An Introduction to Differential Algebra

François Boulier and François Lemaire

June 15, 2023

A first version of these notes was written for an introductory course at the Workshop[1] on Tropical Differential Geometry, organized in December 2019 at the Queen Mary College of the University of London. I have rewritten them for another course at a CIMPA school[2] on Algebraic and Tropical Methods for Solving Differential Equations, organized in June 2023 at Oaxaca, Mexico. This document proves also very useful for documenting the theoretical foundations of the *DifferentialAlgebra* project [4].

I would like to thank many colleagues for their feedback on the first version of this document: François Lemaire, Adrien Poteaux, Julien Sebag, David Bourqui and Mercedes Haiech. I would like also to thank warmly Sebastian Falkensteiner for his interactions which eventually led to this second version.

Contents

1 Differential Polynomials **3**
1.1 Differential Rings . . . 3
1.2 Differential Polynomials . . . 3
1.3 Differential Ideals . . . 4
1.4 Rankings . . . 5
1.5 Ritt's Reduction Algorithms . . . 6
1.6 Formal Power Series Solutions — Principle . . . 8
1.7 Computation of the Series Coefficients — Easy Case . . . 9
1.8 Reduction to the Autonomous Case . . . 10
1.9 A Note for the Partial Differential Case . . . 11
1.10 Formal Power Series Solutions — Setting up Difficult Cases . . . 11
1.11 Hurwitz Lemma . . . 12
1.12 On Denef and Lipshitz Theorem 3.1 . . . 13
1.13 An Undecidability Result in the Partial Case . . . 14

[1] `https://sites.google.com/view/tropdiffalgworkshop/home`
[2] `https://www.cimpa.info/en/node/7213`

2 Differential Ideals — A Theorem of Zeros **15**
2.1 Rankings are Well Orderings 15
2.2 Autoreduced sets are Finite 16
2.3 Characteristic Sets as Minimal Autoreduced Sets 17
2.4 Characteristic Sets of Prime Differential Ideals 18
2.5 Differential Ideals Defined by Characteristic Sets 18
2.6 The Ritt-Raudenbush Basis Theorem 19
2.7 Zeros of a Prime Differential Ideal 23
2.8 A Differential Theorem of Zeros 26

3 Regular Differential Chains **27**
3.1 The Lasker-Noether Theorem 27
3.2 Ideals Defined by Triangular Sets 28
3.3 Regular Chains 30
3.4 Regular Differential Chains — Ordinary Case 30
3.5 Regular Differential Chains — Partial Case 31
3.6 Properties of Regular Differential Chains 32
3.7 Testing the Inclusion of Differential Ideals 32
3.8 Formal Power Series Solutions — Principle 33
3.9 Algorithmic Decomposition of a Perfect Differential Ideal 33
3.10 Classical Properties of The Resultant 38
3.11 Proof of the Equivalence Theorem on Regular Chains 39
3.12 Proof of the Unmixedness Theorem and Lazard's Lemma 43

In the early 2000 I had the opportunity to teach differential elimination methods at Paris VI University (today Sorbonne University) in some Master course. The beginning of the course — up to differential ideals — is taught quite easily. But difficulties actually occur as soon as one writes a first equation: what do you mean by a solution of a differential equation whose left hand side is a general differential polynomial ? The approach followed by Ritt (a solution is a prime differential ideal which contains the equation) is very elegant but it is also terribly abstract for students. This time, I have decided to start with a more tedious but much more intuitive approach: we look for formal power series solutions. This approach actually perfectly suits tropical differential contexts.

The reference book is the one of Kolchin [17]. In particular, I have tried to use as much as possible Kolchin's notations. However, this book is notoriously difficult to read and the structure of this document is much inspired by the book of Ritt [24], which I recommend for casual readers.

1 Differential Polynomials

1.1 Differential Rings

The following basic notions are introduced in [17, chap. I, sect. 1].

An operator δ on a ring is called a *derivation operator* if $\delta(a+b) = \delta a + \delta b$ and $\delta(a\,b) = (\delta a)\,b + a\,\delta b$ for all elements a, b of the ring.

A *differential ring* $\mathscr{R}$ is defined as a ring with finitely many derivation operators which commute pairwise i.e. such that $\delta_1\delta_2 a = \delta_2\delta_1 a$ for all derivation operators δ_1, δ_2 and all $a \in \mathscr{R}$.

A *differential field* is a differential ring which is a field. If the number m of derivation operators is equal to 1 then the differential ring is said to be *ordinary*. If it is greater than 1, the differential ring is said to be *partial*.

The operator δ which maps every element of a ring to zero is a derivation so that every ring can be viewed as a trivial differential ring. If the ring is the field $\mathbb{Q}$ of the rational numbers, this derivation is the only possible one since

$$\begin{array}{rclcrcl} \delta(0) & = & \delta(0+0) & = & 2\,\delta(0) & = & 0\,, \\ \delta(1) & = & \delta(1\times 1) & = & 2\,\delta(1) & = & 0\,, \end{array}$$

hence the derivative of any rational number must be zero. More generally, it can be proved that the derivative of any complex number must be zero. Since a *constant* is defined as an element the derivative of which is zero, we see that $\mathbb{C}$ is a field of constants.

The equations we handle will have coefficients in a differential field $\mathscr{F}$ of characteristic zero i.e. a field which contains $\mathbb{Q}$ as a subfield (such fields are sometimes called *Ritt fields*). Readers who feel uncomfortable with this general setting may however most often assume $\mathscr{F}$ is the field of the complex numbers. In some cases, differential equations explicitly depend on "independent variables". We then assume that there exist symbols $x_1, \ldots, x_m$ related to the derivation operators $\delta_1, \ldots, \delta_m$ by the relations: $\delta_i x_i = 1$ and $\delta_i x_j = 0$ for all $1 \leq i, j \leq m$ such that $i \neq j$. There are two ways to incorporate them in the differential algebra setting: they can be viewed as elements of the base field $\mathscr{F}$ — which is then not a field of constants; they can also be viewed as differential indeterminates, constrained by the above relations. In both cases, we may interpret δ_i as the partial derivative $\partial/\partial x_i$ — or $\mathrm{d}/\mathrm{d}x$ in the ordinary case.

1.2 Differential Polynomials

From the differential algebra point of view, *differential indeterminates* are symbols such as y, z over which derivation operators may apply, giving an infinite set of *derivatives*. In the ordinary case, interpreting δ as $\mathrm{d}/\mathrm{d}x$, one may view differential indeterminates as representing unknown functions $y(x)$ and $z(x)$ and their derivatives

$$y, z, \dot{y}, \dot{z}, \ddot{y}, \ddot{z}, \ldots, y^{(r)}, z^{(r)}, \ldots$$

as representing the functions obtained by differentiation.

In the partial case, interpreting the derivation operators as $\delta_i = \partial/\partial x_i$ for $1 \leq i \leq m$, one may view differential indeterminates as representing unknown functions $y(x_1, \ldots, x_m)$ and $z(x_1, \ldots, x_m)$ and their derivatives as representing the functions obtained by partial differentiations.

In the general case it is convenient, following [17, chap. I, sect. 1] to introduce the commutative semigroup (written multiplicatively) Θ generated by the derivation operators. Each *derivative operator* $\theta \in \Theta$ has the form

$$\theta \quad = \quad \delta_1^{e_1} \cdots \delta_m^{e_m}$$

where $e_1, \ldots, e_m \in \mathbb{N}$ (the set of the nonnegative integers). Then the corresponding derivative of the differential indeterminate (say) y will be denoted

$$\theta y \quad \text{or} \quad y_{x_1^{e_1} \cdots x_m^{e_m}} .$$

It represents the function

$$\frac{\partial^{e_1 + \cdots + e_m} y}{\partial x_1^{e_1} \cdots \partial x_m^{e_m}} (x_1, \ldots, x_m) .$$

The nonnegative integer $e_1 + \cdots + e_m$ is said to be the *order* of the derivative operator θ. A derivative operator θ is said to be *proper* if its order is strictly positive.

If $\mathscr{F}$ is a differential field and $Y = \{y_1, \ldots, y_n\}$ is a set of n differential indeterminates then the polynomials in the derivatives in ΘY, with coefficients in $\mathscr{F}$ — the elements of $\mathscr{F}[\Theta Y]$ — are called *differential polynomials*. All together, they form a *differential polynomial ring* denoted

$$\mathscr{F}\{y_1, \ldots, y_n\} .$$

1.3 Differential Ideals

Let $\mathscr{R}$ denote the differential polynomial ring $\mathscr{F}\{y_1, \ldots, y_n\}$ with $m > 0$ derivation operators. The following definitions are borrowed from [24, chap. I, 7] in the ordinary case. They readily apply to the general case, as pointed out in [24, chap. IX].

A nonempty subset $\mathfrak{A}$ of $\mathscr{R}$ is said to be a *differential ideal* of $\mathscr{R}$ if:

1. it is an ideal of $\mathscr{R}$ and
2. it is stable under the action of the derivations i.e. if it is such that $p \in \mathfrak{A} \Rightarrow \theta p \in \mathfrak{A}$ for all derivation operator $\theta \in \Theta$.

A differential ideal contains an infinite number of differential polynomials unless it consists of the single differential polynomial 0. The intersection of any finite or infinite number of differential ideals is a differential ideal.

A differential ideal $\mathfrak{A}$ is said to be *perfect* if it is equal to its radical i.e. if $(\exists d \in \mathbb{N},\ p^d \in \mathfrak{A}) \Rightarrow p \in \mathfrak{A}$. The intersection of any finite or infinite number of perfect differential ideals is a perfect differential ideal.

A differential ideal $\mathfrak{A}$ is said to be *prime* if it is prime in the usual sense i.e. if it is such that $p\,q \in \mathfrak{A} \Rightarrow (p \in \mathfrak{A}$ or $q \in \mathfrak{A})$. Every prime differential ideal is perfect.

Let Σ be any subset of $\mathscr{R}$.

One denotes $[\Sigma]$ the *differential ideal of* $\mathscr{R}$ *generated by* Σ. It is defined as the intersection of all differential ideals of $\mathscr{R}$ containing Σ. It is the set of all finite linear combinations, with arbitrary elements of $\mathscr{R}$ for coefficients, of elements of Σ and their derivatives of any order.

One denotes $\{\Sigma\}$ the *perfect differential ideal of* $\mathscr{R}$ *generated by* Σ. It is defined as the intersection of all perfect differential ideals of $\mathscr{R}$ containing Σ.

It is clear that $[\Sigma] \subset \{\Sigma\}$. More precisely, we have the following

Proposition 1 *Let Σ be any subset of $\mathscr{R}$. Then $\{\Sigma\} = \sqrt{[\Sigma]}$. With words, $\{\Sigma\}$ is the set of all differential polynomials $p \in \mathscr{R}$ for which there exists some $r \in \mathbb{N}$ such that $p^r \in [\Sigma]$.*

The only part of the proof which is not immediate is given by the following Lemma, which essentially is [24, chap. I, 9, Lemma].

Lemma 1 *Let Σ be any subset and p be any element of $\mathscr{R}$. If there exists some positive integer r such that $p^r \in [\Sigma]$ then $\dot{p}^{2\,r-1} \in [\Sigma]$, where the dot indicates any derivation operator of $\mathscr{R}$.*

Proof Assume $p^r \in [\Sigma]$. Differentiating p^r and dividing by r we have $p^{r-1}\,\dot{p} \in [\Sigma]$. We thus have proved the Lemma in the case $r = 1$. For the general case $r \geq 2$, observe that we have proved (1) below for $k = 1$:

$$p^{r-k}\,\dot{p}^{2\,k-1} \quad \in \quad [\Sigma] \tag{1}$$

We need to establish that (1) holds for $k = r$. Assume thus (1) holds with $r \geq 2$ and $r > k \geq 1$. Differentiating (1) we get

$$(r-k)\,p^{r-k-1}\,\dot{p}^{2\,k} + (2\,k-1)\,p^{r-k}\,\dot{p}^{2\,k-2}\,\ddot{p} \quad \in \quad [\Sigma] \tag{2}$$

Multiply (2) by $\dot{p}$. Subtract (1) multiplied by $(2\,k-1)\,\ddot{p}$. Divide the result by $r-k$. One gets

$$p^{r-k-1}\,\dot{p}^{2\,k+1} \quad \in \quad [\Sigma] \tag{3}$$

Repeating the above computation (more rigorously, putting it some proof by induction on $r-k$), we see that the Lemma holds in general. □

1.4 Rankings

Let $Y = \{y_1, \ldots, y_n\}$ be a set of differential indeterminates. A *ranking* [17, chap. I, sect. 8] is a total order on the infinite set ΘY which satisfies the two following axioms, for all derivatives $v, w \in \Theta Y$ and every derivative operator $\theta \in \Theta$:

1. $v \leq \theta v$ and

2. $v < w \Rightarrow \theta v < \theta w$.

Let $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$ be a differential polynomial ring. Fix some ranking and consider some differential polynomial $p \in \mathscr{R} \setminus \mathscr{F}$.

The *leading derivative* (the *leader* in Kolchin's terminology) of p is the highest derivative v such that $\deg(p, v) > 0$.

Let v be the leading derivative of p and $d = \deg(p, v)$.

The *rank* of p is defined as the monomial v^d.

The ranking induces a *total ordering on ranks* as follows. A rank v^d is said to be less than a rank w^e if $v < w$ with respect to the ranking or $v = w$ and $d < e$. It is convenient to extend the above definitions by introducing some artificial rank, common to all nonzero elements of $\mathscr{F}$ and considering that it is strictly less than the rank of any element of $\mathscr{R} \setminus \mathscr{F}$. If p, q are two nonzero differential polynomials, we will write $p < q$ to express the fact that the rank of p is strictly less than the one of q. Proposition 7 implies that any such ordering on ranks is a well-ordering.

The *initial* of p is the leading coefficient of p, viewed as a univariate polynomial in v. In general, the *initial* of p is a differential polynomial of $\mathscr{R}$.

The *separant* of p is the differential polynomial $\partial p / \partial v$.

The second axiom of rankings implies that any proper derivative θp of p has rank θv; its initial is the separant of p.

Let $q \in \mathscr{R}$ and $p \in \mathscr{R} \setminus \mathscr{F}$ be two differential polynomials. Let p have rank v^d.

The differential polynomial q is said to be *partially reduced* with respect to p if it does not depend on any proper derivative of v i.e. if, for every proper derivative operator θ, we have $\deg(q, \theta v) = 0$.

The differential polynomial q is said to be (fully) *reduced* with respect to p if it is partially reduced with respect to p and $\deg(q, v) < d$.

As an example, consider the ordinary differential polynomial ring $\mathscr{F}\{y\}$ and the following example of a differential polynomial $p \in \mathscr{F}\{y\}$ and its first derivatives:

$$\begin{aligned} p &= \dot{y}^2 + y^3\,, \\ \dot{p} &= 2\,\dot{y}\,\ddot{y} + 3\,y^2\,\dot{y}\,, \\ \ddot{p} &= 2\,\dot{y}\,y^{(3)} + 2\,\ddot{y}^2 + 3\,y^2\,\ddot{y} + 6\,y\,\dot{y}^2\,. \end{aligned}$$

The axioms of rankings imply that $\dot{y}$ is the leading derivative of p (whatever the ranking) hence that $\ddot{y}$ and $y^{(3)}$ are the leading derivatives of $\dot{p}$ and $\ddot{p}$. The rank of p is $\dot{y}^2$. Its initial is 1 and its separant is $2\,\dot{y}$.

1.5 Ritt's Reduction Algorithms

Let f, g be two polynomials of $\mathscr{S}[x]$, where $\mathscr{S}$ is a ring and $\deg(g, x) > 0$, one denotes $\mathrm{prem}(f, g, x)$ the pseudoremainder of f by g (it is the polynomial $r(x)$ mentioned in [31, chap. I, 17, Theorem 9, page 30]).

Let now $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials and $f \in \mathscr{R}$ be a differential polynomial. Assume that a ranking is fixed so that every element of A admits a leading derivative.

The *partial remainder* of f by A, denoted $\mathrm{partialrem}(f, A)$ is defined inductively as follows:

1. if f is partially reduced with respect to all elements of A then $\mathrm{partialrem}(f, A) = f$;
2. if f is *not* partially reduced with respect to all elements of A then there must exist some $p \in A$ with leading derivative v and some proper derivative operator θ such that $\deg(f, \theta v) > 0$. Among all such triples (p, v, θ), choose one such that θv is maximal with respect to the ranking. Then

$$\mathrm{partialrem}(f, A) \;=\; \mathrm{partialrem}(\mathrm{prem}(f, \theta p, \theta v), A)\,.$$

In the ordinary differential polynomial ring $\mathscr{F}\{y, z\}$, take $f = \ddot{y} + z$ and A made of a single differential polynomial $p = \dot{y}^2 + z$. Assume the leading derivative of p is $\dot{y}$. The differential polynomial f is not partially reduced with respect to p. Differentiating, we get $\dot{p} = 2\,\dot{y}\,\ddot{y} + \dot{z}$. The pseudodivision of f by $\dot{p}$ computes the following relation. The differential polynomial g is the partial remainder of f by p.

$$\underbrace{2\,\dot{y}}_{h}\,\underbrace{(\ddot{y} + z)}_{f} \;=\; \underbrace{1}_{q} \times \underbrace{(2\,\dot{y}\,\ddot{y} + \dot{z})}_{\dot{p}} + \underbrace{(2\,z\,\dot{y} - \dot{z})}_{g}\,. \tag{4}$$

Proposition 2 *Let $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials, $f \in \mathscr{R}$ be a differential polynomial and $g = \mathrm{partialrem}(f, A)$. Then g is partially reduced with respect to A and there exists a power product h of the separants of A such that*

$$h\,f \;=\; g \mod [A]\,. \tag{5}$$

The *full remainder* of f by A, denoted $\mathrm{fullrem}(f, A)$, is defined as follows. Denote $A = \{p_1, \ldots, p_r\}$, assuming $p_1 < \cdots < p_r$.

1. if f is reduced with respect to all elements of A then $\mathrm{fullrem}(f, A) = f$;
2. if f is *not* partially reduced with respect to all elements of A then

$$\mathrm{fullrem}(f, A) \;=\; \mathrm{fullrem}(\mathrm{partialrem}(f, A), A)$$

3. if f is partially reduced but *not* reduced with respect to all elements of A there must exist some index $i \in [1, r]$ such that $\deg(f, v_i) \geq \deg(p_i, v_i)$ where v_i denotes the leading derivative of p_i. Among all such indices i, fix the maximal one. Then

$$\mathrm{fullrem}(f, A) \;=\; \mathrm{fullrem}(\mathrm{prem}(f, p_i, v_i), A)\,.$$

The rules above perform the partial reduction stage before the non differential one. However, it is also possible to interlace the two stages and process, at each step, the ranks which prevent f to be reduced by decreasing order — according to the ranking.

In the partial differential polynomial ring $\mathscr{F}\{y,z\}$ endowed with derivations with respect to x and t, take $f = 2\,y\,y_t\,z_{xt} + 2\,y_t^2\,z_x - 4\,y_x$ and $A = p_1, p_2, p_3$ with $p_1 = y_t^2 - 4\,y$, $p_2 = y_x - z_x\,y$ and $p_3 = z_t$. Assume the leading derivatives are y_t, y_x and z_t. The reduction of f is achieved by three pseudodivisions. The full remainder is g_3. The power product $h = h_1\,h_2\,h_3 = 1$.

$$\begin{aligned}
\underbrace{1}_{h_1} \times \underbrace{(2\,y\,y_t\,z_{xt} + 2\,y_t^2\,z_x - 4\,y_x)}_{f} &= \underbrace{2\,y\,y_t}_{q_1}\,\underbrace{z_{xt}}_{\delta_x p_3} + \underbrace{2\,y_t^2\,z_x - 4\,y_x}_{g_1}\,, \\
\underbrace{1}_{h_2} \times \underbrace{(2\,y_t^2\,z_x - 4\,y_x)}_{g_1} &= \underbrace{2\,z_x}_{q_2}\,\underbrace{(y_t^2 - 4\,y)}_{p_1} + \underbrace{8\,y\,z_x - 4\,y_x}_{g_2}\,, \\
\underbrace{1}_{h_3} \times \underbrace{(8\,y\,z_x - 4\,y_x)}_{g_2} &= \underbrace{-4}_{q_3} \times \underbrace{(y_x - z_x\,y)}_{p_2} + \underbrace{4\,y\,z_x}_{g_3}\,.
\end{aligned} \tag{6}$$

Proposition 3 *Let $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials, $f \in \mathscr{R}$ be a differential polynomial and $g = \mathrm{fullrem}(f, A)$. Then g is reduced with respect to A and there exists a power product h of the initials and the separants of A such that*

$$h\,f \;=\; g \mod [A]\,. \tag{7}$$

1.6 Formal Power Series Solutions — Principle

We illustrate the principle over the example of a non *non autonomous* differential polynomial i.e. a differential polynomial which explicitly depends on the independent variable x. We are looking for a formal power series centered at $x = \alpha$

$$\bar{\bar{y}} \;=\; y_0 + y_1\,(x-\alpha) + y_2\,\frac{(x-\alpha)^2}{2} + + y_3\,\frac{(x-\alpha)^3}{6} + \cdots \tag{8}$$

solution of the order $n = 1$ differential polynomial

$$p(x,y) \;=\; \dot{y}^2 + 8\,x\,y - y\,. \tag{9}$$

Step 1: differentiate p

$$\begin{aligned}
\dot{y}^2 + 8\,x\,y - y &= 0\,, \\
2\,\dot{y}\,\ddot{y} + 8\,x\,\dot{y} - \dot{y} + 8\,y &= 0\,, \\
2\,\dot{y}\,y^{(3)} + 2\,\ddot{y}^2 + 8\,x\,\ddot{y} - \ddot{y} + 16\,\dot{y} &= 0\,, \\
&\vdots
\end{aligned}$$

Step 2: rename $y^{(i)}$ as y_i

$$\begin{aligned}
y_1^2 + 8\,x\,y_0 - y_0 &= 0\,, \\
2\,y_1\,y_2 + 8\,x\,y_1 - y_1 + 8\,y_0 &= 0\,, \\
2\,y_1\,y_3 + 2\,y_2^2 + 8\,x\,y_2 - y_2 + 16\,y_1 &= 0\,, \\
&\vdots
\end{aligned}$$

Step 3: evaluate the polynomials at $x = \alpha$ and denote them p_i (Denef and Lipshitz would denote them $p^{(i)}(\alpha, y_0, y_1, y_2, \ldots)$ in [12]):

$$\begin{array}{lll} p_0 & y_1^2 + 8\,\alpha - y_0 & = \; 0\,, \\ p_1 & 2\,y_1\,y_2 + 8\,\alpha\,y_1 - y_1 + 8\,y_0 & = \; 0\,, \\ p_2 & 2\,y_1\,y_3 + 2\,y_2^2 + 8\,\alpha\,y_2 - y_2 + 16\,y_1 & = \; 0\,, \\ & & \vdots \end{array} \tag{10}$$

Step 4: "solve" and substitute the solution in (8). A possible solution (assuming $\alpha = 0$) is

$$(y_0, y_1, y_2, y_3, \ldots) \;=\; (1, 1, -\frac{7}{2}, -22, \ldots)\,. \tag{11}$$

The corresponding formal power series solution, centered at the origin, then starts as follows:

$$\bar{\bar{y}} \;=\; 1 + x - \frac{7}{4}\,x^2 + \cdots$$

This principle relies on the following proposition ("nothing but a simple computational rule" according to [27, page 160]) that we state over our example but which holds for a general differential polynomial p:

Proposition 4 *Let $\bar{\bar{y}}$ be the generic formal power series defined in* (8) *and p_i the polynomials defined in* (10)*. Then*

$$p(x, \bar{\bar{y}}) \;=\; p_0 + p_1\,(x - \alpha) + p_2\,\frac{(x-\alpha)^2}{2} + p_3\,\frac{(x-\alpha)^3}{6} + \cdots \tag{12}$$

Proof By induction. The Proposition holds for $p \in \mathscr{F}$ and p a differential indeterminate. If it holds for two differential polynomials p and q, it holds for their sum, product and derivatives. □

Indeed, the formal power series $p(x, \bar{\bar{y}})$ is identically zero if and only if $(y_0, y_1, y_2, \ldots)$ annihilates the infinite system $p_0 = p_1 = p_2 = \cdots = 0$. Moreover, if $\bar{\bar{y}}$ annihilates p, it annihilates every derivative of p. Therefore, the formal power series $\bar{\bar{y}}$ that we have built in this section annihilates the whole differential ideal $[p]$ of the differential polynomial ring $\mathscr{F}[x]\{y\}$ (the independent variable x should not be considered as a base field element because the above process evaluates it). It even annihilates the perfect differential ideal $\{p\}$ since a power of a formal power series is zero if and only if the series itself is zero.

In summary, the formal power series $\bar{\bar{y}}$ built in this section is a zero of the differential ideal $\{p\}$. Here also, this statement holds for a general differential polynomial p.

1.7 Computation of the Series Coefficients — Easy Case

The easy case happens when the expansion point and the "initial values" y_0 and y_1 (the coefficients of $\bar{\bar{y}}$ which occur in the polynomial p_0 of (10)) do not cancel the leading coefficients

of the infinite system (10) i.e. the initial and the separant of the polynomial p. In this case, the coefficients of the formal power series (8) can easily be obtained using Ritt's reduction algorithm: for any non negative integer e, performing Ritt's partial or full reduction method over $y^{(e)}$, one gets a relation $h\,y^{(e)} = r \pmod{[p]}$ where h is a power product of initials and separants of p and r is a differential polynomial partially reduced w.r.t. p. Then the value of y_e is obtained by evaluating r/h at the initial values and the expansion point. Over our example we get

$$\begin{aligned} \underbrace{2\,\dot{y}}_{h}\,\ddot{y} &= \underbrace{(1-8\,x)\,\dot{y}-8\,y}_{r} \pmod{[p]}\,, \\ \underbrace{2\,\dot{y}^3}_{h}\,y^{(3)} &= \underbrace{4\,y\,((24\,x-3)\,\dot{y}-8\,y)}_{r} \pmod{[p]}\,. \end{aligned}$$

In both cases, evaluating r/h at $(\alpha, y_0, y_1) = (0, 1, 1)$ yields the values of y_2 and y_3 given in (11).

Anticipating on a further section, let us mention that the value of y_e can also be obtained by computing the *normal form* of $y^{(e)}$ modulo the regular differential chain p and evaluating it at the initial values and the expansion point. Over our example, we get

$$\begin{aligned} \ddot{y} &= \frac{8\,\dot{y}-64\,x^2+16\,x-1}{2\,(8\,x-1)} \pmod{[p]}\,, \\ y^{(3)} &= \frac{-2\,(8\,\dot{y}+192\,x^2-48\,x+3)}{(8\,x-1)^2} \pmod{[p]}\,. \end{aligned}$$

In both cases, evaluating the normal forms at $(\alpha, y_0, y_1) = (0, 1, 1)$ yields also the values of y_2 and y_3 given in (11). Observe also that the expansion point $\alpha = \frac{1}{8}$ forces $y_1 = 0$ since p_0 must vanish.

1.8 Reduction to the Autonomous Case

Classical differential algebra books [24, 17] do not mention "non autonomous" differential polynomials i.e. differential polynomials whose coefficients depend on the independent variables. Here we show how formal power series centered at some $x = \alpha$ can be obtained from formal power series centered at the origin, on "autonomous" differential polynomials at the price of an extra differential indeterminate. We illustrate the process over our example (9).

The "independent" variable x is encoded by an extra differential indeterminate. For legibility, the symbol x is kept for the differential indeterminate. The symbol used for the derivation is renamed as ξ which means that formal power series are sought in $\mathscr{F}[[\xi]]$ and that the derivation operator should be interpreted as $\mathrm{d}/\mathrm{d}\xi$. The differential equation $p = 0$ is thus equivalent to the following "autonomous" differential polynomial system of $\mathscr{F}\{y, x\}$

$$\dot{y}^2 + 8\,x\,y + 1 = 0\,, \tag{13}$$

$$\dot{x} - 1 = 0\,. \tag{14}$$

Since we are looking for a formal power series centered at α i.e. such that $x(0) = \alpha$, we fix the "initial condition" of the second equation to α (the expansion point has been encoded as an initial condition). Applying the process described in section 1.6 to (14) at $\xi = 0$ yields

$$\bar{\bar{x}} \;=\; \alpha + \xi\,. \tag{15}$$

Applying the process described in section 1.6 to (13) at $\xi = 0$ then yields

$$\bar{\bar{y}} \;=\; p_0 + p_1\,\xi + p_2\,\frac{\xi^2}{2} + \cdots \tag{16}$$

Substitute now $x - \alpha$ to ξ in the above formal power series (thanks to (15)) and the formal power series (12) is recovered.

1.9 A Note for the Partial Differential Case

The content of sections 1.6 to 1.8 readily generalize to the case of m derivation operators, replacing formula (8) by the more general one

$$\bar{\bar{y}} \;=\; \sum_{(e_1,\ldots,e_m)\in\mathbb{N}^m} \frac{1}{e_1\,!\cdots e_m\,!}\,y_{i,(e_1,\ldots,e_m)}\,(x_1-\alpha_1)^{e_1}\cdots(x_m-\alpha_m)^{e_m}\,,\quad 1\le i\le n\,.$$

1.10 Formal Power Series Solutions — Setting up Difficult Cases

Difficult cases arise when expansion points and/or initial values cancel initials and separants. For simplicity, we assume that the expansion point is zero. In such situations, the number of needed initial values cannot always be clearly read from the order of the differential polynomial to be solved. In general, this number actually depends on the values of the initial values! A way to overcome this difficulty consists in providing arbitrarily many initial values $y_0, y_1, y_2, \ldots$ and encode them by means of a formal power series

$$\bar{y} \;=\; y_0 + y_1\,x + y_2\,\frac{x^2}{2} + \cdots$$

Of course, these initial values must be compatible with the differential polynomial to be solved: they must satisfy system (10) up to some order β.

In summary, we consider an order n differential polynomial $p(x, y, \dot{y}, \ldots, y^{(n)})$ of $\mathscr{F}[x]\{y\}$ (Denef and Lipshitz consider more generally a differential polynomial over $\mathscr{F}[[x]]$) and an initial values encoding formal power series $\bar{y}$. We are looking for two non negative integers β and δ such that, if

$$p(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) \;=\; 0 \mod x^\beta$$

then there exists a unique formal power series $\bar{\bar{y}}$ such that

$$\begin{aligned} \bar{\bar{y}} &= \bar{y} \mod x^\delta\,,\\ p(x, \bar{\bar{y}}, \bar{\bar{y}}', \ldots, \bar{\bar{y}}^{(n)}) &= 0\,. \end{aligned}$$

1.11 Hurwitz Lemma

The next Lemma is due to Hurwitz [15]. See also [12, Lemma 2.2].

Lemma 2 *Let $k \in \mathbb{N}$. Then*

$$p^{(2\,k+2)} = y^{(n+2\,k+2)}\,f_n + y^{(n+2\,k+1)}\,f_{n+1} + y^{(n+2\,k)}\,f_{n+2} + \cdots + y^{(n+k+2)}\,f_{n+k} + f_{n+k+1}\,, \qquad (17)$$

where the f_j are differential polynomials of order at most j for $j = n, n+1, \ldots, n+k+1$ and f_n is the separant of p. The differential polynomials $f_{n+1}, f_{n+2}, \ldots$ depend on k but the separant f_n does not. Let now $q \in \mathbb{N}$. Then, if we differentiate (17) q times we get

$$\begin{aligned} p^{(2\,k+2+q)} = {} & y^{(n+2\,k+2+q)}\,f_n + y^{(n+2\,k+2+q-1)}\,[f_{n+1} + q\,f'_n] \\ & + \cdots + y^{(n+2\,k+2+q-r)}\left[f_{n+r} + q\,f'_{n+r-1} + \cdots + \binom{q}{r} f_n^{(r)}\right] \\ & + \cdots + y^{(n+2\,k+2+q-k)}\left[f_{n+k} + q\,f'_{n+k-1} + \cdots + \binom{q}{k} f_n^{(k)}\right] + h_{n+k+q+1} \end{aligned} \qquad (18)$$

where $h_{n+k+q+1}$ has order at most $n+k+q+1$.

Proof We have $p' = y^{(n+1)}\,f_n + g_n$ where g_n is a differential polynomial of order at most n. Formula (17) is easily proved by induction on k. Formula (18) by differentiating (17) q times and using Leibniz rule. □

The remaining part of this section is due to Denef and Lipshitz. See [12, Lemma 2.3].

Definition 1 *(definition of k)*
Assume $\bar{y} \in \mathscr{F}[[x]]$ does not annihilate the separant f_n of p. Then one defines k as the valuation of $f_n(x, \bar{y}, \ldots, \bar{y}^{(n)})$ i.e. as the non negative integer k such that

$$f_n(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) = c_0\,x^k + c_1\,x^{k+1} + \cdots \quad (c_0 \neq 0)$$

Assume that the formal power series $f_n(x, \bar{y}, \ldots, \bar{y}^{(n)})$ is nonzero. Then $f_n^{(k)}(0, y_0, y_1, \ldots)$, which is an element of $\mathscr{F}$ equal to c_0 is also nonzero (the polynomial $f_n^{(k)}(0, y_0, y_1, \ldots)$ is an analogue of the polynomials p_i of (10)). Therefore the following integer r is well-defined:

Definition 2 *(definition of r)*
Let $\bar{y}$ and k as in definition 1. One defines r $(0 \leq r \leq k)$ as the smallest integer such that

$$\left[f_{n+r} + q\,f'_{n+r-1} + \cdots + \binom{q}{r} f_n^{(r)}\right](0, y_0, y_1, \ldots) \neq 0\,. \qquad (19)$$

The left hand side of (19) is a nonzero polynomial of $\mathscr{F}[q]$. It is denoted $A(q)$.

Proposition 5 *Let $\bar{y}$, k and r as in definitions 1 and 2. Let $\gamma \in \mathbb{N}$ be bigger than any non negative integer root of $A(q)$. Let $\beta = 2\,k + 2 + \gamma + r$ and $\delta = n + 2\,k + 2 + \gamma$. Then, if*

$$p(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) \;=\; 0 \mod x^{\beta}$$

then there exists a unique formal power series $\bar{\bar{y}}$ such that

$$\begin{aligned} \bar{\bar{y}} &= \bar{y} \mod x^{\delta}\,, \\ p(x, \bar{\bar{y}}, \bar{\bar{y}}', \ldots, \bar{\bar{y}}^{(n)}) &= 0\,. \end{aligned}$$

Proof See the proof of [12, Lemma 2.3] for the details, which are technical. The key argument is that the values of the coefficients y_i of $\bar{\bar{y}}$, for $i \geq \delta$ (which need not be equal to the coefficients y_i of $\bar{y}$) are defined by the following formula [12, Formula (6)], which comes from (18):

$$p^{(2\,k+2+q)}(0, y_0, y_1, \ldots) \;=\; y_{n+2\,k+2+q-r}\, A(0, y_0, y_1, \ldots, q) + h_{n+2\,k+1+q-r}(0, y_0, y_1, \ldots)\,.$$

Observe that $n + 2\,k + 2 + q - r \geq \delta$ whenever $q \geq \gamma - r$. The differential polynomial $h_{n+2\,k+1+q-r}$ has order at most $n + 2\,k + 1 + q - r$. Since $A(0, y_0, y_1, \ldots, q)$ is nonzero for any non negative integer $q \geq \gamma \geq \gamma - r$, the value of $y_{n+2\,k+2+q-r}$ (for $n + 2\,k + 2 + q - r \geq \delta$) is uniquely defined by equating $p^{(2\,k+2+q)}(0, y_0, y_1, \ldots)$ to zero. □

Let us come back to example (9) and seek a formal power series solution for $(\alpha, y_0, y_1) = (0, 0, 0)$ and $y_2 \neq 0$. Observe that the inequality constraint is necessary to fix k. Then we find $k = r = 1$ and $A(q) = 2\,q\,y_2 + 8\,y_2 - 1$. Looking at p_2 in system (10), we see that y_2 must be equal to 0 or $\frac{1}{2}$. Let us pick $y_2 = \frac{1}{2}$ since we have assumed $y_2 \neq 0$. We see that $A(q)$ has no non negative integer root so that we can pick $\gamma = 0$. Then we get $\beta = \delta = 5$. Solving $p_0 = p_1 = \cdots = p_4$ we find a unique solution $(y_3, y_4) = (-6, -8)$. According to Proposition 5, these five values can be prolongated to a unique formal power series $\bar{\bar{y}}$ solution of (9).

1.12 On Denef and Lipshitz Theorem 3.1

Denef and Lipshitz [12, Theorem 3.1] claim that there exists an algorithm which decides whether a system of polynomial ordinary differential equations admits formal power series solutions centered at any given expansion point α.

Roughly speaking, the idea consists in using Proposition 5 over an initial values encoding formal power series $\bar{y}$ with parametric coefficients and use tools such as universal quantifier elimination and cylindrical algebraic decomposition in order to discuss cases.

The situation then becomes much more complicated. Uniqueness of formal power series is no more guaranteed. Actually, a result of Singer [28, Problem (3)] proves that the existence problem of *nonzero* formal power series solutions is undecidable, thanks to the negative answer to Hilbert's Tenth Problem [20]. Even existence cannot be guaranteed for *every* formal power series $\bar{y}$ satisfying the constraints produced by the algorithm. The existence for *some* formal power series $\bar{y}$ is guaranteed by [12, Lemma 2.9].

However, there seems to be at last minor flaws in the proof and it seems that this algorithm has never been implemented.

1.13 An Undecidability Result in the Partial Case

Denef and Lipshitz prove [12, Theorem 4.11] that the problem "*given a system of linear PDE and an expansion point, determine if there exists a formal power series solution*" is undecidable whenever the number m of derivations is large enough (say $m \geq 9$), thanks again to the negative answer to Hilbert's Tenth Problem [20].

Observe that the generalization of the polynomial $A(q)$ to the partial differential case $m > 1$ is a multivariate polynomial $A(q_1, \ldots, q_m)$ for which we would have to find non negative integer solutions. Thus even for $m = 2$, the approach of section 1.11 cannot be applied. Here are a few details.

Let $f \in \mathscr{F}[z]$ be a polynomial in the usual sense. To fix ideas, take

$$f(z) \;=\; z^2 - 2\,. \tag{20}$$

Let $p \in \mathscr{F}\{y\}$ be the differential polynomial defined as follows, using f to form some differential operator and applying it to the differential indeterminate y

$$p \;=\; f\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\right) y\,. \tag{21}$$

Over our example, one obtains

$$p \;=\; \left(\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\right)^2 - 2\right) y\,, \;=\; x\,\frac{\mathrm{d}}{\mathrm{d}x}\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\,y\right) - 2\,y\,, \;=\; x^2\,\ddot{y} + x\,\dot{y} - 2\,y\,.$$

Fact 1. Fix the expansion point at the origin. Then

$$p(\bar{y}) \;=\; \sum_{i\geq 0} y_i\, f(i)\, x^i\,. \tag{22}$$

Fact 2. The following identities hold:

$$\begin{aligned} \frac{1}{1-x} \;&=\; \sum_{i\geq 0} x^i\,, \quad \text{and more generally,} \\ \frac{1}{1-x_1}\cdots\frac{1}{1-x_m} \;&=\; \sum_{(i_1,\ldots,i_m)\in\mathbb{N}^m} x_1^{i_1}\cdots x_m^{i_m}\,. \end{aligned}$$

Combining the two above facts, we see that the differential polynomial equation

$$\begin{aligned} p \;&=\; \frac{1}{1-x}\,, \quad \text{which is equivalent to} \\ (1-x)\,p - 1 \;&=\; 0 \end{aligned}$$

has a formal power series solution (which is convergent if it exists), centered at the origin, if and only if $y_i = 1/f(i)$ for each $i \in \mathbb{N}$. In particular, the formal power series solution exists

if and only if the polynomial f has no positive integer root. This construct generalizes to the partial case. Take any $f \in \mathscr{F}[z_1, \ldots, z_m]$ and form the differential polynomials

$$\begin{aligned} p &= f\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_m \frac{\partial}{\partial x_m}\right) y\,, \\ q &= (1 - x_1) \cdots (1 - x_m)\, p - 1\,. \end{aligned}$$

Then q has a formal power series (which is convergent if it exists), centered at the origin, if and only if the polynomial equation $f = 0$ has no positive integer solution. By [20], there does not exist any algorithm for determining whether this is the case of not, provided that m is large enough.

2 Differential Ideals — A Theorem of Zeros

2.1 Rankings are Well Orderings

A sequence of derivative operators

$$\theta_1, \theta_2, \theta_3, \ldots \tag{23}$$

is called a *Dickson sequence* if none of the θ_i divides any of its successors i.e. if, for all $k > i \geq 1$, there does not exist any derivative operator φ such that $\theta_k = \varphi\theta_i$. See Figure 1.

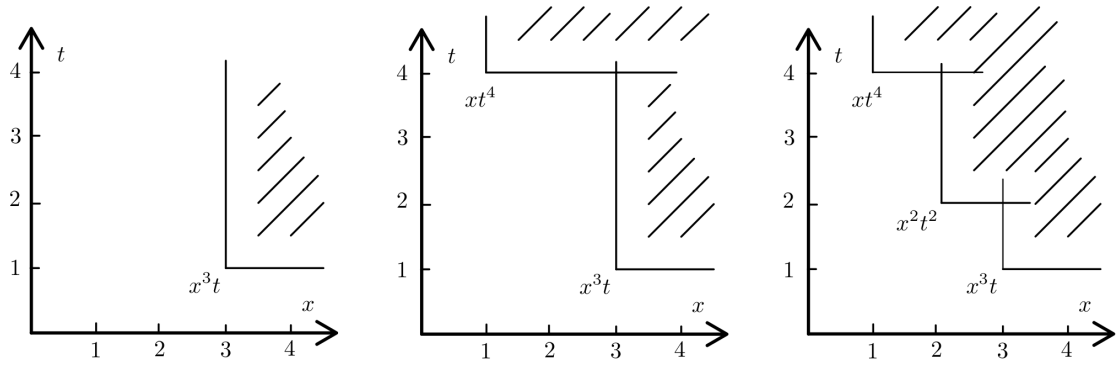

Figure 1: Graphical illustration of the beginning of a Dickson sequence in two derivations θ_1, θ_2, $\theta_3 = \delta_x^3\delta_t$, $\delta_x\delta_t^4$, $\delta_x^2\delta_t^2$. Each time a derivative operator is introduced, the set of possible following operators, corresponding to the non shaded area, shrinks. It is clear that all possible prolongations are finite, though it is possible to build sequences of arbitrary length.

Proposition 6 *(Dickson's Lemma) Every Dickson sequence is finite.*

Proof By induction on the number m of derivation operators. The Proposition is clear if $m = 1$ since every strictly decreasing sequence of nonnegative integers is finite. Assume $m > 1$ and that the Lemma holds for every Dickson sequence built with less than m derivation operators. Denote $\theta_i = \delta_1^{e_i}\varphi_i$ for all $i \geq 1$ where the derivative operators φ_i are free of the derivation operator δ_1. Every infinite sequence of nonnegative integers contains an infinite increasing subsequence. Thus if some Dickson sequence (23) were infinite, it would contain an infinite subsequence (θ_i) whose orders e_i would be increasing. The corresponding subsequence (φ_i) would then be an infinite Dickson sequence. This contradiction with the induction hypothesis concludes the proof of the Lemma. □

Let us recall the definition of rankings. Let $Y = \{y_1, \ldots, y_n\}$ be a set of differential indeterminates. A *ranking* [17, chap. I, sect. 8] is a total order on the infinite set ΘY which satisfies the two following axioms, for all derivatives $v, w \in \Theta Y$ and every derivative operator $\theta \in \Theta$:

1. $v \leq \theta v$ and
2. $v < w \Rightarrow \theta v < \theta w$.

Proposition 7 *Every ranking is a well-ordering (i.e. every strictly decreasing sequence of derivatives is finite).*

Proof If a strictly decreasing sequence of derivatives were infinite, it would contain an infinite subsequence $(\theta_i y)$ of derivatives of the same differential indeterminate y. The first axiom of rankings implies that the corresponding subsequence of derivative operators (θ_i) is a Dickson sequence. By Dickson's Lemma, such a sequence cannot be infinite. □

2.2 Autoreduced sets are Finite

A set of differential polynomials $A \subset \mathscr{R} \setminus \mathscr{F}$ is said to be *autoreduced* if its elements are pairwise reduced with respect to each other i.e. if, for every pair (p, q) of distinct elements of A, we have q reduced with respect to p.

Proposition 8 *Every autoreduced set is finite.*

Proof Let A be an autoreduced set. If A were infinite, it would contain an infinite subset of differential polynomials whose leading derivatives $\theta_i y$ would be derivatives of the same differential indeterminate y. Enumerating the corresponding derivative operators θ_i according to any order, one gets a Dickson sequence. By Dickson's Lemma, such a sequence cannot be infinite. Thus A is finite. □

2.3 Characteristic Sets as Minimal Autoreduced Sets

Let A be an autoreduced set and $p \in \mathscr{R} \setminus \mathscr{F}$ be a differential polynomial reduced with respect to A (i.e. with respect to all elements of A). Then $B = A \cup \{p\}$ is not autoreduced but, if one removes from B any differential polynomial which is not reduced with respect to p, one gets another autoreduced set A'. This process can actually be viewed as an extremely simplified version of some "completion process". It plays an important role in the theory. The following definition actually permits us to say that A' is lower than A.

Let $A = \{p_1, \ldots, p_r\}$ and $A' = \{p'_1, \ldots, p'_{r'}\}$ be two autoreduced sets such that $p_1 < \cdots < p_r$ and $p'_1 < \cdots < p'_{r'}$ (differential polynomials are ordered by increasing rank). The set A' is said to be *lower than* the set A if

1. there exists some index $j \in [1, \min(r, r')]$ such that $p'_j < p_j$ and the two subsets $\{p_1, \ldots, p_{j-1}\}$ and $\{p'_1, \ldots, p'_{j-1}\}$ have the same set of ranks ; or
2. no such j exists and $r < r'$ (longer sets are lower).

Observe that the above relation is transitive [24, chap. I, 4] and defines a total ordering on autoreduced sets of ranks. The proof of the following proposition comes from [17, chap. I, sect. 10, Prop. 3].

Proposition 9 *Every nonempty set of autoreduced sets contains a minimal element.*

Proof Let $\mathscr{A}$ be a nonempty set of autoreduced sets. Define an infinite sequence

$$\mathscr{A} = \mathscr{A}_0 \supset \mathscr{A}_1 \supset \mathscr{A}_2 \supset \cdots$$

by defining $\mathscr{A}_i$ $(i > 0)$ as the set of all the autoreduced sets belonging to $\mathscr{A}_{i-1}$, which involve at least i elements, and whose ith element has lowest possible rank, $v_i^{d_i}$. If all the subsets $\mathscr{A}_i$ were nonempty then the set of all (v_i) would form an infinite autoreduced set: a condraction to Proposition 8. Thus there exists some $i \geq 0$ such that $\mathscr{A}_i$ is nonempty and $\mathscr{A}_j = \varnothing$ for $j > i$. Any element of $\mathscr{A}_i$ is a minimal element of $\mathscr{A}$. □

The next Proposition actually is nothing but a restatement of Proposition 9.

Proposition 10 *Every strictly decreasing sequence of autoreduced sets is finite.*

Proof By Proposition 8. □

If Σ is any subset of $\mathscr{R}$ then Σ contains autoreduced subsets, since the empty set is an autoreduced set.

Definition 3 *Let Σ be any subset of $\mathscr{R}$. A* characteristic set *of Σ is any minimal autoreduced subset of Σ.*

The next proposition is emphasized in [24, chap. I, 5].

Proposition 11 *Let Σ be any subset of $\mathscr{R}$, A be a characteristic set of Σ and $p \in \mathscr{R} \setminus \mathscr{F}$ be a differential polynomial reduced with respect to A.*

Denote $\Sigma + p$ the set obtained by adjoining p to Σ.

The characteristic sets of $\Sigma + p$ are lower than A.

Corollary 1 *Let Σ be any subset of $\mathscr{R}$ and A be a characteristic set of Σ. Then Σ does not contain any differential polynomial of $\mathscr{R} \setminus \mathscr{F}$, reduced with respect to A.*

2.4 Characteristic Sets of Prime Differential Ideals

Consider a prime differential ideal $\mathfrak{P}$ different from $\mathscr{R}$. Assume a ranking is fixed and a characteristic set A of $\mathfrak{P}$ is known.

Proposition 12 *Let f be any differential polynomial of $\mathscr{R}$. Then* $\mathrm{fullrem}(f, A) = 0$ *if and only if $f \in \mathfrak{P}$.*

Proof Denote $g = \mathrm{fullrem}(f, A)$. The implication $\Leftarrow$ from right to left. Assume $f \in \mathfrak{P}$. Since $A \subset \mathfrak{P}$ we have $g \in \mathfrak{P}$ by the relation (7) of Proposition 3. The differential polynomial g cannot belong to $\mathscr{R} \setminus \mathscr{F}$ by Corollary 1, since it is reduced with respect to all elements of A. It cannot be a nonzero element of $\mathscr{F}$ because $\mathfrak{P} \neq \mathscr{R}$. Thus $g = 0$.

The implication $\Rightarrow$ from left to right. Assume $g = 0$. Then the product $h\, f \in \mathfrak{P}$. By Corollary 1, the initials and separants of A do not belong to $\mathfrak{P}$ since they are reduced with respect to all elements of A. Since h is a power product of these initials and separants and $\mathfrak{P}$ is prime, we have $f \in \mathfrak{P}$. □

2.5 Differential Ideals Defined by Characteristic Sets

The following notations are defined in [17, chap. sect. 0, 1; and chap. I, sect. 9]. In Kolchin's book, the notation $[A] : H_A^\infty$ seems to occur for the first time in [17, chap. IV, sect. , Lemma 2].

If S is a subset and $\mathfrak{A}$ is an ideal of $\mathscr{R}$ then $\mathfrak{A} : S^\infty$ is the ideal of the elements $p \in \mathscr{R}$ such that, for some power product h of elements of S, we have $h\, p \in \mathfrak{A}$ (if $\mathfrak{A}$ is a differential ideal, so is $\mathfrak{A} : S^\infty$). An alternative definition is provided by means of a localization [18, chap. II, 3]: if M denotes the multiplicative family generated by S and $M^{-1}\mathfrak{A}$ denotes the ideal generated by $\mathfrak{A}$ in the localized ring $M^{-1}\mathscr{R}$, then $\mathfrak{A} : S^\infty = M^{-1}\mathfrak{A} \cap \mathscr{R}$.

Denote now H_A the set of the initials and separants of A. Proposition 12 implies that, if A is a characteristic set of a prime differential ideal $\mathfrak{P}$ then

$$\mathfrak{P} \;=\; [A] : H_A^\infty \,.$$

2.6 The Ritt-Raudenbush Basis Theorem

It is the key to Theorem 4. The differential polynomial ring is $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$. The two next propositions are slight adaptations of [24, chap. I, 10].

Proposition 13 *Let f, g be two differential polynomials and $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$ such that $f\,g \in \mathfrak{A}$. Then, for all derivative operators θ, φ, the product $(\theta f)(\varphi g) \in \mathfrak{A}$.*

Proof The proof is by induction on the sum of the orders of the derivative operators θ and φ. The basis of the induction (case of two operators of order zero) holds by assumption. Assume that the Proposition holds for all derivative operators θ, φ such that the sum of their orders is equal to some positive integer and consider any derivation operator δ. Then, differentiating $(\theta f)(\varphi g)$, we have $(\delta\theta f)(\varphi g) + (\theta f)(\delta\varphi g) \in \mathfrak{A}$ Multiply by θf and use the fact that $(\theta f)(\varphi g) \in \mathfrak{A}$ (induction hypothesis). Then $(\theta f)^2(\delta\varphi g) \in \mathfrak{A}$ and, since $\mathfrak{A}$ is perfect, $(\theta f)(\delta\varphi g) \in \mathfrak{A}$. The fact that $(\delta\theta f)(\varphi g) \in \mathfrak{A}$ is proved similarly. □

Proposition 14 *Let f, g be two differential polynomials and Σ be a set of differential polynomials of $\mathscr{R}$. Then $\{\Sigma + f\,g\} = \{\Sigma + f\} \cap \{\Sigma + g\}$.*

Proof The inclusion $\subset$ is clear. Let us prove the converse one. Let $h \in \{\Sigma + f\} \cap \{\Sigma + g\}$. Then there exist differential polynomials $p, q \in [\Sigma]$, $\overline{f} \in [f]$, $\overline{g} \in [g]$ and, by Proposition 1, a positive integer t such that $h^t = p + \overline{f}$ and $h^t = q + \overline{g}$. Multiply these two equalities termwise. Then there exists a differential polynomial $r \in [\Sigma]$ such that $h^{2t} = r + \overline{f}\,\overline{g}$. Since $\overline{f} \in [f]$ and $\overline{g} \in [g]$, there exist finitely many differential polynomials $m_{\theta,\varphi}$ such that

$$\overline{f}\,\overline{g} \;=\; \sum_{\theta,\varphi\in\Theta} m_{\theta,\varphi}\,(\theta f)(\varphi g)\,.$$

The product $f\,g \in \{\Sigma + f\,g\}$. Thus, by Proposition 13, every product $(\theta f)(\varphi g) \in \{\Sigma + f\,g\}$. Thus we have $h \in \{\Sigma + f\,g\}$. □

The remaining part of this section comes from [24, chap. I, 12-16]. Let Σ be an infinite subset of $\mathscr{R}$. A subset Φ of Σ is said to be a *basis* of Σ if Φ is finite and $\Sigma \subset \{\Phi\}$.

Lemma 3 *Let Σ be an infinite subset of $\mathscr{R}$. If Σ contains a nonzero element of $\mathscr{F}$ then Σ has a basis.*

Proof Let a be any nonzero element of $\Sigma \cap \mathscr{F}$. Then the set $\{a\}$ is a basis of Σ. □

It is sometimes useful to have at our disposal a version of the Ritt-Raudenbush Basis Theorem for $\mathscr{F}[[x_1, \ldots, x_m]]\{y_1, \ldots, y_n\}$ i.e. differential polynomial rings over rings of formal power series or, more simply, for $\mathscr{F}[x_1, \ldots, x_m]\{y_1, \ldots, y_n\}$. Such generalized versions of the Theorem actually hold. They can be proved using the same proof as below by slightly generalizing Lemma 3 to cover the case of a base ring element a, a derivative of which is invertible. See [5] for more details.

Theorem 1 *(Ritt-Raudenbush Basis Theorem) Every infinite subset of $\mathscr{R}$ has a basis.*

Proof We assume that there exist infinite subsets of $\mathscr{R}$ with no basis and seek a contradiction. Let Σ be such a subset and assume moreover that, among all infinite sets with no basis, Σ is such that its characteristic sets are minimal.

Let A be a characteristic set of Σ.

"Perform" Ritt's full reduction algorithm, with respect to A, over all $q \in \Sigma \setminus A$. For each $q \in \Sigma \setminus A$, there exists a power product h_q of initials and separants of A and a differential polynomial g_q, reduced with respect to A such that

$$h_q\, q \;=\; g_q \mod [A]\,. \tag{24}$$

Introduce the two following sets (the plus sign standing for "union"):

$$\begin{aligned} \Lambda &= \{h_q\, q \mid q \in \Sigma \setminus A\} + A\,, \\ \Omega &= \{g_q \mid q \in \Sigma \setminus A\} + A\,. \end{aligned}$$

The set Ω must have a basis. Indeed, if it contains any nonzero element of $\mathscr{F}$ it has a basis by Lemma 3. Otherwise, since the differential polynomials g_q are reduced with respect to A, its characteristic sets are lower than A by Proposition 11 thus it cannot lack a basis by the minimality assumption on Σ.

Thus there exist finitely many differential polynomials $q_1, \ldots, q_t \in \Sigma \setminus A$ such that the set $\Phi = \{g_{q_1}, \ldots, g_{q_t}\} + A$ is a basis of Ω (observe that is is always possible to enlarge a basis with finitely many further differential polynomials).

Claim: the set $\Psi = \{h_{q_1}\, q_1, \ldots, h_{q_t}\, q_t\} + A$ is a basis of Λ.

Each $h_{q_i}\, q_i - g_{q_i}$ $(1 \leq i \leq t)$, belongs to the perfect differential ideals $\{\Phi\}$ and $\{\Psi\}$ by Proposition 3 and the fact that A is a subset of both Φ and Ψ.

Thus, since each $g_{q_i} \in \Phi$ $(1 \leq i \leq t)$, we see that each $h_{q_i}\, q_i \in \{\Phi\}$ $(1 \leq i \leq t)$ and $\Psi \subset \{\Phi\}$. Conversely, since each $h_{q_i}\, q_i \in \Psi$, we see that each $g_{q_i} \in \{\Psi\}$ and $\Phi \subset \{\Psi\}$. Thus both perfect differential ideals $\{\Phi\}$ and $\{\Psi\}$ are equal.

Since Φ is a basis of Ω we have $\Omega \subset \{\Phi\}$. Since the full remainder g_q of each $q \in \Sigma$ belongs to Ω, we see that the corresponding product $h_q\, q$ of each $q \in \Sigma$ belongs to $\{\Omega\}$, which is included in $\{\Phi\} = \{\Psi\}$. Thus $\Lambda \subset \{\Psi\}$ and the claim is proved.

Let $f_1, \ldots, f_s$ denote the initials and separants of A. By Lemma 4, there exists an index $1 \leq i \leq s$ such that the set $\Sigma + f_i$ has no basis. The differential polynomial $f_i \notin \mathscr{F}$ by Lemma 3. Thus the set $\Sigma + f_i$ has a characteristic set lower than A by Proposition 11. This contradiction with the minimality assumption on Σ completes the proof of the Theorem. □

The next Lemma is involved in the proof of the Ritt-Raudenbush Basis Theorem. The differential polynomials f_i actually are the initials and separants of some characteristic set of Σ.

Lemma 4 *Let Σ be an infinite subset of $\mathscr{R}$ and $f_1, \ldots, f_s$ be differential polynomials of $\mathscr{R}$. Let*

$$\Lambda \;=\; \{h_q\, q \mid q \in \Sigma \text{ and } h_q \text{ is some power product of } f_1, \ldots, f_s\}\,.$$

If Σ has no basis and Λ has a basis then at least one of the sets $\Sigma + f_i$, for $1 \leq i \leq s$, has no basis.

Proof We assume that all sets $\Sigma + f_i$ $(1 \leq i \leq s)$ have a basis and seek a contradiction.

Let $\Psi = \{h_{q_1}\, q_1, \ldots, h_{q_t}\, q_t\}$ be a basis of Λ. Since a basis can always be enlarged as long as it remains finite, there exists some finite set $\Phi \subset \Sigma$ such that: 1) $\Phi + f_i$ is a basis of $\Sigma + f_i$ $(1 \leq i \leq s)$ and; 2) $q_1, \ldots, q_t \in \Phi$. Let g denote the product $f_1 \cdots f_s$.

By Proposition 14, the perfect differential ideal $\{\Sigma + g\}$ is the intersection of the perfect differential ideals $\{\Sigma + f_i\}$ $(1 \leq i \leq s)$; similarly, the perfect differential ideal $\{\Phi + g\}$ is the intersection of the perfect differential ideals $\{\Phi + f_i\}$. Since each $\Phi + f_i$ is a basis of $\Sigma + f_i$ we have

$$\{\Sigma + g\} \;=\; \bigcap_{i=1}^{s} \{\Sigma + f_i\} \;\subset\; \bigcap_{i=1}^{s} \{\Phi + f_i\} \;=\; \{\Phi + g\}\,.$$

Thus $\Phi + g$ is a basis of $\Sigma + g$.

Thus, for each differential polynomial $p \in \Sigma$, there exists a relation

$$p^d \;=\; r + m_1\, \theta_1 g + \cdots + m_e\, \theta_e g$$

where $d \geq 1$, $e \geq 0$, the m_i are differential polynomials of $\mathscr{R}$ and $r \in [\Phi]$. Multiplying by p we get

$$p^{d+1} \;=\; r\, p + m_1\, p\, \theta_1 g + \cdots + m_e\, p\, \theta_e g \tag{25}$$

Since $q_1, \ldots, q_t \in \Phi$ we have $\Psi \subset \{\Phi\}$. Since, moreover, $p \in \Sigma$ and g is the product of the f_i, we have $p\, g \in \{\Lambda\} \subset \{\Psi\} \subset \{\Phi\}$. Thus, by Proposition 14, we have $p\, \theta_i g \in \{\Phi\}$ for $1 \leq i \leq e$. Since $r \in [\Phi]$ we have $r\, p \in \{\Phi\}$. Thus, using (25), we have $p \in \{\Phi\}$, which means that Φ is a basis of Σ: the sought contradiction. □

Corollary 2 *Let $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$. Then there exists a finite $\Phi \subset \mathfrak{A}$ such that $\mathfrak{A} = \{\Phi\}$.*

Theorem 2 *Every perfect differential ideal $\mathfrak{A}$ is a finite intersection of prime differential ideals.*

Proof We assume that there exists some perfect differential ideal $\mathfrak{A}$ with no such presentation and seek a contradiction. The perfect differential ideal $\mathfrak{A}$ thus cannot be prime. Let f, g be two differential polynomials such that the product $f\, g \in \mathfrak{A}$ but $f, g \notin \mathfrak{A}$. By Proposition 13 we have $\mathfrak{A} = \{\mathfrak{A} + f\} \cap \{\mathfrak{A} + g\}$. At least one of these two perfect differential ideals — say $\mathfrak{A}_1 = \{\mathfrak{A} + f\}$ — is not a finite intersection of prime differential ideals; and we have $\mathfrak{A} \subsetneq \mathfrak{A}_1$. Repeating this argument, we see that there exists an infinite sequence of perfect differential ideals

$$\mathfrak{A} \subsetneq \mathfrak{A}_1 \subsetneq \mathfrak{A}_2 \subsetneq \cdots \tag{26}$$

Let Ω be the union of all these ideals. By the Ritt-Raudenbush Basis Theorem, there exists a finite set $\Phi \subset \Omega$ such that $\Omega \subset \{\Phi\}$. The set Φ must be a subset of some $\mathfrak{A}_t$ in (26). Thus $\mathfrak{A}_{t+1} \subset \{\Phi\} \subset \mathfrak{A}_t$. This contradiction with the fact that the inclusions of (26) are strict completes the proof of the Theorem. □

Let $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$. A representation

$$\mathfrak{A} \quad = \quad \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_\varrho \tag{27}$$

of $\mathfrak{A}$ as an intersection of prime differential ideals $\mathfrak{P}_i$ is said to be *minimal* if, for all indices $1 \leq i, j \leq \varrho$ such that $i \neq j$ we have $\mathfrak{P}_i \not\subset \mathfrak{P}_j$. Anticipating on Theorem 3, these prime differential ideals are uniquely defined. Ritt calls them the *essential prime divisors* of $\mathfrak{A}$ [24, chap. I, 17]. We prefer to call them the *essential components* of $\mathfrak{A}$.

Theorem 3 *There exists a unique minimal representation of a perfect differential ideal $\mathfrak{A}$ as a finite intersection of prime differential ideals.*

Proof The existence comes from Theorem 2.

For the uniqueness, fix some representation (27). It suffices to prove that if $\mathfrak{P}$ is a prime differential ideal such that $\mathfrak{A} \subset \mathfrak{P}$ then there exists some index $1 \leq i \leq \varrho$ such that $\mathfrak{P}_i \subset \mathfrak{P}$. If this were not the case then each $\mathfrak{P}_i$ would contain some differential polynomial f_i such that $f_i \notin \mathfrak{P}$ $(1 \leq i \leq \varrho)$. Since $\mathfrak{P}$ is prime, the product $f = f_1 \cdots f_\varrho$ would not belong to $\mathfrak{P}$ either. However, it would belong to $\mathfrak{A}$. This contradiction with the hypothesis $\mathfrak{A} \subset \mathfrak{P}$ completes the proof of the Theorem. □

The following example comes from [24, chap. II, 8].

$$\{\dot{y}^2 - 4\,y\} \quad = \quad [\dot{y}^2 - 4\,y\,, \ddot{y} - 2] \cap [y]\,.$$

The differential polynomial $\dot{y}^2 - 4\,y$ is irreducible but its first derivative actually factors as $2\,\dot{y}\,(\ddot{y} - 2)$. The perfect differential ideal on the left hand side of (28) is not prime. It has two essential components, given on the right hand side of (28). The solution of the first component is the family of parabolas $(x + c)^2$ where c is an arbitrary constant. The solution of the second component is the zero function. The singleton $\dot{y}^2 - 4\,y$ is a characteristic set of the prime differential ideal $[\dot{y}^2 - 4\,y\,, \ddot{y} - 2]$.

A variant comes from [24, chap II, 19]. The perfect differential ideal generated by $\dot{y}^2 - 4\,y^3$ is actually prime. Its solution is the family of functions $(x + c)^{-2}$ where c is an arbitrary constant. The zero function also is a solution but (quoting Ritt) "we see, letting $|c|$ increase, that a differential polynomial which vanishes for every $(x + c)^{-2}$ vanishes for $y = 0$. Thus $y = 0$ is in the general solution". The prime differential ideal $[y]$ is not an essential component of $\{\dot{y}^2 - 4\,y^3\}$. See also [17, chap. IV, sect. 15, Remark 1].

2.7 Zeros of a Prime Differential Ideal

This section is much inspired by papers of Seidenberg. See the proof of [26, Theorem 6].

The differential polynomial ring is $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$ endowed with m derivations. We may with no loss of generality assume that all differential polynomials are autonomous (see section 1.8). Since we are going to solve polynomial systems and look for solutions in $\mathscr{F}$, there are constraints on $\mathscr{F}$. The content of this section is valid if $\mathscr{F}$ is a universal field extension of the field $\mathbb{Q}$ of the rational numbers (i.e. if $\mathscr{F}$ is algebraically closed and has an infinite transcendence degree over $\mathbb{Q}$) [31, chap. VI, 5bis]. To fix ideas, we may consider that $\mathscr{F}$ is the field $\mathbb{C}$ of the complex numbers.

Consider a prime differential ideal $\mathfrak{P}$ different from $\mathscr{R}$. Assume a ranking is fixed and a characteristic set A of $\mathfrak{P}$ is known. Denote $p_1, \ldots, p_r$ the elements of A and assume that $p_1 < \cdots < p_r$.

Denote X the finite set of the derivatives A depends on and $V \subset X$ the set of leading derivatives of A. Then $\Theta Y \setminus \Theta V$ denotes the possibly infinite set of the elements of ΘY which are not the derivative of any element of V. Let Θ^* denote the set of all proper derivative operators. Then $\Theta^* V$ denotes the set of all derivatives which are proper derivatives of some element of V. The three sets V, $\Theta Y \setminus \Theta V$ and $\Theta^* V$ are pairwise disjoint. Their union is ΘY.

As an example, consider the non autonomous differential polynomial $x\,y^2 + y - 1$ of $\mathscr{F}[x]\{y\}$. By reduction to the autonomous case (section 1.8), transform it into an equivalent autonomous characteristic set $A = \{\dot{y}_1 - 1,\ y_1\,\dot{y}_2^2 + y_2 - 1\}$ of the prime differential ideal $\mathfrak{P} = [A] : H_A^\infty$ of $\mathscr{F}\{y_1, y_2\}$. Then $X = \{\dot{y}_1,\ y_1,\ \dot{y}_2,\ y_2\}$ and $V = \{\dot{y}_1, \dot{y}_2\}$ and $\Theta Y \setminus \Theta V$ is the set of all the derivatives of y_1 and y_2 of order at least two,

Process. The following process builds a tuple of n formal power series $s_i(x_1, \ldots, x_m)$ defined by

$$s_i(x_1, \ldots, x_m) \;=\; \sum_{\theta = \delta_1^{e_1} \cdots \delta_m^{e_m} \in \Theta} y_{i,\theta}\, x_1^{e_1} \cdots x_m^{e_m} \tag{28}$$

by assigning values $y_{i,\theta} \in \mathscr{F}$ to all derivatives $\theta y_i \in \Theta Y$. This process is nothing but a generalization of the approach sketched in section 1.6.

1. Solve the following system as a nondifferential polynomial system of $\mathscr{F}[X]$, where h denotes the product of the initials and separants of A

$$p_1 = \cdots = p_r = 0\,, \quad h \neq 0\,.$$

2. Assign any value from $\mathscr{F}$ to the derivatives of $\Theta Y \setminus \Theta V$ which were not already assigned values at Step 1.

3. Let v be any element of $\Theta^* V$. By Ritt's partial reduction process, compute a power product h of separants of A and a differential polynomial g such that

$$h\,v \;=\; g \mod [A]\,. \tag{29}$$

Then assign to v the value of g/h.

Remarks.

- the polynomial system to be solved at Step 1 is triangular in the sense that each equation $p_i = 0$ introduces at least one indeterminate;
- if the field $\mathscr{F}$ is the field of the complex numbers, which is algebraically closed, the polynomial system to be solved has solutions;
- over our example, the inequation is $y_1 \neq 0$, which forbids the initial value $y_{1,1} = 0$ hence forbids the origin as expansion point when considering the non autonomous differential polynomial we started with;
- at Step 3, the differential polynomials h and g depend on derivatives which were assigned values at Steps 1 and 2.

Proposition 15 *The tuple of formal power series* (28) *provides a zero of the prime differential ideal* $\mathfrak{P}$.

Proof We prove that the coefficients $y_{\ell,\theta}$ computed by the process annihilate every $f \in \mathfrak{P}$.

The proof is by induction on the leading derivative $v = \theta y_\ell$ of the differential polynomials $f \in \mathfrak{P}$, ordered by the ranking. This transfinite induction [30, chap. 9, 4] is allowed by Proposition 7.

Basis. Thanks to Proposition 12, the elements $f \in \mathfrak{P}$ with lowest leading derivative satisfy $h\,f = q\,p_1$ where h is a power of the initial of p_1 (the lowest element of A) and q is some differential polynomial. Since p_1 is annihilated by the coefficients $y_{\ell,\theta}$ and h is not, the differential polynomial f must vanish.

General case. Let v be the leading derivative of some $f \in \mathfrak{P}$. Assume (induction hypothesis) that every element of $\mathfrak{P}$ with leading derivative less than v is annihilated by the coefficients $y_{\ell,\theta}$. We may assume, without loss of generality, that the initial of f does not belong to $\mathfrak{P}$. Thus, thanks to Proposition 12, we must have $v \in \Theta V$.

Subcase 1. Assume $v \in V$. Perform Ritt's full reduction algorithm over f. Then there exists a power product h of initials and separants of A such that $h\,f \in [A]$ by Propositions 3 and 12. Observe now that, in this reduction process, the first pseudodivision is performed with respect to the differential polynomial $p_i \in A$ with leading derivative v. The following pseudodivisions are performed with respect to differential polynomials of ΘA with leading derivatives strictly less than v; and the differential polynomial h does not depend either on any derivative greater than or equal to v. Removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that there exists a differential polynomial q such that $h\,f = q\,p_i$. Since p_i is annihilated by the coefficients $y_{\ell,\theta}$ and h is not, the differential polynomial f must vanish.

Subcase 2. Assume $v \in \Theta^* V$ and that there is a single differential polynomial $p_i \in A$, with leading derivative v_i such that, for some $\theta \in \Theta^*$, we have $v = \theta v_i$.

Consider Ritt's partial reduction (29) which yielded the value of v. In this reduction process, the first pseudodivision is performed with respect to θp_i and since the differential polynomial to be reduced is a mere derivative, the first pseudoquotient is 1. Then, argumenting as in Subcase 1 and removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that $h\, v = g + \theta p_i$. Since the value assigned to v is g/h, we see that the coefficients $y_{\ell,\theta}$ annihilate θp_i.

Perform now Ritt's full reduction algorithm over f. Then there exists a power product h of initials and separants of A such that $h\, f \in [A]$ by Proposition 3. Argumenting as in Subcase 1 and removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that there exists a differential polynomial q such that $h\, f = q\, \theta p_i$. Since θp_i is annihilated by the coefficients $y_{\ell,\theta}$ and h is not, the differential polynomial f must vanish.

Subcase 3. Assume $v \in \Theta^* V$ and that there exist many different (say two) differential polynomials $p_i, p_j \in A$, with leading derivatives v_i, v_j such that, for some $\theta_i, \theta_j \in \Theta^*$, we have $v = \theta_i v_i = \theta_j v_j$.

One of these two differential polynomials (say p_i) was used to assign a value to v. As proved in Subcase 2, the differential polynomial $\theta_i p_i$ is annihilated by the coefficients $y_{\ell,\theta}$.

Denote s_i and s_j the separants of p_i and p_j. The cross derivative $s_j\, \theta_i p_i - s_i\, \theta_j p_j$ belongs to $\mathfrak{P}$ and either is zero or has a leading derivative strictly less than v. Thus it is annihilated by the coefficients $y_{\ell,\theta}$, according to the induction hypothesis. Since $\theta_i p_i$ is annihilated and the separants are not, the differential polynomial $\theta_j p_j$ must vanish also.

Perform now Ritt's full reduction algorithm over f. Argumenting as in Subcase 2, we see that f must vanish at the coefficients $y_{\ell,\theta}$ also. □

In the proof of the next Proposition, some field $\mathscr{D}$ is introduced. This field seems to be a *field of definition*, which is a notion introduced in [17, chap. III, sect. 3].

Proposition 16 *Let f be a differential polynomial and $\mathfrak{P}$ be a prime differential ideal of $\mathscr{R}$.*
If $f \notin \mathfrak{P}$ then $\mathfrak{P}$ has a zero which does not annihilate f.

Proof The idea of the proof consists in proving that $\mathfrak{P}$ has a *generic* (or *general*) zero $(y_{\ell,\theta})$ i.e. a zero which only annihilates the elements of $\mathfrak{P}$. A zero $(y_{\ell,\theta})$ is generic if $\mathscr{F}(y_{\ell,\theta})$ is isomorphic to the field of fractions of $\mathscr{R}/\mathfrak{P}$. See [30, chap. 16].

In the field of fractions of $\mathscr{R}/\mathfrak{P}$, the derivatives in $\Theta Y \setminus \Theta V$ are transcendental over $\mathscr{F}$. This is an easy corollary to Proposition 12. Moreover, the process described at the beginning of this section for building a zero of $\mathfrak{P}$ shows that, for every derivative $v \in \Theta V$, the set $(\Theta Y \setminus \Theta V) + v$ is algebraically dependent over $\mathscr{F}$ in $\mathscr{R}/\mathfrak{P}$. Thus $\Theta Y \setminus \Theta V$ provides a transcendence basis of the field of fractions of $\mathscr{R}/\mathfrak{P}$ over $\mathscr{F}$.

In order to obtain a zero $(y_{\ell,\theta})$ of $\mathfrak{P}$ which does not annihilate f, it is thus sufficient to assign to the derivatives in $\Theta Y \setminus \Theta V$, values which are transcendental over $\mathscr{F}$.

The issue (solved below) is that the coordinates of $(y_{\ell,\theta})$ belong to $\mathscr{F}$ thus cannot be transcendental over $\mathscr{F}$.

Perform Ritt's full reduction algorithm over f using some characteristic set A of $\mathfrak{P}$. Then, by Proposition 3, there exists a power product h of initials and separants of A and differential polynomials $g, m_{i,\theta}$ such that

$$h\, f \;=\; g + \sum_{\substack{1 \leq i \leq r,\\ \theta \in \Theta}} m_{i,\theta}\; \theta p_i\,.$$

Since Ritt's reduction algorithm is "rational", the above formula holds in any differential polynomial ring $\mathscr{D}\{y_1, \ldots, y_n\}$ such that $\mathscr{D}$ contains the rational numbers plus the finitely many coefficients of f and the elements of the characteristic set A. We can thus choose for $\mathscr{D}$ a finite extension of the field of the rational numbers, over which the field $\mathscr{F}$ has an infinite degree of transcendency.

Thus, assigning values in $\mathscr{F}$ which are transcendental over $\mathscr{D}$ to the derivatives in $\Theta Y \setminus \Theta V$, we obtain a generic zero $(y_{\ell,\theta})$ of the prime differential ideal $\mathfrak{P} \cap \mathscr{D}\{y_1, \ldots, y_n\}$. Since $f, g \notin \mathfrak{P}$, they do not belong to $\mathfrak{P} \cap \mathscr{D}\{y_1, \ldots, y_n\}$ either so that they are not annihilated by $(y_{\ell,\theta})$. In the differential polynomial ring $\mathscr{R}$, the zero $(y_{\ell,\theta})$ is no more generic but it still does not annihilate f, which is the result we are looking for. □

2.8 A Differential Theorem of Zeros

Let $\mathscr{F}$ be a universal extension of the field of the rational numbers. To fix ideas, one may let $\mathscr{F}$ be the field $\mathbb{C}$ of the complex numbers. Let $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$ endowed with m derivations.

Theorem 4 *(Differential Theorem of Zeros)*

Let $p_1 = \cdots = p_r = 0$ be a system of polynomial differential equations and f be a differential polynomial of $\mathscr{R}$. Let $\mathfrak{A} = \{p_1, \ldots, p_r\}$ be the perfect differential ideal of $\mathscr{R}$ generated by the left hand sides of the equations.

If $f \in \mathfrak{A}$ then f annihilates over every solution of the system of equations.

Conversely, if every solution of the system of equations annihilates f then $f \in \mathfrak{A}$.

Proof The first statement is clear and is valid for any field $\mathscr{F}$. For the second statement, we assume $f \notin \mathfrak{A}$ and prove that the system of equations has a solution which does not annihilate f. By Theorem 3, there exists a prime differential ideal $\mathfrak{P}$ such that $\mathfrak{A} \subset \mathfrak{P}$ and $f \notin \mathfrak{P}$. By Proposition 16, the prime differential ideal $\mathfrak{P}$ has a zero which does not annihilate f. This zero is a solution of the system of equations. □

The Theorem implies that a system has no solution if and only if $1 \in \mathfrak{A}$ where $\mathfrak{A}$ denotes the perfect differential ideal that generated by the system. As we shall see in Theorem 12, there exists an algorithm which decides if $1 \in \mathfrak{A}$ and, more generally, membership to $\mathfrak{A}$.

The proof of the Theorem relies on the existence of a formal power series of some prime differential ideal $\mathfrak{P}$ avoiding the differential polynomial f (Proposition 16). Observe that

there are constraints on the possible initial values of that formal power series — hence constraints on the possible expansion points of the formal power series, if $p_1, \ldots, p_r$ are obtained by reduction to the autonomous case of some non autonomous system. Thus, in the non autonomous case, the Theorem still holds provided that the formal power series under consideration belong to $\mathscr{F}[[x_1 - \alpha_1, \ldots, x_m - \alpha_m]]$ where $(\alpha_1, \ldots, \alpha_m)$ is an expansion point left unspecified.

Recall that, if the expansion point is fixed then the existence problem of formal power series solutions is undecidable (section 1.13).

3 Regular Differential Chains

This section aims at explaining the ideas of regular differential chains and the related decomposition algorithms. A key theorem — absent from Ritt and Kolchin books — is Theorem 6. The key issue to be solved is: given a triangular set A defining some ideal $\mathfrak{a}$, how to decide whether a polynomial is a zerodivisor modulo $\mathfrak{a}$? The progression of the following sections is much inspired from [10].

3.1 The Lasker-Noether Theorem

Let $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$ be a polynomial ring over a field of characteristic zero. The ring $\mathscr{R}$ is Noetherian (because the number of variables is finite). See [31, chap. IV].

An ideal $\mathfrak{p} \subset \mathscr{R}$ is *prime* if, for all $a, b \in \mathscr{R}$ we have $a\,b \in \mathfrak{p} \Rightarrow [a \in \mathfrak{p}$ or $b \in \mathfrak{p}]$.

An ideal $\mathfrak{q} \subset \mathscr{R}$ is *primary* if, for all $a, b \in \mathscr{R}$ we have $a\,b \in \mathfrak{q} \Rightarrow [a \in \mathfrak{q}$ or $\exists\, e \in \mathbb{N}, b^e \in \mathfrak{q}]$.

Every prime ideal is primary.

If $\mathfrak{q}$ is a primary ideal then its radical is a prime ideal $\mathfrak{p}$, called the *associated prime* ideal of $\mathfrak{q}$.

Every intersection of primary ideals $\mathfrak{q}_i$ can be made *minimal* by applying two theoretical processes:

- removal of the $\mathfrak{q}_i$ which contain some other $\mathfrak{q}_j$;
- gluing in a single primary ideal subsets of primary ideals whose intersection is itself primary.

Theorem 5 *(Lasker-Noether Theorem)*
Every ideal $\mathfrak{a}$ of $\mathscr{R}$ is a finite minimal intersection of primary ideals:

$$\mathfrak{a} \;=\; \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r\,. \tag{30}$$

Such a minimal primary decomposition *of $\mathfrak{a}$ is not necessarily unique but, if*

$$\mathfrak{a} \;=\; \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{r'}$$

is another minimal primary decomposition of $\mathfrak{a}$ *then, the number of components is the same (i.e.* $r = r'$*) and the set of the associated prime ideals* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *of the two decompositions is uniquely defined (the* $\mathfrak{p}_i$ *are called the* associated prime *ideals of* $\mathfrak{a}$*).*

If $\mathfrak{q}_i$ and $\mathfrak{q}_j$ are two primary components of a minimal primary decomposition of $\mathfrak{a}$ then $\mathfrak{q}_i \not\subset \mathfrak{q}_j$ but it may happen that $\mathfrak{p}_i \subset \mathfrak{p}_j$.

An associated prime ideal of $\mathfrak{a}$ is said to be *isolated* if it does not contain any other associated prime ideal of $\mathfrak{a}$.

An associated prime ideal of $\mathfrak{a}$ which is not isolated is said to be *embedded* (or *imbedded*).

The radical of an ideal $\mathfrak{a}$ is the intersection of the associated prime ideals of $\mathfrak{a}$. Since embedded associated prime ideals are redundant in this intersection, we see that the radical of an ideal $\mathfrak{a}$ is the intersection of its isolated associated prime ideals.

As an example, consider the ideal

$$\mathfrak{a} \;=\; (p_1, p_2) \;=\; (x_1\,(x_1 + t_1),\, t_1\,x_1\,x_2)$$

of $\mathscr{R} = \mathscr{F}[t_1, x_1, x_2]$. A minimal primary decomposition is

$$\begin{array}{rcccccc} \mathfrak{a} & = & \mathfrak{q}_1 & \cap & \mathfrak{q}_2 & \cap & \mathfrak{q}_3\,, \\ & = & (x_1) & \cap & (t_1,\, x_1^2) & \cap & (x_2,\, x_1 + t_1)\,. \end{array}$$

The associated prime ideals of $\mathfrak{a}$ are $\mathfrak{p}_1 = (x_1)$ which is isolated, $\mathfrak{p}_2 = (t_1,\, x_1)$ which is embedded since it contains $\mathfrak{p}_1$ and $\mathfrak{p}_3 = (x_2,\, x_1 + t_1)$ which is isolated. Then

$$\sqrt{\mathfrak{a}} \;=\; \mathfrak{p}_1 \cap \mathfrak{p}_3 \;=\; (x_1\,(x_1 + t_1),\, x_1\,x_2)\,.$$

An element f of a ring $\mathscr{S}$ is said to be a *zerodivisor* if there exists some nonzero $g \in \mathscr{S}$ such that $f\,g = 0$. An element which is not a zerodivisor is said to be *regular*. Thus a polynomial $f \in \mathscr{R}$ is a zerodivisor modulo an ideal $\mathfrak{a}$ if there exists some $g \in \mathscr{R}$ such that $g \notin \mathfrak{a}$ and $f\,g \in \mathfrak{a}$.

The set of the zerodivisors modulo $\mathfrak{a}$ (or in $\mathscr{R}/\mathfrak{a}$) is the union of associated prime ideals of $\mathfrak{a}$ (isolated *and embedded*). Over our example, $t_1 \in \mathfrak{p}_2$ is a zerodivisor modulo $\mathfrak{a}$.

Let $h \in \mathscr{R}$ be any polynomial. Then the saturation of $\mathfrak{a}$ by h, denoted $\mathfrak{a} : h^\infty$, is the intersection of the primary components $\mathfrak{q}_i$ of $\mathfrak{a}$ whose associated prime ideal $\mathfrak{p}_i$ does not contain h. Thus h is a zerodivisor modulo $\mathfrak{a}$ if and only if $\mathfrak{a} \neq \mathfrak{a} : h^\infty$; and h is regular (i.e. not a zerodivisor) modulo $\mathfrak{a} : h^\infty$.

3.2 Ideals Defined by Triangular Sets

Let $A = \{p_1, \ldots, p_r\}$ be a set of polynomials of the ring $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$ such that $\deg(p_i, x_i) > 0$ and $\deg(p_i, x_{i+j}) = 0$ for $1 \leq j \leq r - i$. Such a set A is said to be *triangular*. The variable x_i is the *leading variable* of p_i (it is the analogue of the leading derivative in the context of differential algebra). The initial and the separant of p_i are the leading coefficient of p_i with respect to x_i and the polynomial $\partial p_i/\partial x_i$. The product of the initials is $I_A = i_1 \cdots i_r$.

Definition 4 *(ideal defined by a triangular set)*
The ideal defined *by the triangular set A is the ideal $\mathfrak{a} = (A) : I_A^\infty$.*

Over our example, we have $I_A = t_1\, x_1$ and

$$(A) : I_A^\infty \;\; = \;\; \mathfrak{q}_3$$

In the sequel, we will also consider the ideals $(A) : S_A^\infty$ and $(A) : H_A^\infty$ where S_A is the product of the separants of A and H_A is the product of the initials and the separants of A.

We will also often need to consider the polynomial ring $\mathscr{R}' = \mathscr{F}[x_1, \ldots, x_{r-1}, t_1, \ldots, t_m]$ (so that $\mathscr{R} = \mathscr{R}'[x_r]$), the triangular set $A' = \{p_1, \ldots, p_{r-1}\}$ and the ideal $\mathfrak{a}' = (A') : I_{A'}^\infty$ defined by A' in $\mathscr{R}'$.

Theorem 6 *(unmixedness property of ideals defined by triangular sets)*
Let $A = \{p_1, \ldots, p_r\}$ be a triangular set of $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$ and $\mathfrak{a}$ denote either $(A) : I_A^\infty$ or $(A) : S_A^\infty$. Then for every associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ we have $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

In particular all the associated prime ideals of $(A) : I_A^\infty$ and $(A) : S_A^\infty$ have the same dimension and are isolated. Moreover, the nonzero elements of $\mathscr{F}[t_1, \ldots, t_m]$ are regular modulo each of these ideals. Similar statements hold also for $(A) : H_A^\infty$.

Theorem 7 *(Lazard's Lemma)*
Let A be a triangular set of $\mathscr{R}$. The ideal $(A) : S_A^\infty$ is radical.

Since $(A) : S_A^\infty$ is radical, this ideal is an intersection of prime ideals. Thus $(A) : H_A^\infty$, which is the intersection of the prime ideals which contain $(A) : S_A^\infty$ but do not contain any initial of A must be radical also.

Definition 5 *Let A be a possibly empty triangular set and f be a polynomial. The* pseudoremainder of f by A, *denoted* $\mathrm{prem}(f, A)$ *is defined as follows:*

- *if $A = \varnothing$ then* $\mathrm{prem}(f, A) = f$;
- *if $A = \{p_1, \ldots, p_r\}$ then* $\mathrm{prem}(f, A) = \mathrm{prem}(\mathrm{prem}(f, p_r, x_r), A \setminus \{p_r\})$.

Definition 6 *Let A be a possibly empty triangular set and f be a polynomial. The* resultant of f by A, *denoted* $\mathrm{res}(f, A)$ *is defined as follows:*

- *if $A = \varnothing$ then* $\mathrm{res}(f, A) = f$;
- *if $A = \{p_1, \ldots, p_r\}$ then* $\mathrm{res}(f, A) = \mathrm{res}(\mathrm{res}(f, p_r, x_r), A \setminus \{p_r\})$.

3.3 Regular Chains

Definition 7 *(regular chains)*
In the polynomial ring $\mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$, let $\mathfrak{a}$ be the ideal defined by a triangular set $A = \{p_1, \ldots, p_r\}$ and $\mathfrak{a}'$ be the ideal defined by $A' = \{p_1, \ldots, p_{r-1}\}$.

Then A is a regular chain *if $r = 1$ or $r > 1$, A' is a regular chain and the initial i_r of p_r is regular modulo $\mathfrak{a}'$.*

Theorem 8 *(equivalence theorem for regular chains)*
Let $A = \{p_1, \ldots, p_r\}$ be a triangular set of $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$. Denote i_ℓ the initial of p_ℓ and $\mathfrak{a} = (A) : I_A^\infty$. The following conditions are equivalent:

1. *A is a regular chain ;*

2. *for each $2 \leq \ell \leq r$ we have $\operatorname{res}(i_\ell, A) \neq 0$;*

3. *for each $f \in \mathscr{R}$ we have $f \in \mathfrak{a}$ if and only if $\operatorname{prem}(f, A) = 0$;*

4. *for each $f \in \mathscr{R}$ we have f regular modulo $\mathfrak{a}$ if and only if $\operatorname{res}(f, A) \neq 0$.*

Over our example, the set A is triangular. It is however not a regular chain since the resultant of $t_1\, x_1$ (the initial of p_2) and $p_1 = x_1\,(x_1 + t_1)$ with respect to x_1 is zero (since both polynomials have a common factor with positive degree in x_1). Therefore $\operatorname{res}(t_1\, x_1, A) = 0$ and A is not a regular chain by Theorem 8 (implication $\mathbf{1} \Rightarrow \mathbf{2}$). Thanks to the implication $\mathbf{1} \Rightarrow \mathbf{4}$, the following definition is algorithmic.

Definition 8 *(squarefree regular chain)*
A regular chain A is said to be squarefree *if the separant of each element of A is regular modulo the ideal $(A) : I_A^\infty$.*

If A is squarefree then the separants of A do not belong to any associated prime ideal of $(A) : I_A^\infty$. Thus $(A) : I_A^\infty$ is equal to $(A) : H_A^\infty$, which is radical by Lazard's Lemma. In summary:

Proposition 17 *Let A be a squarefree regular chain.*
Then $(A) : I_A^\infty$ is radical and is equal to $(A) : {H_A}^\infty$.

3.4 Regular Differential Chains — Ordinary Case

In this section, $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$ is an ordinary differential polynomial ring. A ranking is supposed to be fixed and we apply the results of the former sections to triangular sets $A = \{p_1, \ldots, p_r\}$ of differential polynomials which are pairwise partially reduced (such sets are said to be *partially autoreduced*). The leading derivatives of the elements of A play the role of the leading variables $x_1, \ldots, x_r$ of the former sections. The other derivatives present in A play the role of the variables $t_1, \ldots, t_m$.

Definition 9 *(regular differential chains — ordinary case)*

In the ordinary differential polynomial ring $\mathscr{F}\{y_1, \ldots, y_n\}$, a partially autoreduced triangular set A is a regular differential chain *if it is a squarefree regular chain.*

3.5 Regular Differential Chains — Partial Case

In this section, $\mathscr{R} = \mathscr{F}\{y_1, \ldots, y_n\}$ is a partial differential polynomial ring. A ranking is supposed to be fixed and, as in the ordinary case, we consider a partially autoreduced triangular set of differential polynomials $A = \{p_1, \ldots, p_r\}$.

Since the number of derivation operators is strictly greater than 1 it may happen that the leading derivatives $\theta_i y$ and $\theta_j y$ of two elements p_i and p_j of A are derivatives of the same differential indeterminate y. Such a pair of differential polynomials is called a *critical pair* of A. Denote θ_{ij} the least common multiple of θ_i and θ_j so that $\theta_{ij} y$ is the least common derivative of the two leading derivatives $\theta_i y$ and $\theta_j y$. Then, denoting s_i and s_j the separants of p_i and p_j, the Δ-polynomial $\Delta_{ij} = \Delta(p_i, p_j)$ is defined as

$$\Delta(p_i, p_j) \;=\; s_j \, \frac{\theta_{ij}}{\theta_i} \, p_i - s_i \, \frac{\theta_{ij}}{\theta_j} \, p_j \, . \tag{31}$$

It is either an element of $\mathscr{F}$ or a differential polynomial with leading derivative *strictly less* than $\theta_{ij} y$. Indeed, in (31), the leading derivatives of the differential polynomials $(\theta_{ij}/\theta_i)p_i$ and $(\theta_{ij}/\theta_j)p_j$ are both equal to $\theta_{ij} y$ but a cancellation occurs (by design of the Δ–polynomial) so that $\deg(\Delta_{ij}, \theta_{ij} y) = 0$.

Denote $A_{ij} \subset \Theta A$ the set of the derivatives of the elements of A with leading derivatives *strictly less* than $\theta_{ij} y$. The critical pair (p_i, p_j) of A is said to be *solved* if the Δ-polynomial Δ_{ij} belongs to the nondifferential ideal defined by A_{ij} i.e. if $\Delta_{ij} \in (A_{ij}) : H_{A_{ij}}^{\infty}$. Remarks:

1. if we denote $\mathscr{R}_{ij}$ the ring of all differential polynomials of $\mathscr{R}$ with leading derivatives strictly less than $\theta_{ij} y$. We have $(A_{ij}) : H_{A_{ij}}^{\infty} \subset \mathfrak{A} \cap \mathscr{R}_{ij}$ but the equality does not hold in general ; in particular, if the critical pair is not solved, the inclusion is strict ;

2. if $\mathrm{fullrem}(\Delta_{ij}, A) = 0$ then the critical pair is solved ;

3. for a given finite set A, there are only finitely many critical pairs.

Definition 10 *(coherence)*

A partially autoreduced triangular set A of differential polynomials is said to be coherent *if all its critical pairs are solved.*

Since a partially autoreduced triangular set has no critical pair in the ordinary differential case, the following definition holds in both the ordinary and the partial differential context.

Remarks **2** and **3** above show that the coherence property is algorithmic but this algorithmic character does not appear in Kolchin's book. Indeed [17, chap. IV, sect. 8, cond. **C3**], which generalizes Rosenfeld's coherence, deals with the critical pairs associated to *all* multiples of the differential operators θ_i and θ_j, not only with their least common multiple.

Definition 11 *(regular differential chain — general case)*

In the differential polynomial ring $\mathscr{F}\{y_1, \ldots, y_n\}$, a partially autoreduced triangular set A is a regular differential chain *if it is a coherent squarefree regular chain.*

3.6 Properties of Regular Differential Chains

To a regular differential chain A we can associate the ring $\mathscr{R}_1 \subset \mathscr{R}$ of the differential polynomials partially reduced with respect to A, the differential ideal $\mathfrak{A} = [A] : H_A^\infty$ of $\mathscr{R}$ and the non differential ideal $\mathfrak{a} = (A) : H_A^\infty$ of $\mathscr{R}_1$.

Theorem 9 *(Rosenfeld's Lemma)*

Let A be a regular differential chain of $\mathscr{R}$. Then

$$\mathfrak{A} \cap \mathscr{R}_1 \quad = \quad \mathfrak{a}\,.$$

The original version of Rosenfeld's Lemma [25] is formulated for a set A which is autoreduced and coherent. The concept of regular differential chain did not exist at that time. The following Theorem is a consequence of Rosenfeld's Lemma and Lazard's Lemma.

Theorem 10 *Let A be a regular differential chain. Then $\mathfrak{A}$ is radical. Moreover, there is a one-to-one correspondence between the essential components $\mathfrak{P}_1, \ldots, \mathfrak{P}_\varrho$ of $\mathfrak{A}$ and the associated prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_\varrho$ of $\mathfrak{a}$ given by*

$$\mathfrak{P}_i \cap \mathscr{R}_1 \quad = \quad \mathfrak{p}_i \qquad (i = 1, \ldots, \varrho)\,.$$

Theorem 11 *(equivalence theorem for regular differential chains)*

Let A be a coherent, partially autoreduced triangular set and f be a differential polynomial of $\mathscr{R}$. Then the following properties are equivalent:

1. *A is a regular differential chain,*

2. *for each $2 \leq \ell \leq r$ we have* $\mathrm{res}(i_\ell, A) \neq 0$ *and each $1 \leq \ell \leq r$ we have* $\mathrm{res}(s_\ell, A) \neq 0$,

3. *$f \in \mathfrak{A}$ if and only if* $\mathrm{fullrem}(f, A) = 0$,

4. *f is regular modulo $\mathfrak{A}$ if and only if* $\mathrm{res}(\mathrm{partialrem}(f, A), A) \neq 0$.

3.7 Testing the Inclusion of Differential Ideals

Let A and B be two regular differential chains, defining differential ideals $\mathfrak{A}$ and $\mathfrak{B}$ in $\mathscr{R}$. If $A \not\subset \mathfrak{B}$ then $\mathfrak{A} \not\subset \mathfrak{B}$. If $A \subset \mathfrak{B}$ and all elements of H_A are regular in $\mathscr{R}/\mathfrak{B}$ then $\mathfrak{A} \subset \mathfrak{B}$. However, if $A \subset \mathfrak{B}$ and there exists some $h \in H_A$ which is either zero or a zero divisor in $\mathscr{R}/\mathfrak{B}$ then we cannot conclude.

The problem comes from the fact that A is not a basis of $\mathfrak{A}$. In the nondifferential case, the inclusion problem can be decided since, thanks to Gröbner bases and the Rabinowitsch trick, it is possible to compute a basis of $(A) : H_A^\infty$.

3.8 Formal Power Series Solutions — Principle

We have described in section 2.7 a process for computing a formal power series solution of a prime differential ideal presented by a characteristic set. The very same process permits to compute formal power series solutions of any differential ideal $[A] : H_A^\infty$ presented by a regular differential chain.

3.9 Algorithmic Decomposition of a Perfect Differential Ideal

There exist algorithms such as the *RosenfeldGröbner* algorithm (see [6, 7]) which gather as input a finite set Σ of differential polynomials and a ranking and yield finitely many regular differential chains $A_1, \ldots, A_\varrho$ which provide a decomposition of the perfect differential ideal $\{\Sigma\}$ as an intersection of the perfect differential ideals defined by the regular differential chains:

$$\{\Sigma\} \quad = \quad [A_1] : H_{A_1}^\infty \cap \cdots \cap [A_\varrho] : H_{A_\varrho}^\infty \,. \tag{32}$$

If $1 \in \{\Sigma\}$ then the intersection is empty (i.e. $\varrho = 0$). Decomposition (32) may be redundant but no algorithm is known to make it irredundant (see section 3.7). However, it is possible to decompose each differential ideal $[A_i] : H_{A_i}^\infty$ as an intersection of prime differential ideals (thanks to Theorem 10). Decomposition (32) provides also a decomposition of the solution set of $\{\Sigma\}$ as the union of the solution sets of the differential ideals $[A_i] : H_{A_i}^\infty$.

Theorem 12 *Decomposition* (32) *permits to decide membership to the perfect differential ideal* $\{\Sigma\}$ *hence to decide whether* Σ *admits formal power series solutions. However, it does not permit to decide regularity modulo* $\{\Sigma\}$.

Proof A differential polynomial f belongs to $\{\Sigma\}$ if and only if it belongs to each differential ideal $[A_i] : H_{A_i}^\infty$ for $1 \leq i \leq \varrho$. Membership testing to these differential ideals is algorithmic by Theorem 11.

If $\varrho = 0$ then $1 \in \{\Sigma\}$ and Σ has no formal power series solution. If $\varrho > 0$ then all regular differential chains A_i have formal power series solutions (section 3.8) and each of these formal power series is a solution of $\{\Sigma\}$ (see Theorem 4).

Though it is possible to decide regularity modulo a differential ideal defined by a regular differential chain (Theorem 11), decomposition 32 is not sufficient for deciding regularity modulo $\{\Sigma\}$ because it may contain redundant components (see section 3.7). □

Last observe that membership testing to differential ideals was proved to be undecidable in general [13]. Membership testing to differential ideals of the form $[\Sigma]$ with Σ finite is undecidable also whenever the number of derivations is greater than or equal to 2 [29]. Membership testing to *ordinary* differential ideals of the form $[\Sigma]$ with Σ finite is still open.

Description of the algorithm. The following text is much inspired from the descriptions of the *RosenfeldGroebner* algorithm given in [7, 2].

This algorithm proceeds in two main steps. In the first step, it computes finitely many *regular differential systems* of the form $A = 0, S \neq 0$ where A is a coherent, partially autoreduced triangular set of differential polynomials and S is a set of differential polynomials partially reduced with respect to A containing the initials and the separants of A.

A regular differential system $A = 0, S \neq 0$ defines the differential ideal $[A] : S^\infty$ which is the ideal of the differential polynomials which vanish over all the solutions of the system. Theorems 9 and 10 hold for the differential ideal $[A] : S^\infty$ though A is not yet necessarily a regular differential chain. The main difference is that it may happen that $1 \in [A] : S^\infty$ i.e. that $A = 0, S \neq 0$ has no solution but this can be decided by determining if $1 \in (A) : S^\infty$, thanks to Rosenfeld's Lemma.

The perfect differential ideal $\{\Sigma\}$ is the intersection of the perfect differential ideals defined by the regular differential systems produced at the first step.

In the second step, the algorithm transforms each regular differential system $A = 0, S \neq 0$ into finitely many regular differential chains (none if the regular differential system has no solution). The intersection of the perfect differential ideals defined by the regular differential chains is equal to the perfect differential ideal $[A] : S^\infty$.

Let us sketch the algorithm, called *regCharacteristic*, for the second step [8]. Its principle consists in testing whether A is a squarefree regular chain by testing the regularity of the initials and separants of A, processing the elements of A from bottom up and implementing the regularity test of Theorem 11. This being done, A is proved to be a regular differential chain and the regularity of all the elements of S can be verified. Every regular element of S which is proved regular is discarded. Of course, it may happen that some differential polynomial is proved to be a zero divisor at some stage. In that case, a factorization of some $p_i \in A$ is discovered. This exhibited factorization permits to split the current system into two branches. If one of the factors of p_i divides an element of S then the corresponding branch is discarded. The regularity test can be achieved by means of resultant computations (Theorem 11) however this test "as is" does not provide the factorization. A possibility consists in using a recursive variant of the extended Euclidean algorithm (or of algorithms for computing subresultants) such as the one provided in [3, Appendix].

An ordinary differential example. The differential polynomial ring is $\mathscr{F}\{y, z\}$. See Figure 2.

$$(\Sigma_1) \qquad \ddot{y} + z = 0, \quad \dot{y}^2 + z = 0.$$

The ranking is such that every derivative of y is greater than any derivative of z (the differential indeterminate y is eliminated). The leading derivatives of the two differential polynomials are $\ddot{y}$ and $\dot{y}$. The first differential polynomial is not partially reduced with respect to the first one. The partial remainder computation is carried out in (4), page 7. This computation amounts to differentiate the second equation, giving

$$2\,\dot{y}\,\ddot{y} + \dot{z} = 0$$

then replace $\ddot{y}$ by $-\dot{z}/(2\,\dot{y})$ in the first one, giving

$$-\frac{\dot{z}}{2\,\dot{y}} + z = 0.$$

Then replace the first equation by the numerator of the reduced equation, which is the partial remainder g, provided that the separant $2\,\dot{y}$, which is the differential polynomial h of (4), is different from zero. The solutions of (Σ_1) which annihilate the separant are considered separately. We obtain a splitting[3] of (Σ_1) into

$$(\Sigma_2) \qquad \ddot{y} + z = 0, \quad \dot{y}^2 + z = 0, \quad \dot{y} = 0$$

and

$$(\Sigma_3) \qquad 2\,z\,\dot{y} - \dot{z} = 0, \quad \dot{y}^2 + z = 0, \quad \dot{y} \neq 0.$$

Consider (Σ_2). Simplify the second equation using the third one. One gets $z = 0$. This system thus simplifies as a regular differential system

$$(\Sigma_4) \qquad \dot{y} = 0, \quad z = 0$$

whose solutions are $y(x) = c$ and $z(x) = 0$ where c is an arbitrary constant. This system is a regular differential chain. Consider now (Σ_3). The two first equations have the same leading derivative: it is not triangular. To get a triangular set, apply Ritt's reduction algorithm which informally amounts to proceed as follows: replace $\dot{y}$ by $\dot{z}/(2\,z)$ in the second equation, giving

$$\left(\frac{\dot{z}}{2\,z}\right)^2 + z = 0.$$

Replace the second equation by the numerator of the reduced equation, provided that $z \neq 0$ and consider separately the solutions of (Σ_3) which annihilate z. One obtains a splitting of (Σ_3) into two systems

$$(\Sigma_5) \qquad 2\,z\,\dot{y} - \dot{z} = 0, \quad \dot{y}^2 + z = 0, \quad z = 0, \quad \dot{y} \neq 0$$

and

$$(\Sigma_6) \qquad 2\,z\,\dot{y} - \dot{z} = 0, \quad \dot{z}^2 + 4\,z^3 = 0, \quad \dot{y} \neq 0, \quad z \neq 0.$$

Consider (Σ_5). The equation $z = 0$ reduces to zero the first one, by Ritt's reduction algorithm. It also permits to simplify the second equation. We then get a system

$$(\Sigma_7) \qquad \dot{y}^2 = 0, \quad z = 0, \quad \dot{y} \neq 0$$

which is a regular differential system. The *regCharacteristic* algorithm may then be applied over it. By a gcd computation between the equation $\dot{y}^2 = 0$ and the inequation $\dot{y} \neq 0$, it concludes that this system has no solution. Let us discard it and come back to (Σ_6). It is

[3]It is actually not the same type of splitting as in *regCharacteristic* because it does not correspond to a factorization.

not yet a regular differential system because the separant $2\,\dot{z}$ of the second equation does not belong to the inequation set. This is solved by splitting (Σ_6) into two systems which separate the solutions of (Σ_6) which satisfy $\dot{z} = 0$ from the ones which satisfy $\dot{z} \neq 0$. One gets two systems

$$(\Sigma_8) \qquad 2\,z\,\dot{y} - \dot{z} = 0, \quad \dot{z}^2 + 4\,z^3 = 0, \quad \dot{z} = 0, \quad \dot{y} \neq 0, \quad z \neq 0.$$

$$(\Sigma_9) \qquad 2\,z\,\dot{y} - \dot{z} = 0, \quad \dot{z}^2 + 4\,z^3 = 0, \quad \dot{z} \neq 0, \quad \dot{y} \neq 0, \quad z \neq 0.$$

Argumenting as for (Σ_7), we see that (Σ_8) has no solution. The system (Σ_9) (Σ_9) is a regular differential system. Its set of equations actually form a regular differential chain. We may then discard the inequation $\dot{y} \neq 0$ which is not an initial or a separant of the chain. The solutions of (Σ_9) actually are $y(x) = c_1 - \ln(x + c_2)$ and $z(x) = -1/(x + c_2)^2$ where c_1 and c_2 are arbitrary constants.

In summary, every solution of (Σ_1) is either a solution of (Σ_4) or of (Σ_9). Conversely, the solutions of (Σ_4) and (Σ_9) are solutions of (Σ_1). Therefore,

$$\{\ddot{y} + z,\, \dot{y}^2 + z\} \;=\; [\dot{y},\, z] \cap [2\,z\,\dot{y} - \dot{z},\; \dot{z}^2 + 4\,z^3] : (z\,\dot{z})^\infty\,.$$

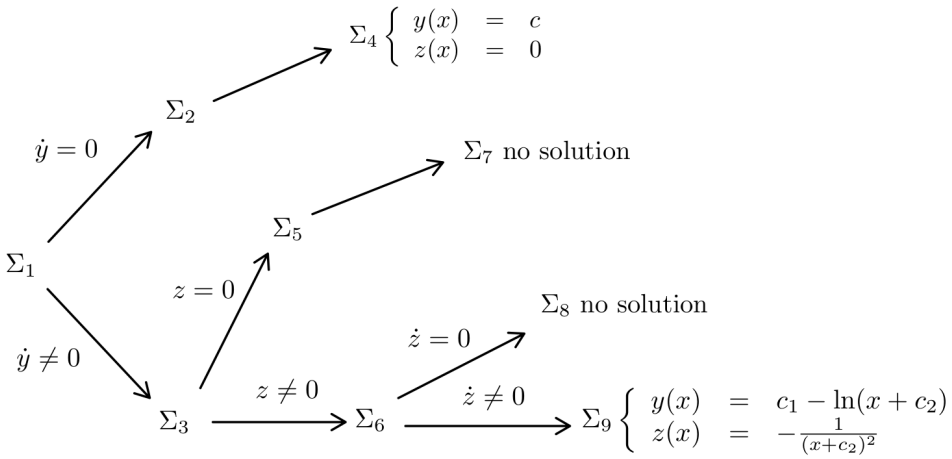

Figure 2: The splitting tree of the ordinary differential example

A partial differential example. The differential polynomial ring is $\mathscr{F}\{y, z\}$ endowed with two derivations δ_x and δ_t. See Figure 3.

The three differential polynomials of Σ_1 are denoted f_1, f_2 and f_3.

$$(\Sigma_1) \qquad y_t^2 - 4\,y = 0, \quad y_x - z_x\,y = 0, \quad z_t = 0.$$

The ranking is

$$\cdots > y_{xx} > y_{xt} > y_{tt} > z_{xx} > z_{xt} > z_{tt} > y_x > y_t > z_x > z_t > y > z.$$

The leading derivatives are thus y_t, y_x and z_t. The system is partially autoreduced and triangular. Is it coherent ? The two first equations form a critical pair $\{f_1,\, f_2\}$. To form the Δ-polynomial, differentiate the first equation by δ_x

$$\delta_x\, f_1 = 2\, y_t\, y_{xt} - 4\, y_x.$$

Differentiate the second equation by δ_t and multiply it by the separant $2\, y_t$ of the first equation, giving

$$2\, y_t\, \delta_t\, f_2 = 2\, y_t(y_{xt} - z_{xt}\, y - z_x\, y_t).$$

Subtract,

$$\Delta(f_1,\, f_2) = 2\, y\, y_t\, z_{xt} + 2\, y_t^2\, z_x - 4\, y_x.$$

The full reduction of this Δ-polynomial by (Σ_1) is detailed in (6), page 8. One gets a fourth equation $f_4 = y\, z_x = 0$ (the full remainder) which is inserted in the system

$$(\Sigma_2) \qquad y_t^2 - 4\, y = 0, \quad y_x - z_x\, y = 0, \quad z_t = 0, \quad y\, z_x = 0.$$

The insertion of f_4 implies that the critical pair $\{f_1,\, f_2\}$ is now solved. However, a new critical pair $\{f_3,\, f_4\}$ is generated. Before forming the new Δ-polynomial, the system is split on the initial of f_4. One then considers separately the solutions of (Σ_2) which annihilate y from the ones which do not. One gets

$$(\Sigma_3) \qquad y_t^2 - 4\, y = 0, \quad y_x - z_x\, y = 0, \quad z_t = 0, \quad y\, z_x = 0, \quad y = 0$$

and

$$(\Sigma_4) \qquad y_t^2 - 4\, y = 0, \quad y_x = 0, \quad z_t = 0, \quad z_x = 0, \quad y \neq 0.$$

The system (Σ_3) simplifies to

$$z_t = 0, \quad y = 0$$

which actually is a regular differential chain. Its solutions are $y(x,\, t) = 0$ and $z(x,\, t) = \varphi(x)$ where $\varphi(x)$ is an arbitrary function of x.

Consider (Σ_4). The critical pair $\{f_1,\, f_2\}$ is solved. The critical pair $\{f_3,\, f_4\}$ is solved also since $\Delta(f_3,\, f_4) = 0$. This system is thus coherent. It is not yet a regular differential system because the separant y_t of f_1 does not belong to the inequation set. One then splits (Σ_4) into

$$(\Sigma_5) \qquad y_t^2 - 4\, y = 0, \quad y_x = 0, \quad z_t = 0, \quad z_x = 0, \quad y_t = 0, \quad y \neq 0$$

and

$$(\Sigma_6) \qquad y_t^2 - 4\, y = 0, \quad y_x = 0, \quad z_t = 0, \quad z_x = 0, \quad y_t \neq 0, \quad y \neq 0.$$

System (Σ_5) has no solution: the new equation $y_t = 0$ permits to simplify the first one and obtain $y = 0$, which is incompatible with the inequation $y \neq 0$. System (Σ_6) is a regular differential system. Its set of equations even for a regular differential chain. The *regCharacteristic* algorithm permits to prove that the inequation $y \neq 0$, which is not an initial or a separant of the chain, is regular modulo the differential ideal defined by the

chain. It is thus discarded. The solutions of (Σ_6) are $y(x,\,t) = (t + c_1)^2$ and $z(x,\,t) = c_2$ where c_1 and c_2 are arbitrary constants.

In summary, every solution of (Σ_1) is a solution of (Σ_3) or (Σ_6), and conversely. Thus

$$\{y_t^2 - 4\,y,\, y_x - z_x\,y,\, z_t\} \;=\; [y,\, z_t] \cap [y_t^2 - 4\,y,\, y_x,\, z_t,\, z_x] : (y_t)^\infty\,.$$

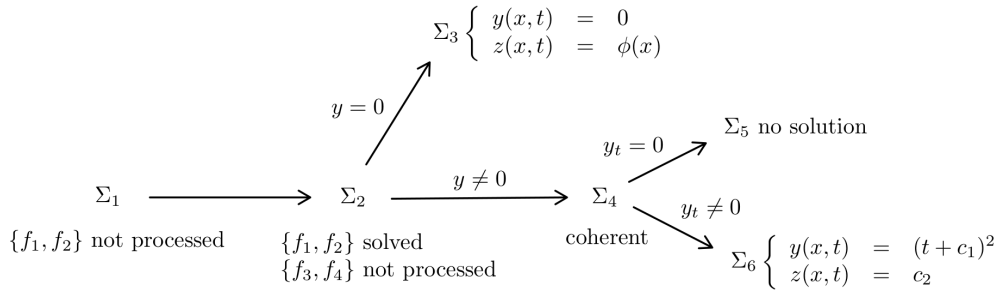

Figure 3: The splitting tree of the partial differential example

3.10 Classical Properties of The Resultant

This section, borrowed from [10], provides generalizations of basic properties of the usual resultant of two polynomials. These generalizations aim at covering cases which are usually not considered, such as one of the two polynomials being zero. The case of two polynomials of degree less than or equal to zero i.e. two constant polynomials is however excluded. The results are used in the next section for proving Theorem 8.

Let f and g be two polynomials of $\mathscr{R}[x]$, where $\mathscr{R}$ is a unitary ring of characteristic zero:

$$f = a_m\,x^m + \cdots + a_1\,x + a_0\,, \quad g = b_n\,x^n + \cdots + b_1\,x + b_0\,.$$

If f or g is zero, then the resultant of f and g is taken to be zero. Assume that f and g are nonzero and that at least one of them has positive degree. Then, the resultant of f and g is the determinant of the Sylvester matrix $S(f,g)$ of f and g, which has dimensions $(m+n)\times(m+n)$ and rows, from top down $x^{n-1}\,f, \ldots, x\,f, f, x^{m-1}\,g, \ldots, x\,g, g$. See [1, 4.2, page 105].

Lemma 5 *Assume f is nonzero and $n = 0$ (i.e. $g = b_0$). Then* $\mathrm{res}(f,g,x) = g^m$. *In particular, if $m = 1$ then* $\mathrm{res}(f,g,x) = g$.

Proof The Lemma is clear if $g = 0$. Otherwise, expand the determinant of the Sylvester matrix, which is diagonal. □

Lemma 6 *Assume $\mathscr{R}$ is a domain and let $\mathscr{F}$ denote its fraction field. Let f and g be two polynomials of $\mathscr{R}[x]$, not both zero. Then* $\mathrm{res}(f,g,x) = 0$ *if and only if f and g have a positive degree common factor in $\mathscr{F}[x]$.*

Proof The Lemma is clear if f or g is zero. Otherwise, see [1, 4.2, Proposition 4.15, page 106]. □

Remark: if f and g have a positive degree common factor in $\mathscr{F}[x]$ then f is a zerodivisor modulo (g) in $\mathscr{R}[x]$. Indeed, clearing denominators, we see that there exist nonzero $a, b \in \mathscr{R}$ and polynomials $f', g', h \in \mathscr{R}[x]$ such that $a\,f = h\,f'$, $b\,g = h\,g'$ and $\deg(h) > 0$. Since $\mathscr{R}$ is a domain, every nonzero element of the ideal (g) has degree greater than or equal to $\deg(g)$ and $\deg(h) + \deg(g') = \deg(g)$. Thus $\deg(g') < \deg(g)$ and $a\,g' \notin (g)$. However, $f\,a\,g' = h\,f'\,g' = b\,f'\,g$ belongs to (g). Thus f is a zerodivisor modulo (g).

Lemma 7 *Let $\mathscr{R}$ be a ring. If f and g are nonzero polynomials of $\mathscr{R}[x]$ then there exist two polynomials $u, v \in \mathscr{R}[x]$ with $\deg(u) < n$ and $\deg(v) < m$ such that $\operatorname{res}(f, g, x) = u\,f + v\,g$.*

Proof See [1, 4.2, Proposition 4.18, page 108]. □

The following Lemma generalizes [1, 4.2, Proposition 4.20, page 109] and deserves a proof.

Lemma 8 *(specialization property of the resultant)*
Let f, g be two polynomials of $\mathscr{R}[x]$. Let $\phi : \mathscr{R} \to \mathscr{S}$ be a ring homorphism such that $\phi(a_m) \neq 0$. Extend ϕ to a ring homomorphism $\mathscr{R}[x] \to \mathscr{S}[x]$. Denote $t = \deg(\phi(g), x)$. Then $\phi(\operatorname{res}(f, g, x)) = \phi(a_m)^{n-t} \operatorname{res}(\phi(f), \phi(g), x)$.

Proof If g is zero, then so is $\phi(g)$ and both resultants are zero. Assume g nonzero. Developing the determinant of $S(f, g)$ w.r.t. its last row, we see that any monomial of the resultant admits a coefficient of g as a factor. Thus, if $\phi(g)$ is zero, i.e. if ϕ maps all the coefficients of g to zero, then $\operatorname{res}(f, g, x) = 0$ and the Lemma holds.

Assume g and $\phi(g)$ are nonzero. If the ring homomorphism ϕ, which does not annihilate a_m, does not annihilate b_n either, then $\phi(S(f, g)) = S(\phi(f), \phi(g))$ and the Lemma is proved. Assume $\deg(\phi(g)) = t < n$. Then the Sylvester matrix $S(\phi(f), \phi(g))$ appears as the $(m + t) \times (m + t)$ submatrix of $\phi(S(f, g))$ (Fig. 4) at the bottom-right corner. Developing the determinant of $\phi(S(f, g))$ w.r.t. its $n - t$ first columns, we see that $\phi(\operatorname{res}(f, g, x)) = \phi(a_m)^{n-t} \operatorname{res}(\phi(f), \phi(g), x)$. □

3.11 Proof of the Equivalence Theorem on Regular Chains

In this section, which aims at proving Theorem 8, $A = \{p_1, \ldots, p_r\}$ is a triangular set of $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$. The initials of the elements of A are $i_1, \ldots, i_r$, their product is I_A and the ideal defined by A is $\mathfrak{a} = (A) : I_A^\infty$. Similarly, one defines $A' = \{p_1, \ldots, p_{r-1}\}$, $\mathscr{R}' = \mathscr{F}[x_1, \ldots, x_{r-1}, t_1, \ldots, t_m]$ so that $\mathscr{R} = \mathscr{R}'[x_r]$ and $\mathfrak{a}' = (A') : I_{A'}^\infty$ is an ideal of $\mathscr{R}'$.

Let φ denote the canonical ring homomorphism $\mathscr{R} \to (\mathscr{R}'/\mathfrak{a}')[x_r]$ and consider some polynomial $f \in \mathfrak{a}$. Then, by the definition of $\mathfrak{a}$, there exist non negative integers $\alpha_1, \ldots, \alpha_r$ and polynomials $q_1, \ldots, q_r \in \mathscr{R}$ such that

$$i_1^{\alpha_1} \cdots i_r^{\alpha_r}\, f \;=\; q_1\, p_1 + \cdots + q_r\, p_r\,. \tag{33}$$

$$\phi(S(f,g)) = \left(\begin{array}{cccccccccc}
\phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) & 0 & 0 \\
\vdots & & \ddots & \ddots & & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & \phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) \\
0 & 0 & \phi(b_t) & \cdots & \cdots & \cdots & \phi(b_0) & 0 & \cdots & 0 \\
0 & & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & 0 & \phi(b_t) & \cdots & \cdots & \cdots & \phi(b_0)
\end{array}\right) \begin{array}{l} \} n-t \\ \\ \\ \} t \\ \\ \\ \} m \\ \\ \end{array}$$

Figure 4: The image by ϕ of the Sylvester matrix $S(f,g)$.

In $(\mathscr{R}'/\mathfrak{a}')[x_r]$, this formula becomes

$$\varphi(i_1)^{\alpha_1} \cdots \varphi(i_r)^{\alpha_r}\, \varphi(f) \;\; = \;\; \varphi(q_r)\, \varphi(p_r)\,. \tag{34}$$

The images $\varphi(i_1), \ldots, \varphi(i_{r-1})$ of the $r-1$ first initials are regular elements of $\mathscr{R}'/\mathfrak{a}'$ since $\mathfrak{a}'$ is saturated by them. Assume now that A is a regular chain. Then the image $\varphi(i_r)$ of i_r is regular also and we have $\deg(p_r, x_r) = \deg(\varphi(p_r))$ and either $\varphi(f) = 0$ or $\deg(\varphi(f)) \geq \deg(\varphi(p_r))$.

The next proposition[4] proves **1** $\Rightarrow$ **3**.

Proposition 18 *Let A be a regular chain. Then $f \in \mathfrak{a}$ if and only if* $\mathrm{prem}(f, A) = 0$.

Proof The implication $\Leftarrow$ from the right to the left is clear. Let us prove the converse inclusion $\Rightarrow$ by induction on r. Consider some $f \in \mathfrak{a}$. Basis: if $r = 1$ then the proposition is clear by considering the degrees in x_r. General case: assume $r > 1$ and the proposition holds for A'. Denote φ the ring homomorphism $\mathscr{R} \to (\mathscr{R}'/\mathfrak{a}')[x_r]$. Since $f \in \mathfrak{a}$ we have $\mathrm{prem}(f, p_r, x_r) \in \mathfrak{a}$. Applying (33) and (34) to this pseudoremainder, we have

$$\varphi(i_1)^{\alpha_1} \cdots \varphi(i_r)^{\alpha_r}\, \varphi(\mathrm{prem}(f, p_r, x_r)) \;\; = \;\; \varphi(q_r)\, \varphi(p_r)$$

with $\deg(\varphi(\mathrm{prem}(f, p_r, x_r))) < \deg(\varphi(p_r))$. Thus $\varphi(\mathrm{prem}(f, p_r, x_r)) = 0$ which means that $\mathrm{prem}(f, p_r, x_r) \in \mathfrak{a}'\mathscr{R}$ i.e. all the coefficients of the pseudoremainder belong to $\mathfrak{a}'$. By the induction hypothesis, $\mathrm{prem}(\mathrm{prem}(f, p_r, x_r), A')$, which is equal to $\mathrm{prem}(f, A)$, is equal to zero. $\square$

Theorem 6 states that the following theorem actually holds for general triangular sets. The restricted version we give here relies on much more elementary arguments.

[4]The authors would like to dedicate this proof to Marc Moreno Maza, for his 60th birthday!

Proposition 19 *(unmixedness property of ideals defined by regular chains)*
Let A be a regular chain and $\mathfrak{p}$ be an associated prime ideal of $\mathfrak{a}$. Then $\dim \mathfrak{p} = m$ *and* $\mathfrak{p} \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

Proof Let $f \in \mathscr{R}$ be a polynomial and h be a nonzero element of $\mathscr{F}[t_1, \ldots, t_m]$. Then $\mathrm{prem}(f, A) \neq 0$ if and only if $\mathrm{prem}(h\,f, A) \neq 0$. Then $f \in \mathfrak{a}$ if and only if $h\,f \in \mathfrak{a}$ by Proposition 18. Then h is regular modulo $\mathfrak{a}$ which means that $\mathfrak{p} \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$. Thus $\dim \mathfrak{p} \geq m$. The initials of the elements of A are regular modulo $\mathfrak{a}$ since $\mathfrak{a}$ is saturated by them. Thus $x_1, \ldots, x_r$ are algebraically dependent over $t_1, \ldots, t_m$ modulo $\mathfrak{p}$. Thus $\dim \mathfrak{p} \leq m$. Combining both inequality, we conclude $\dim \mathfrak{p} = m$. □

The above proposition implies in particular that all the associated prime ideals of $\mathfrak{a}$ are isolated. It is a key to detect associated prime ideals of $\mathfrak{a}$, hence zerodivisors modulo $\mathfrak{a}$. The argument is: if $\mathfrak{p}$ is a prime ideal containing $\mathfrak{a}$ and $\dim \mathfrak{p} = m$ then $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$ (for if an associated prime ideal $\bar{\mathfrak{p}}$ where located between $\mathfrak{a}$ and $\mathfrak{p}$, it would have dimension strictly greater than m: a contradiction with Proposition 19).

A "well-known" theorem [17, chap. 0, 16, Prop. 11] states that, if $\mathfrak{p}$ has dimension m and $f \notin \mathfrak{p}$ then every isolated associated prime ideal of $(\mathfrak{p}, f)$ has dimension $m - 1$. Thus if $\mathfrak{p}'$ is a prime ideal of $\mathscr{R}'$ has dimension m and $p_r \in \mathscr{R}'[x_r]$ does not belong to $\mathfrak{p}'\,\mathscr{R}'[x_r]$ then every isolated associated prime ideal of $(\mathfrak{p}', p_r)$ in $\mathscr{R}'[x_r]$ has dimension m (one more variable, one more polynomial: the dimension remains the same). In general, the ideal $(\mathfrak{p}', p_r)$ may very well be the unit ideal (take $\mathfrak{p}' = (x_1)$ and $p_r = x_1\,x_r + 1$). However, if $\deg p_r > 0$ (our case) and the initial i_r of p_r does not belong to $\mathfrak{p}'$ (the case of regular chains) then $(\mathfrak{p}', p_r)$ is a proper ideal. All these arguments, rewritten more accurately, lead to the following proposition.

Proposition 20 *(associated prime ideals of ideals defined by regular chains)*
Let A be a regular chain. Then $\mathfrak{a}$ and $\mathfrak{a}'$ are proper ideals. Given any associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$, $\mathfrak{p} \cap \mathscr{R}'$ is an associated prime ideal of $\mathfrak{a}'$. Conversely, given any associated prime ideal $\mathfrak{p}'$ of $\mathfrak{a}'$, there exists an associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ such that $\mathfrak{p} \cap \mathscr{R}' = \mathfrak{p}'$.

Proof The proof is by induction on r.

Basis: the case $r = 1$. Then $\mathfrak{a}' = (0)$ is proper. It has a single associated prime ideal $\mathfrak{p}' = (0)$. The ideal $\mathfrak{a} = (p_1) : i_1^\infty$ is proper too. Its associated prime ideals, are the prime ideals generated by the irreducible factors of p_1 with positive degree in x_1. The proposition thus holds for $r = 1$.

General case: $r > 1$. By induction hypothesis, $\mathfrak{a}'$ is proper. Let $\mathfrak{p}' \subset \mathscr{R}'$ be any of its associated prime ideals. Since A is a regular chain, the initial i_r of p_r does not belong to $\mathfrak{p}'$. Thus the ideal $(\mathfrak{p}', p_r) : I_A^\infty$ is proper hence: 1) the ideal $\mathfrak{a}$ si proper too since the inclusion $\mathfrak{a} \subset (\mathfrak{p}', p_r) : I_A^\infty$ holds; and 2) the associated prime ideals of $(\mathfrak{p}', p_r) : I_A^\infty$ have the same dimension as that of $\mathfrak{a}$ (Proposition 19) hence are associated prime ideals of $\mathfrak{a}$. Conversely, consider any associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$. We have $\mathfrak{a}' \subset \mathfrak{a} \cap \mathscr{R}' \subset \mathfrak{p} \cap \mathscr{R}'$. Since the prime ideal $\mathfrak{p} \cap \mathscr{R}'$ has the same dimension as the associated prime ideals of $\mathfrak{a}'$, it is one of them. □

The two following propositions prove **1** ⇒ **4**.

Proposition 21 *Let A be a regular chain. If f is a zero divisor modulo $\mathfrak{a}$ then* $\mathrm{res}(f, A) = 0$.

Proof Assume f is a zero divisor modulo $\mathfrak{a}$ i.e. that f belongs to some associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$. Then $\mathrm{res}(f, A) \in \mathfrak{p}$ by Lemma 7. Since $\mathrm{res}(f, A) \in \mathscr{F}[t_1, \ldots, t_m]$, it is equal to zero by Proposition 19. □

Let us illustrate the last paragraph of the following proof with an example. Take $A = \{(x_2 - x_1)(x_2 + x_1), x_1 - 1\}$ and $f = x_2 - 1$. Notice f is a zero divisor modulo $\mathfrak{a}$. Take $\mathfrak{p} = (x_2 + x_1, x_1 - 1)$. Then $\mathfrak{p}' = (x_1 - 1)$ and the homomorphism φ evaluates x_1 at 1. Then $\gcd(\varphi(p_r), \varphi(f)) = \gcd((x_2 + 1)(x_2 - 1), x_2 - 1) = g = x_2 - 1$ and $\varphi^{-1}(g)$ is the ideal $(x_2 - x_1, x_1 - 1)$. It is equal to its unique associated prime ideal $\bar{\mathfrak{p}}$ which has the same dimension as $\mathfrak{p}$ and is an associated prime ideal of $\mathfrak{a}$.

Proposition 22 *Let A be a regular chain. If f is regular modulo $\mathfrak{a}$ then* $\mathrm{res}(f, A) \neq 0$.

Proof Assume f is regular modulo $\mathfrak{a}$. Let $\mathfrak{p}$ be an associated prime ideal of $\mathfrak{a}$. Let $\mathfrak{p}'$ be the prime ideal $\mathfrak{p} \cap \mathscr{R}'$ and φ denote the ring homomorphism which maps $\mathscr{R}$ to $(\mathscr{R}'/\mathfrak{p}')[x_r]$. It is sufficient to prove that $\mathrm{res}(f, p_r, x_r) \notin \mathfrak{p}$ i.e. that $\varphi(\mathrm{res}(f, p_r, x_r)) \neq 0$ for, by Proposition 20, the resultant $\mathrm{res}(f, p_r, x_r)$ is then regular modulo $\mathfrak{a}'$.

Since A is a regular chain, $i_r \notin \mathfrak{p}'$ (which is an associated prime ideal of $\mathfrak{a}'$ by Proposition 20 again) hence $\varphi(i_r) \neq 0$ and there exists some $\alpha \geq 0$ such that $\varphi(\mathrm{res}(f, p_r, x_r)) = \varphi(i_r)^\alpha \, \mathrm{res}(\varphi(f), \varphi(p_r))$ by Lemma 8. It is thus sufficient to prove that $\mathrm{res}(\varphi(f), \varphi(p_r)) \neq 0$.

Let us assume $\mathrm{res}(\varphi(f), \varphi(p_r)) = 0$ and seek a contradiction. The ring $\mathscr{R}'/\mathfrak{p}'$ is a domain thus $\varphi(f)$ and $\varphi(p_r)$ have a positive degree common factor g in $\mathrm{Fr}(\mathscr{R}'/\mathfrak{p}')[x_r]$ by Lemma 6. Thus $\varphi(f)$ is a zerodivisor modulo $(\varphi(p_r))$ in $(\mathscr{R}'/\mathfrak{p}')[x_r]$ (see the remark following Lemma 6). Thus $\varphi(f)$ belongs to some associated prime ideal of $(\varphi(p_r))$. This prime ideal has the form $\varphi(\bar{\mathfrak{p}})$ where $\bar{\mathfrak{p}}$ is a prime ideal of $\mathscr{R}$ such that $\bar{\mathfrak{p}} \cap \mathscr{R}' = \mathfrak{p}'$. The ideal $\bar{\mathfrak{p}}$ contains p_r, does not contain i_r hence $\dim \bar{\mathfrak{p}} = \dim \mathfrak{p}$ and $\bar{\mathfrak{p}}$ is an associated prime ideal of $\mathfrak{a}$. Since $f \in \bar{\mathfrak{p}}$, we see that f is a zero divisor modulo $\mathfrak{a}$. This contradiction with the regularity assumption of f proves the proposition. □

The next proposition is an easy corollary to the former one. It proves **2** ⇒ **1**.

Proposition 23 *Let A be a triangular set.*
If $\mathrm{res}(i_\ell, A) \neq 0$ *for each* $2 \leq \ell \leq r$ *then A is a regular chain.*

Proof The proof is by induction on r. Basis: if $r = 1$ the proposition is clear since any singleton is a regular chain. General case: assume $r > 1$ and the proposition holds for A'. Assume $\mathrm{res}(i_\ell, A) \neq 0$ for each $2 \leq \ell \leq r$. Then by induction hypothesis, A' is a regular chain. Since $\mathrm{res}(i_r, A) \neq 0$ we have $\mathrm{res}(i_r, A') \neq 0$ by Lemma 5 hence i_r is regular modulo $\mathfrak{a}'$ by Proposition 22. Thus A is a regular chain. □

The next proposition proves **3** ⇒ **1**.

Proposition 24 *If* $\mathrm{prem}(f, A) = 0$ *for each* $f \in \mathfrak{a}$ *then A is a regular chain.*

Proof We assume A' is a regular chain but A is not and we conclude that there exists some $f \in \mathfrak{a}$ such that $\mathrm{prem}(f, A) \neq 0$. The initial i_r must then be a zero divisor modulo $\mathfrak{a}'$. Thus there exist some $f \in \mathscr{R}$ and some $\alpha > 0$ such that $\mathrm{prem}(f, A') \neq 0$ and $\mathrm{prem}(i_r^\alpha f, A') = 0$, by Proposition 18 applied to A'. Since $\deg(i_r, x_r) = 0$ we may assume without loss of generality that $\deg(f, x_r) = 0$. Thus $\mathrm{prem}(f, A) \neq 0$. However $f \in \mathfrak{a}$. □

Last, observe that **4** ⇒ **2** is straightforward: since $\mathfrak{a}$ is saturated by the initials of the elements of A, these initials are regular modulo $\mathfrak{a}$ and, assuming **4**, their resultant w.r.t A is nonzero. This last implication achieves the proof of Theorem 8.

3.12 Proof of the Unmixedness Theorem and Lazard's Lemma

This section is borrowed from [10]. It provides proofs for two important Theorems which do not appear in [17].

In this section, $A = \{p_1, \ldots, p_r\}$ is a triangular set of $\mathscr{R} = \mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$. The initials of the elements of A are $i_1, \ldots, i_r$ and their separants are $s_1, \ldots, s_r$.

An ideal of $\mathscr{R}$ is said to be *unmixed* if all its associated prime ideals have the same dimension [31, chap. VII, sect. 7, page 196].

The following Theorem is a restatement of our Theorem 6. It already appeared in [9, Theorem 1.6]. Its main ingredient is Macaulay's unmixedness Theorem, whose importance in the theory of triangular sets was first pointed out by [22, 23]. In the particular case of h being the product of the initials of A, it is [14, Theorem 4.4].

Theorem 13 *(unmixedness property of ideals defined by triangular sets)*

Let A be a triangular set, h denote either the product of its initials or the product of its separants and $\mathfrak{a} = (A) : h^\infty$. Assume $\mathfrak{a}$ is proper.

Then, the ideal $\mathfrak{a}$ is unmixed. Moreover, if $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$ then $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

Denote $\varphi : \mathscr{R} \to h^{-1}\mathscr{R}$ the localization at h. With the terminology of Zariski and Samuel, $h^{-1}\mathscr{R} = \mathscr{R}_M$ where M denotes the multiplicative family generated by h. Extended and contracted ideals [31, chap. IV, sect. 8] are taken with respect to φ and the ideal $\mathfrak{a} = (A) : h^\infty$ is a contracted ideal i.e. $\mathfrak{a} = \mathfrak{a}^{ec}$. The extended ideal $\mathfrak{a}^e$ is the ideal generated by $A/1 = \{p_1/1, \ldots, p_r/1\}$ in $h^{-1}\mathscr{R}$.

Let us now introduce the ring $\mathscr{R}' = \mathscr{R}[x_{r+1}]$, the polynomial $p_{r+1} = h\, x_{r+1} - 1$ and the ideal $\mathfrak{a}' = (A,\, p_{r+1})$ of $\mathscr{R}'$. Let $\pi : \mathscr{R}' \to \mathscr{R}'/(p_{r+1})$ denote the quotient of $\mathscr{R}'$ by the ideal (p_{r+1}). These two constructs are related by the ring isomorphism: $h^{-1}\mathscr{R} \simeq \mathscr{R}'/(p_{r+1})$. Indeed, every element of $h^{-1}\mathscr{R}$ is a fraction f/h^d with $f \in \mathscr{R}$ and corresponds to the equivalence class of $f\, x_{r+1}^d$ modulo (p_{r+1}).

The two ideals $\mathfrak{a}^e$ and $\pi\, \mathfrak{a}'$ are the same ideal, since they share a generating family: A.

Lemma 9 *The ideal $\mathfrak{a}'$ is proper.*

Proof Since $\mathfrak{a} = \mathfrak{a}^{ec}$ is assumed to be proper, so is $\mathfrak{a}^e$. Since $\pi\,\mathfrak{a}' = \mathfrak{a}^e$ the ideal $\mathfrak{a}'$ is proper also. □

The next Proposition already appears in [11] or as [16, Theorem 3.1], in the case of $\mathfrak{a} = (A) : I_A^\infty$.

Proposition 25 *We have* $\dim \mathfrak{a}' = m$. *If* $\mathfrak{p}'$ *is an isolated prime ideal of* $\mathfrak{a}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

Proof The ideal $\mathfrak{a}'$ is proper by Lemma 9. Applying [31, chap. VII, sect. 7, Theorem 22, page 196] (the principal ideal theorem) with[5] $(R, r, s, \mathfrak{A}) = (\mathscr{R}', r + m + 1, r + 1, \mathfrak{a}')$, we see that every isolated prime ideal of $\mathfrak{a}'$ has dimension $\geq m$. Since the dimension of an ideal is the maximum of the dimensions of its associated prime ideals, we see that $\dim \mathfrak{a}' \geq m$.

We now claim that $\dim \mathfrak{a}' \leq m$. Let $\mathfrak{p}'$ be an associated prime ideal of $\mathfrak{a}'$ and consider some polynomial $p_i \in A$. Dropping the index i for legibility, let us write

$$p \;=\; a_d\, x^d + a_{d-1}\, x^{d-1} + \cdots + a_1\, x + a_0\,.$$

Because of the triangular nature of A, the coefficients

$$a_d, a_{d-1}, \ldots, a_0 \;\in\; \mathscr{F}[t_1, \ldots, t_m, x_1, \ldots, x_{i-1}]\,.$$

We have $p \in \mathfrak{p}'$ and, depending on the definition of h, either

$$a_d \notin \mathfrak{p}'\,, \quad \text{or} \quad d\, a_d\, x^{d-1} + (d-1)\, a_{d-1}\, x^{d-2} + \cdots + a_1 \notin \mathfrak{p}'\,.$$

This implies that, in $\mathscr{R}'/\mathfrak{p}'$, the polynomial p cannot become a trivial relation: in the first case, the degree of p cannot decrease while, in the second, it cannot decrease down to zero. Therefore $x = x_i$ must be algebraic over $t_1, \ldots, t_m, x_1, \ldots, x_{i-1}$ in $\mathscr{R}'/\mathfrak{p}'$. Putting this remark in an inductive argument, we see that $x_1, \ldots, x_r$ are algebraic over $t_1, \ldots, t_m$ in $\mathscr{R}'/\mathfrak{p}'$. Thus $\dim \mathfrak{p}' \leq m$.

Combining both inequalities, we have $\dim \mathfrak{p}' = m$ for all isolated prime ideals of $\mathfrak{a}'$ hence $\dim \mathfrak{a}' = m$. Considering again the arguments developed in the claim, we immediately see also that, if $\mathfrak{p}'$ is an isolated prime of $\mathfrak{a}'$ then $\mathfrak{p}' \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$. □

Proposition 26 *The ideal* $\mathfrak{a}'$ *is unmixed. If* $\mathfrak{p}'$ *is an associated prime ideal of* $\mathfrak{a}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

Proof By Proposition 25 and [31, chap. VII, sect. 13, Theorem 26, page 203] (Macaulay's unmixedness Theorem) with $(R, \mathfrak{A}, n, h) = (\mathscr{R}', \mathfrak{a}', m + r + 1, r + 1)$. □

We are now ready to prove Theorem 13. Recall that $\mathfrak{a}'$ is supposed to be proper.

[5] The left-hand side symbols correspond to the book notations. The right-hand side ones correspond to our notations.

Proof Let $\mathfrak{a}' = \cap_{i=1}^{\varrho} \mathfrak{q}'_i$ be an irredundant primary representation of $\mathfrak{a}'$ and $\mathfrak{p}'_i = \sqrt{\mathfrak{q}'_i}$.

Let us apply [31, chap. IV, sect. 5, Remark concerning passage to a residue class ring, page 213] with $(R, \mathfrak{a}, \mathfrak{b}) = (\mathscr{R}', \mathfrak{a}', (p_{r+1}))$. We see that $\pi\,\mathfrak{a}' = \cap_{i=1}^{\varrho} (\pi\,\mathfrak{q}'_i)$ is an irredundant primary representation of $\pi\,\mathfrak{a}'$ and that the $\pi\,\mathfrak{p}'_i$ are the associated prime ideals of $\pi\,\mathfrak{a}'$.

Using Proposition 26 and the fact that the π ring homomorphism removes one indeterminate and one polynomial, one sees that each prime ideal $\pi\,\mathfrak{p}'$ (dropping the index i), satisfies $\dim \pi\,\mathfrak{p}' = m$ and (with a slight abuse of notation) $\pi\,\mathfrak{p}' \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

Recall the ring isomorphism between $h^{-1}\,\mathscr{R}$ and $\mathscr{R}'/(p_{r+1})$. We have $\mathfrak{a} = \mathfrak{a}^{ec}$ and $\mathfrak{a}^e = \pi\,\mathfrak{a}'$. Let us apply [31, chap. IV, sect. 10, Theorem 17, page 225] with $(R, \mathfrak{a}, M) = (\mathscr{R}, \mathfrak{a}, \{h^d \mid d \geq 0\})$. Then $\mathfrak{a} = \cap_{i=1}^{\varrho} (\pi\,\mathfrak{q}'_i)^c$ is an irredundant primary representation of $\mathfrak{a}$. A polynomial f belongs to some $(\pi\,\mathfrak{q}')^c$ (dropping the index i) if, and only if, the fraction $f/1 \in \pi\,\mathfrak{q}'$. Thus $\dim(\pi\,\mathfrak{p}')^c = m$ and $(\pi\,\mathfrak{p}')^c \cap \mathscr{F}[t_1, \ldots, t_m] = (0)$.

The ideal $\mathfrak{a}$ is thus unmixed. Its associated prime ideals all have dimension m and do not contain any nonzero element of $\mathscr{F}[t_1, \ldots, t_m]$. □

The following Theorem is a restatement of our Theorem 7. It is known as Lazard's Lemma. See [6, Lemma 2], [7, Section 2], [9, Theorem 2.1] and [22, 23]. It appears also as [14, Theorem 7.5]. Variants of this Theorem also appear in earlier works such as [19, Proposition 5.1] and [21, Theorem III.5].

Theorem 14 *(Lazard's Lemma)*
Let A be a triangular set of $\mathscr{R}$. The ideal $(A) : S_A^\infty$ is radical.

Proof Denote $\mathfrak{a} = (A) : S_A^\infty$ in $\mathscr{R}$ and $\mathfrak{a}_0 = (A) : S_A^\infty$ in $\mathscr{R}_0 = \mathscr{F}(t_1, \ldots, t_m)[x_1, \ldots, x_r]$. To prove that $\mathfrak{a}$ is radical, it is sufficient to prove that the total ring of fractions of $\mathscr{R}/\mathfrak{a}$, denoted $\mathrm{Fr}(\mathscr{R}/\mathfrak{a})$, does not involve any nilpotent element. Since a direct product (or sum) of fields does not involve any nilpotent element, it is sufficient to prove that $\mathrm{Fr}(\mathscr{R}/\mathfrak{a})$ is isomorphic to such a ring. $\mathrm{Fr}(\mathscr{R}/\mathfrak{a})$ is equal to $(M/\mathfrak{a})^{-1}\,\mathscr{R}/\mathfrak{a}$ where M is the multiplicative family of the elements of $\mathscr{R}$ which are regular in $\mathscr{R}/\mathfrak{a}$. By Theorem 13, the nonzero elements of $\mathscr{F}[t_1, \ldots, t_m]$ belong to M. Therefore, inverting these elements first, we conclude that $\mathrm{Fr}(\mathscr{R}/\mathfrak{a}) \simeq \mathrm{Fr}(\mathscr{R}_0/\mathfrak{a}_0)$.

It is thus sufficient to prove that $\mathscr{R}_0/\mathfrak{a}_0$ is a direct sum of fields. This we do by induction on r. This ring can be constructed incrementally as $\mathscr{S}_r$ defined by:

$$\mathscr{S}_0 = \mathscr{F}(t_1, \ldots, t_m)\,, \quad \mathscr{S}_i = \mathscr{S}_{i-1}[x_i]/(p_i) : s_i^\infty\,.$$

The basis $r = 0$ is trivial.

Assume $\mathscr{S}_{r-1}$ is a direct sum of fields $\mathscr{F}_1 \oplus \cdots \oplus \mathscr{F}_\varrho$. Then $\mathscr{S}_r$ is isomorphic to the direct sum $(1 \leq j \leq \varrho)$ of the rings $\mathscr{F}_j[x_r]/(p_r) : s_r^\infty$.

Thus, in $\mathscr{F}_j[x_r]$, the ideal $(p_r) : s_r^\infty$ is generated by the product of the irreducible simple factors of p_r. It is thus the intersection of the maximal ideals $\mathfrak{m}_\ell$ generated by these factors. According to the Chinese Remainder Theorem [31, chap. III, sect. 13, Theorem 32, page 178], $\mathscr{F}_j[x_r]/(p_r) : s_r^\infty$ is isomorphic to the direct sum of the fields $\mathscr{F}_j[x_r]/\mathfrak{m}_\ell$. Since direct sums are associative, the ring $\mathscr{S}_r$ itself is a direct sum of fields. □

References

[1] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer Verlag, 2003.

[2] François Boulier. Réécriture algébrique dans les systèmes d'équations différentielles polynomiales en vue d'applications dans les Sciences du Vivant, May 2006. Mémoire d'habilitation à diriger des recherches. Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France. `http://tel.archives-ouvertes.fr/tel-00137153`.

[3] François Boulier and François Lemaire. A Normal Form Algorithm for Regular Differential Chains. *Mathematics in Computer Science*, 4(2):185–201, 2010. 10.1007/s11786-010-0060-3.

[4] François Boulier and al. DifferentialAlgebra. `https://codeberg.org/francois.boulier/DifferentialAlgebra`.

[5] François Boulier and Mercedes Haiech. The Ritt-Raudenbush Theorem and Tropical Differential Geometry. Available at `https://hal.archives-ouvertes.fr/hal-02403365`, 2019.

[6] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 158–166, New York, NY, USA, 1995. ACM Press. `http://hal.archives-ouvertes.fr/hal-00138020`.

[7] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20(1):73–121, 2009. (1997 Techrep. IT306 of the LIFL).

[8] François Boulier and François Lemaire. Computing canonical representatives of regular differential ideals. In *ISSAC'00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation*, pages 38–47, New York, NY, USA, 2000. ACM Press. `http://hal.archives-ouvertes.fr/hal-00139177`.

[9] François Boulier, François Lemaire, and Marc Moreno Maza. Well known theorems on triangular systems and the D^5 principle. In *Proceedings of Transgressive Computing 2006*, pages 79–91, Granada, Spain, 2006. `http://hal.archives-ouvertes.fr/hal-00137158`.

[10] François Boulier, François Lemaire, Marc Moreno Maza, and Adrien Poteaux. An Equivalence Theorem For Regular Differential Chains. *Journal of Symbolic Computation*, 93:34–55, 2019. doi:`10.1016/j.jsc.2018.04.011`.

[11] Shang-Ching Chou and Xiao-Shan Gao. On the dimension of an arbitrary ascending chain. *Chinese Bulletin of Science*, 38:799–904, 1993.

[12] Jan Denef and Leonard Lipshitz. Power Series Solutions of Algebraic Differential Equations. *Mathematische Annalen*, 267:213–238, 1984.

[13] Giovanni Gallo, Bubaneshwar Mishra, and François Ollivier. *Some constructions in rings of differential polynomials*, volume 539 of *Lecture Notes in Computer Science*, pages 171–182. , Montréal, Canada, 1991.

[14] Évelyne Hubert. Notes on triangular sets and triangulation–decomposition algorithm I: Polynomial Systems. *Symbolic and Numerical Scientific Computing 2001*, pages 243–158, 2003.

[15] A. Hurwitz. Sur le développement des fonctions satisfaisant à une équation différentielle algébrique. *Annales de l'École Normale Supérieure*, 6:327–332, 1889.

[16] Mickael Kalkbrener. A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. *Journal of Symbolic Computation*, 15:143–167, 1993.

[17] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.

[18] Serge Lang. *Algebra*. Addison-Wesley, 1965. Second printing (1967).

[19] Daniel Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Applied Mathematics*, 33:147–160, 1991.

[20] Youri Matiiassevitch. Enumerable sets are diophantine. *Sov. Math. Dokl.*, 11:354–357, 1970.

[21] Marc Moreno Maza. *Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques*. PhD thesis, Université Paris VI, France, 1997.

[22] Sally Morrison. Yet another proof of Lazard's lemma. private communication, december 1995.

[23] Sally Morrison. The Differential Ideal $[P] : M^{\infty}$. *Journal of Symbolic Computation*, 28:631–656, 1999.

[24] Joseph Fels Ritt. *Differential Algebra*, volume 33 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York, 1950.

[25] Azriel Rosenfeld. Specializations in differential algebra. *Trans. Amer. Math. Soc.*, 90:394–407, 1959.

[26] Abraham Seidenberg. An elimination theory for differential algebra. *Univ. California Publ. Math. (New Series)*, 3:31–65, 1956.

[27] Abraham Seidenberg. Abstract differential algebra and the analytic case. *Proc. Amer. Math. Soc.*, 9:159–164, 1958.

[28] Michael Singer. The Model Theory of Ordered Differential Fields. *Journal of Symbolic Logic*, 43(1):82–91, 1978.

[29] Ualbai Umirbaev. Algorithmic problems for differential algebras. *Journal of Algebra*, 455:77–92, 2016.

[30] Bruno Louis van der Waerden. *Algebra*. Springer Verlag, Berlin, seventh edition, 1966.

[31] Oscar Zariski and Pierre Samuel. *Commutative Algebra*. Van Nostrand, New York, 1958. Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag.