrast to van Hoeij's algorithm [14], which also relies on Puiseux expansions, we use Hensel's lemma as a key ingredient. This allows us to compute factors corresponding to groups of conjugate Puiseux expansions, without actually computing the individual expansions. In this way, we make substantially less use of the Newton-Puiseux algorithm. In addition, our algorithm is inherently parallel. As a result, it outperforms in most cases any other algorithm known to us by far. Typical applications are the computation of adjoint ideals and, based on this, the computation of Riemann-Roch spaces and the parametrization of rational curves.

1. Introduction

Let A be a reduced Noetherian ring, and let $\mathrm{Q}(A)$ be its total ring of fractions. The *normalization* of A is the integral closure of A in $\mathrm{Q}(A)$. We denote the normalization by $\overline{A}$ and call A *normal* if $A = \overline{A}$. Recall that if A is a reduced affine (that is, finitely generated) algebra over a field, then $\overline{A}$ is a finite A-module by Emmy Noether's finiteness theorem (see [13]).

In this paper, we are interested in the case where A is the coordinate ring of an algebraic curve defined over a field K of characteristic zero. More precisely, let $f \in K[X,Y]$ be an irreducible polynomial in two variables, let $C \subset \mathbb{A}^2(K)$ be the affine plane curve defined by f, and let

$$A = K[C] = K[X,Y]/\langle f(X,Y)\rangle$$

be the *coordinate ring* of C. We write x and y for the residue classes of X and Y in A, respectively. Throughout the paper, we suppose that f is monic in Y (due to Noether normalization, this can always be achieved by a linear change of coordinates). Then the *function field* of C is of type

$$K(C) = \mathrm{Q}(A) = K(x,y) = K(X)[Y]/\langle f(X,Y)\rangle,$$

x is a separating transcendence basis of $K(C)$ over K, and y is integral over $K[x]$, with integral equation $f(x,y) = 0$. In particular, A is integral over $K[x]$, which implies that $\overline{A}$ coincides with the integral closure $\overline{K[x]}$ of $K[x]$ in $K(C)$. We may, hence, represent $\overline{A}$ either by generators over A or by generators over $K[x]$. For the latter, note that $\overline{A} = \overline{K[x]}$ is a free

$K[x]$–module of rank

$$n := \deg_y(f) = [K(C) : K(x)].$$

Indeed, this follows by applying [12, Theorem 3.3.4] to the PID

$$K[x] \subset K(x) \subset K(C) = K(x)[y].$$

Definition 1.1. An *integral basis* for $\overline{A}$ over $K[x]$ is a set $b_0, \ldots, b_{n-1}$ of free generators for $\overline{A}$ over $K[x]$:

$$\overline{A} = K[x]b_0 \oplus \cdots \oplus K[x]b_{n-1}.$$

Remark 1.2. There is always an integral basis of type

$$1, \frac{p_1(x,y)}{d(x)}, \ldots, \frac{p_{n-1}(x,y)}{d(x)},$$

with $d \in K[x]$, and with polynomials $p_i \in K[x][y]$ of degree i in y. Such a basis is obtained from any given set $1 = c_0, \ldots, c_{m-1}$ of $K[x]$-module generators for $\overline{A}$ by unimodular row operations over the PID $K[x]$: For each i, write $c_{n-1-i} = \sum_{j=0}^{n-1} c_{ij} y^{n-1-j}$, with coefficients $c_{ij} \in K(x)$. Then take d to be the least common denominator of the c_{ij}, transform the matrix $(d \cdot c_{ij})$ into row echolon form (p_{ij}), and set $p_{n-1-i} = \sum_{j=0}^{n-1} p_{ij} y^{n-1-j}$, for each i.

Remark 1.3. To find an integral basis, we may use any normalization algorithm, regardless of how $\overline{A}$ is represented by the algorithm. The algorithms in [9], [1], for example, are designed to find A-module generators for $\overline{A}$. More precisely, they return an ideal $U \subset A$ together with an element $d \in A$ such that $\overline{A} = \frac{1}{d}U \subset \mathrm{Q}(A)$. Here, as we will recall in Section 2, any non-zero element of the Jacobian ideal M of $A = K[x,y]$ can be taken to be d. In particular, we can choose d to be a generator of the elimination ideal $M \cap K[x]$. The roots of d in the algebraic closure $\overline{K}$ of K are then precisely the x-coordinates of the singularities of the curve defined by f in $\mathbb{A}^2(\overline{K})$. If $u_0 = d(x), u_1, \ldots, u_r$ generate the ideal U, the $y^i u_j(x,y)/d(x)$, $0 \le i \le n-1$, $0 \le j \le r$, generate $\overline{A}$ over $K[x]$. An integral basis is then obtained by operations as described in Remark 1.2.

Example 1.4. Consider the standard cusp: Let

$$A = K[x,y] = K[X,Y]/\langle Y^3 - X^2 \rangle.$$

As a module over A, we may represent $\overline{A}$ as

$$\overline{A} = A \cdot \frac{y^2}{x} + A \cdot 1 = \frac{1}{x} \left\langle y^2, x \right\rangle_A$$

(see [9, Example 2.5]). Considering $\overline{A}$ over $K[x]$, we get

$$\overline{A} = K[x] \cdot \frac{y^2}{x} + K[x] \cdot y \cdot \frac{y^2}{x} + K[x] \cdot y^2 \cdot \frac{y^2}{x} + K[x] \cdot 1 + K[x] \cdot y + K[x] \cdot y^2.$$

Since $y^3 = x^2$ and $K[x] \cdot y^2 \subset K[x] \cdot y^2/x$, we have

$$\overline{A} = K[x] \cdot \frac{y^2}{x} \oplus K[x] \cdot 1 \oplus K[x] \cdot y.$$

Hence, $1, y, y^2/x$ is an integral basis as in Remark 1.2.

From here on adjust to writing the algorithm in a better way.

So integral bases can be found using any normalization algorithm. In Section 2, to fix some of our notation and give a first example, we briefly discuss the normalization algorithm of Greuel et al. [9], which is of global nature. In Section 3, as a first step towards a better performance, we recall the local to global normalization algorithm of Böhm et al. [1], which finds $\overline{A}$ by computing a local contribution at each prime ideal contained in the singular locus of A, and putting these together. In Section 4, we start describing our new approach by showing that at least theoretically, we can go one step further. In fact, taking an analytic point of view, we explain how to obtain the local contribution at a singularity from the normalization of the completion, which in turn is obtained by splitting into branches, and finding the normalization of each branch. In Section 5, which is the heart of this paper, we show how to carry this out in practical terms, working with approximations by suitably truncated Puiseux series. This approach is inspired by van Hoeij's paper [14], but differs completely from van Hoeij's algorithm, with Hensel lifting as a crucial new ingredient. We have implemented our algorithms in the computer algebra system SINGULAR. In Section 6, we compare the different approaches, relying on our implementations as well as on implementations of van Hoeij's algorithm in MAPLE and MAGMA, and running various examples coming from algebraic geometry.

2. The Global Normalization Algorithm

We first fix our notation and give some general facts on normalization. For this, let A be any reduced Noetherian ring. We write

$$\operatorname{Spec}(A) = \{P \subset A \mid P \text{ prime ideal}\}$$

for the *spectrum* of A. The *vanishing locus* of an ideal J of A in $\operatorname{Spec}(A)$ is the set $V(J) = \{P \in \operatorname{Spec}(A) \mid P \supset J\}$. We denote by

$$N(A) = \{P \in \operatorname{Spec}(A) \mid A_P \text{ is not normal}\}$$

the *non-normal locus* of A, and by

$$\operatorname{Sing}(A) = \{P \in \operatorname{Spec}(A) \mid A_P \text{ is not regular}\}$$

the *singular locus* of A. Then $N(A) \subset \operatorname{Sing}(A)$, with equality holding if A is the coordinate ring of a curve (see [4, Theorem 4.4.9]).

Definition 2.1. The *conductor* of A is

$$\mathcal{C}_A = \operatorname{Ann}_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}.$$

Note that $\mathcal{C}_A$ is the largest ideal of A which is also an ideal of $\overline{A}$.
To emphasize the role of the conductor, we note:

Lemma 2.2. *Let A be a reduced Noetherian ring. Then $N(A) \subset V(\mathcal{C}_A)$. Furthermore, $\overline{A}$ is a finite A-module iff $\mathcal{C}_A$ contains a non-zerodivisor of A. In this case, $N(A) = V(\mathcal{C}_A)$.*

Note, however, that the conductor can only be computed a posteriori when $\overline{A}$ is already known.

Definition 2.3. Let A be a reduced Noetherian ring. A *test ideal* for A is a radical ideal $J \subset A$ such that $V(\mathcal{C}_A) \subset V(J)$. A *test pair* for A consists of a test ideal J together with a non–zerodivisor $g \in J$ of A.

Test pairs appear in the Grauert and Remmert normality criterion which is fundamental to algorithmic normalization (see [8], [10, Prop. 3.6.5]). The normalization algorithm of de Jong (see [3], [5]) and its improvement, the algorithm of Greuel et al. [9], are based on this criterion. Both algorithms apply to any reduced affine algebra $A = K[X_1, \ldots, X_n]/I$ over a perfect field K. By means of primary decomposition, we can reduce to the case where A is equidimensional. In this case, since we assume that K is perfect, the Jacobian ideal[1] M of A is non-zero and contained in the conductor $\mathcal{C}_A$, so that we may choose the radical $J = \sqrt{M}$ together with any non–zero element g of M as a test pair (see [9, Lemma 4.1]). The idea of finding $\overline{A}$ is then to successively enlarge A by finite extensions $A_{i+1} \cong \mathrm{Hom}_{A_i}(J_i, J_i) \cong \frac{1}{g}(gJ_i :_{A_i} J_i) \subset \overline{A} \subset \mathrm{Q}(A)$, with $A_0 = A$ and $J_i = \sqrt{JA_i}$, until the normality criterion of Grauert and Remmert allows us stop. As already pointed out in Remark 1.3, the algorithm of Greuel et al. is designed so that it returns an ideal $U \subset A$ together with an element $d \in A$ such that $\overline{A} = \frac{1}{d}U \subset \mathrm{Q}(A)$.

Remark 2.4. If M is non-zero and contained in $\mathcal{C}_A$ as above, then any non-zero element of M is valid as a denominator: If $0 \neq c \in M$, then $c \cdot \frac{1}{d}U =: U'$ is an ideal of A, and $\frac{1}{d}U = \frac{1}{c}U'$.

Example 2.5. Let A be the coordinate ring of the curve C with defining polynomial $f(X, Y) = X^5 - Y^2(Y-1)^3$. Then

$$J := \langle x, y\,(y-1)\rangle_A$$

is the radical of the Jacobian ideal, so that we can take (J, x) as a test pair. In its first step, the normalization algorithm yields

$$A_1 = \frac{1}{x}U_1 = \frac{1}{x}\left\langle x, y(y-1)^2\right\rangle_A.$$

In the next steps, we get

$$A_2 = \frac{1}{x^2}U_2 = \frac{1}{x^2}\left\langle x^2, xy(y-1), y(y-1)^2\right\rangle_A$$

and

$$A_3 = \frac{1}{x^3}U_3 = \frac{1}{x^3}\left\langle x^3, x^2y(y-1), xy(y-1)^2, y^2(y-1)^2\right\rangle_A.$$

In the final step, we find that A_3 is normal and, hence, equal to $\overline{A}$.

3. Normalization of Curves via Localization

In this section, we discuss the local to global variant of the normalization algorithm presented in [1]. Our starting point is Proposition 3.1 below. In formulating the proposition, if $P \in \mathrm{Spec}(A)$ and $A \subset A' \subset \overline{A}$ is an intermediate ring, we write A'_P for the localizaton of A' at $A \setminus P \subset A'$.

[1]The *Jacobian ideal* M of $A = K[X_1, \ldots, X_n]/I$ is generated by the images of the $c \times c$ minors of the Jacobian matrix $\left(\frac{\partial f_i}{\partial X_j}\right)$, where c is the codimension, and $f_1, \ldots, f_r$ are generators for I. By the Jacobian criterion, $V(M) = \mathrm{Sing}(A)$ (see [7, Theorem 16.19]).

Proposition 3.1. *Let A be a reduced Noetherian ring with a finite singular locus* $\mathrm{Sing}(A) = \{P_1, \ldots, P_s\}$. *For $i = 1, \ldots, s$, let an intermediate ring $A \subset A^{(i)} \subset \overline{A}$ be given such that $A^{(i)}_{P_i} = \overline{A_{P_i}}$. Then*

$$\sum_{i=1}^{s} A^{(i)} = \overline{A}.$$

Proof. This is a special case of [1, Proposition 3.2]. □

Definition 3.2. We call any ring $A^{(i)}$ as in the proposition a *local contribution* to $\overline{A}$ at P_i. If in addition $A^{(i)}_{P_j} = A_{P_j}$ for $j \neq i$, we speak of a *minimal local contribution* to $\overline{A}$ at P_i.

Remark 3.3. The algorithms discussed in this paper will return minimal local contributions. Note that such a contribution is uniquely determined since, by definition, its localization at each $P \in \mathrm{Spec}(A)$ is determined.

Proposition 3.1 applies, in particular, if A is the coordinate ring of a curve. From now on,

$$A = K[C] = K[X, Y]/\langle f(X, Y)\rangle$$

will always denote the coordinate ring of an irreducible plane curve C as in the introduction. Proposition 3.1 allows us, then, to split the computation of $\overline{A}$ into local tasks at the primes $P_i \in \mathrm{Sing}(A)$. One way of finding the local contributions to $\overline{A}$ at the P_i is to apply the local version of the normalization algorithm discussed in [1]. For each i, the basic idea is to use P_i together with a suitable element g_i of the Jacobian ideal instead of a test pair as in Definition 2.3.

Example 3.4. Let A be the coordinate ring of the curve C with defining polynomial $f(X, Y) = X^5 - Y^2(Y-1)^3$ from Example 2.5. Note that C has a double point of type A_4 at $(0, 0)$ and a triple point of type E_8 at $(0, 1)$. If we apply the strategy above, taking $P_1 = \langle x, y\rangle_A$, $P_2 = \langle y - 1, x\rangle_A$ and $g_1 = g_2 = x$, we get local contributions $\frac{1}{d_i}U_i$, $i = 1, 2$. Exactly,

$$\begin{aligned} d_1 &= x^2 \quad \text{and} \quad U_1 = \left\langle x^2, y(y-1)^3 \right\rangle_A, \\ d_2 &= x^3 \quad \text{and} \quad U_2 = \left\langle x^3, x^2y^2\,(y-1)\,, y^2\,(y-1)^2 \right\rangle_A. \end{aligned}$$

Summing up the local contributions, we get $\bar{A} = \frac{1}{d}U$ with $d = x^3$ and

$$U = \left\langle x^3,\ y(y-1)^3x,\ y^2\,(y-1)\,x^2,\ y^2\,(y-1)^2 \right\rangle_A.$$

Note that U coincides with the ideal U_3 computed in Example 3.4.

Remark 3.5. In Example 3.4, the normalization of the local ring A_{P_2} is $\overline{A_{P_2}} = \frac{1}{x^3}\langle x^3, x^2(y-1), (y-1)^2\rangle_{A_{P_2}}$. Indeed, since y^2 is a unit in $\overline{A_{P_2}}$, this follows by localizing U_2 at P_2. Note, however, that $(y-1)/x$ and $(y-1)^2/x^3$ are not integral over A. Hence, $\frac{1}{x^3}\langle x^3, x^2(y-1), (y-1)^2\rangle_A$ is not a local contribution to A at P_2.

In what follows, we describe a way of finding the local contributions which is custom-made for the case of plane curves.

4. Normalization of Plane Curves via Localization and Completion: Decomposing into Branches

In this section, we focus on the case where the origin is a singularity of C, that is, we suppose that $P = \langle x, y\rangle \in \mathrm{Sing}(A)$. Our goal is to reduce the problem of finding the minimal local contribution to $\overline{A}$ at P to the problem of finding an integral basis at each branch of the singularity. At the same time, we indicate one possible approach to finding the integral bases at the branches. In the next section, which is the heart of this paper, we will carry out the details of this approach.

Focusing on the singularity at the origin means to consider f as an element of the formal power series ring $K[[X,Y]] = K[[X]][Y]$. Then f is regular of order n in Y. By the Weierstrass preparation theorem, we may write f as a product $f = u \cdot \widetilde{f}$, where u is a unit in $K[[X,Y]]$, and $\widetilde{f}$ is a Weierstrass polynomial (see, for example, [4]). Decomposing $\widetilde{f}$ into its irreducible factors, we obtain a factorization of type

$$f = u \prod_{i=1}^{r} g_i,$$

with irreducible Weierstrass polynomials g_i. Then, passing from the local ring A_P to its completion and normalizing, we get

$$\overline{\widehat{A_P}} = \overline{K[[X]][Y]/\langle f\rangle} \cong \bigoplus_{i=1}^{s} \overline{K[[X]][Y]/\langle g_i\rangle}.$$

We call each ring $K[[X]][Y]/\langle g_i\rangle$ a *branch* of A at P.

Remark 4.1. Let $g \in K[[X,Y]]$ be an irreducible Weierstraß polynomial of degree m in Y. Write $K((x))[y] = K(x,y) = K[[X,Y]]/\langle g\rangle$. Then the normalization of $K[[x]][y]$ coincides with the integral closure $\overline{K[[x]]}$ of $K[[x]]$ in $K((x))[y]$. Applying [12, Theorem 3.3.4] to the PID

$$K[[x]] \subset K((x)) \subset K((x))[y],$$

we see that $\overline{K[[x]][y]} = \overline{K[[x]]}$ is a free $K[[x]]$-module of rank m.

Definition 4.2. An *integral basis* for $\overline{K[[x]][y]}$ over $K[[x]]$ is a set of free generators for $\overline{K[[x]][y]}$ over $K[[x]]$.

Lemma 4.3. *Let $g \in K[[X]][Y]$ be an irreducible Weierstraß polynomial of degree m in Y. Then there exist monic polynomials $1 = p_0, p_1, \ldots, p_{m-1} \in K[X][Y]$ in Y of degree i and $e_i \in \mathbb{N}$ such that $p_0, \frac{p_1(x,y)}{x^{e_1}}, \ldots, \frac{p_{m-1}(x,y)}{x^{e_{m-1}}}$ is an integral basis for $\overline{K[[X]][Y]/\langle g\rangle}$ over $K[[x]]$. The e_i satisfy $e_1 \le \cdots \le e_{m-1}$. Moreover, if $q(X,Y) \in K[[X]][Y]$ is monic in Y of degree $1 \le i \le m-1$, and e is an integer such that $\frac{q(x,y)}{x^e}$ is integral over $K[[x]]$, then $e \le e_i$. In particular, the e_i are uniquely determined.*

Proof. Each square matrix with entries in $K[[X]]$ of maximal rank has a uniquely determined upper triangular Hermite normal form (p_{ij}), where the diagonal elements are of type $p_{ii} = x^{\nu_i}$, and where the (p_{ij}), $j > i$, are polynomials in $K[X]$ of degree $< \nu_i$ (see [6]). Hence, if we start from any integral basis for $\overline{K[[x]][y]}$ over $K[[x]]$ and apply unimodular row operations

as in Remark 1.2, we get an integral basis $b_0 = 1, b_1, \dots b_{m-1}$, where the b_i are of type $\frac{p_i(x,y)}{x^{e_i}}$, with polynomials p_i which are monic in y of degree i, and with integers e_i. By induction, multiplying b_i by y and expressing the result as a $K[[x]]$-linear combination of the b_k, we see that $0 \leq e_1 \leq \cdots \leq e_{m-1}$. The last statement of the lemma follows similarly. □

Definition 4.4. If $q(X,Y) \in K[[X]][Y]$ is monic in Y of degree $1 \leq i \leq m-1$, and e is the maximal integer such that $\frac{q(x,y)}{x^e}$ is integral over $K[[x]]$, then we call e the *integrality exponent of q with respect to g*, written $e(q) = e$. With notation as in the lemma, for each i, we call e_i the *maximal integrality exponent with respect to g in degree i*.

Lemma 4.5. *Let $g \in K[[X]][Y]$ be an irreducible Weierstraß polynomial of degree m in Y. Let p_i be polynomials which are monic in Y of degree i and such that $e(p_i)$ is the maximal integrality exponent with respect to g in degree i. Then $p_0 = 1, \frac{p_1}{X^{e_1}}, \dots, \frac{p_{m-1}}{X^{e_{m-1}}}$ is an integral basis for $\overline{K[[X]][Y]/\langle g\rangle}$ over $K[[x]]$.*

Proof. $A' = \langle 1, \frac{p_1}{x^{e(p_1)}}, \dots, \frac{p_{n-1}}{x^{e(p_{n-1}}}\rangle$

$A'_j = \langle 1, \dots, \frac{p_j}{x^{e(p)}}, \rangle$

Induction: $q \in K[[x]][y]$, $\deg_y q = j$, $\frac{q}{x^e} \in \overline{A} \Rightarrow \frac{q}{x^e} \in A'_j$. Let $q = x^e \cdot \widetilde{q}, x \nmid \widetilde{q} \Rightarrow \exists\ u$ unit in $K[[x,y]]\widetilde{q} = u \cdot \overline{q}$, $\overline{q}$ Weierstraß poly in y of degree $\leq j$.

$\frac{x^e \overline{q} u}{x^e} \in \overline{A} \Rightarrow \frac{\overline{q}}{x^{e-c}} \in \overline{A}$. If $e - c \leq 0$ there is nothing to prove. We may assume $c = 0$. If $\deg y\overline{q} < j \Rightarrow \frac{\overline{q}}{x^e} \in A'_k$ (induction). If $\deg y\overline{q} = j$ then $u \in K$ and we may assume that q is monic. This implies $e \leq e(p_j)$. We obtain $\frac{q}{x^e} = \frac{x^{e(p_j)-e}q}{x^{e(p_j)}} = x^{e(p_j)-e} \cdot \frac{p_j}{x^{e(p_j)}} + \frac{r}{x^{e(p_j)}}$, $\deg_y r < j$.

We obtain the claim using induction. It remains to prove $\frac{\overline{q}}{x^e} \in A'_k \Rightarrow \frac{u\overline{q}}{x^e} \in A'_j$.

We know $\deg_y u = j - k$. This implies $u \in A'_{j-k}$. But $\frac{\overline{q}}{x^e} \in k \Rightarrow y^i \frac{\overline{q}}{x^e} \in A'_{k+i}$ for $i \leq j - k$. This implies $\frac{u\overline{q}}{x^e} \in A'_j$.

□

Lemma 4.6. *Let $f \in K[X,Y]$ be a Weierstraß polynomial in $K[[X]][Y]$ with respect to Y and*

$$f = f_1 \cdot \ldots \cdot f_s$$

be the decomposition into irreducible polynomials, and let $h_i = \frac{f}{f_i}$. By the Euclidean algorithm in $Q(K[[X]])[Y]$ for the coprime f_i and h_i, there are $a_i, b_i \in K[[X]][Y]$, $c \in \mathbb{N}$ with

$$a_i f_i + b_i h_i = X^c.$$

The normalization splits as

$$\overline{K[[X]][Y]/\langle f\rangle} = \overline{K[[X]][Y]/\langle f_i\rangle} \oplus \overline{K[[X]][Y]/\langle h_i\rangle}$$

and the splitting is given by

$$(a \bmod f_i, b \bmod h_i) \mapsto \frac{b_i h_i a + a_i f_i b}{X^c}.$$

Proof. Follows by the Chinese remainder theorem. □

Lemma 4.7. *With the notation as in Lemma 4.6, let*

$$p_0^{(i)}, \frac{p_1^{(i)}}{X^{e_1^{(i)}}}, \ldots, \frac{p_{d_i-1}^{(i)}}{X^{e_{d_i-1}^{(i)}}}$$

be the integral basis obtained from Lemma 4.3 for $\overline{K[[X]][Y]/\langle f_i\rangle}$ *and define the* $K[[X]]$*-modules*

$$B^{(i)} = \left\langle 1, y, \ldots, y^{d_i}, \frac{b_i h_i}{X^c}, \frac{b_i h_i p_1^{(i)}}{X^{c+e_1^{(i)}}}, \ldots, \frac{b_i h_i p_{d_i-1}^{(i)}}{X^{c+e_{d_i-1}^{(i)}}} \right\rangle.$$

Then the normalization is

$$\overline{K[[X]][Y]/\langle f\rangle} = \sum_{i=1}^{s} B^{(i)}.$$

Proof. Follows from Lemma 4.6. □

Proposition 4.8. *With the notation as in Lemma 4.7, let* $\tilde{b}_i, \tilde{h}_i \in K[x,y]$ *with*

$$\tilde{b}_i \tilde{h}_i \equiv b_i h_i \bmod X^{c+e_{d_i}^{(i)}-1}$$

define the $K[x]_{\langle x\rangle}$*-modules*

$$A^{(i)} = \left\langle 1, y, \ldots, y^{d_i}, \frac{\tilde{b}_i \tilde{h}_i}{X^c}, \frac{\tilde{b}_i \tilde{h}_i p_1^{(i)}}{X^{c+e_1^{(i)}}}, \ldots, \frac{\tilde{b}_i \tilde{h}_i p_{d_i-1}^{(i)}}{X^{c+e_{d_i-1}^{(i)}}} \right\rangle.$$

Then

$$\widehat{A^{(i)}} = B^{(i)}$$

and

$$\overline{K[X,Y]_{\langle X,Y\rangle}/\langle f\rangle} = \sum_{i=1}^{s} A^{(i)}.$$

Proof. Follows from Lemma 4.7 by faithfully flatness and since $\widehat{\overline{R}} = \overline{\widehat{R}}$ for any excellent ring R. □

To compute a local contribution to the normalization at $\langle x, y\rangle$, we have to take into account the unit in the factorization of f.

Proposition 4.9. *Let* $f = u\prod_{i=1}^{r} f_i$ *as at the beginning of this section, with* $u \in K[X,Y]$ *a unit in* $K[[X,Y]]$ *of degree* d *in* Y *and* f_i, $1 \le i \le r$, *irreducible Weierstrass polynomials*

With the notation as in Proposition 4.8, define the $K[x]_{\langle x\rangle}$*-modules*

$$\tilde{A}^{(i)} = \left\langle 1, y, \ldots, y^{d_i+d-1}, \frac{u\tilde{b}_i \tilde{h}_i}{X^c}, \frac{u\tilde{b}_i \tilde{h}_i p_1^{(i)}}{X^{c+e_1^{(i)}}}, \ldots, \frac{u\tilde{b}_i \tilde{h}_i p_{d_i-1}^{(i)}}{X^{c+e_{d_i-1}^{(i)}}} \right\rangle.$$

Then $\sum_{i=1}^{s} \tilde{A}^{(i)}$ *is a minimal local contribution to the normalization at the origin.*

In Section 5, we will design algorithms to compute rings $A^{(i)}$ with the properties specified in Proposition 4.8.

In particular, such rings exist.

Example 4.10. Let

$$A = K[X,Y]/\left\langle (Y^3+X^8)(Y^6+Y^3X^7-2Y^3X^4+X^8)+X^{20}\right\rangle = K[x,y].$$

In $K[[X]][Y]$, the polynomial $f=(Y^3+X^8)(Y^6+Y^3X^7-2Y^3X^4+X^8)+X^{20}$ decomposes into two irreducible factors. Hence, A has a singularity at the origin with two branches.

With the computational means presented in Section 5, we compute the integral bases of the rings $A^{(1)}$ and $A^{(2)}$ as in Proposition 4.9:

$$A^{(1)} = \left\langle 1, y, y^2, y^3, y^4, y^5, \frac{h_1}{x^8}, \frac{h_1 y}{x^{10}}, \frac{h_1 y^2}{x^{13}} \right\rangle,$$

where $h_1 = (y^6 + y^3x^7 - 2y^3x^4 + x^8)$ and

$$A^{(2)} = \left\langle 1, y, y^2, \frac{h_2}{x^4}, \frac{h_2 y}{x^5}, \frac{h_2 y^2}{x^6}, \frac{h_2 h_3}{x^9}, \frac{h_2 h_3 y}{x^{10}}, \frac{h_2 h_3 y^2}{x^{12}} \right\rangle,$$

where $h_2 = (y^3 + x^8)$ and $h_3 = (y^3 - x^4)$

Combining the results, we get $\overline{A} = A^{(1)} + A^{(2)}$.

We finish the section with an example including expansions that do not vanish at the origin.

Example 4.11. Let

$$A = K[X,Y]/\left\langle (Y^3-X^7)(Y^2-X^3)+Y^6\right\rangle = K[x,y].$$

In $K[[X]][Y]$, the polynomial $f=(Y^3-X)(Y^2+X^3)+Y^7$ can be factorized as $f = uf_1f_2$ with $u = Y^2+(-X)Y+1+\ldots$, $f_1 = Y^3+XY^2-X+\ldots$ and $f_2 = Y^2+X^3+\ldots$ where the dots represent in all cases terms with degree greater than 1 in X.

The rings $K[[X]][Y]/\langle f_i\rangle$, $i=1,2$, have integral bases $\{1, \frac{y}{x}, \frac{y^2}{x}\}$ and $\{1, \frac{y}{x}\}$. Adding the factors as in Proposition 4.9, we get

$$A^{(1)} = \left\langle 1, y, y^2, uy, uf_2, \frac{uf_2 y}{x}, \frac{uf_2 y^2}{x} \right\rangle$$

and

$$A^{(2)} = \left\langle 1, y, y^2, uy, uy^2, \frac{uf_1}{x}, \frac{uf_1 y}{x^2} \right\rangle.$$

5. Normalization of Plane Curves via Localization and Completion: Handling the Branches Using Puiseux Expansions and Hensel's Lemma

Let A be the ring

$$A = K[x,y] = K[X,Y]/\langle f(X,Y)\rangle$$

as before. For such a ring, in this section we show how to compute a local contribution to $\overline{A}$ at each prime ideal $P \in \mathrm{Sing}(A)$ via Puiseux expansions and Hensel's lemma. Once the local contribution at each component of the singular locus is obtained, the global integral basis is computed applying Proposition 4.9.

We start with a sketch of the algorithm.

(1) **Translation of the singularity to the origin.** If the prime component corresponds to a singular point, apply a translation to the variables so that the singularity is moved to the origin. If the prime component corresponds to a groups of conjugated singular points, apply first a linear transformation so that no point has the same X-coordiante and then apply a translation so that one of the singularity is moved to the origin (an algebraic field extension is needed in this case).

For the singularity at the origin,

(2) Determine the maximum integrality exponent $e = e_{n-1}$. (See Defintion 4.4.)
(3) **Factorization by Hensel Lemma.** Applying Hensel Lemma, compute the factorization $f = h \prod_{i=1}^{r} f_i$ as in Section 4, developing the factors h and f_i, $1 \leq i \leq s$ up to degree e in X.
(4) **Local contribution of each factor.** For each $1 \leq i \leq r$, compute the local contribution $A^{(i)}$ from Proposition 4.9 as follows
   (a) For each $j = 0, \ldots, s-1$, $s = \deg(f_i)$, compute a polynomial p_j of degree j in Y with maximal valuation $d_j = v_{f_i}(p_j)$ among all the polynomials of the same degree.
   (b) Develop the product $F_i = \prod_{j \neq i} f_j$ up to degree e in X.
   (c) The local contribution $A^{(i)}$ to the integral basis of the singularity at the origin is
$$\left\{1, y, y^2, \ldots, y^{\deg h + \deg F_i - 1}, hF_i, hF_i \frac{p_1}{x^{d_1}}, \ldots, hF_i \frac{p_{s-1}}{x^{d_{s-1}}}\right\}.$$
(5) Apply the inverse translation to the elements of the local contribution to restore the singularity to the original position.
(6) If the component corresponds to a groups of singularities, modify the numerators and denominators of the local contribution to obtain the local contribution of the component over the original field.

In the following subsections we explain these steps in more detail.

5.1. **Basic Remarks on Puiseux Series.** We fix our notation and recall a few results in the context of Puiseux series.

Puiseux Series. Let $K \subset L$ be a field extension, with L algebraically closed. Write $L[[X]]$ for the ring of formal power series in X over L and $L((X)) = \mathrm{Q}(L[[X]])$ for the field of formal Laurent series. The *field of Puiseux series* over L is the field
$$L\{\{X\}\} = \bigcup_{m=1}^{\infty} L((X^{1/m})).$$
This field arises naturally in the context of Emmy Noether's finiteness theorem. In fact, $L\{\{X\}\}$ is the algebraic closure of $L((X))$, and the integral closure of $L[[X]]$ in $L((X^{1/m}))$ is $L[[X^{1/m}]]$ (see [7, Corollary 13.15]).

We have a canonical *valuation map*
$$v : L\{\{X\}\} \setminus \{0\} \to \mathbb{Q},\ \gamma \mapsto v(\gamma),$$
where $v(\gamma)$ is the smallest exponent appearing in a term of γ. By convention, $v(0) = \infty$. The corresponding *valuation ring* $L\{\{X\}\}_{v \geq 0}$ consists of

all Puiseux series with non–negative exponents only. Henceforth it will be denoted by $\mathcal{P}_X$.

If $p \in L\{\{X\}\}[Y]$ is any polynomial in Y with coefficients in $L\{\{X\}\}$, the *valuation* of p at $\gamma \in L\{\{X\}\}$ is defined to be $v_\gamma(p) := v(p(\gamma))$.

Conjugate Puiseux Series. Two Puiseux series in $L\{\{X\}\}$ are called *conjugate* if they are conjugate as field elements over $K((X))$.

Rational Part. Let $\gamma = a_1X^{t_1} + a_2X^{t_2} + \cdots + a_kX^{t_k} + a_{k+1}X^{t_{k+1}} + \cdots \in \mathcal{P}_X$, with $0 \le t_1 < t_2 < \ldots$. Let $k \ge 0$ be such that $a_iX^{t_i} \in K[X]$ for $1 \le i \le k$ and $a_{k+1}X^{t_{k+1}} \notin K[X]$. Then we call $a_1X^{t_1} + \cdots + a_kX^{t_k}$ the *rational part* of γ, and $a_{k+1}X^{t_{k+1}}$ its *first non–rational term.*

Characteristic Exponents. For $\gamma \in \mathcal{P}_X$, let $m \in \mathbb{N}$ be minimal with $\gamma \in L[[X^{1/m}]]$, and write $\gamma = \sum_{i\ge 0} b_iX^{i/m}$, with coefficients $b_i \in L$. If $m = 1$, there are no characteristic exponents. If $m \ge 2$, the *characteristic exponents* of γ are defined inductively by

$$e_1 := \min\{i \mid b_i \neq 0 \text{ and } m \nmid i\},$$
$$e_\nu := \min\{i \mid b_i \neq 0,\ \gcd(e_1, \ldots, e_{\nu-1}) \nmid i\} \text{ for } \nu > 1.$$

Then $e_1 < e_2 < \ldots$; in fact, there are only finitely e_ν, and these are coprime.

Example 5.1. If $\gamma = 2X^{1/2} + X^{3/4} + 6X^{5/4} - 5X^{17/8}$, the common denominator is $m = 8$. Writing $\gamma = 2X^{4/8} + X^{6/8} + 6X^{10/8} - 5X^{17/8}$, we see that the characteristic exponents are $e_1 = 4$, $e_2 = 6$, and $e_3 = 17$.

Puiseux Expansions. Since $L\{\{X\}\}$ is algebraically closed, the polynomial $f \in K[X,Y] = K[X][Y]$ has $n = \deg_Y(f)$ roots $\gamma_1, \ldots, \gamma_n$ in $L\{\{X\}\}$. These roots are called the *Puiseux expansions* of f (at $X = 0$). Since f is supposed to be monic in Y, we have a factorization of type

$$f = (Y - \gamma_1)\cdots(Y - \gamma_n) \in L\{\{X\}\}[Y].$$

In particular, each γ_i is integral over $L[[X]]$ and, thus, contained in some $L[[X^{1/m}]] \subset \mathcal{P}_X$. That is, the terms of γ_i have non–negative exponents only.

Regularity Index and Singular Part. If $\gamma = a_1X^{t_1} + a_2X^{t_2} + \ldots$ is a Puiseux expansion of f, with $0 \le t_1 < t_2 < \ldots$ and no a_i zero, we define the *regularity index* of γ to be the least exponent t_k such that no other Puiseux expansion of f has the same initial part $a_1X^{t_1} + \cdots + a_kX^{t_k}$. This initial part is, then, called the *singular part* of γ.

The Newton-Puiseux Algorithm. The Puiseux expansions of f can be computed recursively up to any given order using the Newton-Puiseux algorithm. Essentially, to get a solution $a_1X^{t_1} + a_2X^{t_2} + \ldots$ of $f(X, \gamma(X)) = 0$, with $t_1 < t_2 < \ldots$, the algorithm proceeds as follows: Starting from $f^{(0)} = f$ and $K^{(0)} = K((X))$, we commence the ith step of the algorithm by looking at a polynomial $f^{(i-1)} \in K^{(i-1)}[Y]$. We then choose one face Δ of the Newton polygon of $f^{(i-1)}$ such that all the other points of the polygon lie on or above the line containing the face. Let $f_\Delta^{(i-1)}$ be the sum of terms of $f^{(i-1)}$ involving the monomials of $f^{(i-1)}$ on Δ. That is, if $-\frac{w_1}{w_2}$ is the slope of Δ, then $f_\Delta^{(i-1)}$ is the sum of terms of $f^{(i-1)}$ of lowest $(1, \frac{w_2}{w_1})$–weighted

degree. We write d_i for this degree. Choose an irreducible factor of $f_\Delta^{(i-1)}$ over $K^{(i-1)}$ and a root q_i of that factor. Note that q_i is of type $q_i = c_i X^{\frac{w_2}{w_1}}$, where c_i is a root of the polynomial $f_\Delta^{(i-1)}(1, Y)$. Now, let $K^{(i)} = K^{(i-1)}(q_i)$ and set $f^{(i)} = \frac{1}{X^{d_i}} p^{(i-1)}(X, q_i \cdot (1+Y))$. Then the ith term of the expansion to be constructed is $a_i X^{t_i} = q_1 \cdots q_i$. It is clear from this construction that different conjugacy classes of expansions arise from different choices for the faces and irreducible factors of $f_\Delta^{(i-1)}$ over $K^{(i-1)}$, respectively.

Example 5.2. The eight Puiseux expansions of the polynomial

$$\begin{aligned} f = {} & Y^8 + (-4X^3 + 4X^5)Y^7 + (4X^3 - 4X^5 - 10X^6)Y^6 + (4X^5 - 6X^6)Y^5 \\ & + (6X^6 - 8X^8)Y^4 + (8X^8 - 4X^9)Y^3 + (4X^9 + 4X^{10})Y^2 + 4X^{11}Y + X^{12} \\ & \in \mathbb{Q}[X, Y] \end{aligned}$$

are conjugate over $\mathbb{Q}((X))$; their singular parts are of type

$$q_1 + q_1 q_2 + q_1 q_2 q_3,$$

where the q_i satisfy

$$q_1^2 + X^3 = 0, \qquad q_2^2 + \tfrac{1}{2X} q_1 = 0, \qquad \text{and} \quad q_3^2 + \tfrac{1}{16X} q_1 = 0.$$

To see this, note that the Newton polygon of $f^{(0)} = f$ has only one face Δ_0, leading to $f_{\Delta_0}^{(0)} = \left(X^3 + Y^2\right)^4$ and the extension

$$K_0 = \mathbb{Q}((X)) \subset K_1 = K_0[iX^{\frac{3}{2}}].$$

In the next step, $f^{(1)}$ has only one face Δ_1, yielding

$$f_{\Delta_1}^{(1)} = 4\left(2Y^2 + \frac{q_1}{X}\right)^2$$

and

$$K_1 \subset K_2 = K_0[iX^{\frac{3}{2}}, (1-i)X^{\frac{1}{4}}].$$

Finally, also $f^{(2)}$ has only one face Δ_2, which corresponds to

$$f_{\Delta_2}^{(2)} = -2 \cdot \left(8Y^2 - \frac{q_1}{X}\right)$$

and the extension

$$K_2 \subset K_3 = K_0[iX^{\frac{3}{2}}, (1-i)X^{\frac{1}{4}}, (1+i)X^{\frac{1}{4}}] = K_0[i, X^{\frac{1}{4}}].$$

Puiseux Blocks. To simplify the presentation of our algorithms, we introduce some special terminology. We partition the set of all Puiseux expansions of f into *Puiseux blocks*. A Puiseux block represented by an expansion γ with $\gamma(0) = 0$ is obtained by collecting all expansions whose rational part agrees with that of γ and whose first non–rational term is conjugate to that of γ over $K((X))$. A *Puiseux segment* is defined as the union of all blocks having the same initial exponent. That is, we have one Puiseux segment for each face of the Newton polygon of f. In addition, all Puiseux expansions γ of f with $\gamma(0) \neq 0$ are grouped together to a single Puiseux block of an extra Puiseux segment. In this way, the Puiseux expansions of f are divided into Puiseux segments, each segment consists of Puiseux blocks, and each block is the union of classes of conjugate expansions.

that is?

Example 5.3. Suppose that the Puiseux expansions of a polynomial f are

$$\begin{aligned}
\gamma_1 &= 1 + X^2 + \dots, & \gamma_6 &= X + b_1 X^{5/2} + X^3 + \dots,\\
\gamma_2 &= -1 + 3X + \dots, & \gamma_7 &= X + b_2 X^{5/2} + X^3 + \dots,\\
\gamma_3 &= a_1 X^{3/2} + 2X^2 + \dots, & \gamma_8 &= X + b_1 X^{5/2} + X^4 + \dots,\\
\gamma_4 &= a_2 X^{3/2} + 2X^2 + \dots, & \gamma_9 &= X + b_2 X^{5/2} + X^4 + \dots,\\
\gamma_5 &= X + 3X^2 + \dots,
\end{aligned}$$

where $\{\gamma_3, \gamma_4\}$, $\{\gamma_6, \gamma_7\}$ and $\{\gamma_8, \gamma_9\}$ are pairs of conjugate Puiseux series. Then $\{\gamma_1, \gamma_2\}$ is the segment of expansions γ with $\gamma(0) \neq 0$. Another segment is $\{\gamma_3, \gamma_4\}$ (which consists of one block containing a single class of conjugate expansions). All the other expansions form a single segment, consisting of the blocks $\{\gamma_5\}$ and $\{\gamma_6, \gamma_7, \gamma_8, \gamma_9\}$. The last block contains two classes of conjugate expansions, namely $\{\gamma_6, \gamma_7\}$ and $\{\gamma_8, \gamma_9\}$.

Maximal Integrality Exponents. Let $\Gamma = \{\gamma_1, \dots, \gamma_n\}$ be the set of Puiseux expansions of f at $x = 0$, and let $p \in \mathcal{P}_X[Y]$. The *valuation* of p at f is defined to be $v_f(p) = \min_{1 \le i \le n} v_{\gamma_i}(p)$. Note that if p is monic of degree d, where $1 \le d \le n-1$, and

$$p = (Y - \eta_1(X)) \cdots (Y - \eta_d(X)), \text{ with all } \eta_i \in \mathcal{P}_X,$$

is the factorization of p in $\mathcal{P}_X[Y]$, then

$$v_f(p) = \min_{1 \le i \le n} \sum_{j=1}^{d} v(\gamma_i - \eta_j).$$

Lemma 5.4. *With notation as above, fix an integer d with $1 \le d \le n-1$. If $\mathcal{A} \subset \{1, \dots, n\}$ is a subset of cardinality d, set*

$$\mathrm{Int}(\mathcal{A}) = \min_{i \notin \mathcal{A}} \left(\sum_{j \in \mathcal{A}} v(\gamma_i - \gamma_j) \right).$$

Choose a subset $\widetilde{\mathcal{A}} \subset \{1, \dots, n\}$ of cardinality d such that $\mathrm{Int}(\widetilde{\mathcal{A}})$ is maximal among all $\mathrm{Int}(\mathcal{A})$ as above, and set $\widetilde{p} = \prod_{j \in \widetilde{\mathcal{A}}} (Y - \gamma_j)$. Then $v_f(\widetilde{p}) = \mathrm{Int}(\widetilde{\mathcal{A}})$, and this number is the maximum valuation $v_f(p)$, for $p \in \mathcal{P}_X[Y]$ monic in Y of degree d.

Proof. It is clear from the definitions that $v_f(\widetilde{p}) = \mathrm{Int}(\widetilde{\mathcal{A}})$. That this number is the maximum valuation $v_f(p)$ as claimed follows as in the proof of [14, Theorem 5.1], where the case $d = n-1$ is treated. □

Notation 5.5. In the situation of the lemma, we write $o(\Gamma, d) = v_f(\tilde{p})$. In case $d = n-1$, we abbreviate

$$\mathrm{Int}_i = \mathrm{Int}(\{1, \dots, i-1, i+1, \dots, n\}) = \sum_{j \neq i} v(\gamma_i - \gamma_j).$$

Example 5.6. Let $f = (Y^2 + 2X^3) + Y^3 \in \mathbb{Q}[X, Y]$. The Puiseux expansions of f are

$$\begin{aligned}
\gamma_1 &= a_1 X^{3/2} + X^3 + \dots\ ,\\
\gamma_2 &= a_2 X^{3/2} + X^3 + \dots\ ,
\end{aligned}$$

$$\gamma_3 = -1 - 2X^3 + \dots ,$$

where a_1, a_2 are the roots of $X^2 = -2$. Then $\mathrm{Int}_1 = 3/2 + 0 = 3/2$, $\mathrm{Int}_2 = 3/2 + 0 = 3/2$, and $\mathrm{Int}_3 = 0 + 0 = 0$, so that both $i = 1$ and $i = 2$ maximize the valuation. Taking $i = 1$, we get $\widetilde{p} = (Y - \gamma_2)(Y - \gamma_3)$ and $o(\Gamma, 2) = e(\widetilde{p}) = \lfloor 3/2 \rfloor = 1$.

Example 5.7. Let $f = (Y^3+X^8)(Y^6+Y^3X^7-2Y^3X^4+X^8)+X^{20} \in \mathbb{Q}[X, Y]$ be the polynomial from Example 4.10. The Puiseux expansions of f at $X = 0$ are

$$\gamma_1 = -X^{8/3} + \dots, \qquad \gamma_2 = \xi_1 X^{8/3} + \dots, \qquad \gamma_3 = \xi_2 X^{8/3} + \dots,$$

$$\begin{aligned} \gamma_4 &= X^{4/3} + \xi_3 X^{17/6} + \dots, & \gamma_7 &= X^{4/3} + \xi_4 X^{17/6} + \dots, \\ \gamma_5 &= -\xi_1 X^{4/3} + \xi_5 X^{17/6} + \dots, & \gamma_8 &= -\xi_1 X^{4/3} + \xi_6 X^{17/6} + \dots, \\ \gamma_6 &= -\xi_2 X^{4/3} + \xi_7 X^{17/6} + \dots, & \gamma_9 &= -\xi_2 X^{4/3} + \xi_8 X^{17/6} + \dots \end{aligned}$$

where ξ_1, ξ_2 are the complex roots of $X^3 + 1 = 0$; ξ_3, ξ_4 are the roots of $X^2 + 1/9 = 0$; ξ_5, ξ_6 are the roots of $X^2 + 1/9\xi_1 - 1/9 = 0$ and ξ_7, ξ_8 are the roots of $X^2 + 1/9\xi_2 - 1/9 = 0$.

Then $\mathrm{Int}_1 = \mathrm{Int}_2 = \mathrm{Int}_3 = 2 \cdot 8/3 + 6 \cdot 4/3 = 40/3$ and $\mathrm{Int}_4 = \mathrm{Int}_5 = \mathrm{Int}_6 = \mathrm{Int}_7 = \mathrm{Int}_8 = \mathrm{Int}_9 = 3 \cdot 4/3 + 17/6 + 4 \cdot 4/3 = 73/6$. We conclude that $o(\Gamma, 8) = \lfloor 40/3 \rfloor = 13$.

Remark 5.8. In general, applying the trace map as in the proof of [14, Theorem 5.1], we see from Lemma 5.4 that for each d, we may characterize the number $o(\Gamma, d)$ also as the maximal valuation $v_f(p)$, for $p \in K[X][Y]$ monic in Y of degree d. Note that by construction,

$$o(\Gamma, 1) \leq \cdots \leq o(\Gamma, n-1).$$

The reason for considering the valuations $v_f(p)$ is that they are directly related to integrality:

Lemma 5.9. *Let $p \in K[X, Y] = K[X][Y]$ be monic in Y of degree d. Then the integer part $\lfloor v_f(p) \rfloor$ of $v_f(p)$ is the integrality exponent of p with respect to f, that is, it is the maximum number $e \in \mathbb{N}$ such that $p(x, y)/x^e$ is integral over $A = K[x, y]$.*

Proof. Note that $p(x, y)/x^e$ is integral over A iff $v_{\gamma_i}(p(x, y)/x^e) \geq 0$ for each $1 \leq i \leq n$ (see [12, Theorem 3.2.6] and [14, Section 2.4]). Since $v_f(p)$ is defined to be the minimum of the $v_{\gamma_i}(p)$, the result follows. □

Taking Remark 5.8 into account, we conclude that $o(\Gamma, d)$ is the *maximal integrality exponent of f in degree d*, as defined in Definition 4.4. We note

$$E(f) := o(\Gamma, d-1),$$

the *maximal integrality exponent of f*.

5.2. **Computation of the maximum integrality exponent e.** Denote by $\gamma_1(X), \ldots, \gamma_n(X)$ the Puiseux expansions of f at $X = 0$. As noted in [14, Theorem 5.1], if we allow for a more general $\tilde{p} \in \mathcal{P}_X[Y]$ which is a polynomial in Y with coefficients in Puiseux series in X, the maximal integrality exponent can be obtained by choosing $\{\eta_1(X), \ldots, \eta_{n-1}(X)\}$ to be a subset of $\{\gamma_1(X), \ldots, \gamma_n(X)\}$. In that paper it is also explained how to determine which subset to take (see also Section 5.1).

The coefficients of $\tilde{p}$ may not lie in the ground field K, and furthermore $\tilde{p}$ may contain fractional exponents. As mentioned before, by using the trace map, van Hoeij proves that there exists $p \in K[X, Y]$ monic of Y–degree $n-1$ with $e(p) = e(\tilde{p})$.

In [14] these ideas are only used to fix bounds for the algorithm but not for constructing p. In this work, we show that p can be easily constructed, using Hensel's Lemma to efficiently compute the product $(Y-\eta_1(X)) \cdots (Y-\eta_{n-1}(X))$, or more precisely, the product of the truncated expansions of these factors up to appropriate degrees.

5.3. **Hensel's Lemma.** In this subsection and the following, we explain how to use Hensel's lemma to compute the products $(Y - \gamma_1) \cdots (Y - \gamma_s)$ up to any X–degree, with $\gamma_1, \ldots, \gamma_s$ conjugate expansions belonging to a Puiseux segment or block, without computing each individual expansion. Computing all the expansions separately and then computing the product is usually much slower.

We recall Hensel's Lemma.

Lemma 5.10. *Let $f \in K[[X]][Y]$ be a monic polynomial over the power series ring, and assume that $f(0, Y) = g_0 h_0$ for monic polynomials $g_0, h_0 \in K[Y]$ such that $\langle g_0, h_0 \rangle = K[Y]$. Then there exist monic polynomials $g, h \in K[[X]][Y]$ such that*

(1) $f = gh$
(2) $g(0, Y) = g_0$, $h(0, Y) = h_0$.

Moreover, for each $m \in \mathbb{N}$, there exist unique $g_m, h_m \in K[X, Y]$ of X–degree m such that

(1) $f \equiv g_m h_m$ in $(K[[X]]/\langle X^{m+1} \rangle)[Y]$
(2) $g_m \equiv g_i$, $h_m \equiv h_i$ in $(K[[X]]/\langle X^{i+1} \rangle)[Y]$, $i = 0, \ldots, m-1$.

These last conditions imply that the polynomials g_m and h_m can be computed inductively along the X–degree, solving for each m a determined system of linear equations of n equations and n unknowns, where n is the Y–degree of f. (For each i, $0 \leq i \leq n-1$, we get an equation by comparing the coefficients of $X^m Y^i$ in f and in $g_m h_m$.) For further reference in the paper, we present this well-known procedure as Algorithm 1, omitting the actual computation steps. (This algorithm has been made available in SINGULAR since version 3.1.3 via the command `factmodd`.)

We will usually use Hensel's lifting to separate the component that vanishes at the origin from the component that vanishes outside. Alternatively, we could perform this decomposition by means of the Weierstrass Division Theorem. (See for example, [4, Theorem 3.2.3].) However, the use of Hensel's Lemma allows for more generality, since we do not need to move the singularity to the origin. This is particularly useful when the singularity

Algorithm 1 Hensel's lifting

Input: $f \in K[X,Y]$ irreducible polynomial, monic in Y; $g_0, h_0 \in K[Y]$ such that $f(0,Y) = g_0 h_0$ and $\langle g_0, h_0 \rangle = K[Y]$; $d \in \mathbb{N}_0$

Output: $g, h \in K[X,Y]$ such that $g(0,Y) = g_0$, $h(0,Y) = h_0$ and $f \equiv gh$ in $(K[[X]]/\langle X^{d+1} \rangle)[Y]$

has no rational coordinates, as we avoid to use algebraic extensions. Also the linear algebra techniques involved in Hensel's Lemma are usually faster than computing division of polynomials with remainders.

In the following example, we show how to use the lemma to decompose a polynomial and compute the integral basis in a simple case.

Example 5.11. Let $f = (Y-X)(Y+X)(Y+2X)+Y^7$. There are 3 Puiseux expansions at $Y = 0$ and 4 expansions outside $Y = 0$. (The degree of f in Y is 7, so there must be a total of 7 expansions.)

We call $\gamma_1 = X + \ldots, \gamma_2 = -X + \ldots, \gamma_3 = -2X + \ldots$ the expansions at the origin and $\gamma_4, \ldots, \gamma_7$ the expansions outside the origin. We want to compute $(Y-\gamma_4)\cdots(Y-\gamma_7)$ up to a given degree in X without computing each expansion separately.

Here $\mathrm{Int}_i = 2$ for $i = 1, 2, 3$ and this is maximal. So $e(\tilde{g}) = 2$ and we need to compute the product up to degree 2 in X.

Since $f(0,Y) = Y^3 + Y^7$, we take $g_0 = Y^3$, $h_0 = 1 + Y^4$, and apply Hensel's lemma to lift these factors up to degree 2. We obtain $g_2 = Y^3 + 2XY^2 - 2X^2Y$ and $h_2 = 5X^2Y^2 - 2XY^3 + Y^4 + 1$, and we conclude that $(Y-\gamma_4)\cdots(Y-\gamma_7) \equiv 5X^2Y^2 - 2XY^3 + Y^4 + 1$ modulo X^3.

Taking $i = 1$, to compute p, we still have to compute γ_2 and γ_3 up to degree 2. We obtain $\bar{\gamma}_2 = -X$ and $\bar{\gamma}_3 = -2X$. Combining all this we compute

$$p = \prod_{i=2}^{7} (Y - \bar{\gamma}_i) = (Y-X)(Y+X)(Y+2X)(5X^2Y^2 - 2XY^3 + Y^4 + 1).$$

5.4. **A local version of Hensel's Lemma.** When we want to lift two factors g, h that vanish at $Y = 0$ (for example, to compute $(Y-\gamma_1)(Y-\gamma_2)(Y-\gamma_3)$ as in Example 4.10 up to any given order), the condition $\langle g(0,Y), h(0,Y) \rangle = K[Y]$ is not satisfied.

We explain how to transform the polynomials so that Hensel's lemma can still be applied.

Let f have the following Puiseux expansions at 0:

$$\begin{aligned} \gamma_1 &= a_1^1 X^{t_1^1} + a_2^1 X^{t_2^1} + \ldots \\ \gamma_2 &= a_1^2 X^{t_1^2} + a_2^2 X^{t_2^2} + \ldots \\ &\ldots \\ \gamma_s &= a_1^s X^{t_1^s} + a_2^s X^{t_2^s} + \ldots \end{aligned}$$

and assume $t = t_1^1 = \min_{1 \le i \le s} t_1^i$. We define $f_0 = (Y-\gamma_1)\ldots(Y-\gamma_s)$, $f_0 \in K[[X]][Y]$.

We would like to replace Y by $X^t Y$, so that we can factor out X^t in all factors. But this will introduce fractional exponents in f_0, so we first write

$t = u/v$ and replace X by X^v and Y by X^uY. We define

$$\begin{aligned}\tilde{f}_0(X,Y) &= f_0(X^v, X^uY)\\ &= (X^uY - (a_1^1 X^{vt_1^1} + \dots)) \cdots (X^uY - (a_1^s X^{vt_1^s} + \dots)\\ &= X^{su}(Y - (a_1^1 + a_2^1 X^{\tilde{t}_2^1} + \dots)) \cdots (Y - (a_1^s X^{\tilde{t}_1^s} + \dots))\end{aligned}$$

and

$$\begin{aligned}F(X,Y) &= \tilde{f}_0(X,Y)/X^{su}\\ &= (Y - (a_1^1 + a_2^1 X^{\tilde{t}_2^1} + \dots)) \cdots (Y - (a_1^s X^{\tilde{t}_1^s} + \dots)),\end{aligned}$$

with $F(X,Y) \in K[[X]][Y]$.

So we can first use Hensel's lemma to compute the factor f_0 up to the required degree, and then compute F as defined above.

Now F has factors that do not vanish at the origin. So we can use again Hensel's lemma to separate the factors that vanish at the origin from the factors that do not. We get $F = GH$. We obtain the factors g and h by reversing the transformations, $g(X,Y) = G(X^{1/v}, Y/X^{u/v})$, and likewise for h.

We thus arrive to Algorithm 2.

Algorithm 2 Segment splitting

Input: $f \in K[X,Y]$ irreducible polynomial, monic of degree s in Y, with no Puiseux expansions vanishing outside the origin; $d \in \mathbb{N}_0$.

Output: $g_1, \dots, g_k \in K[X,Y]$ such that the expansions of g_i correspond to the i-th Puiseux segment of f, developed up to degree d.

1: $t_1, \dots, t_k$ the different initial exponents of the Puiseux expansions of f (which are obtained from the Newton polygon of f)
2: **if** $k = 1$ **then**
3: **return** f
4: $t = u/v = \min\{t_1, \dots, t_k\}$, with $u, v \in \mathbb{N}$
5: $\tilde{f}(X,Y) = f(X^v, X^uY)$
6: $F = \tilde{f}/X^{su}$
7: Compute $G_0, H_0 \in K[Y]$ such that $F(0,Y) = G_0H_0$, $G_0 = Y^w$, for some $w \in \mathbb{N}$ and $Y \nmid H_0$
8: $(G,H) = \text{Hensel}(F, G_0, H_0, vd)$
9: $g_1 = G(X^{1/v}, Y/X^{u/v})$, $h = G(X^{1/v}, Y/X^{u/v})$
10: **return** $\{g_1\} \cup \text{SegmentSplitting}(h)$.

See also [4, Theorem W] for an alternative approach extending the Weierstrass Division Theorem.

Example 5.12. We return to Example 4.10, $f = Y^6 - (Y^2 + 2X^3)((Y + 2X^2)^2 + X^5)$. We want to compute $(Y - \gamma_1)(Y - \gamma_2)$ up to order 5. We first use Hensel's lemma to lift the factors Y^4 and $1 + Y^2$ up to degree 8 (we must lift up to this degree so that no information from f is lost). We obtain

$$\begin{aligned}f_0 &= 48X^8Y^3 + 46X^8Y^2 - 8X^7Y^3 - 16X^8Y - 8X^7Y^2 + 32X^6Y^3 + 2X^8 - 4X^6Y^2\\ &\quad - 8X^5Y^3 + 8X^7 + X^5Y^2 + 8X^5Y + 4X^4Y^2 + 2X^3Y^2 + 4X^2Y^3 + Y^4\\ f_1 &= -48X^8Y + 210X^8 + 8X^7Y - 56X^7 - 32X^6Y + 4X^6 + 8X^5Y - X^5 + 12X^4 - 2X^3 - 4X^2Y + Y^2 - 1\end{aligned}$$

(Note that $f_1 = (Y - \gamma_5)(Y - \gamma_6)$ up to order 8, so we can truncate it up to order 5 to get the product of the expansions outside the origin.)

The smallest t is $t = u/v = 3/2$. We compute $\tilde{f}_0 = f_0(X^2, X^3Y) = X^{12}(48X^{13}Y^3 - 8X^{11}Y^3 + 46X^{10}Y^2 + 32X^9Y^3 - 8X^8Y^2 - 8X^7Y^3 - 16X^7Y - 4X^6Y^2 + X^4Y^2 + 2X^4 + 4X^2Y^2 + 4XY^3 + Y^4 + 8X^2 + 8XY + 2Y^2) = X^{12}F(X, Y)$.

Now, $F(0, Y) = (Y^2 + 2)Y^2$ and we use Hensel's lemma to lift the factors $Y^2 + 2$ and Y^2. After lifting and mapping the factors back to the original X and Y, we obtain

$$g = -4X^6 - 8X^5Y + 2X^3 + Y^2$$
$$h = X^5 + 4X^4 + 4X^2Y + Y^2$$

Note that $g = (Y^2 + 2X^3) - 8X^5Y - 4X^6$ and $h = (Y + 2X^2)^2 + X^5$ are equal in the low degree terms to the factors appearing in f.

We can now compute $p = (Y - \bar{\gamma}_1)(Y - \bar{\gamma}_2)(Y - \bar{\gamma}_4)(Y - \bar{\gamma}_5)(Y - \bar{\gamma}_6) = ((Y^2 + 2X^3) - 8X^5Y - 4X^6)Y(8X^5Y - X^5 + 12X^4 - 2X^3 - 4X^2Y + Y^2 - 1)$.

To separate all the Puiseux segments, we can use this method iteratively. In each step we separate the segment with smallest initial exponent from the rest. Now consider blocks inside a segment which have the same initial exponents but whose initial terms are not conjugate. In this case we can also use Hensel's lemma to split the blocks after applying the above transformation, hence we can still proceed in the same way.

To be able to separate all blocks, it remains to consider the separation of blocks that have the same initial rational term (and therefore the same initial exponent). Suppose that f_1 is a factor of f containing some Puiseux blocks of f such that they all have the same initial terms $\eta = a_1X^{m_1} + \cdots + a_kX^{m_k}$, $a_i \in K, m_k \in \mathbb{N}_0$. (There can be fewer terms than in the rational part of the expansions.) In this case, we first apply the transformation $Y = Y_1 + \eta$, and compute $f_2(X, Y_1) = f_1(X, Y_1 + \eta)$. Then f_2 will contain the same expansions as f_1 but without the initial terms η. We can now proceed as before to separate the blocks. After computing the factors corresponding to each block, we replace Y_1 by $Y - \eta$, to get the factor we were looking for.

Algorithm 3 summarizes these ideas.

The ideas from [4, Theorem 5.1.20] can in some cases also be used for our purpose. However, the cited theorem is not as general as we require, and the details on how to initiate the algorithm are not given.

Our final goal is to separate all factors corresponding to different conjugacy classes of expansions. In this case, we do not know of any algorithm to do it without working in algebraic extensions. We compute the conjugate Puiseux expansions $\bar{\gamma}_1, \ldots, \bar{\gamma}_s$ up to the desired degree and then compute the product $(Y - \bar{\gamma}_1) \cdots (Y - \bar{\gamma}_s)$. This last step is only needed when a Puiseux block contains more than one conjugacy class of expansions.

In Algorithm 4 we combine all the contents of this subsection in a general splitting algorithm.

5.5. **Local integral basis.** Let $g \in K[[X]][Y]$ be an irreducible Weierstrass polynomial of degree m. We show how to compute the integral basis for

Algorithm 3 Block splitting

Input: $f \in K[X,Y]$ irreducible polynomial, monic of Y–degree n; $d \in \mathbb{N}_0$.
Output: $f_0, f_1, \ldots, f_r$ such that the expansions of each f_i are the same as the i-th Puiseux block of f up to order d in X.

compute $g_0, h_0 \in K[Y]$ such that $g_0 h_0 = f(0,Y)$, $g_0 = Y^k$ for some $k \in \mathbb{N}_0$ and $\langle g_0, h_0 \rangle = K[Y]$
$(f_0, g) = \text{Hensel}(f, g_0, h_0, d)$, where f_0 is the lifting of h_0 and g is the lifting of g_0, up to order d in X
$\{g_1, \ldots, g_s\} = \text{SegmentSplitting}(g, d)$, the factors corresponding to the different Puiseux segments of g
for all g_i, $i = 1, \ldots, s$ **do**
    $\eta_i :=$ the common rational part of all expansions in g_i
    $\tilde{g}_i = g_i(X, Y + \eta_i)$
    $\{\tilde{g}_{i,1}, \ldots, \tilde{g}_{i,r_i}\} = \text{BlockSplitting}(\tilde{g}_i, d)$
    $g_{i,j}(X,Y) = \tilde{g}_{i,j}(X, Y - \eta_i)$, $j = 1, \ldots, r_i$
$\{f_1, \ldots, f_r\} = \cup_{i=1}^{s} \{g_{i,1}, \ldots, g_{i,r_i}\}$
return $\{f_0, f_1, \ldots, f_r\}$

Algorithm 4 Splitting

Input: $f \in K[X,Y]$ irreducible polynomial, monic of Y-degree n; $e \in \mathbb{N}_0$.
Output: $L = \{f_0, f_1, \ldots, f_r\}$ such that the expansions of each f_i are the same as the i-th conjugacy class of Puiseux expansions of f up to order e in X.

compute $\{g_0, g_1, \ldots, g_s\} = \text{BlockSplitting}(f, e)$
$L = \{g_0\}$
for $i = 1, \ldots, s$ **do**
    Compute $\Gamma = \{\gamma_1, \ldots, \gamma_l\}$, the singular part of the expansions of g_i
    $k =$ number of conjugacy classes in Γ
    if $k > 1$ **then**
        for $j = 1, \ldots, k$ **do**
            Compute $\Gamma_j = \{\gamma_{j,1}, \ldots, \gamma_{j,s_j}\}$, the expansions of the j-th conjugacy class of Γ, up to order e in X
            $h_j = (Y - \gamma_{j,1}) \cdots (Y - \gamma_{j,s_j})$
        $L = L \cup \{h_1, \ldots, h_k\}$
    else
        $L = L \cup \{g_i\}$
return L.

$\overline{K[[X]][Y]/\langle g \rangle}$ over $K[[X]]$. That is, we compute the polynomials $p_1, \ldots, p_{m-1}$ described in Lemma 4.5 and their corresponding integrality exponents.

For each d, $0 \leq d \leq m-1$, we look for a polynomial $p_d \in K[X][Y]$ of degree d with maximal valuation at g.

Let Γ be the set of Puiseux expansions of g. Since we are assuming g is irreducible, all the expansions of g are conjugate.

For any $d \in \mathbb{N}_0$, $0 \leq d < m$, we define

$$o(\Gamma, d) = \max_{\substack{N \subset \Gamma \\ \#N = d}} \left\{ v_g \left(\prod_{\eta \in N} (Y - \eta) \right) \right\}.$$

Recall that for a given $N \subset \Gamma$, we have the formula

$$v_g \left(\prod_{\eta \in N} (Y - \eta) \right) = \min_{\delta \in \Gamma \setminus N} \left\{ \sum_{\eta \in N} v(\delta - \eta) \right\}.$$

To compute $o(\Gamma, d)$, $1 \leq d < m$, we do not apply the above formulas but we compute a polynomial $p_d \in K[X, Y]$ of Y–degree d such that $v_g(p_d) = o(\Gamma, d)$, recursively truncating the expansions of g.

We assume first that there exists $t \in \mathbb{Q}$ such that the conjugated expansions $\gamma_1, \ldots, \gamma_m$ of g agree in the terms of degree lower than t and have conjugate coefficients $c_i \in \overline{K}$ at the monomial X^t, that is

$$\gamma_i = a_1 X^{d_1} + a_2 X^{d_2} + \cdots + a_k X^{d_k} + c_i X^t + \ldots$$

where $a_j \in K$ and $d_j \in \mathbb{N}$ for $1 \leq j \leq k$. That is, the inital part $a_1 X^{d_1} + a_2 X^{d_2} + \cdots + a_k X^{d_k}$ is rational. To compute the numerator of the element of degree d in the integral basis, we truncate γ_i to $\bar{\gamma}_i$ for $1 \leq i \leq d$ to degree d_k and we set

$$p_d = (Y - \bar{\gamma}_1) \cdots (Y - \bar{\gamma}_d) \in K[X, Y]$$

Lemma 5.13. *The polynomial p_d defined above have maximal integrality exponents among all monic polynomials of degree d in Y.*

Proof. Let $\tilde{p}_d \in \mathcal{P}_X[y]$ be an element of degree d in Y of largest valuation e_d at g. We know that we can take $\tilde{p}_d = (Y - \gamma_{i_1}) \ldots (Y - \gamma_{i_d})$ for some $1 \leq i_1 \leq \cdots \leq i_d \leq m$. Let i' be an index not appearing in $\{i_1, \ldots, i_d\}$. We have by construction

$$v_g(\tilde{p}_d) = v_{\gamma_{i'}}(\tilde{p}_d) = \sum_{j=1}^{d} v(\gamma_{i'} - \gamma_j) = \sum_{j=1}^{d} v(\gamma_{i'} - \bar{\gamma}_j) = v_{\gamma_{i'}}(p_d).$$

Since $\gamma_1, \ldots, \gamma_s$ are conjugate and $p_d \in K[X, Y]$, $v_{\gamma_j}(p_d) = v_{\gamma_{i'}}(p)$ for $1 \leq j \leq m$.

Recall that $v_g(p_d) = \min_{1 \leq j \leq s} v_{\gamma_j}(p_d)$. So $v_g(p_d) = v_g(\tilde{p}_d)$, as wanted. □

In the general case, the truncation has to be done iteratively. We describe a recursive process to obtain p_d, the numerator of the integral basis of degree d in Y.

Let $\tilde{p}_d \in \mathcal{P}_X[y]$ be as in Lemma 5.13.

The singular parts

$$\gamma_j^{\text{sing}} = a_1^j X^{t_1} + \cdots + a_k^j X^{t_k},\ t_1 < \ldots < t_k$$

of the expansions γ_j, $1 \leq j \leq m$, are pairwise different and algebraically conjugate over $K((X))$.

Since $\gamma_1^{\text{sing}} \neq \gamma_j^{\text{sing}}$, if we truncate the expansions γ_j, $1 \leq j \leq m$, to degree t_{k-1}:

$$\gamma_j^{(1)} = a_1^j X^{t_1} + \cdots + a_{k-1}^j X^{t_{k-1}}$$

and define

$$\tilde{q} = \prod_{j=1}^{d}(Y - \gamma_{i_j}^{(1)}),$$

we have

$$v_{\gamma_{i'}}(\tilde{q}) = v_{\gamma_{i'}}(\tilde{p_d}).$$

for any $i' \notin \{i_1, \ldots, i_d\}$. That is, the valuation at $\gamma_{i'}$ does not decrease.

For simplicity, we explain first how to compute recursively the element of degree $m-1$, assuming $\tilde{p}_{m-1} = (Y - \bar{\gamma}_2)\cdots(Y - \bar{\gamma}_m)$.

For the recursion, we define $g_0 = \prod_{j=1}^{m}(Y - \gamma_j)$ and $\overline{g_0} = \prod_{j=1}^{m}(Y - \gamma_j^{(1)})$. Since t_k was the smallest integer for which all the truncated expansions were different, the expansions $\gamma_j^{(1)}$, $1 \le j \le m$, can now be grouped into sets of identical expansions, each set having the same number of elements. Denote by $\eta_1, \ldots, \eta_r$ the mutually distinct expansions, and set $g_1 = (Y - \eta_1)\cdots(Y - \eta_r) \in K[X, Y]$. By construction $\overline{g_0} = g_1^{u_1}$, with $u_1 = s/r \in \mathbb{N}$.

We start the i-th step by applying the whole procedure inductively to g_{i-1}, computing $\overline{g_{i-1}}$, g_i and u_i such that $\overline{g_{i-1}} = g_i^{u_i}$ and $\overline{g_{i-1}}$ comes from truncating the expansions of g_{i-1}. In each step the degree r_i of g_i is smaller or equal than the degree r_{i-1} of g_{i-1}, and it will be equal to 1 after a finite number w of steps (bounded by the degree t_k of the expansions in g_0). For that value w, $r_w = 1$ and all the expansions in g_w are equal. The desired polynomial is

$$p_{s-1} = g_1^{u_1 - 1} g_2^{u_2 - 1} \cdots g_w^{u_w - 1} \in K[X, Y].$$

We obtain Algorithm 5.

Algorithm 5 Truncated Factor

Input: $\Delta = \{\gamma_i = a_1^{(i)} X^{t_1} + \cdots + a_k^{(i)} X^{t_k}\}_{1 \le i \le m}$, a conjugacy class of Puiseux series of finite length.

Output: $q \in K[X, Y]$ of degree $m-1$ in Y such that $v_{\gamma_1}(q) = v_{\gamma_1}(\tilde{q})$, with $\tilde{q} = (Y - \gamma_2)\cdots(Y - \gamma_m)$.

```
Set η_1, ..., η_r the different expansions in the set {γ̄_1^{t_{k-1}}, ..., γ̄_s^{t_{k-1}}}
p = (Y − η_1) ··· (Y − η_r)
u = s/r
if r > 1 then
    p' = TruncatedFactor({η_1, ..., η_r})
    return q = p^{u−1} p'.
else
    return q = p^{u−1}.
```

Lemma 5.14. *With notation as above, let p_{m-1} = TruncatedFactor$(\gamma_1, \ldots, \gamma_m)$. Then p_{m-1} has maximal valuation at g over all monic polynomials of degree $m-1$ in Y.*

Proof. As in the proof of Lemma 5.13, it is enough to show that $v_{\gamma_1}(p_{m-1}) = v_{\gamma_1}(\tilde{p}_{m-1})$. Let $\overline{\gamma_2}, \ldots, \overline{\gamma_m}$ be the Puiseux expansions of p_{m-1}, corresponding to truncations of the expansions $\gamma_2, \ldots, \gamma_m$ of g. By construction, $v(\gamma_1 - \overline{\gamma_i}) = v(\gamma_1 - \gamma_i)$ for $i = 2, \ldots, m$. Hence $v_g(p_{m-1}) = v_{\gamma_1}(p_{m-1}) = v_{\gamma_1}(\tilde{p}_{m-1}) = v_g(\tilde{p}_{m-1})$ as wanted. □

Example 5.15. Returning to Example 5.2, the singular parts of the Puiseux expansions are

$$\begin{aligned}
\gamma_1^{\text{sing}} &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} + 1/4iX^2 \\
\gamma_2^{\text{sing}} &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} - 1/4iX^2 \\
\gamma_3^{\text{sing}} &= iX^{3/2} + (1/2i + 1/2)X^{7/4} + 1/4iX^2 \\
\gamma_4^{\text{sing}} &= iX^{3/2} + (1/2i + 1/2)X^{7/4} - 1/4iX^2 \\
\gamma_5^{\text{sing}} &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} + 1/4iX^2 \\
\gamma_6^{\text{sing}} &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} - 1/4iX^2 \\
\gamma_7^{\text{sing}} &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} + 1/4iX^2 \\
\gamma_8^{\text{sing}} &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} - 1/4iX^2
\end{aligned}$$

with $i^2 = -1$.

Truncating γ_i^{sing} to degree $7/4$ we obtain

$$\begin{aligned}
\overline{\gamma_1}^{7/4} = \overline{\gamma_2}^{7/4} &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} \\
\overline{\gamma_3}^{7/4} = \overline{\gamma_4}^{7/4} &= iX^{3/2} + (1/2i + 1/2)X^{7/4} \\
\overline{\gamma_5}^{7/4} = \overline{\gamma_6}^{7/4} &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} \\
\overline{\gamma_7}^{7/4} = \overline{\gamma_8}^{7/4} &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4}
\end{aligned}$$

hence $u_1 = 2$ and

$$\begin{aligned}
g_1 &= (Y - \overline{\gamma_1}^{7/4})(Y - \overline{\gamma_3}^{7/4})(Y - \overline{\gamma_5}^{7/4})(Y - \overline{\gamma_7}^{7/4}) \\
&= Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7
\end{aligned}$$

Applying the whole procedure inductively to g_1 we obtain $g_2 = Y^2 + X^3$, $u_2 = 2$ and $g_3 = Y$, $u_3 = 2$. Combining the factors, we get

$$g = g_1^{u_1-1} g_2^{u_2-1} g_3^{u_3-1} = \left(Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + \frac{1}{4}X^7\right)(Y^2 + X^3)Y.$$

For computing the elements of any degree d, $1 \leq d \leq m-1$, we can easily extend the above construction. We getAlgorithm 6.

Lemma 5.16. *Let $g \in K[[X]][Y]$ be a Weierstrass polynomial of degree m in Y . Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be the expansions of g at the origin, which correspond all to the same conjugacy class. Then, for any c, $1 \leq c < m$, the output $p_c =$ `TruncatedFactorGeneral`(Γ, c) is a polynomial with maximal valuation at the origin in the ring $K[[X]][Y]/\langle g \rangle$ among all polynomials in $K[X, Y]$ monic of degree c in Y.*

Proof. Let $\bar{\gamma}_1, \ldots, \bar{\gamma}_s$ be the singular part of the expansions in Γ. Let t_k be the degree in X of these expansions. Let $g_0, \overline{g_0}, \ldots, g_{w-1}, \overline{g_{w-1}}, g_w$ be defined as before.

We have noted in Section 5.2 that a polynomial p_d satisfying the requirements of the lemma can be chosen so that all the Puiseux expansions of p_d at the origin are truncations of the expansions in Γ. This implies that we can take p_d to be a product $p_d = g_1^{d_1} \ldots g_w^{d_w}$ of the polynomials g_i with appropriate exponents. To find the exponents, we note that for all i the

polynomials $g_{i+1}^{u_{i+1}}$ and g_i have the same degree, but the valuation of g_i at g is larger than the valuation of $g_{i+1}^{u_{i+1}}$ (since the expansions are developed up to a larger degree). Hence, to construct p_d, we must first take d_1 as large as possible. Then maximize d_2 and so on iteratively. This is done by Algorithm 6. □

We can now compute $o(\Gamma, c)$ by the formula

$$o(\Gamma, c) = \sum_{\eta \in N} v(\gamma - \eta),$$

where $N = \{\eta_1, \dots \eta_d\}$ are the expansions appearing in p_d and $\gamma \in \Gamma$. (For any expansion $\gamma \in \Gamma$ the result of the sum is the same, because conjugating the above expression does not modify N.)

Algorithm 6 Truncated Factor General

Input: $\Delta = \{\gamma_i = a_1^{(i)} X^{t_1} + \cdots + a_k^{(i)} X^{t_k}\}_{1 \le i \le s}$, a conjugacy class of Puiseux series of finite length; $c \in \mathbb{N}$, $c < s$.

Output: $p \in K[X, Y]$ of Y–degree c such that $v_{f_\Delta}(p) = v_{f_\Delta}(\tilde{p})$, with $\tilde{p}$ the element in $\mathcal{P}_X[Y]$ of degree c with maximal valuation at f_Δ.

1: Set $\eta_1, \dots, \eta_r$ the different expansions in the set $\{\overline{\gamma_1}^{t_{k-1}}, \dots, \overline{\gamma_s}^{t_{k-1}}\}$
2: $u = \lfloor c/r \rfloor$, $c' = c - ur$
3: $g_1 = \text{TruncatedFactorGeneral}(\{\eta_1, \dots, \eta_r\}, c')$
4: **if** $u > 0$ **then**
5: $\quad g = (Y - \overline{\gamma_1}^{t_{k-1}}) \cdots (Y - \overline{\gamma_d}^{t_{k-1}})$
6: $\quad$ **return** $p = g^u g_1$.
7: **else**
8: $\quad$ **return** $p = g_1$.

Example 5.17. We carry on Example 5.15, computing all the numerators of the elements of the integral basis. We have obtained that the element of the integral basis of degree $m - 1 = 7$ is the product $p_7 = g_1 g_2 g_3$, where g_1, g_2 and g_3 have degrees 4, 2 and 1 respectively. To obtain the numerators of the elements of the integral basis of smaller degree d, $1 \le d \le 6$, following Algorithm 6, we have to first take the largest possible power of g_1 so that the total degree is smaller than or equal to d, then choose the power of g_2 in the same way and finally the power of g_3. We get the following elements $p_6 = g_1 g_2$, $p_5 = g_1 g_3$, $p_4 = g_1$, $p_3 = g_2 g_3$, $p_2 = g_2$ and $p_1 = g_3$.

The denominators are powers of x. To obtain the exponents, we compute $o(\Gamma, d)$ for $1 \le d \le 7$ by looking at the expansions corresponding to each g_i, $i = 1, 2, 3$, given in Example 5.15. Setting N_{g_i} the expansions appearing in g_i, $i = 1, 2, 3$, we have $\sum_{\eta \in N_{g_1}} v(\gamma - \eta) = 27/4$, $\sum_{\eta \in N_{g_2}} v(\gamma - \eta) = 13/4$ and $\sum_{\eta \in N_{g_3}} v(\gamma - \eta) = 3/2$ for any $\gamma \in \Gamma$. Hence $o(\Gamma, 1) = 3/2$, $o(\Gamma, 2) = 13/4$, $o(\Gamma, 3) = 13/4 + 3/2 = 19/4$, $o(\Gamma, 4) = 27/4$, $o(\Gamma, 5) = 27/4 + 3/2 = 33/4$, $o(\Gamma, 6) = 27/4 + 13/4 = 10$ and $o(\Gamma, 7) = 27/4 + 13/4 + 3/2 = 23/2$. The exponents in the denominators are the integer part of these valuations and the integral basis is

$$\left\{ \frac{g_3}{x}, \frac{g_2}{x^3}, \frac{g_2 g_3}{x^4}, \frac{g_1}{x^6}, \frac{g_1 g_3}{x^8}, \frac{g_1 g_2}{x^{10}}, \frac{g_1 g_2 g_3}{x^{11}} \right\}.$$

We have shown how to compute the local integral basis when $g \in K[[X]][Y]$ is an irreducible Weierstrass polynomial. For the general case when g is not irreducible, we add up all the contributions of the branches following Proposition 4.8. We get Algorithm 7.

Algorithm 7 Local integral basis

Input: $L = \{\{\Gamma_1, f_1\}, \ldots, \{\Gamma_r, f_r\}\}$, where $\Gamma_i = \{\gamma_{i,1}, \ldots, \gamma_{i,s_i}\}$ is the set of singular parts of the i-th conjugacy class of expansions that vanish at the origin of a polynomial $f \in K[X,Y]$ monic in Y and f_i is the corresponding factor developed up to X–degree $E(f)$.

Output: $\{(p_0,e_0), \ldots, (p_m,e_m)\}$ such that $\{\frac{p_0}{x^{e_0}}, \ldots, \frac{p_{m-1}}{x^{e_{m-1}}}\}$ is the local integral basis at the origin and $(p_m,e_m) = (f,\infty)$.

1: $m = \deg_Y(f_1 \cdots f_r)$
2: **for** $i = 1, \ldots, r$ **do**
3: $\quad h = \prod_{j \neq i} f_j$
4: $\quad$ **for** $j = 0, \ldots, m - s_i - 1$ **do**
5: $\quad\quad p_j = Y^j$, $e_j =$ the integrality exponent of p_j
6: $\quad$ **for** $c = 0, \ldots, s_i - 1$ **do**
7: $\quad\quad q_c = \text{TruncatedFactorGeneral}(\Gamma_i, c)$
8: $\quad\quad p_{m-s+c} = h \cdot q_c$, $e_{m-s+c} =$ the integrality exponent of p_{m-s+c}
9: $\quad A^{(i)} = \left\langle \frac{p_0}{x^{e_0}}, \frac{p_1}{x^{e_1}}, \ldots, \frac{p_{m-1}}{x^{e_{m-1}}} \right\rangle_{K[x]}$
10: From $A^{(1)} + \cdots + A^{(r)}$, compute the integral basis $\{b_0, \ldots, b_{m-1}\}$, as explained in Section 2
11: **return** $\{(p_0,e_0), \ldots, (p_m,e_m)\}$, where p_i the denominator of b_i and e_i the exponent of the numerator for $0 \leq i \leq m-1$ and $(p_m,e_m) = (f,\infty)$.

Example 5.18. Let $f = (Y^3 + X^8)(Y^6 + Y^3X^7 - 2Y^3X^4 + X^8) + X^{20} \in \mathbb{Q}[X,Y]$, from Example 4.10, and $A = K[X,Y]/\langle f \rangle$.

As we have seen in Example 5.7, the maximal integrality exponent is $e = 13$.

We have two conjugacy classes, $\Gamma_1 = \{\gamma_i : i = 1,2,3\}$ and $\Gamma_2 = \{\gamma_i : i = 4, \ldots, 9\}$, so we compute two local rings $A^{(1)}$ and $A^{(2)}$.

For $A^{(1)}$, the development of $(Y - \gamma_4) \ldots (Y - \gamma_9)$ up to order 13 in X is $h_1 = Y^6 + Y^3X^7 - 2Y^3X^4 + X^8$ (we omit the details of this computation which can be done using Hensel's lemma). Since $n - s_1 - 1 = 9 - 3 - 1 = 5$, the first 5 numerators of the integral basis are the powers of y. For $c = 0,1,2$, the truncated factors corresponding to Γ_1 are $1, Y, Y^2$. Therefore, the numerators of the generators of $A^{(1)}$ are $1, y, y^2, y^3, y^4, h_1, h_1y, h_1y^2$. Computing the integrality exponents, we get the integral basis

$$A^{(1)} = \left\langle 1, y, y^2, y^3, y^4, y^5, \frac{h_1}{x^8}, \frac{h_1 y}{x^{10}}, \frac{h_1 y^2}{x^{13}} \right\rangle_{K[x]}.$$

Similarly, for $A^{(2)}$, the development of $(Y - \gamma_1)(Y - \gamma_2)(Y - \gamma_3)$ up to degree 13 is $h_2 = Y^3 + x^8$. Now $n - s_2 - 1 = 9 - 6 - 1 = 2$ and the first numerators of the integral basis are $1, y, y^2$. For $c = 0, \ldots, 5$, the truncated factors corresponding to Γ_2 are $1, Y, Y^2, Y^3 - X^4, (Y^3 - X^4)Y, (Y^3 - X^4)Y^2$.

Computing the integrality exponents, we get

$$A^{(2)} = \left\langle 1, y, y^2, \frac{h_2}{x^4}, \frac{h_2 y}{x^5}, \frac{h_2 y^2}{x^6}, \frac{h_2(y^3-x^4)}{x^9}, \frac{h_2(y^3-x^4)y}{x^{10}}, \frac{h_2(y^3-x^4)y^2}{x^{10}} \right\rangle_{K[x]}.$$

The normalization of the local ring is $A^{(1)} + A^{(2)}$.

We finish this section with a special algorithm for the case of simple singularities.

Lemma 5.19. *Let $f \in K[[x]][y]$ be an irreducible Weierstraß polynomial with respect to y and $\deg_y f = n$. Let $y(x)$ be a Puiseux expansion, and $y(x) = \sum_{i \geq m} a_i x^{\frac{i}{n}}$, $a_m \neq 0$, $m > n$ and $\gcd(m,n) < n$. Let $k_0 = n$, $k_1 = m$, $k_2, \ldots, k_g$ be the characteristic exponents and let ε be a primitive root of unity. The following holds (cf.* [4, Lemma 5.2.18(1)] *and the proof thereof):*

(1) $f = \prod_{i=1}^{n} (y - y(\varepsilon^i x))$

(2) For $j = 1, \ldots, g$ denote by N_j the set of all $i \in \{1, \ldots, n\}$ such that

$$\frac{k_0}{\gcd(k_0, \ldots, k_{j-1})} \mid i \text{ and } \frac{k_0}{\gcd(k_0, \ldots, k_j)} \not| i.$$

Then

$$\operatorname{ord}_x(y(x) - y(\varepsilon^i x)) = \frac{k_j}{n}$$

for all $i \in N_j$. In particular, if $g = 1$ then

$$\operatorname{ord}_x(y(x) - y(\varepsilon^i x)) = \frac{k_1}{n}$$

if i is not a multiple of n.

(3) We have

$$\begin{aligned} \operatorname{ord}_x \frac{\partial f}{\partial y}(x, y(x)) &= \sum_{j=1}^{g} (\gcd(k_0, \ldots, k_{j-1}) - \gcd(k_0, \ldots, k_j)) \frac{k_j}{n} \\ &= \operatorname{Int}_{\{1, \ldots, \hat{i}, \ldots, n\}} \end{aligned}$$

for all i.

Proposition 5.20. *With notation as above*

(1) For $e = \left\lfloor \operatorname{ord}_x \frac{\partial f}{\partial y}(x, y(x)) \right\rfloor$ the element $\frac{\frac{\partial f}{\partial y}}{x^e}$ is integral over $K[[x]]$ and e is maximal.

(2) Let

$$e = \left\lfloor \operatorname{ord}_x \frac{\partial^{n-1} f}{\partial y^{n-1}}(x, y(x)) \right\rfloor$$

Then $\frac{\frac{\partial^{n-1} f}{\partial y^{n-1}}}{x^e}$ is integral over $K[[x]]$, $e = \left\lfloor \frac{k_1}{n} \right\rfloor$ and e is maximal.

(3) If $g = 1$ then

$$1, \frac{\frac{\partial^{n-1} f}{\partial y^{n-1}}}{x^{e_1}}, \ldots, \frac{\frac{\partial f}{\partial y}}{x^{e_{n-1}}}$$

with

$$e_i = \left\lfloor \operatorname{ord}_x \frac{\partial^{n-i} f}{\partial y^{n-i}}(x, y(x)) \right\rfloor$$

form an integral basis of $\overline{K[[x,y]]/(f)}$ *over* $K[[x]]$.

Remark 5.21. If $f = y^4 - 2x^3y^2 - 4x^{11}y + x^6 - x^{19}$ then $y(x) = x^{\frac{6}{4}} + x^{\frac{19}{4}}$ is a Puiseux expansion, $g = 2$ and (3) in Proposition 5.20 does not hold.

We now prove Proposition 5.20.

Proof. Choose $\Omega \subseteq \{1, \ldots, n\}$ with $|\Omega| = d$ and $\operatorname{Int}_\Omega$ maximal. Then

$$\bar{p} := \prod_{j \in \Omega} \left(y - y(\varepsilon^j x)\right)$$

is a polynomial of degree d with respect to y and $\operatorname{ord}_x \bar{p}(x, y(x))$ is maximal. Let

$$e = \lfloor \operatorname{ord}_x \bar{p}(x, y(x)) \rfloor .$$

By Lemma 5.16, for some approximation p of $\bar{p}$, we can choose $\frac{p(x,y)}{x^e}$ as the degree d element in the integral basis.

We obtain (1) for $d = n - 1$ and (2) for $d = 1$, and $\operatorname{Int}_\Omega$ is independent of Ω. The same holds true for (3) in case $g = 1$.

To see (4) we compute $\left\lfloor \operatorname{ord}_x \frac{\partial^2 f}{\partial y^2}(x, y(x)) \right\rfloor = 4$. However,

$$\bar{p} = (y - y(-x))\,(y - y(ix))$$

gives $\lfloor \operatorname{ord}_x \bar{p}(x, y(x)) \rfloor = 6$. □

5.6. **Computation of the local contribution to the integral basis.** For computing the local contribution to the integral basis at the origin, we have to multiply the numerators of the local integral basis at the origin by the factor corresponding to the expansions that do not vanish at the origin. As noted in the sketch of the algorithm at the beginning of this section, for the terms of degree smaller than the degree of that factor, the integrality exponent will be 0.

Combining the results of the previous sections we obtain Algorithm 8.

In order to obtain a (global) integral basis of $\overline{A}$ over $K[x]$ we can now use Proposition 3.1.

Remark 5.22. In the presence of conjugated singularities, to get a better perfomance, our local algorithm can handle groups of conjugate singularities simultaneously, in a similar way as in [14, Section 4]. If $I \subset k[X, Y]$ is an associated prime of the singular locus, corresponding to a group of conjugate singularities, we apply a linear coordinate change if necessary, so that no two of these singularities have the same X-coordinate. Then we can find polynomials $q_1, q_2 \in K[X]$ such that $I = \langle q_1(X), Y - q_2(X) \rangle$. We take α a root of $q_1(X)$ and traslate the singularity $(\alpha, q_2(\alpha))$ to the origin. We compute the local contribution to integral basis at the origin and apply the inverse traslation to the output. The common denominator of the resulting generators will be a power of $x - \alpha$. We replace $(x - \alpha)$ by $q_1(x)$ in the denominators and we eliminate α from the numerators by considering α as a new variable and reducing each numerator by the numerators of smaller

Algorithm 8 Local contribution to the integral basis

Input: $f \in K[X,Y]$ irreducible polynomial, monic of Y–degree n, with only one singularity, located at the origin.
Output: $b_0, \ldots, b_{n-1}$, an integral basis of $K[X,Y]/\langle f \rangle$.

1: Compute $\Gamma = \{\bar{\gamma}_1, \ldots, \bar{\gamma}_s\}$, the singular part of the Puiseux expansions $\{\gamma_1, \ldots, \gamma_s\}$ of f that vanish at $Y = 0$
2: Compute $e = E(f)$ as indicated in Section 5.2
3: $\{h, f_1, \ldots, f_r\} = \text{Splitting}(f, e)$, where f_i, $i = 1, \ldots, r$ are the factors corresponding to the conjugacy classes of expansions of f that vanish at the origin and h is the factor of the expansions that vanish outside, both developed up to degree e
4: From Γ and $\{f_1, \ldots, f_r\}$, set $L = \{L_1, \ldots, L_s\}$, where $L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \ldots, (\Gamma_{(i,u_i)}, f_{\Gamma_{(i,u_i)}})\}$, the singular parts of the conjugacy classes of the i-th Puiseux block of f and the corresponding factors
5: $m = n - \deg(h)$
6: $\{(p_0, o_0), \ldots, (p_m, o_m)\} = \text{LocalIntegralBasis}(L)$
7: **for** $i = 0, \ldots, \deg(h) - 1$ **do**
8: $\quad b_i = y^i$
9: **for** $i = 0, \ldots, m - 1$ **do**
10: $\quad b_{\deg(h)+i} = h \cdot p_i / x^{\lfloor o(i) \rfloor}$
11: **return** $\{b_0, \ldots, b_{n-1}\}$.

degree (written all with the same common denominator), using an elimination ordering $\alpha \gg y \gg x$. Since an integral basis over the original ring always exists, the elimination process is garanteed to eliminiate α from the numerators.

Example 5.23. Let $A = k[X,Y]$ and $f(X,Y) = Y^3 - (X^2-2)^2$. The singular locus contains only one primary component $\langle X^2-2, Y^2 \rangle$, with radical $\langle X^2-2, Y \rangle$. It consists of the two conjugated points $(-\sqrt{2}, 0)$ and $(\sqrt{2}, 0)$. We take $\alpha = \sqrt{2}$ and compute the local contribution at $(\alpha, 0)$ translating that point to the origin. After after the inverse translation, we get the integral basis of the local contribution

$$\left\{1, y, \frac{y^2}{x-\alpha}\right\}.$$

The local contribution to the integral basis at the conjugated singularity is $\left\{1, y, \frac{y^2}{x+\alpha}\right\}$. Hence the global integral basis is $\left\{1, y, \frac{y^2}{x^2-2}\right\}$. (In this simple case, we did not need to eliminate α from the denominator.)

Example 5.24. Let $A = k[X,Y]$ and $f(X,Y) = (Y-X)^3 - (X^2-2)^2$. Now the radical of singular locus is the prime ideal $\langle X^2-2, Y-X \rangle$. It consists of the two conjugated points $(-\sqrt{2}, -\sqrt{2})$ and $(\sqrt{2}, \sqrt{2})$. We take $\alpha = \sqrt{2}$ and compute the local contribution at (α, α). We get the integral basis of the local contribution

$$\left\{1, y, \frac{y^2 - 2\alpha y + 2}{x-\alpha}\right\}.$$

To eliminate α from the last numerator, we write all the fractions with the same denominator $\left\{\frac{x-\alpha}{x-\alpha}, \frac{y(x-\alpha)}{x-\alpha}, \frac{y^2-2\alpha y+2}{x-\alpha}\right\}$, and we can now reduce the last one to get $\left\{1, y, \frac{y^2-2xy+2}{x-\alpha}\right\}$. Hence the global integral basis is $\left\{1, y, \frac{y^2-2xy+2}{x^2-2}\right\}$.

Is this what is implemented? I am a bit puzzled with respect to the following text: On the first 24 pages we talk about how fast our new approach is, and now we say that it is slow. What is the truth?

5.7. **Appendix: Direct approach.**

The local approach of Algorithm 7 can be computationally slow, since summing up the local results and computing the integral basis from that requires the computation of Groebner bases of possibly complicated ideals.

We present a direct approach that computes the integral basis at the origin handling all the different conjugacy classes together, without computing Groebner bases, and which is therefore usually faster.

However, since the details are very technical, we only give a sketch of the algorithms for this approach.

The main result for constructing p is given in the following theorem, which generalizes the results in [14].

Theorem 5.25. *Let $f \in K[X,Y]$ and $\tilde{p} \in \mathcal{P}_X[Y]$ of Y–degree d with maximal valuation at f. Then there exists $p \in K[X,Y]$ of Y–degree d such that $v_f(\tilde{p}) = v_f(p)$ and such that the Puiseux expansions of p are all truncations of expansions of f.*

Proof. In [14] it is proved that there exists $q \in K[X,Y]$ of Y–degree d such that $v_f(\tilde{p}) = v_f(q)$. To construct p we truncate the expansions appearing in q, removing all the terms that do not coincide with the initial parts of Puiseux expansions of f. By doing this, the valuation does not decrease, $v_f(p) = v_f(q) = v_f(\tilde{p})$, and $p \in K[X,Y]$. □

For the algorithm, instead of starting with $\tilde{p}$ and then building p from it in such a way that the valuation at f does not decrease, we will directly build a polynomial p of maximal valuation among all polynomials coming from truncating expansions of f.

adjust

What is more important, by Proposition 4.8, the choice and truncation of a given number of expansions in a conjugacy class can be done independently of the choice and truncation of expansions in other classes.

Lemma 5.26. *Let $f \in K[X,Y]$ and v the maximal valuation at f among all polynomials in $K[X,Y]$ of Y–degree d. Let $\Gamma_1, \dots, \Gamma_r$ be the conjugacy classes of expansions of f. There exist $q_1, \dots, q_r \in K[X,Y]$ such that $p = q_1 \cdots q_r$ has Y–degree d, $v_f(p) = v$ and q_i has maximal valuation at $f_i = \prod_{\gamma \in \Gamma_i}(Y-\gamma)$, $1 \le i \le r$, among all the polynomials of the same Y–degree as q_i.*

adjust

Proof. This is a direct corollary of Proposition 4.8. □

We can therefore compute the polynomials of each degree restricting to products of polynomials q_i which only depend on the number of expansions chosen in each conjugacy class, and therefore we only have to decide optimally how many expansions to choose in each conjugacy class. We explain this in more detail.

Let n_i, $1 \leq i \leq r$, be the number of expansions in the i-th conjugacy class. We define $p_i(c) = \text{TruncatedFactorGeneral}(\Gamma_i, c)$ for $0 \leq c < n_i$ and $p_i(n_i) = f_i$ developed up to degree e in X (which can be done by Algorithm 4). We call $N_i(c)$ the Puiseux expansions appearing in $p_i(c)$.

Next, we consider the set of tuples $T_d = \{(c_1, \ldots, c_r), c_i \in \mathbb{N}_0, 0 \leq c_i \leq n_i, c_1 + \cdots + c_r = d\}$. For $w = (c_1, \ldots, c_r) \in T_d$, the polynomial of maximal valuation at f containing c_i expansions in the i-th conjugacy class is $p_w = p_1(c_1) \cdots p_r(c_r)$. The valuation of p_w at f can be computed by the formula

$$v_f(p_w) = \min_{1 \leq i \leq r} \left\{ o(\Gamma_i, c_i) + \sum_{j \neq i} v_{\gamma_{(i,1)}}(p_j(c_j)) \right\}.$$

We look for the vector $w = (c_1, \ldots, c_r)$ for which $v_f(p_w)$ is maximal, and for such w we set $p_d := p_w$. The numerator of the element of degree d in the integral basis is p_d and the denominator is $x^{\lfloor v_f(p_d) \rfloor}$.

Algorithm 9 Integral element

Input: $(\Gamma_1, f_1), \ldots, (\Gamma_r, f_r)$, the singular parts of the conjugacy classes of expansions that vanish at the origin of a polynomial $f \in K[X, Y]$ monic in Y and their corresponding factors developed up to X–degree $E(f)$; $d \in \mathbb{N}_0$, $0 \leq d \leq m = \deg_Y(f_1 \cdots f_r)$.

Output: (p, o), with $p \in K[X, Y]$ of Y–degree d of maximal valuation at f; $o \in \mathbb{Q}_{\geq 0}$, the valuation of p at f.

$m_i = \#\Gamma_i$ for $i = 1, \ldots, r$
$T = \{(c_1, \ldots, c_r)\}_{c_i \in \mathbb{N}_0,\ 0 \leq c_i \leq m_i,\ c_1 + \cdots + c_r = d}$
for all $w = (c_1, \ldots, c_r) \in T$ **do**
  for $i = 1, \ldots, r$ **do**
    if $0 \leq c_i < m_i$ **then**
      $p_i(c_i) = \text{TruncatedFactorGeneral}(\Gamma_i, c_i)$
    else
      $p_i(c_i) = f_i$
  $p_w = p_1(c_1) \cdots p_r(c_r)$
  $v_g(p_w) = \min_{1 \leq i \leq r} \left\{ o(\Gamma_i, c_i) + \sum_{j \neq i} v_{\gamma_i}(p_j(c_j)) \right\}$, where γ_i is any expansion of Γ_i.
$p = p_w$ for w such that $v_g(p_w)$ is maximal
return $(p, v_g(p))$.

To apply the algorithm as described above, we must run over all the elements of T_d and compute the corresponding valuations. This can still be slow when T_d is large.

We explain how to find the optimal $(c_1, \ldots, c_r) \in T_d$ in an efficient way. Instead of considering tuples of r elements, we will always consider tuples of 2 elements and proceed iteratively.

For each Puiseux block Π_i, $1 \leq i \leq a$, we define

$$L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \ldots, (\Gamma_{(i,r_i)}, f_{\Gamma_{(i,r_i)}})\},$$

where $\Gamma_{(i,j)}$ are the singular parts of the j-th conjugacy classes of the i-th block and $f_{\Gamma_{(i,j)}}$ is the corresponding factor of f developed up to X–degree in e.

For a list L of this kind, we define $f_L = \prod_{(\Gamma,f_\Gamma)\in L} f_\Gamma$ and we show how to compute $p_L(c)$, the polynomial in $K[X,Y]$ of Y–degree c of maximal valuation at f_L, $0 \leq c \leq m$, where m is the degree of f_L. For a Puiseux series γ, the notation $\gamma \in L$ will mean that there exists $(\Gamma, f_\Gamma) \in L$ such that $\gamma \in \Gamma$.

We group the lists in new lists $\Lambda_1, \ldots, \Lambda_u$ such that all the expansions in the same list Λ_i have the same initial term (or conjugate initial terms). We order them in increasing order by the initial exponent. (The order among groups with the same initial exponent is not important.) Since $v(\gamma_i)$ is the same for any $\gamma_i \in \Lambda_i$, we define $v(i) = v(\gamma_i)$. The key property is that if $1 \leq i < j \leq u$, then $v(\gamma_i - \gamma_j) = v(i)$ for any $\gamma_i \in \Lambda_i$ and $\gamma_j \in \Lambda_j$.

Let m_i be the number of expansions in Λ_i, $1 \leq i \leq u$. We define $\Theta_i = \Lambda_i + \cdots + \Lambda_u$ and we want to compute inductively $p_{\Theta_i}(c)$, for $0 \leq c \leq m_i + \cdots + m_u$.

We start by computing $p_{\Theta_u}(c) = p_{\Lambda_u}(c)$ for $0 \leq c \leq m_u$. For any $1 \leq i \leq u$ and $1 \leq c \leq m_u$ we can compute $p_{\Lambda_i}(c)$ using Algorithm 9, or applying this new algorithm recursively as we will see below.

Now, proceeding inductively, once we have computed $p_{\Theta i+1}(c)$ for all $0 \leq c \leq m_{i+1} + \cdots + m_u$, we want to compute $p_{\Theta_i}(c)$ for all $0 \leq c \leq m_i + \cdots + m_u$.

The property mentioned above implies that $v(\gamma_i - \gamma_{i+1}) = v(i)$ for any $\gamma_i \in \Lambda_i$ and $\gamma_{i+1} \in \Theta_{i+1}$.

Hence for any set N_1 of c_1 expansions of Λ_i and any set N_2 of c_2 expansions of Θ_{i+1}, if $q_1 = \prod_{\eta\in N_1}(Y-\eta)$, $q_2 = \prod_{\eta\in N_2}(Y-\eta)$ and $q = q_1 q_2$, then

$$v_{\gamma_i}(q_2) = c_2 v(i)$$

Since $v_{f_{\Lambda_i}}(q_1)$ is the minimum of $v_{\gamma_i}(q_1)$ for $\gamma_i \in \Lambda_i$, we obtain that

$$\min_{\gamma\in\Lambda_i} v_\gamma(q) = v_{f_{\Lambda_i}}(q_1) + c_2 v(i)$$

Similarly,

$$\min_{\gamma\in\Theta_{i+1}} v_\gamma(q) = c_1 v(i) + v_{f_{\Theta_{i+1}}}(q_2)$$

We conclude that

$$v_{f_{\Theta_i}}(q) = \min\{v_{f_{\Lambda_i}}(q_1) + c_2 v(i), c_1 v(i) + v_{f_{\Theta_{i+1}}}(q_2)\}$$

This allows us to compute inductively

$$o(\Theta_i, c) = \max_{c_1+c_2=c} v_{f_{\Theta_i}}(p_{\Lambda_i}(c_1) p_{\Theta_{i+1}}(c_2))$$

and define $p_{\Theta_i}(c)$ as the polynomial for which the maximum is obtained.

The numerator of the element of degree d in the integral basis is

$$p_d = p_{\Theta_1}(d)$$

and the denominator is $x^{\lfloor v_f(p_d)\rfloor}$.

For computing the best polynomials in each block, we can use this strategy recursively. We summarize the method in Algorithm 10.

We apply this algorithm to Example 4.10, to compare with Algorithm 7.

Algorithm 10 Local integral basis, combinatorial approach

Input: $L = \{L_1, \dots, L_r\}$, where $L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \dots, (\Gamma_{(i,u_i)}, f_{\Gamma_{(i,u_i)}})\}$, $1 \le i \le r$, are the singular parts of the conjugacy classes of some Puiseux blocks of f and their corresponding factors developed up to X–degree e.

Output: $\{(p_0, o_0), \dots, (p_m, o_m)\}$ such that $p_i \in K[X,Y]$ $(0 \le i \le m)$ has Y–degree i and maximal valuation at $g = f_{\Gamma_{(1,1)}} \cdots f_{\Gamma_{(r,u_r)}}$; and $o_i \in \mathbb{Q}_{\ge 0}$, $o_i = v_g(p_i)$, where $m = \deg_Y(g)$.

if $r = 1$ **then**
  return $\{\text{IntegralElements}(L_1, c)\}_{c=0,\dots,m}$
else
  $f_{L_i} = \prod_{j=1}^{u_i} f_{\Gamma_{(i,j)}}$, for $i = 1, \dots, r$.
  Group the lists $L_1, \dots, L_r$ in lists $\Lambda_1, \dots, \Lambda_u$ such that all the expansions in the same list Λ_i have the same or conjugate initial terms (without considering the common rational part of all expansions, if any), ordered by the initial exponent in increasing order
  $f_{\Lambda_i} = \prod_{L_j \in \Lambda_i} f_{L_j}$ and $m_i = \deg(f_{\Lambda_i})$, for $i = 1, \dots, u$
  $\Theta_u = \Lambda_u$, $f_{\Theta_u} = f_{\Lambda_u}$
  $\{(p_{\Theta_u}(c), o(\Theta_u, c))\}_{c=0,\dots,m_u} = \text{LocalIntegralBasis}(\Theta_u)$
  for $i = u-1, \dots, 1$ **do**
    $\Theta_i = \Lambda_i \cup \Theta_{i+1}$, $f_{\Theta_i} = f_{\Lambda_i} f_{\Theta_{i+1}}$
    $\{(p_{\Lambda_i}(c), o(\Lambda_i, c))\}_{c=0,\dots,m_i} = \text{LocalIntegralBasis}(\Lambda_i)$
    for $0 \le c \le m_i + \cdots + m_u$ **do**
      $C = \{(c_1, c_2) \in \mathbb{Z}^2_{\le 0} \mid c_1 + c_2 = c,\ 0 \le c_1 \le m_i,\ 0 \le c_2 \le m_{i+1} + \cdots + m_u\}$
      $o(\Theta_i, c) = \max_{(c_1,c_2) \in C} v_{f_{\Theta_i}}(p_{\Lambda_i}(c_1) p_{\Theta_{i+1}}(c_2))$
      $p_{\Theta_i}(c) =$ the polynomial for which the maximum is obtained
  return $\{(p_{\Theta_1}(c), o(\Theta_1, c))\}_{c=0,\dots,m}$.

TWOBRANCHES modify this example using the new example with no inclusion

Example 5.27. Let $f = (Y^3 - X^7)(Y^2 - X^3) + Y^6 \in \mathbb{Q}[X,Y]$. The input for Algorithm 10 is $L = \{L_1, L_2\} = \{\{(\Gamma_1, f_1)\}, \{(\Gamma_2, f_2)\}\}$, where Γ_1 and Γ_2 are the same as in Example 5.18 and $f_1 = h_2$, $f_2 = h_1$.

We have $\Lambda_1 = L_1$, $\Lambda_2 = L_2$ and $u = 2$. Also $f_{\Lambda_1} = f_1$, $f_{\Lambda_2} = f_2$, $m_1 = 3$ and $m_2 = 2$.

Hence $\Theta_2 = \Lambda_2$, $f_{\Theta_2} = f_{\Lambda_2}$ and the local integral basis corresponding to Θ_2 is $\{(1,0), (y,1), (f_2, \infty)\}$.

For $i = 1$, $\Theta_1 = L$ and $f_{\Theta_1} = f_1 f_2$. The local integral basis corresponding to Λ_1 is $\{(1,0), (y,2), (y^2,4), (f_1, \infty)\}$.

Now we have to choose the best combinations for each $c = 0, \dots, m$. For example, for $c = 3$, we try the pairs $(c_1, c_2) \in \{(1,2), (2,1), (3,0)\}$ and find that the best choice is $(c_1, c_2) = (1,2)$, for which $v_{f_{\vartheta_1}}(p_{\Lambda_1(2)} p_{\Theta_2}(0)) = v_{f_{\vartheta_1}}(Y f_2) = 16/3$.

Applying the formulas for all c, $0 \le c \le 5$, we get the output

$$\{(1,0), (y,1), (f_2, 3), (y f_2, 16/3), (y^2 f_2, 23/3), (f_1 f_2, \infty)\}.$$

The first five elements define the integral basis $\left\langle 1, \frac{y}{x}, \frac{f_2}{x^3}, \frac{f_2 y}{x^5}, \frac{f_2 y^2}{x^7} \right\rangle_{K[x]}$.

6. Timings

Which algorithm is meant? We also have the appendix.

We present some timings which compare the implementation of our algorithm in Singular with that of van Hoeij's algorithm in Maple. We compute integral bases for $A = \mathbb{Q}[X,Y]/\langle f\rangle$ with polynomials f as specified. All timings are in seconds, taken on an AMD Opteron 6174 machine with 48 cores, 2.2GHz, and 128GB of RAM running a Linux operating system. We do not make use of parallel computation so far; this is subject to ongoing implementation work. In the cases where f has only one singular point, this point is given as part of the input to both algorithms. That is, no computation or decomposition of the singular locus is done. In the cases where the singular locus has more than one point, the timings are taken for decomposing the singular locus, computing the local contributions, and combining these. We remark that for obtaining the integral bases, singularities at infinity of the curve $\{f = 0\}$ do not matter.

We should have more columns for the timings. 1) Use the global normalization algorithm. 2) Use the local normalization algorithm. 2) Magma.

6.1. **A_k-singularity.** The plane curves with defining equation $f(X,Y) = Y^2 + X^{k+1} + Y^d$, $k \geq 1$, $d \geq 3$ have exactly one singularity at the origin, which is of type A_k.

k	d	Singular	Maple
5	10	0	0
5	100	0	2.4
5	500	14	262
50	60	0	2.6
50	100	0	7
50	500	16	385
90	100	0	12
90	500	13	509
400	500	16	1689

6.2. **D_k-singularity.** The plane curves with defining equation $f(X,Y) = X(X^{k-1} + Y^2) + Y^d$, $k \geq 2$, $d \geq 3$ have exactly one D_k-singularity at the origin.

k	d	Singular	Maple
5	10	0	0
5	100	2	2.6
5	500	51	206
50	60	1	14
50	100	2	45
50	500	49	2114
90	100	2	142
90	500	50	5918
400	500	50	> 6000

6.3. **Ordinary multiple points.** We consider random curves of degree d with an ordinary k-fold point at the origin. The defining polynomials were generated by the function `polyDK` from the Singular library `integralbasis.lib` (using the random seed 1231).

k	d	SINGULAR	MAPLE
5	10	0	0
15	20	0	3
15	30	1	1095
20	25	0	13
20	30	1	352

6.4. **Curves with many A_k singularities.** The plane curves with defining equations

$$f = \left(X^{k+1} + Y^{k+1} + Z^{k+1}\right)^2 - 4\left(X^{k+1}Y^{k+1} + Y^{k+1}Z^{k+1} + Z^{k+1}X^{k+1}\right)$$

were given in [11] and have $3\,(k+1)$ singularities of type A_k if n is even. To ensure that all singularities of the curves are in the affine chart $\{Z \neq 0\}$, we substitute $Z = 2X - Y + 1$.

k	SINGULAR	MAPLE
6	2	11
8	18	109
10	240	4756

The plane curves with defining equations

$$f_{5,n} = X^{2n} + Y^{2n} + Z^{2n} + 2(X^nZ^n - X^nY^n + Y^nZ^n)$$

were given in [2] and have $3n$ singularities of type A_{n-1} if n is odd. We now substitute $Z = X - 2Y + 1$.

n	SINGULAR	MAPLE
5	1	3
7	2	37
9	27	478
11	53	> 6000

6.5. **More general singularities.** We now consider some examples of curves which have singularities of a type other than ADE or ordinary multiple points:

(1) $f = -X^{15}+21X^{14}-8X^{13}Y+6X^{13}+16X^{12}Y-20X^{11}Y^2+X^{12}-8X^{11}Y+36X^{10}Y^2-24X^9Y^3-4X^9Y^2+16X^8Y^3-26X^7Y^4+6X^6Y^4-8X^5Y^5-4X^3Y^6+Y^8$: one singularity at the origin with multiplicity $m = 8$ and delta invariant $\delta = 42$, a node, and a set of 6 conjugate nodes. [Pfister]

Pfister refers to?

(2) $f = (Y^4 + 2X^3Y^2 + X^6 + X^5Y)^3 + X^{11}Y^{11}$: one singularity at the origin with $m = 12$ and $\delta = 133$. [Pfister]

Pfister refers to?

(3) $f = (Y^5 + Y^4X^7 + 2X^8)(Y^3 + 7X^4)(Y^7 + 2X^{12})(Y^{11} + 2X^{18}) + Y^{30}$: one singularity at the origin with $m = 26$ and $\delta = 523$.

(4) $f = (Y^{15} + 2X^{38})(Y^{19} + 7X^{52}) + Y^{36}$: one singularity at the origin with $m = 34$ and $\delta = 1440$.

(5) $f = (Y^{15} + 2X^{38})(Y^{19} + 7X^{52}) + Y^{100}$: higher degree, but same type of singularity.

(6) $f = Y^{40} + XY^{13} + X^4Y^5 + X^5 + 2X^4 + X^3$: one double point with $\delta = 2$ and one triple point with $\delta = 19$ (see [14, Section 6.1]).

(7) $f = Y^{200} + XY^{13} + X^4Y^5 + X^5 + 2X^4 + X^3$: higher degree, but same type of singularity.

(8) $f = (Y^{35} + Y^{34}X^7 + 2X^{38})(Y^{33} + 7X^{44})(Y^{37} + 2X^{52}) + Y^{110}$: one singularity at the origin with $m = 105$ and $\delta = 6528$.

Although some of the examples have only one singularity at the origin, we apply the local and the global algorithm in all cases. That is, in the columns labelled *Origin*, we compute the timings for the local contribution to the integral basis at the origin, which does not involve the decomposition of the singular locus. In the columns labelled *Global*, we decompose the singular locus, compute the local contributions, and combine them.

How are the Maple timings under origin taken? In the Singular* column, I do not understand the two bad timings in the middle.

	Origin		Global			
No.	SINGULAR	MAPLE	SINGULAR	SINGULAR*	MAPLE	Y–degree
1	0	0	0	5	1	8
2	36	2	37	37	2	12
3	2	6	> 6000	41	16	30
4	1	10	1	> 6000	12	36
5	0	47	1	> 6000	115	100
6	1	0	1	1	1	40
7	9	12	35	10	50	200
8	154	5708	> 6000	> 6000	> 6000	110

In the column SINGULAR*, we use modular techiques for computing the decomposition of the singular locus.

In this table, the computations in Singular that did not finish are all due to the computation of the decomposition of the singular locus (although we know that these examples have only one singularity at the origin).

We note that in most cases, our proposed algorithm is much faster than the algorithm implemented in Maple. Note, however, that in the last table, there is one example in which Singular is significantly slower than Maple. In this example, the algorithm runs into an algebraic field extension of high degree. At current state, the handling of such extensions in Singular is far from being optimal.

This can easily be avoided. First insert the origin into the equations of the singular locus to check whether the origin is a singular point. Then there are two possibilities. 1) Compute a global and a local Groebner basis and compare dimensions. See Lecture 9 in the book Decker/Lossen. 2) Saturate in the maximal ideal of the origin. That might be slower than 1), but if there are more singularities, it will lead to an easier primary decomposition problem. Santiago, please make tests.

References

[1] J. Boehm, W. Decker, S. Laplagne, G. Pfister, A. Steenpaß, and S. Steidel. Parallel algorithms for normalization. 2011.

[2] J. I. Cogolludo. Fundamental group for some cuspidal curves. 31:136–142, 1999.

[3] T. de Jong. An algorithm for computing the integral closure. *J. Symbolic Comput.*, 26(3):273–277, 1998.

[4] Theo de Jong and Gerhard Pfister. *Local analytic geometry*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2000. Basic theory and applications.

[5] Wolfram Decker, Theo de Jong, Gert-Martin Greuel, and Gerhard Pfister. The normalization: a new algorithm, implementation and comparisons. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 177–185. Birkhäuser, Basel, 1999.

[6] Clémence Durvye. *Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation*. PhD thesis, Université de Versailles - Saint-Quentin, 2008.

[7] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[8] H. Grauert and R. Remmert. *Analytische Stellenalgebren*. Springer-Verlag, Berlin, 1971. Unter Mitarbeit von O. Riemenschneider, Die Grundlehren der mathematischen Wissenschaften, Band 176.

[9] G.-M. Greuel, S. Laplagne, and F. Seelisch. Normalization of rings. *J. Symbolic Comput.*, 2010.

[10] G.-M. Greuel and G. Pfister. *A Singular introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX).

[11] A. Hirano. Construction of plane curves with cusps. 10:21–24, 1992.

[12] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Publishing Company, Incorporated, 2nd edition, 2008.

[13] Irena Swanson and Craig Huneke. *Integral closure of ideals, rings, and modules*, volume 336 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[14] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, 18(4):353–363, 1994.