Computing integral bases via localization and Hensel lifting

Janko Böhm, Wolfram Decker, Santiago Laplagne, Gerhard Pfister

Computing integral bases via localization and Hensel lifting

Janko Böhm

Department of Mathematics, University of Kaiserslautern
Erwin-Schrödinger-Str. - (67663) Kaiserslautern, Germany

Wolfram Decker

Department of Mathematics, University of Kaiserslautern
Erwin-Schrödinger-Str. - (67663) Kaiserslautern, Germany

Santiago Laplagne

Departamento de Matemática, FCEyN, Universidad de Buenos Aires
Ciudad Universitaria Pabellón I - (C1428EGA) - Buenos Aires, Argentina

Gerhard Pfister

Department of Mathematics, University of Kaiserslautern
Erwin-Schrödinger-Str. - (67663) Kaiserslautern, Germany

Abstract

We present a new algorithm for computing integral bases in algebraic function fields of one variable, or equivalently for constructing the normalization of a plane curve. Our basic strategy makes use of the concepts of localization and completion, together with the Chinese remainder theorem, to reduce the problem to the task of finding integral bases for the branches of each singularity of the curve. To solve the latter task, in turn, we work with suitably truncated Puiseux expansions. In contrast to van Hoeij's algorithm (van Hoeij, 1994), which also relies on Puiseux expansions (but pursues a different strategy), we use Hensel's lemma as a key ingredient. This allows us at some steps of the algorithm to compute factors corresponding to conjugacy classes of 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 (Böhm et al., 2017) and, based on this, the computation of Riemann-Roch spaces and the parametrization of rational curves.

Keywords: Normalization, integral closure, integral basis, curve singularity, Puiseux series

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

Email addresses: boehm@mathematik.uni-kl.de (Janko Böhm), decker@mathematik.uni-kl.de (Wolfram Decker), slaplagn@dm.uba.ar (Santiago Laplagne), pfister@mathematik.uni-kl.de (Gerhard Pfister)

normal if $A = \overline{A}$. Recall that if A is a reduced *affine* (that is, finitely generated) algebra over a field K, then $\overline{A}$ is a finite A-module by the splitting of normalization (see de Jong and Pfister (2000, Theorem 1.5.20)) and Emmy Noether's finiteness result below (see Eisenbud (1995, Chapter 13) for a proof):

Theorem 1 (Emmy Noether)**.** *Let R be a Noetherian domain and let L be a finite extension field of $F = \mathrm{Q}(R)$. Suppose that R is an affine domain over a field K or that R is normal and L is separable over F. Then the integral closure S of R in L is a finitely generated R-module.*

Remark 2. *With notation and assumptions as in the theorem, suppose that R is a PID. Then S, as a finitely generated torsion-free module over a PID, is free. In fact, it is free of rank $[L : F]$ since a set of free generators for S over R is also a basis for $L = SF$ over F.*

Definition 3. *If $R \subset T$ is a ring extension such that the integral closure S of R in T is a free R-module, then we call any set of free generators for S over R an* integral basis *for S over R.*

In this paper, we focus on 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 modulo f, 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

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

where x is a separating transcendence basis of $K(C)$ over K, and y is integral over $K[x]$, with integrality equation $f(x, y) = 0$. Indeed, we have the isomorphism $\mathrm{Q}(K[x][y]) \to K(x)[y]$ defined by mapping $1/h(x, y) \mapsto b(x, y)/x^c$, where $X^c = af + bh \in K[X][Y]$ is a representation which arises from a Bézout identity in $K(X)[Y]$ by clearing denominators.

In particular, A is integral over $K[x]$, which implies that $\overline{A}$ coincides with the integral closure of $K[x]$ in $K(C)$. We may, hence, represent $\overline{A}$ either by generators over A or by generators over $K[x]$. Note that by Remark 2, $\overline{A}$ is a free $K[x]$-module of rank

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

Remark 4. *In the context outlined above, there exist polynomials $p_i \in K[X][Y]$ of degree i in Y and polynomials $d_i \in K[X]$ such that*

$$\left\{1, \frac{p_1(x, y)}{d_1(x)}, \ldots, \frac{p_{n-1}(x, y)}{d_{n-1}(x)}\right\}$$

is an integral basis for $\overline{A}$ over $K[x]$. In fact, such a basis is obtained from any given set of $K[x]$-module generators for $\overline{A}$ by unimodular row operations over the PID $K[X]$: Represent the given generators by polynomials of type $c_i = \sum_{j=0}^{n-1} c_{ij} Y^{n-1-j}$, 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 Hermite normal form (p_{ij}), set $\widetilde{p}_i = \sum_{j=0}^{n-1} p_{n-1-i,j} Y^{n-1-j}$ for each $i = 0, \ldots, n-1$, and let the $p_i(X, Y)/d_i(X)$ be obtained by reducing the $\widetilde{p}_i(X, Y)/d(X)$ to lowest terms.

Remark 5. *The general normalization algorithms presented in (Greuel et al., 2010), (Böhm et al., 2013) are designed to 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 will become clear in Section 2, we may take a generator of the elimination ideal $\langle \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y}, f\rangle \cap K[X]$ to represent d (note that this ideal defines the X-coordinates of the singularities of the curve defined by f over the algebraic closure $\overline{K}$). 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 the remark above.*

Remark 6. *In practical terms, $u_0, \ldots, u_r$ are given as polynomials in $K[X,Y]$ of Y-degree at most $n-1$. If these polynomials, together with f, form a Gröbner basis with respect to the lexicographical ordering, taking $Y > X$, then already the elements $y^i u_j(x,y)/d(x)$, $0 \le i \le n-1-\deg(u_j)$, $0 \le j \le r$, generate $\overline{A}$ over $K[x]$.*

Example 7. *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 Greuel et al. (2010, 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 4.

The algorithms in (Greuel et al., 2010), (Böhm et al., 2013) work for any reduced affine algebra A over a perfect field. They rely on the Grauert and Remmert normalization criterion which applies in global or local settings (see Grauert and Remmert (1971), Greuel and Pfister (2007, Prop. 3.6.5), Böhm et al. (2013, Prop. 3.3)): whereas the algorithm in (Greuel et al., 2010) is of global nature, the idea in (Böhm et al., 2013) is to consider a finite stratification of the singular locus $\mathrm{Sing}(A)$, apply a local version of the normalization algorithm at each stratum, and find $\overline{A}$ by putting the resulting local contributions together. If A is the coordinate ring of a curve, then $\mathrm{Sing}(A)$ is finite, and we may stratify it by considering each $P \in \mathrm{Sing}(A)$ separately. Computing an integral basis for $\overline{A}$ over $K[x]$ is then equivalent to computing a local contribution to $\overline{A}$ at each P.

In this paper, we present a new method for the latter task which is custom-made for our case of interest here. From now on, let $A = K[C] = K[x][y]$ be the coordinate ring of a plane curve C with notation and assumptions as before. To describe the main ideas of the new method, we suppose for simplicity that the prime ideal $P \in \mathrm{Sing}(A)$ under consideration defines a K-rational singularity of C, and that this singularity is the origin, that is, $P = \langle x, y\rangle$.

Consider the completion of A at $\langle x \rangle$:

$$\widehat{A} = K[[x]][y] = K[[X]][Y]/\langle f \rangle.$$

Since A is a reduced excellent ring, $\widehat{A}$ is reduced as well (see Grothendieck (1966, Section 7.8)). The normalization $\widehat{\overline{A}}$ in turn is a free $K[[x]]$-module of rank $n = \deg_Y(f)$. Indeed, consider the decomposition

$$f = f_0 \widetilde{f} = f_0 f_1 \cdots f_r \tag{1}$$

given by the Weierstrass preparation theorem (see Abhyankar (1990), de Jong and Pfister (2000)). Here, $f_0 \in K[[X]][Y]$ is a unit in $K[[X, Y]]$, and $f_1, \ldots, f_r \in K[[X]][Y]$ are irreducible Weierstrass polynomials to which we refer as the *branches* of f (over K, centered at the origin). It follows from Remark 2 that if g is one of the branches, then the normalization of the ring $B = K[[x]][y] = K[[X]][Y]/\langle g \rangle$ is a free $K[[x]]$-module, a result which extends to the cases $g = \widetilde{f}$ and $g = f$ by the splitting of normalization. In each case, we refer to an integral basis for B over $K[[x]]$ as an *integral basis for* g. Our new algorithm is designed so that it computes such bases $\mathcal{B}_{f_1}, \ldots, \mathcal{B}_{f_r}$ for the branches of f, and so that it finds the desired local contribution to $\overline{A}$ at P from the $\mathcal{B}_{f_i}$.

We present more details of the algorithm while outlining the structure of our paper.

To fix our ideas, in Sections 2 and 3, we give a more detailed account of the Grauert and Remmert type algorithms. Furthermore, we discuss an efficient criterion for detecting whether a given point is the only singularity of the curve under consideration. In Section 4, we review Puiseux expansions and their connection to integrality via valuations.

A crucial theoretical result proved in Section 5 is that $f_1, \ldots, f_r$ admit integral bases of type

$$\mathcal{B}_{f_i} = \left\{ 1 = p_0^{(i)}, \frac{p_1^{(i)}(x, y)}{x^{e_1^{(i)}}}, \ldots, \frac{p_{m-1}^{(i)}(x, y)}{x^{e_{m-1}^{(i)}}} \right\},$$

with monic polynomials $p_d^{(i)} \in K[X][Y]$ of degree d in Y: We then speak of integral bases of *monic triangular type*. Using an explicit version of the splitting of normalization via the Chinese remainder theorem, we show how such bases fit together to an integral basis for $\widetilde{f} = f_1 \cdots f_r$. Any such basis, in turn, can be transformed into an integral basis $\mathcal{B}_{\widetilde{f}}$ for $\widetilde{f}$ of monic triangular type by computing a Hermite normal form over the PID $K[[x]]$. Going one step further, in Section 6, we show how to turn $\mathcal{B}_{\widetilde{f}}$ into an integral basis $\mathcal{B}_f$ for f which is of monic triangular type: Under the additional assumption that the origin is the only singularity of C with X-coordinate zero, we prove that the $K[x]$-module generated by the elements of $\mathcal{B}_f$ is a ring which is a local contribution to A at P.

How to actually construct integral bases $\mathcal{B}_{f_i}$ for the branches is a topic of Section 7, which is the algorithmic heart of the paper. Working with suitably truncated Puiseux series, we describe an effective way to obtain the $\mathcal{B}_{f_i}$. Though inspired by van Hoeij's paper (van Hoeij, 1994), our strategy is different, with Hensel lifting providing a crucial new ingredient. In summarizing the whole algorithm, we also show that we can actually avoid the use of the Chinese remainder algorithm when computing $\mathcal{B}_{\widetilde{f}}$ from the $\mathcal{B}_{f_i}$. This improves the performance of the algorithm considerably.

We have implemented our algorithm in the computer algebra system Singular (Decker et al., 2015). In Section 8, we compare its performance with that of the local to global Grauert and Remmert type algorithm. We also give timings for the implementation of van Hoeij's algorithm in Maple and for the variant of the Round 2 algorithm implemented in Magma.

2. The Global Normalization Algorithm

In this section, we review the global version of the normalization algorithm. To begin with, we fix our notation and present some general facts on normalization. For this, A may be any reduced Noetherian ring. We write

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

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

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

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

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

the *singular locus* of A. Then $N(A) \subset \mathrm{Sing}(A)$, with equality holding if A is the coordinate ring of a curve (see de Jong and Pfister (2000, Theorem 4.4.9)).

Definition 8. *The* conductor *of A is*

$$C_A = \mathrm{Ann}_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}.$$

Note that 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 9. *Let A be a reduced Noetherian ring. Then $N(A) \subset V(C_A)$. Furthermore, $\overline{A}$ is a finite A-module iff C_A contains a non-zerodivisor of A. In this case, $N(A) = V(C_A)$.*

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

Definition 10. *Let A be a reduced Noetherian ring. A* test ideal *for A is a radical ideal $J \subset A$ such that $V(C_A) \subset V(J)$. 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 Grauert and Remmert (1971), Greuel and Pfister (2007, Prop. 3.6.5)). The algorithm by de Jong (see de Jong (1998), Decker et al. (1999)) and its improvement, the algorithm by Greuel et al. (2010), are based on this criterion, and apply to any reduced affine algebra $A = L[X_1, \ldots, X_n]/I$ over a perfect field L. Initially, by means of equidimensional decomposition, we may reduce to the case where A is equidimensional. In this case, since we work over a perfect field, the Jacobian ideal[1] M of A is non-zero and contained in the conductor C_A. This implies that the radical $J = \sqrt{M}$ together with any non-zero divisor $g \in J$ of A is a test pair (see Greuel et al. (2010, Lemma 4.1)). Given such a pair (see Greuel et al. (2010, Remark 4.6) for how to find g), the idea of computing $\overline{A}$ is to successively enlarge A by finite ring 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 by Grauert and Remmert allows us to stop. The algorithm by Greuel et al. then returns an ideal $U \subset A$ together with a power d of g such that $\overline{A} = \frac{1}{d}U \subset \mathrm{Q}(A)$.

[1] The *Jacobian ideal* M of $A = L[X_1, \ldots, X_n]/I$ is generated by the images of the $c \times c$ minors of the Jacobian matrix $(\frac{\partial f_i}{\partial X_j})$, where we suppose that I is of pure codimension c, and where $f_1, \ldots, f_r$ are generators for I. By the Jacobian criterion, $V(M) = \mathrm{Sing}(A)$ (see Eisenbud (1995, Theorem 16.19)).

Remark 11. *If M is non-zero and contained in C_A, then any non-zerodivisor $c \in M$ of A is a valid denominator: If $\overline{A} = \frac{1}{d}U$ as above, then $c \cdot \frac{1}{d}U =: U'$ is an ideal of A, and $\frac{1}{d}U = \frac{1}{c}U'$.*

Example 12. *Let A be the coordinate ring of the curve C with defining polynomial $f(X,Y) = X^5 - Y^2(Y-1)^3 \in \mathbb{Q}[X,Y]$. Then*

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

is the radical of the Jacobian ideal, so 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 proposed by Böhm et al. (2013). To simplify our presentation, we focus on the case of a reduced Noetherian ring with a finite singular locus (such as the coordinate ring of a curve). Our starting point is Proposition 13 below which, as we will see later on, is also fundamental to our new algorithm. In formulating the proposition, if $P \in \operatorname{Spec}(A)$ and $A \subset A' \subset \overline{A}$ is an intermediate ring, we write A'_P for the localization of A' at $A \setminus P \subset A'$.

Proposition 13. *Let A be a reduced Noetherian ring with a finite singular locus $\operatorname{Sing}(A) = \{P_1, \ldots, P_s\}$. 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. A more general result is proved in Böhm et al. (2013, Proposition 3.2). □

Definition 14. *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 15. *Note that a minimal local contribution is uniquely determined since, by definition, its localization at each $P \in \operatorname{Spec}(A)$ is determined.*

Given a reduced affine algebra A over a perfect field L with a finite singular locus, Proposition 13 allows us to split the computation of $\overline{A}$ into local tasks at the primes $P_i \in \operatorname{Sing}(A)$. One way of finding the minimal local contributions $A^{(i)}$ is to apply the local version of the normalization algorithm from Böhm et al. (2013), which relies on a local variant of the Grauert and Remmert criterion. 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 10.

Example 16. *As in Example 12, let A be the coordinate ring of the curve C with defining polynomial $f(X,Y) = X^5 - Y^2(Y-1)^3 \in \mathbb{Q}[X,Y]$. 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 $\frac{1}{d_i}U_i$, $i = 1,2$. Specifically,*

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

Summing up the local contributions, we get $\overline{A} = \frac{1}{d}U$ 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 12.

Remark 17. *In Example 16, 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.

Relying on the Jacobian criterion, we may find the primes in $\mathrm{Sing}(A)$ by means of primary decomposition. If there is precisely one such prime, this requires (possibly expensive) computations which are only needed to detect this fact. In the case of a plane curve C considered here, supposing that one singularity P of C is already known to us, we may check whether P is the only singularity of C by comparing the local Tjurina number of C at P with the total Tjurina number of C. Computing the total Tjurina number via Gröbner bases over the rational numbers, however, can be expensive due to coefficient swell. To overcome this problem, we provide an efficient modular criterion. Note that though singularities at infinity do not matter for obtaining integral bases, the criterion takes these singularities into account. That is, it is formulated in the projective setting.

Let L be any field, let $F \in L[X,Y,Z]$ be a square-free homogeneous polynomial of positive degree, and let $\Gamma = \mathrm{Proj}(L[X,Y,Z]/\langle F\rangle)$ be the projective curve defined by F. Moreover, write

$$S = L[X,Y,Z]/\langle F_X, F_Y, F_Z\rangle,$$

where F_X, F_Y, F_Z are the partial derivatives of F. Then, taking Euler's rule into account, $\Gamma_{\mathrm{sing}} = \mathrm{Proj}(S) \subset \Gamma$ is the singular locus of Γ. For any $Q \in \Gamma_{\mathrm{sing}}$, let $S_{(Q)}$ be the homogeneous localization of S at Q. Then

$$\tau_Q(\Gamma) = \dim_L S_{(Q)}$$

is the Tjurina number of Γ at Q. For example, if $P = \langle X, Y\rangle$, then

$$\tau_P(\Gamma) = \dim_L \left(L[X,Y]_{\langle X,Y\rangle}/\langle f,\ f_X, f_Y\rangle\right),$$

with $f = F(X,Y,1)$. The Tjurina number of Γ in the chart $X \neq 0$ is

$$\tau_{X\neq 0}(\Gamma) = \dim_L \left(L[X,Y]/\langle f,\ f_X, f_Y\rangle\right),$$

and similarly for the other coordinate charts. Finally,

$$\tau(\Gamma) = \deg \operatorname{Proj}(S) = \sum_{Q \in \Gamma_{\text{sing}}} \tau_Q$$

is the total Tjurina number of Γ.

Proposition 18. *Let $F \in \mathbb{Q}[X, Y, Z]$ be a square-free homogeneous polynomial of positive degree with integer coefficients. Let q be a prime number such that the reduction F_q of F modulo q is non-zero. Consider the curves $\Gamma = \operatorname{Proj}(\mathbb{Q}[X, Y, Z]/\langle F\rangle)$ and $\Gamma_q = \operatorname{Proj}(\mathbb{F}_q[X, Y, Z]/\langle F_q\rangle)$, and let $P = \langle X, Y\rangle$. Suppose that*

$$\tau_P(\Gamma_q) = \tau_P(\Gamma) > 0 \quad \text{and} \quad \tau_{X\neq 0}(\Gamma_q) = \tau_{Y\neq 0}(\Gamma_q) = 0.$$

Then $\Gamma_{\text{sing}} = \{P\}$.

Proof. By Arnold (2003, Theorem 5.3), considering the Hilbert functions of

$$\begin{aligned} S &= \mathbb{Q}[X, Y, Z]/\langle F_X, F_Y, F_Z\rangle \text{ and} \\ S_q &= \mathbb{F}_q[X, Y, Z]/\left\langle (F_X)_q, (F_Y)_q, (F_Z)_q\right\rangle, \end{aligned}$$

we have

$$\operatorname{HF}_S(t) \leq \operatorname{HF}_{S_q}(t), \text{ for all } t.$$

Since the Tjurina numbers are the leading coefficients of the respective Hilbert polynomials, this implies that

$$\tau(\Gamma) \leq \tau(\Gamma_q).$$

On the other hand, if $\tau_{X\neq 0}(\Gamma_q) = \tau_{Y\neq 0}(\Gamma_q) = 0$, then $(\Gamma_q)_{\text{sing}} = \{P\}$, so that

$$\tau(\Gamma_q) = \tau_P(\Gamma_q) = \tau_P(\Gamma) \leq \tau(\Gamma).$$

Combining both inequalities yields

$$\tau_P(\Gamma) = \tau(\Gamma)$$

and, thus, $\Gamma_{\text{sing}} = \{P\}$. □

Remark 19. *The invariants in the criterion can be obtained efficiently by a standard basis computation over $\mathbb{Q}$ with respect to a local monomial ordering and by standard basis computations over $\mathbb{F}_p$ with respect to a global and a local monomial ordering, respectively.*

4. Puiseux Series, Valuations, and Integrality

In this section, we discuss some basic facts about Puiseux series and their connection to integrality. As in the introduction, K will denote a field of characteristic zero. Moreover, $K \subset L$ will be a field extension, with L algebraically closed.

4.1. Puiseux Series

The *field of Puiseux series* over L is the field

$$L\{\{X\}\} = \bigcup_{k=1}^{\infty} L((X^{1/k})).$$

The Newton-Puiseux theorem, which is closely related to the aforementioned finiteness theorem of Emmy Noether, says that $L\{\{X\}\}$ is the algebraic closure of $L((X))$. In particular, $L[[X^{1/k}]]$ is the integral closure of $L[[X]]$ in $L((X^{1/k}))$. See Eisenbud (1995, Chapter 13), Abhyankar (1990, Lecture 12).

We have a canonical *valuation map*

$$\upsilon : L\{\{X\}\} \setminus \{0\} \to \mathbb{Q},\ \gamma \mapsto \upsilon(\gamma),$$

where $\upsilon(\gamma) = \mathrm{ord}_X(\gamma)$ is the smallest exponent appearing in a term of γ. By convention, $\upsilon(0) = \infty$. The corresponding *valuation ring* $L\{\{X\}\}_{\upsilon\geq 0} = \bigcup_{k=1}^{\infty} L[[X^{1/k}]]$ consists of all Puiseux series with non-negative exponents only. Henceforth it will be denoted by $\mathcal{P}_X$.

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

4.2. Conjugate Puiseux Series

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

4.3. Rational Part

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

4.4. Notation

In what follows, $g \in K[[X]][Y]$ will be a square-free monic polynomial of degree $m \geq 1$ in Y. In subsequent sections, we will consider the defining polynomial $f \in K[X, Y]$ of an affine plane curve as in the introduction and its factorization

$$f = f_0\widetilde{f} = f_0f_1 \cdots f_r$$

given by the Weierstrass preparation theorem as in Equation (1) of the introduction. The polynomial g will then be either one of the branches $f_1, \ldots, f_r$ or their product $\widetilde{f}$ or f itself.

4.5. Puiseux Expansions

By the Newton-Puiseux theorem, the polynomial $g \in K[[X]][Y]$ has m roots $\gamma_1, \ldots, \gamma_m \in L\{\{X\}\}$:

$$g = (Y - \gamma_1) \cdots (Y - \gamma_m).$$

The γ_i are called the *Puiseux expansions* of g. The monic assumption guarantees that these expansions are integral over $K[[X]]$. In particular, they are all contained in some $L[[X^{1/k}]] \subset \mathcal{P}_X$, so that their terms have non-negative exponents only. Furthermore, each γ_i is algebraic

over $K((X))$, and its minimal polynomial over $K((X))$ has all its coefficients in $K[[X]]$ (see, for example, Swanson and Huneke (2006, Theorem 2.1.17)). We conclude that the γ_i can be grouped into conjugacy classes which correspond to the irreducible factors of g in $K[[X]][Y]$. If g is *absolutely irreducible*, that is, g is irreducible in $L[[X]][Y]$, then m is the least positive integer such that all γ_i are contained in $L[[X^{1/m}]]$. In fact, in this case, we have a representation of type

$$g(T^m, Y) = \prod (Y - \zeta(\omega^\ell T)),$$

where $\zeta \in L[[T]]$, and $\omega \in L$ is a primitive mth root of unity. That is, the Puiseux expansions of g are of type $\gamma_\ell(X) = \zeta(\omega^\ell X^{1/m})$. See Abhyankar (1990, Lecture 12), de Jong and Pfister (2000, Section 5.1).

4.6. Regularity Index and Singular Part

If $\gamma = a_1X^{t_1} + a_2X^{t_2} + \dots$ is a Puiseux expansion of g, with $0 \le t_1 < t_2 < \dots$ and no a_i zero, we define the *regularity index* of γ (with respect to g) to be the least exponent t_k such that no other Puiseux expansion of g has the same initial part $a_1X^{t_1} + \dots + a_kX^{t_k}$. This initial part is called the *singular part* of γ (with respect to g).

4.7. The Newton-Puiseux Algorithm

The Puiseux expansions of g can be computed recursively up to any given X-degree using the Newton-Puiseux algorithm (see, for example, de Jong and Pfister (2000)). Essentially, to get a solution $a_1X^{t_1} + a_2X^{t_2} + \dots$ of $g(X, \gamma(X)) = 0$, with $t_1 < t_2 < \dots$, the algorithm proceeds as follows: Starting from $g^{(0)} = g$ and $K^{(0)} = K((X))$, we commence the ith step of the algorithm by looking at a polynomial $g^{(i-1)} \in K^{(i-1)}[Y]$. We then choose one face Δ of the Newton polygon of $g^{(i-1)}$ such that all the other points of the polygon lie on or above the line containing the face. Let $g_\Delta^{(i-1)}$ be the sum of terms of $g^{(i-1)}$ involving the monomials of $g^{(i-1)}$ on Δ. That is, if $-\frac{w_1}{w_2}$ is the slope of Δ, then $g_\Delta^{(i-1)}$ is the sum of terms of $g^{(i-1)}$ of lowest $(1, \frac{w_2}{w_1})$-weighted degree. We write d_i for this degree. Choose an irreducible factor of $g_\Delta^{(i-1)}$ over $K^{(i-1)}$ and a root q_i of that factor. Note that q_i is of type $q_i = c_iX^{\frac{w_2}{w_1}}$, where c_i is a root of the polynomial $g_\Delta^{(i-1)}(1, Y)$. Now, let $K^{(i)} = K^{(i-1)}(q_i)$ and set $g^{(i)} = \frac{1}{X^{d_i}} g^{(i-1)}(X, q_i \cdot (1 + Y))$. Then the ith term of the expansion to be constructed is $a_iX^{t_i} = q_1 \cdots q_i$. It is clear from this construction that different conjugacy classes of expansions arise from different choices for the faces and irreducible factors of $g_\Delta^{(i-1)}$ over $K^{(i-1)}$, respectively.

Example 20. *The eight Puiseux expansions of the polynomial*

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

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

$$q_1 + q_1q_2 + q_1q_2q_3,$$

where the q_i satisfy

$$q_1^2 + X^3 = 0, \quad q_2^2 + \frac{1}{2X}q_1 = 0, \quad \textit{and} \quad q_3^2 - \frac{1}{8X}q_1 = 0.$$

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

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

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

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

and

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

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

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

and the extension

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

4.8. Maximal Integrality Exponents

Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be the set of Puiseux expansions of g. The *valuation* of a polynomial $q \in L\{\{X\}\}[Y]$ at g is defined to be $\upsilon_g(q) = \min_{1 \le i \le m} \upsilon_{\gamma_i}(q)$. Note that if q is monic of degree $d \ge 1$ in Y, and

$$q = (Y - \eta_1(X)) \cdots (Y - \eta_d(X))$$

is the factorization of q in $L\{\{X\}\}[Y]$, then

$$\upsilon_g(q) = \min_{1 \le i \le m} \sum_{j=1}^{d} \upsilon(\gamma_i - \eta_j).$$

Lemma 21. *Let $g \in K[[X]][Y]$ be a square-free monic polynomial of degree $m \ge 1$ in Y, with Puiseux expansions $\gamma_1, \ldots, \gamma_m$. Fix an integer d with $1 \le d \le m-1$. If $\mathcal{A} \subset \{1, \ldots, m\}$ is a subset of cardinality d, set*

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

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

Proof. That $\upsilon_g(\widetilde{p}_d) = \mathrm{Int}(\widetilde{\mathcal{A}})$ is clear from the definitions. That this number is the maximum valuation $\upsilon_g(q)$ as claimed follows as in the proof of van Hoeij (1994, Theorem 5.1), where the case $d = m - 1$ is treated. □

In the situation of the lemma, we write

$$o(\Gamma, d) = \upsilon_g(\widetilde{p}_d).$$

In case $d = m - 1$, we abbreviate

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

Remark 22. *By construction, we have*

$$o(\Gamma, 1) \leq \ldots \leq o(\Gamma, m-1).$$

Example 23. *Let* $g = (Y^2 + 2X^3) + Y^3 \in \mathbb{Q}[X, Y]$. *The Puiseux expansions of* g *are*

$$\begin{aligned} \gamma_1 &= a_1 X^{3/2} + X^3 + \ldots, \\ \gamma_2 &= a_2 X^{3/2} + X^3 + \ldots, \\ \gamma_3 &= -1 - 2X^3 + \ldots, \end{aligned}$$

where a_1, a_2 *are the roots of* $Z^2 + 2$. *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* $\widetilde{p}_2 = (Y - \gamma_2)(Y - \gamma_3)$ *and* $o(\Gamma, 2) = 3/2$.

Example 24. *Let* $g = (Y^3 + X^2)(Y^2 - X^3) + Y^6 \in \mathbb{Q}[X, Y]$. *The Puiseux expansions of* g *are*

$$\begin{aligned} \gamma_1 &= a_1 X^{2/3} + \ldots, & \gamma_4 &= X^{3/2} - 1/2x^{11/2} + \ldots, \\ \gamma_2 &= a_2 X^{2/3} + \ldots, & \gamma_5 &= -X^{3/2} + \ldots, \\ \gamma_3 &= a_3 X^{2/3} + \ldots, & \gamma_6 &= 1 + \ldots, \end{aligned}$$

where the a_i *are the roots of* $Z^3 + 1$. *Then* $\mathrm{Int}_1 = \mathrm{Int}_2 = \mathrm{Int}_3 = 2/3 + 2/3 + 2/3 + 2/3 + 0 = 8/3$, $\mathrm{Int}_4 = \mathrm{Int}_5 = 3/2 + 2/3 + 2/3 + 2/3 + 0 = 7/2$, *and* $\mathrm{Int}_6 = 0$. *We conclude that* $o(\Gamma, 5) = 7/2$.

Lemma 25. *Let* $g \in K[[X]][Y]$ *be a square-free monic polynomial of degree* $m \geq 1$ *in* Y, *let* $1 \leq d \leq m - 1$, *and let* R *be one of the rings* $K[X]$, $K[X]_{\langle X \rangle}$, $K[[X]]$, $K((X))$, $\mathcal{P}_X$, *or* $L\{\{X\}\}$. *The maximal valuation* $v_g(q)$, $q \in R[Y]$ *monic of degree* d *in* Y, *is independent of the choice of* R *from among this list.*

Proof. For any ring R as in the assertion, we have natural inclusions $K[X] \subset R \subset L\{\{X\}\}$. Hence, the value $\upsilon_g(q)$ is defined for any polynomial $q \in R[Y]$ and it suffices to show that there is a polynomial $p_d \in K[X][Y]$ such that $\upsilon_g(p_d)$ maximizes the valuation over $L\{\{X\}\}$ in degree d. For this, we recall from Lemma 21 that there is a polynomial $\widetilde{p}_d = \prod_{j \in \widetilde{\mathcal{A}}}(Y - \gamma_j) \in \mathcal{P}_X[Y]$ which maximizes the valuation over $L\{\{X\}\}$ in degree d. We may choose an integer k such that $\widetilde{p}_d \in L[[X^{1/k}]][Y]$. By truncating each γ_j to degree $\upsilon_g(\widetilde{p}_d)$, we get a polynomial $\overline{p}_d = \prod_{j \in \widetilde{\mathcal{A}}}(Y - \overline{\gamma}_j) \in L[X^{1/k}][Y]$ with $\upsilon_g(\overline{p}_d) = \upsilon_g(\widetilde{p}_d)$. Since $\overline{p}_d$ is monic in Y, by applying the trace map for $L(X^{1/k})$ over $L(X)$ to $\overline{p}_d$ and dividing by the integer leading coefficient of the resulting polynomial, we get a monic polynomial $p'_d \in L[X][Y]$ of degree d in Y with $\upsilon_g(p'_d) \geq \upsilon_g(\widetilde{p}_d)$ (note that the trace map sends $X^{1/k}$ to zero). Next, considering p'_d as a polynomial in X, Y with coefficients in L and adjoining these coefficients to K, we get a finite field extension $K \subset K'$ such that $p'_d \in K'[X][Y]$. Applying the trace map of this extension to p'_d and dividing by the integer leading coefficient of the resulting polynomial, we get a monic polynomial $p_d \in K[X][Y]$ of degree d in Y with $\upsilon_g(p_d) \geq \upsilon_g(\widetilde{p}_d)$. In fact, by Lemma 21 and the choice of $\widetilde{p}_d$, equality holds since $\widetilde{p}_d$ maximizes the valuation over $L\{\{X\}\}$. □

Example 26. *In Example 24, choosing* $\widetilde{p}_2 = (Y - \gamma_2)(Y - \gamma_3)$*, we get* $\overline{p}_2 = (Y - a_2X^{3/2})(Y + 1)$ *and, thus,* $p_2 = p_2' = Y(Y + 1)$*.*

The reason for considering the valuations $v_g(q)$ is that they are directly related to integrality: If $q \in K[[X]][Y]$ is monic of degree $0 \le d \le m - 1$ in Y, then $\lfloor v_g(q) \rfloor$ is the maximum integer e such that $q(x, y)/x^e$ is integral over

$$B = K[[x]][y] = K[[X]][Y]/\langle g \rangle .$$

For the lack of reference in this generality, we show this in Theorem 29 below (see also de Jong and Pfister (2000, Chapter 5, §1) and Walker (1978, Chapter 5, §10)). We refer to Swanson and Huneke (2006, Chapter 6) for a general introduction to valuations and their connection to integrality.

We will use the following result to reduce problems concerning a possibly reducible polynomial $g \in K[[X]][Y]$ to the irreducible case:

Proposition 27 (Splitting of Normalization)**.** *Let* $g \in K[[X]][Y]$ *be a square-free monic polynomial of degree* ≥ 1 *in* Y*, and let* $g = g_1 \cdots g_s$ *be its decomposition into irreducible factors* $g_i \in K[[X]][Y]$*. For each* i*,* $1 \le i \le s$*, set* $h_i = \prod_{j=1,\ j\neq i}^{s} g_j$*. Then the* g_i *and* h_i *are coprime in* $K((X))[Y]$*, so that there are polynomials* $a_i, b_i \in K[[X]][Y]$ *and integers* $c_i \in \mathbb{N}$ *fitting into Bézout identities of type*

$$a_i g_i + b_i h_i = X^{c_i}, \ \ \textit{for} \ \ i = 1, \ldots, s.$$

Furthermore, the normalization of $K[[X]][Y]/\langle g_1 \cdots g_s \rangle$ *splits as*

$$\overline{K[[X]][Y]/\langle g_1 \cdots g_s \rangle} \cong \bigoplus_{i=1}^{s} \overline{K[[X]][Y]/\langle g_i \rangle}, \tag{2}$$

where the splitting is given by

$$(t_1 \mod g_1, \ldots, t_s \mod g_s) \mapsto \sum_{i=1}^{r} \frac{b_i h_i t_i}{X^{c_i}} \mod g_1 \cdots g_s.$$

Proof. Clear by the Chinese remainder theorem and its proof. See de Jong and Pfister (2000, Theorem 1.5.20). □

We are now ready to clarify the relation between valuations and integrality. To prove the theorem which is relevant to us here, we need the result below:

Proposition 28. *Let* R *be an integral domain with quotient field* $\mathrm{Q}(R)$*. Then* $\phi \in \mathrm{Q}(R)$ *is integral over* R *iff* $v(\phi) \ge 0$ *for every valuation* v *on* $\mathrm{Q}(R)$ *whose valuation ring contains* R*. If* R *is Noetherian, it is enough to consider discrete valuations.*

Proof. See, for example, Swanson and Huneke (2006, Proposition 6.8.14). □

Theorem 29. *Let* $g \in K[[X]][Y]$ *be a square-free monic polynomial of degree* $m \ge 1$ *in* Y*. Let* $q \in K[[X]][Y]$ *be monic of degree* $0 \le d \le m - 1$ *in* Y*, and let* e *be the maximal integer such that* $\frac{q(x,y)}{x^e}$ *is integral over* $K[[x]][y] = K[[X]][Y]/\langle g \rangle$*. Then*

$$e = \lfloor v_g(q) \rfloor.$$

Proof. Let Γ be the set of Puiseux expansions of g. Then $\upsilon_g(q) = \min_{\gamma\in\Gamma} \upsilon_\gamma(q)$ by the very definition of $\upsilon_g(q)$ in Section 4.8. Hence, the assertion of the theorem is equivalent to the following statement:

$$\begin{aligned} \text{If } \widetilde{e} \text{ is a non-negative integer, then } q(x,y)/x^{\widetilde{e}} \text{ is integral over } K[[x]][y] \\ \iff \upsilon_\gamma(q) \geq \widetilde{e} \text{ for each } \gamma \in \Gamma. \end{aligned} \tag{3}$$

To show this statement, we proceed in four steps:

Step 1: We may assume that K is algebraically closed. To see this, we consider a field extension $K \subset L$ with L algebraically closed as before, and show that an element $w \in K((x))[y] = \mathrm{Q}(K[[X]][y]) \subset \mathrm{Q}(L[[X]][y]) = L((x))[y]$ is integral over $K[[x]][y]$ iff it is integral over $L[[x]][y]$. One direction is immediate: any integral equation for w over $K[[x]][y]$ is also an integral equation for w over $L[[x]][y]$. Conversely, if $p(w) = 0$ is an integral equation for w over $L[[x]][y]$, then adjoining the coefficients of p to K yields a finite field extension of K. Applying the trace map of this extension to p and dividing by the integer leading coefficient of the resulting polynomial, we get an integral equation for w over $K[[x]][y]$.

Step 2: We may assume that g is irreducible. Indeed, if $g = g_1 \cdots g_s$ is the factorization of g as in Proposition 27, each g_i, $1 \leq i \leq s$, corresponds to a conjugacy class of the Puiseux expansions of g (see Section 4.5). Hence, by Proposition 27, statement (3) holds for g iff it holds for each g_i.

Step 3: We may assume that g is a Weierstrass polynomial. Indeed, since we already assume that g is irreducible, g is either a Weierstrass polynomial or a unit in $K[[x,y]]$. In the latter case, $g(0,0) \neq 0$, and it follows from Hensel's lemma that $g(0,Y) = (Y-c)^m$ for some $c \in K$ (see Section 7.3 below for Hensel's lemma). Hence, the translation $Y \to Y + c$ turns g into a Weierstrass polynomial.

Step 4: From the Newton-Puiseux theorem, we know that under the assumptions above, the Puiseux expansions of g are of type $\eta(\omega^\ell X^{1/m})$, $l = 1, \ldots, m$, where $\eta \in TK[[T]]$, and ω is a primitive mth root of unity (see Section 4.5). In particular, the value $\upsilon_\gamma(q)$ on the right hand hand side of (3) is independent of the choice of $\gamma \in \Gamma$. To show that (3) holds, we may, hence, work with the fixed expansion $\gamma(X) = \eta(X^{1/m})$.

For the implication from left to right in (3), we then note that

$$\upsilon_\gamma : K((x))[y] \to \mathbb{Z} \cup \{\infty\},\ \phi \mapsto m\upsilon_\gamma(\phi),$$

is a well-defined valuation on $K((x))[y]$ whose valuation ring contains $K[[x]][y]$. Thus, Remark 28 implies that if $\upsilon_\gamma(q) < \widetilde{e}$, then $q/x^{\widetilde{e}}$ is not integral.

For the converse implication, we conclude from de Jong and Pfister (2000, Theorem 5.1.3) that the map $K[[x,y]] \to K[[T]]$ defined by $(x,y) \mapsto (T^m, \eta(T))$ allows us to regard $K[[T]]$ as the normalization of $K[[x,y]]$. Hence, if $q(x,y)/x^{\widetilde{e}}$ is not integral, then the fraction $q(T^m, \eta(T))/T^{m\widetilde{e}} \notin K[[T]]$, that is, the fraction has negative order in T. But

$$\mathrm{ord}_T(q(T^m, \eta(T))/T^{m\widetilde{e}}) = m \cdot \mathrm{ord}_X(q(X, \gamma(X))/X^{\widetilde{e}}),$$

which shows that $\upsilon_\gamma(q) < \widetilde{e}$. This concludes the proof. □

Definition 30. *Let $g \in K[[X]][Y]$ be as above. If $q \in K[[X]][Y]$ is monic of degree $0 \leq d \leq m-1$ in Y, then we call*

$$e_g(q) := \lfloor v_g(q) \rfloor$$

the integrality exponent of q with respect to g. *Furthermore, we call*

$$e_{g,d} := \max\left\{e_g(q) \mid q \in K[[X]][Y] \text{ monic in } Y,\ \deg q = d\right\} = \lfloor o(\Gamma, d)\rfloor$$

the maximal integrality exponent with respect to g in degree d.

Remark 31. *By Remark 22, we have*

$$0 = e_{g,0} \leq e_{g,1} \leq \ldots \leq e_{g,m-1}.$$

Definition 32. *With notation as above, we call*

$$E(g) = e_{g,m-1}$$

the maximal integrality exponent with respect to g.

For the defining equation of an affine plane curve as in the introduction, the analogue to Theorem 29 is well-known:

Proposition 33. *Let $f \in K[X][Y]$ be an irreducible monic polynomial of degree $n \geq 1$ in Y. Let $q \in K[X][Y]$ be monic of degree $0 \leq d \leq n-1$ in Y, and let e be the maximal integer such that $\frac{q(x,y)}{x^e}$ is integral over $A = K[x][y] = K[X][Y]/\langle f\rangle$. Then*

$$e = \lfloor \upsilon_f(q)\rfloor.$$

Proof. We know that an element $\phi \in \mathrm{Q}(A) = K(x)[y]$ is integral over A iff it is integral over $K[x]$. By Stichtenoth (2009, Theorem 3.2.6), the latter is equivalent to the condition that $\upsilon(\phi) \geq 0$ for every (discrete) valuation υ on $\mathrm{Q}(A)$ whose valuation ring contains $K[x]$. Similar to the proof of Theorem 29, this in turn means that $v_\gamma(\phi) \geq 0$ for all Puiseux expansions γ of f (see van Hoeij (1994, Section 2.4)). The result follows. □

5. Integral Bases and Integrality Exponents

As in the previous section, let $g \in K[[X]][Y]$ be a square-free monic polynomial of degree $m \geq 1$ in Y, and write

$$B = K[[x]][y] = K[[X]][Y]/\langle g\rangle\,.$$

Then $\overline{B}$ coincides with the integral closure of $K[[x]]$ in $K((x))[y]$. In fact, $\overline{B}$ is a free $K[[x]]$-module of rank m: If g is irreducible, this follows from Remark 2; if g is arbitrary, apply the splitting of normalization as in Proposition 27 to reduce to the irreducible case.

Definition 34. *With notation as above, we refer to any integral basis for $\overline{B}$ over $K[[x]]$ as an* integral basis for g.

In this section, we study the shape of integral bases in terms of integrality exponents, and we show how to construct an integral basis for g from given integral bases for its irreducible factors. With regard to integrality exponents, we use the terminology from Definition 30. Specifically, $e_{g,d}$ denotes the maximal integrality exponent with respect to g in degree d, for $d = 0, \ldots, m-1$.

Proposition 35. *With notation as above, for each $d = 1, \dots, m-1$, let a monic polynomial $p_d \in K[[X]][Y]$ of degree d in Y and an integer e_d be given. Then*

$$\overline{\mathcal{B}} = \left\{ 1 = p_0, \frac{p_1(x,y)}{x^{e_1}}, \dots, \frac{p_{m-1}(x,y)}{x^{e_{m-1}}} \right\}$$

is an integral basis for g iff $e_d = e_g(p_d) = e_{g,d}$, for $d = 1, \dots, m-1$.

Proof. Write $B'_d = \left\langle 1, \frac{p_1(x,y)}{x^{e_1}}, \dots, \frac{p_d(x,y)}{x^{e_d}} \right\rangle_{K[[x]]}$ for each d, and $B' = \left\langle \overline{\mathcal{B}} \right\rangle = B'_{m-1}$.

First suppose that $\overline{\mathcal{B}}$ is an integral basis for g, and consider a fixed d. Then $e_d \le e_g(p_d) \le e_{g,d}$. To show that these numbers are equal, we choose an element $q \in K[[X]][Y]$ which is monic in Y of degree d and satisfies $e_g(q) = e_{g,d}$. Then $\frac{q(x,y)}{x^{e_{g,d}}}$ is integral over $K[[x]]$ by Theorem 29, so $\frac{q(x,y)}{x^{e_{g,d}}} \in B'_d$ since $\overline{\mathcal{B}}$ is an integral basis for g. Writing $\frac{q(x,y)}{x^{e_{g,d}}}$ as a $K[[x]]$-linear combination of the generators of B'_d, and comparing the coefficients of y^d, we get $e_d = e_{g,d}$, as desired.

Conversely, suppose that the equalities $e_d = e_g(p_d) = e_{g,d}$ hold. Then the $p_d(x,y)/x^{e_d}$ are integral over B. In particular, $B \subset B' \subset \overline{B}$. Hence, to show that $B' = \overline{B}$ (and, thus, that $\overline{\mathcal{B}}$ is an integral basis for g), it is enough to prove the following: Given a polynomial $q \in K[[X]][Y]$ of degree $0 \le d \le m-1$ in Y such that $\frac{q(x,y)}{x^e} \in \overline{B}$ for some $e \in \mathbb{N}$, we must have $\frac{q(x,y)}{x^e} \in B'_d$.

We do induction on d. There is nothing to show in case $d = 0$. If $d \ge 1$, let $c \in K[[X]]$ be the leading coefficient of $q \in K[[X]][Y]$. After factoring out a unit in $K[[X]]$, we can assume that $c = X^t$, for some $t \in \mathbb{N}$. Write q as a product $q = X^t \widetilde{q}$, with $\widetilde{q} \in K((X))[Y]$ monic in Y. Then, by Lemma 25 and Theorem 29, we have $\lfloor \upsilon_g(\widetilde{q}) \rfloor \le e_{g,d} = e_d$, hence

$$e \le t + e_g(\widetilde{q}) = t + \lfloor \upsilon_g(\widetilde{q}) \rfloor \le t + e_d.$$

This implies $\frac{x^t p_d(x,y)}{x^e} = \frac{p_d(x,y)}{x^{e-t}} \in B'_d \subset \overline{B}$. Since $\deg_Y(q - X^t p_d) < d$ and $\frac{q(x,y)}{x^e} - \frac{x^t p_d(x,y)}{x^e} \in \overline{B}$, the induction hypothesis gives $\frac{q(x,y)}{x^e} - \frac{x^t p_d(x,y)}{x^e} \in B'_{d-1} \subset B'_d$. Therefore $\frac{q(x,y)}{x^e} \in B'_d$, as claimed. □

Remark 36. *We say that an integral basis as in Proposition 35 is of* monic triangular type. *Together with Lemmas 21 and 25, the proposition shows the existence of such bases, where the p_d can even be chosen to be polynomials in $K[X][Y]$. Henceforth, whenever we speak of an integral basis of monic triangular type, we tacitly assume that the p_d are chosen that way. How to actually compute bases of this type in the case where $g = f_i$ is a branch of our given polynomial f is a topic of Section 7.5.*

Proposition 37. *Let $g = g_1 \cdots g_s \in K[[X]][Y]$ be the decomposition of a square-free monic polynomial g of degree ≥ 1 in Y into its irreducible factors. For $i = 1, \dots, s$, let*

$$\mathcal{B}^{(i)} = \left\{ 1 = p_0^{(i)}, \frac{p_1^{(i)}}{X^{e_1^{(i)}}}, \dots, \frac{p_{m_i-1}^{(i)}}{X^{e_{m_i-1}^{(i)}}} \right\}$$

represent an integral basis for g_i as in Proposition 35. With notation as in Proposition 27, for each i, set

$$\widetilde{\mathcal{B}}^{(i)} = \left\{ \frac{b_i h_i}{X^{c_i}}, \frac{b_i h_i p_1^{(i)}}{X^{c_i + e_1^{(i)}}}, \dots, \frac{b_i h_i p_{m_i-1}^{(i)}}{X^{c_i + e_{m_i-1}^{(i)}}} \right\}.$$

Then $\widetilde{\mathcal{B}}^{(1)} \cup \ldots \cup \widetilde{\mathcal{B}}^{(s)}$ represents an integral basis for g.

Proof. Immediate from Proposition 27. □

There is an algorithmic way of transferring an integral basis for g as in the proposition to an integral basis for g of monic triangular type:

Remark 38. *Each matrix M with entries in the PID $K[[X]]$ of maximal column rank has a uniquely determined upper triangular Hermite normal form $H = (p_{ij})$, where the diagonal elements are of type $p_{ii} = X^{\nu_i}$, and the p_{ij}, $j > i$, are polynomials in $K[X]$ of degree $< \nu_i$. So the entries of H are polynomials in X, while the entries of M are power series in X. To compute H from M via unimodular row operations, we have to consider suitably truncated power series, that is, we work over $K[[X]]/\langle X^{t+1}\rangle$, where t is a precision which guarantees a correct result H (see Durvye (2008)). Applying this in the situation of Proposition 37, starting from a set $\widetilde{\mathcal{B}}^{(1)} \cup \ldots \cup \widetilde{\mathcal{B}}^{(s)}$ as in the proposition and proceeding as in Remark 4, we get an integral basis for g of type*

$$\overline{\mathcal{B}} = \left\{ p_0(x,y), \frac{p_1(x,y)}{x^{e_1}}, \ldots, \frac{p_{m-1}(x,y)}{x^{e_{m-1}}} \right\},$$

with polynomials $p_d \in K[X][Y]$ of degree d in Y.

Corollary 39. *With notation as in Remark 38 above, let $\overline{\mathcal{B}}$ be obtained by the recipe given in that remark. Then $\overline{\mathcal{B}}$ is an integral basis for g of monic triangular type.*

Proof. Fix a degree d, and write $\overline{\mathcal{B}}_d$ for the set of elements in $\overline{\mathcal{B}}$ of y-degree $\leq d$. By construction, the leading coefficient of p_d is a power of x, say $x^{\widetilde{e}_d}$. Now consider an integral basis $\overline{\mathcal{B}}'$ for g of monic triangular type (according to Remark 36, such bases exist). Expressing the dth element of $\overline{\mathcal{B}}'$ as a $K[[x]]$-linear combination of the elements in $\overline{\mathcal{B}}_d$ and comparing the coefficients of y^d, we see that $\widetilde{e}_d = 0$ and $e_d = e_{g,d}$. □

6. Normalization of Plane Curves via Localization and Completion: Local Contributions From Integral Bases for the Branches

In this section, $f \in K[X,Y]$ denotes the defining polynomial of an irreducible plane curve $C \subset \mathbb{A}^2(K)$ with assumptions as in the introduction. For simplicity of the presentation, we focus on the case of a K-rational singularity, supposing that this singularity is the origin: let $P = \langle x, y\rangle \in \mathrm{Sing}(A)$. How to reduce to the case of such a singularity is a topic of Section 7.

As in Equation (1) of the introduction, factorize f as

$$f = f_0 \widetilde{f} = f_0 f_1 \cdots f_r,$$

where $f_0 \in K[[X]][Y]$ is a unit in $K[[X,Y]]$, and $f_1, \ldots, f_r$ are irreducible Weierstrass polynomials in $K[[X]][Y]$, the branches of f (over K, centered at the origin).

Remark 40. *Recall from Section 4.5 that the irreducible factors of f in $K[[X]][Y]$ correspond to the conjugacy classes of the Puiseux expansions of f. Developed up to a given degree, the f_i, $0 \leq i \leq r$, may hence be found by computing all expansions via the Newton-Puiseux algorithm. There is, however, a more effective approach: in Section 7.2, we will present a method which, based on Hensel's lemma, makes considerably less use of the Newton-Puiseux algorithm.*

Proposition 37 shows us how to obtain an integral basis for f from integral bases for its irreducible factors. It turns out, however, that factors whose zeros on the line $X = 0$ are non-singular points of C can be treated simultaneously, in a more efficient way. To further simplify our presentation, we assume in addition that f_0 is the product of these factors. Suppose from now on that the origin is the only singularity of C with X-coordinate zero. That is, if $\langle x\rangle \subset Q \in \mathrm{Sing}(A)$, then $Q = P = \langle x, y\rangle$. We then also say, that P is the only singularity (of A) at $X = 0$. How to reduce to this case is another topic of Section 7.

Using Puiseux series, we show in Proposition 41 that under the additional assumption above, we can read off an integral basis for f from such a basis for $\widetilde{f}$. More precisely, taking Remark 36 into account and starting from a basis for $\widetilde{f}$ of monic triangular type, we will specify a basis for f of the same type. This will allow us to prove in Proposition 43 that the set $\mathcal{B}_f$ representing the latter basis also represents a set of $K[x]$-module generators for the local contribution to $\overline{A}$ at P. This is a crucial result on our way to computing an integral basis for $\overline{A}$ over $K[x]$ via our local approach. An interesting side remark is that $\mathcal{B}_f$ represents, in addition, a set of free generators for $\overline{K[X]_{\langle X\rangle}[Y]/\langle f\rangle}$ over $K[X]_{\langle X\rangle}$.

Proposition 41. *Write f as a product $f = f_0\widetilde{f}$ as in Equation* (1) *of the introduction, where $f_0 \in K[[X]][Y]$ is a unit in $K[[X, Y]]$ of degree m_0, and $\widetilde{f} \in K[[X]][Y]$ is a Weierstrass polynomial of degree m. Suppose that $P = \langle x, y\rangle$ is the only singularity at $X = 0$. Let*

$$\mathcal{B}_{\widetilde{f}} = \left\{1 = p_0, \frac{p_1}{X^{e_1}}, \ldots, \frac{p_{m-1}}{X^{e_{m-1}}}\right\}$$

represent an integral basis for $\widetilde{f}$ of monic triangular type. Let $\overline{f}_0 \in K[X][Y]$ be a (monic) polynomial such that

$$\overline{f}_0 \equiv f_0 \bmod X^{e_{m-1}}.$$

Then

$$\mathcal{B}_f = \left\{1, Y, Y^2, \ldots, Y^{m_0-1}, \overline{f}_0 p_0, \frac{\overline{f}_0 p_1}{X^{e_1}}, \ldots, \frac{\overline{f}_0 p_{m-1}}{X^{e_{m-1}}}\right\}$$

represents an integral basis for f of monic triangular type.

Proof. Set $e_0 = 0$. Since $\mathcal{B}_{\widetilde{f}}$ represents an integral basis for $\widetilde{f}$, we obtain from Proposition 35 that the maximal integrality coefficients with respect to $\widetilde{f}$ satisfy $e_{\widetilde{f},d} = e_d$, for $d = 0, \ldots, m-1$. Our assertion, in turn, will follow by applying Proposition 35 to f, provided we show that $e_{f,d} = 0$, for $d = 1, \ldots, m_0 - 1$, and $e_{f,d} = e_{d-m_0}$, for $d = m_0, \ldots, n-1$. For this, let $q \in K[[X]][Y]$ be any monic polynomial of degree $1 \le d \le n-1$ in Y, and let $\eta_1, \ldots, \eta_d$ be the Puiseux expansions of q. Factorize q as

$$q = q_0\widetilde{q},$$

where $q_0 \in K[[X]][Y]$ is a unit in $K[[X, Y]]$ and $\widetilde{q} \in K[[X]][Y]$ is a Weierstrass polynomial.

Let $\gamma_1, \ldots, \gamma_{m_0}$ be the Puiseux expansions of f_0, and let $\gamma_{m_0+1}, \ldots, \gamma_n$ be those of $\widetilde{f}$. Note that for the latter γ_i, the constant terms are zero. For the former γ_i, the constant terms, say $a_0^{(i)}$, are non-zero and, since we suppose that the origin is the only singularity at $X = 0$, pairwise different. Further note that if for some $1 \le i \le m_0$ there is no expansion η_j, $1 \le j \le d$, with initial term $a_0^{(i)}$, then

$$v_f(q) = \min_{1\le i\le n} v_{\gamma_i}(q) = \min_{1\le i\le n} \sum_{j=1}^{d} v(\gamma_i - \eta_j) = 0.$$

If $d < m_0$, then we can always find an initial term $a_0^{(i)}$ as above since there are m_0 pairwise different initial terms. Since q was chosen arbitrarily, this implies that $e_{f,d} = 0$ for $d < m_0$.

Now suppose that $d \geq m_0$. Then, if $e_f(q) > 0$, any $a_0^{(i)}$ must appear as the initial term of some η_j, $1 \leq j \leq d$. In particular,

$$m_0 \leq \deg_Y(q_0).$$

We claim that $e_f(q) \leq e_{d-m_0}$. This is clear if $e_f(q) = 0$. To prove the claim if $e_f(q) > 0$, note that for any i, we have

$$\upsilon_{\gamma_i}(q) = \upsilon_{\gamma_i}(q_0) + \upsilon_{\gamma_i}(\widetilde{q}) = \begin{cases} \upsilon_{\gamma_i}(\widetilde{q}) & \text{if } \gamma_i(0) = 0 \\ \upsilon_{\gamma_i}(q_0) & \text{if } \gamma_i(0) \neq 0. \end{cases}$$

Hence,

$$\begin{aligned} \upsilon_f(q) &= \min_{1\leq i\leq n} \upsilon_{\gamma_i}(q) = \min\left\{ \min_{1\leq i\leq m_0} \upsilon_{\gamma_i}(q_0), \min_{m_0<i\leq n} \upsilon_{\gamma_i}(\widetilde{q}) \right\} \\ &= \min\{\upsilon_{f_0}(q_0), \upsilon_{\widetilde{f}}(\widetilde{q})\} \leq \upsilon_{\widetilde{f}}(\widetilde{q}). \end{aligned}$$

Since $m_0 \leq \deg_Y(q_0)$, we conclude that

$$e_f(q) = \left\lfloor \upsilon_f(q) \right\rfloor \leq \left\lfloor \upsilon_{\widetilde{f}}(\widetilde{q}) \right\rfloor \leq e_{\widetilde{f},d-\deg_Y(q_0)} \leq e_{\widetilde{f},d-m_0} = e_{d-m_0},$$

which shows our claim. Since q was chosen arbitrarily, it follows that $e_{f,d} \leq e_{d-m_0}$. To prove that these numbers are equal, we set $k = d - m_0$ and show that $\overline{f}_0 p_k / x^{e_k}$ is integral over A. For this, let $\gamma = \gamma_i$ be any Puiseux expansion of f. If $\gamma(0) = 0$, then $\upsilon_\gamma(\overline{f}_0 p_k) \geq \upsilon_\gamma(p_k) \geq \upsilon_{\widetilde{f}}(p_k) \geq e_k$. If $\gamma(0) \neq 0$, then $\upsilon_\gamma(\overline{f}_0 p_k) \geq \upsilon_\gamma(\overline{f}_0) \geq e_{m-1} \geq e_k$ by the very definition of $\overline{f}_0$. □

Remark 42. *It is clear from Proposition 35 that Proposition 41 holds more generally for polynomials p_d in $K[[X]][Y]$ instead of just $K[X][Y]$; in addition, it is not necessary to truncate f_0 to $\overline{f}_0$. However, in its above form, $\mathcal{B}_f$ also represents both a set of free generators for $\overline{K[X]_{\langle X\rangle}[Y]/\langle f\rangle}$ over $K[X]_{\langle X\rangle}$ (by faithful flatness) and (as we will show next) a set of $K[x]$-module generators for the minimal local contribution to $\overline{A}$ at P.*

Proposition 43. *Let*

$$\mathcal{B} = \left\{1 = p_0, \frac{p_1}{X^{e_1}}, \ldots, \frac{p_{n-1}}{X^{e_{n-1}}}\right\}$$

represent an integral basis for f of monic triangular type. Suppose that $P = \langle x, y\rangle$ is the only singularity at $X = 0$. Then $\mathcal{B}$ also represents a set of $K[x]$-module generators for the minimal local contribution to $\overline{A}$ at P.

Proof. By the assumption and Proposition 35, we have $e_d = e_g(p_d) = e_{g,d}$ for all d. Write $A'_d = \left\langle 1, \frac{p_1(x,y)}{x^{e_1}}, \ldots, \frac{p_d(x,y)}{x^{e_d}} \right\rangle_{K[x]}$ for each d, and $A' = A'_{n-1}$. Then $A \subset A' \subset \overline{A}$ by Proposition 33. To show that A' is the minimal local contribution to A at P, we proceed in three steps.

Step 1: We show: If $q \in K[X][Y]$ is a polynomial of degree $0 \leq d \leq n-1$ in Y such that $\frac{q(x,y)}{x^e} \in \overline{A}$ for some $e \in \mathbb{N}$, then $\frac{q(x,y)}{x^e} \in A'_d$.

As in the proof of Proposition 35, we do induction on d. There is nothing to show in case $d = 0$. If $d \geq 1$, let $c \in K[X]$ be the leading coefficient of $q \in K[X][Y]$ and write $q = c\widetilde{q} = X^t \widetilde{c}\widetilde{q}$,

where $\widetilde{q} \in K((X))[Y]$ is monic in Y of degree d, and $\tilde{c} \in K[X]$ is not a multiple of X. Then, by Lemma 25 and Theorem 29, $\lfloor v_f(\widetilde{q}) \rfloor \leq e_{g,d} = e_d$, hence

$$e \leq t + e_g(\widetilde{q}) = t + \lfloor v_f(\widetilde{q}) \rfloor \leq t + e_d.$$

This implies $\frac{c(x)p_d(x,y)}{x^e} = \tilde{c}(x)\frac{p_d(x,y)}{x^{e-t}} \in A'_d \subset \overline{A}$. Since $\deg_Y(q - cp_d) < d$ and $\frac{q(x,y)}{x^e} - \frac{c(x)p_d(x,y)}{x^e} \in \overline{A}$, the induction hypothesis gives $\frac{q(x,y)}{x^e} - \frac{c(x)p_d(x,y)}{x^e} \in A'_{d-1} \subset A'_d$. Therefore $\frac{q(x,y)}{x^e} \in A'_d$, as claimed.

Step 2: Having defined A' as an intermediate $K[x]$-module $A \subset A' \subset \overline{A}$, we now show that A' is, in fact, an intermediate ring and, thus, an A-module. That is, we show that A' is closed under multiplication. For this, note that any product of two elements of A' takes the form

$$\frac{q(x,y)}{x^e} \cdot \frac{q'(x,y)}{x^{e'}} = \frac{q''(x,y)}{x^{e+e'}} \in \overline{A},$$

where $q'' \in K[X][Y]$ satisfies $\deg_Y(q'') < n$. But then, by step 1, the product is in A'.

Step 3: We finally localize: Set

$$D = K[x]_{\langle x \rangle}[y] = K[X]_{\langle X \rangle}[Y]/\langle f \rangle \text{ and } D' = \left\langle 1, \frac{p_1(x,y)}{x^{e_1}}, \ldots, \frac{p_{n-1}(x,y)}{x^{e_{n-1}}} \right\rangle_{K[x]_{\langle x \rangle}}.$$

Then $D \subset D' \subset \overline{D}$. In fact, it follows by faithful flatness that $D' = \overline{D}$ (see Remark 42 above). We also give a direct argument for this equality: Let $\frac{q(x,y)}{h(x)} \in \overline{D}$ be an arbitrary element of $\overline{D}$, with polynomials $q \in K[X][Y]$ of Y-degree $< n$ and $h \in K[X]$. Write h as a product $h = X^e \cdot \widetilde{h}$, where $\widetilde{h}(x)$ is a unit in $K[x]_{\langle x \rangle}$. Then also $\frac{q(x,y)}{x^e} \in \overline{D}$, so that there exists a polynomial $p \in K[X]$ such that $p(x)$ is a unit in $K[x]_{\langle x \rangle}$ and $p(x)\frac{q(x,y)}{x^e} \in \overline{A}$. It follows from step 1 that $p(x)\frac{q(x,y)}{x^e} \in A' \subset D'$, so that $\frac{q(x,y)}{h(x)} \in D'$ and, hence, $D' = \overline{D}$. This implies that

$$A'_Q = \overline{D}_Q = \overline{D_Q} = \overline{A_Q}$$

for all $Q \in \operatorname{Spec}(A)$ with $\langle x \rangle \subset Q$. On the other hand, since we suppose that $P = \langle x, y \rangle$ is the only singularity at $X = 0$, we have $\overline{A_Q} = A_Q$ for all $Q \in \operatorname{Spec} A$ with $\langle x \rangle \subset Q$ and $Q \neq P$. Moreover, $A'_Q = A_Q$ for all Q with $\langle x \rangle \not\subset Q$ since the denominators of the generators of A' are contained in $\langle x \rangle$. We conclude that A' is the minimal contribution to A at P. □

Remark 44. *Computing a set $\mathcal{B}$ as in Proposition 43 requires that we know the precision t up to which all power series in X appearing in the process must be developed. Of course, the maximum power of X appearing in the denominators of the elements of $\mathcal{B}$ will do. However, this number is known to us only a posteriori, once $\mathcal{B}$ has already been computed. We will address this problem in Section 7.*

In the setting of the example below, it turns out that the desired precision is $t = 3$.

Example 45. *Factorizing the polynomial $f = (Y^3 + X^2)(Y^2 - X^3) + Y^6$ from Example 24 as in Equation 1 of the introduction, we get $f = f_0 \cdot f_1 \cdot f_2$, where $f_0 \equiv Y + (-X^3 - X^2 + 1)$, $f_1 \equiv Y^3 + (X^3 + X^2)Y^2 + (-X^2)Y + X^2$, $f_2 \equiv Y^2 - X^3 \mod X^4$.*

Applying Proposition 27 to the product $f_1 \cdot f_2$, we set $h_1 = f_2$ and use the extended Euclidean algorithm to compute the Bézout identity $a_1 f_1 + b_1 h_1 = X^2$, where $a_1 \equiv -4X^3Y - 2X^3 - 2X^2Y - X^2 + XY - Y - 1$, $b_1 \equiv -4X^3Y^2 - 2X^3Y - 2X^2Y^2 - 3X^3 - 2X^2Y + XY^2 - Y^2 - Y \mod X^4$.

Computing integral bases for f_1 and f_2, we get $\left\{1, y, \frac{y^2}{x}\right\}$ and $\left\{1, \frac{y}{x}\right\}$, respectively (proceed as in Section 7.5 below). Hence, by Proposition 37, the union of the sets

$$\widetilde{\mathcal{B}}^{(1)} = \left\{\frac{b_1 f_2}{X^2}, \frac{b_1 f_2 Y}{X^2}, \frac{b_1 f_2 Y^2}{X^3}\right\} \qquad \text{and} \qquad \widetilde{\mathcal{B}}^{(2)} = \left\{\frac{a_1 f_1}{X^2}, \frac{a_1 f_1 Y}{X^3}\right\}$$

represents an integral basis for $f_1 \cdot f_2$. Proceeding as in Remark 38, we get the set

$$\left\{1, Y, \frac{Y^2}{X}, \frac{Y^3}{X^2}, \frac{Y^4 + X^2 Y}{X^3}\right\}$$

which represents an integral basis for $f_1 \cdot f_2$ of monic triangular type.

Finally, applying Proposition 41, with $\overline{f}_0 = Y + (-X^3 - X^2 + 1)$, we conclude that

$$\left\{1, \overline{f}_0, \overline{f}_0 Y, \frac{\overline{f}_0 Y^2}{X}, \frac{\overline{f}_0 Y^3}{X^2}, \frac{\overline{f}_0 (Y^4 + X^2 Y)}{X^3}\right\}$$

represents an integral basis for f of monic triangular type.

7. Normalization of Plane Curves via Localization and Completion: The Algorithmic Point of View

Let $A = K[C] = K[x, y] = K[X, Y]/\langle f(X, Y)\rangle$ be as before. In this section, we present our complete algorithm for computing the minimal local contributions to $\overline{A}$ at the primes $P \in \mathrm{Sing}(A)$. In particular, we discuss effective ways of finding the branches of f, and of computing integral bases for these. The normalization $\overline{A}$ itself and an integral basis for $\overline{A}$ over $K[x]$, respectively, are then obtained along the lines of Proposition 13 and Remark 5.

We start with a sketch of the algorithm. Here, for simplicity of the presentation, we assume that there are no two singular points of C with the same X-coordinate. This allows us to apply the results of Section 6 to all singularities. How to deal with a curve having singular points with the same X-coordinate will be addressed in Remarks 73 and 75. See Examples 74 and 76 for illustrations.

7.1. Summary of the Algorithm

From a **theoretical point of view**, the algorithm involves the following steps which will be applied to each prime $P \in \mathrm{Sing}(A)$:

1. If P corresponds to a K-rational singularity, **translate the singularity to the origin**. If P corresponds to a set of conjugate singularities over K, extend the base field K as needed, and **translate one of the singularities to the origin**.

For the singularity at the origin, do (to simplify the presentation, we will still write K and f for the extended field and the transformed equation of our curve, respectively):

2. Taking Lemma 25 and Theorem 29 into account, use the recipe from Lemma 21 to determine the **maximum integrality exponent** $E(f)$.

3. Set $c_0 = 0$. For $i = 1, \ldots, r$, determine integers c_i as in Proposition 27. Then **factorize** $f = \prod_{i=0}^{r} f_i$ as in Equation (1) of the introduction, developing each f_i up to X-degree $E(f) + c_i$. For this, make use of Hensel's lemma and the Newton-Puiseux algorithm as described in Sections 7.3 and 7.4 below.

4. For $i = 1, \ldots, r$, compute the Bézout coefficients b_i from Proposition 27 up to X-degree $E(f) + c_i$.

5. Use Algorithm 6 in Section 7.5 below to compute for each $1 \leq i \leq r$ an **integral basis for the branch** f_i of monic triangular type.

6. Based on the results of the previous steps, use the recipe from Proposition 37 to construct for each $1 \leq i \leq r$ a set $\mathcal{B}^{(i)}$ as in the proposition. Then convert $\mathcal{B}^{(1)} \cup \ldots \cup \mathcal{B}^{(r)}$ into an integral basis for $f_1 \cdots f_r$ of monic triangular type by using unimodular row operations as in Remark 38 (take Corollary 39 into account).

7. Starting from the integral basis for $f_1 \cdots f_r$ obtained in step (6), compute an integral basis $\overline{\mathcal{B}}$ for f of monic triangular type. Here, use Algorithm 9 in Section 7.8 below which is based on Proposition 41. It is then clear from the proposition that $\overline{\mathcal{B}}$ also represents a set of $K[x]$-module generators for the minimal local contribution to $\overline{A}$ at $\langle x, y \rangle$.

8. If necessary, apply the **inverse translation** to the elements of the local contribution to restore the singularity to the original position.

9. If P corresponds to a set of conjugate singularities, then use Remark 70 below to modify the numerators and denominators of the local contribution obtained in steps (7) and (8) for one of the singularities over the extended field in order to obtain the **minimal local contribution to $\overline{A}$ at P** over the original field.

From a **practical point of view**, we face the problem that in the approach outlined above, we need to determine the c_i *a priori*. Moreover, the computation of the Bézout coefficients b_i via the extended Euclidean algorithm is very time consuming. To remedy these issues, relying on Proposition 63 below, we will replace the b_i and c_i in steps (3) and (4) by easier to construct polynomials $\beta_i \in K[X, Y]$ and appropriate vanishing orders, respectively.

We refer to the following subsections for more details.

7.2. Puiseux Expansions

As already pointed out in Remark 40, the factors f_i appearing in the decomposition

$$f = f_0 \widetilde{f} = f_0 f_1 \cdots f_r$$

of f as in Equation (1) of the introduction can be found by computing the Puiseux expansions of f (up to a given degree). Since this is expensive, however, we propose a different approach which, via Hensel's lemma, makes considerably less use of the Newton-Puiseux algorithm.

In describing the new approach, we use the following terminology. If $g \in K[[X]][Y]$ is any square-free monic polynomial of degree ≥ 1 in Y, we partition the set of all Puiseux expansions of g into *Puiseux blocks*. The 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 $K((X))$. The *Puiseux segment* represented by an

expansion γ with $\gamma(0) = 0$ is defined to be the union of all blocks whose expansions have the same initial exponent as γ. That is, we have one Puiseux segment for each face of the Newton polygon of g. In addition, all Puiseux expansions γ of g 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 g are divided into Puiseux segments, each segment consists of Puiseux blocks, and each block is the union of classes of conjugate expansions.

Example 46. *Suppose that the Puiseux expansions of our given 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 of f 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 $\{\gamma_8, \gamma_9\}$.

7.3. Hensel's Lemma

We will use Hensel's lemma in the following form:

Lemma 47 (Hensel's Lemma)**.** *Let $F \in K[[X]][Y]$ be a monic polynomial in Y. Assume that $F(0, Y) = g_0 h_0$, with monic polynomials $g_0, h_0 \in K[Y]$ such that $\langle g_0, h_0 \rangle = K[Y]$. Then there exist unique monic polynomials $G, H \in K[[X]][Y]$ such that*

1. *$F = GH$,*
2. *$G(0, Y) = g_0$, $H(0, Y) = h_0$.*

In fact, for each $k \in \mathbb{N}$, there exist unique $g_k, h_k \in K[X, Y]$ of X-degree $\leq k$ such that

3. *$F \equiv g_k h_k$ in $(K[[X]]/\langle X^{k+1} \rangle)[Y]$,*
4. *$g_k \equiv g_i$, $h_k \equiv h_i$ in $(K[[X]]/\langle X^{i+1} \rangle)[Y]$, $i = 0, \dots, k-1$.*

Proof. See, for example, Abhyankar (1990). □

Conditions (3) and (4) imply that the polynomials g_k and h_k can be computed inductively along the X-degree, solving for each k a system of ℓ linear equations in ℓ variables, where ℓ is the Y-degree of F: For each $0 \leq i \leq \ell - 1$, we get an equation by comparing the coefficients of $X^k Y^i$ in F with those in $g_k h_k$. For further reference in this paper, we state the resulting procedure as Algorithm 1, `HenselLift`, omitting the actual computation steps.

Our first application of `HenselLift` is to address the Puiseux segment consisting of all Puiseux expansions γ of f with $\gamma(0) \neq 0$. That is, we decompose f as $f = f_0 \widetilde{f}$ as in Equation (1) of the introduction, separating the unit f_0 from the component $\widetilde{f}$ vanishing at the origin (we develop f_0 and $\widetilde{f}$ up to the desired X-degree). This is summarized in Algorithm 2, `SeparateUnit`.

Algorithm 1 `HenselLift`

Input: $e \in \mathbb{N}$; $F \in K[X,Y]$ monic in Y; $g_0, h_0 \in K[Y]$ monic with $F(0,Y) = g_0 h_0$, $\langle g_0, h_0 \rangle = K[Y]$.

Output: $G, H \in K[[X]][Y]$ developed up to X-degree e, with $G(0,Y) = g_0$, $H(0,Y) = h_0$, and $F \equiv GH \mod X^{e+1}$.

Algorithm 2 `SeparateUnit`

Input: $e \in \mathbb{N}$; $f \in K[X,Y]$ irreducible and monic in Y, with $f(0,0) = 0$.

Output: $f_0, \widetilde{f} \in K[[X]][Y]$ as in Equation (1) of the introduction, developed up to X-degree e.

1: compute monic $g_0, h_0 \in K[Y]$ with $Y \nmid g_0$, $h_0 = Y^k$ for some $k \in \mathbb{N}_{\geq 1}$, and $f(0,Y) = g_0 h_0$

2: **return** `HenselLift`(e, f, g_0, h_0)

Example 48. *Let $f = (Y-X)(Y+X)(Y+2X) + Y^7 \in \mathbb{Q}[X,Y]$. Then there are four Puiseux expansions of f with $\gamma(0) \neq 0$ and three expansions with $\gamma(0) = 0$ (note that $f(0,Y) = Y^3 + Y^7 = Y^3(1+Y^4)$). We write $\gamma_1, \ldots, \gamma_4$ for the former expansions and $\gamma_5 = X + \ldots$, $\gamma_6 = -X + \ldots$, $\gamma_7 = -2X + \ldots$ for the latter ones. We apply Algorithm 2 to develop the products $f_0 = \gamma_1 \cdots \gamma_4$ and $\widetilde{f} = \gamma_5\gamma_6\gamma_7$ up to X-degree 2, calling* `HenselLift`$(2, f, g_0, h_0)$ *with $g_0 = 1 + Y^4$ and $h_0 = Y^3$. The output is $g_2 = 5X^2Y^2 - 2XY^3 + Y^4 + 1$, $h_2 = Y^3 + 2XY^2 - 2X^2Y$.*

An alternative way would be to decompose $f = f_0\widetilde{f}$ by means of the Weierstrass Division Theorem. However, applying Hensel's lemma allows for more generality since it does not require to have one factor vanishing at the origin. This will be useful in Section 7.4 below, where we will study a local version of Hensel's lemma. Furthermore, in cases where the singularity under consideration has no K-rational coordinates, we may use Hensel's lemma to modify our algorithms so that there is no need to move the singularity to the origin. As a consequence, no field extension is required at this point. For brevity of the presentation, we do not give the details of this strategy.

7.4. A Local Version of Hensel's Lemma

Being able to decompose $f = f_0\widetilde{f}$ as discussed above, we now aim at factorizing $\widetilde{f} \in K[[X]][Y]$ into the branches $f_1, \ldots, f_r$ of f.

We begin by separating the different Puiseux segments of $\widetilde{f}$. To describe how, let $g \in K[[X]][Y]$ be any square-free monic polynomial of degree $m \geq 1$ in Y, and such that $\gamma(0) = 0$ for each Puiseux expansion γ of g. Then, since all factors of g vanish at the origin, we cannot apply Hensel's lemma directly: no matter how we choose g_0, h_0 with $g = g_0 h_0$, the condition $\langle g_0, h_0 \rangle = K[Y]$ will not be satisfied (consider, for example, the products $(Y-\gamma_1)(Y-\gamma_2)(Y-\gamma_3)$ and $(Y-\gamma_4)(Y-\gamma_5)$ in Example 24).

To overcome this problem, we transform g as explained in what follows. Write

$$\begin{aligned}
\gamma_1 &= a_1^{(1)} X^{t_1^{(1)}} + a_2^{(1)} X^{t_2^{(1)}} + \ldots, \\
\gamma_2 &= a_1^{(2)} X^{t_1^{(2)}} + a_2^{(2)} X^{t_2^{(2)}} + \ldots, \\
&\vdots \\
\gamma_m &= a_1^{(m)} X^{t_1^{(m)}} + a_2^{(m)} X^{t_2^{(m)}} + \ldots
\end{aligned}$$

for the Puiseux expansions of g, where all $a_1^{(i)}$ are non-zero. Suppose for simplicity that $t := t_1^{(1)} = \min_{1\le i\le m} t_1^{(i)}$. Naively, to separate the Puiseux segment corresponding to t from the rest, we are tempted to substitute X^tY for Y in $g = (Y-\gamma_1)\cdots(Y-\gamma_m) \in K[[X]][Y]$ and cancel out X^t in all factors. However, this would introduce fractional exponents and force us, thus, to leave $K[[X]][Y]$. We therefore proceed in a different way: Write $t = u/v$, with $u, v \in \mathbb{N}_{\ge 1}$ coprime, and set

$$\begin{aligned} F(X,Y) &= g(X^v, X^uY)/X^{mu} \\ &= (Y - (a_1^{(1)} + a_2^{(1)}X^{t_2^{(1)}} + \dots))\cdots(Y - (a_1^{(m)}X^{t_1^{(m)}} + \dots)) \in K[[X]][Y]. \end{aligned}$$

Then F has factors not vanishing at the origin, and these correspond to the Puiseux expansions of f forming the Puiseux segment with smallest initial exponent t. Applying Hensel's lemma, reversing the transformation, and iterating the process yields Algorithm 3.

Algorithm 3 `SegmentSplitting`

Input: $e \in \mathbb{N}$; $g \in K[[X]][Y]$ monic in Y, developed up to X-degree e; we suppose that $\gamma(0) = 0$ for each Puiseux expansion γ of g.

Output: Weierstrass polynomials $g_1, \dots, g_\ell \in K[[X]][Y]$, developed up to X-degree e, with $g \equiv g_1\cdots g_\ell \mod X^{e+1}$, and each g_i corresponding to precisely one Puiseux segment of g as outlined above.

1: from the Newton polygon of g, read off the pairwise different initial exponents $t_1, \dots, t_\ell$ of the Puiseux expansions of g
2: **if** $\ell = 1$ **then**
3: **return** $\{g\}$
4: $t = u/v = \min\{t_1, \dots, t_\ell\}$, with $u, v \in \mathbb{N}_{\ge 1}$ coprime
5: $m = Y$-degree of g
6: $F = g(X^v, X^uY)/X^{mu}$
7: compute monic $g_0, h_0 \in K[Y]$ with $Y \nmid g_0$, $h_0 = Y^k$ for some $k \in \mathbb{N}_{\ge 1}$, and $F(0,Y) = g_0h_0$
8: $G, H =$ `HenselLift`(ve, F, g_0, h_0)
9: $\widetilde{G} = X^{(\deg_Y G)u}G$, $\widetilde{H} = X^{(\deg_Y H)u}H$
10: $g_1 = \widetilde{G}(X^{1/v}, Y/X^{u/v})$, $h = \widetilde{H}(X^{1/v}, Y/X^{u/v})$
11: **return** $\{g_1\} \cup$ `SegmentSplitting`(e, h)

Remark 49. *See de Jong and Pfister (2000, Theorem 5.1.17) for an alternative approach which extends the Weierstrass Division Theorem.*

Example 50. *Let* $f = (Y^2 + 2X^3)((Y + 2X^2)^2 + X^5) + Y^6 \in \mathbb{Q}[X, Y]$. *Evaluating* f *at* $X = 0$, *we get* $f(0, Y) = (Y^2 + 1)Y^4$. *Applying* `SeparateUnit`$(8, f)$ *gives the (truncated) factors*

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

The Puiseux expansions of $\widetilde{f}$ *are*

$$\begin{aligned} \gamma_{1,2} &= a_{1,2}X^{3/2} + a_{1,2}X^{9/2} - 4X^5 - 6a_{1,2}X^{11/2} + 16X^6 + 41/2a_{1,2}X^{13/2} - 52X^7 + \dots, \\ \gamma_{3,4} &= -2X^2 + b_{1,2}X^{5/2} + 16b_{1,2}X^{13/2} + 48X^7 + \dots, \end{aligned}$$

with roots $a_{1,2}$ of Z^2+2 and $b_{1,2}$ of Z^2+1.
The smallest initial exponent t of these expansions is $t = u/v = 3/2$. We compute

$$F(X,Y) = \widetilde{f}(X^2, X^3Y)/X^{12} = -46X^{10}Y^2 - 32X^9Y^3 - 64X^9Y + 8X^8Y^2 + 8X^7Y^3 + 16X^8 + 16X^7Y + 4X^6Y^2 + X^4Y^2 + 2X^4 + 4X^2Y^2 + 4XY^3 + Y^4 + 8X^2 + 8XY + 2Y^2.$$

Now note that $F(0,Y) = (Y^2+2)Y^2$. Applying Hensel's lemma to the factors Y^2+2 and Y^2, we obtain

$$G(X,Y) = \ldots + 116X^{10} - 48X^9Y - 16X^8 + 8X^7Y + 4X^6 + Y^2 + 2,$$
$$H(X,Y) = \ldots + 30X^{10} + 16X^9Y - 8X^8 + X^4 + 4X^2 + 4XY + Y^2.$$

So if we set $\widetilde{G}(X,Y) = X^6G(X,Y)$, $\widetilde{H}(X,Y) = X^6H(X,Y)$ and apply the inverse transformations, we get

$$g_1 = \widetilde{G}(X^{1/2}, Y/X^{3/2}) = \ldots + 116X^8 - 48X^6Y - 16X^7 + 8X^5Y + 4X^6 + Y^2 + 2X^3,$$
$$h = \widetilde{H}(X^{1/2}, Y/X^{3/2}) = \ldots + 30X^8 + 16X^6Y - 8X^7 + X^5 + 4X^4 + 4X^2Y + Y^2.$$

Since there are only two conjugacy classes of Puiseux expansions of $\widetilde{f}$, we may conclude that $f_1 = g_1$ and $f_2 = h$ are the branches of f.

The next step is to split the Puiseux segments of $\widetilde{f}$ into their Puiseux blocks. Fix such a segment $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$. Then the γ_i satisfy $\gamma_i(0) = 0$. Moreover, by the very definition of a segment, the γ_i must have the same initial exponent, say, $t = u/v$. Write g for the factor of $\widetilde{f}$ corresponding to Γ, and η for the largest common initial part of the rational parts of the γ_i.

If $\eta = 0$, set $F(X,Y) = g(X^v, X^uY)/X^{mu}$ as above. Then $F(0,Y)$ will have different factors, all not vanishing at the origin, and corresponding to the individual blocks. Hence, we can separate these blocks iteratively, using Hensel's lemma as above.

If $\eta \neq 0$, set

$$\widetilde{g}(X,Y) = g(X, Y+\eta).$$

Then the Puiseux expansions of $\widetilde{g}$ coincide with those of g, except that we omit the common initial term η. We can then use segment splitting combined with block splitting to separate the blocks. Substituting $Y - \eta$ for Y to reverse the transformation, we get the desired factors.

We summarize this strategy in Algorithm 4, `BlockSplitting`. In Line 11 of the algorithm, the presence of a power of a linear factor implies that the relevant expansions share a common non-zero rational part. It is, then, possible to decompose the corresponding factor further.

Remark 51. *We expect that the ideas from de Jong and Pfister (2000, Theorem 5.1.20) can in some cases also be used for our purposes. However, as stated in de Jong and Pfister (2000), the theorem is not as general as we require.*

The final step on our way to find the branches f_i is to separate the factors corresponding to different conjugacy classes of Puiseux expansions within each given block. For this, all algorithms known to us require that we extend our base field K – a factor $(Y-\gamma_1)\cdots(Y-\gamma_s)$ is obtained by computing the individual γ_i up to the desired X-degree via the Newton-Puiseux algorithm, and expanding the product. Of course, this last step is only needed if there is a Puiseux block containing more than one conjugacy class of Puiseux expansions.

In Algorithm 5, we sum up the discussion above, arriving at a general `Splitting` algorithm.

Algorithm 4 `BlockSplitting`

Input: $e \in \mathbb{N}$; $g \in K[[X]][Y]$ monic in Y, developed up to X-degree e; we suppose that $\gamma(0) = 0$ for each Puiseux expansion γ of g, and that these expansions form a single Puiseux segment.

Output: Weierstrass polynomials $g_1, \ldots, g_k \in K[[X]][Y]$, developed up to X-degree e, with $g \equiv g_1 \cdots g_k \mod X^{e+1}$, and each g_i corresponding to precisely one Puiseux block of the given Puiseux segment.

$L = \emptyset$
η = the common rational part of all Puiseux expansions of g
if $\eta = 0$ **then**
  $t = u/v$, with $u, v \in \mathbb{N}_{\geq 1}$ coprime, the initial exponent of the Puiseux expansions of g (which is the same for all expansions by assumption and is obtained from the Newton polygon of g)
  $m = Y$-degree of g
  $F = g(X^v, X^u Y)/X^{mu}$
  compute $g_0, h_0 \in K[Y]$ with $g_0 \neq 1$ irreducible or a power of an irreducible polynomial, g_0, h_0 coprime, and $F(0, Y) = g_0 h_0$.
  if $h_0 \neq 1$ **then**
    $G, H =$ `HenselLift`(ve, F, g_0, h_0)
    $g_1 = G(X^{1/v}, Y/X^{u/v})$, $h = H(X^{1/v}, Y/X^{u/v})$
    if g_0 is not a power of a linear factor in Y **then**
      return $\{g_1\} \cup$ `BlockSplitting`(e, h)
    else
      return `BlockSplitting`$(e, g_1) \cup$ `BlockSplitting`(e, h)
  else
    return $\{g\}$
else
  $\widetilde{g} = g(X, Y + \eta)$
  $\{g_1, \ldots, g_\ell\} =$ `SegmentSplitting`$(e, \widetilde{g})$
  for $1 \leq i \leq \ell$ **do**
    $\{h_1, \ldots, h_s\} =$ `BlockSplitting`(e, g_i)
    $L = L \cup \{h_1(X, Y - \eta), \ldots, h_s(X, Y - \eta)\}$
  return L

Algorithm 5 `Splitting`

Input: $e \in \mathbb{N}$; $f \in K[X][Y]$ irreducible and monic in Y of degree n.

Output: $f_0, f_1, \ldots, f_r \in K[[X]][Y]$ with $f = f_0 f_1 \cdots f_r$ as in Equation (1) of the introduction, all developed up to X-degree e.

1: $f_0, \widetilde{f} =$ `SeparateUnit`(e, f)
2: $L = \{f_0\}$
3: $\{g_1, \ldots, g_\ell\} =$ `SegmentSplitting`$(e, \widetilde{f})$, the factors corresponding to the different Puiseux segments of $\widetilde{f}$
4: **for** $i = 1, \ldots, \ell$ **do**
5: $\quad \{h_1, \ldots, h_s\} =$ `BlockSplitting`(e, g_i)
6: $\quad$ **for** $j = 1, \ldots, s$ **do**
7: $\quad\quad \Delta_1, \ldots, \Delta_m =$ sets of singular parts of the Puiseux expansions of h_j, grouped into conjugacy classes
8: $\quad\quad$ **if** $m > 1$ **then**
9: $\quad\quad\quad$ **for** $k = 1, \ldots, m$ **do**
10: $\quad\quad\quad\quad \gamma_1, \ldots, \gamma_s =$ Puiseux expansions associated to Δ_k, developed up to X-degree e
11: $\quad\quad\quad\quad p = (Y - \gamma_1) \cdots (Y - \gamma_s)$, developed up to X-degree e
12: $\quad\quad\quad\quad L = L \cup \{p\}$
13: $\quad\quad$ **else**
14: $\quad\quad\quad L = L \cup \{h_j\}$
15: **return** L

7.5. Integral Bases for the Branches

We now explain how to find integral bases for the branches of f. More generally, let $g \in K[[X]][Y]$ be an irreducible Weierstrass polynomial of degree m. Then the Puiseux expansions of g form a complete conjugacy class $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$. Let $K \subset K(\alpha)$ be a finite field extension over which all γ_i are defined.

Taking Proposition 35 and Corollary 39 into account, our goal is an algorithm, Algorithm 6, which constructs for each $1 \leq d \leq m-1$ a monic polynomial $p_d \in K[X][Y]$ of degree d in Y whose integrality exponent satisfies $e_g(p_d) = \lfloor v_g(p_d) \rfloor$. We begin by introducing what we call the extended characteristic exponents of g. We use the following notation:

Notation 52. *Given $\gamma \in L\{\{X\}\}$ and $t \in \mathbb{Q}_{\geq 0}$, we write $\overline{\gamma}^{(t)}$ (respectively $\overline{\gamma}^{(<t)}$) for the truncation of γ to degree t (respectively $< t$).*

Consider the factorization

$$g = g_1 \cdots g_s \tag{4}$$

of g into absolutely irreducible Weierstrass polynomials $g_i \in K(\alpha)[[X]][Y]$, and write $k := \deg(g_1) = \ldots = \deg(g_s)$. Factorize g_1 as

$$g_1 = \prod (Y - \zeta(\omega^\ell X^{1/k})),$$

where $\zeta \in K(\alpha)[[T]]$, and ω is a primitive kth root of unity (see Section 4.5). Consider the action of $\mathrm{Gal}(K(\alpha)/K)$ on $K(\alpha)[[T]]$, let $G = \mathrm{Gal}(K(\alpha)/K)/\mathrm{Stab}(\zeta)$, and set $H = G \times \mathbb{Z}/k\mathbb{Z}$. Let $\eta(X) = \zeta(X^{1/k})$. Given $\sigma = (\overline{\varphi}, \ell) \in H$, write $\sigma\eta(X) = \varphi\zeta(\omega^\ell X^{1/k})$. Then

$$g = \prod\nolimits_{\sigma \in H} (Y - \sigma\eta(X)).$$

Now we truncate: If $t \in \mathbb{Q}_{\geq 0}$, let

$$l(t) = \left| H\overline{\eta}^{(t)} \right|$$

be the orbit length under the action of H after truncation. Moreover, write

$$\{l_0, \ldots, l_\nu\} := \{l(t) \mid t \in \mathbb{Q}_{\geq 0}\},$$

where the l_i are sorted such that $1 = l_0 < \ldots < l_\nu = m$. Then $l_i | l_{i+1}$, for $0 \leq i < \nu$. The corresponding minimal truncation degrees achieving these orbit lengths are

$$t_i := \min\{t \in \mathbb{Q}_{\geq 0} \mid l(t) = l_i\}.$$

We call $t_0, t_1, \ldots, t_\nu$ the *extended characteristic exponents* of g.

Let $M = H\overline{\eta}^{<t_\nu}$ be the orbit of the truncation to degree $< t_\nu$, and set

$$\overline{m} := |M| = l_{\nu-1}.$$

Then

$$\overline{g} := \prod\nolimits_{\rho(X) \in M} (Y - \rho(X)) \in K[X, Y] \tag{5}$$

is an irreducible Weierstrass polynomial with extended characteristic exponents $t_0, \ldots, t_{\nu-1}$.

Remark 53. *Characteristic exponents as introduced, for example, in de Jong and Pfister (2000, Section 5.2) are classical invariants of irreducible complex plane curve singularities. With notation as above, if g is absolutely irreducible (then $s = 1$ in (4) and $k = m$), and if we assume for simplicity that $v(\gamma) > 1$, the* characteristic exponents *of g are defined recursively as*

$$\begin{aligned} k_0 &:= m, \\ k_1 &:= \min\{j \mid b_j \neq 0 \text{ and } k_0 \nmid j\}, \\ k_i &:= \min\{j \mid b_j \neq 0,\ \gcd(k_0, k_1, \ldots, k_{i-1}) \nmid j\} \text{ for } i > 1, \text{ if this set is non-empty}, \end{aligned}$$

where $\gamma = \sum_{j>m} b_j X^{j/m}$. There are only finitely many such numbers $k_0 < k_1 < \cdots < k_\nu$, we have $\gcd(k_0, k_1, \ldots, k_\nu) = 1$, and the t_i and k_i are related by the following equalities:

$$t_i = \frac{k_i}{m}, \quad \text{for } 1 \leq i \leq \nu.$$

Furthermore, de Jong and Pfister (2000, Theorem 5.2.16) yields the valuation formula below (see also Section 7.7):

$$v_g(\overline{g}) = \frac{k_\nu}{m} + \sum_{j=1}^{\nu-1} \frac{\gcd(k_0, k_1, \ldots, k_{j-1}) - \gcd(k_0, k_1, \ldots, k_j)}{\gcd(k_0, k_1, \ldots, k_{\nu-1})} \frac{k_j}{m}.$$

We will use the following results to show the correctness of Algorithm 6.

Lemma 54. *Let $p, q \in K[X][Y]$ be two monic polynomials of the same degree d in Y, where $1 \leq d \leq m - 1$. Suppose that the Puiseux expansions of both p and q are truncations of Puiseux expansions of g, and that there is a bijection between the sets of expansions of p and q such that each expansion of p is a truncation of the corresponding expansion of q. Then $v_g(p) \leq v_g(q)$.*

Proof. Let $p = \prod_{1\le\ell\le d}(Y-\overline{\gamma}_{i_\ell}^{(s_\ell)})$ and $q = \prod_{1\le\ell\le d}(Y-\overline{\gamma}_{i_\ell}^{(t_\ell)})$, with Puiseux expansions γ_{i_ℓ} of g. Let $\gamma\in\Gamma$ be an arbitrary Puiseux expansion of g. Then $v(\gamma-\overline{\gamma}_{i_\ell}^{(s_\ell)})\le v(\gamma-\overline{\gamma}_{i_\ell}^{(t_\ell)})$, for each $1\le\ell\le d$. Indeed, no cancellation in $\gamma-\overline{\gamma}_{i_\ell}^{(s_\ell)}$ can occur that does not occur in $\gamma-\overline{\gamma}_{i_\ell}^{(t_\ell)}$ as well. Hence, by the valuation formula in Section 4.8, $v_g(p)=\min_{\gamma\in\Gamma}\sum_{1\le\ell\le d}v(\gamma-\overline{\gamma}_{i_\ell}^{(s_\ell)})\le\min_{\gamma\in\Gamma}\sum_{1\le\ell\le d}v(\gamma-\overline{\gamma}_{i_\ell}^{(t_\ell)})=v_g(q)$, as claimed. □

Remark 55. *Recall that all Puiseux expansions of g are conjugate by our assumptions on g. Hence, if $p\in K[X][Y]$, then $v_g(p)=v_\gamma(p)$ for each Puiseux expansion γ of g. We conclude that v_g is additive in our setting here: If $p,q\in K[X][Y]$, then $v_g(pq)=v_g(p)+v_g(q)$ (this is not true in general since it may happen that the valuations of g at p and q are obtained as the valuations at expansions of g in different orbits).*

Lemma 56. *For each $d=1,\dots,m-1$, there is a monic polynomial $p_d\in K[X][Y]$ of degree d in Y whose Puiseux expansions are all truncations of Puiseux expansions of g and whose valuation at g is the maximal valuation $v_g(q)$, for $q\in K[[X]][Y]$ monic of degree d in Y.*

Proof. By Lemmas 21 and 25, for each given d, there is a polynomial $q_d\in K[X][Y]$ of degree d in Y such that $v_g(q_d)$ is the maximal valuation $v_g(q)$, for $q\in K[[X]][Y]$ monic of degree d in Y. Arguing as in Section 4.5, since $q_d\in K[X][Y]$, we may group the Puiseux expansions of q_d into conjugacy classes over $K(X)$ which correspond to the irreducible factors of q_d in $K[X,Y]$.

Let $\{\chi_1,\dots,\chi_s\}$ be any of these classes, and let $u=(Y-\chi_1)\cdots(Y-\chi_s)$ be the corresponding factor of q_d. Then no χ_i coincides with a Puiseux expansion of g since otherwise all expansions of g would arise as expansions of q_d, a contradiction to $m>s$. The maximum degree $t\in\mathbb{Q}_{\ge0}$ of a term of χ_i for which $\chi_i^{(t)}$ is a truncation of a Puiseux expansion of g is independent of the choice of i. We have $w=(Y-\overline{\chi}_1^{(t)})\cdots(Y-\overline{\chi}_s^{(t)})\in K[X,Y]$ since the truncated expansions are conjugate over $K(X)$ as well. Moreover, by construction, $v_g(w)\ge v_g(u)$.

Replacing u by w and proceeding in the same way with the other conjugacy classes of expansions of q_d, we obtain a polynomial $p_d\in K[X][Y]$ with $v_g(p_d)=v_g(q_d)$, and such that each Puiseux expansion of p_d is a truncation of an expansion of g. □

Example 57. *Consider the polynomial*

$$g=X^{10}-2X^9-2X^8-4X^7Y-2X^5Y^2+X^4Y^2+X^3Y^2+2X^2Y^3+Y^4\in\mathbb{Q}[X,Y],$$

and fix the degree $d=3$. The Puiseux expansions of g are

$$\gamma_{1,2}=a_{1,2}X^{3/2}-X^2-\frac{1}{2}a_{1,2}X^{11/2}+\dots,$$
$$\gamma_{3,4}=b_{1,2}X^{5/2}-\frac{1}{4}b_{1,2}X^{9/2}+\dots,$$

with roots $a_{1,2}$ of Z^2+1 and $b_{1,2}$ of Z^2-2. From Lemma 21 we see that $\widetilde{p}_3=(Y-\gamma_1)(Y-\gamma_2)(Y-\gamma_3)\in\overline{\mathbb{Q}}\{\{X\}\}[Y]$ is a polynomial of degree 3 in Y such that $v_g(\widetilde{p}_3)=11/2$ is the maximal valuation $v_g(q)$, for $q\in K[[X]][Y]$ monic of degree 3 in Y. Now note that the polynomial $q_3=(X^6+2X^5+X^4+2X^3Y+X^3+2X^2Y+Y^2)(Y-X^4)\in\mathbb{Q}[X][Y]$, whose Puiseux expansions are $\chi_{1,2}=a_{1,2}X^{3/2}-X^2-X^3$ and $\chi_3=X^4$, satisfies $v_g(q_3)=11/2$. Proceeding as in the previous proof, we truncate $\chi_{1,2}$ to $\overline{\chi}_{1,2}=a_{1,2}X^{3/2}-X^2$. Then, since no Puiseux expansion of g starts with the term X^4, we truncate χ_3 to $\overline{\chi}_3=0$. In sum, $p_3=(Y-\overline{\chi}_1)(Y-\overline{\chi}_2)(Y-\overline{\chi}_3)=X^4Y+X^3Y+2X^2Y^2+Y^3$ is a polynomial as in Lemma 56.

The result below is the key lemma for the recursion step of Algorithm 6:

Lemma 58. *The polynomial $\overline{g} \in K[X][Y]$ of degree $\overline{m}$ in Y defined in (5) is such that $v_g(\overline{g})$ is the maximal valuation $v_g(q)$, for $q \in K[[X]][Y]$ monic of degree $\overline{m}$ in Y.*

Proof. Choose a monic polynomial $p = p_{\overline{m}} \in K[X][Y]$ of degree $\overline{m}$ in Y as in Lemma 56. That is, the Puiseux expansions of p are all truncations of Puiseux expansions of g, and $v_g(p)$ is the maximal valuation $v_g(q)$, for $q \in K[[X]][Y]$ monic of degree $\overline{m}$ in Y. We may suppose:

$$\begin{gathered}\text{From among all polynomials of degree } \overline{m} \text{ as in Lemma 56,} \\ p \text{ has the least number of irreducible factors in } K[X,Y].\end{gathered} \tag{6}$$

We show that p is irreducible. Suppose the contrary, and let $p = p_1 \cdots p_s$ be the decomposition of p into irreducible factors $p_i \in K[X][Y]$ which are monic in Y, say of degrees d_i, where we suppose that $d_1 \leq d_2 \leq \ldots \leq d_s$. Then $\{d_1, \ldots, d_s\} \subset \{l_1, \ldots, l_{\nu-1}\}$, we have $d_i | d_{i+1}$, for $1 \leq i < s$, and $d_s | \overline{m}$. Let s' be maximal such that $d_1 = d_2 = \ldots = d_{s'}$. Then $s' > 1$. Indeed, since both $d_2 + \ldots + d_s$ and $d_1 + d_2 + \ldots + d_s = \overline{m}$ are divisible by d_2, also d_1 is divisible by d_2, so that $d_1 = d_2$. If $s' < s$, the same argument shows that $d_1 + \ldots + d_{s'}$ is divisible by $d_{s'+1}$. Hence, since $d_1 = d_2 = \ldots = d_{s'}$, there exists $1 < t \leq s'$ such that $d_1 + \ldots + d_t = d_{s'+1}$. If $s' = s$, let $t = s$. Then $d_1 + \ldots + d_t = \overline{m}$, and we set $p_{s'+1} = \overline{g}$.

In any case, considering that the Puiseux expansions of the p_i are finite, we may suppose that the largest exponent appearing in the expansions of p_t is greater than or equal to the respective exponent of each p_i, $1 \leq i \leq t-1$. Then the expansions of $p_1, \ldots, p_{t-1}$ arise as truncations of those of p_t.

Therefore, by Lemma 54, $v_g(p_1 \cdots p_t) \leq v_g(p_t^t) \leq v_g(p_{s'+1})$ (for the second inequality note that if we write $p_{s'+1}$ in terms of its Puiseux expansions, and truncate these expansions to the degree of the expansions of p_t, we get p_t^t). It follows that $v_g(p) \leq v_g(p_{s'+1} \cdot p_{t+1} \cdots p_s)$, a contradiction to (6). Hence p is irreducible, as claimed.

Since p is irreducible, and by the very definition of $\overline{g}$, the polynomials p and $q = \overline{g}$ satisfy the assumptions of Lemma 54. So $v_g(p) \leq v_g(\overline{g})$, which concludes the proof. □

We are now ready to formulate Algorithm 6 and proof its correctness.

Theorem 59. *Algorithm 6 works correctly as specified.*

Proof. We have to show that the polynomial p_d returned by the algorithm has the desired maximal valuation at g in degree d. For this, we retain the notation introduced in the previous discussion. We write $p = \overline{g} = \prod_{i=1}^{\overline{m}} (Y - \rho_i(X))$ and distinguish two cases.

Case 1: Let $\overline{d} = 0$. Then necessarily $u > 1$ and $p_d = p^u$. By Lemma 56, there is a monic polynomial $p'_d \in K[X][Y]$ of degree d in Y whose Puiseux expansions are all truncations of Puiseux expansions of g and whose valuation at g is maximal in degree d. We have to show that $v_g(p'_d) \leq v_g(p_d)$. Supposing the contrary, we may write p'_d as a product $p'_d = p^{u'} q'$, with $0 \leq u' < u$ and $q' \in K[X][Y]$ monic in Y. Then $\deg(q') \geq \deg(p) = \overline{m}$. We may assume that $p^{u'}$ is the maximal power of p appearing as a factor of a monic polynomial $q_d \in K[X][Y]$ of degree d in Y with $v_g(q_d) > v_g(p_d)$. To get a contradiction, it suffices to show that q' has a monic factor $p' \in K[X][Y]$ of degree $\deg(p)$ in Y. Indeed, Lemma 58 then gives $v_g(p) \geq v_g(p')$ and, thus, $v_g(p^{u'+1}(q'/p')) \geq v_g(p'_d)$, a contradiction to the maximality assumption on u'.

To show that a factor p' of q' as desired exists, let $q' = q_1 \cdots q_s$ be the decomposition of q' into irreducible factors $q_i \in K[X][Y]$, all monic in Y, say of degrees d_i, where we suppose that

Algorithm 6 `IntegralBasisElement`

Input: $\Delta = \{\delta_1, \ldots, \delta_m\}$, the set of singular parts of the Puiseux expansions of an irreducible Weierstrass polynomial $g \in K[[X]][Y]$ of degree m; an integer d with $1 \leq d \leq m-1$.

Output: $p_d \in K[X][Y]$ monic of degree d in Y such that $v_g(p)$ is the maximal valuation $v_g(q)$, for $q \in K[X][Y]$ monic of degree d in Y.

1: let $t = t_\nu$ be the maximal extended characteristic exponent of g
2: let $\rho_1, \ldots, \rho_{\overline{m}}$ be the pairwise different elements of $\left\{\overline{\delta}_1^{<t}, \ldots, \overline{\delta}_m^{<t}\right\}$
3: $u = \left\lfloor \frac{d}{\overline{m}} \right\rfloor$
4: $\overline{d} = d - u \cdot \overline{m}$
5: $q = 1$, $p = 1$
6: **if** $\overline{d} > 0$ **then**
7: $\quad q =$ `IntegralBasisElement`$(\{\rho_1, \ldots, \rho_{\overline{m}}\}, \overline{d})$
8: **if** $u > 0$ **then**
9: $\quad p = \prod_{i=1}^{\overline{m}} (Y - \rho_i(X))$
10: **return** $p_d = p^u q$

$d_1 \leq d_2 \leq \ldots \leq d_s$. Due to our assumption on the Puiseux expansions of p'_d, it follows as in the proof of Lemma 58 that $d_i | d_{i+1}$, for $1 \leq i < s$, and that $d_s | \deg(p)$. Then $d_s | (\deg(p) - d_s)$ and $d_j | (\deg(p) - (d_{j+1} + \ldots + d_{s-1} + d_s))$, for $1 \leq j < s$. Hence, if $\deg(p) - (d_{j+1} + \ldots + d_{s-1} + d_s) > 0$, then $d_j \leq \deg(p) - (d_{j+1} + \ldots + d_{s-1} + d_s)$. Equivalently, $d_{j+1} + \ldots + d_{s-1} + d_s < \deg(p)$ implies $d_j + d_{j+1} + \ldots + d_{s-1} + d_s \leq \deg(p)$. Therefore, since $d_1 + \ldots + d_{s-1} + d_s = \deg(q') \geq \deg(p)$, there exists $1 \leq j \leq s$ such that $\deg(p) = d_j + d_{j+1} + \ldots + d_{s-1} + d_s$, and we may take $p' = \prod_{i=j}^{s} q_i$.

Case 2: Let $\overline{d} > 0$. Then the algorithm executes the recursive call in step 7. With each such call, the number ν of extended characteristic exponents of g decreases by one. The recursion continues until $\overline{d}$ is zero, so it stops at latest when ν is 1. Taking case 1 and Lemma 60 below into account, we may, thus, assume that the valuation of the resulting polynomial

$$q = \texttt{IntegralBasisElement}(\{\rho_1, \ldots, \rho_{\overline{m}}\}, \overline{d}).$$

at g is maximal in degree $\overline{d}$. To conclude, we consider two cases. If $u = 0$, then $d = \overline{d}$ and $p_d = q$, so we are done. Let $u > 0$. Since $p_d = p^u q$, the same argument as in case 1 shows that there is a polynomial of type $p'_d = p^u q'$, with $q' \in K[X][Y]$ monic in Y of degree $\deg(q') = \deg(q)$, and such that the valuation of p'_d at g is maximal in degree d. But then $v_g(q') \leq v_g(q)$, hence $v_g(p'_d) = v_g(p^u q') \leq v_g(p^u q) = v_g(p_d)$ by Remark 55. So we are done again. □

Lemma 60. *With $\overline{d}$ as in step 4 of Algorithm 6, let $q \in K[X][Y]$ be a monic polynomial of degree $\overline{d}$ in Y such that $v_{\overline{g}}(q)$ is the maximal valuation at $\overline{g}$ in degree $\overline{d}$. Then $v_g(q)$ is the maximal valuation at g in degree $\overline{d}$.*

Proof. Let $q' \in K[X][Y]$ be any monic polynomial of degree $\overline{d}$ in Y. Then no Puiseux expansion of $\overline{g}$ coincides with the initial part of a Puiseux expansion of q' since $\overline{d} \leq \overline{m} - 1$. Hence, taking into account that each expansion of $\overline{g}$ is the truncation of an expansion of g, it easily follows from the valuation formula in Section 4.8 that $v_{\overline{g}}(q') = v_g(q')$ (in particular, $v_{\overline{g}}(q) = v_g(q)$). We conclude that $v_g(q') = v_{\overline{g}}(q') \leq v_{\overline{g}}(q) = v_g(q)$, as desired. □

Example 61. *The polynomial g considered in Example 20 has degree $m = 8$ in Y. We apply Algorithm 6 to the set of Puiseux expansions of g, where $d = m - 1 = 7$ is chosen maximal. The singular parts of the Puiseux expansions of g are*

$$\begin{aligned}
\delta_1 &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} + 1/4iX^2,\\
\delta_2 &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} - 1/4iX^2,\\
\delta_3 &= iX^{3/2} + (1/2i + 1/2)X^{7/4} + 1/4iX^2,\\
\delta_4 &= iX^{3/2} + (1/2i + 1/2)X^{7/4} - 1/4iX^2,\\
\delta_5 &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} + 1/4iX^2,\\
\delta_6 &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} - 1/4iX^2,\\
\delta_7 &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} + 1/4iX^2,\\
\delta_8 &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} - 1/4iX^2,
\end{aligned}$$

where $i^2 = -1$. Truncating the δ_i to degree $< t = t_3 = 2$, we obtain

$$\begin{aligned}
\overline{\delta}_1 = \overline{\delta}_2 &= iX^{3/2} + (-1/2i - 1/2)X^{7/4},\\
\overline{\delta}_3 = \overline{\delta}_4 &= iX^{3/2} + (1/2i + 1/2)X^{7/4},\\
\overline{\delta}_5 = \overline{\delta}_6 &= -iX^{3/2} + (1/2i - 1/2)X^{7/4},\\
\overline{\delta}_7 = \overline{\delta}_8 &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4}.
\end{aligned}$$

Hence, in step 3 of Algorithm 6, we get $u_1 = u = 1$. Denoting the polynomial generated in step 9 of the algorithm by $p_{\overline{m}}$, we have

$$\begin{aligned}
p_4 &= (Y - \overline{\delta}_1)(Y - \overline{\delta}_3)(Y - \overline{\delta}_5)(Y - \overline{\delta}_7)\\
&= Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7.
\end{aligned}$$

Applying the whole procedure recursively gives $p_2 = Y^2 + X^3$, $u_2 = 1$ and $p_1 = Y$, $u_3 = 1$. Combining all factors, we get

$$p_7 = p_4^{u_1} p_2^{u_2} p_1^{u_3} = \left(Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + \frac{1}{4}X^7\right)(Y^2 + X^3)Y.$$

If $p_d = \texttt{IntegralBasisElement}(\Gamma, d)$ is a polynomial returned by Algorithm 6, we may find the exponent of x in the denominator of the corresponding integral basis element via the formula

$$o(\Gamma, d) = v_g(p_d) = \sum_{\eta \in N_d} v(\gamma - \eta).$$

Here, $N_d = \{\eta_1, \ldots \eta_d\}$ is the set of Puiseux expansions of p_d and $\gamma \in \Gamma$ is any of the Puiseux expansions of g (recall that the latter expansions are all conjugate).

Example 62. *Continuing Example 61, we now compute all elements of the integral basis.*

We first use Algorithm 6 to find all numerators p_d. We already know that $p_7 = p_4p_2p_1$. Computing the p_d for $1 \le d \le 6$ then amounts to the following: Start with the largest possible power of p_4 whose degree in Y is $\le d$. Then successively address powers of p_2 and p_1 in the obvious way. This yields $p_6 = p_4p_2$, $p_5 = p_4p_1$, p_4, $p_3 = p_2p_1$, p_2, and p_1.

We now compute the powers of x in the denominators via the formula for the $o(\Gamma, d)$ above. By construction, for any $\gamma \in \Gamma$, we have $\sum_{\eta \in N_{p_4}} v(\gamma - \eta) = 27/4$, $\sum_{\eta \in N_{p_2}} v(\gamma - \eta) = 13/4$, and $\sum_{\eta \in N_{p_1}} v(\gamma - \eta) = 3/2$. We conclude that $o(\Gamma, 1) = 3/2$, $o(\Gamma, 2) = 13/4$, $o(\Gamma, 3) = 13/4 + 3/2 = 19/4$, $o(\Gamma, 4) = 27/4$, $o(\Gamma, 5) = 27/4 + 3/2 = 33/4$, $o(\Gamma, 6) = 27/4 + 13/4 = 10$ and $o(\Gamma, 7) = 27/4 + 13/4 + 3/2 = 23/2$. Hence, the desired integral basis for g is

$$\left\{1 = p_0, \frac{p_1}{x}, \frac{p_2}{x^3}, \frac{p_2 p_1}{x^4}, \frac{p_4}{x^6}, \frac{p_4 p_1}{x^8}, \frac{p_4 p_2}{x^{10}}, \frac{p_4 p_2 p_1}{x^{11}}\right\}.$$

7.6. Merging the Integral Bases for the Branches

We now know how to find integral bases for the branches of f. The next step is to combine the individual bases to an integral basis for the product $\widetilde{f} = f_1 \cdots f_r$ of the branches. In principle, this could be done by applying the splitting of normalization as in Proposition 37. However, as already discussed in Section 7.1, this would involve the use of the extended Euclidean algorithm for finding the respective Bézout coefficients and is not very practical. Our next result, which extends Proposition 37, provides a different strategy, replacing the Bézout coefficients by polynomials in $K[X, Y]$ which are both simpler and easier to calculate.

Proposition 63. *Write $f = f_0 \widetilde{f} = f_0 f_1 \cdots f_r$ as before. For $i = 1, \ldots, r$, set $h_i = \prod_{j=1,\ j \neq i}^{r} f_j$, and let*

$$\mathcal{B}^{(i)} = \left\{1 = p_0^{(i)}, \frac{p_1^{(i)}}{X^{e_1^{(i)}}}, \ldots, \frac{p_{m_i-1}^{(i)}}{X^{e_{m_i-1}^{(i)}}}\right\}$$

represent an integral basis for f_i as in Proposition 35. Furthermore, for each i, let $\beta_i \in K[X, Y]$ be a polynomial such that $v_{f_i}(\beta_i h_i)$ is an integer $c_i \geq 0$, and set

$$\widetilde{\mathcal{B}}^{(i)} = \left\{\frac{\beta_i h_i}{X^{c_i}}, \frac{\beta_i h_i p_1^{(i)}}{X^{c_i + e_1^{(i)}}}, \ldots, \frac{\beta_i h_i p_{m_i-1}^{(i)}}{X^{c_i + e_{m_i-1}^{(i)}}}\right\}.$$

Then $\widetilde{\mathcal{B}}^{(1)} \cup \ldots \cup \widetilde{\mathcal{B}}^{(r)}$ represents an integral basis for $\widetilde{f} = f_1 \cdots f_r$.

Proof. For each integer i with $1 \leq i \leq r$, f_i and $\beta_i h_i$ are coprime in $K((X))[Y]$ since otherwise we would have $v_{f_i}(\beta_i h_i) = \infty$. Hence, there are polynomials $a_i, b_i \in K[[X]][Y]$ and an integer $\widetilde{e_i} \in \mathbb{N}$ which fit into a Bézout identity of type $a_i f_i + b_i \beta_i h_i = X^{\widetilde{e_i}}$. Then $\widetilde{e_i} = e_i + c_i$, where $e_i := v_{f_i}(b_i) \in \mathbb{N}$. We conclude from Theorem 29 that both $g_i := b_i / X^{e_i}$ and $\beta_i h_i / X^{c_i}$ represent elements which are integral over $K[[X]][Y]/\langle f_i \rangle$. Moreover, $g_i \frac{\beta_i h_i}{X^{c_i}} \equiv \delta_{ij} \mod f_j$, for $1 \leq j \leq r$. Hence, as in Proposition 27, the well-defined map of $K[[X]]$-modules

$$(t_1 \mod f_1, \ldots, t_r \mod f_r) \mapsto \sum_{i=1}^{r} g_i \frac{\beta_i h_i}{X^{c_i}} t_i \mod f_1 \ldots f_r$$

maps $\bigoplus_{i=1}^{r} \overline{K[[X]][Y]/\langle f_i \rangle}$ isomorphically onto $\overline{K[[X]][Y]/\langle f_1 \cdots f_r \rangle}$. So if we set

$$C^{(i)} = \left\{g_i \frac{\beta_i h_i}{X^{c_i}}, g_i \frac{\beta_i h_i p_1^{(i)}}{X^{c_i + e_1^{(i)}}}, \ldots, g_i \frac{\beta_i h_i p_{m_i-1}^{(i)}}{X^{c_i + e_{m_i-1}^{(i)}}}\right\}$$

for $1 \leq i \leq r$, then $C^{(1)} \cup \ldots \cup C^{(r)}$ represents an integral basis for $f_1 \cdots f_r$.

Algorithm 7 `CoefficientsForMerging`

Input: $\Delta_1, \ldots, \Delta_r$, the sets of singular parts of the Puiseux expansions of the branches $f_1, \ldots, f_r$ of an irreducible polynomial $f \in K[X][Y]$ which is monic in Y.

Output: A set $\{(\beta_i, c_i)\}_{1 \le i \le r}$ of pairs $(\beta_i, c_i) \in K[X, Y] \times \mathbb{N}$ with $\upsilon_{f_i}(\beta_i h_i) = c_i$, where $h_i = \prod_{j \ne i} f_j$.

1: **for** $i = 1, \ldots, r$ **do**
2: from the given singular parts, compute $\upsilon_{f_i}(h_i)$
3: **if** $\upsilon_{f_i}(h_i) \in \mathbb{N}$ **then**
4: $\beta_i = 1$, $c_i = \upsilon_{f_i}(h_i)$
5: **else**
6: for $1 \le j \le r$, $j \ne i$, and $1 \le k < \deg_Y(f_j)$, set $f_{j,k} =$ `IntegralBasisElement`(Δ_j, k), $f_{j,\deg_Y(f_j)} = \prod_{\delta \in \Delta_j}(Y - \delta)$
7: for each prime divisor a of the denominator of $\upsilon_{f_i}(h_i)$, choose a polynomial[2] from the $f_{j,k}$ whose valuation at f_i has a multiple of a as its denominator, and whose Y-degree is minimal among the $f_{j,k}$ with this property
8: set up a linear congruence equation to find for each $f_{j,k}$ selected in step 7 an exponent $\ell_{j,k}$ such that the product β_i of the powers $f_{j,k}^{\ell_{j,k}}$ satisfies $\upsilon_{f_i}(\beta_i) \in \mathbb{N}$; choose a solution of the linear congruence equation which minimizes the Y-degree of β_i
9: $c_i = \upsilon_{f_i}(\beta_i h_i)$
10: **return** $\{(\beta_i, c_i)\}_{1 \le i \le r}$

Now, for each i, it is easy to see that $C^{(i)}$ and $\mathcal{B}^{(i)}$, as well as $\mathcal{B}^{(i)}$ and $\widetilde{\mathcal{B}}^{(i)}$, represent the same $K[[x]]$-submodule of $K[[x]][y] = K[[X]][Y]/\langle f_i \rangle$: Use that $g_i \frac{\beta_i h_i}{X^{c_i}} \equiv 1 \mod f_i$ and that $g_i(x, y)$ is integral over $K[[x]][y]$. Since in addition $C^{(i)}$ and $\widetilde{\mathcal{B}}^{(i)}$ reduce to zero modulo f_j for $j \ne i$, we see that $C^{(i)}$ and $\widetilde{\mathcal{B}}^{(i)}$ represent the same $K[[x]]$-submodule of $K[[x]][y] = K[[X]][Y]/\langle f_1 \cdots f_r \rangle$, which concludes the proof. □

To find pairs (β_i, c_i) as in the proposition, it is enough to compute the singular parts of the Puiseux expansions of f. In fact, if $\upsilon_{f_i}(h_i) \in \mathbb{N}$, set $\beta_i = 1$. Otherwise, set $\overline{h}_i = \prod_{\delta \in \Delta^{(i)}}(Y - \delta)$, where $\Delta^{(i)}$ is the set of singular parts of the Puiseux expansions of h_i. Then an appropriate power of $\overline{h}_i$ will do. Indeed, $\upsilon_{f_i}(h_i^\ell) = \ell \cdot \upsilon_{f_i}(h_i)$ and $\upsilon_{f_i}(h_i) = \upsilon_{f_i}(\overline{h}_i)$. Typically, however, it is more efficient to apply Algorithm 7 below. Examples 64 and 65 show the algorithm at work.

Example 64. *Let $f = (Y^3 + X^2)(Y^2 - X^3) + Y^6 \in \mathbb{Q}[X, Y]$ be as in Examples 24 and 45, with branches $f_1 = (Y - \gamma_1)(Y - \gamma_2)(Y - \gamma_3)$ and $f_2 = (Y - \gamma_4)(Y - \gamma_5)$. We apply Algorithm 7 to compute the polynomial β_1 and the set $\widetilde{\mathcal{B}}^{(1)}$ from Proposition 63.*

In Example 45, we found the integral basis $\mathcal{B}^{(1)} = \{1, y, \frac{y^2}{x}\}$ for f_1. Considering $h_1 = f_2$, we see from the initial terms of the γ_i as written in Example 24 that $\upsilon_{f_1}(h_1) = 4/3$. In step 6 of the algorithm, we get

$$f_{2,1} = \texttt{IntegralBasisElement}(h_1, 1) = Y.$$

[2]Polynomials $f_{j,k}$ as desired exist since the polynomial $\overline{h}_i = \prod_{\delta \in \Delta^{(i)}}(Y - \delta)$ considered in the text is a factor of the product of all the $f_{j,k}$.

Since $v_{f_1}(Y) = 2/3$, we have $v_{f_1}(Yf_1) = 2 \in \mathbb{N}$. So we can take $\beta_1 = Y$ and, thus,

$$\widetilde{\mathcal{B}}^{(1)} = \left\{ \frac{Yh_1}{X^2}, \frac{Yh_1Y}{X^2}, \frac{Yh_1Y^2}{X^3} \right\}.$$

Note that this set is simpler than the set $\widetilde{\mathcal{B}}^{(1)}$ obtained in Example 45.

Here is a slightly more complicated example:

Example 65. *Let $f(X,Y) = (Y^6 - 6X^3Y^4 - 2X^7Y^3 + 12X^6Y^2 - 12X^{10}Y - 8X^9)(Y^2 - 2YX^3 - 2X^3)(Y^2 + X^7) + X^{30} \in \mathbb{Q}[X,Y]$. The Puiseux expansions of f are*

$$\begin{aligned}
\gamma_1 &= a_1X^{3/2} + X^{7/3} + \dots, & \gamma_6 &= a_2X^{3/2} + b_2X^{7/3} + \dots,\\
\gamma_2 &= a_1X^{3/2} + b_1X^{7/3} + \dots, & \gamma_7 &= a_1X^{3/2} + X^3 + \dots,\\
\gamma_3 &= a_1X^{3/2} + b_2X^{7/3} + \dots, & \gamma_8 &= a_2X^{3/2} + X^3 + \dots,\\
\gamma_4 &= a_2X^{3/2} + X^{7/3} + \dots, & \gamma_9 &= c_1X^{7/2} + \dots,\\
\gamma_5 &= a_2X^{3/2} + b_1X^{7/3} + \dots, & \gamma_{10} &= c_2X^{7/2} + \dots,
\end{aligned}$$

with roots a_1, a_2 of Z^2-2, b_1, b_2 of Z^2+Z+1, and c_1, c_2 of Z^2+1. Corresponding to the conjugacy classes $\Delta_1 = \{\gamma_1, \gamma_2\,\gamma_3, \gamma_4, \gamma_5, \gamma_6\}$, $\Delta_2 = \{\gamma_7, \gamma_8\}$, and $\Delta_3 = \{\gamma_9, \gamma_{10}\}$, there are three branches f_1, f_2, and f_3 of f. We show how to compute the polynomial β_1 from Proposition 63.

Let $h_1 = f_2f_3$. Then $v_{f_1}(h_1) = 41/6$. In step 6 of Algorithm 7, we get $f_{2,1} = Y$, $f_{2,2} = Y^2-2YX^3-2X^3$, and $f_{3,1} = Y$, $f_{3,2} = Y^2+X^7$. Furthermore, we have $v_{f_1}(y) = 3/2$, $v_{f_1}(y^2-2yx^3-2x^3) = 23/6$, and $v_{f_1}(y^2+x^7) = 3$. So we can take a polynomial of type $\beta_1 = y^{\ell_1}(y^2-2yx^3-2x^3)^{\ell_2}$, with exponents $\ell_1, \ell_2 \in \mathbb{N}$ such that $\ell_1\frac{3}{2} + \ell_2\frac{23}{6} + \frac{41}{6} \in \mathbb{Z}$. The corresponding linear congruence equation is $9\ell_1 + 23\ell_2 + 41 \equiv 0 \mod 6$. Choosing the solution which minimizes the Y-degree of β_1, we get $\ell_1 = 1$, $\ell_2 = 2$ and, thus, $\beta_1 = y(y^2 - 2yx^3 - 2x^3)^2$.

Merging the integral bases for the branches using Proposition 63 requires that we know the precision t up to which all power series in X appearing in the process must be developed. Taking Remark 44 into account, we can use $t = e_c + E(f)$, where $e_c = \max_{1\le i\le r} c_i$. Indeed, the integrality exponent of any polynomial appearing in the construction will be at most this number. We obtain Algorithm 8 below.

Remark 66. *Note that if $e = v_{\widetilde{f}}(y)$, then the fractions $y^i/x^{\lfloor ei \rfloor}$, $0 \le i < m = \deg_Y(\widetilde{f})$, are integral over $K[[x]][y] = K[[X]][Y]/\langle\widetilde{f}\rangle$. To enhance the performance of Algorithm 8, we propose to add these elements to $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$ before applying Remark 38.*

7.7. Ad-hoc Formulas for Absolutely Irreducible Weierstrass Polynomials

It turns out that in the case where $g \in K[[X]][Y]$ is an absolutely irreducible Weierstrass polynomial, we can get simple formulas for computing valuations and, thus, maximal integrality exponents. In particular, if g is absolutely irreducible and there is only one characteristic exponent, then these formulas allow us to write down an integral basis for g directly, without using Algorithm 6, `IntegralBasisElement`. We need:

Lemma 67. *Let $g \in K[[X]][Y]$ be an absolutely irreducible Weierstrass polynomial of degree m in Y. Factorize g as*

$$g = \prod(Y - \gamma_\ell(X)) := \prod(Y - \eta(\omega^\ell X^{1/m}))$$

Algorithm 8 `MergingIntegralBases`

Input: Lists of pairs $\{(\Delta_i, f_i)\}_{1\le i\le r}$, $\{(\beta_i, c_i)\}_{1\le i\le r}$, where

- $\Delta_1, \dots, \Delta_r$ are the sets of singular parts of the Puiseux expansions of the branches $f_1, \dots, f_r$ of an irreducible polynomial $f \in K[X][Y]$ which is monic in Y,
- $\{(\beta_i, c_i)\}_{1\le i\le r}$, the output of `CoefficientsForMerging`$(\Delta_1, \dots, \Delta_r)$
- the f_i are developed up to X-degree $e_c + E(f)$, where $e_c = \max_{1\le i\le r} c_i$.

Output: A list $\{(p_i, e_i)\}_{1\le i\le r}$ of pairs $(p_i, e_i) \in K[X, Y] \times \mathbb{N}$ such that $\left\{1 = p_0, \frac{p_1}{x^{e_1}} \dots, \frac{p_{m-1}}{x^{e_{m-1}}}\right\}$ is an integral basis for $\widetilde{f} = f_1 \cdots f_r$ of monic triangular type.

$m = \deg_Y(f_1 \cdots f_r)$
for $i = 1, \dots, r$ **do**
  $h_i = \prod_{j\neq i} f_j$
  for $d = 0, \dots, m_i - 1$ **do**
    $q_d =$ `IntegralBasisElement`(Δ_i, d)
    $p_d = b_i h_i q_d$
    $e_d = c_i + e_{f_i}(q_d)$
  $\mathcal{B}^{(i)} = \left\{\frac{p_0}{x^{e_0}}, \frac{p_1}{x^{e_1}}, \dots, \frac{p_{m_i-1}}{x^{e_{m_i-1}}}\right\}$
applying the recipe from Remark 38 to $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$, compute an integral basis $\left\{1 = p_0, \frac{p_1}{x^{e_1}} \dots, \frac{p_{m-1}}{x^{e_{m-1}}}\right\}$ of monic triangular type for $f_1 \cdots f_r$
return $\{(p_i, e_i)\}_{1\le i\le r}$

as in Section 4.5, where $\eta \in L[[T]]$, and ω is a primitive mth root of unity. Set $\gamma = \gamma_m$. As in Remark 53, assume that $v(\gamma) > 1$, and let $k_0, \dots, k_\nu$ be the characteristic exponents of g. Then, with notation as in Section 4.8, we have:

1. *For $j = 1, \dots, \nu$, denote by N_j the set of all $i \in \{1, \dots, m-1\}$ such that*

$$\frac{k_0}{\gcd(k_0, \dots, k_{j-1})} \mid i \quad \text{and} \quad \frac{k_0}{\gcd(k_0, \dots, k_j)} \nmid i.$$

   Then

$$v(\gamma - \gamma_i) = \frac{k_j}{m} \text{ for all } i \in N_j.$$

   In particular, if $\nu = 1$, then for $i \neq m$,

$$v(\gamma - \gamma_i) = \frac{k_1}{m}.$$

2. *For all i, we have*

$$\begin{aligned} v_\gamma\left(\frac{\partial g}{\partial Y}\right) &= \sum_{j=1}^{\nu} \left(\gcd(k_0, \dots, k_{j-1}) - \gcd(k_0, \dots, k_j)\right) \frac{k_j}{m} \\ &= \mathrm{Int}_i \end{aligned}$$

Proof. See de Jong and Pfister (2000, Lemma 5.2.18(1)) and its proof. □

Proposition 68. *With notation and assumptions as in Lemma 67, set*

$$e_d = \left\lfloor \upsilon_\gamma\left(\frac{\partial^{m-d} g}{\partial Y^{m-d}}\right)\right\rfloor, \text{ for } d = 1, \ldots, m-1.$$

Then we have:

1. *The element $\frac{\frac{\partial g}{\partial Y}}{X^{e_{m-1}}}$ is integral over $K[[X]][Y]/\langle g\rangle$, and e_{m-1} is the maximal integrality exponent with respect to g in degree $m-1$.*
2. *The element $\frac{\frac{\partial^{m-1} g}{\partial Y^{m-1}}}{X^{e_1}}$ is integral over $K[[X]][Y]/\langle g\rangle$, $e_1 = \left\lfloor \frac{k_1}{m}\right\rfloor$, and this number is the maximal integrality exponent with respect to g in degree 1.*
3. *If $\nu = 1$, then $e_d = \left\lfloor \frac{dk_1}{m}\right\rfloor$, $1 \le d \le m-1$, and*

$$\left\{1, \frac{\frac{\partial^{m-1} g}{\partial Y^{m-1}}}{X^{e_1}}, \ldots, \frac{\frac{\partial g}{\partial Y}}{X^{e_{m-1}}}\right\}$$

represents an integral basis for g.

Proof. As in Lemma 21, for each $1 \le d \le m-1$, choose a subset $\widetilde{\mathcal{A}} \subseteq \{1, \ldots, m-1\}$ of cardinality d with $\mathrm{Int}(\widetilde{\mathcal{A}})$ maximal among all $\mathrm{Int}(\mathcal{A})$, $\mathcal{A} \subseteq \{1, \ldots, m-1\}$ of cardinality d, and set

$$\widetilde{p}_d := \prod_{j \in \widetilde{\mathcal{A}}} \big(Y - \gamma_j(X)\big) \in \mathcal{P}_X[Y].$$

Then $\upsilon_g(\widetilde{p}_d) = \mathrm{Int}(\widetilde{\mathcal{A}})$, and this number is the maximal valuation $\upsilon_g(q)$, for $q \in L\{\{X\}\}[Y]$ monic of degree d in Y. Hence, items (1), (2) and the first part of (3) follow from the previous lemma, computing the derivatives of $g = \prod_{i=1}^{m}(Y - \gamma_i(X))$ by the product rule and evaluating the result at $Y = \gamma(X)$. The second part of (3) follows then from Proposition 35. □

Example 69. *The Weierstrass polynomial $g = Y^4 - 2X^3Y^2 - 4X^{11}Y + X^6 - X^{19} \in \mathbb{C}[[X]][Y]$ is (absolutely) irreducible. It factors as*

$$g = \prod (Y - \eta(\omega^\ell X^{1/4})),$$

where $\eta(T) = T^6 + T^{19} \in \mathbb{C}[[T]]$, and $\omega = e^{\pi i/2}$. We compute that $\upsilon_g\left(\frac{\partial^2 g}{\partial Y^2}\right) = 3$, but for

$$\widetilde{p}_2 = \big(Y - \eta(X^{1/4})\big)\big(Y - \eta(iX^{1/4})\big),$$

we have $\upsilon_g(\widetilde{p}_2) = \frac{25}{4}$. So here $\nu = 2$, and the assertion of Proposition 68, (3) *does not hold.*

7.8. Computing Minimal Local Contributions

Summing up, we now present our algorithm for finding minimal local contributions. For this, as we already know, we may restrict ourselves to the case of a K-rational singularity, which may be chosen to be the origin. That is, we consider the prime ideal $P = \langle x, y\rangle \in \mathrm{Sing}(A)$. If we assume in addition that the origin is the only singularity at $X = 0$, we may apply the recipe given in Proposition 41, which allows us to compute the minimal contribution from an integral basis of monic triangular type for $f_1 \cdots f_r$ (take Proposition 43 into account). We describe the resulting procedure in Algorithm 9.

Algorithm 9 `MinimalLocalContribution`

Input: $f \in K[X][Y]$ irreducible and monic in Y of degree n, with $P = \langle X, Y\rangle \in \mathrm{Sing}(A)$, where $A = K[x,y] = K[X,Y]/\langle f(X,Y)\rangle$, and such that P is the only singularity of A at $X = 0$.

Output: A set of $K[x]$-module generators for the minimal local contribution to $\overline{A}$ at P.

1: Δ_0 = set of singular parts of the Puiseux expansions of f not vanishing at the origin, $\Delta_1, \ldots, \Delta_r$ = sets of singular parts of the Puiseux expansions of f vanishing at the origin, grouped into conjugacy classes.
2: compute the maximal integrality exponent $E(f)$ as indicated in Section 4.8
3: $\{(\beta_i, c_i)\}_{1\le i\le r}$ = `CoefficientsForMerging`$(\Delta_1, \ldots, \Delta_r)$
4: $e_c = \max_{1\le i\le r} c_i$
5: $\{f_0, f_1, \ldots, f_r\}$ = `Splitting`$(E(f) + e_c, f)$, where f_0 corresponds to Δ_0 and $f_1, \ldots, f_r$ correspond to $\Delta_1, \ldots, \Delta_r$
6: $m_0 = \deg(f_0)$, $m = n - m_0$
7: $\{(p_i', e_i')\}_{1\le i\le r}$ = `MergingIntegralBases`$(\{(\Delta_i, f_i)\}_{1\le i\le r}, \{(\beta_i, c_i)\}_{1\le i\le r})$
8: **for** $i = 0, \ldots, m_0 - 1$ **do**
9: $\quad p_i = y^i$, $e_i = 0$
10: **for** $i = 0, \ldots, m - 1$ **do**
11: $\quad p_{m_0+i} = f_0 \cdot p_i'$, $e_{m_0+i} = e_i'$
12: **return** $\left\{1 = p_0, \frac{p_1}{x^{e_1}} \ldots, \frac{p_{m-1}}{x^{e_{m-1}}}\right\}$

Remark 70. *In the presence of conjugate singularities, we get a better performance by handling groups of conjugate singularities simultaneously (see also van Hoeij (1994, Section 2.3)). Let $P \in \mathrm{Sing}(A)$ correspond to such a group of singularities, where we assume that no two of the singularities have the same X-coordinate. Then we can find polynomials $q_1, q_2 \in K[X]$ such that $P = \langle q_1(X), Y - q_2(X)\rangle$. We take α to be a root of $q_1(X)$ and translate the singularity $(\alpha, q_2(\alpha))$ to the origin. We compute the local contribution to the integral basis at the origin and apply the inverse translation to the output. The least common denominator of the resulting generators will be a power of $x - \alpha$. We rewrite all generators using this denominator. Then we regard α as a variable and eliminate it from all numerators by successively reducing each numerator with respect to the numerators of smaller degree, using an elimination ordering for which $\alpha > y > x$ (this works since we can always find an integral basis which is defined over the original base field). Finally, we replace $(x - \alpha)$ by $q_1(x)$ in all denominators.*

Example 71. *Let $f(X,Y) = Y^3 - (X^2-2)^2 \in \mathbb{Q}[X,Y]$. Then $\mathrm{Sing}(A)$ consists of the single prime ideal $P = \langle X^2-2, Y\rangle$, that is, the conjugate points $(\sqrt{2}, 0)$ and $(-\sqrt{2}, 0)$ are the only singularities. Taking $\alpha = \sqrt{2}$, the recipe above yields the set $\left\{1, y, \frac{y^2}{x-\alpha}\right\}$ of $K[x]$-module generators for the minimal local contribution at $(\alpha, 0)$. Hence, $\left\{1, y, \frac{y^2}{x^2-2}\right\}$ is an integral basis for $\overline{A}$ over $K[x]$. So in this simple case, we did not need to eliminate α from the numerators.*

Example 72. *Let $f(X,Y) = (Y-X)^3 - (X^2-2)^2 \in \mathbb{Q}[X,Y]$. Now the singular locus consists of the single prime ideal $P = \langle X^2 - 2, Y - X\rangle$, that is, the conjugate points $(-\sqrt{2}, -\sqrt{2})$ and $(\sqrt{2}, \sqrt{2})$ are the only singularities. Taking $\alpha = \sqrt{2}$ and computing the minimal local contribution at (α, α), we get*

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

Reducing $y^2 - 2\alpha y + 2$ with respect to $x - \alpha$ and $y(x - \alpha)$ as described above, we get $y^2 - 2xy + 2$ and, thus, the new set of $K[x]$-module generators $\left\{1, y, \frac{y^2-2xy+2}{x-\alpha}\right\}$. So in this example, the final result of our algorithm is $\left\{1, y, \frac{y^2-2xy+2}{x^2-2}\right\}$.

Remark 73. *If there are two singularities with the same X-coordinate, we may apply a linear change of coordinates of type $X \to X + aY$, $a \in K$, to remedy the situation. After the integral basis has been computed, we apply the inverse transformation $X \to X - aY$ to the elements obtained. This will give us a representation for the normalization of type $\overline{A} = \frac{1}{d_1}U_1$, where the denominator d_1 may not depend on x alone. By choosing an element $d_2 \in K[x]$ of the conductor of A (consider the Jacobian ideal of A), and computing the ideal quotient $U_2 = (d_2U_1) : d_1$, we arrive at a representation $\overline{A} = \frac{1}{d_2}U_2$ whose denominator does not depend on y. From this, we obtain an integral basis for A over $K[x]$ following the recipe given in Remark 5.*

Example 74. *Let $f(X, Y) = (Y^2-2)^2 + X^5 = Y^4 - 4Y^2 + X^5 + 4 \in \mathbb{Q}[X, Y]$. Then* Sing$(A)$ *consists of the single prime ideal $P = \langle Y^2 - 2, X\rangle$. That is, the conjugate points $(0, \sqrt{2})$ and $(0, -\sqrt{2})$, which have the same X-coordinate, are the only singularities.*

Implementing the recipe from Remark 73, we apply the coordinate change $X \to X + Y$ which yields the polynomial $g(X, Y) = f(X+Y, Y) = Y^5+5Y^4X+Y^4+10Y^3X^2+10Y^2X^3-4Y^2+5YX^4+X^5+4$ of Y-degree 5. The singular locus of the coordinate ring of the plane curve defined by g consists of the single prime ideal $Q = \langle y^2 - 2, x + y\rangle$. We extend the base field from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{2})$, and consider the prime ideals $Q_1 = \langle y + \sqrt{2}, x + y\rangle$ and $Q_2 = \langle y - \sqrt{2}, x + y\rangle$. Then we apply the translation $X \to X + \sqrt{2}$, $Y \to Y - \sqrt{2}$ to move the point $(-\sqrt{2}, \sqrt{2})$ corresponding to Q_1 to the origin. This yields the polynomial $h(X, Y) = g(X + \sqrt{2}, Y - \sqrt{2}) = X^5 + 5X^4Y + 10X^3Y^2 + 10X^2Y^3 + 5XY^4 + Y^5 + Y^4 - 4\sqrt{2}Y^3 + 8Y^2$. The decomposition of h given by the Weierstrass preparation theorem is $h = h_0h_1 \in \mathbb{Q}(\sqrt{2})[[X]][Y]$, where the unit $h_0 \in \mathbb{Q}(\sqrt{2})[[X, Y]]$ is a factor of Y-degree 3, and where h_1, which has Y-degree 2, is the single branch of h. The two Puiseux expansions of h_1 are $\gamma_{1,2} = \pm\frac{\sqrt{2}}{4}iX^{5/2} + \dots$. Hence, by Proposition 35, $\left\{1, \frac{y}{x^2}\right\}$is an integral basis for h_1. Incorporating the truncation $\overline{h}_0 = Y^3 + Y^2 + 5XY^2 + (-4\sqrt{2})Y + 8$ of h_0 to X-degree 1 as in Proposition 41, we get the local contribution

$$\left\{1, y, y^2, y^3, \frac{\overline{h}_0(x, y) \cdot y}{x^2}\right\}$$

to $\overline{\mathbb{Q}(\sqrt{2})[X, Y]/\langle h\rangle}$ at the origin. Translating the singularity back to its original location via $X \to X - \sqrt{2}$, $Y \to Y + \sqrt{2}$ gives us the local contribution

$$\left\{1, y - \sqrt{2}, (y - \sqrt{2})^2, (y - \sqrt{2})^3, \frac{\overline{h}_0(x - \sqrt{2}, y + \sqrt{2}) \cdot (y + \sqrt{2})}{(x - \sqrt{2})^2}\right\}$$

to $\overline{\mathbb{Q}(\sqrt{2})[X, Y]/\langle g\rangle}$ at Q_1, where the first four elements generate the same $\mathbb{Q}(\sqrt{2})[x]$-module as $\{1, y, y^2, y^3\}$. To get the local contribution to $\overline{\mathbb{Q}[X, Y]/\langle g\rangle}$ at Q, we reduce the numerator of the last element $\overline{h}_0(x - \sqrt{2}, y + \sqrt{2}) \cdot (y + \sqrt{2})$ modulo $(x - \sqrt{2})^2$ to eliminate $\sqrt{2}$ from the numerator, and then replace the denominator $(x - \sqrt{2})^2$ by $(x^2 - 2)^2$. We obtain the set

$$\overline{\mathcal{B}}_t = \left\{1, y, y^2, y^3, \frac{q_4}{(x^2 - 2)^2}\right\},$$

where

$$q_4 = y^4 + \left(\frac{1}{4}x^3 + \frac{7}{2}x + 1\right)y^3 + \left(\frac{1}{4}x^3 + \frac{15}{2}x^2 - \frac{3}{2}x - 3\right)y^2 + \left(\frac{11}{2}x^3 - 3x - 2\right)y - \frac{1}{2}x^3 + 5x^2 + 3x - 6.$$

Applying the inverse transformation $X \to X - Y$ to $\overline{\mathcal{B}}_t$ yields the local contribution to $\overline{A}$ at P. In fact, since P is the only prime ideal in Sing(A)*, we get a representation for all of $\overline{A}$. This is of type $\overline{A} = U/d_1$, with denominator $d_1 = ((x-y)^2 - 2)^2$. To change the denominator to a polynomial which depends on x alone, we follow the recipe given in Remark 73. Inspecting the Jacobian ideal $\langle x^4, 4y^3 - 8y\rangle$ of A, we see that $d_2 = x^4$ is an element of the conductor of A. Computing the ideal quotient $U_2 = (d_2U_1) : d_1$, we arrive at the representation $\overline{A} = \frac{1}{x^2}\langle y^4 - 4y^2 + 4, x^2y^2 - 2x^2, x^2\rangle$. From this, proceeding as in Remark 5, we get the integral basis*

$$\overline{\mathcal{B}} = \left\{1, y, \frac{y^2-2}{x^2}, \frac{y^3-2y}{x^2}\right\}$$

for $\overline{A}$ over $\mathbb{Q}[x]$.

Remark 75. *As indicated by the last example, applying a coordinate change to separate the X-coordinates of the singularities requires extra computations which may be expensive, in particular in the case where the X-degree of f is considerably larger than its Y-degree. We sketch an alternative approach which avoids such a coordinate change.*

If we face more than one singularity on the line $X = \alpha$, we consider the translation $X \to X + \alpha$ in order to move the singularities to the line $X = 0$. We get the polynomial $f_\alpha(X, Y) = f(X + \alpha, Y)$ and the curve C_α defined by f_α. We then decompose f_α as $f_\alpha = g_0g_1 \cdots g_s$, where $g_1, \ldots, g_s$ are the irreducible factors of f_α in $K[[X]][Y]$ whose zeros on the line $X = 0$ are singular points of C_α, and where g_0 is the product of the remaining factors. Different from our convention so far, we now refer to $g_1, \ldots, g_s$ as the branches *of f_α. Adapted versions of Propositions 41 and 63 allow us to compute an integral basis for $K[[x]][y] = K[[X]][Y]/\langle f_\alpha\rangle$ over $K[[x]]$ in a way similar to that of the previous discussion. In the case where α is K-rational, we may then apply the inverse translation $X \to X - \alpha$ to get an integral basis for $K[[x - \alpha]][y] = K[[X - \alpha]][Y]/\langle f_\alpha\rangle$ over $K[[x - \alpha]]$. In the case of conjugate singularities, we may handle these singularities simultaneously following a recipe similar to that of Remark 70.*

Example 76. *The polynomial $f(X, Y) = (Y^2 - 2)^2 + X^5 = Y^4 - 4Y^2 + 4 + X^5 \in \mathbb{Q}[X, Y]$ from Example 74 has the conjugate points $(0, \sqrt{2})$ and $(0, -\sqrt{2})$ as its only singularities.*

We show how to handle the singularities simultaneously, without applying a coordinate change first. The four Puiseux expansions of f are $\gamma_{1,2,3,4} = a \pm \frac{1}{4}aX^{5/2} + \frac{1}{32}aX^5 + \ldots$, where a is a root of $Z^2 - 2$. Since the expansions are conjugate over $\mathbb{Q}((X))$, we see that f is irreducible in $\mathbb{Q}[[X]][Y]$. That is, f consists of precisely one branch.

We construct the integral basis for the branch by truncating the Pusieux expansions as in Algorithm 6. We get the numerators $p_0 = 1$, $p_1 = y$, $p_2 = (y - \sqrt{2})(y + \sqrt{2}) = y^2 - 2$, with $v_f(p_2) = 2$, and $p_3 = (y^2 - 2)y$, with $v_f(p_3) = 2$. Since there is only one branch, we conclude as in Example 74 that the resulting integral basis

$$\overline{\mathcal{B}} = \left\{1, y, \frac{y^2-2}{x^2}, \frac{y^3-2y}{x^2}\right\}$$

for the branch is already an integral basis for $\overline{A}$ over $\mathbb{Q}[x]$.

8. Timings

We present timings to compare the computation of integral bases via

- the SINGULAR implementation of our integral basis algorithm[3],
- the SINGULAR implementation of the local normalization algorithm[4] from Section 3,
- the MAPLE (Monagan et al., 2014) implementation of van Hoeij's algorithm[5], and
- the MAGMA (Bosma et al., 1997; Ford and Letard, 1994) implementation of the Round 2 algorithm[6].

We apply the algorithms to rings of type $A = \mathbb{Q}[X, Y]/\langle f \rangle$, with polynomials f as specified. All timings are in seconds, taken on an Intel Xeon CPU E5-2643 with 24 cores, 3.4GHz, and 384GB of RAM running a Linux operating system. An asterisk ($*$) indicates that the computation did not finish within 3600 seconds. At current state, parallel computations are used only for the decomposition of the singular locus. A systematic parallelization of the integral basis algorithm and a modular approach following the strategy of Böhm et al. (2015) is subject to ongoing work. Recall that for obtaining the integral bases, singularities at infinity of the curve $\{f = 0\}$ do not matter.

8.1. One Singularity of Type A_k

A plane curve with defining polynomial

$$f(X, Y) = Y^2 + X^{k+1} + Y^d,\ k \geq 1,\ d \geq 3,$$

has exactly one singularity at the origin. This singularity is of type A_k.

k	d	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	0	0	0	0
5	100	0	0	1	168
5	500	0	1	46	$*$
50	60	0	0	1	294
50	100	0	1	2	10751
50	500	0	0	65	$*$
90	100	0	1	3	$*$
90	500	0	1	76	$*$
400	500	0	3	237	$*$

[3] Column SINGULAR INTBAS in the tables;
[4] column SINGULAR NORMAL in the tables;
[5] column MAPLE in the tables;
[6] column MAGMA in the tables.

8.2. One Singularity of Type $\boldsymbol{D_{k+1}}$

A plane curve with defining polynomial

$$f(X, Y) = X(X^{k-1} + Y^2) + Y^d,\ k \geq 3,\ d \geq 3,$$

has exactly one singularity at the origin. This singularity is of type D_{k+1}.

k	d	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	1	0	0	0
5	100	1	1	0	1683
5	500	3	0	29	*
50	60	1	1	3	312
50	100	1	1	8	3480
50	500	3	1	490	*
90	100	1	1	27	*
90	500	3	1	1441	*
400	500	4	4	*	*

8.3. Ordinary Multiple Points

We consider random curves of degree d with an ordinary k-fold point at the origin and no other singularities. The defining polynomials were generated by the function `polyDK` from the SINGULAR library `integralbasis.lib` (with random seed 1231).

k	d	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	0	2	0	0
15	20	0	7784	1	4
15	30	1	*	21	124
20	25	1	*	2	18
20	30	2	*	17	42

8.4. Curves With Many Singularities of Type $\boldsymbol{A_{k-1}}$

If k is odd, the projective plane curves with defining polynomials

$$X^{2k} + Y^{2k} + Z^{2k} + 2(X^kZ^k - X^kY^k + Y^kZ^k)$$

have precisely $3k$ singularities in $\mathbb{P}^2(\mathbb{C})$, all of type A_{k-1} (see Cogolludo (1999)). We consider the affine parts of these curves obtained by substituting $Z = X - 2Y + 1$ (these parts contain all singularities).

k	SINGULAR		MAPLE	MAGMA
	INTBAS	NORMAL		
5	0	1249	1	1
7	1	*	8	8
9	20	*	35	59
11	102	*	297	251

8.5. 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 $\delta = 42$, one node, and one set of 6 conjugate nodes.

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 $\delta = 133$.

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. $f = (Y^{15} + 2X^{38})(Y^{19} + 7X^{52}) + Y^{100}$: same type of singularity as (4), but of higher degree.

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 van Hoeij (1994, Section 6.1)).

7. $f = Y^{200} + XY^{13} + X^4Y^5 + X^5 + 2X^4 + X^3$: same type of singularities as (6), but higher degree.

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 $\delta = 6528$.

No.	Y-degree	Singular		Maple	Magma
		intbas	normal		
(1)	8	1	*	0	0
(2)	12	8	*	1	1
(3)	30	16	*	4	31
(4)	36	1	*	4	59
(5)	100	1	*	28	*
(6)	40	0	2	0	9
(7)	200	2	3	10	*
(8)	110	*	*	*	*

In Example (8), Singular and Maple do not finish due to the computation of the decomposition of the singular locus of the curve (note that the criterion given in Proposition 18 does not apply since the curve has a singularity at infinity). See Section 8.7 for the timings of the computation of the local contribution to the integral basis (normalization) at the origin.

8.6. Summary

We note that in most cases, our new algorithm outperforms the other algorithms by far.

8.7. A More Detailed Analysis of Some of the Examples

The computation of an integral basis with our algorithm has two major components. First, we decompose the singular locus into associated primes; second, we compute the local contribution to the integral basis at each prime and combine the results. In MAPLE, a similar strategy is followed in that all the X-coordinates of the singular points are computed first. With both approaches, the first step may be time consuming. To analyze the difference between the two approaches in more detail, we provide timings for the computation of the integral basis at the origin in examples where it is known to us that the origin is the only singularity. This fact can be specified in SINGULAR and MAPLE by appropriate input options.

Example	k	d	SINGULAR INTBAS	MAPLE
8.1	5	500	0	44
8.1	50	500	0	58
8.1	400	500	0	235
8.2	5	500	2	24
8.2	50	500	2	251
8.2	400	500	2	*
8.3	15	30	0	19
8.3	20	25	0	2
8.3	20	30	0	14
8.5(2)			8	1
8.5(3)			2	2
8.5(5)			1	13
8.5(8)			15	1343

We compare the timings above with those in the previous tables and observe first that for the examples in 8.1, the time required for decomposing the singular locus can be neglected. For the examples in 8.2, MAPLE spends plenty of time for the decomposition, but the part consuming most of the time is nevertheless the computation of the integral basis at the origin. For the examples in 8.3, our algorithm uses most of the time for decomposing the singular locus. The computation of the integral basis at the origin is significantly faster than that in MAPLE. From among the examples in 8.5, Example 8.5(2) sticks out: while the time for the initial decomposition is not significant, the computation of the integral basis at the origin when running our algorithm in SINGULAR is slower than that using van Hoeij's algorithm in 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 not optimal.

References

Abhyankar, S. S., 1990. Algebraic geometry for scientists and engineers. Providence, RI: American Mathematical Society.

Arnold, E. A., 2003. Modular algorithms for computing Gröbner bases. J. Symbolic Comput. 35 (4), 403–419.
URL http://dx.doi.org/10.1016/S0747-7171(02)00140-2

Böhm, J., Decker, W., Fieker, C., Pfister, G., 2015. The use of bad primes in rational reconstruction. Math. Comp. 84 (296), 3013–3027.
URL http://dx.doi.org/10.1090/mcom/2951

Böhm, J., Decker, W., Laplagne, S., Pfister, G., 2017. Local to global algorithms for the Gorenstein adjoint ideal of a curve. In: Algorithmic and experimental methods in algebra, geometry, and number theory. Springer, Cham, pp. 51–96.

Böhm, J., Decker, W., Laplagne, S., Pfister, G., Steenpaß, A., Steidel, S., 2013. Parallel algorithms for normalization. J. Symbolic Comput. 51, 99–114.
URL http://dx.doi.org/10.1016/j.jsc.2012.07.002

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I: The user language. J. Symb. Comput. 24 (3-4), 235–265.

Cogolludo, J. I., 1999. Fundamental group for some cuspidal curves. Bull. London Math. Soc. 31 (2), 136–142.
URL http://dx.doi.org/10.1112/S0024609398005323

de Jong, T., 1998. An algorithm for computing the integral closure. J. Symbolic Comput. 26 (3), 273–277.
URL http://dx.doi.org/10.1006/jsco.1998.0211

de Jong, T., Pfister, G., 2000. Local analytic geometry. Basic theory and applications. Braunschweig: Vieweg.

Decker, W., de Jong, T., Greuel, G.-M., Pfister, G., 1999. The normalization: a new algorithm, implementation and comparisons. In: Computational methods for representations of groups and algebras (Essen, 1997). Vol. 173 of Progr. Math. Birkhäuser, Basel, pp. 177–185.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2015. Singular 4-0-2 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de.

Durvye, C., 2008. Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation. Ph.D. thesis, Université de Versailles - Saint-Quentin.

Eisenbud, D., 1995. Commutative algebra. With a view toward algebraic geometry. Berlin: Springer.

Ford, D., Letard, P., 1994. Implementing the round four maximal order algorithm. J. Théor. Nombres Bordeaux 6 (1), 39–80.
URL http://jtnb.cedram.org/item?id=JTNB_1994__6_1_39_0

Grauert, H., Remmert, R., 1971. Analytische Stellenalgebren. Unter Mitarbeit von O. Riemenschneider. Berlin: Springer.

Greuel, G.-M., Laplagne, S., Seelisch, F., 2010. Normalization of rings. J. Symbolic Comput. 45 (9), 887–901.
URL http://dx.doi.org/10.1016/j.jsc.2010.04.002

Greuel, G.-M., Pfister, G., 2007. A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann. 2nd extended ed. Berlin: Springer.

Grothendieck, A., 1966. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. Inst. Hautes Études Sci. Publ. Math. (28), 255.

Monagan, M. B., Geddes, K. O., Heal, K. M., Labahn, G., Vorkoetter, S. M., McCarron, J., DeMarco, P., 2014. Maple 18 Programming Guide. Maplesoft, Waterloo ON, Canada.

Stichtenoth, H., 2009. Algebraic function fields and codes. 2nd ed., 2nd Edition. Berlin: Springer.

Swanson, I., Huneke, C., 2006. Integral closure of ideals, rings, and modules. Cambridge: Cambridge University Press.

van Hoeij, M., 1994. An algorithm for computing an integral basis in an algebraic function field. J. Symbolic Comput. 18 (4), 353–363.
URL http://dx.doi.org/10.1006/jsco.1994.1051

Walker, R. J., 1978. Algebraic curves. Springer-Verlag, New York-Heidelberg, reprint of the 1950 edition.