Differential and mixed differential-difference equations from the effective viewpoint

By Joris van der Hoeven

December 4, 1996

Introduction

This paper regroups several results in the continuation of my D.E.A. report [VdH 93]. The paper was originally intended to be part of my PhD. thesis. However, because my thesis has grown in size more than expected, I decided to suppress this part, which is independent from the rest of my thesis.

The first chapter concerns the computation with special functions determined by algebraic differential equations and initial conditions. The second part deals with a generalization of effective differential elimination theory to the context of so called D-rings, introduced by Nichols and Weisfeiler. The last, and most original part deals with a generalization of the results of chapter 2 to more general mixed differential-difference equations.

Joris van der Hoeven

Paris, December 4, 1996

Contents

Chapter 1

Computations with special functions

1.1 Introduction

Transcendental functions like $\exp, \log, \sin, \wp$, etc. have been studied since a long time. In our age of symbolic computation it is natural to ask whether computations with such functions can be done automatically. Essentially, this question can be reduced to the following one: given an expression built up from the rationals, a finite number of indeterminates and a given set of elementary functions, can we decide whether the expression is zero? Since the expressions are not necessarily canonically determined (they usually admit non trivial Riemann surfaces), the problem should be specified further: can we decide whether the expression is locally zero at a given point on the Riemann surface? We also have to specify what we mean by elementary functions: in this chapter, we will consider a very large class of elementary functions, namely those which can be entirely specified by a finite number of algebraic partial differential equations with initial conditions. In what follows, such functions will be called D-algebraic functions.

Let us first briefly discuss some of the history of the above problem. Initially, most of the research has been centered around finding canonical ways for representing expressions of the above type, based on our experience with polynomials. The study of functions built up from algebraic functions, exponentiation and logarithm was started by Liouville (see [Li 1837] and [Li 1838]) and culminated one and a half century later in the Risch structure theorem (see [Ris 75]). These techniques were extended to include a few other transcendental functions such as the error function by Cherry and Caviness (see [Ch 83], [CC 85]). However, for many other special functions, the desire of having canonical representations seems to be to ambitious.

The emergence of holonomic functions has provided a new way of looking at the question. Holonomic functions (in one variable) are functions which satisfy a non trivial linear differential equation over the polynomials with rational coefficients. They are represented, although not uniquely, by such a differential equation and a number of initial conditions. The basic idea is now to compute with these representations, without searching for canonical ones. Denef and Lipshitz, followed by others have generalized the holonomic function approach to D-algebraic functions (see [DL 89], [SH 89]). At this moment, the most promising algorithm for computations with D-algebraic functions is due to Péladan-Germa (see [Pél 95]). However, no implementation of this algorithm is available yet.

We finally mention that in the above discussion, we implicitly assumed the existence of an oracle, to perform the necessary computations with constants. Actually, this is a very strong hypothesis since computations with transcendental numbers turn out to be even harder than computations with transcendental functions (modulo a suitable oracle for the constants). Although it is often easy to decide whether a constant is zero (it suffices to perform a floating point evaluation at a sufficient precision), it can be very hard to prove that a constant is zero. Nevertheless, in the case of constants determined by exp-log equations, an algebraic zero-test does exist modulo Schanuel's conjecture and we refer to the introduction for more details.

Let us now come more particularly to the contents of this chapter. We have chosen the differential algebra with initial conditions setting to study local functions. This has the disadvantage of restricting the class of functions which can be studied, but the advantage of being suitable for effective computations by its algebraic character.

In section 1.2, we introduce the formalism of D-rings. This formalism is due to Nichols and Weisfeiler (see [NiWe 82], [Bu 92]) and provides an algebraic setting for studying p.d.e.'s on curved geometrical objects. Its originality with respect to the classical theory of differential algebra (as developed by Riquier, Janet, Ritt, Raudenbush, Seidenberg, Kolchin, etc.; see [Riq 10], [Jan 20], [Ritt 50], [Kol 73], [Kap 76]) is that the derivations do not necessarily commute. Consequently, p.d.e.'s on non affine objects such as spheres can be considered, even though no essentially new functions are introduced by this. Actually, the formalism of D-rings mainly allows us to place ourselves in the coordinates, which correspond to the underlying geometry of the problem. Moreover, we will see in chapter 2 that the main results from classical differential algebra can be generalized without much effort.

In section 1.3, we introduce D-rings with initial conditions. We will mainly consider initial conditions in a point, which correspond to (non differential) maximal ideals of the D-ring.

In section 1.4, we establish the main algorithms for computations with D-algebraic functions. We start with a generalization of an algorithm due to Shackell and an optimization of this algorithm using a local pseudo-Buchberger algorithm. This work was carried out jointly with A. Péladan-Germa in [PV 96]. For the local pseudo-Buchberger algorithm, we refer to section 1.6. We proceed with a zero-equivalence algorithm which is particularly useful when the point in which the zero-test is performed may be chosen randomly: in that case, virtually all functions which evaluate to zero are zero, and this property is exploited in the algorithm.

In section 1.5 we consider some other computations which can be done with D-algebraic functions. Most importantly, we obtain an implicit function theorem, which permits to solve effectively certain systems of implicit equations determined by D-algebraic functions. This is a crucial result on which many algorithms in part B of this thesis rely.

1.2 Basic concepts

1.2.1 Definition of a D-ring and examples

A **D-ring** is a couple (A, D) satisfying

DR1. A is a commutative ring.
DR2. D is an A-module of derivations on A satisfying

$$\begin{aligned} 0_D\, a &= 0; \\ (bd)a &= b(da); \\ (d_1 + d_2)a &= d_1 a + d_2 a, \end{aligned}$$

for all $d, d_1, d_2 \in D$ and $a, b \in A$.
DR3. D has the structure of a Lie algebra and

$$\begin{aligned} [d_1, d_2]a &= d_1 d_2 a - d_2 d_1 a; \\ [d_1, a d_2] &= (d_1 a) d_2 + a[d_1, d_2], \end{aligned}$$

for all $d_1, d_2 \in D$ and $a \in A$.

For simplicity, we often write A instead of (A, D). In practice, (A, D) is **finite dimensional**, i.e. D is a finitely generated A-module. We notice that D-ring theory generalizes ring theory, by taking $D = 0$ for the set of derivations.

Example 1.1. If k is a field, then $(k[x, y], (d_x, d_y))$ is a D-ring. Here d_x and d_y denote the partial derivatives with respect to x resp. y and $D = (d_x, d_y)$ the $k[x, y]$-module generated by d_x and d_y. D has a natural Lie algebra structure, given by

$$\begin{aligned} [A d_x + B d_y, A' d_x + B' d_y] \;=\; & (A A'_x + B A'_y - A_x A' - A_y B') d_x + \\ & (A B'_x + B B'_y - B_x A' - B_y B') d_y. \end{aligned}$$

The D-ring $(k[x, y], (d_x, d_y))$ corresponds to the plane (over k). In a similar fashion, one defines affine n-space $(k[x_1, \cdots, x_n], (d_{x_1}, \cdots, d_{x_n}))$.

Example 1.2. If k is a field, then $(k[x, y]/(x^2 + y^2 - 1), (y d_x - x d_y))$ is a D-ring. This object corresponds to the circle with its natural derivations. Similarly, $(k[x, y, z]/(x^2 + y^2 + z^2 - 1), (d_1, d_2, d_3))$ is a D-ring, where $d_1 = y d_x - x d_y, d_2 = z d_y - y d_z$ and $d_3 = x d_z - z d_x$. We have $[d_1, d_2] = d_3, [d_2, d_3] = d_1$ and $[d_3, d_1] = d_2$.

Finally, $(k[x,y]/(xy),(xd_x,yd_y))$ is a non entire D-ring, which corresponds to the union of two lines.

Example 1.3. Assume that (A,D) is a D-ring and that I is a usual ideal of A. Then $A_{|I} = A/I$ can naturally be given the structure of a D-ring by taking $D_{|I} = \{\overline{d} \in D/ID | dI \subseteq I\}$ for the derivations. Indeed, we have a natural induced Lie bracket on $D_{|I}$, since $dI \subseteq I$ and $d'I \subseteq I$ imply $[d,d']I \subseteq I$, for all $d,d' \in D$. The D-ring $(A_{|I}, D_{|I})$ is called the **restriction of domain** of (A,D) by I. If A is Noetherian and finite dimensional, then so is $A_{|I}$. The D-rings of example 1.2 are obtained as restrictions of domain of $k[x,y]$ by x^2+y^2-1, of $k[x,y,z]$ by $x^2+y^2+z^2-1$ and of $k[x,y]$ by xy.

Example 1.4. Let A be an algebra over R. Denote by $Der_R(A)$ the set of R-derivations on A (i.e. the set of derivations $d : A \to A$ with $dR = 0$). Then $(A, Der_R(A))$ is a D-ring. If A is finitely generated, then this D-ring is finite dimensional.

1.2.2 Morphisms of D-rings

Let us now show how familiar concepts in differential algebra generalize to the context of D-rings. A **morphism of D-rings** or **D-morphism** $(A,D) \xrightarrow{\varphi,\psi} (A',D')$ is a pair of mappings $A \stackrel{\varphi}{\to} A'$ and $D \stackrel{\psi}{\to} D'$, preserving all D-ring operations. Clearly, D-rings with their morphisms form a category. Let us show that each morphism $(A,D) \xrightarrow{\varphi,\psi} (A',D')$ can be factored canonically through $(A', A' \otimes_A D)$, where we consider A' as an A-algebra, by $\lambda a = \varphi(\lambda)a$, for $\lambda \in A$ and $a \in A'$. Roughly speaking, this means that we can decompose a morphism in a part which preserves the structure of the module of derivations, and in a part which preserves the structure of the ring.

As we have a A-bilinear mapping $\mu : A' \times D \to D', (a,d) \mapsto a\psi(d)$, there exists a unique A-linear mapping $A' \otimes_A D \stackrel{\xi}{\to} D'$, such that $\mu = \xi \circ (1 \otimes Id)$. This mapping induces a canonical operation of $A' \otimes_A D$ on A' by $da = \xi(d)a$. This makes it possible two define a Lie bracket on $A' \otimes_A D$ by $[a \otimes d, a' \otimes d'] = aa' \otimes [d,d'] + a(da') \otimes d' - a'(d'a) \otimes d$. Then we have the desired factorization

$$(A,D) \xrightarrow{\varphi,1\otimes Id} (A', A' \otimes_A D) \xrightarrow{Id,\xi} (A',D').$$

A D-morphism is said to be **pure**, if $\xi = Id$ in the above decomposition. By the transitivity of base change, D-rings with pure D-morphisms form a category.

Remark 1.1. Consider the D-ring $(k[x,y],(d_x,d_y))$. Then interchanging x and y resp. d_x and d_y gives a D-automorphism φ of $k[x,y]$. We remark that this would not be the case in differential algebra, because the derivations d_x and d_y are restricted to remain fixed. Nevertheless, φ is not a $k[x,y]$-morphism of D-algebras (see below).

1.2.3 D-ideals, D-A-modules and D-A-algebras

A **D-ideal** of (A, D) is an ideal, stable under D. We denote by $[\Sigma]$ the D-ideal generated by a subset Σ of A. If I is such a D-ideal, then A/I has a canonical **quotient D-ring** structure. If S is a multiplicatively stable subset, we each derivation $d \in D$ naturally gives rise to a derivation on $S^{-1}A$ by $d(a/s) = (da/s) - (a/s^2)$. Therefore, $S^{-1}A$ has a canonical D-ring structure and is called a **local D-ring** of A. We recall that $A \to S^{-1}A$ is injective if and only if S contains no zero divisors. The **total D-ring of fractions** is the D-ring $Q(A) = S^{-1}A$, where S is the set of non zero-divisors. In particular, $Q(A)$ is the **quotient D-field**, if A is entire.

A **D-A-module** or **D-module** over A is an A-module M, such that each derivation $d \in D$ gives rise to a derivation $\hat{d}$ on M, satisfying $\hat{d}(ax) = (da)x + a\hat{d}x$ and $\widehat{[d_1, d_2]}x = \hat{d}_1\hat{d}_2 x - \hat{d}_2\hat{d}_1 x$, for $a \in A$, $d, d_1, d_2 \in D$ and $x \in M$. A **morphism of D-modules** over A is an A-linear mapping, which commutes with the derivations of D.

A **D-A-algebra** or **D-algebra** over A is a D-A-module, which is an A-algebra B, such that $\hat{d}(xy) = x\hat{d}y + (\hat{d}x)y$, for each $x, y \in B$. We remark that (B, D_B) is a D-ring in this case (assuming that B has a unit), where $D_B = B \otimes_A D_A$ acts naturally on B by $(x \otimes d)y = xdy$. We have a canonical D-morphism of (A, D_A) into (B, D_B). Inversely, given such a morphism, we can consider B as a D-A-algebra in a natural way. A **morphism of D-A-algebras** is a morphism of A-algebras, which commutes with the derivations of D.

1.2.4 D-operator algebras

Let (A, D) be a finite dimensional Ritt D-ring. One can naturally associate the **free linear D-operator algebra** $\Omega = A[D]$ to (A, D): this is the free associative A-algebra, generated by A and D, subject to the relations

$$\begin{aligned} a \cdot_\Omega d &= ad; \\ d \cdot_\Omega a &= da; \\ d_1 \cdot_\Omega d_2 - d_2 \cdot_\Omega d_1 &= [d_1, d_2]. \end{aligned}$$

We also define $\Omega_0 = A$ and $\Omega_{r+1} = \Omega_r \cup D\Omega_r$, for each $r \in \mathbb{N}$. These sets are subsets of Ω, with $\Omega = \bigcup_{r \in \mathbb{N}} \Omega_r$. If $\omega \in \Omega$, we define its **order** to be the smallest r, with $\omega \in \Omega_r$.

Proposition 1.1. *Let $d_1, \cdots, d_r$ be in D. Then $d_{\sigma(1)} \cdots d_{\sigma(r)} - d_1 \cdots d_r$ has order strictly inferior to r, for any permutation σ.*

Proof. It suffices to prove this, in the case when σ is a transposition of two subsequent indices i and $i+1$. In that case, we have

$$d_1 \cdots d_{i+1} d_i \cdots d_n - d_1 \cdots d_i d_{i+1} \cdots d_n = d_1 \cdots [d_{i+1}, d_i] \cdots d_n,$$

which has order at most $n-1$. $\square$

Operators of the form $d_1 \cdots d_r$ are called **words**. The word operator $d_{\sigma(1)} \cdots d_{\sigma(r)}$ is said to be a **shuffle** of the word operator $d_1 \cdots d_r$. Suppose that we have fixed generators or a basis $d_1, \cdots, d_n$ for D. Then we denote $\Theta = \{d_1^{\alpha_1} \cdots d_n^{\alpha_n} | \alpha_1, \cdots, \alpha_n \in \mathbb{N}\}$ and $\Theta_r = \{d_1^{\alpha_1} \cdots d_n^{\alpha_n} | \alpha_1 + \cdots + \alpha_n \leqslant r\}$, for each r. Then we have

Proposition 1.2. *The set Θ (resp. Θ_r) generates Ω (resp. Ω_r) as an A-module. It even forms a basis, if $d_1, \cdots, d_n$ form a basis of D.*

Proof. Let us show by induction over r that Θ_r generates Ω_r as an A-module. This is clear for $r = 0$. Assume that Θ_{r-1} generates Ω_{r-1}. By linearity, it suffices to show that $d_i d_1^{\alpha_1} \cdots d_n^{\alpha_n} \in (\Theta_r)$, for each i and $d_1^{\alpha_1} \cdots d_n^{\alpha_n} \in \Theta_{r-1}$. By the previous proposition, we have $d_i d_1^{\alpha_1} \cdots d_i^{\alpha_i} \cdots d_n^{\alpha_n} - d_1^{\alpha_1} \cdots d_i^{\alpha_i+1} \cdots d_n^{\alpha_n} + \omega$, with $\omega \in \Omega_{r-1}$. This completes the induction. As $\Omega = \bigcup_{r \in \mathbb{N}} \Omega_r$ and $\Theta = \bigcup_{r \in \mathbb{N}} \Theta_r$, this implies that Ω is generated by Θ.

Suppose now that $d_1, \cdots, d_n$ form a basis for D. The free A-module Ω' generated by Θ, can naturally be given the structure of an associative A-algebra, and it is easily checked that this algebra satisfies the universal property of Ω. Hence, Ω' is isomorphic to Ω. Therefore, Θ is linearly independent over A, and so is Θ_r, for each r. $\square$

1.2.5 Geometric interpretation of D-rings

The concept of D-rings has a strong geometric appeal: we can interpret A as the space of functions on a manifold and D as its tangent bundle. In order to let things correspond properly, assume that A is entire and that D finitely generated by $d_1, \cdots, d_n$. Then we remark that D is locally trivial. Indeed, whenever we have a relation $a_1 d_1 + \cdots + a_i d_i = 0$, with $a_i \neq 0$, then D is generated by $\{d_1, \cdots, d_n\} \backslash \{d_i\}$, when localizing with respect to the multiplicative subgroup generated by a_i. After a finite number of such localizations, the tangent bundle becomes trivial.

Now the analogy can be carried out further. Finitely generated A-modules (which are locally trivial, by the above argument) correspond to vector bundles. For example, we have the cotangent space $D^* = Lin_A(D, A)$, the tensor bundles

$$D \otimes_A \overset{n \text{ times}}{\cdots} \otimes_A D \otimes_A D^* \otimes_A \overset{m \text{ times}}{\cdots} \otimes_A D^*,$$

etc. Other geometric structures can be imposed on A such as metrics (which are just elements of $D^* \otimes_A D^*$), connections (which are $\mathbb{Z}$-bilinear maps from $D \times D$ into D, such that

$$\begin{aligned} \nabla_{ad} d' &= a \nabla_d d'; \\ \nabla_d (ad') &= (da) d' + a \nabla_d d', \end{aligned}$$

and, optionally, $\nabla_d d' - \nabla_{d'} d = [d, d']$), etc.

Many differential geometric properties admit straightforward algebraic analogues. This observation, combined with the results of subsequent sections, makes it possible to perform many differential geometrical computations automatically.

1.3 D-rings with initial conditions

In this section we will algebrize the notion of a system of partial differential equations with boundary conditions. In section 1.3.1, we first give a very general definition, with arbitrary partial differential equations and partially specified boundary conditions. In section 1.3.2, and all what follows, we will restrict ourselves to initial conditions in a point.

1.3.1 D-boundary value problems

A **D-boundary value problem** is a chain of triplets $(A_n, J_n, I_n), \cdots, (A_1, J_1, I_1)$, where the J_i's are D-ideals of the D-rings A_i, where the I_i's are ideals of A_i/J_i and where $A_{i-1} = (A_i/J_i)_{|I_i}$, for each $2 \leqslant i \leqslant n$. Denote $A_0 = (A_1/J_1)_{|I_1}$. We have canonical mappings

$$A_n \to A_n/J_n \to A_{n-1} \to \cdots \to A_1 \to A_1/J_1 \to A_0.$$

The composite of these mappings is denoted by ε and it is called the **evaluation mapping**. We define an equivalence relation $\sim$ on A_n by

$$a \sim b \Leftrightarrow \forall \theta \in \Theta_{A_n} \quad \varepsilon(\theta(a)) = \varepsilon(\theta(b)),$$

for all a and b in A_n.

Remark 1.2. This definition of equivalence may appear non natural at a first time, because of the example $f = e^{-1/x^2}$. However, f can not be specified in $x = 0$, because $1/x^2$ would not be defined. In fact, the theory of D-rings with initial conditions somehow generalizes complex function theory, where a function is also determined by the values of its iterated derivatives in a point.

The zero-equivalent elements form an ideal, which is easily checked to be a D-ideal. If this ideal is non zero, we say that the D-boundary value problem is **non reduced**. In that case we can transform the problem into a **reduced** D-boundary value problem $(A'_n, J'_n, I'_n), \cdots, (A'_1, J'_1, I'_1)$, with $A'_i = A_i/\sim$, $J'_i = J_i \otimes A'_i$ and $I'_i = I_i \otimes (A'_i/J'_i)$, for all i. If I_1 is a maximal ideal, then A_0 is a field and the D-boundary value problem is said to be **completely specified**.

Example 1.5. Suppose that we wish to represent $f = e^{x+y}$ as a function which is equal to e^y, for $x = 0$, and which satisfies the differential equation $f_x = f$. We take $A_2 = k[x,y]\{f\}$, $J_2 = [f_x - f]$ and $I_2 = (x)$. Then $A_1 \cong k[y]\{f_{|x}\}$ and we take $J_1 = [(f_{|x})_y - f_{|x}]$ and $I_1 = (x, f_{|x} - 1)$. We remark that f can also be specified by two partial differential equations and initial conditions in a point (see the next example).

1.3.2 D-systems

In the rest of this chapter, we will restrict our attention to D-boundary value problems, with $n = 1$, $J_1 = 0$ and where I_1 is maximal. This leads to the notion of a **D-system**, which is a pair $((A, D), \mathfrak{m})$, where (A, D) is a D-ring and $\mathfrak{m}$ a maximal ideal of A. Again, we often write A instead of $((A, D), \mathfrak{m})$. D-systems correspond to D-rings with initial conditions in a point. We have an evaluation mapping $A \to A/\mathfrak{m}$. A morphism of a D-system $((A, D_A), \mathfrak{m}_A)$ into a D-system $((B, D_B), \mathfrak{m}_B)$ is a morphism of D-rings $(A, D_A) \to (B, D_B)$, which commutes with the evaluation mappings. This means that $\mathfrak{m}_A$ is the inverse image of $\mathfrak{m}_B$.

Example 1.6. A D-system in which we can represent the function $f = e^{x+y}$ is

$$(k[x,y]\{f\}/[f_x - f, f_y - f], (x, y, f - 1)),$$

with the usual partial derivations d_x and d_y on $k[x, y]$. Indeed, f is determined by the equations $f_x = f_y = f$ and the initial condition $f(0, 0) = 1$. To represent $g = e^{xe^{x+y}}$, we build a tower on this D-system. Indeed, it suffices to consider the D-supersystem

$$(k[x,y]\{f,g\}/[f_x - f, f_y - f, g_x - f - xf_x, g_y - xf_y], (x, y, f - 1, g - 1)).$$

Example 1.7. An example of a non reduced system is $k[x]\{f, g\}/[f_x - f, g_x - g], (x, f - 1, g - 1)$. Indeed, $f \neq g$ are formally different in $k[x]\{f, g\}/[f_x - f, g_x - g]$, but they both represent the function e^x, so that $f \sim g$.

Example 1.8. Consider the D-system $((k[x, y]/(xy), (xd_x, yd_y)), (x - 1, y))$. A polynomial $P(x, y) = c + xP_1(x) + yP_2(y)$ is zero-equivalent, iff $\varepsilon(\theta(P)) = 0$, for any linear differential operator θ. Now $\varepsilon(yd_yQ) = 0$, for any Q, so that $P \sim 0 \Leftrightarrow x = P_1 = 0$. This means that the behaviour of P on the y-axis is irrelevant for its zero-equivalence. This should not surprise, since the initial point does not lie on the y-axis.

More strikingly, if we took (x, y) as our initial condition, then all polynomials vanishing in 0 would even have been zero-equivalent. This comes from the fact that 0 is a singular point. The same holds true, if we consider $((k[x, y]/(x^2 - y^3), (3y^2d_x + 2xd_y)), (x, y))$.

Proposition 1.3. *Let $((A, D), \mathfrak{m})$ be a D-system, such that $A/\mathfrak{m}$ has characteristic zero. Then $A/{\sim}$ is an entire ring.*

Proof. Suppose that $xy \sim 0$, but $x \not\sim 0$ and $y \not\sim 0$. Let θ and θ' be linear differential operators, of minimal orders k and l, such that $\varepsilon(\theta x) \neq 0$ and $\varepsilon(\theta' y) \neq 0$. Thus, for any $\xi \in \Theta_{k-1}$ and $\xi' \in \Theta_{l-1}$, we have $\varepsilon(\xi x) = \varepsilon(\xi' y) = 0$. As $d_1 \cdots d_k - d_{\sigma(1)} \cdots d_{\sigma(k)}$ has order $< k$, for any derivations $d_1, \cdots, d_k$ and any permutation σ, we have $\varepsilon(d_1 \cdots d_k x) = \varepsilon(d_{\sigma(1)} \cdots d_{\sigma(k)} x)$. Similarly, $\varepsilon(d_1 \cdots d_l y) = \varepsilon(d_{\sigma(1)} \cdots d_{\sigma(l)} y)$.

Let us fix some well ordering $\leqslant$ on D. This ordering induces well orderings on the $\mathcal{M}_p(D)$'s, the sets of multisets of p elements of D. More precisely, we order the elements of multisets in increasing order and take the lexicographical orderings. We also have a well ordering on $\mathcal{M}(D) = \amalg_{p \in \mathbb{N}} \mathcal{M}_p(D)$, by ordering first on size and then using the above ordering on each component. We remark that the union operation is compatible with this ordering, so that $\mathcal{M}(D)$ is an ordered commutative monoid.

Now take $\{d_1, \cdots, d_k\} \in \mathcal{M}_k(D)$ and $\{d_{k+1}, \cdots, d_{k+l}\} \in \mathcal{M}_l(D)$ minimal, such that $\varepsilon(d_1 \cdots d_k x) \neq 0$ and $\varepsilon(d_{k+1} \cdots d_{k+l} y) \neq 0$. Then

$$\varepsilon(d_1 \cdots d_{k+l}(xy)) = \sum_{\{i_1, \cdots, i_k\} \amalg \{j_1, \cdots, j_l\} = \{1, \cdots, k+l\}} \varepsilon(d_{i_1} \cdots d_{i_k} x) \varepsilon(d_{j_1} \cdots d_{j_l} y) = 0.$$

Now if $\{d_{i_1}, \cdots, d_{i_k}\} \neq \{d_1, \cdots, d_k\}$ as a multiset, then either $\{d_{i_1}, \cdots, d_{i_k}\} < \{d_1, \cdots, d_k\}$, or $\{d_{j_1}, \cdots, d_{j_l}\} < \{d_{k+1}, \cdots, d_{k+l}\}$, because of the compatibility of the union with the ordering. Therefore, either $\varepsilon(d_{i_1} \cdots d_{i_k} x) = 0$ or $\varepsilon(d_{j_1} \cdots d_{j_l} y) = 0$ from the minimality hypothesis. We conclude that

$$\varepsilon(d_1 \cdots d_{k+l}(xy)) = m \varepsilon(d_1 \cdots d_k x) \varepsilon(d_{k+1} \cdots d_{k+l} y) = 0,$$

for some integer $m > 0$. This yields a contradiction, since $m \neq 0$ in $A/\mathfrak{m}$. □

We can perform different constructions on a D-system $((A, D), \mathfrak{m})$. First, we can naturally associate the **reduced D-system** $((A/{\sim}, D/{\sim}), \mathfrak{m}/{\sim})$ to it, where, denoting by $\mathfrak{z}$ the D-ideal of zero-equivalent elements, $D/{\sim} = D/\mathfrak{z}D$ and $\mathfrak{m}/{\sim} = \mathfrak{m}/\mathfrak{z}\mathfrak{m}$, with $A/\mathfrak{z} \cong A/{\sim}$.

Secondly, we can associate the **local D-system** $((A_\mathfrak{m}, D_\mathfrak{m}), \mathfrak{m}_\mathfrak{m})$ to it. Here $M_\mathfrak{m}$ denotes the localization of any A-module or ideal M w.r.t. $\mathfrak{m}$. We say that $A_\mathfrak{m}/{\sim}$ is the local ring of **functions at** $\mathfrak{m}$.

Finally, if $I \subseteq \mathfrak{m}$, we have the **restriction of domain** $((A_{|I}, D_{|I}), \mathfrak{m}_{|I})$ of $((A, D), \mathfrak{m})$ w.r.t. I, where $\mathfrak{m}_{|I} = \mathfrak{m}/I\mathfrak{m}$. The next propositions show how these constructions are related.

Proposition 1.4. *Let $((A, D), \mathfrak{m})$ be a D-system. Then $A_\mathfrak{m}/{\sim} \cong (A/{\sim})_{\mathfrak{m}/\sim}$ as D-systems.*

Proof. We claim that the mapping from $A_\mathfrak{m}/{\sim}$ into $(A/{\sim})_{\mathfrak{m}/\sim}$ defined by $\overline{a/s} \mapsto \overline{a}/\overline{s}$ is well defined and bijective. Indeed, $\overline{a/s} = 0$ is equivalent to saying that $\varepsilon(\theta(a/s)) = 0$, for any $\theta \in \Theta_{A_\mathfrak{m}}$. By induction over the order of θ, this is equivalent to $\varepsilon(\theta(a)) = 0$ for each $\theta \in \Theta_{A_\mathfrak{m}}$, since $\varepsilon(s) \neq 0$. Hence, $\overline{a/s} = 0 \Leftrightarrow \overline{a} = 0$. Next,

$\overline{a}/\overline{s} = 0$ is equivalent to the existence of an s', with $\overline{s'}\overline{a} = 0$. By a similar argument, one shows that this is also equivalent to $\overline{a} = 0$. □

Proposition 1.5. *Let $I \subseteq \mathfrak{m}$ be a finitely generated ideal of a D-system $((A, D), \mathfrak{m})$. Then $(A_{\mathfrak{m}})_{|I_{\mathfrak{m}}} \cong (A_{|I})_{\mathfrak{m}_{|I}}$ as D-systems.*

Proof. Let M be an A-module. Then we have a natural isomorphism between $M_{\mathfrak{m}}/I_{\mathfrak{m}}M_{\mathfrak{m}}$ and $(M/IM)_{\mathfrak{m}_{|I}}$, which sends $\overline{x/s}$ to $\overline{x}/\overline{s}$. Therefore, it suffices to check that $\{\overline{d}/\overline{s} | dI \subseteq I\} = \{\overline{d/s} | (d/s)I_{\mathfrak{m}} \subseteq I_{\mathfrak{m}}\}$, when identifying $D_{\mathfrak{m}}/I_{\mathfrak{m}}D_{\mathfrak{m}}$ with $(D/ID)_{\mathfrak{m}_{|I}}$. If $dI \subseteq I$, then clearly $(d/s)I_{\mathfrak{m}} \subseteq I_{\mathfrak{m}}$. Inversely, suppose that $(d/s)I_{\mathfrak{m}} \subseteq I_{\mathfrak{m}}$. If $a_1, \cdots, a_n$ are generators for I, then we have $s_i((d/s)a_i) \in I$, for certain s_i's and all i. This means that $d'I \subseteq I$, where $d' = s_1 \cdots s_n d$, and $d/s = d'/(ss_1 \cdots s_n)$. □

Example 1.9. The restriction of domain operator does not satisfy any simple commutation rule with the equivalence operator: take $A = K[x, y]$, $D = (d_x)$, $\mathfrak{m} = (x, y)$ and $I = (xy)$. Then $y \sim 0$, so that $A/\!\sim\, \cong K[x]$ and $I/\!\sim\, = 0$. However, $Pd_x(xy) = Py$, so that the set of derivations leaving invariant I is generated by xd_x. Thus, all elements of $A_{|I}$ are zero-equivalent.

Example 1.10. The restriction of domain operator does not necessarily satisfy $A_{|I|J_{|I}} \cong A_{|J}$ for $I \subseteq J$. A counterexample is given by $A = K[x, y]$, $D_A = (d_x, d_y)$, $I = (xy)$ and $J = (x)$. Similarly, we do not necessarily have $((A/\sim)_{|I/\sim}/\sim)_{|(J/\sim)_{|I/\sim}/\sim} \cong (A/\sim)_{|J/\sim}$.

1.4 Zero-equivalence algorithms

In this and the next section, we shall borrow without further mention some concepts of the theory of Groebner bases (see for instance [CLO 92]). The sections 1.4.1 and 1.4.2 are the result of a collaboration between A. Péladan-Germa and the author (see also [PV 96]).

Let $\mathfrak{C}$ be an effective field — i.e. we have algorithms for performing the field operations of $\mathfrak{C}$ and we have an effective zero-test. A **simple effective D-system** over $\mathfrak{C}$ is a couple $((\mathfrak{A}, \mathfrak{D}), \mathfrak{m})$ which satisfies the following conditions:

- **ES1.** $\mathfrak{A} = \mathfrak{C}[f_1, \cdots, f_k]/\mathfrak{i}$ and we have a Groebner basis $G_{\mathfrak{A}}$ for the ideal $\mathfrak{i}$.
- **ES2.** $\mathfrak{D}$ is a free $\mathfrak{A}$-module with basis $d_1, \cdots, d_n$.
- **ES3.** $(\mathfrak{A}, \mathfrak{D})$ is an effective D-ring — i.e. $\mathfrak{A}$, the action of $\mathfrak{D}$ on $\mathfrak{A}$ and the Lie bracket on $\mathfrak{D}$ are effective.
- **ES4.** $\mathfrak{m}$ is a maximal ideal of $\mathfrak{A}$, such that $\mathfrak{A}/\mathfrak{m} \cong \mathfrak{C}$, and the evaluation mapping $\varepsilon : \mathfrak{A} \to \mathfrak{C}$ is effective.

In the remainder of this section, $((\mathfrak{A}, \mathfrak{D}), \mathfrak{m})$ is a D-system which satisfies the above requirements.

The aim of this section is to show how to compute with special functions in $\mathfrak{A}_{\mathfrak{m}}/\sim$. Such functions are redundantly represented by rational fractions in $\mathfrak{C}[f_1, \cdots, f_k]$, whose denominators do not evaluate to zero, whence the ring operations in $\mathfrak{A}/\sim$ can be implemented in a straightforward way. However, for the equality test, we need a zero-equivalence test in $\mathfrak{A}$. In this section, we shall provide several of such zero-equivalence tests.

1.4.1 A naive zero-equivalence algorithm

In what follows, `Groebner-basis` stands for an algorithm to compute Groebner basis in $\mathfrak{C}[f_1, \cdots, f_k]$. Given a polynomial $P \in \mathfrak{C}[f_1, \cdots, f_k]$, we will abusively denote its natural projection on $\mathfrak{A}$ by P as well. The following zero-equivalence algorithm generalizes the first algorithm from [Sh 89] to test zero-equivalence in the context of ordinary differential equations over $\mathbb{Q}$:

Algorithm `zero_equivalence_1`(P).
INPUT: A polynomial $P \in \mathfrak{C}[f_1, \cdots, f_k]$.
OUTPUT: The result of the zero-equivalence test for P.

if $\varepsilon(P) \neq 0$ **then return false**
$G :=$ `Groebner-basis`$(G_{\mathfrak{A}} \cup \{P\})$
while $\exists i\, \exists Q \in G \quad d_i Q \mod G \neq 0$ **do**
  if $\varepsilon(d_i Q) \neq 0$ **then return false**
  $G :=$ `Groebner-basis`$(G \cup \{d_i Q\})$
return true

Proposition 1.6. *The algorithm* `zero_equivalence_1` *is correct and terminates.*

Proof. Let us first prove the correctness. It is clear that if the algorithm returns false, then P is not zero-equivalent. If the algorithm returns true, then let G be the Groebner basis at the end of the algorithm. We have $(d_i Q) \in (G)$, for each $1 \leqslant i \leqslant k, Q \in G$. Hence, (G) is stable by Δ, and $\varepsilon(P) = 0$ for each $P \in (G)$. Consequently, all elements of (G) — which contains P — are zero-equivalent.

As to the termination of `zero_equivalence_1`, the heads (see also section 1.6 for this terminology) of the polynomials in the successive values of G form a strictly increasing chain of ideals. Now the termination follows from the Noetherianity of polynomial rings. □

Remark 1.3. A slight modification of the algorithm allows us to exploit previous computations: since we are interested in $\mathfrak{A}/\sim$ rather than $\mathfrak{A}$ itself, we may turn $G_{\mathfrak{A}}$ into a global variable. Then setting $G^{glob} := G$ just before we return true in `zero_equivalence_1` has the effect of remembering all non trivial relations we find between the f_i's in $\mathfrak{A}/\sim$.

Remark 1.4. It is also possible to test several polynomials $P_1, \cdots, P_p$ for zero-equivalence at the same time. This is done by checking first whether they evaluate to zero and then replacing the line $G :=$ `Groebner-basis`$(G_{\mathfrak{A}} \cup \{P\})$ by $G :=$ `Groebner-basis`$(G_{\mathfrak{A}} \cup \{P_1, \cdots, P_p\})$.

Remark 1.5. The algorithm naturally extends to the case when the initial conditions depend on parameters via the automatic case separation strategy (see [VdH 97]). More precisely, we may take $\mathfrak{C}$ to be a parameterized constant field $\mathfrak{C} = \mathfrak{K}(\lambda_1, \cdots, \lambda_p)$ over an effective field $\mathfrak{K}$. This means that the elements in $\mathfrak{C}$ are rational fractions in a finite number of parameters $\lambda_1, \cdots, \lambda_p$. These parameters are subject to polynomial constraints, which are either equations or inequations. The consistency of such systems of constraints can be checked by Groebner basis techniques. Moreover, no infinite loops can arise from the parameterized Groebner basis computations in `zero_equivalence_1` (see [GoDi 94], for instance).

1.4.2 An optimized zero-equivalence algorithm

In the naive zero-equivalence algorithm, we do not exploit the local character of our problem from an algebraic point of view. Now in section 1.6, we show that Buchberger's algorithm can be generalized to local rings, although the computed pseudo-Groebner bases do not possess all of the nice properties of usual Groebner bases. Nevertheless, this local pseudo-Buchberger algorithm can be used instead of the usual one in `zero_equivalence_1`, yielding the following optimized zero-equivalence test:

Algorithm `zero_equivalence_2`(P).
INPUT: A polynomial $P \in \mathfrak{C}[f_1, \cdots, f_k]$.
OUTPUT: The result of the zero-equivalence test for P.

if $\varepsilon(P) \neq 0$ **then return false**
$G :=$ `Pseudo-Groebner-basis`$(G_{\mathfrak{A}} \cup \{P\})$
while $\exists i\ \exists Q \in G \quad Red(d_i Q, G) \neq 0$ **do**
  if $\varepsilon(d_i Q) \neq 0$ **then return false**
  $G :=$ `Pseudo-Groebner-basis`$(G \cup \{d_i Q\})$
return true

Proposition 1.7. *The algorithm* `zero_equivalence_2` *is correct and terminates.*

Proof. The termination is proved in a similar way as before. As to the correctness, it is again clear that if the algorithm returns false, then P is not zero-equivalent. If the algorithm returns true, then let G be the pseudo-Groebner basis at the end of the algorithm. We have $Red(d_i Q, G) = 0$, for each $1 \leqslant i \leqslant k, Q \in G$. In particular, $\Delta G \subseteq (G)_{\mathfrak{A}/\mathfrak{S}}$, where $(G)_{\mathfrak{A}/\mathfrak{S}}$ denotes the ideal in $\mathfrak{A}/\mathfrak{S}$ generated by G. This implies that $(G)_{\mathfrak{A}/\mathfrak{S}}$ is stable by Δ. Since all elements of G evaluate to zero, so do all elements of $(G)_{\mathfrak{A}/\mathfrak{S}}$. Hence all elements of $(G)_{\mathfrak{A}/\mathfrak{S}}$ — which contains P — are zero-equivalent. □

The interest of this local pseudo-Buchberger algorithm is illustrated on the following example, proposed by Shackell: let $\mathfrak{A} = \mathfrak{C}[f_1, f_2, f_3, f_4]$, $\mathfrak{D} = \mathfrak{A}d_x$, $d_x f_1 = 1$, $d_x f_2 = f_2$, $d_x f_3 = 2 f_1 f_3$, $d_x f_4 = 2 f_1 f_4$, $\varepsilon(f_1) = 0$, $\varepsilon(f_2) = \varepsilon(f_3) = \varepsilon(f_4) = 1$. Then the polynomial $P = (f_1^M + f_2)(f_3 - f_4)$ is zero-equivalent since $f_3 - f_4$ is. However, the naive algorithm needs $O(M)$ steps to conclude this, whereas the new one terminates after one step: $d_x P$ is pseudo-reduced to zero by P.

1.4.3 A randomized zero-equivalence algorithm

Often, if we want to determine whether some special function — such as an exp-log function — is zero, then the initial point may be chosen randomly, provided that we avoid singularities. Now the set of points in which a non zero function vanishes, has measure zero. In this section, we show how this observation can be used to speed up the zero-equivalence algorithm, if the initial point may be chosen by the algorithm.

The idea of the algorithm is the following: an initial point is said to be **good**, if all polynomials $P \in \mathfrak{m}$ considered during the computations are actually zero-equivalent. Otherwise, the initial point is said to be **bad**. Under the hypothesis that an initial point is good, we can insert any polynomial which vanishes under evaluation into the Groebner basis $G_{\mathfrak{A}}$. Whenever 1 is in the ideal generated by the Groebner basis G, this means that the initial point is bad, and an exception is raised. This leads to the following algorithm:

Algorithm `zero_equivalence_3`(P).
INPUT: A polynomial $P \in \mathfrak{C}[f_1, \cdots, f_k]$.
OUTPUT: The result of the zero-equivalence test for P. The algorithm aborts whenever a bad initial point was chosen.

if $\varepsilon(P) \neq 0$ **then return false**
$G_{\mathfrak{A}} :=$ `Groebner-basis`$(G_{\mathfrak{A}} \cup \{P\})$
while $\exists i\, \exists Q \in G_{\mathfrak{A}}\;\; d_i Q \mod G_{\mathfrak{A}} \neq 0$ **do**
  if $\varepsilon(d_i Q) \neq 0$ **then raise** "bad initial point"
  $G :=$ `Groebner-basis`$(G_{\mathfrak{A}} \cup \{d_i Q\})$
return true

Remark 1.6. The Groebner basis computations may also be speeded up by inserting each polynomial $P \in \mathfrak{M}$ we encounter during these computations into $G_{\mathfrak{A}}$.

Let us now sketch in which circumstance the above algorithm applies. Assume that we are given an analytic function f defined on some Riemann surface. Assume also that we are given a sequence of points $z_1, z_2, \cdots$ in which f is defined, such that $\{z_1, z_2, \cdots\}$ is dense in some open set U. Assume finally that to each initial point z_i corresponds a simple effective D-system $((\mathfrak{A}, \mathfrak{D}), \mathfrak{m}_i)$, which specifies f in z_i (notice that $\mathfrak{A}$ and $\mathfrak{D}$ do not depend on i). Then we claim that we can test the zero-equivalence of f by the above algorithm, by running it successively in $z_1, z_2, \cdots$ until we have found a good initial point.

First, the zero-equivalence algorithm can be aborted due to the vanishing of only a finite number of non zero functions at the initial point. Now at least one of the parts of a finite partition of U is also dense in some open subset (the measure of the closure of one of the parts has to be non zero). Therefore, if there were no good initial point in the sequence $z_1, z_2, \cdots$, there would exist an open subset on which a non zero function would vanish. This is not possible.

1.4.4 Other algorithms and conclusion

A very nice zero-equivalence algorithm — quite different in spirit from those considered in the previous sections — has been given by Péladan-Germa in [Pél 95] in the context of commutating derivations $d_1, \cdots, d_k$. In a nutshell, the idea is to consider both the initial points and the initial conditions to be *variable*. Then algebraic conditions on the initial point and the initial conditions are given under which a *fixed* function in $\mathfrak{A}$ is zero-equivalent. These algebraic conditions are obtained via Ritt's classical differential elimination theory. Using the generalization of this theory to the context of D-rings in chapter 2, we think that Péladan-Germa's should generalize to our setting.

Another advantage of Péladan-Germa's approach is that her algorithm partially generalizes to the case of more general boundary value problems, where the initial conditions are no longer specified in a point (see [Pél 96]). However, in its full generality, this algorithm crucially depends on Kolchin's problem, which will be discussed in section 2.8. Nevertheless, the algorithm can be applied in several non trivial and interesting cases.

It should be noticed that certain more general boundary value problems can also be treated by the approach of this section. This is for instance the case if the quotient field of $\mathfrak{A}/\sim$ is taken as the constant field w.r.t. a new derivation. We also notice that the algorithms from this section apply in characteristic p, while Péladan-Germa's approach fails in this case.

Another question which can be raised is the following: since the zero-equivalence elements in $\mathfrak{A}$ form an ideal, there exists an ideal $\mathfrak{z}$ with $\mathfrak{A}/\sim = \mathfrak{C}[f_1, \cdots, f_k]/\mathfrak{z}$. Now can we compute a Groebner basis for $\mathfrak{z}$? This question is very hard in general, and algorithms are only known in the case of exp-log functions, using the Risch structure theorem (see [Ris 75]), and in a few other cases (see [Ch 93], [CC 85]).

After all the theoretical considerations made up till here, the reader might wonder how to implement an efficient zero-equivalence algorithm. For this purpose, several remarks of a more heuristic nature should be made.

1. In the zero-equivalence problem the hard thing is to *prove* that a function is zero-equivalent, whenever this is the case. On the contrary, it is usually easy to prove that a function is not zero-equivalent, either by evaluating some terms of the power series expansion, or by choosing a suitable initial point (when we are allowed to do so).

2. Following the previous remark, two types of zero-equivalence problems should be distinguished: those in which the initial point is fixed, and those in which the initial point may be chosen by the algorithm. In the first case, only power series expansions can be used to prove that a function is not zero-equivalent — and many terms may need be evaluated. In the second case, we would rather search for a point in which the function does not vanish; such a point is chosen at random with probability 1.

3. Many different (partial) methods may be used to prove or disprove a function to be zero-equivalent. A good final algorithm should start with cheap tests for zero-equivalence and non zero-equivalence and proceed with the more expensive ones, whenever these tests fail to decide. In particular, the time spent on tries to prove zero-equivalence should be proportional to the time spent on tries to disprove zero-equivalence.

4. In some circumstances, it is not reasonable to demand an immediate answer to a zero-equivalence quest, but we rather postpone a decision to a later moment and temporarily perform a case separation (see [VdH 97]).

5. In relation to 4. it should be noticed that the efficiency of successive zero-equivalence tests may crucially depend on the order in which we perform them (when applying remark 1.3).

1.5 Implicit functions

1.5.1 Inversion of regular matrices

Let $(\mathfrak{A}, \mathfrak{m})$ be a simple effective D-system and let $(M_{i,j})$ be a matrix with $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant n$ and $p \leqslant n$. We say that M is **regular matrix**, if its evaluation

$$\varepsilon(M) = \begin{pmatrix} \varepsilon(M_{1,1}) & \cdots & \varepsilon(M_{1,n}) \\ \vdots & & \vdots \\ \varepsilon(M_{p,1}) & \cdots & \varepsilon(M_{p,n}). \end{pmatrix}$$

has rank p. Given such a matrix, we will now show how to compute an invertible square matrix U with entries in $\mathfrak{A}_\mathfrak{m}$, such that

$$MU = I_{n,p} = \begin{pmatrix} 1 & \cdots & 0 & 0 & \ldots & 0 \\ \vdots & 1 & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & 0 & \ldots & 0 \end{pmatrix} \tag{1.1}$$

in $\mathfrak{A}_\mathfrak{m}/\sim$. The algorithm proceeds by swapping rows and columns in a straightforward manner:

Algorithm $\texttt{invert}(M)$
INPUT: A regular n by p matrix M with entries in $\mathfrak{A}$.
OUTPUT: An invertible n by n matrix U with entries in $\mathfrak{A}_\mathfrak{m}$ satisfying (1.1).

$U := Id$
for $i := 1$ **to** p **do**
  let $j \geqslant i$ **be** such that $\varepsilon(M_{i,j}) \neq 0$
  $\texttt{swap}(M_{i,\cdot}, M_{j,\cdot})$
  $\texttt{swap}(U_{i,\cdot}, U_{j,\cdot})$
  $M_{i,\cdot} := (d_i g_i)^{-1} M_{i,\cdot}$
  $U_{i,\cdot} := (d_i g_i)^{-1} U_{i,\cdot}$
  for $j \in \{1, \cdots, n\} \backslash \{i\}$ **do**
    $M_{\cdot,j} := M_{\cdot,j} - M_{i,j} M_{\cdot,i}$
    $U_{\cdot,j} := U_{\cdot,j} - M_{i,j} U_{\cdot,i}$

1.5.2 Restriction of domain and resolution of implicit equations

Let $(\mathfrak{A}, \mathfrak{m})$ be a simple effective D-system of characteristic zero, such that $\mathfrak{D}_\mathfrak{A}$ admits $d_1, \cdots, d_n$ as a basis. Let $\mathfrak{j} = (g_1, \cdots, g_p)$ be a finitely generated ideal of $\mathfrak{A}$, such that $\varepsilon(g_1) = \cdots = \varepsilon(g_p) = 0$. The **Jacobian matrix** of $g_1, \cdots, g_p$ is defined by

$$J = \begin{pmatrix} d_1 g_1 & \cdots & d_n g_1 \\ \vdots & & \vdots \\ d_1 g_p & \cdots & d_n g_p \end{pmatrix}.$$

We say that the ideal $\mathfrak{j}$ is **regular**, if $\operatorname{rank}(\varepsilon(J)) = p$. Under this assumption, we will now show how to compute a simple effective D-system $(\mathfrak{B}, \mathfrak{n})$, such that

$$\mathfrak{B}_{\mathfrak{n}}/\!\sim \cong (\mathfrak{A}_{\mathfrak{m}}/\!\sim)_{|\mathfrak{j}_{\mathfrak{m}}\not\sim}/\!\sim .$$

We take $\mathfrak{B} = \mathfrak{C}[f_1, \cdots, f_k]/(\mathfrak{i}, \mathfrak{j})$, so that we start by computing a Groebner basis for $(\mathfrak{i}, \mathfrak{j})$. In order to compute a basis for $\mathfrak{D}_{\mathfrak{B}}$, we first compute a matrix U with $JU = I_{n,p}$ by `invert`. Performing the base change

$$\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} := {}^tU \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix},$$

we then reduce the general case to the case when $J = I_{n,p}$. In this case, $d_{p+1}, \cdots, d_n$ leave $\mathfrak{j}$ invariant and it is easily seen that their natural images in $(\mathfrak{A}_{\mathfrak{m}}/\!\sim)_{|\mathfrak{j}_{\mathfrak{m}}\not\sim}/\!\sim$ form a basis for $(\mathfrak{A}_{\mathfrak{m}}/\!\sim)_{|\mathfrak{j}_{\mathfrak{m}}\not\sim}/\!\sim$.

In practice, when we solve the equations $g_1 = \cdots = g_p$, we often want to express the solutions w.r.t. given coordinates $g_{p+1}, \cdots, g_n \in \mathfrak{A}$. In order to make this possible, we need assume that the evaluation

$$\varepsilon(J) = \begin{pmatrix} \varepsilon(d_1 g_1) & \cdots & \varepsilon(d_n g_1) \\ \vdots & & \vdots \\ \varepsilon(d_1 g_n) & \cdots & \varepsilon(d_n g_n). \end{pmatrix}$$

of the Jacobian matrix of $g_1, \cdots, g_n$ is invertible. Now compute a matrix U with $JU = Id$ by `invert`. We again reduce the general case to the case when $J = 1$ via the base change

$$\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} := {}^tU \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}.$$

Then the natural images of $d_{p+1}, \cdots, d_n$ in $\mathfrak{B}_{\mathfrak{n}}/\!\sim$ have the desired property that

$$\begin{pmatrix} d_{p+1} g_{p+1} & \cdots & d_n g_{p+1} \\ \vdots & & \vdots \\ d_{p+1} g_n & \cdots & d_n g_n. \end{pmatrix} = Id.$$

Remark 1.7. As in remark 1.5, the above computations generalize in a straightforward way to the case when the initial conditions depend on parameters, using the automatic case separation strategy (see [VdH 97]).

1.5.3 D-algebraic power series

In this section, all D-systems $(A, \mathfrak{m})$ we consider have characteristic zero; i.e. $A/\mathfrak{m}$ has characteristic zero.

Let $((A, D), \mathfrak{m})$ be a reduced D-system, such that A is a finitely generated algebra over $C = A/\mathfrak{m}$, and D is a free A-module, which is finitely generated by pairwise commuting derivations $\partial/\partial z_1, \cdots, \partial/\partial z_n$. Then A admits a natural differential embedding ν into the ring $C[[z_1, \cdots, z_n]]$ of formal power series by

$$f \mapsto \nu(f) = \sum_{i_1,\cdots,i_n} \frac{1}{i_1! \cdots i_n!} \varepsilon \left(\frac{\partial^{i_1+\cdots+i_n}}{\partial^{i_1} z_1 \cdots \partial^{i_n} z_n} \right) z_1^{i_1} \cdots z_n^{i_n}.$$

A power series of the form $\nu(f)$ (for some D-system $((A, D), \mathfrak{m})$ which satisfies the above hypotheses) is called a **regular D-algebraic power series**.

Remark 1.8. In characteristic $p > 0$, the above embedding does not exist. Actually, we may interpret elements in A as formal Borel transforms of power series in this case.

From our definition, it follows immediately that the regular D-algebraic power series form a local ring, which is stable under the partial derivations, and permutation of coordinates. Moreover, if we are given a regular D-algebraic power series $f \in C[[z_1, \cdots, z_{n+1}]]$, such that $f(0, \cdots, 0) = 0$ and $(\partial f/\partial z_{n+1})(0, \cdots, 0) \neq 0$, then by what has been said in the previous section, there exist derivations $d_1, \cdots, d_{n+1}$, such that the Jacobian matrix of $z_1, \cdots, z_n, f$ is the identity (assuming that $z_1, \cdots, z_n \in A$). It is easily checked that $d_1, \cdots, d_n$ commute for the Lie bracket, whence we have the natural embedding

$$\overline{g} \mapsto \sum_{i_1,\cdots,i_n} \frac{1}{i_1! \cdots i_n!} \varepsilon(d^{i_1} z_1 \cdots d^{i_n} z_n g) z_1^{i_1} \cdots z_n^{i_n}.$$

from $A_{|(f)}/\sim$ into $C[[z_1, \cdots, z_n]]$. This mapping sends f to zero and fixes $z_1, \cdots, z_n$. In other words, the mapping corresponds to the implicit definition of z_{n+1} by $f = 0$. Consequently, the regular D-algebraic power series form a local community (see [VdH 97]).

If $(\mathfrak{A}, \mathfrak{m})$ is a simple effective D-system with a basis of pairwise commuting derivations, the above passage from functions in $\mathfrak{A}_\mathfrak{m}/\sim$ to power series yields an effective way to compute with regular D-algebraic power series over $\mathfrak{C} = \mathfrak{A}/\mathfrak{m}$. In view of the algorithm from the previous section to solve implicit equation, it follows that the set of regular D-algebraic power series over $\mathfrak{C}$ forms an effective local community.

A **regular D-algebraic Laurent series** is a Laurent series f, such that $z_1^{\alpha_1} \cdots z_n^{\alpha_n} f$ is a D-algebraic power series for suitable $\alpha_1, \cdots, \alpha_n \in \mathbb{N}$. Unfortunately, we did not solve the following problem: prove or disprove that if z_i is a power series in $z_1, \cdots, z_n$ and $z_1 f$ is D-algebraic, then so is f. Consequently, we have no proof that the set of D-algebraic Laurent series forms a local community. Nevertheless, we will now define D-algebraic power and Laurent series, which do have the desired property.

Let A be as in the beginning of this section and denote by $\tilde{A}$ the set of those fractions f/s in $Q(A)$, such that there exists a power series g with $\nu(f) = g\nu(s)$. We extend the evaluation mapping on A to $\tilde{A}$ by $\varepsilon(f/s) = g(0, \cdots, 0)$, where $\nu(f) = g\nu(s)$. Clearly, $\tilde{A}$ forms a reduced local D-system over C. The natural inclusion of A into $C[[z_1, \cdots, z_n]]$ also extends to $\tilde{A}$ by $\nu(f/s) = g$, where $\nu(f) = g\nu(s)$. A power series g of the form $\nu(f/s)$ (for some A) is said to be **D-algebraic**. A Laurent series f is said to be **D-algebraic**, if $fz_1^{\alpha_1} \cdots z_n^{\alpha_n}$ is a D-algebraic power series for certain $\alpha_1, \cdots, \alpha_n \in \mathbb{N}$.

Now let $(\mathfrak{A}, \mathfrak{m})$ again be a simple effective D-system with a basis of pairwise commuting derivations. The set $\tilde{\mathfrak{A}} = \widetilde{\mathfrak{A}_\mathfrak{m}/\sim}$ is clearly an effective D-algebra, since it is a subfield of the field of fractions of $\mathfrak{A}_\mathfrak{m}/\sim$. Notice however, that we do not claim that we can test whether a given fraction $f/s \in \mathfrak{A}_\mathfrak{m}/\sim$ is in $\tilde{\mathfrak{A}}$.

Given an element $f/s \in \tilde{\mathfrak{A}}$, we can also compute its evaluation: we first compute a dominant monomial $z_1^{\alpha_1} \cdots z_n^{\alpha_n}$ for $\nu(s)$ by `idm` (see [VdH 97]). Then $\varepsilon(f/s) = [z_1^{\alpha_1} \cdots z_n^{\alpha_n}]f/[z_1^{\alpha_1} \cdots z_n^{\alpha_n}]s$.

Having shown that all D-system operations in $\tilde{\mathfrak{A}}$ can be carried out effectively, the algorithm to solve implicit equations from section 1.5.2 naturally generalizes, if we replace $\mathfrak{A}_\mathfrak{m}/\sim$ by $\tilde{\mathfrak{A}}$. In particular, the sets of D-algebraic power series resp. Laurent series over $\mathfrak{C}$ are both effective local communities.

1.6 A local pseudo-Buchberger algorithm

This section is the result of a collaboration between A. Péladan-Germa and the author (see also [PV 96]).

Let $\mathfrak{A} = \mathfrak{C}[x_1, \ldots, x_n]$ be the ring of polynomials in n indeterminates over an effective field $\mathfrak{C}$ of constants, and $\mathfrak{S}$ be an effective multiplicative subset of $\mathfrak{A}$ — that is, provided with an effective membership test. We present here a method to test whether a given polynomial $P \in \mathfrak{A}$ belongs to the ideal generated by polynomials $Q_1, \ldots, Q_s$ in the quotient ring $\mathfrak{A}/\mathfrak{S}$. We only give a weak membership test in the sense that $P \in (Q_1, \ldots, Q_s)_{\mathfrak{A}/\mathfrak{S}}$, whenever the algorithm returns true. However, in the case of a negative response, P might still be in $(Q_1, \ldots, Q_s)_{\mathfrak{A}/\mathfrak{S}}$. Nevertheless, for the application in section 1.4.2 such a weak membership test is sufficient.

Actually, our algorithm is based on the heuristic idea that the exploitation of local information should accelerate Buchberger's algorithm. Unfortunately, the pseudo-Groebner bases we compute does not have all the theoretical properties of classical Groebner bases. However, up to our knowledge, no complete membership test has been given yet in the case of a general effective multiplicative set $\mathfrak{S}$. Only in some particular cases, Mora's tangent cone algorithm, and A. Logar's algorithms give complete membership tests (see [MPT 92], [Lo 87]).

1.6.1 Pseudo-reduction

Let $\mathfrak{A} = \mathfrak{C}[x_1, \ldots, x_n]$ be the ring of polynomials in n indeterminates over an effective field $\mathfrak{C}$. We use the pure lexicographical order on monomials, with $x_1 < \cdots < x_n$. Let $\mathfrak{S} \supseteq \mathfrak{C}^\star$ be a multiplicative subset of $\mathfrak{C}$ with an effective membership test.

In order to compute "pseudo-bases" of ideals of $\mathfrak{A}/\mathfrak{S}$, we use a classical reduction-completion approach. The keystone of our method lies in the non-classical definitions of the head $H(P)$ and the leading-coefficient $C(P)$ of non-zero polynomials P: they are inspired both by Ritt-Wu's work and Buchberger's terminology.

Each non constant polynomial P in $\mathfrak{A}$ can be written $P = I_P x_P^{d_P} + R_P$, where x_P is the greatest indeterminate involved in P, and d_P the highest order of P with respect to x_P. I_P is usually called the **initial** of P. Now we define $H(P)$ and $C(P)$ for non-zero polynomials:

- if $P \in \mathfrak{S}$ then $H(P) = 1$ and $C(P) = P$;
- if $P \notin \mathfrak{S}$ and $I_P \in \mathfrak{S}$ then $H(P) = x_P^{d_P}$ and $C(P) = I_P$;
- if $P \notin \mathfrak{S}$ and $I_P \notin \mathfrak{S}$ then $H(P) = x_P^{d_P} H(I_P)$ and $C(P) = C(I_P)$.

Example 1.11. Let $\mathfrak{S}$ be the set of polynomials that do not vanish at $x_1 = \ldots = x_n = 0$. If $P = (x_1 + 1)x_2 + x_1$, then $H(P) = x_2$ and $C(P) = x_1 + 1$. Now if $P = ((x_1 + 1)x_2 + x_1)x_3^2 + x_3 x_2$, then $H(P) = x_2 x_3^2$ and $C(P) = x_1 + 1$.

Suppose $Q \neq 0$, $Q \notin \mathfrak{S}$ and $P \neq 0$. We say that P is **reducible** with respect to Q if $H(P)$ is divisible by $H(Q)$. In this case, write $P = UH(Q) + V$, where $U, V \in \mathfrak{A}$, and no monomial appearing in V is divisible by $H(Q)$. P is then **elementary reduced** to $red(P, Q) = C(Q)P - UQ$ by Q. If $Q \in \mathfrak{S}$, then P is reducible with respect to Q and $red(P, Q) = 0$. It can be easily checked, although this is a little technical, that $H(red(P, Q)) < H(P)$ ($H(0) = -\infty$ by convention). Repeating the elementary reduction of P by Q, that is

$$P \rightarrow P_1 = red(P, Q) \rightarrow red(P_1, Q) \rightarrow \cdots,$$

we end up with a polynomial R such that $H(Q)$ does not divide $H(R)$ or $R = 0$. This process stops because the heads of the intermediate polynomials strictly decrease. This polynomial R is called the **reduction** of P by Q and is denoted by $Red(P, Q)$. More generally, we can reduce P by a set E of polynomials by reducing P by $Q \in E$ as long as we can. Although the result R of this procedure is not necessarily unique, we will abusively denote $R = Red(P, E)$. Note that R belongs to the ideal $(P, E)_{\mathfrak{A}/\mathfrak{S}}$ generated by P and E in $\mathfrak{A}/\mathfrak{S}$ and if $R = 0$, then $P \in (E)_{\mathfrak{A}/\mathfrak{S}}$.

Let P, Q be nonzero elements of $\mathfrak{C}[x_1, \ldots, x_n]$. Let i be the highest index such that $C(P)$ and $C(Q)$ are both in $\mathfrak{A}_i = \mathfrak{C}[x_1, \cdots, x_{i-1}]$. We write $P = C_i(P)H_i(P) + R(P)$, where $H_i(P)$ is highest monomial occurring in P, when considered as a polynomial in $x_i, \cdots, x_n$ with coefficients in $\mathfrak{A}_i$. Similarly, we write $Q = C_i(Q)H_i(Q) + R(Q)$. Then the **S-polynomial** of P and Q is defined by

$$SPol(P,Q) := \frac{C_i(Q)H_i(Q)}{\gcd(H_i(P), H_i(Q))}P - \frac{C_i(P)H_i(P)}{\gcd(H_i(P), H_i(Q))}Q.$$

This definition enables us to assert that $H(SPol(P,Q)) < \mathrm{scm}(H(P), H(Q))$. Note also that $Spol(P,Q) \in (P,Q)$ and *a fortiori* $Spol(P,Q) \in (P,Q)_{\mathfrak{A}/\mathfrak{S}}$.

1.6.2 The algorithm

We now apply Buchberger's algorithm (see [CLO 92], [Buch 65]) with our alternative definitions of heads, leading coefficients, reduction, and S-polynomials. We recall hereafter a compact but non optimized version of this algorithm.

Algorithm `Pseudo-Groebner-basis`(E)
INPUT: A finite set E of non zero polynomials in $\mathfrak{A}$.
OUTPUT: A pseudo-Groebner basis G of the ideal generated by E in $\mathfrak{A}/\mathfrak{S}$.

$G := E$
repeat
  $G' := G$
  for each $P \in G'$ **do**
    $P := Red(P, G - \{P\})$
    if $R \neq 0$ **then** $G := G \cup \{R\}$
  for each pair $P \neq Q$ in G' **do**
    $R := Red(SPol(P,Q), G')$
    if $R \neq 0$ **then** $G := G \cup \{R\}$
until $G = G'$

The ideals generated by the heads of the elements of the successive values of G form a strictly increasing sequence of ideals, whence the algorithm terminates. The subsets E and G of $\mathfrak{A}/\mathfrak{S}$ generate the same ideal $I_{\mathfrak{A}/\mathfrak{S}}$. Indeed, we only insert elements that are already in $(E)_{\mathfrak{A}/\mathfrak{S}}$ into G. G is not a Groebner basis, but has the property that if P is in $\mathfrak{A}$ and $Red(P,G) = 0$, then $P \in I_{\mathfrak{A}/\mathfrak{S}}$. The computation of G enables us to quickly extract much information about $I_{\mathfrak{A}/\mathfrak{S}}$, without obtaining a complete description of $I_{\mathfrak{A}/\mathfrak{S}}$. Notice that if G contains a polynomial in $\mathfrak{S}$, then $I_{\mathfrak{A}/\mathfrak{S}}$ is trivial, and every polynomial in $\mathfrak{A}$ is reduced to zero by G.

Our algorithm reduces to the usual Buchberger algorithm if $\mathfrak{S} = \mathfrak{C}^\star$; that is the reason why we call G a pseudo-Groebner basis rather than a pseudo-Ritt basis.

1.7 References

[Buch 65] B. BUCHBERGER. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal. *PhD. thesis, University of Innsbruck.*

[Bui 92] A. BUIUM. Differential algebraic groups of finite dimension. *Lecture Notes in Mathematics 1506, Springer-Verlag.*

[CC 85] G.W. CHERRY, B.F. CAVINESS. Integration in finite terms with special functions. *A progress report, Proc. EUROSAM 84, Lect. Notes in Comp. Sc. 174, Springer-Verlag (p. 351-359).*

[Ch 83] G.W. CHERRY. Algorithms for integrating elementary functions in terms of logarithmic integrals and error functions. *PhD. Thesis, Univ. of Delaware.*

[CLO 92] D. COX, J. LITTLE, D. O' SHEA. *Ideals, varieties and algorithms.* Springer-Verlag, New York.

[DL 89] J. DENEF, L. LIPSHITZ. Decision problems for differential equations. *Journal of Symbolic Logic, Vol 54(3) (p. 941- 950).*

[Fau 94] J.-C. FAUGÈRE. Résolution de systèmes algébriques. *PhD. thesis, Univ. Paris VI.*

[GHL 87] S. GALLOT, D. HULIN, J. LAFONTAINE. *Riemannian geometry.* Springer-Verlag.

[GoDi 94] T. GOMEZ-DIAZ. Quelques applications de l'évaluation dynamique. *PhD. Thesis, Univ. of Limoges, France.*

[Jan 20] M. JANET. *Systèmes d'équations aux dérivées partielles.* J. de Maths, Series 8, Vol. 3.

[Kap 76] I. KAPLANSKI. *An introduction to differential algebra.* Hermann (2-nd ed.).

[Kol 73] E.R. KOLCHIN. *Differential algebra and algebraic groups.* Academic press, New-York.

[Krei 64] H.F. KREIMER. The foundations for an extension of differential algebra. *Transactions A.M.S. 111 (p 482-492).*

[Li 1837] J. LIOUVILLE. Mémoire sur la classification des transcendantes, et sur les racines de certaines équations en fonction finie explicite des coefficients. *J. Math. Pures et Appl. 2 (p. 56-104).*

[Li 1838] J. LIOUVILLE. Suite du mémoire sur la classification des transcendantes, et sur les racines de certaines équations en fonction finie explicite des coefficients. *J. Math. Pures et Appl. 3 (p. 523-546).*

[Lo 87] A. LOGAR. Constructions over localizations of rings. *Le Mathematiche, Vol. 42 (p. 131-149).*

[MPT 92] T. MORA, G. PFISTER, C. TRAVERSO. An introduction to the tangent cone algorithm. *Advances in computing research (1992), vol. 6 (p. 199-270).*

[NiWe 82] W. NICHOLS, B. WEISFEILER. Differential formal groups of J.F. Ritt. *Amer. Jour. Math. 104(5) (p 943-1005).*

[Pél 95] A. PÉLADAN-GERMA. Testing identities of series defined by algebraic partial differential equations. *Lect. Notes in Comp. Science 948.*

[Pél 97] A. PÉLADAN-GERMA. Tests effectifs de nullité dans des extensions d'anneaux différentiels. *PhD. Thesis, École Polytechnique, France.*

[PV 96] A. PÉLADAN-GERMA, J. VAN DER HOEVEN. Un algorithme de Buchberger local. *Submitted to C.R.A.S.*

[Riq 10] RIQUIER. *Les systèmes d'équations aux dérivés partielles.* Gauthiers Villars, Paris.

[Ris 75] R.H. RISCH. Algebraic properties of elementary functions in analysis. *Amer. Journ. of Math. 4, 101 (p. 743-759).*

[Ritt 50] J.F. RITT. *Differential algebra.* Amer. Math. Soc, New-York.

[Sh 89] J. SHACKELL. Zero-equivalence in function fields defined by algebraic differential equations. *Trans. of the AMS, Vol. 336, Number 1, pp 151-171.*

[VdH 97] J. VAND DER HOEVEN. Automatic asymptotics. *PhD. Thesis, École Polytechnique, France.*

[Wu 87] W.T. WU. A Zero structure theorem for polynomial equation solving and its applications. *Proceedings of ISSAC'88, Roma, Springer Verlag.*

[Zeil 82] D. ZEILBERGER. Sister Celine's technique and its generalizations. *Journal of mathematical analysis and applications 82, p 114-145.*

Chapter 2

Differential elimination theory

2.1 Introduction

In classical treatments of differential algebra, such as [Ritt 50] and [Kol 73], one considers ordinary differential equations or partial differential equations, where the partial derivations commute. As stressed already in the previous chapter, this setting is not completely satisfactory if one wants to perform differential calculus on curved geometrical objects, such as spheres. Different generalizations of differential and difference algebra have been considered since (for instance, see [Krei 64], [NiWe 82] and [Bu 92]). The concept of a ring, with a non commutative operator algebra acting on it is fundamental for these generalizations.

The purpose of this chapter is to generalize some of the most important results from Ritt's classical reduction theory and its applications to the setting of finite dimensional Ritt D-rings. Here a finite dimensional D-ring is a ring A, with a finitely generated A-module D of derivations operating on A, such that D is also a Lie-algebra, compatible with this operation. A Ritt ring is a ring which contains the field $\mathbb{Q}$ of rational numbers; in other words, we restrict our attention to characteristic zero. Extensions to the difference case will be developed in chapter 3.

When taking commuting derivations, our theory reduces to the classical theory. Hence, section 1.2 together with this chapter can be used as a quick but self-contained introduction to differential elimination theory. In the non commutative case, our reduction theory is more general than the classical one, although much of the theory carries over easily. Furthermore, we will see in section 2.2.2 that the generalized theory admits some surprising additional non commutative features.

Let us briefly indicate the contents of the different sections. In section 2.2, we introduce D-polynomials. In section 2.3, we study perfect D-ideals, which are the natural analogues of radical ideals. We will establish some of their main properties, and their relationship with models for systems of D-equations and D-inequations. In section 2.4, we introduce the concepts of admissible orderings and Ritt reduction.

In section 2.5 we give a first application of the Ritt reduction theory: a generalization of the Ritt-Raudenbush theorem. This is the differential counterpart for Hilbert's theorem that a finitely generated polynomial ring over a Noetherian ring is again Noetherian. In the differential case, we have to restrict our attention to perfect D-ideals (which are anyway the only ones with a direct geometrical interpretation). The main tools for the Ritt-Raudenbush theorem are autoreduced and characteristic sets, which are introduced in section 2.5.1.

In section 2.7, we give an important effective application of the reduction theory: the Boulier-Seidenberg-Ritt algorithm. This algorithm is the differential analogue of Buchberger's algorithm, although it reduces to the Wu-Ritt algorithm (see [Wu 87]) in the algebraic case (i.e. when we take an empty set of derivations).

In the last section, we discuss the problem of effective prime decomposition. We will see that this problem is equivalent to one of the major unsolved problems in differential algebra: Kolchin's problem. We will conclude this section by giving some equivalent problems to Kolchin's problem.

2.2 Polynomial D-algebras

2.2.1 Polynomial D-algebras

Let F be some set of variables. Free polynomial D-algebras can be introduced in several ways. We first give an abstract definition. Consider the category of pairs $(A \to B, F \to B)$, where B is a D-A-algebra, determined by $A \to B$. The morphisms are morphisms of D-algebras $B \to B'$, which observe the natural commutations. Then the **free polynomial D-A-algebra** $A\{F\}$ in F is a universal object in this category. The existence of such an object is a direct result of universal algebra, and it is determined uniquely up to isomorphism. The ring A is said to be the **ground ring**. Considered as a D-ring, we call $A\{F\}$ the **free polynomial D-ring** over A in F.

Let us now give a more concrete definition, using the free linear D-operator algebra Ω. Let $B = A[\Omega F]$ be the free polynomial algebra in ΩF over A. Here ΩF has to be interpreted as $\Omega \times F$. Let I be the ideal generated by the elements $(\omega + \omega')f - (\omega f) - (\omega' f)$, where $\omega, \omega' \in \Omega$ and $f \in F$. Consider the A-algebra B/I. The derivations $d \in D$ are naturally defined on ΩF by $d(\omega f) = (d\omega)f$. Hence they extend uniquely to derivations on B, and it is easily checked that I is stable under these derivations. Hence B/I is a D-A-algebra and B/I satisfies the above universal property, so that $B/I \cong A\{F\}$.

If D admits a basis $d_1, \cdots, d_n$, then we claim that $A[\Theta F]$ can naturally be given the structure of a D-A-algebra, which is isomorphic to $A\{F\}$. Indeed, by proposition 1.2 above, Ω admits Θ as a basis, so that ΩF admits ΘF as a basis. The derivations on A can naturally be extended to $A[\Theta F]$, by $d(\omega f) = (d\omega)f$, where $d\omega$ can be expressed as a unique linear combination of elements of Θ. Finally, it is easily checked that $A[\Theta F]$ satisfies the above universal property. Hence $A[\Theta F]$ is isomorphic to $A\{F\}$.

2.2.2 Quasi-polynomial D-algebras

The Lie bracket on the free polynomial D-ring $A\{F\}$ extends the Lie bracket on A. It is often useful, to allow more general commutation rules for polynomial D-rings. However, this section can be skipped at a first reading.

Consider another D-ring structure $(\widetilde{A\{F\}}, D_{\widetilde{A\{F\}}})$ on $\widetilde{A\{F\}} \stackrel{\text{def}}{=} A\{F\}$, where $D_{\widetilde{A\{F\}}}$ is isomorphic to $D_{A\{F\}}$ as an $A\{F\}$-module, but different as a Lie algebra operating on $A\{F\}$. Denote by $\tilde{d}$ the canonical image in $D_{\widetilde{A\{F\}}}$ of an element d in $D_{A\{F\}}$. We say that $\widetilde{A\{F\}}$ is a **quasi-polynomial D-ring**, if for each $d \in D_A \subseteq D_{A\{F\}}$ and $P \in A$ resp. $P \in A[\Omega_r F]$, we have $\tilde{d}P = dP$, resp. $\tilde{d}P = dP + Q$, with $Q \in A[\Omega_r F]$. Considered as a D-A-algebra, we call $\widetilde{A\{F\}}$ a **quasi-polynomial D-algebra** in this case.

Let us assume from now on that $\widetilde{A\{F\}}$ is a quasi-polynomial D-algebra. The ring $A[\Omega_r F]$ is the A-algebra of D-polynomials of **order** at most r. The above definition implies that $A[\Omega_{r+1}F]$ is generated by the $\tilde{d}a$'s as an A-algebra, where $d \in D_A$ and $a \in A[\Omega_r F]$. This suggests to define the **order** of a D-polynomial in $\widetilde{A\{F\}}$ to be the order of the same D-polynomial considered as an element of $A\{F\}$.

Let us again assume that $d_1, \cdots, d_n$ form a basis for D. We wish to investigate the structure of $\widetilde{A\{F\}}$. Denote as before $\tilde{\Theta}_r = \{\tilde{d}_1^{\alpha_1} \cdots \tilde{d}_n^{\alpha_n} | \alpha_1 + \cdots + \alpha_n \leqslant r\}$. Denote also $\tilde{\Theta} = \bigcup_{r\in\mathbb{N}} \tilde{\Theta}_r$. We will also denote $\tilde{\theta} = \tilde{d}_1^{\alpha_1} \cdots \tilde{d}_n^{\alpha_n} \in \tilde{\Theta}$, if $\theta = d_1^{\alpha_1} \cdots d_n^{\alpha_n} \in \Theta$.

Proposition 2.1. *We have $A[\Theta F] \cong A[\tilde{\Theta} F]$ as an A-algebra.*

Proof. Let us prove by induction on r that $A[\Theta F]_r \cong A[\tilde{\Theta}_r F]$. The case $r = 0$ is trivial. Now assume that $A[\Theta F]_{r-1} \cong A[\tilde{\Theta}_{r-1} F]$. Let P be in $A[\Theta F]_r$. We interpret P as a polynomial in $(\Theta_r \backslash \Theta_{r-1})F$, with coefficients in $A[\Theta F]_{r-1}$. Then we can write $\theta f = \tilde{\theta} f + g_\theta$, for all $\theta f \in (\Theta_r \backslash \Theta_{r-1})f$, and some $g_\theta \in A[\Theta F]_{r-1}$. This induces an isomorphism between $A[\Theta F]_{r-1}[(\Theta_r \backslash \Theta_{r-1})F]$ and $A[\Theta F]_{r-1}[(\tilde{\Theta}_r \backslash \tilde{\Theta}_{r-1})F]$, thus completing the induction. We observe that the isomorphism between $A[\Theta F]_r$ and $A[\tilde{\Theta}_r F]$ extends the isomorphism between $A[\Theta F]_{r-1}$ and $A[\tilde{\Theta}_{r-1} F]$, when applying the above construction. Therefore these isomorphisms can be glued together into an isomorphism between $A[\Theta F]$ and $A[\tilde{\Theta} F]$. □

This proposition shows that modulo renaming variables, we do not loose in generality, if we assume that $\theta f = \tilde{\theta} f$, for all $\theta f \in \Theta F$. Having made this assumption, we claim that the structure of the quasi-polynomial D-algebra $\widetilde{A\{F\}}$ is completely determined by the values of the commutators $[\tilde{d}_i, \tilde{d}_j]_{\widetilde{A\{F\}}}$, with $i < j$. Indeed, $\tilde{d}_i \tilde{d}_1^{\alpha_1} \cdots \tilde{d}_n^{\alpha_n} f$ can easily be computed using these values, for all $\alpha_1, \cdots, \alpha_n$ and f.

Inversely, we can ask ourselves whether given values for the $[\tilde{d}_i, \tilde{d}_j]_{\widetilde{A\{F\}}}$'s give rise to a quasi-polynomial D-algebra. In fact, this is the case, if and only if all Jacobi identities between the $\tilde{d}_i, \tilde{d}_j$ and $\tilde{d}_k$'s are verified and $[\tilde{d}_i, \tilde{d}_j]_{\widetilde{A\{F\}}} a = \tilde{d}_i \tilde{d}_j a - \tilde{d}_j \tilde{d}_i a$, for each i, j and $a \in A$. The second relation is in particular satisfied, if $d_i a = 0$, for all i and $a \in A$.

Remark 2.1. The Jacobi identities are not necessarily verified, if we choose arbitrary $[\tilde{d}_i, \tilde{d}_j]_{\widetilde{A\{F\}}}$'s. Nevertheless, the Jacobi identities give us relations by which we can divide out to obtain a D-A-algebra. The reader may check, after having read the rest of this chapter, that our theory may still be applied to this case, by including the relations determined by the Jacobi identities in each system of equations being considered.

In what follows, we will suppose that we have renamed variables, so that $\theta f = \tilde{\theta} f$, for all $\theta f \in \Theta F$, whenever we deal with quasi-polynomial D-algebras, such that D admits a basis. Moreover, we will omit all tildes, hoping that no confusion will arise from this.

2.3 Perfect D-ideals

2.3.1 Elementary properties

Let (A, D) be a D-ring. In this section we will establish some basic features of radical D-ideals, which are also called **perfect D-ideals**. Clearly, the set of such ideals is stable under arbitrary intersections and unions of totally ordered sets for inclusion. If Σ is a subset of A, then we denote by $\{\Sigma\}$ the smallest perfect D-ideal containing Σ. Any prime D-ideal is perfect. A prime D-ideal containing a D-ideal is called a **prime component** of the D-ideal, if it is minimal (for inclusion) with this property.

Let us recall that for any ideal I and subset S of an arbitrary ring, one defines the ideals $I : S = \{a | \forall s \in S \;\; as \in I\} = \bigcap_{s \in S} I : s$ and $I : S^\infty = \bigcup_{n \in \mathbb{N}} I : S^n$. It is readily verified that if I is a perfect D-ideal, then so are $I : S$ and $I : S^\infty$. The following properties of perfect D-ideals will be used in the subsequent sections.

Proposition 2.2. *Let E, Σ and T be subsets of A. Then $\{E, \Sigma T\} = \{E, \Sigma\} \cap \{E, T\}$.*

Proof. It suffices to prove the lemma in the case when $E = \phi$, since this would imply $\{E, \Sigma\} \cap \{E, T\} = \{E^2, E\Sigma, ET, \Sigma T\} = \{E, \Sigma T\}$.

The perfect D-ideal $\{\Sigma T\} : \Sigma$ contains T. Therefore, $\{T\} \subseteq \{\Sigma T\} : \Sigma \Leftrightarrow \{T\}\Sigma \subseteq \{\Sigma T\} \Leftrightarrow \Sigma \subseteq \{\Sigma T\} : \{T\}$. Since $\{\Sigma T\} : \{T\}$ is also a perfect D-ideal, we have $\{\Sigma\} \subseteq \{\Sigma T\} : \{T\}$. Consequently, $\{\Sigma\}\{T\} \subseteq \{\Sigma T\} \Rightarrow (\{\Sigma\} \cap \{T\})^2 \subseteq \{\Sigma T\} \Rightarrow \{\Sigma\} \cap \{T\} \subseteq \{\Sigma T\}$. The inclusion in the opposite direction is obvious. □

Proposition 2.3. *Every perfect D-ideal is the intersection of its prime components.*

Proof. Let I be a perfect D-ideal and suppose that $x \in A \backslash I$. By Zorn's lemma, there exists a maximal perfect D-ideal $\mathfrak{m}$, containing I and not containing x. Suppose that $a, b \in A \backslash \mathfrak{m}$. We have $x \in \{\mathfrak{m}, a\} \cap \{\mathfrak{m}, b\} = \{\mathfrak{m}, ab\}$, by proposition 2.2, so that $ab \notin \mathfrak{m}$. Therefore, $\mathfrak{m}$ is prime. Now let $\mathfrak{p}_x$ be a minimal prime D-ideal, containing I but not x, for each x (the existence follows from Zorn's lemma, because the intersection of a totally ordered set of prime D-ideals is prime). Thus, $\mathfrak{p}_x$ is a prime component of I. Denoting the intersection of the prime components of I by J, we have $J \subseteq \cap_{x \in A \backslash I} \mathfrak{p}_x = I \subseteq J$. □

2.3.2 Prime decompositions and Lazard's lemma

The converse of proposition 2.3 also holds: every D-ideal which is equal to the intersection of its prime components, is perfect. Sometimes, the number of prime components of a perfect D-ideal is finite. In that case, we say that the perfect D-ideal admits a **prime decomposition**.

Proposition 2.4. *Let I be a perfect D-ideal, such that I is a finite intersection of prime D-ideals. Then I is the intersection of a finite set of prime D-ideals, one of which does not contain another. This set is unique, being the set of prime components of I.*

Proof. We can write $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_p$, for some prime D-ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$. We may assume without loss of generality that we discarded each $\mathfrak{p}_i$, which contains a $\mathfrak{p}_j$, with $j \neq i$. This proves the first part of the proposition. Let $\mathfrak{p}$ be any prime component of I. Then $\mathfrak{p} \supseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, whence $\mathfrak{p} \supseteq \mathfrak{p}_i$, for some i, and $\mathfrak{p} = \mathfrak{p}_i$. Therefore, all prime components figure among the $\mathfrak{p}_i$'s. Finally, each prime D-ideal containing I contains a prime component of I, so that all $\mathfrak{p}_i$'s are prime components of I. □

The prime decomposable D-ideals I can be characterized as follows, by looking at the total rings $Q(A/I)$ of fractions they induce:

Proposition 2.5. *Let I be a perfect D-ideal. Then I admits a prime decomposition if and only if $Q(A/I)$ is isomorphic to a finite product of D-fields.*

Proof. Suppose that I admits a prime decomposition $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_p$. Let s be such that $s_I = \overline{s} \in A/I$ is a non zero divisor. Then s does not belong to any of the $\mathfrak{p}_i$'s. Now let $a, s \in A$ be such that $a_I/s_I = 0$ in $Q(A/I)$. Then $(as')_I = 0$, for some non zero divisor s'_I, so that $a \in I$. Hence the mapping

$$\begin{array}{ccc} Q(A/I) & \xrightarrow{\varphi} & Q(A/\mathfrak{p}_1) \times \cdots \times Q(A/\mathfrak{p}_p) \\ \dfrac{a_I}{s_I} & \longmapsto & \left(\dfrac{a_{\mathfrak{p}_1}}{s_{\mathfrak{p}_1}}, \cdots \dfrac{a_{\mathfrak{p}_p}}{s_{\mathfrak{p}_p}}\right) \end{array}$$

is well defined. It is easily checked that the kernel of φ is trivial.

As the $\mathfrak{p}_i$'s mutually do not contain one another, there exist $x_1, \cdots, x_p$, such that $x_i \in \mathfrak{p}_i$, but $x_i \notin \mathfrak{p}_j$, for all i and $j \neq i$. Setting $y_i = x_1 \cdots x_{i-1} x^{i+1} \cdots x_p$, we observe that $y_i \notin \mathfrak{p}_i$, but $y_i \in \mathfrak{p}_j$, for all i and $j \neq i$. Now let $a_1, \cdots, a_p, s_1, \cdots, s_p \in A$ be such that $s_i \notin \mathfrak{p}_i$, for all i. Then $t_i = s_i y_i + \sum_{j | s_i y_i \in \mathfrak{p}_j} y_j$ is a non zero divisor and $t_i \equiv s_i y_i$, for all i. Hence, $\varphi((a_1 y_1/t_1)_{Q(A/I)} + \cdots + (a_p y_p/t_p)_{Q(A/I)}) = ((a_1 y_1/t_1)_{Q(A/\mathfrak{p}_1)}, \cdots, (a_p y_p/t_p)_{Q(A/\mathfrak{p}_p)})$, which proves the surjectivity of φ.

Conversely, suppose that we have an isomorphism

$$Q(A/I) \xrightarrow{\varphi} K_1 \times \cdots \times K_p,$$

where $K_1, \cdots, K_p$ are D-fields. Let $J_i = \{(b_1, \cdots, b_p) \in K_1 \times \cdots \times K_p | b_i = 0\}$, for each i. Then $\mathfrak{p}_i = \varphi^{-1}(J_i) \cap A$ is a prime D-ideal, for each i, and none of the $\mathfrak{p}_i$'s contains another. Furthermore, $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_p$ so that we have a prime decomposition of I. Actually, φ coincides with the previously defined mapping. □

The following algebraic lemma is a reformulation of a lemma due to Lazard (see [BLOP 95]). The lemma describes how prime decomposability is related to algebraic extensions, and it will be used in section 2.5.1.

Lemma 2.1. (Lazard's lemma) *Let A be a ring, such that the zero-ideal of A admits a prime decomposition. Let $P \in A[x] \backslash A$ be a non constant polynomial. Then the ideal $(P) : (\partial P/\partial x)$ of $A[x]$ admits a prime decomposition.*

Proof. Let $S = \partial P/\partial x$. By proposition 2.5, we have

$$Q(A/I) \cong K_1 \times \cdots \times K_p,$$

for certain fields $K_1, \cdots, K_p$. Then

$$Q(A[x]/(P)) \cong S^{-1}A[x]/(P) \cong S^{-1}K_1[x]/(P) \times \cdots \times S^{-1}K_p[x]/(P).$$

Hence, it suffices to show that $S^{-1}K_j[x]/(P)$ is isomorphic to a product of fields for each j, by proposition 2.5.

Let us fix j, and decompose $P = \Phi_1^{\alpha_1} \cdots \Phi_h^{\alpha_h}$ in irreducible factors in $K_j[x]$. By the Chinese remainder theorem, we have

$$K_j[x]/(P) \cong K_j[x]/(\Phi_1^{\alpha_1}) \times \cdots \times K_j[x]/(\Phi_h^{\alpha_h}).$$

Since S divides all multiple factors of P, $S^{-1}K_j[x]/(P)$ is isomorphic to the product of those $K_j[x]/(\Phi_m)$'s, with $\alpha_m = 1$. This completes the proof. □

2.3.3 Models for systems of D-equations

The study of perfect D-ideals is closely related to the study of solutions to systems of D-equations and D-inequations. Suppose that A is a D-algebra over a D-field K. Let $\Sigma \subseteq A$ be a set of D-equations and let $T \subseteq A$ be a set of D-inequations. We will always assume that Σ and T are finite. A **model** for (Σ, T) is a D-morphism φ over K of A into a D-overfield L of K, such that $\varphi(\Sigma) = 0$ and $\varphi(Q) \cap \{0\} = \phi$. We remark that the D-field L can be fixed once and for all in the definition, by taking a universal extension of K. We will not use this viewpoint any further; for details, see [Kol 73]. We have:

Proposition 2.6. *Let (Σ, T) be a system of D-equations and D-inequations. Denote by P the product of the elements of T. Then (Σ, T) admits a model, if and only if $P \notin \{\Sigma\}$.*

Proof. Suppose that we have a model $\varphi : A \to L$. Then $\ker \varphi$ is a perfect D-ideal containing Σ (indeed: $a^n \in \ker \varphi \Rightarrow \varphi(a^n) = 0 \Rightarrow \varphi(a) = 0$), which does not contain P. Inversely, suppose that $P \notin \{\Sigma\}$. By proposition 2.3, there exists a prime D-ideal $\mathfrak{p}_P$, containing Σ, which does not contain P. Then $\mathfrak{p}_P$ does not contain any of the elements of T either, because $\mathfrak{p}_P$ is prime. Consequently, the canonical D-morphism $A \to Q(A/\mathfrak{p}_P)$ is a model. □

Corollary. *Let (Σ, T) be a system of D-equations and D-inequations, and let P be a D-equation in A. Then $\varphi(P) = 0$ for each model φ of (Σ, T), if and only if $P \in \{\Sigma\} : T^\infty$.* □

Let us finally introduce some more terminology about models for later use. Two systems are said to be **equivalent**, if they admit the same models. We say that a D-equation P is **implied** by a system (Σ, T), if $\varphi(P) = 0$ for each model φ of (Σ, T). A finite number $(\Sigma_1, T_1), \cdots, (\Sigma_k, T_k)$ of systems are said to form a **decomposition** of a system (Σ, T), if a D-morphism $\varphi : A \to L$ over K is a model for (Σ, T), if and only if it is a model for one of the (Σ_i, T_i)'s.

2.4 Ritt reduction

Let (A, D) be a finite dimensional D-ring, such that $d_1, \cdots, d_n$ form a basis for D, and let F be a finite set of variables. Let $A\{F\}$ be the free polynomial D-A-algebra in F, or any other quasi-polynomial D-A-algebra in F. We recall that

$$\Theta = \{d_1^{\alpha_1} \cdots d_n^{\alpha_n} | \alpha_1, \cdots, \alpha_n \in \mathbb{N}\},$$

and that we have $A\{F\} = A[\Theta F]$.

2.4.1 Admissible orderings

Assume that we dispose of some total ordering $\leqslant$ on ΘF. If P is a D-polynomial in $A[\Theta F]$, then we denote by $V_P \subseteq \Theta F$ the set of **variables** occurring in P. If $V_P \neq \phi$, then V_P has a maximal element for $\leqslant$, which we denote by v_P or $v(P)$, and which is called the **leading variable** or **leader** of P. By convention, we take $v_P = -\infty$, if $V_P = \phi$; that is, if $P \in A$. We say that $\leqslant$ is an **admissible ordering** on ΘF (or a **ranking**, following Ritt), if

A1. $v(\theta f) < v(d_i \theta f)$, for any i and $\theta f \in \Theta F$.
A2. $v(d_i \theta f) \leqslant v(d_i \theta' f')$, for any i and $\theta f \leqslant \theta' f'$ in ΘF.
A3. $v(d_i d_j \theta f) = v(d_j d_i \theta f)$, for any i, j and $\theta f \in \Theta F$.

The main point about admissible orderings is that they exist. For example, enumerating $F = \{f_1, \cdots, f_k\}$, the ordering on the $d_1^{\alpha_1} \cdots d_n^{\alpha_n} f_i$'s, which is obtained by ordering lexicographically on $\alpha_1 + \cdots + \alpha_n$, $\alpha_1, \cdots, \alpha_{n-1}$ and i, is an admissible ordering. Moreover this ordering is an **orderly admissible ordering** , that is, $\theta f < \theta' f'$, whenever the order of θ is strictly inferior to the order of θ'.

Remark 2.2. In the affine case (the d_i's commute), the third condition is automatically verified and our definition of admissible orderings coincides with the classical definition by Ritt. We also remark that an admissible ordering defines derivations $d_1, \cdots, d_n$ on ΘF by $d_i \omega = v(d_i \omega)$. Then the definition of admissible orderings is intrinsic to ΘF with these derivations. From this point of view, an admissible ordering in our sense is necessarily an admissible ordering in Ritt's sense. In particular, admissible orderings are well orderings. The converse is only true in the affine case, although all orderly admissible orderings in Ritt's sense are admissible in our sense.

Suppose that we fixed some admissible ordering $\leqslant$ and let P be some D-polynomial in $A\{F\} \backslash A$. Considering P as a polynomial in v_P, we denote by $\deg P = \deg_{v_P} P$ its degree. We call **initial** I_P of P the coefficient of its highest power in v_P and **separant** S_P of P the polynomial $\partial P / \partial v_P$. We remark that if P is linear (in v_P), then $S_P = I_P$. Moreover, any proper derivative θP of P is linear, and we have $v_{\theta P} = v_{\theta v_P}$ and $I_{\theta P} = S_P$. We also claim that $v_{\omega P} = v_{\theta P}$, if ω is any shuffle of an element θ in Θ. Indeed, it suffices to prove our claim when $P = f \in F$, in which case it follows from **A2** and **A3**, by using induction over r.

One defines a natural partial ordering $\preceq$ on ΘF by $d_1^{\alpha_1} \cdots d_n^{\alpha_n} f \preceq d_1^{\beta_1} \cdots d_n^{\beta_n} f'$, if $\alpha_1 \leqslant \beta_1, \cdots, \alpha_n \leqslant \beta_n$ and $f = f'$. It is not hard to see that any admissible ordering $\leqslant$ on ΘF extends $\preceq$ and that

$$\theta f \preceq \theta' f' \Leftrightarrow \exists \eta \in \Theta \quad v(\eta\theta f) = v(\theta' f').$$

We also remark that $\preceq$ is a **well-quasi-ordering**, that is, $\leqslant$ is well founded and admits no infinite antichains. Indeed, the partial ordering is isomorphic to k disjoint copies the product ordering on $\mathbb{N}^n$ and we use Dickson's lemma. The fact that $\preceq$ is a well-quasi-ordering implies that the set of minimal elements of each **final segment** of ΘF (i.e. a subset $E \subseteq \Theta F$, such that $x \in E \ \wedge \ x \preceq y \Rightarrow y \in E$) is an antichain and thereby finite.

2.4.2 The reduction procedure

We will need some more notations. Let E be a finite subset of $A\{F\}$. If $\boldsymbol{\omega}$ is a mapping from E into Ω, then we denote $\boldsymbol{\omega} E = \sum_{P \in E} \boldsymbol{\omega}(P) P$. If $\boldsymbol{\alpha}$ is a mapping from E into $\mathbb{N}$, then we denote $E^{\boldsymbol{\alpha}} = \prod_{P \in E} P^{\boldsymbol{\alpha}(P)}$. In particular, denoting by $\mathbf{1}$ the constant mapping $P \mapsto 1$, $E^{\mathbf{1}}$ equals the product of the elements of H_Σ. Denoting by δ_P the mapping with $\delta_P(P) = 1$ and $\delta_P(Q) = 0$, for $Q \neq P$, we have $E^{\delta_P} = P$. Now suppose that Σ is a finite subset of $A\{F\} \backslash A$. We denote $I_\Sigma = \{I_P | P \in \Sigma\}$, $S_\Sigma = \{S_P | P \in \Sigma\}$, $H_\Sigma = I_\Sigma \cup S_\Sigma$, $v_\Sigma = \{v_P | P \in \Sigma\}$ and $V_\Sigma = \bigcup_{P \in \Sigma} V_P$. Finally, we denote $[\Sigma]_v = (\{\theta P | \theta \in \Theta \ \wedge \ P \in \Sigma \ \wedge \ v_{\theta P} \leqslant v\})$, for any $v \in \Theta F$.

Let Σ still be a finite subset of $A\{F\} \backslash A$. A D-polynomial $P \in A\{F\}$ is said to be **partially reduced** w.r.t. Σ if we do not have $v_Q \prec w$ for some $Q \in \Sigma$ and $w \in V_P$. We say that P is **reduced** w.r.t. Σ, if, moreover, $\deg_{v_Q} P < \deg Q$, whenever $v_Q = v_P$ for some i. We claim that for any $P \in A\{F\}$, we can write

$$S_\Sigma^{\boldsymbol{\alpha}} P = \boldsymbol{\omega} \Sigma + R, \tag{2.1}$$

for some $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R, where $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$ and where R is partially reduced w.r.t. Σ. Here Q and R are called a **quotient** and a **partial remainder** of partial division of P w.r.t. Σ and $S_\Sigma^{\boldsymbol{\alpha}}$ is said to be the corresponding **multiplier**. We also claim that we can write

$$H_\Sigma^{\boldsymbol{\alpha}} P = \boldsymbol{\omega} \Sigma + R, \tag{2.2}$$

for some $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R, where $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$ and where R is reduced w.r.t. Σ. Here Q and R are called a **quotient** and a **remainder** of division of P w.r.t. Σ and $S_\Sigma^{\boldsymbol{\alpha}}$ is said to be the corresponding **multiplier**. If $R = 0$, this relation implies that $H_C^{\boldsymbol{\alpha}} P$ is in $[\Sigma]$, so that P is in $[\Sigma] : H_C^\infty$. Our claims are summarized in

Proposition 2.7. *Let Σ and P be as above. Then there exist $\boldsymbol{\alpha}, \boldsymbol{\omega}, R$ verifying (2.1) resp. (2.2), where R is partially reduced resp. reduced w.r.t. Σ, and where $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$.*

Proof. We will give algorithms to compute such $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R. If Φ and Ψ are D-polynomials, considered as polynomials in v_Ψ, then we will use the Euclidean division algorithm to compute the rest $R := \texttt{Euclidean\_division}(\Phi, \Psi)$ of the division of $I_\Psi^{\deg_{v_\Psi} \Phi - \deg \Psi + 1} \Phi$ by Ψ.

Algorithm P `part-rem` Σ.

Input: A D-polynomial P and a finite set of non ground D-polynomials Σ.

Output: A partially reduced R w.r.t. Σ satisfying (2.1), for some $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$, with $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$.

$R := P$
while $\exists \Phi \in \Sigma \exists w \in V_R \;\; v_\Phi \prec w$ **do**
- Choose w maximal verifying the above relation.
- Let $\theta \in \Theta$ be such that $v_{\theta\Phi} = w$.

$R := \texttt{Euclidean\_division}(R, \theta\Phi)$
return R

The algorithm clearly terminates, since w strictly decreases during the loop. Let us prove the correctness. At the start of the loop, (2.1) is verified, when we take $\boldsymbol{\alpha} = \boldsymbol{\omega} = \mathbf{0}$. Now suppose that (2.1) is verified for some $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R, with $v_R \leqslant v_P$ and with $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$. If there exist $\Phi \in \Sigma$ and $w \in V_R$, with $v_\Phi \prec w$, let Q resp. R' denote the quotient and the rest of the Euclidean division of R by $\theta\Phi$, with the notations of the algorithm. Taking $\boldsymbol{\alpha}' := \boldsymbol{\alpha} + (\deg_w Q + 1)\delta_{S_P}$ and $\boldsymbol{\omega}' := \boldsymbol{\omega} + Q\theta\delta_\Phi$, we observe that $H_\Sigma^{\boldsymbol{\alpha}'} P = \boldsymbol{\theta}'\Sigma + R'$, with $\boldsymbol{\omega}'\Sigma \in [\Sigma]_{v_P}$. Hence, the property that (2.1) be satisfied, for some $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$, with $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$, is conserved during the execution. By definition, R is partially reduced w.r.t. Σ at the end of the loop.

Algorithm P `rem` Σ.

Input: A D-polynomial P and a finite set of non ground D-polynomials Σ.

Output: We return a reduced R w.r.t. Σ satisfying (2.2), for some $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}\Sigma \in [\Sigma]_{v_P}$.

$R := P$ `part-rem` Σ
while $\exists \Phi \in \Sigma \quad \deg \Phi \leqslant \deg_{v_\Phi} R$ **do**
$R := \texttt{Euclidean\_division}(R, \Phi)$
$R := R$ `part-rem` Σ
return R

The termination and correctness proofs of ' `rem` ' are analogous to the termination and correctness proofs of ' `part-rem` '; this time one should consider the Euclidean division of R by Φ and take $\boldsymbol{\alpha}' := \boldsymbol{\alpha} + (\deg_{v_P} Q + 1)\delta_{I_P}$ and $\boldsymbol{\omega}' := \boldsymbol{\omega} + Q\theta\delta_\Phi$. We remark that the correctness argument shows that we can even compute $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R, satisfying the conditions of the proposition. □

2.5 Finite basis theorems for D-rings

We will now generalize the classical Ritt-Raudenbush theorem (for characteristic zero) to the context of D-rings. A D-ring (A, D) is said to be a **Ritt-Raudenbush D-ring**, if A contains $\mathbb{Q}$ and if each perfect D-ideal of A is finitely generated as a perfect D-ideal. The Ritt-Raudenbush theorem states that a finitely generated quasi-polynomial D-algebra over such a ring is again a Ritt-Raudenbush ring. We first need some preliminaries.

2.5.1 Characteristic sets

A subset $\Sigma \subseteq A\{F\}\backslash A$ is said to be **autoreduced**, if each $P \in \Sigma$ is reduced w.r.t. $\Sigma\backslash\{P\}$. This implies that the v_P's form an antichain for $\preceq$. In particular, Σ must be finite. The following proposition is an easy consequence of Lazard's lemma:

Proposition 2.8. *Let Σ be an autoreduced subset of $A\{F\}$ and assume that the zero-ideal of A admits an algebraic (i.e. non differential) prime decomposition. Then $(\Sigma) : S_\Sigma$ admits an algebraic prime decomposition.*

Proof. Recall that V_Σ denotes the set of variables occurring in the D-polynomials in Σ, and v_Σ the set of their leaders. By hypothesis, the zero-ideal of A admits a prime decomposition, and so does the zero-ideal of $A[V_\Sigma\backslash v_\Sigma]$.

Now enumerate $\Sigma = \{P_1, \cdots, P_p\}$ and put $v_i = v_{P_i}$, for each i. Denote by I_i the ideal $(P_1, \cdots, P_i) : S_{\{P_1,\cdots,P_i\}}$ of $A_i = A[V_\Sigma\backslash\{v_{i+1}, \cdots, v_p\}]$. We will prove by induction over i that I_i admits a prime decomposition. If $p = 0$, then we are already done. Furthermore, assuming that I_{i-1} admits a prime decomposition, then so does I_i, by applying Lazard's lemma to the base ring A_{i-1}/I_{i-1} with $x = v_i$ and $P = P_i$. □

Let $\Sigma = \{P_1, \cdots, P_p\}$ and $T = \{Q_1, \cdots, Q_q\}$ be autoreduced subsets of $A\{F\}$, with $v_{P_1} < \cdots < v_{P_p}$ and $v_{Q_1} < \cdots < v_{Q_q}$. Then we define a partial ordering $\leqslant$ on autoreduced sets by $\{P_1, \cdots, P_p\} < \{Q_1, \cdots, Q_q\}$, if $v_{P_i} = v_{Q_i}$ and $\deg P_i = \deg Q_i$, for i strictly inferior to a certain j, and either $v_{P_j} < v_{Q_j}$, or $v_{P_j} = v_{Q_j}$ and $\deg P_j < \deg Q_j$, or $j = q + 1 \leqslant p$. It is readily verified that $\leqslant$ is a well founded.

Let I be a D-ideal of $K\{F\}$ and let E be the set of autoreduced subsets Σ of I, such that none of the separants S_P is in I, where P runs over Σ. We have $\phi \in E$. As $\leqslant$ is a well founded, E admits a minimal element, which is called a **characteristic set** of I.

Proposition 2.9. *Let C be a characteristic set of a D-ideal $I \subseteq A\{F\}$. Then*

(a) If $P \in I\backslash A$ is reduced w.r.t. C, then $S_P \in I$.
(b) If $P \in I$ is reduced w.r.t. C, then $P \in (I \cap A)$.
(c) For any $P \in C$, we have $I_P \notin I$ and $S_P \notin I$.
(d) If I is prime, then $H_C^{\mathbf{1}} \notin I$.

Proof. Suppose that $P \in I \backslash A$ is reduced w.r.t C, with $S_P \notin I$. Then the set $C' = \{Q \in C | v_Q < v_P\} \cup \{P\}$ would be an autoreduced set of I, strictly smaller than C. This proves (a).

Next, assume that (b) is false, and let $P \in I$ be reduced w.r.t. C, such that v_P and $\deg P$ are minimal. Then $S_P \in (I \cap A)$, by (a) and the minimality hypothesis. Writing $P = P_{\deg P} v_P^{\deg P} + \cdots + P_0$, we have $S_P = (\deg P) P_{\deg P} v_P^{\deg P - 1} + \cdots + P_1$. As $S_P \in (I \cap A)$, we have $P_1, \cdots, (\deg P) P_{\deg P} \in (I \cap A)$. Therefore, $P_1, \cdots, P_{\deg P} \in (I \cap A)$, since A contains $\mathbb{Q}$. Consequently, $P_0 \in I$ and $P_0 \in (I \cap A)$, by the minimality hypothesis. But this implies that $P \in (I \cap A)$.

Now let P be in C. Then $S_P \notin I$, by definition. Suppose that I_P is in I. Then $P' = P - I_P v_P^{\deg P}$ is in I and reduced w.r.t. C. If $\deg P = 0$, we have $\partial P' / \partial v_P = 0 \in I$. In the other case, we also have $S_{P'} = \partial P' / \partial v_P \in I$, by (a). Therefore, $S_P - (\deg P) I_P v_P^{\deg P - 1}$ is in I, so that S_P is in I. This contradiction proves (c).

The implication (c) $\Rightarrow$ (d) is trivial. $\square$

2.5.2 Some lemmas

Lemma 2.2. *Let (A, D_A) be a D-ring and B a D-algebra over (A, D_A). Then there exists another D-ring structure (A, D'_A) on A and another D-algebra structure over (A, D'_A) on B, such that D'_A admits a basis, and such that A and B have the same D-ideals for both structures.*

Proof. Let D_A be finitely generated by $d_1, \cdots, d_n$. Let D'_A be the free A-module generated by $d_1, \cdots, d_n$. We define a Lie bracket on D'_A by

$$\left[\sum_i a_i d_i, \sum_j b_j d_j\right] = \sum_{i,j,k} a_i b_j c_k d_k + \sum_{i,j} a_i (d_i b_j) d_j - b_j (d_j a_i) d_i,$$

where $[d_i, d_j] = \sum_k c_k d_k$. We have a natural action of D'_A on A resp. B by $(a_1 d_1 + \cdots + a_n d_n) b = a_1 d_1 b + \cdots + a_n d_n b$, which is compatible with the Lie bracket on D'_A. Clearly, a subset of A resp. B is stable by D_A, if and only if it is stable by D'_A. $\square$

Lemma 2.3. *Let A be a D-ring, so that there exists a non finitely generated perfect D-ideal. Then the set of non finitely generated perfect D-ideals admits a maximal element, and every such a maximal element is prime.*

Proof. The union of a totally ordered set of non finitely generated perfect D-ideals is again a non finitely generated perfect D-ideal. The existence of a maximal element follows therefore by Zorn's lemma. Now let $\mathfrak{m}$ be any such maximal element. Clearly $\mathfrak{m} \neq A$. Chose $a, b \in A \backslash \mathfrak{m}$. Then $\{\mathfrak{m}, a\}$ and $\{\mathfrak{m}, b\}$, are finitely generated, say by Σ, resp. T. Thus, $\{\mathfrak{m}, ab\} = \{\Sigma\} \cap \{T\}$, by applying proposition 2.2, so that $ab \notin \mathfrak{m}$. Hence $\mathfrak{m}$ is prime. □

Lemma 2.4. *Let E be any subset of a D-ring A and let P be in $\{E\}$. Then there exists a finite subset Σ of E, such that $P \in \{\Sigma\}$.*

Proof. We have $\{E\} = \bigcup_{n \in N} E_n$, where E_n is recursively defined by $E_0 = E$ and $E_{n+1} = \mathrm{rad}[E_n]$. Thus, we have $P \in E_n$ for some n. Let us prove the lemma by induction on n. The case $n = 0$ is trivial. Assume that we have proved the lemma up to $n - 1$. We have $P^k \in [E_{n-1}]$, for some k. Hence, $P^k \in [Q_1, \cdots, Q_q]$ for some $Q_1, \cdots, Q_q$ in E_{n-1}. For each $1 \leqslant i \leqslant q$, there exists a finite subset Σ_i of E, such that $Q_i \in \{\Sigma_i\}$, by the induction hypothesis. Then we can take $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_k$. □

2.5.3 The Ritt-Raudenbush theorem

Theorem 2.1. **(Ritt-Raudenbush's theorem)** *Let A be a Ritt-Raudenbush D-ring and F a finite set. Then any quasi-polynomial D-ring $A\{F\}$ over A in F is Ritt-Raudenbush.*

Proof. By lemma 2.2, we may assume without loss of generality that D_A admits a basis, so that we can fix some admissible ordering on $\Theta_A F$. Suppose that the conclusion of the theorem is false. By lemma 2.3, there exists a maximal non finitely generated perfect D-ideal $\mathfrak{p}$, which is prime. Let C be a characteristic set for $\mathfrak{p}$. Since A is a Ritt-Raudenbush D-ring, there exists a finite set Σ, such that $(\mathfrak{p} \cap A) = \{\Sigma\}$.

Let P be in $\mathfrak{p}$. We can write $H_C^{\boldsymbol{\alpha}} P = \boldsymbol{\omega} C + R$, for some $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R, where R is reduced w.r.t. C. By proposition 2.9(b), we have $R \in (\mathfrak{p} \cap A)$. Hence, $H_C^{\boldsymbol{\alpha}} P \in [C, \Sigma]$, whence $H_C^{\mathbf{1}} P \in \mathrm{rad}[C, \Sigma] \subseteq \{C, \Sigma\}$. This proves that $H_C^{\mathbf{1}} \mathfrak{p} \subseteq \{C, \Sigma\}$.

Now $H_C^{\mathbf{1}} \notin \mathfrak{p}$, by proposition 2.9(d), so that the perfect D-ideal $\{H_C^{\mathbf{1}}, \mathfrak{p}\}$ strictly contains $\mathfrak{p}$. Therefore, $\{H_C^{\mathbf{1}}, \mathfrak{p}\}$ is finitely generated by the minimality hypothesis. Applying lemma 2.4, each generator is in a perfect D-ideal generated by a finite subset of $\mathfrak{p} \cup \{H_C^{\mathbf{1}}\}$. Hence, we can write $\{H_C^{\mathbf{1}}, \mathfrak{p}\} = \{H_C^{\mathbf{1}}, T\}$, for some finite $T \subseteq \mathfrak{p}$. Finally, $\mathfrak{p}$ is finitely generated, since $\mathfrak{p} = \mathfrak{p} \cap \{H_C^{\mathbf{1}}, \mathfrak{p}\} = \mathfrak{p} \cap \{H_C^{\mathbf{1}}, T\} = \{H_C^{\mathbf{1}} \mathfrak{p}, T\} \subseteq \{C, \Sigma, T\}$. □

Having established the Ritt-Raudenbush theorem, let us now come to some important properties of Ritt-Raudenbush D-rings. In fact, these properties are analogous to the properties of Noetherian rings. First, we have the three classical equivalent conditions for a D-ring to be Ritt-Raudenbush:

(a) Each perfect D-ideal is finitely generated.
(b) Each strictly ascending sequence of perfect D-ideals is finite.
(c) Each set of perfect D-ideals admits a maximal element.

The equivalence proof is left to the reader. We also have the usual prime decomposition theorem:

Proposition 2.10. *Any perfect D-ideal of a Ritt-Raudenbush D-ring A admits a prime decomposition.*

Proof. If the set of perfect D-ideals of A, which are not finite intersections of prime D-ideals were not empty, this set would have a maximal element I, by the condition (c) above. Now I is clearly not prime and not equal to R. Let $a, b \in A$ be such that $ab \in I$ and $a, b \notin I$. Then $\{I, a\}$ and $\{I, b\}$ would be finite intersections of prime D-ideals, and so would $I = \{I, ab\} = \{I, a\} \cap \{I, b\}$, by proposition 2.2. We conclude by proposition 2.4. $\square$

2.6 Coherent autoreduced sets

If we want to solve a system of D-equations, the first step is to search for some more canonical equivalent system of equations. For theoretical purposes, characteristic sets are very useful; for example, they are used to prove the Ritt-Raudenbush theorem. However, as characteristic sets are hard to compute, we will introduce the weaker, but more effective concept of coherent autoreduced sets. We then prove Rosenfeld's lemma, which is a key result for later applications.

Let Σ be an autoreduced set. Let $P, Q \in \Sigma$ be such that $v_P = \theta f$ and $v_Q = \eta f$. Writing $\theta = d_1^{\alpha_1} \cdots d_n^{\alpha_n}$ and $\eta = d_1^{\beta_1} \cdots d_n^{\beta_n}$, we denote

$$\begin{aligned} \theta \wedge \eta &= d_1^{\max(\alpha_1,\beta_1)} \cdots d_n^{\max(\alpha_n,\beta_n)}, \\ \theta' &= d_1^{\max(\alpha_1,\beta_1)-\beta_1} \cdots d_n^{\max(\alpha_n,\beta_n)-\beta_n}, \\ \eta' &= d_1^{\max(\alpha_1,\beta_1)-\alpha_1} \cdots d_n^{\max(\alpha_n,\beta_n)-\alpha_n}. \end{aligned}$$

We will also denote $(\theta \wedge \eta)f = v_P \wedge v_Q$. The **$\Delta$-polynomial** of P and Q is defined by $\Delta(P, Q) = S_Q \eta' P - S_P \theta' Q$. We remark that $v_{\Delta(P,Q)} < (\theta \wedge \eta)f$. We say that Σ is **coherent** if all Δ-polynomials $\Delta(P, Q)$ are reduced w.r.t. Σ.

We need some preliminaries in order to prove Rosenfeld's lemma. If Q is any D-polynomial in $A\{F\} \backslash A$, then we denote $[\Sigma]_Q = (\{\theta P | \theta \in \Theta \ \wedge \ P \in \Sigma \ \wedge \ v_{\theta P} \leqslant v_Q\})$ and $[\Sigma]_{<Q} = (\{\theta P | \theta \in \Theta \ \wedge \ P \in \Sigma \ \wedge \ v_{\theta P} < v_Q\})$, for any $Q \in A\{F\} \backslash F$. The following proposition follows trivially from proposition 1.1, if $\leqslant$ is orderly; its proof in the general case is left as an exercise to the reader.

Proposition 2.11. *Let ω be a shuffle of $\theta \in \Theta$. Then for any $P \in \Sigma$, we have $(\omega - \theta)P \in [\Sigma]_{<\theta P}$.* $\square$

Lemma 2.5. *Let C be a coherent autoreduced set. Then for any P, Q in C and $\theta, \eta \in \Theta$, with $v_{\theta P} = v_{\eta Q}$, we have $S_Q \theta P - S_P \eta Q \in [C]_{<\theta P} : H_C^\infty$.*

Proof. Let $\theta', \eta' \in \Theta$ be such that $w = v_P \wedge v_Q = v_{\theta' P} = v_{\eta' Q}$. We claim that

$$\Delta_\sigma = S_Q \sigma \theta' P - S_P \sigma \eta' Q \in [C]_{<\sigma w} : H_C^\infty,$$

for any $\sigma \in \Theta$. We proceed by induction over the order of σ. By proposition 2.7, we have $\Delta(P, Q) \in [C]_{<w} : H_C^\infty$. This gives $\Delta_1 = \Delta(P, Q) \in [C]_{<w} : H_C^\infty$, for $\sigma = 1$.

Now suppose that $\sigma \neq 1$, and write $\sigma = d_i \sigma'$, for some i. By the induction hypothesis, $H_C^{\boldsymbol{\alpha}} \Delta_{\sigma'} \in [C]_{<\sigma' w}$, for some $\boldsymbol{\alpha}$. Hence, $d_i(H_C^{\boldsymbol{\alpha}} \Delta_{\sigma'}) \in [C]_{<\sigma w}$, by proposition 2.11. Moreover,

$$d_i(H_C^{\boldsymbol{\alpha}} \Delta_{\sigma'}) = d_i(H_C^{\boldsymbol{\alpha}}) \Delta_{\sigma'} + H_C^{\boldsymbol{\alpha}} d_i \Delta_{\sigma'},$$

where $d_i(H_C^{\boldsymbol{\alpha}}) \Delta_{\sigma'} \in [C]_{<\sigma w}$. Therefore, $d_i \Delta_{\sigma'} \in [C]_{<\sigma w} : H_C^\infty$ and

$$\Delta_\sigma = d_i \Delta_{\sigma'} - (d_i S_Q) \sigma' \theta' P + (d_i S_P) \sigma \eta' Q \in [C]_{<\sigma w} : H_C^\infty.$$

This proves our claim; to conclude, take σ such that $v_{\sigma w} = v_{\theta P} = v_{\eta Q}$. Then

$$S_Q \theta P - S_P \eta Q = \Delta_\sigma + S_Q(\theta - \sigma \theta') P - S_P(\eta - \sigma \eta') Q \in [C]_{<\theta P} : H_C^\infty,$$

by proposition 2.11. □

Lemma 2.6. (Rosenfeld's lemma) *Let C be a coherent autoreduced subset of $A\{F\}$, such that H_C has no zero divisors. Then any D-polynomial in $[C] : H_C^\infty$, which is partially reduced w.r.t. C belongs to $(C) : H_C^\infty$.*

Proof. Let Q be a D-polynomial in $[C] : H_C^\infty$, which is partially reduced w.r.t. C. We may write

$$H_C^{\boldsymbol{\alpha}} Q = \sum_{i=1}^{r} \Phi_i \theta_i P_i + \sum_{j=1}^{s} \Phi'_j \theta'_j P'_j + \sum_{k=1}^{t} \Phi''_k P''_k, \tag{2.3}$$

where $\Phi_i, \Phi'_j, \Phi''_k \in A\{F\}$, $\theta_i, \theta'_j \in \Theta$ and $P_i, P'_j, P''_k \in C$, for all i, j, k. Moreover, we assume that there exists some v, so that $v_{\theta_i P_i} = v$, for each i and such that $v > v_{\theta'_j P'_j}$, for each j. We also assume that the θ_i's and the θ'_j's have non zero order. If there exists an equation (2.3) for Q, such that $r = s = 0$, then we clearly do have nothing to prove. In the other case, we may assume that among possible equations (2.3) for Q, we chose one, such that v is minimal, and we search for a contradiction.

We claim that without loss of generality, we may assume that $r = 1$. Clearly, $r = 0$ would contradict the minimality hypothesis for v. Assume that $r > 1$. Multiplying both sides of (2.3) by S_{P_1}, we have

$$\begin{aligned} H_C^{\boldsymbol{\alpha}} S_{P_1} Q &= \left(\sum_{i=1}^{r} \Phi_i S_{P_i}\right) \theta_1 P_1 + \sum_{j=1}^{s} \Phi'_j S_{P_1} \theta'_j P'_j + \sum_{k=1}^{t} \Phi''_k S_{P_1} P''_k + \\ & \sum_{i=1}^{r} \Phi_i (S_{P_1} \theta_i P_i - S_{P_i} \theta_1 P_1). \end{aligned}$$

By the previous lemma, the last term of the right hand member of this equation is in $[C]_{<v} : H_C^{\infty}$. Therefore, multiplying through both sides of the equation by $H_C^{\boldsymbol{\beta}}$, for some $\boldsymbol{\beta}$, we can rewrite this last term as a linear combination of θP's with $\theta P < v$. This proves our claim.

So let us assume that $r = 1$. We can write $\theta_1 P_1 = S_{P_1} v + R$, where v does not occur in R. Then $\sum_{j=1}^{s} \Phi'_j \theta'_j P'_j + \sum_{k=1}^{t} \Phi''_k P''_k$ can be considered as a polynomial in v of degree γ. Multiplying it by $S_{P_1}^{\gamma}$, and replacing $S_{P_1} v$ systematically by $\theta_1 P_1 - R$, we obtain a polynomial, which depends on $\theta_1 P_1$, but not on v. Thus, multiplying both sides of (2.3) by $S_{P_1}^{\gamma}$ and applying this transformation we get an equation

$$H_C^{\boldsymbol{\alpha}} S_{P_1}^{\gamma} Q = \widetilde{\Phi_1} \theta_1 P_1 + \sum_{j=1}^{s'} \widetilde{\Phi'_j} \theta'_j P'_j + \sum_{k=1}^{t'} \widetilde{\Phi''_k} P''_k,$$

with similar notations as in (2.3), and where the $\widetilde{\Phi'_j}$'s and the $\widetilde{\Phi''_k}$'s do not depend on v. Here we recall that the $\theta'_j P'_j$'s and the P''_k's do not depend on v (because the P''_k's are partially reduced w.r.t. C). Now $H_C^{\boldsymbol{\alpha}} S_{P_1}^{\gamma} Q$ does not depend on v (since Q is partially reduced w.r.t. C) so that $\widetilde{\Phi_1}$ is necessarily zero (recall that S_{P_1} is not a zero divisor). Hence, Q is in $[C]_{<v} : H_C^{\infty}$, which contradicts the minimality hypothesis of v. □

Corollary I. *The D-ideal $[C] : H_C^{\infty}$ is perfect resp. prime, if the ideal $(C) : H_C^{\infty}$ is radical resp. prime.*

Proof. Suppose that P and Q are in $A\{F\} \backslash [C] : H_C^{\infty}$. Then P `part-rem` C and Q `part-rem` C are not in $[C] : H_C^{\infty}$, and neither in $(C) : H_C^{\infty}$. If $(C) : H_C^{\infty}$ is prime, then (P `part-rem` C)(Q `part-rem` C) $\notin (C) : H_C^{\infty}$. By Rosenfeld's lemma, this implies (P `part-rem` C)(Q `part-rem` C) $\notin [C] : H_C^{\infty}$. Hence $PQ \notin [C] : H_C^{\infty}$. The proof for radical ideals is similar, by reasoning on P^{α}, instead of PQ. □

Corollary II. *The D-ideal $[C] : H_C^{\infty}$ is perfect.*

Proof. By the previous corollary, it suffices to prove that $(C) : H_C^{\infty}$ is a radical ideal. But this follows immediately from the fact that $(C) : S_C$ is a radical ideal, by proposition 2.8. □

2.7 The Boulier-Seidenberg-Ritt algorithm

In this section we present a membership test for finitely generated perfect D-ideals, due to Boulier (see [Boul 94], [BLOP 95]). Similar ideas were used by Seidenberg in order to establish a differential elimination theory (see [Seid 56], [Boul 94]). We will restrict our attention to finitely generated quasi-polynomial D-algebras over a field. More precisely, we will suppose that $\mathfrak{K}\{F\}$ is an **algorithmic quasi-polynomial D-$\mathfrak{K}$-algebra**. This means that all relevant operations are effective. Moreover, we assume that we dispose of an effective admissible ordering on Θ. Now testing whether $P \in \{\Sigma\}$ is equivalent to testing whether $(\Sigma, \{P\})$ admits a model, by proposition 2.6. We will use the second criterion for the membership test. .

In fact, we will give an algorithm, which we call the Boulier-Seidenberg-Ritt algorithm (Boulier calls it the Rosenfeld-Gröbner algorithm), which decomposes any system (Σ, T) of D-equations and D-inequations in a finite list of equivalent, more canonical systems. More precisely, we define a system (Σ, T) to be **regular**, if Σ is a coherent autoreduced set, such that $H_\Sigma \subseteq T$, and such that $\Sigma \backslash H_\Sigma = \{R\}$, where R is partially reduced w.r.t. Σ. If (Σ, T) is a regular, then we say that $\{\Sigma\} : T^\infty$ is a **regular D-ideal**. Whenever we speak about a regular D-ideal, we assume that we can represent it by a regular system.

We claim that a regular system (Σ, T) admits a model, if and only if (Σ, T) admits an algebraic model, that is, if the ideal $(\Sigma) : T^\infty$ of $\mathfrak{K}[V_\Sigma \cup V_T]$ does not contain 1. Indeed, this is an easy consequence of Rosenfeld's lemma combined with proposition 2.6. Moreover, $\{\Sigma\} : T^\infty$ is a radical ideal, by corollary II to Rosenfeld's lemma. Let P be any D-polynomial. We have $P \in \{\Sigma\} : T^\infty$, if and only if P `part-rem` Σ is in $(\Sigma) : T^\infty$, using Rosenfeld's lemma. By the usual Buchberger algorithm, we can compute a Gröbner base for $(\Sigma) : T^\infty \subseteq \mathfrak{K}[V_\Sigma \cup V_T]$. This is done by introducing a new formal variable w_Q for each Q in T. We then use an ordering such that each variable in $V_\Sigma \cup V_T$ is smaller than each w_Q. Finally, we compute a Gröbner base for $(\Sigma, \{v_Q Q - 1\}_{Q \in T})$ and take the intersection with $\mathfrak{K}[V_\Sigma \cup V_T]$. The obtained Gröbner base gives a membership test for $(\Sigma) : T^\infty$, and in particular we can decide whether $(\Sigma) : T^\infty$ contains 1.

As its name suggests, the Boulier-Seidenberg-Ritt algorithm has two main subalgorithms. The first subalgorithm reduces a system (Σ, T) of D-equations and D-inequations into an equivalent **semiregular system**, which is a system (Σ, T) to which is associated a coherent autoreduced subset C of Σ, such that all elements of Σ reduce to zero w.r.t. C. The second subalgorithm splits a semiregular system (Σ, T) up into a finite number $(\Sigma_1, T_1), \cdots, (\Sigma_\nu, T_\nu)$ of simpler systems, which form a decomposition for (Σ, T). Repeating these two subalgorithms, we ultimately end up with a decomposition of the initial system into a finite number of regular systems.

Subalgorithm `reduce`(Σ, T).
INPUT: A finite system of D-equalities $\Sigma \subseteq \mathfrak{K}\{F\}$ and D-inequalities $T \subseteq \mathfrak{K}\{F\}$.
OUTPUT: A triple (Σ', T, C), where (Σ', T) is an equivalent semiregular system, with C as associated coherent autoreduced set.

$\Sigma' := \Sigma$
repeat
  • Let C be a minimal coherent autoreduced subset of Σ'.
  $E := (\Sigma' \cup \{\Delta(P, Q) | P, Q \in C\}) \backslash C$, *flag*:=**true**
  for $P \in E$ **do**
    $R := P$ `rem` C
    if $R \neq 0$ **then** $\Sigma' := \Sigma' \cup \{R\}$, *flag*:=**false**
until *flag*
return (Σ', T, C)

The termination of this subalgorithm follows from the fact that the ordering on autoreduced subsets of $\mathfrak{K}\{F\}$ is well founded. As to the correctness, it is clear that all new elements which are inserted into Σ' are in $\{\Sigma\}$ and at the end of the program, the set C is a coherent autoreduced subset of Σ', which reduces all elements of Σ' to zero. We remark that whenever P reduces to zero w.r.t. C, that is $H_C^{\boldsymbol{\alpha}} = \boldsymbol{\theta} C$, for some computable $\boldsymbol{\alpha}$ and $\boldsymbol{\theta}$, then P can optionally be eliminated from Σ', if $\{H | \boldsymbol{\alpha}(H) \neq 0\} \subseteq T$.

Subalgorithm `split`(Σ, T, C).
INPUT: On input we have a semiregular system (Σ, T), with associated coherent autoreduced set C.
OUTPUT: A decomposition of (Σ, T), given by a list of systems. Moreover, the first element in this list is a regular system.

• Enumerate $H_C = \{H_1, \cdots, H_\nu\}$.
$\Sigma_0 := C$
$T_0 := H_C \cup \{(\prod_{P \in T \backslash H_C} P)$ `part-rem` $C\}$
for $i := 1$ **to** ν **do**
  $\Sigma_i := \Sigma \cup \{H_i\}$
  $T_i := T \cup \{H_{i+1}, \cdots, H_\nu\}$
return $((\Sigma_0, T_0), \cdots, (\Sigma_\nu, T_\nu))$

The correctness of this algorithm relies on the simple fact that an element of a field is either zero or non zero. Hence, if φ is any morphism over $\mathfrak{K}$ of $\mathfrak{K}\{F\}$ into a D-superfield L, then we have either $\varphi(H_1) \neq 0, \cdots, \varphi(H_\nu) \neq 0$, or $\varphi(H_i) = 0$ and $\varphi(H_{i+1}) \neq 0, \cdots, \varphi(H_\nu) \neq 0$, for exactly one index i. The system (Σ_0, T_0) is regular, by definition. We remark that for each system (Σ_i, T_i), with $i > 0$, there exists an autoreduced subset of Σ_i, which is smaller than C.

Algorithm `B-S-R`(Σ, T).
INPUT: A system (Σ, T) of D-equalities and D-inequalities.
OUTPUT: A list $((\Sigma_0, T_0), \cdots, (\Sigma_\nu, T_\nu))$ of non contradictory regular systems, whose elements form a decomposition of (Σ, T).

$L := ()$, $M := ((\Sigma, T))$
while $M \neq ()$ **do**
  $(\Sigma', T') :=$ `first`(M)
  $M :=$ `concat(split(reduce(`Σ', T'`))`$, M)$
  $(\Sigma', T') :=$ `first`(M)
  if `consistent`(Σ', T') **then** `insert`$(L, (\Sigma', T'))$
return L

Remark 2.3. The subalgorithm `first` takes out the first element of a list, the subalgorithm `insert` inserts a new element at the end of a list, and the subalgorithm `concat` concatenates two lists. Finally, the subalgorithm `consistent`(Σ', T') checks whether (Σ', T') is algebraically consistent. It starts by checking whether Σ' contains an element of $\mathfrak{K}$, which would trivially yield a contradiction.

Let us now prove the termination of `B-S-R`. Encode the reduce and splitting process by a tree labeled by systems of D-equalities and D-inequalities; the root of this tree is the initial system, and the children of a node are the systems we obtain by applying `reduce` and then `split` on it. None of the branches of this tree may be infinite, because the ordering on autoreduced sets is well founded. By Königs lemma, we conclude that the tree is finite (see also [Boul 94], p 44, p 71). The correctness of `B-S-R` follows trivially from the correctness' of the subalgorithms `reduce` and `split`.

Let $((\Sigma_1, T_1), \cdots, (\Sigma_k, T_k))$ be the output of the algorithm. By the corollary to proposition 2.6, a D-polynomial P is in $\{\Sigma\} : T^\infty$, iff $\varphi(P) = 0$ for every model φ for (Σ, T). Now φ is a model for (Σ, T), iff φ is a model for one of the (Σ_i, T_i)'s. Therefore, $\varphi(P) = 0$ for every model φ for (Σ, T), iff for each i we have $\varphi(P) = 0$, for every model φ for (Σ_i, T_i). Applying the corollary to proposition 2.6 once again, we have proved

$$\{\Sigma\} : T^\infty = \{\Sigma_1\} : T_1^\infty \cap \cdots \cap \{\Sigma_k\} : T_k^\infty.$$

As we have an effective membership test for each $\{\Sigma_i\} : T_i^\infty$, we have one for $\{\Sigma\} : T^\infty$. The perfect D-ideals $\{\Sigma_i\} : T_i^\infty$ in this decomposition are regular.

2.8 On effective prime decomposition

Considering the Ritt-Raudenbush theorem and proposition 2.10, it would be nice to have an algorithm, which performs the prime decomposition of a finitely generated perfect D-ideal automatically. Clearly, in order to answer this question, we have to be able to deal with the algebraic case. Now it is known (see [VdW 30]), that the problem of effective algebraic prime decomposition can be solved, if we have a factorization algorithm for univariate polynomials over $\mathfrak{K}$. From now on, we assume that this is the case.

Under the above assumption, the effective prime decomposition problem remains open. Nevertheless, we will show that there is an algorithm for "semi prime decomposition". By this, we mean, that given a finitely generated perfect D-ideal I, we can compute prime D-ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$, such that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_p$, where each $\mathfrak{p}_i$ is a regular ideal. The harder question is which terms are superfluous in this decomposition, because no test is known to decide whether $\mathfrak{p}_i \subseteq \mathfrak{p}_j$, even if the $\mathfrak{p}_i$'s are given by characteristic sets; this problem was raised by Kolchin (see [Kol 73], p. 166, problem 3). In this section we will give a list of equivalent problems.

Let us start by sketching a semi prime decomposition algorithm. This is done by adding a third subalgorithm `decompose` to the Boulier-Seidenberg-Ritt algorithm. This subalgorithm takes a regular system (Σ, T) on input, and returns (Σ, T), if $\{\Sigma\} : T^\infty$ is prime, and a finite list of systems $((\Sigma_1, T), \cdots, (\Sigma_\nu, T))$, such that $(\Sigma_1) : T^\infty, \cdots, (\Sigma_\nu) : T^\infty$ forms a prime decomposition of $(\Sigma) : T^\infty$ in $\mathfrak{K}[V_\Sigma \cup V_T]$. Here we have a prime decomposition algorithm in $\mathfrak{K}[V_\Sigma \cup V_T]$, by the above hypothesis. Finally, we modify the Boulier-Seidenberg-Ritt algorithm by inserting the lines $M := \mathtt{concat}(\mathtt{decompose}(\Sigma', T'))$ and $(\Sigma', T') := \mathtt{first}(M)$ into the algorithm. The termination of this modified algorithm is still assured by König's lemma and it returns a semi prime decomposition of (Σ, T).

Let us now discuss two interesting properties of the Boulier-Seidenberg-Ritt algorithm, due to Boulier, in the case that we have a prime D-ideal on input (i.e. a system (Σ, T), where $\{\Sigma\} : T$ is prime). First, we claim that the first element of the returned list is a system, which is equivalent to (Σ, T). Inspection shows, that it suffices to prove this for the subalgorithm `split`; we will adopt its notations. Let i be maximal, such that $H_i \in \{\Sigma\} : T^\infty$, allowing i to be -1. Then $(\Sigma_1, T_1), \cdots, (\Sigma_i, T_i)$ admit no models. Hence, $i < \nu$, because $\{\Sigma\} \neq \mathfrak{K}\{F\}$, and $T \notin \{\Sigma\} : T^\infty$. Therefore, $\Sigma_{i+1} \cdots \Sigma_\nu T \notin \{\Sigma\} : T^\infty$, since $\{\Sigma\} : T^\infty$ is prime, so that (Σ_{i+1}, T_{i+1}) admits a model. Moreover, $P \in \{\Sigma_{i+1}\} : T_{i+1}$ implies $PT_{i+1} \in \{\Sigma_{i+1}\} \subseteq \{\Sigma\} : T^\infty$, and $P \in \{\Sigma\} : T^\infty$, since $\{\Sigma\} : T^\infty$ is prime. This proves our claim.

A second, interesting property is that we can extract a characteristic set of a regular prime D-ideal, represented by a regular system. For this procedure, we refer to [Boul 94] and [BLOP 95]. We also remark that a prime D-ideal $\mathfrak{p}$, given by a characteristic set C, i.e. $\mathfrak{p} = \{C\} : H_C^\infty$, is a regular D-ideal; indeed, we have $H_C^{\mathbf{1}} \notin \mathfrak{p}$, by proposition 2.9(d). This shows, that it is equivalent to represent a prime D-ideal by a characteristic set or by a regular system. As we will see below, it is not known whether there exists an algorithm to extract a finite set of generators for a prime D-ideal, given by a characteristic set or a regular system.

We are now in a position to discuss effective prime decomposition and related problems. Recall that whenever we speak about regular D-ideals, we will always assume that they are represented by a regular system. In the case of regular prime D-ideals, we may equivalently represent them by characteristic sets. Similarly, we assume that any usual perfect D-ideal (i.e. without the regularity hypothesis) is given by a finite set of generators.

Theorem 2.2. *The following problems are equivalent to Kolchin's problem, whenever $\mathfrak{K}$ is an algorithmic field, such that we have a factorization algorithm for univariate polynomials over $\mathfrak{K}$:*

- *(a) Testing whether $\mathfrak{p} \subseteq \mathfrak{q}$, for regular prime D-ideals.*
- *(b) Finding the prime decomposition of a perfect D-ideal.*
- *(c) Testing whether a perfect D-ideal is prime.*
- *(d) Testing whether a regular prime D-ideal $\{\Sigma\} : T^\infty$ is generated by a finite subset Σ'.*
- *(e) Finding generators of a regular prime D-ideal.*
- *(f) Finding generators of the intersection $I \cap \mathfrak{K}\{E\}$ of a perfect D-ideal I and a polynomial D-subalgebra $\mathfrak{K}\{E\}$, where E is a strict subset of F.*

Proof. By definition, (a) is equivalent to Kolchin's problem. The implication (a) $\Rightarrow$ (b), follows from the semi prime decomposition algorithm. A perfect D-ideal is prime, iff its prime decomposition contains only one prime D-ideal; this proves (b) $\Rightarrow$ (c).

Now suppose that we have can solve (c) and let show how to solve (d). We can test whether $\{\Sigma'\}$ is prime. If this is not the case, then we certainly do not have $\{\Sigma\} : T^\infty = \{\Sigma'\}$. Assume that $\{\Sigma\}$ is prime and let P be in $\{\Sigma\} : T^\infty$, that is, $PT^{\boldsymbol{\alpha}} \in \{\Sigma\} \subseteq \{\Sigma'\}$ for some $\boldsymbol{\alpha}$. As $\{\Sigma\} : T^\infty$ is prime, we have $T \cap \{\Sigma\} : T^\infty = \phi$, whence $P \in \{\Sigma'\}$, since $\{\Sigma'\}$ is prime. Hence $\{\Sigma\} : T^\infty = \{\Sigma'\}$, and we are done.

Let us now assume (d) and let $\{\Sigma\} : T$ be a regular prime D-ideal. For each r, we can compute generators for the radical ideal $\mathrm{rad}(\Theta_r\Sigma) : T^\infty \subseteq \mathfrak{K}[V_{\Theta_r\Sigma} \cup V_T]$. For r sufficiently large, these generators also generate $\{\Sigma\} : T^\infty$ as a perfect D-ideal (here we use the fact the radical of a D-ideal in characteristic zero is perfect; for an easy to generalize proof, see for example [Kol 73], p 62, lemma 2). Because of (d), we have an effective test, for knowing whether r is sufficiently large. This proves (d) $\Rightarrow$ (e). We remark that more efficient algorithms can be given here.

Let us now prove (e) $\Rightarrow$ (a). Let $\mathfrak{p}$ and $\mathfrak{q}$ be two regular prime D-ideals. If (e) holds, then we can find a generating set Σ for $\mathfrak{p}$. In this case, $\mathfrak{p} \subseteq \mathfrak{q}$, if and only if $\Sigma \subseteq \mathfrak{q}$. We notice, that we have an effective membership test for $\mathfrak{q}$, since $\mathfrak{q}$ is regular.

We finally give the idea of the equivalence proof of (e) and (f). Seidenberg's elimination algorithm (see [Seid 56]) can be generalized in a straightforward way to our context, following the lines of Boulier (see [Boul 94]). In particular, given I and E like in (f), we can write the radical ideal $I \cap \mathfrak{K}\{E\}$ of $\mathfrak{K}\{E\}$ as a finite intersection of regular D-ideals. From this, we trivially deduce (e) $\Rightarrow$ (f). Inversely, a regular D-ideal $\{\Sigma\} : T^{\infty}$ can be interpreted as the intersection of $\mathfrak{K}\{F\}$ with $\{\Sigma, s_1Q_1 - 1, \cdots, s_kQ_k - 1\}$, where $s_1, \cdots, s_k$ are formal inverses of the elements $Q_1, \cdots, Q_k$ of T. □

Remark 2.4. It should be emphasized that in the case of linear D-equations, none of the above problems arise; in this case, all initials and separants are constants, and all regular ideals are of the form $\{\Sigma\} : T^{\infty}$, with $T = \phi$.

2.9 References

[BLOP 95] F. Boulier, D. Lazard, F. Ollivier, M. Petitot. Représentation du radical d'un idéal différentiel de type fini. *Proc. ISSAC 1995, Montreal.*

[Boul 94] F. Boulier. Étude et implantation de quelques algorithmes en algèbre différentielle. *PhD. Thesis, University of Lille I, France.*

[BrP 93] M. Bronstein, M. Petrovšek. On Ore rings, linear operators and factorization. *Technical Report 200, ETH Zürich.*

[Buch 65] B. Buchberger. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal. *PhD. thesis, University of Innsbruck.*

[Bui 92] A. Buium. Differential algebraic groups of finite dimension. *Lecture Notes in Mathematics 1506, Springer-Verlag.*

[Herz 34] F. Herzog. *Systems of algebraic mixed difference equations.* Proc. A.M.S. (p 286-300).

[Kol 73] E.R. Kolchin. *Differential algebra and algebraic groups.* Academic press, New-York.

[Krei 64] H.F. Kreimer. The foundations for an extension of differential algebra. *Transactions A.M.S. 111 (p 482-492).*

[Lip 89] L. Lipshitz. D-finite power series. *Journal of algebra 122 (p 353-373).*

[Mans 91] E. Mansfield. Differential Gröbner bases. *PhD. Thesis, University of Sydney, Australia.*

[NiWe 82] W. Nichols, B. Weisfeiler. Differential formal groups of J.F. Ritt. *Amer. Jour. Math. 104(5) (p 943-1005).*

[Ol 90] F. Ollivier. Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité. *PhD. Thesis, École Polytechnique, France.*

[Ore 33] O. Ore. Theory of non-commutative polynomials. *Annals of Math. 34 (p 480-508).*

[Raud 33] H.W. Raudenbush. Differential fields and ideals of differential forms. *Annals of mathematics, vol. 34.*

[Ritt 32] J.F. Ritt. *Differential equations from the algebraic standpoint.* Amer. Math. Soc. Coll. Publ. 14, New-York.

[Ritt 50] J.F. Ritt. *Differential algebra.* Amer. Math. Soc, New-York.

[Seid 56] A. SEIDENBERG. An elimination theorem for differential algebra. *Univ. California Publ. Math. (N.S.) (p 31-38).*

[VdH 93] J. VAN DER HOEVEN. Théorie des bases standard et séries Mahlériennes généralisées. *Unpublished D.E.A. report, Ecole Polytechnique, France.*

[VdW 30] B.L. VAN DER WAERDEN. *Moderne Algebra I.* Springer Verlag, Berlin.

[Wu 87] W.T. WU. A Zero structure theorem for polynomial equation solving and its applications. *Proceedings of ISSAC'88, Roma, Springer Verlag.*

Chapter 3

Generalized elimination theory

3.1 Introduction

Although the previous two chapters were exclusively concerned with differential equations, many of the techniques we have used can be generalized to the case of difference equations, mixed differential difference equations, and even more general equations. This raises the question what is the most general setting in which a systematic elimination theory exists.

From a theoretical point of view, the generalization of Ritt-reduction to difference and mixed differential-difference equations started shortly after the appearance of the Ritt-Raudenbush theorem (e.g. see [Herz 34]). More general types of operator algebras have been considered by Kreimer (see [Krei 64]), although the emphasize rather lies on extensions of Picard-Vessiot theory than reduction theory in his work.

The effective elimination theory for differential and difference equations started only much later: Galligo was the first to consider Buchberger's algorithm in the context of linear differential operator rings (see [Gal 85]). Kandry-Rodi and Weispfennig gave conditions under which Buchberger's classical algorithm naturally extends to the non-commutative case (see [KRW 86]). These conditions were weakened by the author in his D.E.A. report (see [VdH 93]). The linear case has given rise to several implementations (see [KRW 86], [SZ 92], [Tak 93], [BrP 93], [Chyz 95]).

As to algebraic differential and difference equations, only the classical setting of differential equations with commutative derivations has been considered until now (see [Ol 90], [Mans 91], [Boul 94], [BLOP 95]). Moreover, Boulier's algorithm has been implemented (see [Boul 94]). In this chapter, we generalize the theory from the previous chapter to a setting as general as possible. However, no implementations are available yet.

Despite the efforts to generalize elimination theory to the case of mixed differential-difference equations, most functional equations involving composition — even linear equations — can not be treated by the generalized theory. For instance, equations like

$$a(x)f(x+1) + b(x)f(x^2+x^3) + c(x)f(x) = d(x),$$

which involve non-commutative difference operators, cannot usually be treated. Essentially, mixed differential-difference elimination theory mainly applies to shift- and q-operators.

Let us now describe the contents of this chapter. In section 3.2, we sketch a setting as general yet simple as possible for dealing with non commutative linear operators, to which the usual Buchberger algorithm can be extended naturally. Essentially, we restate the main results from [VdH 93] in a slightly simpler nomenclature. We intend to rework the proofs of these results in a forthcoming paper. Our setting incorporates most of the previous settings, such as the algebras of solvable type (see [KRW 86]) and Ore algebras (see [Chyz 95]). However, contrary to Kandry-Rodi and Weispfennig we only consider left ideals, although it should be possible to treat bilateral ideals as well, following the approach in [KRW 86].

In section 3.3, we study the generalization of the results from chapter 2 to the case of certain types of DD-rings. DD-rings are rings with a mixed differential-difference structure. For reduction purposes, the difference operators need to commute up to some finite non commutative group. Because of the high degree of generality, this section has become quite technical. We intend to treat the special case of commutative difference operators in a forthcoming paper.

3.2 Linear non commutative reduction theory

3.2.1 Reduction algebras of finite type

In all what follows, rings A are not necessarily commutative, but always unitary, and by ideals we will always mean left ideals. Furthermore, A always acts on modules and algebras on the left, and A-algebras are always assumed to be unitary. We say that a ring resp. module is **Noetherian**, if its ideals resp. sub-modules verify the ascending chain condition.

Let B be an A-algebra, which admits a basis $\Theta \ni 1$, when considered as an A-module. Fix a total ordering on X. Then the support (w.r.t. X) of any non zero element $P \in B$ admits a unique maximal element l_P, which is called the **leading monomial** of P. The coefficient $c_P = P_{l_P}$ of this monomial is called the **leading coefficient** of P. By convention, we take $l_0 = -\infty$ and $c_0 = 0$.

We say that B is a **reduction algebra** over A, if the ordering $\leqslant$ is **admissible** in the following sense:

A0. For all $x, y \in B$, there exists a unit $u \in B^*$ with $c_{xy} = uc_xc_y$.
A1. $1 \leqslant \theta$ for all $\theta \in \Theta$.
A2. $\theta \leqslant \xi \ \wedge \ \theta' \leqslant \xi' \Rightarrow l_{\theta\theta'} \leqslant l_{\xi\xi'}$, for all $\theta, \theta', \xi, \xi' \in \Theta$.
Equality holds if and only if $\theta = \xi$ and $\theta' = \xi'$.

We notice that **A0** is in particular satisfied if A is a field. Furthermore, if $\leqslant$ is admissible, then the operator $\delta_\theta : A \to A; a \mapsto c_{\theta a}$ is a difference operator for all $\theta \in \Theta$. If the additional condition

A3. $l_{\theta\theta'} = l_{\theta'\theta}$, for all $\theta, \theta' \in \Theta$.

is satisfied, then we say that B is a **quasi-commutative algebra**. Most of the natural examples of reduction algebras are actually quasi-commutative.

To the ordering $\leqslant$ on Θ we can naturally associate a partial ordering $\preccurlyeq$ by

$$\theta \preccurlyeq \theta' \Leftrightarrow \exists \xi \in \Theta \quad \theta' = l_{\xi\theta}.$$

We call $\preccurlyeq$ the **divisibility ordering** on Θ. If $\leqslant$ is admissible, and if $\preccurlyeq$ is a Noetherian ordering, then we say that B is a quasi-commutative algebra **of finite type** over A. Usually, the ordering $\preccurlyeq$ is isomorphic to a power $\mathbb{N}^n$ of $\mathbb{N}$.

The usual reduction theory from commutative algebra generalizes to reduction algebras of finite type. In particular, we have the following generalization of Hilbert's basis theorem:

Theorem 3.1. *Let A be a Noetherian ring and B a reduction algebra of finite type over A. Then B is Noetherian.*

Let us now give some examples of reduction algebras of finite type.

Example 3.1. Let (A, D) be a (finite dimensional) D-ring. Then the free linear D-operator algebra $\Omega = A[D]$ from section 1.2.4 is a quasi-commutative algebra of finite type over A.

Example 3.2. Let (A, Δ) be a (classical) difference ring, such that $\delta a \in aA^*$ for each $\delta \in \Delta$ and $a \in A$. Then the free linear difference operator algebra $\Omega = A[\Delta]$ (which is constructed in a similar fashion as free linear D-operator algebras) is a quasi-commutative algebra of finite type over A.

We recall that (A, Δ) is a difference ring, if $\Delta = \{\delta_1, \cdots, \delta_n\}$ is a finite set of pairwise commutating difference operators (i.e. injective ring homomorphisms) acting on A. Geometrically, difference operators correspond to right compositions with a fixed function. The most classical difference operators are the **shift operator** $S_x : f(x) \mapsto f(x+1)$, the q-**operator** $Q_{x,q} : f(x) \mapsto f(qx)$ and the **Mahlerian operator** $M_{x,p} : f(x) \mapsto f(x^p)$.

Example 3.3. A univariate Ore-extension of A is a ring $B = A[\delta]$, where δ satisfies the following commutation rule w.r.t. elements $a \in A$:

$$\delta a = \sigma(a)\delta + d(a).$$

Here σ is a difference operator and d a σ-derivation:

$$d(ab) = \sigma(a)db + bda,$$

for all $a, b \in A$. An Ore-algebra over A is an algebra obtained from A by a finite number of univariate Ore-extensions. Ore-algebras are in particular quasi-commutative algebras of finite type.

Example 3.4. Let K be a field and $q \in K^*$. The **quantum plane** is an abstract object with coordinate functions x and y that commute via the law $yx = qxy$ (see [Man 88]). Those linear transformations which respect this commutation law, can be represented by **q-matrices**, which are 2×2 matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

whose entries satisfy the following commutation laws:

$$\begin{cases} ba = qab; \\ dc = qcd; \\ ca = qac; \\ bd = qdb; \\ cb = bc; \\ da = ad + (q - q^{-1})bc. \end{cases}$$

Taking $\Theta = a^{\mathbb{N}} b^{\mathbb{N}} c^{\mathbb{N}} d^{\mathbb{N}}$, we have the following (orderly) admissible ordering on Θ:

$$1 < b < c < a < d < \cdots < bc < \cdots < ad < \cdots.$$

In particular, $K[a, b, c, d]$ is a quasi-commutative algebra of finite type over K.

Example 3.5. Not all reduction algebras of finite type are quasi-commutative. Consider for instance the algebra $K[x, y]$ over a commutative field, with $yx = xy^2$ and the lexicographical admissible ordering on $x^{\mathbb{N}} y^{\mathbb{N}}$:

$$1 < x < x^2 < \cdots < y < xy < \cdots.$$

Then $K[x, y]$ is a reduction algebra of finite type over K, which is clearly not quasi-commutative.

Example 3.6. The partial ordering $\preccurlyeq$ on Θ is not necessarily isomorphic to $\mathbb{N}^n$ for some n, as the above example shows already. Other interesting partial orderings are obtained, even in the fully commutative case, by considering polynomial algebras in finitely generated submonoids of $\mathbb{N}$, such as $B = K[x^2, xy, y^2]$. In such cases, two elements in B may admit a set of S-polynomials instead of a unique S-polynomial in Buchberger's algorithm (see also [Ol 90]).

Example 3.7. The setting of reduction algebras allows to construct towers of extensions in several ways. First, we may consider reduction algebras over reduction algebras, and construct towers like

$$A \subset A[x] \subset A[x, \partial_x] \subset A[x, \partial_x, S_x].$$

Secondly, in the case of D-equations for instance, we may enrich A with the solutions of a system of D-equations. In this case, we obtain towers like

$$A[x] \subset A[x, \sin x] \subset A[x, \sin x, e^{\sin x}].$$

3.2.2 Groebner algebras

Now let $\mathfrak{A}$ be an effective (not necessarily commutative) ring. We will say that $\mathfrak{A}$ is an **effective Noetherian ring**, if $\mathfrak{A}$ is Noetherian and the following conditions are satisfied:

NR1. There exists an algorithm which given $a_1, \cdots, a_k, b \in \mathfrak{A}$ tests whether $b \in (a_1, \cdots, a_k)$ and determines elements $c_1, \cdots, c_k$ with $b = c_1 a_1 + \cdots + c_k a_k$ if this is the case.

NR2. Each prime component of the zero ideal of $\mathfrak{A}$ is given explicitly.

NR3. There exists an algorithm to compute the intersection of any two ideals $\mathfrak{i}, \mathfrak{j}$ of $\mathfrak{A}$.

In conditions **NR2** and **NR3**, we understand that ideals are effectively represented by sets of generators. (Left) Noetherian A-modules M resp. effective Noetherian A-modules $\mathfrak{M}$ are defined in a similar way, by considering A-submodules instead of ideals.

The following property of effective Noetherian rings is equivalent to **NR3**:

Proposition 3.1. *Let $\mathfrak{A}$ be an effective Noetherian ring. Then there exists an algorithm to compute the kernel of any linear form $\mathfrak{A}^n \to \mathfrak{A}$.*

Effective Noetherian rings are precisely those objects which allow the most common algebraic operations to be carried out effectively. For instance, we have:

Proposition 3.2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be effective Noetherian rings. Then:*

(a) $\mathfrak{A} \times \mathfrak{B}$ is an effective Noetherian ring.

(b) If $\mathfrak{i}$ is an ideal of $\mathfrak{A}$, then $\mathfrak{A}/\mathfrak{i}$ is an effective Noetherian ring.

(c) If $\varphi : \mathfrak{A} \to \mathfrak{B}$ is an effective morphism, then there are algorithms to compute $\varphi(\mathfrak{i})$ and $\varphi^{-1}(\mathfrak{j})$, for ideals $\mathfrak{i} \subseteq \mathfrak{A}$ resp. $\mathfrak{j} \subseteq \mathfrak{B}$.

Let $\mathfrak{A}$ be an effective Noetherian ring and let $\mathfrak{B}$ be a reduction algebra of finite type over $\mathfrak{A}$. We say that $\mathfrak{B}$ is a **Groebner algebra**, if each element in $\mathfrak{B}$ can be effectively decomposed w.r.t. Θ, if $\leqslant$ is effective, and if $\preccurlyeq$ is an effective Noetherian ordering. Here an effective Noetherian ordering is a Noetherian ordering, such that there exists an algorithm to compute intersections of final segments (actually, we also require that there exist algorithms to compute the minimal elements and the successor of each element, but this is not of importance to us here).

We were not able to prove the following conjecture in [VdH 93]:

Conjecture 3.1. *Let (A, δ) be a Noetherian difference ring and let $\varphi : A^n \to A$ be a linear form. If G generates $\ker \varphi$, then $\delta(G)$ generates $\ker \varphi \circ (\delta, \cdots, \delta)$.*

The conjecture obviously holds, if δ is invertible, or A is a commutative field. Now if $\mathfrak{B}$ is a Groebner algebra over $\mathfrak{A}$, such that the conjecture holds for all δ_θ's with $\theta \in \Theta$, then Buchberger's algorithm generalizes to the present setting. This yields:

Theorem 3.2. *Let $\mathfrak{B}$ be a Groebner algebra over $\mathfrak{A}$. With the above notations, assume that for each linear form $\varphi : \mathfrak{A}^n \to \mathfrak{A}$ and each $\theta \in \Theta$, the set $\delta_\theta(G)$ generates $\ker \varphi \circ (\delta_\theta, \cdots, \delta_\theta)$, whenever G generates $\ker \varphi$. Then $\mathfrak{B}$ is an effective Noetherian ring.*

3.3 DD-rings

In this section we will generalize Ritt reduction to systems of mixed differential difference equations of a certain type. Assume that (A, D) is a D-ring, endowed with a semigroup Δ of difference operators acting on A, and with an additional commutation mapping $D \times \Delta \to D; (d, \delta) \mapsto d_\delta$, which has a inverse $d \mapsto d_{\delta^{-1}}$ for fixed δ and which satisfies

$$\begin{aligned} d_\delta \delta a &= \delta d a; \\ d_{Id} &= d; \\ d_{\delta\delta'} &= (d_{\delta'})_\delta; \\ [d, d']_\delta &= [d_\delta, d'_\delta]; \\ (ad)_\delta &= (\delta a) d_\delta \end{aligned}$$

for each $d, d' \in D$, $\delta, \delta' \in \Delta$ and $a \in A$. A triple (A, D, Δ), verifying the above conditions is said to be a **DD-ring**. We will again denote by Ω the corresponding DD-operator algebra; that is, the free associative generated by A, D and Δ, subject to the natural laws. Finally, for convenience, D and Δ are always assumed to be finitely generated.

Example 3.8. Geometrically, difference operators correspond to right compositions with a fixed function. It is easily verified that the commutation conditions from above are satisfied for such difference operators. The difference operators of main interest are the **shift operator** $S_x : f(x) \mapsto f(x+1)$, the **$q$-operator** $Q_{x,q} : f(x) \mapsto f(qx)$ and the **Mahlerian operator** $M_{x,p} : f(x) \mapsto f(x^p)$.

3.3.1 Perfect DD-ideals and Ritt DD-rings

There are two main problems if we want to extend our results to this new context. First, we have to extend our results about perfect ideals, and secondly we have to establish an appropriate reduction theory. Now ordinary radical DD-ideals, do not satisfy the properties from section 2.3 in general. Therefore, a DD-ideal I is defined to be **perfect**, if $\prod_{\delta\in\Delta}(\delta a)^{k_\delta} \in I \Rightarrow a \in I$, for each a in A and all families of natural numbers $\{k_\delta\}$, with finite support. An equivalent condition is that $a^2 s \in I \Rightarrow (\omega a)s \in I$, for every $a, s \in I$ and $\omega \in D \cup \Delta$. This second condition shows us at once that if I is a perfect DD-ideal, then so is $A : s$, for any $s \in A$. Hence, all results from section 2.3 generalize to the present context.

Unfortunately, in order to generalize Ritt's reduction theory, one is forced to make some additional hypothesis on the DD-ring A. We say that A is a **Ritt DD-ring**, if there are subsets Δ_g and Δ_c of Δ, such that the following conditions are satisfied:

R1. If $D \neq \{0\}$, then A contains $\mathbb{Q}$.
R2. Δ_g is a finite group.
R3. Δ_c is a commutative monoid.
R4. For any $\delta_c \in \Delta_c$ we have $\delta_c\Delta_g = \Delta_g\delta_c$.
R5. Any $\delta \in \Delta$ can be uniquely decomposed as $\delta = \delta_g\delta_c \in \Delta_g\Delta_c$.

From now on we will assume that A is a Ritt DD-ring. As before, we will assume that D is freely generated by $d_1, \cdots, d_n$. We will also assume that Δ_c is freely generated, say by $\delta_1, \cdots, \delta_m$. For simplicity, we will only study the case in which $\Delta_g = \{1\}$, although some brief indications about to treat the general case will be made in section 3.3.7

Remark 3.1. Our study will not loose in generality, if we assume that Δ_c is freely generated by $\delta_1, \cdots, \delta_m$. Indeed, we will be considering systems of DD-equations in $A\{F\}$ below. If we have a relation $\delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} = \delta_1^{\beta_1} \cdots \delta_m^{\beta_m}$, if suffices to add the equations $\delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} f = \delta_1^{\beta_1} \cdots \delta_m^{\beta_m} f$ to the system we are considering, for each $f \in F$.

3.3.2 Polynomial DD-algebras

We need to introduce polynomial DD-algebras. We denote

$$\Theta = \{\delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} d_1^{\beta_1} \cdots d_n^{\beta_n} | \alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n \in \mathbb{N}\}.$$

If F is a finite set, then $A[\Theta F]$ can naturally be given the structure of a polynomial DD-algebra. Again it is possible to impose alternative commutation rules $[d_i, d_j], (d_i)_{\delta_j}, (d_i)_{\delta_j^{-1}} \in A[F](d_1, \cdots, d_n)$, assuming that they extend the commutation rules defined on A. Doing this, we obtain quasi polynomial DD-algebras. As before the orders of DD-polynomials and DD-operators are defined in a natural way.

An important change with respect to the differential case is that shuffles are a bit more tricky to define. In fact, a **shuffle** of a word with letters in $D \cup \Delta$ is obtained by repeated transpositions of adjacent letters, except in the case of a derivation d and a difference operator δ, which commute following the law $d_\delta \delta = \delta d$. Hence, the letters of a shuffle of a word may be distinct from the original letters. If ω is a word of length r and ω' a shuffle of ω, then $\omega' - \omega$ has order at most $r-1$.

As we will be shuffling elements of Θ a lot, it will be convenient to introduce some more notations. We first define the partial ordering $\preceq$ on Θ by

$$\theta = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} d_1^{\beta_1} \cdots d_n^{\beta_n} \preceq \delta_1^{\alpha'_1} \cdots \delta_m^{\alpha'_m} d_1^{\beta'_1} \cdots d_n^{\beta'_n} = \theta',$$

if and only if $\alpha_1 \leqslant \alpha'_1, \cdots, \alpha_m \leqslant \alpha'_m$ and $\beta_1 \leqslant \beta'_1, \cdots, \beta_n \leqslant \beta'_n$. If this is the case, putting $\delta = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m}$, we denote

$$\theta'/\theta = \delta_1^{\alpha'_1 - \alpha_i} \cdots \delta_m^{\alpha'_m - \alpha_m} d_{1,\delta}^{\beta'_1 - \beta_1} \cdots d_{n,\delta}^{\beta'_n - \beta_n}.$$

Then $(\theta'/\theta)\theta$ is a shuffle of θ'. The set of words θ'/θ so obtained will be denoted by $\breve{\Theta}$. Whenever we will write $\breve{\eta}\theta$, with $\breve{\eta} \in \breve{\Theta}$, we implicitly assume that $\breve{\eta}$ is of the form θ'/θ, so that $\breve{\eta}\theta$ is a shuffle of an element of Θ. In case of ambiguity, we will also write $\breve{\eta} = \eta_\theta$. We remark that to any $\eta = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} d_1^{\beta_1} \cdots d_n^{\beta_n}$ in Θ there corresponds a $\breve{\eta} = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} d_{1,\delta}^{\beta_1} \cdots d_{n,\delta}^{\beta_n}$ in $\breve{\Theta}$, such that $\breve{\eta}\theta$ is in Θ.

3.3.3 Admissible orderings

Let ΘF be totally ordered by $\leqslant$ and define leaders as before. Then $\leqslant$ is said to be **admissible**, if

A1. $v(\theta f) < v(\breve{d}_i \theta f)$, for any i and $\theta f \in \Theta F$;
$v(\theta f) < v(\delta_i \theta f)$, for any i and $\theta f \in \Theta F$.

A2. $v(d_{i,\theta'} \theta f) \leqslant v(d_{i,\theta'} \theta' f')$, for any i and $\theta f \leqslant \theta' f'$ in ΘF;
$v(\delta_i \theta f) \leqslant v(\delta_i \theta' f')$, for any i and $\theta f \leqslant \theta' f'$ in ΘF.

A3. $v(\breve{d}_i \breve{d}_j \theta f) = v(\breve{d}_j \breve{d}_i \theta f)$, for any i, j and $\theta f \in \Theta F$.

Again, admissible orderings exist. For instance, enumerating $F = \{f_1, \cdots, f_k\}$, one can take the lexicographical ordering on the $\delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} d_1^{\beta_1} \cdots d_n^{\beta_n} f_i$'s, by ordering successively on order, $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_{n-1}$ and i.

The next problem we have to handle is the fact that $\deg \delta P = \deg P$, for difference operators δ. Hence if P and Q are DD-polynomials with $v_P \succ v_Q$, then P can not necessarily be reduced w.r.t. Q. This makes the usual partial ordering on ΘF inadequate for our purposes. The solution to this dilemma is to take into account the leaders of DD-polynomials, together with their degrees. This leads to the notion of an **extended variable**, which is an element of ΘF raised to some strictly positive power. The set of such variables will be denoted by $(\Theta F)^*$, and we use letters with star exponents v^* to denote extended variables. The **extended leader** of a non ground DD-polynomial P is denoted by $v_P^* = v^*(P) = v_P^{\deg P}$. Finally, we introduce **extended operators** as being operators of the form $v^*\breve{\eta}$, which act on DD-polynomials P, with $v = \breve{\eta} v_P$. The set of such operators is denoted by $\breve{\Theta}^*$, and we use names like $\breve{\eta}^*$ to denote such operators themselves.

We define a partial ordering $\preceq$ on extended variables by $v^* = (\theta f_i)^\gamma \preceq (\theta' f_{i'})^{\gamma'} = (v')^*$, if and only if $i = i'$, $\theta \preceq \theta'$ and either $\gamma \leqslant \gamma'$, or θ'/θ is not a pure difference operator. If this is the case, we denote by $(v')^*/v^*$ the extended operator $v^{\gamma' - \deg(\theta'/\theta)v^*}(\theta'/\theta)$. Then the extended leader of $((v')^*/v^*)v^*$ is $(v')^*$. We remark that $\preceq$ is still a well-quasi-ordering. We also extend the admissible ordering $\leqslant$ on variables to extended variables by $v^\gamma \leqslant (v')^{\gamma'}$, if and only if either $v < v'$, or $v = v'$ and $\gamma \leqslant \gamma'$. Finally, let Σ be a set of non ground polynomials and v^* an extended variable. Then we define

$$[\Sigma]_{v^*} = \left\{ \sum_i \Lambda_i \breve{\theta}_i P_i \middle| \breve{\theta}_i \in \breve{\Theta} \ \wedge \ P_i \in \Sigma \ \wedge \ \Lambda_i \in A[\Theta F \backslash \{v_{\breve{\theta}_i P_i}\}] \ \wedge \ v^*(\breve{\theta}_i P_i) \leqslant v^* \right\}.$$

3.3.4 Ritt reduction

Before introducing the generalization of Ritt reduction, let us define $H_\Sigma = \Delta \breve{H}_\Sigma$, where $\breve{H}_\Sigma = I_\Sigma \cup S_\Sigma$, for any finite set Σ of non ground DD-polynomials. In the pure difference case, i.e. $D = \{0\}$, one may even take $\breve{H}_\Sigma = I_\Sigma$, and the hypothesis that $\mathbb{Q} \subseteq A$ becomes superfluous. However, there is no equivalent for corollary II of Rosenfeld's lemma in this case. For simplicity, we assume from now on that $\mathbb{Q} \subseteq A$, and we take $\breve{H}_\Sigma = I_\Sigma \cup S_\Sigma$. We also remark that although H_Σ is infinite in general, $\breve{H}_\Sigma$ is finite. The key reason why Ritt's reduction theory extends to the DD-case, is that $H_\Sigma^{\boldsymbol{\alpha}} \in I \Rightarrow \breve{H}_\Sigma^{\mathbf{1}} \in I$, for any perfect DD-ideal I and all $\boldsymbol{\alpha}$.

Using the notion of extended leaders, Ritt's reduction principles can now be stated quite elegantly. A DD-polynomial P is said to be reduced w.r.t. a finite subset Σ of $A\{F\}\backslash A$, if there exists no $Q \in \Sigma$ and $w^* \in V_P^*$, with $v_Q^* \preceq w^*$. Here V_P^* denotes the set of extended variables occurring in P. We claim that in general, there exist $\boldsymbol{\alpha}, \boldsymbol{\omega}$ and R verifying (2.2), such that R is reduced w.r.t. Σ, and such that $\boldsymbol{\omega} P \in [\Sigma]_{v_P^*}$. This is proved in the same way as before, by replacing the main loop of the reduction procedure by the following:

while $\exists \Phi \in \Sigma \exists w^* \in V_R^* \ \ v_\Phi^* \preceq w$ **do**
- Choose w^* for $\leqslant$.

$R :=$ `Euclidean_division`$(R, (w/v_\Phi)\Phi)$

Remark 3.2. In the case when $\Delta_g \neq \{1\}$, we define $\hat{\Theta} = \Delta_g \Theta$. Shuffles are defined in a similar way as before, but for the partial ordering $\preceq$ we demand that $\hat{\theta}'/\hat{\theta} \in \breve{\Theta}$, whenever $\hat{\theta} \preceq \hat{\theta}'$. For example, if $\Delta_g = \{Id, \tau\}$ and $\Delta_c = (\delta_1)$ commute, then $Id \preceq \delta_1$, but $\tau \not\preceq \delta_1$. The admissible ordering is fixed on $\hat{\Theta}F$, and the admissibility conditions are the same, modulo putting hats on the θ's.

3.3.5 The Ritt-Raudenbush theorem

As before, a subset $\Sigma \subseteq A\{F\}\backslash A$ is said to be **autoreduced**, if each $P \in \Sigma$ is reduced w.r.t. $\Sigma\backslash\{P\}$. Let $\Sigma = \{P_1, \cdots, P_p\}$ and $T = \{Q_1, \cdots, Q_q\}$ be autoreduced subsets of $A\{F\}$, with $v_{P_1} < \cdots < v_{P_p}$ and $v_{Q_1} < \cdots < v_{Q_q}$. We define a partial ordering $\leqslant$ on autoreduced sets by $\{P_1, \cdots, P_p\} < \{Q_1, \cdots, Q_q\}$, if $v^*_{P_i} = v^*_{Q_i}$, for i strictly inferior to a certain j, and either $v^*_{P_j} < v^*_{Q_j}$, or $j = q + 1 \leqslant p$. It is readily verified that $\leqslant$ is a well founded. Characteristic sets are defined in the same way as before, and we have the analogue of proposition 2.9, when replacing H_C by $\breve{H}_C$ in statement (d). Consequently, the proof of the Ritt-Raudenbush theorem goes through modulo some trivial changes.

3.3.6 The Boulier-Seidenberg-Ritt algorithm

In order to generalize the Boulier-Seidenberg-Ritt algorithm, we now have to generalize Rosenfeld's lemma. Supposing that we have done this, the only change we will have to make in Boulier's algorithm, is to perform the splittings on the elements of $\breve{H}_C$ instead of H_C. Our results on prime decomposition also go through modulo a generalization of Rosenfeld's lemma.

Let Σ be an autoreduced set, let $P \neq Q$ be in Σ, and let v^* be an extended variable, with $v^*_P \prec v^*$ and $v^*_Q \prec v^*$. We define the **Δ-polynomial** of P and Q **relative to** v^* by

$$\Delta_{v^*}(P,Q) = I_{(v/v_Q)Q}(v^*/v^*_P)P - I_{(v/v_P)P}(v^*/v^*_A)Q$$

We define $v^*_P \wedge v^*_Q$ to be the smallest extended variable v^*, with $v^*_P \prec v^*$ and $v^*_Q \prec v^*$. We say that Δ_{v^*} is a **principal Δ-polynomial**, if either $v^* = v^*_P \wedge v^*_Q$, or $v^* = \breve{d}_i(v_P \wedge v_Q)$, for some i, and $(v^*_P \wedge v^*_Q)/v^*_P$ or $(v^*_P \wedge v^*_Q)/v^*_Q$ is an extended difference operator. In the pure differential or difference case, we remark that there is only one principal Δ-polynomial. Now Σ is said to be **coherent**, if all principal Δ-polynomials of elements of Σ reduce to zero with respect to Σ.

We will again need some preliminaries in order to prove the generalization of Rosenfeld's lemma. If Q is any D-polynomial in $A\{F\}\backslash A$, then we denote

$$[\Sigma]_Q = \left\{ \textstyle\sum_i \Lambda_i \breve{\theta}_i P_i \,\middle|\, \breve{\theta}_i \in \breve{\Theta} \ \wedge\ P_i \in \Sigma \ \wedge\ \Lambda_i \in A[\Theta F \backslash \{v_{\breve{\theta}_i P_i}\}] \ \wedge\ v^*(\breve{\theta}_i P_i) \leqslant v^*_Q \right\};$$
$$[\Sigma]_{<Q} = \left\{ \textstyle\sum_i \Lambda_i \breve{\theta}_i P_i \,\middle|\, \breve{\theta}_i \in \breve{\Theta} \ \wedge\ P_i \in \Sigma \ \wedge\ \Lambda_i \in A[\Theta F \backslash \{v_{\breve{\theta}_i P_i}\}] \ \wedge\ v^*(\breve{\theta}_i P_i) < v^*_Q \right\}.$$

We observe that proposition 2.11 generalizes to the present context. We also have the following generalization of lemma 2.5:

Lemma 3.1. *Let C be a coherent autoreduced set. Then $\Delta_{v^*}(P,Q) \in [C]_{<v^*} : H_C^\infty$, for any Δ-polynomial of elements $P \neq Q$ in C.*

Proof. Let us first consider the case in which $\breve{\theta}^* = v^*/(v_P^* \wedge v_Q^*)$ is an extended difference operator. Then we have $\Delta_{v^*} = \breve{\theta}^* \Delta_{v_P^* \wedge v_Q^*}$ and $\breve{\theta}^*[C]_{<(v_P^* \wedge v_Q^*)} \subseteq [C]_{<v^*}$, from which the lemma follows easily. In the other case, we may assume without loss of generality that $v^* = v$. Indeed, we have $\Delta_{vv^*}(P,Q) = v\Delta_{v^*}(P,Q)$, for any P and Q, and $\deg(v/v_P)P = \deg(v/v_Q)Q = 1$. Now let $w^* = v_P^* \wedge v_Q^*$, if $(v_P^* \wedge v_Q^*)/v_P^*$ or $(v_P^* \wedge v_Q^*)/v_P^*$ are not both extended difference operators. In the other case, we may factor $\breve{\theta} = \breve{\eta}\breve{d}_i$, for some i, and we take $w^* = \breve{d}_i(v_P^* \wedge v_Q^*)$.

Now let $\breve{\eta} = v/w$. Using induction over $\breve{\eta}$, we may assume without loss of generality, that we proved the lemma for all smaller $\breve{\eta}$'s. Now we may either factorize $\breve{\eta} = \delta_i\breve{\eta}'$, or $\breve{\eta} = \breve{d}_i\breve{\eta}'$, for some i. In the first case, we apply a similar argument as above. In the second case, the choice of w assures us that $I_{(v/v_P)P} = I_{(v_{\breve{\eta}'w}/v_P)P}$ and $I_{(v/v_Q)Q} = I_{(v_{\breve{\eta}'w}/v_Q)Q}$, and a similar argument as at the end of the proof of lemma 2.5 can be applied to conclude. □

Lemma 3.2. *Let C be a coherent autoreduced subset of $A\{F\}$, such that H_C has no zero divisors. Then any DD-polynomial in $[C] : H_C^\infty$, which is reduced w.r.t. C belongs to $(C) : H_C^\infty$.*

Proof. The proof runs along the same lines as the proof of Rosenfeld's lemma. Therefore, we will content ourselves to indicate at which points the two proofs differ. Instead of (2.3), we write

$$H_C^\alpha Q = \sum_{i=1}^{r} \Phi_i \breve{\theta}_i^* P_i + \sum_{j=1}^{s} \Phi_j'(\breve{\theta}_j')^* P_j' + \sum_{k=1}^{t} \Phi_k'' P_k'', \tag{3.2}$$

with similar notations as before, and where $v_{\breve{\theta}_i^*}$ does not occur in Φ_i, for any i, and similarly for the Φ_j''s. Next, the variable v is replaced by an extended variable v^*; it is assumed that $v^*(\breve{\theta}_i^* P_i) = v$, for each i, and $v^*((\breve{\theta}_j')^* P_j') < v$, for each j.

Again, we may assume without loss of generality that $r = 1$, using the previous lemma, as can be seen by multiplying both sides of (3.2) by $I_{\breve{\theta}_1^* P_1}$, yielding

$$\begin{aligned} H_C^\alpha I_{\breve{\theta}_1^* P_1} Q \quad = \quad & \left(\sum_{i=1}^{r} \Phi_i I_{\breve{\theta}_i^* P_i}\right) \theta_1 P_1 + \sum_{j=1}^{s} \Phi_j' I_{\breve{\theta}_1^* P_1} \theta_j' P_j' + \sum_{k=1}^{t} \Phi_k'' I_{\breve{\theta}_1^* P_1} P_k'' + \\ & \sum_{i=1}^{r} \Phi_i \Delta_{v^*}(P_i, P_1). \end{aligned}$$

So assume that $r = 1$. We can interpret $\breve{\theta}_1^* P_1$ and $\sum_{j=1}^s \Phi'_j (\breve{\theta}'_j)^* P'_j + \sum_{k=1}^t \Phi''_k P''_k$ as polynomials in v. Performing the Euclidean division of the second polynomial by the first, transforms (2.3) in an equation of the form

$$H_C^{\alpha} I_{\breve{\theta}_1^* P_1}^{\gamma} Q = \widetilde{\Phi_1} \breve{\theta}_1^* P_1 + \sum_{j=1}^{s'} \widetilde{\Phi'_j} (\breve{\theta}'_j)^* P'_j + \sum_{k=1}^{t'} \widetilde{\Phi''_k} P''_k,$$

where the degrees in v of all terms except of $\widetilde{\Phi_1} \breve{\theta}_1^* P_1$ are strictly inferior to $\deg \breve{\theta}_1^* P_1$. Consequently, the degree of $\widetilde{\Phi_1} \breve{\theta}_1^* P_1$ in v must also strictly inferior to $\deg \breve{\theta}_1^* P_1$, whence $\widetilde{\Phi_1} = 0$ and Q is in $[C]_{<v^*} : H_C^{\infty}$. This contradicts the minimality hypothesis of v^*. □

Remark 3.3. In the case when $\Delta_g \neq \{1\}$, we define a subset Σ of $A\{F\} \backslash A$ to be Δ_g-**invariant**, if $\sigma P \in \Sigma$, for all $\sigma \in \Delta_g$ and $P \in \Sigma$. We remark that if $Q \in [\Sigma]$, where Σ is Δ_g-invariant, then Q is a linear combination of elements of the form $\Phi \breve{\theta} P$, with $\breve{\theta} \in \breve{\Theta}$ and P in Σ. In the definitions of characteristic sets and coherent autoreduced sets, we add the condition that the set be Δ_g-invariant. Modulo these modifications, the results of this section extend to the general case. In the subalgorithm 'reduce' of the reduce-and-split algorithm, we make Σ' stable under Δ_g at the end of the main loop.

3.3.7 Conclusion

We have shown that effective elimination theory extends to a setting which is far more general than the classical setting of differential algebra. Actually, we feel that the Ritt DD-ring setting is the most general one, which admits both a natural interpretation and an effective elimination theory.

In particular, there exist reduction bialgebras, which do *not* give rise to effective algebraic elimination theories. An example of this situation is obtained by considering the quantum matrices from example 3.4: the algebra $K[a, b, c, d]$ is actually a bialgebra (and even a Hopf algebra) for the following coproduct:

$$\begin{cases} a \mapsto a \otimes a + b \otimes c; \\ b \mapsto a \otimes b + b \otimes d; \\ c \mapsto c \otimes a + d \otimes c; \\ d \mapsto c \otimes b + d \otimes d. \end{cases}$$

However, no ordering on $\Theta = a^{\mathbb{N}} b^{\mathbb{N}} c^{\mathbb{N}} d^{\mathbb{N}}$ is both compatible with the product and the coproduct. Hence, it seems that no algebraic elimination theory exists for the entries of q-matrices, although a linear elimination theory does. Maybe this situation is "explained" by the fact that no convincing geometrical interpretation is available, contrary to the case of Ritt DD-algebras.

3.4 References

[BLOP 95] F. Boulier, D. Lazard, F. Ollivier, M. Petitot. Représentation du radical d'un idéal différentiel de type fini. *Proc. ISSAC 1995, Montreal.*

[Boul 94] F. Boulier. Etude et implantation de quelques algorithmes en algèbre différentielle. *PhD. Thesis, University of Lille I, France.*

[BrP 93] M. Bronstein, M. Petrovšek. On Ore rings, linear operators and factorization. *Technical Report 200, ETH Zürich.*

[Chyz 95] F. Chyzac. Formal manipulations of linear operators and holonomic calculations. *D.E.A. report.*

[Herz 34] F. Herzog. *Systems of algebraic mixed difference equations.* Proc. A.M.S. (p 286-300).

[Krei 64] H.F. Kreimer. The foundations for an extension of differential algebra. *Transactions A.M.S. 111 (p 482-492).*

[Lip 89] L. Lipshitz. *D*-finite power series. *Journal of algebra 122, p 353-373.*

[Man 88] Yu. I. Manin. *Quantum groups and non-commutative geometry.* Centre de Recherches Mathématiques, Montréal.

[Mans 91] E. Mansfield. Differential Gröbner bases. *PhD. Thesis, University of Sydney, Australia.*

[Mora 86] T. Mora. Groebner bases for non-commutative polynomial rings. *Proc. AAECC-3, Lect. Notes Comp. Sc., Springer 229 (p. 353-362).*

[Ol 90] F. Ollivier. Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité. *PhD. Thesis, École Polytechnique, France.*

[Ore 33] O. Ore. Theory of non-commutative polynomials. *Annals of Math. 34 (p 480-508).*

[SZ 92] B. Salvy, P. Zimmermann. Gfun: a Maple package for the manipulation of generating and holonomiac functions in one variable. *A.C.M. transactions on mathematical software.*

[Tak 92] N. Takayama. An approach to the zero recognition problem by Buchberger's algorithm. *Journal of Symbolic Computation 14, p 265-282.*

[Tak 93] N. Takayama. Kan-library reference manual. *Oct. 1993.*

[VdH 93] J. van der Hoeven. Théorie des bases standard et séries Mahlériennes généralisées. *Unpublished D.E.A. report, Ecole Polytechnique, France.*

[Zeil 82] D. Zeilberger. Sister Celine's technique and its generalizations. *Journal of mathematical analysis and applications 82, p 114-145.*

[Zeil 90] D. Zeilberger. A holonomic systems approach to special functions identities. *Journal of computational and applied mathematics 32, p 321-368.*

Glossary

Conventions

$f_{i,j} = (f_i)_j$	index convention
$\leqslant_E, +_E, \cdots$	the implicit ordering, sum, etc. on a set E
$E + F$	sum of two sets: $E + F = \{x + y \mid x \in E, y \in F\}$. A similar notation is often used for other operations
$(x_i)_{i \in I}$	sequence or family notation
Id_E	the identity mapping $E \to E$
$E \amalg F$	the disjoint union or direct sum of A and B
$E \backslash F$	the set elements in E which are not in F
$E \triangle F$	the set $E \backslash F \cup F \backslash E$
$\lvert x \rvert, \lvert E \rvert$	absolute value of x or cardinality of E
$\mathbb{N}$	the natural numbers including zero
$\mathbb{N}_k$	the set $\{1, \cdots, k\}$
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the integers, rationals, reals and complex numbers
R^*	the set of invertible (resp. non zero) elements of a ring (resp. a field)
R^+	positive elements of an ordered ring
R^+_*	positive invertible elements of an ordered ring

Main notations

A	a D-ring, 8
D	the Lie algebra of derivations on A, 8
$[\Sigma]$	D-ideal generated by a set Σ, 10
$Q(A)$	quotient field or total ring of fractions of A, 10
Ω	free linear D-operator algebra $\Omega = A[D]$, 10
Θ	basis for $A[D]$, 11
ε	evaluation mapping, 12
$\mathfrak{A}$	effective D-ring of the form $\mathfrak{C}[f_1, \cdots, f_k]/\mathfrak{i}$, 16
$G_{\mathfrak{A}}$	Groebner basis for $\mathfrak{i}$, 16
$\mathfrak{D}$	effective Lie-algebra of derivations on $\mathfrak{A}$, 16
$\mathfrak{m}$	maximal ideal of $\mathfrak{A}$, which determines ε, 16
$A\{F\}$	free polynomial D-ring, 30
$\widetilde{A\{F\}}$	quasi-polynomial D-algebra, 31
$\{\Sigma\}$	perfect D-ideal generated by a set Σ, 32
$I : S, I : S^\infty$	ideal quotient, 32

v_P	leader of D-polynomial P, 36
I_P	initial of D-polynomial P, 37
S_P	initial of D-polynomial P, 37
Σ	finite subset of $A\{F\}\backslash A$, 37
P `part-rem` Σ	partial remainder of P after Ritt division by Σ, 37
P `rem` Σ	remainder of P after Ritt division by Σ, 37
d_δ	"pull-back" of d by δ: $d_\delta\delta = \delta d$, 57
$v^*(P)$	extended leader of P, 60

Index