A Reduction for Regular Differential Systems

Manuel Bronstein
INRIA – Projet CAFÉ
2004 Route des Lucioles
06902 Sophia Antipolis Cedex
Manuel.Bronstein@inria.fr

Barry M. Trager
IBM Watson Research Center
PO Box 218
Yorktown Heights, NY 10598
bmt@us.ibm.com

June 8, 2003

Abstract

We propose a definition of regularity of a linear differential system with coefficients in a monomial extension of a differential field, as well as a global and truly rational (*i.e.* factorisation–free) iteration that transforms a system with regular finite singularities into an equivalent one with simple finite poles. We then apply our iteration to systems satisfied by bases of algebraic function fields, obtaining algorithms for computing the number of irreducible components and the genus of algebraic curves.

Introduction

This paper is concerned with differential systems of the form

$$\begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix} = A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \tag{1}$$

where the entries of the matrix A are in a differential field F. While the cyclic vector method [2, 5, 14] reduces (in theory) the study of such systems to the study of scalar differential equations, that method is well-known to be impractical except for very small n (see for example the timings in [2]), which motivates the study of *direct algorithms* that do not require uncoupling the system (1). Direct algorithms are based on computing $T \in GL_n(F)$ such that the change of variable $Y = TZ$ transforms (1) into an equivalent differential system $Z' = BZ$ where the matrix B has some desired property, which can be related either to its shape (e.g. triangular) or the nature of its poles. For example, when F is the rational function field $C(x)$ with the derivation d/dx, the Moser form algorithm [12] yields a matrix B whose denominator $b(x)$ divides the denominator of A, and such that the multiplicity of x as a factor of $b(x)$ is minimal among all $T \in GL_n(C(x))$. Knowledge of that minimal multiplicity determines

whether the eventual singularity of (1) at $x = 0$ is regular or irregular, and yields its indicial equation when the singularity is regular [8]. That algorithm can be performed successively at all the poles of A, yielding a matrix B with a minimal denominator [1]. When all the singularities of (1) are regular, that algorithm is sufficient to be able to compute all the solutions in $C(x)^n$ of the system (see [2]), otherwise a stronger normal form (the super-irreducible form) is required [9]. Other direct algorithms [6, 11] are based on computing special lattices in the associated differential module. All those algorithms are local, in that they work at a given singularity $x = \alpha$ of the differential system, so their calculations are performed in the algebraic extension $C(\alpha)$ of the constant field (or in the quotient field $C[x]/(p)$ where p is the minimal polynomial of α, which is equivalent). Those calculations must then be repeated at each irreducible factor of the denominator of A in order to produce a global normal form.

We present in this paper a global and rational algorithm that reduces all the finite singularities of (1) without having to factor the denominator of A, and without having to consider individual singularities separately. In exchange for being simpler than the previously known methods, our algorithm is only applicable to systems for which a minimal denominator over all gauge transformations is known a priori, which is in particular the case when all the finite singularities of the system are regular. In that case, our algorithm produces a matrix B that has only simple finite poles. The indicial equations and exponents of the system $Z' = BZ$ in the affine plane are then easy to compute by classical methods. Our algorithm is applicable in particular when all the solutions of (1) are algebraic over F, so we apply it to differential systems associated with algebraic curves, obtaining alternatives to the algorithms of [7] for computing the irreducible components of the curve and their genus, without requiring generic coordinates or scalar differential equations. Another application when F is a rational function field, is that our algorithm is a global alternative to the Moser form for computing the rational solutions of systems whose singularities (including at infinity) are all regular. Finally, our algorithm is applicable whenever F is a monomial extension of a differential field, which allows quite general functions as coefficients of (1).

All rings and fields in this paper are commutative and have characteristic 0.

1 Monomial extensions

We recall in this section the required terminology and results from [3] that will be used in this paper. Let (K, D) be a differential field and (E, D) a differential ring extension (*i.e.* a differential ring containing K and with a compatible derivation). We say that $t \in E$ is a *monomial (w.r.t. D)* if t is transcendental over K and $K[t]$ is closed under D. It follows immediately that $K(t)$ is also closed under D. From now on, let $t \in E$ be a monomial over K. A polynomial $q \in K[t]$ is *special (w.r.t. D)* if $q \mid Dq$, *normal (w.r.t. D)* if $\gcd(q, Dq) = 1$. Note that normal polynomials are squarefree. Conversely, for a squarefree $q \in K[t]$, let $q_s = \gcd(q, Dq)$ and $q_n = q/q_s$. Then, q_s is special and q_n is normal. Further-

more, factors and products of specials are special, and factors and least common multiples of normals are normal. An irreducible $p \in K[t]$ must be either normal or special.

Definition 1 *For any $q \in K[t]$, the* normal part of q*, denoted q^*, is the product of all the irreducible normal factors of q.*

To simplify further statements we define

$$\delta_D(p) = \begin{cases} 1 & \text{if } p \text{ is normal} \\ 0 & \text{if } p \text{ is special} \end{cases}$$

With the above notation,

$$q^* = \prod_{\substack{p \mid q \\ p \text{ irreducible}}} p^{\delta_D(p)}$$

It follows immediately that q^* is always normal and that $q/q^* \in K$ if and only if q is normal. Normal parts can be computed using only gcd computations as follows: let $q = q_1 q_2^2 \dots q_m^m$ be a squarefree factorization of q, $q_{i,s} = \gcd(q_i, q_i')$ and $q_{i,n} = q_i/q_{i,s}$. Then, $q^* = q_{1,n} \cdots q_{m,n}$.

2 The reduction algorithm

2.1 Extending a module

Let R be a principal ideal domain where gcd's can be effectively computed as well as the cofactors (for example any Euclidean domain). Let F be the field of fractions of R, V a finite dimensional vector space over F and M be the R-module generated by $v_1, \dots, v_m \in V$. Pick an F-basis $b = b_1, \dots, b_n$ of V and let d be a common denominator of the coordinates of $v_1, \dots, v_m$ with respect to b. Then, $dv_i = \sum_{j=1}^n r_{ij} b_j$ for each i where the r_{ij} are in R, and the rows of the matrix $A = (r_{ij})$ generate the module dM over R. Let $H = (h_{ij})$ be the Hermite normal form of A (see [13]) and I be the set of indices i such that the i^{th} row of H is nonzero. Then, $M = \sum_{i \in I} R w_i$ where $w_i = d^{-1} \sum_{j=1}^n h_{ij} b_j \in V$ and the w_i are linearly independent over F.

Consider now the special case where $M = R^n + Rw = \sum_{i=1}^n R b_i + Rw$ where $w = \sum_{i=1}^n f_i b_i \in V$. Let d be a common denominator of $f_1, \dots, f_n$ and $a_i = df_i \in R$. Then, the matrix A has the special form

$$A = \begin{pmatrix} d & & & \\ & d & & \\ & & \ddots & \\ & & & d \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

so an R-basis $u_1, \ldots, u_n$ of M is produced by performing the following iteration for $i = 1$ through n:

$$\begin{gathered} g_i \leftarrow \gcd(d, a_i) = \alpha d + \beta a_i, \text{ for } \alpha, \beta \in R \\ u_i \leftarrow \frac{1}{d}\left(g_i b_i + \beta \sum_{j=i+1}^{n} a_j b_j \right) \\ (a_1, \ldots, a_n) \leftarrow (0, \ldots, 0, \frac{d}{g_i} a_{i+1}, \ldots, \frac{d}{g_i} a_n) \end{gathered} \tag{2}$$

Let $T \in GL_n(F)$ be the square matrix whose rows contains the coordinates of the u_i with respect to b. It follows from (2) that T is upper triangular with g_i/d on its diagonal. Furthermore, since $\sum_{i=1}^{n} Ru_i = \sum_{i=1}^{n} Rb_i + Rw$, there are $r_{ij} \in R$ such that $b_i = \sum_{j=1}^{n} r_{ij} u_j$ for each i. This implies that

$$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} T = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

hence that T^{-1} has all its entries in R.

2.2 The single reduction step

Let now t be a monomial over the differential field (K, D) and $A = (a_{ij})$ be a square matrix with entries in $K(t)$. For each i, let $d_i \in K[t]$ be a common denominator of the i^{th} row of A and M_i be the $K[t]$-submodule of $K(t)^n$ given by

$$M_i = K[t]^n + K[t] \begin{pmatrix} d_i^* a_{i1} \\ \vdots \\ d_i^* a_{in} \end{pmatrix} \tag{3}$$

Clearly, $M_i = K[t]^n$ if and only if $d_i^*/d_i \in K$, which is equivalent to d_i normal. Suppose that d_j is not normal for some j. Using the algorithm of Section 2.1, we compute a basis $(u_1, \ldots, u_n)$ for M_j over $K[t]$ and the upper triangular matrix $T \in GL_n(K(t))$ whose rows are the coordinates of $u_1, \ldots, u_n$. The change of variable $Z = TY$ then transforms the differential system $DY = AY$ into the equivalent one $DZ = (TAT^{-1} + (DT)T^{-1})Z$.

2.3 The algorithm

Our reduction algorithm is simply to repeat the above change of variable as long as the denominator of some row of the matrix is not normal. Clearly, if this process terminates, then it yields a differential system $DZ = BZ$ where the denominator of B is normal. Our main result is that our algorithm terminates on a specific class of systems, namely systems whose finite singularities are all regular. In order to prove this, we need to properly define the concept of regularity for monomial extensions, as well as to introduce some machinery, which we do in the next section.

3 Regular modules and systems

We start by recalling some results from [14] about differential systems, differential modules and gauge transformations. Let (K, D) be a differential field, t be a monomial over K, and $\mathcal{D} = K(t)[D]$ be the ring of linear ordinary differential operators with coefficients in $K(t)$. A *differential module* (M, ∂) is a finite dimensional $K(t)$-vector space M together with an additive map $\partial : M \to M$ satisfying

$$\partial(\alpha m) = (D\alpha)m + \alpha\partial m$$

for all $\alpha \in K(t)$ and $m \in M$. It is clear from those properties that ∂ is uniquely defined by its action on a $K(t)$-basis of M. The action $D * m = \partial m$ turns any differential module into a $\mathcal{D}$-module. Given a subring R of $K(t)$ whose field of fractions is $K(t)$, an *R-lattice* N of a differential module (M, ∂) is an R-submodule of M of the form $N = \sum_{i=1}^{n} Rf_i$ where $f_1, \ldots, f_n$ is some $K(t)$-basis of M.

Let $A = (a_{ij})$ be an $n \times n$ square matrix with entries in $K(t)$. The differential module associated with the differential system $DY = AY$ is $M = K(t)^n$ with basis $e_1, \ldots, e_n$, and $\partial : M \to M$ defined by $\partial e_i = -\sum_{j=1}^{n} a_{ji} e_j$ for each i.

For any invertible matrix $T \in GL_n(K(t))$, the associated *gauge transformation* is the change of variable $Y = TZ$ in the differential system $DY = AY$. The resulting differential system for Z is

$$DZ = \big(T^{-1}AT - T^{-1}DT\big)Z = T_D[A]Z$$

where $T_D[A]$ denotes the matrix $T^{-1}AT - T^{-1}DT$. Let (M, ∂) be the differential module associated with $DY = AY$ and $f_1, \ldots, f_n$ be the basis of M given by

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = T^t \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \tag{4}$$

where T^t denotes the transpose of T. Writing $T = (t_{ij})$ we have

$$\begin{aligned} \partial f_i &= \sum_{j=1}^{n} Dt_{ji} e_j + \sum_{j=1}^{n} t_{ji} \partial e_j = \sum_{j=1}^{n} Dt_{ji} e_j - \sum_{j=1}^{n} t_{ji} \sum_{k=1}^{n} a_{kj} e_k \\ &= \sum_{j=1}^{n} \left(Dt_{ji} - \sum_{k=1}^{n} a_{jk} t_{ki} \right) e_j = \mathrm{row}(i, (DT - AT)^t) \cdot (e_1, \ldots, e_n)^t \\ &= \mathrm{row}(i, (DT - AT)^t) \cdot (T^t)^{-1} (f_1, \ldots, f_n)^t \\ &= \mathrm{row}(i, -(T_D[A])^t) \cdot (f_1, \ldots, f_n)^t = -\sum_{j=1}^{n} b_{ji} f_j \end{aligned} \tag{5}$$

where $T_D[A] = (b_{ij})$. Therefore, the systems $DY = AY$ and $DZ = T_D[A]Z$ are associated with the same differential module, and the change of variable $Y = TZ$ corresponds to the change of basis (4).

We can now give our definition of affine regularity.

Definition 2 *We say that a $K[t]$-lattice N of a differential module is* normal *if $p\partial N \subseteq N$ for some normal $p \in K[t] \setminus \{0\}$. The differential module (M, ∂) is* affine regular *if it contains a normal $K[t]$-lattice. Finally, a differential system $DY = AY$ is* affine regular *if its associated differential module is affine regular.*

Let $L = \sum_{i=1}^{n} K[t]f_i$ be any $K[t]$-lattice of M. Then, the set

$$I_L = \{q \in K[t] \text{ s.t. } q\partial L \subseteq L\}$$

is an ideal of $K[t]$, which is therefore principal. Let $q \in K[t]$ be such that $q\partial f_i \in L$ for each i. Then,

$$q\partial \sum_{i=1}^{n} p_i f_i = \sum_{i=1}^{n} qD(p_i)f_i + \sum_{i=1}^{n} p_i(q\partial f_i) \in L$$

for any $p_1, \ldots, p_n \in K[t]$, so $q \in I_L$. This means that in order to prove that $q\partial L \subseteq L$, it is sufficient to prove that $q\partial f_i \in L$ for each i. Let now $b_{ij} \in K(t)$ be such that $\partial f_i = \sum_{j=1}^{n} b_{ij} f_j$ and $d \in K[t] \setminus \{0\}$ be a common denominator for all the b_{ij}. Then, $db_{ij} \in K[t]$ for all i, j, so $d\partial f_i \in L$ for all i, which implies that $d \in I_L$. Therefore, $I_L \neq (0)$, so we call its unique monic generator the *denominator* of ∂L. If L is normal, then I_L contains a nonzero normal polynomial, which implies that its generator must be normal. Therefore, a lattice L is normal if and only if the denominator of ∂L is normal. It turns out that as in the classical case (when $D = d/dt$) affine regular systems are gauge-equivalent to systems with simple normal finite poles.

Theorem 1 *The differential system $DY = AY$ is affine regular if and only if there exist $T \in GL_n(K(t))$ such that $T_D[A]$ has a normal common denominator.*

Proof. Write $A = (a_{ij})$ and let (M, ∂) be the differential module associated with $DY = AY$, with basis $e_1, \ldots, e_n$ such that $\partial e_i = -\sum_{j=1}^{n} a_{ji} e_j$. Suppose first that $DY = AY$ is affine regular and let $N = \sum_{i=1}^{n} K[t]f_i$ be a normal $K[t]$-lattice of M and $d \in K[t] \setminus \{0\}$ be its normal denominator. Since $f_1, \ldots, f_n$ is a $K(t)$-basis of M, let $T \in GL_n(K(t))$ be such that $(f_1, \ldots, f_n)^t = T^t(e_1, \ldots, e_n)^t$. Writing $T_D[A] = (b_{ij})$, the calculation (5) shows that $\partial f_i = -\sum_{j=1}^{n} b_{ji} f_j$ for each i. Since $d\partial f_i \in N$ for all i, it follows that $db_{ji} \in K[t]$ for all i, j, hence that the least common denominator of $T_D[A]$ is a factor of d, so it must be normal. Conversely, suppose now that there exist $T \in GL_n(K(t))$ such that the common denominator p of $T_D[A]$ is normal. As above, write $T_D[A] = (b_{ij})$ and let $N = \sum_{i=1}^{n} K[t]f_i$ where $(f_1, \ldots, f_n)^t = T^t(e_1, \ldots, e_n)^t$. The calculation (5) shows that $\partial f_i = -\sum_{j=1}^{n} b_{ji} f_j$ for each i, hence that $p\partial f_i \in N$. Therefore, $p\partial N \subseteq N$, which implies that N is normal, hence that $DY = AY$ is affine regular. □

The change of variable matrix T given by Theorem 1 has rational entries. However, it is possible to multiply T by its common denominator in order to obtain a polynomial change of variable that transforms an affine regular system to one with simple normal finite poles.

Lemma 1 *Let (F, D) be a differential field. For any $n \times n$ matrix A with entries if F, any $T \in GL_n(F)$ and any $\alpha \in F^*$,*

$$(\alpha T)_D[A] = T_D[A] - \frac{D\alpha}{\alpha}\,.$$

Proof. By a direct calculation:

$$\begin{aligned}(\alpha T)_D[A] &= (\alpha T)^{-1}A(\alpha T) - (\alpha T)^{-1}D(\alpha T) \\ &= T^{-1}\alpha^{-1}A\alpha T - T^{-1}\alpha^{-1}(\alpha DT + D(\alpha)T) = T_D[A] - \frac{D\alpha}{\alpha}\,.\end{aligned}$$

□

Corollary 1 *The differential system $DY = AY$ is affine regular if and only if there exist a nonsingular $n \times n$ matrix T with entries in $K[t]$ such that $T_D[A]$ has a normal common denominator.*

Proof. If there exists such a matrix T, then $DY = AY$ is affine regular by Theorem 1. Conversely, if $DY = AY$ is affine regular, then Theorem 1 yields $T \in GL_n(K(t))$ such that $T_D[A]$ has a normal common denominator. Let d be a common denominator of T, $d = \prod_j p_j^{e_j}$ be its irreducible factorisation and $U = dT$, which is nonsingular and has entries in $K[t]$. By Lemma 1 and the logarithmic derivative identity,

$$U_D[A] = (dT)_D[A] = T_D[A] - \frac{Dd}{d} = T_D[A] - \sum_j e_j \frac{Dp_j}{p_j}$$

so the common denominator of $U_D[A]$ is the least common multiple of the common denominator of $T_D[A]$ and the normal p_j's, which is itself normal. □

Corollary 2 *Let (M, ∂) be a differential module and $e_1, \ldots, e_n$ a given $K(t)$-basis of M. Then, M is affine regular if and only if it contains a normal $K[t]$-lattice N such that $N \subseteq \sum_{i=1}^n K[t]e_i$.*

Proof. If M contains such a normal $K[t]$-lattice, then it is affine regular by definition. Conversely, suppose that M is affine regular and let $A = (a_{ij})$ be the matrix given by $\partial e_i = -\sum_{j=1}^n a_{ji}e_j$. Then, $DY = AY$ is regular, so by Corollary 1, there exists a nonsingular matrix T with entries in $K[t]$ such that $T_D[A]$ has a normal common denominator. Let then $N = \sum_{i=1}^n K[t]f_i$ where $(f_1, \ldots, f_n)^t = T^t(e_1, \ldots, e_n)^t$. As in the proof of Theorem 1, N is a normal $K[t]$-lattice. However, $f_i \in \sum_{i=1}^n K[t]e_i$ since the entries of T are in $K[t]$, so $N \subseteq \sum_{i=1}^n K[t]e_i$. □

The *dual module* of a differential module (M, ∂) is the $K(t)$-vector space $M^* = \mathrm{Hom}_{K(t)}(M, K(t))$ of $K(t)$-linear maps from M into $K(t)$, together with the derivation ∂^* defined by

$$\partial^*\phi = D\phi - \phi\partial \quad \text{for all } \phi \in M^*\,.$$

The *dual basis* of a $K(t)$-basis $f_1, \ldots, f_n$ of M is the $K(t)$-basis $f_1^*, \ldots, f_n^*$ of M^* defined by $f_i^*(f_j) = \delta_{ij}$ where δ_{ij} is the Kronecker symbol (1 if $i = j$, 0 otherwise). We recall a useful formula connecting the dual bases corresponding to two bases: if $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ are $K(t)$-bases of M connected by

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = P \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

for some $P \in GL_n(K(t))$, then

$$\begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix} = P^t \begin{pmatrix} f_1^* \\ \vdots \\ f_n^* \end{pmatrix} . \tag{6}$$

Let $A = (a_{ij})$ be an $n \times n$ square matrix with entries in $K(t)$ and (M, ∂) the differential module associated with $DY = AY$, with basis $e_1, \ldots, e_n$ where $\partial e_i = -\sum_{j=1}^n a_{ji} e_j$ for each i. We have

$$(\partial^* e_i^*)(e_j) = D(e_i^*(e_j)) - e_i^*(\partial e_j) = -e_i^*\left(-\sum_{s=1}^n a_{sj} e_s\right) = \sum_{s=1}^n a_{sj} e_i^*(e_s) = a_{ij}$$

which implies that

$$\partial^* e_i^* = \sum_{j=1}^n a_{ij} e_j^* \quad \text{for all } i \tag{7}$$

so we can view $(e_1^*, \ldots, e_n^*)^t$ as a "formal solution" of $DY = AY$.

Lemma 2 *Let (M, ∂) be a differential module. If $N = \sum_{i=1}^n K[t] f_i$ is a normal $K[t]$-lattice of M, then $N^* = \sum_{i=1}^n K[t] f_i^*$ is a normal $K[t]$-lattice of M^*.*

Proof. Let $p \in K[t] \setminus \{0\}$ be normal and such that $p\partial N \subseteq N$. Then, there are $p_{ij} \in K[t]$ such that $p\partial f_i = \sum_{j=1}^n p_{ij} f_j$ for all i. Therefore,

$$\begin{aligned} (p\partial^* f_i^*)(f_j) &= pD(f_i^*(f_j)) - p f_i^*(\partial f_j) = -f_i^*(p\partial f_j) \\ &= -f_i^*\left(\sum_{s=1}^n p_{js} f_s\right) = -\sum_{s=1}^n p_{js} f_i^*(f_s) = p_{ji} \in K[t] \end{aligned}$$

which implies that

$$p\partial^* f_i^* = \sum_{j=1}^n (p\partial^* f_i^*)(f_j) f_j^* = \sum_{j=1}^n p_{ji} f_j^* \in N^*$$

hence that $p\partial^* N^* \subseteq N^*$, so N^* is normal. □

Since $M^{**} = M$, it follows that (M, ∂) is affine regular if and only if (M^*, ∂^*) is affine regular.

Lemma 3 *A $K[t]$-lattice N of a differential module is normal if and only if*

$$q\partial m \in N \Rightarrow q^*\partial m \in N \tag{8}$$

for all $m \in N$ and $q \in K[t]$.

Proof. Suppose that $p\partial N \subseteq N$ for some normal $p \in K[t] \setminus \{0\}$. Let $m \in N$ and $q \in K[t]$ be such that $q\partial m \in N$, and $g = \gcd(q,p) = aq + bp$ for some $a, b \in K[t]$. Since p is normal, it is squarefree and all its irreducible factors are normal, so g is a normal factor of q, which implies that $q^* = hg$ for some $h \in K[t]$. Therefore,

$$q^*\partial m = h(aq+bp)\partial m = ha(q\partial m) + hb(p\partial m) \in N\,.$$

Conversely, suppose that (8) holds for all $m \in N$ and $q \in K[t]$ and let $d \neq 0$ be the denominator of ∂N. Then, for any $m \in N$, $d\partial m \in N$, which implies that $d^*\partial m \in N$, hence that $d^*\partial N \subseteq N$. This means that $d \mid d^*$ in $K[t]$, hence that d is normal. □

We can finally prove the termination of our algorithm.

Theorem 2 *Let A be any square matrix with entries in $K(t)$. If the differential system $DY = AY$ is affine regular, then the algorithm of Section 2 terminates after a finite number of iterations, yielding a nonsingular upper triangular matrix U with entries in $K[t]$ such that $U_D[A]$ has a normal common denominator.*

Proof. Write $A = (a_{ij})$ and let (M, ∂) be the differential module associated with $DY = AY$, with basis $e_1, \ldots, e_n$ such that $\partial e_i = -\sum_{j=1}^n a_{ji}e_j$. Since the differential system is affine regular, Corollary 2 implies that M contains a normal $K[t]$-lattice $N = \sum_{i=1}^n K[t]f_i$ such that $N \subseteq \sum_{i=1}^n K[t]e_i$. By Lemma 2, $N^* = \sum_{i=1}^n K[t]f_i^*$ is a normal $K[t]$-lattice of the dual module (M^*, ∂^*). Since $N \subseteq \sum_{i=1}^n K[t]e_i$,

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = P \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

for some $n \times n$ nonsingular matrix P with entries in $K[t]$. It then follows from (6) that $e_i^* \in N^*$ for each i, hence that $\sum_{i=1}^n K[t]e_i^* \subseteq N^*$. Using the notation of Section 2.2, suppose that the algorithm picks some d_j not normal and computes a basis $u_1, \ldots, u_n$ for M_j over $K[t]$ (see (3)). Let $T \in GL_n(K(t))$ be the upper triangular matrix whose rows are the coordinates of $u_1, \ldots, u_n$, and L be the lattice $L = \sum_{i=1}^n K[t]h_i^*$ where

$$(h_1^*, \ldots, h_n^*) = (e_1^*, \ldots, e_n^*)T^t \tag{9}$$

Each $w = (w_1, \ldots, w_n)^t \in M_j$ can be written $w = \sum_{s=1}^n p_s u_s$ for some $p_1, \ldots, p_n$ in $K[t]$. Writing $u_s = (u_{s1}, \ldots, u_{sn})^t$ for each s, we get $w_i = \sum_{s=1}^n p_s u_{si}$ for each i, whence

$$\sum_{i=1}^n w_i e_i^* = \sum_{i=1}^n \sum_{s=1}^n p_s u_{si} e_i^* = \sum_{s=1}^n p_s \left(\sum_{i=1}^n u_{si} e_i^* \right) = \sum_{s=1}^n p_s h_s^* \in L\,.$$

Conversely, each $m = \sum_{s=1}^{n} m_i e_i^* \in L$ can be written $m = \sum_{s=1}^{n} p_s h_s^*$ for some $p_1, \ldots, p_n \in K[t]$. Therefore,

$$m = \sum_{s=1}^{n} p_s h_s^* = \sum_{s=1}^{n} p_s \sum_{i=1}^{n} u_{si} e_i^* = \sum_{i=1}^{n} \left(\sum_{s=1}^{n} p_s u_{si} \right) e_i^* = \sum_{s=1}^{n} m_i e_i^*$$

so $m_i = \sum_{s=1}^{n} p_s u_{si}$, which implies that $(m_1, \ldots, m_n)^t = \sum_{s=1}^{n} p_s u_s \in M_j$. Therefore,

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in M_j \iff \sum_{s=1}^{n} w_i e_i^* \in L \,.$$

Since $K[t]^n \subset M_j$, it then follows that $\sum_{i=1}^{m} K[t] e_i^* \subset L$. By (7) we have $d_j^* \partial^* e_j^* = \sum_{i=1}^{n} d_j^* a_{ji} e_i^*$. Since $(d_j^* a_{j1}, \ldots, d_j^* a_{jn})^t \in M_j$, we have $d_j^* \partial^* e_j^* \in L$, so L contains $\sum_{i=1}^{m} K[t] e_i^* + K[t] d_j^* \partial^* e_j^*$. Conversely, let $m = \sum_{s=1}^{n} m_i e_i^* \in L$. Then, $(m_1, \ldots, m_n)^t \in M_j$, so

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} + q \begin{pmatrix} d_j^* a_{j1} \\ \vdots \\ d_j^* a_{jn} \end{pmatrix}$$

for some $q, p_1, \ldots, p_n \in K[t]$. Therefore,

$$m = \sum_{i=1}^{n} p_i e_i^* + q d_j^* \sum_{i=1}^{n} a_{ji} e_i^* = \sum_{i=1}^{n} p_i e_i^* + q d_j^* \partial^* e_j^*$$

so $L = \sum_{i=1}^{m} K[t] e_i^* + K[t] d_j^* \partial^* e_j^*$. We also have $d_j \partial^* e_j^* \in N^*$ since d_j is a common denominator for $a_{j1}, \ldots, a_{jn}$. Since N^* contains e_j^* and is normal, $d_j^* \partial^* e_j^* \in N^*$ by Lemma 3, so $L \subseteq N^*$. Since d_j is not normal, $d_j^*/d_j \notin K[t]$, which implies that $d_j^* \partial^* e_j^* \notin \sum_{i=1}^{n} K[t] e_i^*$. The change of basis (9) has thus constructed a lattice $L = \sum_{i=1} K[t] h_i^*$ such that

$$\sum_{i=1}^{n} K[t] e_i^* \subsetneq L \subseteq N^* \,.$$

The change of variable $Z = TY$ corresponds to replacing the basis $e_1^*, \ldots, e_n^*$ of M^* by $h_1^*, \ldots, h_n^*$, *i.e.* replacing $\sum_{i=1}^{n} K[t] e_i^*$ by L. Therefore, any sequence of reduction steps of our algorithm produces a stricly ascending chain of sublattices of N^*. Since N^* is a finitely generated module over the principal ideal domain $K[t]$, it is Noetherian [10, Chap. XV], so any such chain is finite, which implies that our algorithm terminates after a finite number of iterations.
At each iteration, the change of variable $Z = TY$ corresponds to the gauge transformation $Y = T^{-1}Z$, so $U_D[A]$ has a normal common denominator, where $U \in GL_n(K(t))$ is the product of all the T^{-1} at each step. Since each T^{-1} is upper triangular and has all its entries it $K[t]$, this is also the case for U. □

We conclude with a remark about adapting our algorithm to systems with irregular singularities. Suppose that the dual module M^* contains a lattice N^*, not necessarily normal, such that $\sum_{i=1}^n K[t]e_i^* \subseteq N^*$. Let $q \in K[t] \setminus \{0\}$ be the denominator of $\partial^* N^*$. We can modify the definition of the module M_i by replacing d_i^* in (3) by $\gcd(d_i, q)$, and apply the single reduction step as long as $\deg(\gcd(d_i, q)) < \deg(d_i)$. Since $q\partial^* e_i^* \in N^*$ and $d_i \partial^* e_i^* \in \sum_{j=1}^n K[t]e_j^* \subseteq N^*$, $\gcd(d_i, q)\partial^* e_i^* \in N^*$, so the proof of Theorem 2 then remains valid as we construct a lattice L such that $\sum_{i=1}^n K[t]e_i^* \subsetneq L \subseteq N^*$. So the modified algorithm also terminates, and it yields a system $DZ = BZ$ where the denominator of B divides q. In the regular case, we can take q to be the normal part of the denominator of A, which yields our original algorithm. In the presence of finite irregular singularities, we could use the modified algorithm if we knew a priori the Poincaré rank at each singularity, which would yield the minimal such q. Even if we do not know such a q, our algorithm could still be used to compute it if we can detect nontermination after a bounded number of iterations.

4 Regular singularities and the local reduction

We outline in this section the local version of our algorithm at a single regular singularity. Recall that the *local ring at an irreducible* $p \in K[t]$ is defined by

$$\mathcal{O}_p = \{f \in K(t) \text{ such that } af \in K[t] \text{ for some } a \in K[t] \text{ with } \gcd(a, p) = 1\}$$

and it is easy to check that $D\mathcal{O}_p \subset \mathcal{O}_p$ since $Dt \in K[t]$. Any $f \in K(t)^*$ can be written uniquely $f = p^{-\mu}g$ where $\mu \geq 0$ is an integer and $g \in \mathcal{O}_p$ is such that $g \in \mathcal{O}_p^*$ whenever $\mu > 0$. We can then call g and p^μ the (local) numerator and denominator of f at p. Since $\mathcal{O}_p$ is a principal ideal domain whose nonzero ideals are all of the form $p^m\mathcal{O}_p$ for $m \geq 0$, we can define the denominator of ∂L for an $\mathcal{O}_p$-lattice L as we did earlier. If we call such a lattice *normal* if its denominator is normal, the definition of local regularity of [14] is then just the local version of affine regularity.

Definition 3 *Let $p \in K[t]$ be irreducible. We say that the differential module (M, ∂) is* regular singular at p *if it contains an $\mathcal{O}_p$-lattice N such that $p^{\delta_D(p)}\partial N \subseteq N$. The differential system $DY = AY$ has a* regular singularity at p *if p divides the denominator of at least one entry of A and if the associated differential module is regular singular at p.*

Let now $DY = AY$ be a differential system and $p \in K[t]$ an irreducible factor of the denominator of A. We can replace $K[t]$ by $\mathcal{O}_p$ and denominators by local denominators at p in our algorithm. The proof of termination is then the same than in the affine case, with $K[t]$ replaced by $\mathcal{O}_p$ throughout, so our algorithm can be used to transform $DY = AY$ to a system with a simple pole at p.

Theorem 3 *Let A be any square matrix with entries in $K(t)$ and $p \in K[t]$ an irreducible factor of the denominator of A. If the differential system $DY = AY$*

has a regular singularity at p, then the algorithm of Section 2 over $\mathcal{O}_p$ terminates after a finite number of iterations, yielding a nonsingular upper triangular matrix U with entries in $\mathcal{O}_p$ such that the entries of $p^{\delta_D(p)}U_D[A]$ are all in $\mathcal{O}_p$.

Since β in (2) can always be taken in $K[t]$ when $R = \mathcal{O}_p$, and since the diagonal elements of U are powers of p, it follows that the poles of $U_D[A]$ are among the poles of A. We note that the local version of our algorithm is very similar to the regular case of the one-step saturation of [6], but not quite the same.

5 Applications to algebraic curves

We now apply our algorithm to differential systems arising from algebraic curves. Let X, Y be indeterminates over the a field K, $\overline{K}$ be the algebraic closure of K and $P \in K[X,Y]$ be squarefree (not necessarily irreducible). Considering P as a univariate polynomial in Y over $K(X)$, let R be the $K(X)$-algebra $R = K(X)[Y]/(P) = K(X,y)$ where y denotes the image of Y in R. It is a vector space of dimension $n = \deg_Y(P)$ over $K(X)$. Let $b_1, \ldots, b_n$ be a $K(X)$-basis of R. Since $1, y, \ldots, y^{n-1}$ is also a basis,

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = T \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{n-1} \end{pmatrix} \tag{10}$$

for some $T \in GL_n(K(X))$. Let D be a derivation of $K(X)$ such that $DK \subset K$ and $DX \in K[X]$ (for example $D = d/dX$). Then, X is a monomial over K with respect to D, and since P is squarefree, D extends uniquely to R. Therefore, there exists an $n \times n$ matrix A with entries in $K(X)$ such that

$$D \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = A \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} .$$

This implies that $D(TV) = A(TV)$ where V is the Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ y_1 & y_2 & \cdots & y_n \\ \vdots & \vdots & & \vdots \\ y_1^{n-1} & y_2^{n-1} & \cdots & y_n^{n-1} \end{pmatrix}$$

and $y_1, \ldots, y_n$ are the distinct roots of P in the algebraic closure of $K(X)$. Therefore, the system $DY = AY$ has a fundamental solution matrix whose entries are all algebraic over $K(X)$, so it is affine regular (this is a classical result for $D = d/dX$, in general it is a consequence of the fact that the integral closure of $K[X]$ in R is a normal $K[X]$-lattice of R, see [4]). Applying our

algorithm to it yields an upper triangular nonsingular matrix U with entries in $K[X]$ such that $U_D[A]$ has a normal denominator. Thus, the basis

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = U^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \tag{11}$$

of R over $K(X)$ is a solution of the differential system $DZ = U_D[A]Z$, whose finite poles are all simple and normal. The differential system $DZ = U_D[A]Z$ can be used instead of the operator L_P of [7] in order to compute the same quantities, namely a basis of $\mathrm{Const}_D(R)$ over $\mathrm{Const}_D(K(X))$ (hence an absolute factorisation of P over $\overline{K}$ when $D = d/dX$), the genus of the curve $P(X, Y) = 0$ or the geometric Galois group of $P(X, Y)$. Since $U^{-1}TV$ is a fundamental solution matrix of $DZ = U_D[A]Z$, all the solutions of that system also are algebraic over $K(X)$, so, unlike in [7], we do not require that the roots of P are linearly independent over $\overline{K}$, in fact we can even allow roots of P to be in $\overline{K}$.

Suppose from now on that $D = d/dX$ (this is not really necessary but allows us to rely on the classical theory of regular differential systems) and let $p \in K[X]$ be an irreducible factor of the common denominator of $U_D[A]$. The indicial equation of $DZ = U_D[A]Z$ at a root $\alpha \in \overline{K}$ of p is the characteristic polynomial of the matrices of the residues of $U_D[A]$ at $X = \alpha$, namely

$$E_\alpha(\lambda) = \det\left(((X - \alpha)U_D[A])(\alpha) - \lambda\right) \in K(\alpha)[\lambda]\,. \tag{12}$$

Since $DZ = U_D[A]Z$ has a fundamental solution matrix of algebraic functions, all the roots of $E_\alpha(\lambda)$ are in the field $\mathbb{Q}$ of rational numbers, so it factors as

$$E_\alpha(\lambda) = c\prod_j (\lambda - q_j)^{\mu_j} \tag{13}$$

where $c \in K(\alpha)^*$, $q_j \in \mathbb{Q}$ for each j, and the multiplicities $\mu_j > 0$ satisfy $\sum_j \mu_j = \deg_\lambda(E_\alpha) = n$. The q_j, called the *exponents* of the system at $X = \alpha$, are independent of the choice of α, so they can be computed using a single root α of p. Furthermore, $DZ = U_D[A]Z$ has a basis of Puiseux series solutions $Z_1, \ldots, Z_n$ of the form $Z_i = (X-\alpha)^{q_i}\phi_i(X-\alpha)$ where $\phi_i(X-\alpha) \in \overline{K}[[X-\alpha]]^n$ is a vector of Taylor series such that $\phi_i(\alpha) \neq 0$.

We now describe how the rational exponents of $DZ = U_D[A]Z$ at all its finite poles allow us to compute the genus of the curve $P(X, Y) = 0$ as in [7]. Define the *degree of the ramification divisor* to be the integer

$$\delta = \sum_{\alpha \in \overline{K} \cup \{\infty\}} \sum_{\mathcal{P}} (e(\mathcal{P}) - 1) \tag{14}$$

where the inner sum is taken over all the places $\mathcal{P}$ above α, and $e(\mathcal{P})$ stands for the ramification index of $\mathcal{P}$. For a rational number $r \in \mathbb{Q}$, define the fractional part of r, denoted $r \bmod \mathbb{Z}$, to be the unique $r' \in \mathbb{Q}$ such that $0 \leq r' < 1$ and $r - r' \in \mathbb{Z}$.

Proposition 1 *Let $p \in K[X]$ be an irreducible factor of the common denominator of $U_D[A]$, $\alpha \in \overline{K}$ be a root of p, $P_1, \ldots, P_h$ be the places above $X = \alpha$ and $e_1, \ldots, e_h$ their respective ramification indices. Then,*

$$\sum_{i=1}^{h}(e_i - 1) = 2\sum_j \mu_j(q_j \bmod \mathbb{Z})$$

where the q_j are the exponents given by (13) and the μ_j their multiplicities.

Proof. Let $y_1 \in \overline{K((X-\alpha))}$ be a solution of $P(X,Y) = 0$ of ramification e_1. Then, $y_1 \in \overline{K}((X-\alpha)^{1/e_1})$, so $y_1^m \in \overline{K}((X-\alpha)^{1/e_1})$ for all $m \geq 0$, whence

$$\begin{pmatrix} 1 \\ y_1 \\ \vdots \\ y_1^{n-1} \end{pmatrix} = \sum_{j=0}^{e_1-1}(X-\alpha)^{j/e_1}F_{1,j}$$

where $F_{1,j} \in \overline{K}((X-\alpha))^n$ for each j. The e_1 conjugates $y_{1,0}, \ldots, y_{1,e_1-1}$ of y_1 are obtained by replacing $(X-\alpha)^{1/e_1}$ by $\zeta_1^k(X-\alpha)^{1/e_1}$ where $\zeta_1 \in \overline{\mathbb{Q}}$ is a primitive e_1-th root of unity. Therefore,

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ y_{1,0} & y_{1,1} & \cdots & y_{1,e_1-1} \\ \vdots & \vdots & & \vdots \\ y_{1,0}^{n-1} & y_{1,1}^{n-1} & \cdots & y_{1,e_1-1}^{n-1} \end{pmatrix} = M_1 \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta_1 & \cdots & \zeta_1^{e_1-1} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_1^{e_1-1} & \cdots & \zeta_1^{(e_1-1)(e_1-1)} \end{pmatrix} \quad (15)$$

where M_1 is the $n \times e_1$ matrix whose columns are $F_{1,0}$, $(X-\alpha)^{1/e_1}F_{1,1}$, …, $(X-\alpha)^{(e_1-1)/e_1}F_{1,e_1-1}$. Writing $W(y_1, e_1)$ for the matrix on the left-hand side of (15) and $V(\zeta_1, e_1)$ for the Vandermonde matrix of $1, \zeta_1, \ldots, \zeta_1^{e_1-1}$ on its right-hand side, and repeating the above at $P_1, \ldots, P_h$, we get

$$(W(y_1,e_1) \mid \cdots \mid W(y_h,e_h)) = (M_1|M_2|\cdots|M_h)\begin{pmatrix} V(\zeta_1,e_1) & & \\ & \ddots & \\ & & V(\zeta_h,e_h) \end{pmatrix} \quad (16)$$

where ζ_i is a primitive e_i-th root of unity. Since $\sum_{j=1}^{h} e_j = n$,

$$U^{-1}T(W(y_1,e_1) \mid \cdots \mid W(y_h,e_h))$$

is a local fundamental solution matrix of $DZ = U_D[A]Z$ where T is the change of basis matrix given by (10) and U is the matrix returned by our algorithm. Since the block-diagonal Vandermonde matrix on the right-side of (16) is in $GL_n(\overline{\mathbb{Q}})$, it follows that $(M_1|M_2|\cdots|M_h)$ is also a a local fundamental solution matrix of $DZ = U_D[A]Z$. Therefore, the valuations of each column of $(M_1|M_2|\cdots|M_h)$ differ from some root q_j of the indicial equation by an integer. Since the valuation of $(X-\alpha)^{k/e_i}F_{i,k}$ is $k/e_i + n_{i,k}$ where $n_{i,k} \in \mathbb{Z}$ and $\sum_j \mu_j = n$ is the

number of columns, we get

$$2\sum_j \mu_j(q_j \bmod \mathbb{Z}) = 2\sum_{i=1}^{h}\sum_{k=0}^{e_i-1}\frac{k}{e_i} = 2\sum_{i=1}^{h}\frac{e_i-1}{2} = \sum_{i=1}^{h}(e_i-1)\,.$$

□

Our algorithm for computing the degree of the ramification divisor is then the following: we first do the change of variable $X = N + 1/Z$ where $N \in \mathbb{Z}$ is chosen such that $\Delta(N) \neq 0$ where Δ is the discriminant of $P(X,Y)$ with respect to Y. This yields an equivalent curve $Q(Z,Y) = 0$ with the same δ but where the places at infinity are unramified, so the summand $\alpha = \infty$ can be dropped from (14). We then pick any basis $b = b_1, \ldots, b_n$ of $K(Z)[Y]/(Q)$ (for example $1, y, \ldots, y^{n-1}$), differentiate it in order to obtain the matrix A such that $db/dZ = Ab$ and apply our algorithm to obtain the gauge transformation U such that the denominator d of $U_{d/dZ}[A]$ is squarefree. Proposition 1 and (14) then give the degree as

$$\delta = 2 \sum_{\substack{\alpha \in \overline{K} \\ d(\alpha) = 0}} \sum_j \mu_j(q_j \bmod \mathbb{Z})$$

where the q_j and μ_j are given by (13). Since the roots of $E_\alpha(\lambda)$ are the same for all roots α of the same irreducible factor of d, the above formula can be refined into

$$\delta = 2 \sum_{\substack{p \in K[Z] \text{ irreducible} \\ p \mid d}} \deg(p) \sum_j \mu_j(q_j \bmod \mathbb{Z})\,.$$

Of course, only the irreducible p that divide the discriminant of Q need to be considered. As explained if [7], we do not need to compute $E_\alpha(\lambda)$ when all the points above $Z = \alpha$ are nonsingular, since $2\sum_j \mu_j(q_j \bmod \mathbb{Z})$ is the multiplicity of $Z - \alpha$ dividing the discriminant in that case. This is in particular the case when p is a simple factor of the discriminant, so only multiple factors of the discriminant may require the computation of the local indicial equation.

If $P(X,Y)$ is absolutely irreducible (that is irreducible in $\overline{K}[X,Y]$, then the curve $P(X,Y) = 0$ is irreducible and its genus g is given by Hurwitz' formula:

$$g = 1 - n + \frac{\delta}{2}$$

where δ is the degree of the ramification divisor, which we compute as explained above. If $P(X,Y)$ is irreducible in $K[X,Y]$ and splits into m conjugate factors over $\overline{K}$, then all the irreducible components of the curve have the same genus g, which is given by

$$g = 1 - \frac{n}{m} + \frac{\delta}{2m}$$

Knowledge of the rational exponents of $DZ - U_D[A]Z$ at all its finite singularities can be also used to compute the denominators of its solutions in $K(X)^n$, and eventually to compute those rational solutions (by sending ∞ to 0 and repeating our algorithm locally there). This allows us to compute a basis over K of $\mathrm{Const}_{d/dX}(R)$ since

$$D\sum_{i=1}^{n} c_i w_i = 0 \iff D\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = -(U_D[A])^t \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

where $w_1, \ldots, w_n$ is the basis of R over $K(X)$ given by (11). It is therefore sufficient to find the solutions in $K(X)$ of the above differential system, which has only simple affine poles. A basis of the constant ring then yields an absolute factorisation of P as in [7]. Since $\dim_K(\mathrm{Const}_{d/dX}(R))$ is the number of irreducible components of the curve, we can use our algorithm to compute the genus of each irreducible component of the curve $P(X, Y) = 0$ whenever P is squarefree.

References

[1] M. Barkatou. A rational version of Moser's algorithm. In A.H.M. Levelt, editor, *Proceedings of ISSAC'95*, pages 297–302. ACM Press, 1995.

[2] Moulay A. Barkatou. On rational solutions of systems of linear differential equations. *Journal of Symbolic Computation*, 28(4–5):547–567, October/November 1999.

[3] M. Bronstein. *Symbolic Integration I – Transcendental Functions*. Springer, Heidelberg, 1997.

[4] M. Bronstein. The lazy Hermite reduction. Rapport de Recherche RR–3562, INRIA, 1998.

[5] F.T. Cope. Formal solutions of irregular linear differential equations II. *American Journal of Mathematics*, 58:130–140, 1936.

[6] E. Corel. Algorithmic computation of exponents for linear differential systems. *in preparation*.

[7] O. Cormier, M.F. Singer, B.M. Trager, and F. Ulmer. Linear differential operators for polynomial equations. *Journal of Symbolic Computation*, 34(5):355–398, 2002.

[8] F. Gantmacher. *The theory of matrices*. Chelsea Publishing Co., New York, 1959.

[9] A. Hilali and A. Wazner. Formes super–irréductibles des systèmes différentiels linéaires. *Numerical Mathematics*, 50:429–449, 1987.

[10] S. Lang. *Algebra*. Addison Wesley, Reading, Massachusetts, 1970.

[11] A.H.M. Levelt. Stabilizing differential operators. In M. Singer, editor, *Differential Equations and Computer Algebra*, pages 181–228. Academic Press, London, 1991.

[12] J. Moser. The order of a singularity in Fuch's theory. *Mathematische Zeitschrift*, 72:379–398, 1960.

[13] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1989.

[14] M.F. Singer and M. van der Put. *Differential Galois Theory*. to appear. Springer, 2003.