Afternotes on Differential Algebra

François Boulier
CRIStAL CFHP
Francois.Boulier@univ-lille1.fr

July 6, 2016

Introduction

In April 2016, I was offered to give a set of mini-lectures at the *Séminaire de Géométrie et Singularités* at IRMAR, on the simplification theory for differential polynomial systems. A set of mini-lectures is not just a long talk and the audience may want to get more than a flavour of the topic. However, the topic is really large and, if we really enter details, the allocated time is likely to be elapsed before any interesting notion gets addressed.

Actually, I teach computer science and numerical analysis in an Engineering School and this situation is classical ... at least for scientific courses. I have thus decided to proceed as I do at school: write every lecture as one could dream it, if we had no strong constraint on the allocated time and on the freshness of students. Afterwards, in front of students, real lectures are, somewhat, the "trailers" of the chapters.

Thus, every chapter of this document is thought as a lecture. It addresses a single key question and tries to stress what the issue is, with the help of the computer algebra MAPLE package `DifferentialAlgebra` [1]. I have tried also to design chapters so that they can be read as independently as possible, summarizing whenever it seemed reasonable to do it, at the beginning, some notions that are detailed in former chapters. As for lecture notes, I have restricted citations to the books and papers that I have actually used to write the chapters. In a survey paper, I would certainly have cited much more people.

Quite often, I rewrite lecture notes after the actual lectures, in the spirit of Stewart *Afternotes on Numerical Analysis* [5]. However, the simplification theory in differential algebra is much less taught than numerical analysis and the title of these *Afternotes on Differential Algebra* expresses a wish rather than a fact. Indeed, I think it would be quite important to have good "Afternotes" on Ritt and Kolchin differential algebra since I do not know any good introductory text to enter the topic. The book of Kolchin [2] is a very important reference book but is definitely not an introductory text. Ritt books [3, 4] are a good starting point but they were written quite some time ago and, for that reason, miss many important developments and clarifications which arose later. Besides them, there are also many research papers and PhD theses but I find them not so easy to read either. Indeed, there is something in differential algebra which makes it difficult to write simply.

Concerning the content, I have focused on the theory of *regular differential chains*, which are a modern variant of Ritt *characteristic sets*. Lectures 2, 3 and 4 address non-differential commutative algebra key issues on regular chains. This is necessary since systems of polynomial equations are particular cases of systems of differential polynomial equations. Lectures 5, 7, 6 and 9 address differential issues. Lectures 10 and 11 apply the theory to applications. A dependency graph between chapters is given in Figure 1 but, as mentioned before, readers should feel free to start with any chapter.

Last, I would like to thank my colleagues from the *Calcul Formel et Haute Performance* team of CRIStAL at Lille University and, more generally, from the *Computing and Control* research group, who were the first audience of these notes and helped me to improve them. And, of course, I would like to thank the organizers of the *Séminaire de Géométrie et Singularités* at IRMAR for their nice invitation.

Bibliography

[1] François Boulier and Edgardo Cheb-Terrab. `DifferentialAlgebra`. Package of MapleSoft MAPLE standard library since MAPLE 14, 2008.

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

[3] Joseph Fels Ritt. *Differential equations from the algebraic standpoint*, volume 14 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York, 1932.

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

[5] Gilbert W. Stewart. *Afternotes on Numerical Analysis*. SIAM, 1996.

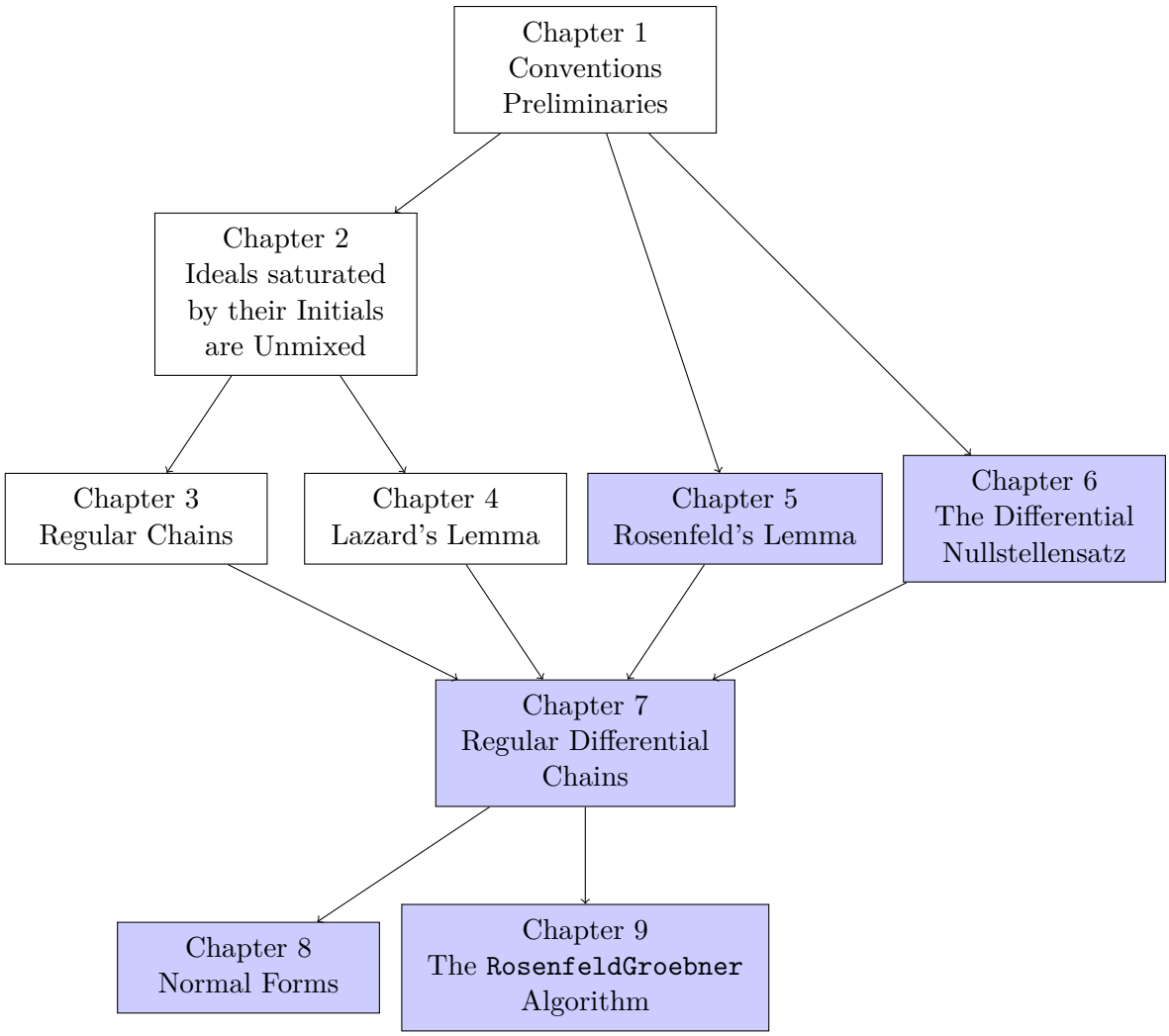


Figure 1: Logical progression between course chapters. Application chapters are not listed. Blue chapters are specifically concerned by differential algebra.

Contents

Chapter 1

Conventions and Preliminaries

The first section lists a few conventions applied in these lecture notes. The second one focuses on an ubiquitous ideal construct: the saturation of an ideal by a multiplicative family.

1.1 Conventions

These lecture notes contain many different theorems, propositions and lemmas. Some of them are the object of the course while some others are classical results, recalled for the convenience of the reader. By convention, all results falling in the first class are "propositions" while all "theorems" and "lemmas" are recalled classical results.

All rings are commutative, involve an identity and have characteristic zero. Domains are rings which are free of zero-divisors.

An element a of a ring R is a zero-divisor if there exists some nonzero $b \in R$ such that $a\,b = 0$. Therefore zero is a zero-divisor [3, I, 5, page 8]. An element a which is not a zero-divisor of R is said to be a *regular* element of R.

Many propositions involve statements such as "a polynomial f is zero (or a zero-divisor) in $R/\mathfrak{A}$ (R being a ring, $\mathfrak{A}$ being an ideal of R) if and only if f is reduced to zero (by some reduction process)". The word "zero" is used twice, here, but has different meanings. The expression "f is zero in $R/\mathfrak{A}$" should actually be written "the image of f by the canonical ring homomorphism $R \to R/\mathfrak{A}$ is zero" or, "f belongs to the ideal $\mathfrak{A}$". Similarly, the expression "f is a zero-divisor in $R/\mathfrak{A}$" should actually be written "the image of f by the canonical ring homomorphism $R \to R/\mathfrak{A}$ is a zero-divisor" or, "f is a zero-divisor modulo the ideal $\mathfrak{A}$". These are the properties for which we want a decision procedure: testing zero needs not be obvious in this context. The other expression "f is reduced to zero" means that the reduction process, which is a computational procedure, transforms f to zero, syntactically: in this context, testing zero is straightforward.

1.2 The Saturation

Let R be a ring.

An ideal $\mathfrak{p}$ is said to be *prime* if the residue class ring $R/\mathfrak{p}$ is a domain or — this is equivalent — if $a\,b \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

An ideal $\mathfrak{q}$ is said to be *primary* if all zero-divisors present in the residue class ring $R/\mathfrak{q}$ are nilpotent or — this is equivalent — if $a\,b \in \mathfrak{q}$ and $a \notin \mathfrak{q}$ imply that there exists some nonnegative

integer e such that $b^e \in \mathfrak{q}$.

The radical of a primary ideal $\mathfrak{q}$ is a prime ideal $\mathfrak{p} = \sqrt{\mathfrak{q}}$, called the *associated prime ideal* of $\mathfrak{q}$.

In these lecture notes, a very important operation on ideals is the *saturation* of an ideal $\mathfrak{A}$ by some $h \in R$ (more precisely, by the multiplicative family of R generated by h). It is the ideal

$$\mathfrak{A} : h^\infty \quad = \quad \{f \in R \mid \exists\, d \geq 0\,,\ h^d\, f \in \mathfrak{A}\}\,.$$

We have $\mathfrak{A} \subset \mathfrak{A} : h^\infty$. This construct somehow encodes the "division by h" since $f \in \mathfrak{A} : h^\infty$ whenever $h\, f \in \mathfrak{A} : h^\infty$.

It is important to study the behaviour of the saturation over primary ideals and intersections of primary ideals. Let $\mathfrak{q}$ be a primary ideal and $\mathfrak{p} = \sqrt{\mathfrak{q}}$ be its associated prime ideal. Then

- $\mathfrak{q} : h^\infty = R$ if and only if $h \in \mathfrak{p}$,
- $\mathfrak{q} : h^\infty = \mathfrak{q}$ if and only if $h \notin \mathfrak{p}$.

Let

$$\mathfrak{A} \quad = \quad \cap_{i=1}^r \mathfrak{q}_i\,, \quad (\text{with } \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}) \tag{1.1}$$

be a representation of $\mathfrak{A}$ as a finite intersection of primary ideals. From the above remarks, one sees that $\mathfrak{A} : h^\infty$ is the intersection of the primary ideals $\mathfrak{q}_i$ such that $h \notin \mathfrak{p}_i$, for $1 \leq i \leq r$. If all prime ideals $\mathfrak{p}_i$ contain h, then the intersection is empty and $\mathfrak{A} : h^\infty = R$.

To summarize, the saturation by h has the effect of removing from (1.1) the primary ideals whose associated prime ideals contain h.

Therefore, if $\mathfrak{A}$ is an intersection of primary ideals whose associated prime ideals share a common property then, provided that the intersection is not empty, $\mathfrak{A} : h^\infty$ is also an intersection of primary ideals whose associated prime ideals share this same property. In these lecture notes, we will encounter two important cases:

1. the case of unmixed ideals i.e. ideals whose associated primes all have the same dimension,
2. the case of radical ideals i.e. ideals whose primary components are prime ideals.

The representation (1.1) is said to be *irredundant* if 1) $\mathfrak{q}_i \not\subset \mathfrak{q}_j$ and, 2) $\mathfrak{q}_i \cap \mathfrak{q}_j$ is not primary, for $1 \leq i < j \leq r$. In such a case, the prime ideals $\mathfrak{p}_i$ are called the *associated prime ideals* of $\mathfrak{A}$ and the set of the zero-divisors of $R/\mathfrak{A}$ is the union of the associated prime ideals of $\mathfrak{A}$ (it is Condition 1 which is important, here).

This remark holds if R is a Nötherian ring, since every ideal of R has an irredundant representation (1.1). See [3, IV, Corollary 3 to Theorem 11, page 214]. However, it may hold also if R is not Nötherian. We will encounter such a situation in the case of R being a differential polynomial ring, where general differential ideals have no representation (1.1) but every radical differential ideal $\mathfrak{A}$ is an irredundant intersection of prime differential ideals. The set of the zero-divisors of $R/\mathfrak{A}$ is then the union of these prime differential ideals.

This remark has two consequences, related to the saturation. Given any ideal $\mathfrak{A}$ and any $h \in R$,

1. h is a regular element (i.e. is not a zero-divisor) in $R/\mathfrak{A} : h^\infty$,
2. h is a regular element of $R/\mathfrak{A}$ if and only if $\mathfrak{A} = \mathfrak{A} : h^\infty$.

Saturations can also be presented via localizations. Let h be an element of R and M the multiplicative family that it generates. Let R_M be the ring of all quotients[1] a/m such that $a \in R$ and $m \in M$ [3, IV, 9, page 221] and φ be the ring homomorphism $R \to R_M$. Then, the ideal of R_M generated by $\varphi(\mathfrak{A})$ is the *extended* ideal $\mathfrak{A}^e$ and the ideal $\varphi^{-1}(\mathfrak{A}^e)$, the *contracted* ideal $\mathfrak{A}^{ec}$, is equal to $\mathfrak{A} : h^\infty$. Some of the properties mentioned above are then given in [3, IV, 10, Theorem 15, page 223 and Theorem 17, page 225].

Saturations are also related to the Hilbert Nullstellensatz [3, VII, 3, Theorem 14, page 164]. Let R be a polynomial ring and consider a system $p_1 = \cdots = p_n = 0$, $h \neq 0$ of polynomial equations and inequations. Then $\sqrt{(p_1, \ldots, p_n)} : h^\infty$ is the ideal of all the polynomials that vanish over the solution set of the polynomial system (taken in the algebraic closure of the ground field of R).

1.3 The Pseudodivision

Let R be a ring, x be an indeterminate, f and $g \neq 0$ be two polynomials of $R[x]$

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

If b_n is not an invertible element of r then the Euclidean division of f by g may not be possible. However, it is always possible to carry out the pseudodivision of f by g, which is a close variant [2, 6, 5, page 302]. The pseudoremainder $r = \mathsf{prem}(f, g, x)$ and the pseudoquotient $q = \mathsf{pquo}(f, g, x)$ are defined as follows:

- if $m < n$ then $r = f$ and $q = 0$;
- if $m \geq n$ then (r, q) is the unique pair of polynomials of $R[x]$ such that $\deg r < n$, $\deg q = m - \deg r$ and

$$b_n^{m-n+1}\, f \;\; = \;\; g\, q + r\,.$$

The pseudodivision is connected to the saturation because, if $r = 0$ then $f \in (g) : b_n^\infty$.

1.4 The Resultant

This section is much inspired from [1, 4.2, pages 105-109]. A complete and precise presentation of resultants would be much too long for these notes. This section only states the properties of resultants which are actually needed for the following chapters. Let R be a ring, x be an indeterminate, f and g be two polynomials of $R[x]$

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

If f or g is zero, then the resultant of f and g is taken to be zero. Assume f and g are nonzero. Then, the resultant of f and g is the determinant of the Sylvester matrix $S(f, g)$ of f and g, which

[1] We adopt here the notation of Zariski and Samuel. With a more modern terminology, R_M would be denoted $h^{-1}\, R$, i.e. the ring R localized at h.

is the following matrix, with dimensions $(m+n)\times(m+n)$.

$$S(f,g)=\begin{pmatrix} a_m & \cdots & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & \cdots & \cdots & \cdots & \cdots & a_0 \\ b_n & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_n & \cdots & \cdots & \cdots & b_0 \end{pmatrix}$$

Assume f is nonzero. The particular case $n=0$ (i.e. $g=b_0$) will show up in the following chapters. Then, the Sylvester matrix $S(f,g)$ is a diagonal matrix of dimensions $m\times m$ with b_0 on its diagonal and $\mathsf{res}(f,g,x)=b_0^m$.

Assume f and g are nonzero. Any two polynomials $u=u_{n-1}\,x^{n-1}+\cdots+u_1\,x+u_0$ and $v=v_{m-1}\,x^{m-1}+\cdots+v_1\,x+v_0$ of degrees $n-1$ and $m-1$ can be identified with the vector $(u_{n-1}\cdots u_0\ v_{m-1}\cdots v_0)^T$. The Sylvester matrix above is then the transpose of the matrix of the linear mapping $(u,v)\mapsto u\,f+v\,g$. The following Theorem is [1, 4.2, Proposition 4.15, page 106].

Theorem 1 *Assume R is a domain and let K denote its fraction field. Let f and g be two polynomials of $R[x]$, not both zero. Then $\mathsf{res}(f,g,x)=0$ if and only if f and g have a common factor in $K[x]$.*

Proof The Theorem obviously holds if one of the polynomials is zero. Assume both are nonzero. By the above remark, $\mathsf{res}(f,g,x)=0$ if and only if there exists nonzero polynomials $u,v\in K[x]$ with $\deg u<n$ and $\deg v<m$ such that $u\,f+v\,g=0$. Thus $\mathsf{res}(f,g,x)=0$ if and only if f and g have a common multiple in $K[x]$ of degree strictly less than $m+n$, hence a common factor in $K[x]$. □

The following Theorem is adapted from [1, 4.2, Lemma 4.17, page 107].

Theorem 2 *Let R be a domain, f and g be two polynomials in $R[x]$. Assume g is nonzero and let $r=c_t\,x^t+\cdots+c_1\,x+c_0$ be the pseudoremainder of f by g. If f is zero or r is zero then $\mathsf{res}(f,g,x)=\mathsf{res}(g,r,x)=0$. Otherwise,*

$$\mathsf{res}(f,g,x) \;=\; (-1)^{m\,n}\,b_n^{\max(0,m-t-(m-n+1)\,n)}\;\mathsf{res}(g,r,x)\,.$$

Proof If f is zero then r is zero and both resultants are zero. Assume f is nonzero. If r is zero, then $\mathsf{res}(g,r,x)=0$ and there exists a polynomial $q\in R[x]$, such that $b_n^{m-n+1}\,f=q\,g$. Thus f is a multiple of g in $K[x]$, where K denotes the fraction field of R. By Theorem 1, we have $\mathsf{res}(f,g,x)=0$.

Assume f and r are nonzero. If $m<n$ then $r=f$, $m=t$ and $\max(0,m-t-(m-n+1)\,n)=0$. The matrix $S(g,r)$ is obtained from $S(f,g)$ by performing $m\,n$ exchanges of rows. We thus have $\mathsf{res}(f,g,x)=(-1)^{m\,n}\,\mathsf{res}(g,r,x)$ and the Theorem holds. Assume $m\geq n$. The Sylvester matrix $S(g,r)$ can be obtained from $S(f,g)$ by performing the following steps.

Step 1. Form the Sylvester matrix $S(b_n^{m-n+1} f, g)$. Since this amounts to multiply the n first rows of $S(f,g)$ by b_n^{m-n+1}, we have $b_n^{(m-n+1)\,n}\ \mathsf{res}(f,g,x) = \det(S(b_n^{m-n+1} f, g))$.

Step 2. Form the Sylvester matrix of r and g *as if* we had $t = m$. Let us denote $S^*(r,g)$ this matrix (see below). Let q denote the pseudoquotient so that $b_n^{m-n+1} f - g\,q = r$. Since adding to a row a multiple of another row does not change the determinant, we see that $\det(S(b_n^{m-n+1} f, g)) = \det(S^*(r,g))$.

$$S^*(r,g) = \begin{pmatrix} 0 & 0 & c_t & \cdots & \cdots & c_0 & 0 & \cdots & 0 \\ 0 & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & c_t & \cdots & \cdots & c_0 \\ b_n & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_n & \cdots & \cdots & \cdots & b_0 \end{pmatrix}$$

Step 3. Perform $m\,n$ exchanges of rows, yielding the matrix $S^*(g,r)$ (see below). We have $\det(S^*(r,g)) = (-1)^{m\,n} \det(S^*(g,r))$. The Sylvester matrix $S(g,r)$ appears as the $(n+t)\times(n+t)$ submatrix of $S^*(g,r)$ on the bottom-right corner.

$$S^*(g,r) = \begin{pmatrix} b_n & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & b_n & \cdots & \cdots & \cdots & b_0 & 0 & 0 \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \ddots & 0 & b_n & \cdots & \cdots & \cdots & b_0 \\ 0 & 0 & c_t & \cdots & \cdots & c_0 & 0 & \cdots & 0 \\ 0 & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & c_t & \cdots & \cdots & c_0 \end{pmatrix}$$

Step 4. Developing the determinant of $S^*(g,r)$ w.r.t. its $m-t$ first columns, one obtains $\det(S^*(g,r)) = b_n^{m-t}\, S(g,r)$.

Combining all these formulas, the Theorem is proved. □

Corollary 1 *Keep the same notations as Theorem 2. Assume* $g = b_1\,x + b_0$. *Then* $\mathsf{res}(f,g,x) = \pm r$.

Proof If the pseudoremainder r is zero then the Corollary is just a particular case of Theorem 2. Assume r is nonzero. Then $t = 0$ and $m - t - (m-n+1)\,n = 0$. According to Theorem 2, we have $\mathsf{res}(f,g,x) = \pm\,\mathsf{res}(g,r,x)$. Since $n = 1$ and $t = 0$, the Sylvester matrix $S(g,r)$ has dimensions 1×1. Its determinant is r. □

The following Theorem is [1, 4.2, Proposition 4.18, page 108].

Theorem 3 *Let R be a ring. If f and g are nonzero polynomials of $R[x]$ then there exists two polynomials $u, v \in R[x]$ with $\deg(u) < n$ and $\deg(v) < m$ such that $\mathsf{res}(f, g, x) = u\, f + v\, g$.*

Proof The proof is the one of [1, 4.2, Proposition 4.18, page 108].

Let $S^*(f, g)$ be the matrix obtained from $S(f, g)$ by replacing the elements of its last column by $x^{n-1}\, f, \ldots, x\, f, f, x^{m-1}\, g, \ldots, x\, g, g$. In the particular case $(m, n) = (3, 2)$, we get

$$S^*(f,g) = \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & x\, f \\ 0 & a_3 & a_2 & a_1 & f \\ b_2 & b_1 & b_0 & 0 & x^2\, g \\ 0 & b_2 & b_1 & b_0 & x\, g \\ 0 & 0 & b_2 & b_1 & g \end{pmatrix}.$$

Developing the determinant w.r.t. the last column, it is clear that there exists two polynomials $u, v \in R[x]$ with $\deg(u) < n$ and $\deg(v) < m$ such that $\det(S^*(f, g)) = u\, f + v\, g$.

The key idea is now that the determinant is a linear function of the last column of the matrix. Over our example, the last column of $S^*(f, g)$ is equal to the one of $S(f, g)$ plus the vector

$$\begin{pmatrix} x\, f \\ f - a_0 \\ x^2\, g \\ x\, g \\ g - b_0 \end{pmatrix} = x \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ b_0 \\ b_1 \end{pmatrix} + x^2 \begin{pmatrix} a_1 \\ a_2 \\ b_0 \\ b_1 \\ b_2 \end{pmatrix} + \cdots + x^4 \begin{pmatrix} a_3 \\ 0 \\ b_2 \\ 0 \\ 0 \end{pmatrix}.$$

If one replaces the last column of $S^*(f, g)$ by one of the vectors occuring on the right-hand side above, the determinant vanishes (the matrix has two identical columns). Coming back to the general case, we see that

$$\det(S^*(f,g)) \quad = \quad \mathsf{res}(f, g, x) + \sum_{i=1}^{m+n-1} D_i\, x^i$$

where the D_i denote determinants all equal to zero. The proof is completed. □

The following Theorem is adapted from [1, 4.2, Proposition 4.20, page 109].

Theorem 4 *Let R be a ring. Let f and g be two polynomials of $R[x]$ such that $a_m = 1$ and $m \geq n$. Let $\phi : R \to S$ be a ring homorphism, extending to a ring homomorphism $R[x] \to S[x]$. Then $\phi(\mathsf{res}(f, g, x)) = \mathsf{res}(\phi(f), \phi(g), x)$.*

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 $\mathsf{res}(f, g, x) = 0$ and the Theorem holds.

Assume g and $\phi(g)$ are nonzero. The ring homomorphism ϕ does not change a_m, which is equal to 1. If it does not annihilate b_n then $S(f, g) = S(\phi(f), \phi(g))$ and the Theorem is proved. Assume

$\deg(\phi(g)) = t < n$. Then

$$\phi(S(f,g)) = \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \phi(a_0) & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & 1 & \cdots & \cdots & \cdots & \phi(a_0) & 0 & 0 \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \ddots & 0 & 1 & \cdots & \cdots & \cdots & \phi(a_0) \\ 0 & 0 & \phi(b_t) & \cdots & \cdots & \phi(b_0) & 0 & \cdots & 0 \\ 0 & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & \phi(b_t) & \cdots & \cdots & \phi(b_0) \end{pmatrix}.$$

The Sylvester matrix $S(\phi(f), \phi(g))$ appears as the $(m+t) \times (m+t)$ submatrix of $\phi(S(f,g))$ at the bottom-right corner. Developing the determinant of $\phi(S(f,g))$ w.r.t. its $n-t$ first columns, we see that $\phi(\mathsf{res}(f,g,x)) = \mathsf{res}(\phi(f), \phi(g), x)$. $\square$

Bibliography

[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] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms. An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer Verlag, New York, 2nd edition, 1996.

[3] 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.

Chapter 2

Ideals Defined by Triangular Sets are Unmixed

This chapter aims at proving Proposition 4, which is necessary for proving many further results of these lecture notes. However, for a casual reader, this chapter is probably one of the most difficult to read because it is technical and addresses an issue which is not evident for a beginner. The informal introduction below, which unfortunately suggests Proposition 4 only remotely, was used to present differential elimination during a very first course. It should be easy to follow.

2.1 Informal Introduction

First we load the `DifferentialAlgebra` MAPLE package.

```
> with (DifferentialAlgebra):
```

The variable `sys` is assigned a system of polynomial PDE, in jet notation. The very same system, written using Jacobi's notation for partial derivatives, is assigned to `sys_diff`. The equations (the sign "$= 0$" is omitted but the polynomials are viewed as left hand-sides of equations) are polynomials. The two *differential indeterminates* u and v represent unknown functions of the two independent variables x and y. The constant 1 represents the constant function of the two variables x and y, equal to 1. In commutative algebra, polynomials belong to polynomial rings. In *differential algebra* [8, 5], *differential polynomials* belong to *differential polynomial rings*. Such a differential polynomial ring is assigned to the `R` variable.

```
> R := DifferentialRing(derivations = [x,y], blocks = [[v,u]]);
                              R := differential_ring

> sys := [u[x]^2-4*u, u[x,y]*v[y]-u+1, v[x,x]-u[x]];
                         2
          sys := [u[x]  - 4 u, u[x, y] v[y] - u + 1, v[x, x] - u[x]]

> sys_diff := Equations(sys, R, notation=diff);
              / 2         \
              |d          |   /d         \
sys_diff := [|--- v(x, y)| - |-- u(x, y)|,
              |  2        |   \dx        /
              \dx         /
```

```
/  2          \
| d           | /d         \                /d         \2
|----- u(x, y)| |-- v(x, y)| - u(x, y) + 1, |-- u(x, y)|  - 4 u(x, y)]
\dy dx        / \dy        /                \dx        /
```

There exists a notion of *leading derivative* of a differential polynomial. This notion is by no means intrinsic. It is defined by an ordering (a *ranking*) on the set of all the derivatives of the differential indeterminates. In the variable `R` above, a ranking was defined together with the more mathematical differential polynomial ring. The following command returns the differential polynomials of `sys` in "solved form" i.e. as equations, with the leading derivatives on the left hand-sides and differential fractions on the right-hand sides.

```
> Equations(sys, R, solved);
                                              -u + 1      2
                [v[x, x] = u[x], u[x, y] = - ------, u[x]  = 4 u]
                                               v[y]
```

Just to show that rankings are by no means intrinsic, the variable `Rbis` is assigned the same mathematical differential polynomial ring, with another ranking (look at the change on the `block` list). In the solved form of `sys`, some other derivatives become leading derivatives.

```
> Rbis := DifferentialRing(derivations = [x,y], blocks = [v,u]);
                           Rbis := differential_ring

> Equations(sys, Rbis, solved);
                                            -u + 1       2
                 [v[x, x] = u[x], v[y] = - -------, u[x]  = 4 u]
                                            u[x, y]
```

The following command shows that there exists an algorithm which takes as input 1) a system of differential polynomials, 2) a ranking. It returns a list of *regular differential chains*. As one can see, regular differential chains are sets of differential polynomials.

```
> ideal := RosenfeldGroebner(sys,R);
                      ideal := [regular_differential_chain]

> ideal := ideal[1]:
> Equations(ideal, solved);
                               -u[x] u[y] u + u[x] u[y]      2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u,
                                        u

        2
    u[y]  = 2 u]
```

A regular differential chain permits to expand solutions of the initial system into formal power series, from given initial values. The example is very particular because all its solutions are polynomials. The commands below compute the solution, plug it in the input system and check the equation evaluate to zero.

```
> iv := [u=c[0]^2, u[y]=sqrt(2)*c[0], u[x]=2*c[0], v=c[1], v[x]=c[2]];
                    2          1/2
   iv := [u = c[0] , u[y] = 2    c[0], u[x] = 2 c[0], v = c[1], v[x] = c[2]]
```

```
> sols := PowerSeriesSolution(ideal, 3, iv);
                          /                  1/2\
                          |        2  1/2   2   |                          2
sols := [v(x, y) = c[1] + |1/2 c[0]  2    - ----| y + c[2] x + 1/2 c[0] y
                          \                  2  /

                                    1/2  3      2    1/2  2       3
       1/2                   2   2    y    x y    2    x  y    x
    + 2    c[0] x y + c[0] x  + ------- + ---- + --------- + ----,
                                  12       2         2        3

                                                 2
                 2    1/2                       y      1/2        2
   u(x, y) = c[0]  + 2    c[0] y + 2 c[0] x + ---- + 2    x y + x ]
                                              2

> expand (eval (sys_diff, sols));
                                  [0, 0, 0]
```

Why do initial values look so complicated? Well, the differential equations state equalities between functions of x and y. In particular, these equalities must be satisfied at the origin. The following command shows the constraints that initial values must satisfy. Knowing that `D[1](u)` stands for $\partial u/\partial x$, one sees that the constraints are obtained by stating that the regular differential chain equations must be satisfied at the origin. Only the leading nonlinear equations need to be given.

```
> PowerSeriesSolution(conditions, ideal);
              2                                 2
[[D[1](u)(0, 0)  - 4 u(0, 0) = 0, D[2](u)(0, 0)  - 2 u(0, 0) = 0],

    [u(0, 0) <> 0, D[1](u)(0, 0) <> 0, D[2](u)(0, 0) <> 0]]
```

Much less obvious: every algebraic solution of the above system can be prolongated into a differential solution (a formal power series). This property holds for the regular differential chain but not for the input system. From a theoretical point of view, it is due to the fact that regular differential chains satisfy Rosenfeld's Lemma [9].

The conditions on initial values involve inequations ($\neq 0$): the *initials* and *separants* of the regular differential chain must not vanish at the origin. This condition is quite intuitive for initials, since they are the polynomials which show up as denominators of the equations, in solved form. Separants are the polynomials which show up as denominators of the proper derivatives of the equations, in solved form.

```
> Tools:-Initial (ideal);
                                [1, 4 u, 1, 1]

> Tools:-Separant (ideal);
                           [1, 4 u, 2 u[x], 2 u[y]]

> Equations (Tools:-Differentiate (u[x]^2 - 4*u, y, R), R, solved);
                                      2 u[y]
                                u[x] = ------
                                       u[x]
```

We have computed a regular differential chain from some input system. We have solved the regular differential chain and obtained a solution for the input system. Do they have the same solutions? Short answer: yes. This is due to the fact that they *define* (in some way) the same *differential ideal*. The computation of formal power series solutions is strongly related to the computation of some *normal forms* of differential fractions, modulo the differential ideal under consideration. In our case (by opposition to the Gröbner bases theory), normal form computations raise two issues: 1) deciding membership to differential ideals, and 2) deciding zero-divisorship (i.e. non-regularity) modulo differential ideals.

```
> NF1 := NormalForm (v[x,x,y], ideal);
                                          u[x] u[y]
                              NF1 := 1/2 ---------
                                             u

> NF2 := NormalForm (1/v[x,x,y], ideal);
                                          u[x] u[y]
                              NF2 := 1/4 ---------
                                             u

> NormalForm (NF1 * NF2, ideal);
                                       1
```

To understand more precisely the ideas evocated in this section, we are going to study, in the next sections, the structure of the non-differential ideals defined by regular differential chains. The unmixedness property of these ideals permits to view any regular differential chain, such as our example, as a triangular system of four monic polynomials (i.e. with initials all equal to 1) in a polynomial ring in four indeterminates (v_{xx}, v_y, u_x, u_y), over a field of rational fractions $(K(u))$. This is precisely what the following command illustrates and this will prove most helpful in Chapter 3.

```
> Equations (ideal, solved);
                              -u[x] u[y] u + u[x] u[y]      2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u,
                                          u

       2
   u[y]  = 2 u]
```

2.2 The Issue

The rest of this talk is uniquely concerned by non-differential problems. We consider a triangular system $A = \{p_1, \ldots, p_n\}$ in a polynomial ring $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. The system is triangular in the following sense: each polynomial p_k introduces at least one variable, its leading variable x_k. Our introductory regular differential chain is a particular case of a triangular system

$$\underbrace{v_{xx} - u_x}_{p_4}, \quad \underbrace{4\,u\,v_y + u_x\,u_y\,u - u_x\,u_y}_{p_3}, \quad \underbrace{u_x^2 - 4\,u}_{p_2}, \quad \underbrace{u_y^2 - 2\,u}_{p_1},$$

by renaming $(x_1, x_2, x_3, x_4) = (u_y, u_x, v_y, v_{xx})$ and $(t_1) = (u)$. For each $1 \leq k \leq n$, the initial of p_k is the leading coefficient of p_k w.r.t. x_k and the separant of p_k is the polynomial $s_k = \partial p_k / \partial x_k$.

To a triangular system A, we are going to associate some ideal $\mathfrak{A}$ of R. Observe this ideal may be equal to R. Assume this is not the case, i.e. that $\mathfrak{A}$ is proper. We will address questions such as: given some $f \in R$, is f zero? or a zero-divisor in $R/\mathfrak{A}$? Rather than working in the ring R, we would like to work in the ring

$$R_0 \quad = \quad K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$$

which is obtained from R by inverting all nonzero polynomials of $K[t_1, \ldots, t_m]$.

The issue. We need first to prove that nonzero elements of $K[t_1, \ldots, t_m]$ are not zero-divisors in $R/\mathfrak{A}$. This is a basic requirement, stated in [11, I, 19, page 42] — and related to the notion of the *total quotient ring* of a ring. By [11, IV, 6, Corollary 3 to Theorem 11, page 214], we thus need to prove that, if $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{A}$ (isolated or imbedded), then $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$.

A Note on the Lasker-Nöther Theorem. Isolated and imbedded associated primes are notions strongly related to the Lasker-Nöther Theorem [11, IV, 4-5, pages 208-212].

Theorem 5 *(Lasker-Nöther Theorem)*
In a Nötherian ring R, every ideal $\mathfrak{a}$ can be represented by an irredundant primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. Irredundant means that, for $i \neq j$, 1) $\mathfrak{q}_i \not\subset \mathfrak{q}_j$ and 2) $\mathfrak{q}_i \cap \mathfrak{q}_j$ is not primary.

The prime ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are the *associated* prime ideals of $\mathfrak{a}$. The associated primes of $\mathfrak{a}$ which contain no other associated prime are said to be *isolated*. The ones which are not isolated are said to be *imbedded*.

In $\mathbb{R}[x, y]$, take $\mathfrak{a} = (x^2, x\,y)$. Then $\mathfrak{a} = (x) \cap (x^2, y)$ is an irredundant primary decomposition of $\mathfrak{a}$. The associated prime ideals are (x) (isolated) and (x, y) (imbedded).

In polynomial rings, an ideal defines an algebraic variety. Isolated primes correspond to irreducible components of the variety (the line $x = 0$). Imbedded primes correspond to embedded varieties (the point $(x, y) = (0, 0)$).

The Ideal Under Consideration. Let h denote *either* the product of the initials *or* the product of the separants of the polynomials p_k. We are going to handle both cases in the same proof. We could actually even handle more cases since the only property we actually need is that, if $\mathfrak{p}$ is an associated prime ideal of the ideal $\mathfrak{A}$, then the polynomials p_k cannot *completely* degenerate in $R/\mathfrak{p}$ (see the proof of Proposition 2 for more details).

Let thus $\mathfrak{A}$ denote the ideal $(A) : h^\infty$ (the ideal generated by A, saturated by the multiplicative family generated by h) i.e.

$$\mathfrak{A} \quad = \quad \{f \in R \mid \exists\, d \geq 0,\, h^d\, f \in (A)\}$$

Sketch of Proof. The sketch of proof of Proposition 4 is as follows:

1. Consider $\mathfrak{A}' = (A, \underbrace{h\, x_{n+1} - 1}_{p_{n+1}})$ in $R' = R[x_{n+1}]$.

2. Use the "principal ideal theorem" [11, IV, 9, Theorem 30, page 240] or its reformulation [11, VII, 7, Theorem 22, page 196] and the structure of h in order to prove that, if $\mathfrak{p}'$ is an isolated prime of $\mathfrak{A}'$ then $\dim \mathfrak{p}' = m$ and $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

3. Use then Macaulay's unmixedness theorem [11, VII, 8, Theorem 26, page 203] in order to prove that all associated prime ideals of $\mathfrak{A}'$ are isolated.

4. Last, use the behaviour of the irredundant primary decomposition of $\mathfrak{A}'$ under passage to residue class ring (p_{n+1}) [11, IV, 5, page 213] and contraction (with respect to the localization at h) [11, IV, 10, Theorem 17, page 225]. Proposition 4 is proved.

2.3 The Result

Almost all references are towards the *Commutative Algebra* of Zariski and Samuel [11]. To simplify proof checking, the key theorems used from [11] are restated almost as is. I have only shortened some of them and often renamed rings and ideals to make correspondences easier to state.

Denote φ the localization at h i.e. the ring homomorphism

$$R \quad \xrightarrow{\varphi} \quad h^{-1} R \,.$$

With the terminology of Zariski and Samuel, $h^{-1} R = R_M$ where M denotes the multiplicative family generated by h. Extended and contracted ideals [11, IV, 8] are taken with respect to the ring homomorphism φ, and the ideal $\mathfrak{A}$ is a contracted ideal i.e. $\mathfrak{A} = \mathfrak{A}^{ec}$ (see Chapter 1). The extended ideal $\mathfrak{A}^e$ is just the ideal generated by $A/1 = \{p_1/1, \ldots, p_n/1\}$ in the localized ring $h^{-1} R$. Let us now introduce the ring $R' = R[x_{n+1}]$, the polynomial $p_{n+1} = h\, x_{n+1} - 1$ and the ideal $\mathfrak{A}' = (A,\, p_{n+1})$ of R'. Let π denote the ring homomorphism (quotient of R' by the ideal (p_{n+1}))

$$R' \quad \xrightarrow{\pi} \quad R'/(p_{n+1}) \,.$$

These two constructs are related by the ring isomorphism:

$$h^{-1} R \quad \simeq \quad R'/(p_{n+1}) \,.$$

Indeed, every element of $h^{-1} R$ is a fraction f/h^d with $f \in R$ and corresponds to the equivalence class of $f\, x_{n+1}^d$ modulo (p_{n+1}). The two ideals $\mathfrak{A}^e$ and $\pi\, \mathfrak{A}'$ are the same ideal, since they share a same generating family: A.

Proposition 1 *The ideal $\mathfrak{A}$ is proper if and only if the ideal $\mathfrak{A}'$ is proper.*

Proof Both ideals contain 1 if and only if some power of h belongs to the ideal (A). □

In the sequel, we assume $\mathfrak{A}'$ is proper. Let us recall [11, VII, 7, Theorem 22, page 196], which is nothing but a reformulation, using the terminology of the dimension theory of [11, IV, 9, Theorem 30, page 240]. It is a form of the "principal ideal theorem".

Theorem 6 *If S is a finite integral domain, of transcendence degree r, and $\mathfrak{B}$ is a proper ideal in S wich admits a basis of s elements, then every isolated prime ideal of $\mathfrak{B}$ has dimension $\geq r - s$.*

Proposition 2 *We have* $\dim \mathfrak{A}' = m$. *If* $\mathfrak{p}'$ *is an isolated prime ideal of* $\mathfrak{A}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Proof Applying Theorem 6 (the principal ideal theorem) with $(S, r, s, \mathfrak{B}) = (R', n+m+1, n+1, \mathfrak{A}')$, 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

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

Because of the triangular nature of A, the coefficients

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

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 $R'/\mathfrak{p}'$, 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 $R'/\mathfrak{p}'$. Putting this remark in an inductive argument, we see that $x_1, \ldots, x_n$ are algebraic over $t_1, \ldots, t_m$ in $R'/\mathfrak{p}'$. 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 $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$. □

Let us recall the following theorem, due to Macaulay [11, VII, 13, Theorem 26, page 203]. An ideal is said to be *unmixed* if all its associated prime ideals have the same dimension [11, VII, 7, page 196].

Theorem 7 *Let* $\mathfrak{B}$ *be an ideal in* $S = K[y_1, \ldots, y_r]$ *of dimension* $r - s$. *If* $\mathfrak{B}$ *is generated by* s *elements, then* $\mathfrak{B}$ *is unmixed.*

Proposition 3 *The ideal* $\mathfrak{A}'$ *is unmixed. If* $\mathfrak{p}'$ *is an associated prime ideal of* $\mathfrak{A}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Proof It is an immediate corollary to Theorem 7 (Macaulay's unmixedness Theorem) and Proposition 2. □

Let us now recall an important information, stated as a remark [11, IV, 5, Remark concerning passage to a residue class ring, page 213].

> Let S be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ two ideals of S such that $\mathfrak{b} \subset \mathfrak{a}$. [...]. Consequently, if $\mathfrak{a} = \cap_i \mathfrak{q}_i$ is an irredundant primary representation of $\mathfrak{a}$ and if $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, then $\mathfrak{a}/\mathfrak{b} = \cap_i (\mathfrak{q}_i/\mathfrak{b})$ is an irredundant primary representation of $\mathfrak{a}/\mathfrak{b}$, and the $\mathfrak{p}_i/\mathfrak{b}$ are the associated prime ideals of $\mathfrak{a}/\mathfrak{b}$.

Let us also recall [11, IV, 10, Theorem 17, page 225]. In this theorem, S is a Nötherian ring and the ring homomorphism with respect to which contractions and extensions are considered is the localization at some multiplicative family M. We are going to apply it with M being the set of all powers of h.

Theorem 8 *Let $\mathfrak{a}$ be an ideal of S admitting an irredundant primary representation $\mathfrak{a} = \cap_{i=1}^{s} \mathfrak{q}_i$. Suppose that, for $1 \leq i \leq r$, we have $\mathfrak{q}_i \cap M = \varnothing$, and that, for $r+1 \leq j \leq s$, we have $\mathfrak{q}_j \cap M \neq \varnothing$. Then $\mathfrak{a}^e = \cap_{i=1}^{r} \mathfrak{q}_i{}^e$ is an irredundant primary representation of $\mathfrak{a}^e$, and we have $\mathfrak{a}^{ec} = \cap_{i=1}^{r} \mathfrak{q}_i$, that is, $\mathfrak{a}^{ec}$ is the intersection of those primary components of $\mathfrak{a}$ which are disjoint from M.*

In the last sentence, the theorem does not say that $\mathfrak{a}^{ec} = \cap_{i=1}^{r} \mathfrak{q}_i$ is an irredundant primary representation of $\mathfrak{a}^{ec}$ but this is obvious, since a sub-intersection of an irredundant primary representation must be irredundant.

Proposition 4 *The ideal $\mathfrak{A}$ is unmixed. If $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{A}$ then $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$.*

Proof Let $\mathfrak{A}' = \cap_{i=1}^{r} \mathfrak{q}'_i$ be an irredundant primary representation of $\mathfrak{A}'$ and $\mathfrak{p}'_i = \sqrt{\mathfrak{q}'_i}$. Let us apply the "remark concerning passage to a residue class ring" with $(S, \mathfrak{a}, \mathfrak{b}) = (R', \mathfrak{A}', (p_{n+1}))$ and recall the definition of the π ring homomorphism. We see that $\pi\,\mathfrak{A}' = \cap_{i=1}^{r} (\pi\,\mathfrak{q}'_i)$ is an irredundant primary representation of $\pi\,\mathfrak{A}'$ and that the $\pi\,\mathfrak{p}'_i$ are the associated prime ideals of $\pi\,\mathfrak{A}'$.

Recall Proposition 3 and observe that the π ring homomorphism removes one indeterminate and one polynomial. For each prime ideal $\pi\,\mathfrak{p}'$ (dropping the index i), one thus still has $\dim \pi\,\mathfrak{p}' = m$ and (with a slight abuse of notation) $\pi\,\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Recall the ring isomorphism between $h^{-1}\,R$ and $R'/(p_{n+1})$. We have $\mathfrak{A} = \mathfrak{A}^{ec}$ and $\mathfrak{A}^e = \pi\,\mathfrak{A}'$. Let us apply Theorem 8 with $(S, \mathfrak{a}, M) = (R, \mathfrak{A}, \{h^d \mid d \geq 0\})$. Then $\mathfrak{A} = \cap_{i=1}^{r} (\pi\,\mathfrak{q}'_i)^c$ 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 $(\pi\,\mathfrak{p}')^c \cap K[t_1, \ldots, t_m] = (0)$.

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

2.4 Concluding Remarks

Proposition 4 is not mentionned in [5].

There were quite some papers mentioning the unmixedness properties of algebraic varieties defined by triangular sets or — this is equivalent — of radicals of ideals defined by triangular sets. The earlier reference I know is [10, page 59]. Let me mention also [4, 3]. Let us stress the fact that these results do not address the question of the possible imbedded associated prime ideals.

As far as I know, Sally Morrison was the first one to point out the issue mentioned in Section 2.2, the importance of Macaulay's unmixedness theorem and to provide a complete proof in the case of ideals saturated by separants. See [6, 7].

The proof exposed here, covering all cases in the same argument (Proposition 2), is essentially the one given in [2, 1]. I have reorganized it to make it simpler to understand and I have added the remark that Proposition 4 can be applied to more cases than just the case of h being the product of the initials, or the product of the separants.

Bibliography

[1] 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`.

[2] 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`.

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

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

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

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

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

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

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

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

[11] 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.

Chapter 3

Regular Chains

Regular differential chains are particular cases of *regular chains*. This chapter aims at proving Proposition 5.

3.1 Informal Introduction

A regular chain is a triangular system of $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ which can be transformed into an equivalent monic triangular system in $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. Beware to the fact that the transformation must be bottom up and, at each step, must only involve already processed polynomials. From an algorithmic point of view, this condition is simple and natural, though it looks so complicated when stated formally in Definition 1.

Let us consider a triangular system $A = \{p_1, p_2\}$ of the polynomial ring $R = K[t_1, x_1, x_2]$. Let us view it as a polynomial system of $K(t_1)[x_1, x_2]$.

```
> p1 := t[1]*x[1]^2 - x[1];
                                          2
                              p1 := t[1] x[1]  - x[1]

> p2 := (x[1]-1)*x[2]^3 - x[1]*x[2] + t[1];
                                              3
                      p2 := (x[1] - 1) x[2]  - x[1] x[2] + t[1]
```

The initial of $p_1 \in K(t_1)$. Let us invert it and obtain a monic version of p_1, denoted p_{01}.

```
> p01 := collect (p1 / t[1], x[1]);
                                        2   x[1]
                           p01 := x[1]  - ----
                                          t[1]
```

What about the initial $i_2 = x_1 - 1$ of p_2? It depends on x_1. We want to know if it is invertible modulo the already processed polynomials, i.e. p_1 or p_{01} (it is equivalent). We may use the extended Euclidean algorithm for computing a Bézout identity $u\,(x_1 - 1) + v\,p_1 = (x_1 - 1) \wedge p_1$ between this initial and p_1. We will see later that we might have used resultants.

```
> gcdex (x[1]-1, p1, x[1], 'u', 'v');
                                      1
```

The gcd is equal to 1, proving that the initial is invertible in $R/(p_{01})$. Let us have a look to the cofactors u (the inverse of the initial) and v. They are polynomials in $K(t_1)[x_1]$, since they were computed using polynomials in $K(t_1)[x_1]$.

```
> 'u' = u, 'v' = v;
                                    t[1] x[1]          1
                        u = -1 - ---------, v = ---------
                                   -1 + t[1]      -1 + t[1]
```

Therefore, if we multiply p_2 by u, the result p_{02} keeps being a polynomial in $K(t_1)[x_1, x_2]$ and the overall system keeps being triangular.

```
> p02 := collect (rem (u*p2, p01, x[1]), x[2]);
                                                        2
                           3   t[1] x[1] x[2]   t[1]  x[1]
                 p02 := x[2]  + --------------- - ---------- - t[1]
                                   -1 + t[1]      -1 + t[1]
```

These computations actually prove that the triangular set $\{p_1, p_2\}$ is a regular chain.

3.2 Definition and Characterization

Let $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ be a polynomial ring over a field K of characteristic zero. Let $A = \{p_1, \ldots, p_n\}$ be a triangular system of polynomials such that the leading variable of p_k is x_k, the leading degree of p_k is $d_k = \deg(p_k, x_k)$, and the initial of p_k, i.e. the leading coefficient of p_k with respect to x_k, is denoted i_k, for $1 \leq k \leq n$. Let h denote the product of the initials of the polynomials p_k and $\mathfrak{A}$ denote the ideal $(A) : h^\infty$ of R (the ideal generated by A, saturated by the multiplicative family generated by h) i.e.

$$\mathfrak{A} \quad = \quad \{f \in R \mid \exists\, d \geq 0,\, h^d\, f \in (A)\}$$

If f is any polynomial of R, one defines the pseudoremainder of f by A by

$$\mathsf{prem}(f, A) \quad = \quad \mathsf{prem}(\ldots \mathsf{prem}(f, p_n, x_n), \ldots, p_1, x_1)$$

and the resultant of f by A by

$$\mathsf{res}(f, A) \quad = \quad \mathsf{res}(\ldots \mathsf{res}(f, p_n, x_n), \ldots, p_1, x_1)\,.$$

See Chapter 1 for details on the pseudodivision and the resultant.

The following Proposition does not list all the properties of regular chains but it explains why this concept is important. Many different variants of triangular systems were defined and studied from 1990 to 2010. The Proposition essentially states that, if any such variant permits to recognize zero, or zero-divisors, in $R/\mathfrak{A}$, then it must be another definition of regular chains.

Definition 1 *A triangular system of R is said to be a* regular chain *if the initial i_k of p_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$ for $2 \leq k \leq n$.*

Proposition 5 *Let A be a triangular system and f be a polynomial of R. The following conditions are equivalent:*

a *A is a* regular chain*;*

b $\mathsf{prem}(f, A) = 0$ *if and only if f is zero in $R/\mathfrak{A}$;*

c $\mathsf{res}(f, A) = 0$ *if and only if f is a zero-divisor in $R/\mathfrak{A}$.*

Proposition 6 *If a triangular set A satisfies any of Conditions **a**, **b** or **c** then the ideal $\mathfrak{A}$ is necessarily proper.*

Proof If $\mathfrak{A} = R$ then every element of $R/\mathfrak{A}$ is zero and a zero-divisor. Thus Condition **a** cannot hold. Moreover, if f is any nonzero element of $K[t_1, \ldots, t_m]$ then $\mathsf{prem}(f, A) \neq 0$ and $\mathsf{res}(f, A) \neq 0$. Thus Conditions **b** and **c** cannot hold either. □

3.3 Reduction to Dimension Zero

Let $K_0 = K(t_1, \ldots, t_m)$ and $R_0 = K_0[x_1, \ldots, x_n]$ be the polynomial ring obtained by moving $t_1, \ldots, t_m$ to the base field of the polynomials. Define $\mathfrak{A}_0 = (A) : h^\infty$ in the ring R_0.

Proposition 5 is all about testing whether a given polynomial f of R is zero, or a zero-divisor in some ring S. By [9, I, 19, page 42], f is zero, or a zero-divisor if and only if it is zero, or a zero-divisor in the total quotient ring of S.

There are many different rings involved in Proposition 5. Proposition 4 plays a key role here, since it tells us that in all these rings, the nonzero elements of $K[t_1, \ldots, t_m]$ are regular. Because of this, we are allowed to study Proposition 5 in R_0 rather than in R.

By Proposition 4, all associated prime ideals of $\mathfrak{A}$ have dimension m. Therefore, all associated prime ideals of $\mathfrak{A}_0$ have dimension zero and, in $R_0/\mathfrak{A}_0$, an element is regular if and only if it is invertible.

3.4 The Algorithmic Test

Ideas seem quite simple but one needs to be careful. As a warning, the reader may want to find out where is the mistake in the following "false proposition".

False Proposition. *In the ring R_0, every triangular system is a regular chain.* **Proof** Assume A is a triangular system. The initials i_k are invertible in $R_0/\mathfrak{A}_0$ (this is definitely true since the saturation by h ensures that h belongs to none of the associated prime ideals of $\mathfrak{A}_0$). Multiplying all the initials by their inverses, one gets a triangular system A_0 which generates $\mathfrak{A}_0$, with initials all equal to 1: a regular chain. □

Being warned, let us proceed more carefully and consider a triangular system A of R_0 satisfying the regular chain condition. Then there exists polynomials u_i and v_{ij} such that (this is nothing but a formal reformulation of Section 3.1)

$$\begin{array}{lcll} u_1\, i_1 & = & 1\,, & u_1 \in K_0\,, \\ u_2\, i_2 & = & 1 + v_{21}\, p_1\,, & u_2, v_{21} \in K_0[x_1]\,, \\ u_3\, i_3 & = & 1 + v_{31}\, p_1 + v_{32}\, p_2\,, & u_3, v_{31}, v_{32} \in K_0[x_1, x_2]\,, \\ & \vdots & & \\ u_n\, i_n & = & 1 + v_{n1}\, p_1 + \cdots + v_{n,n-1}\, p_{n-1}\,, & u_n, v_{n1}, \ldots, v_{n,n-1} \in K_0[x_1, \ldots, x_{n-1}]\,. \end{array} \tag{3.1}$$

Recall $d_k = \deg(p_k, x_k)$ for $1 \leq k \leq n$ and define

$$\begin{array}{lcll} p_{01} & = & u_1\, p_1\,, & p_{01} \in K_0[x_1]\,, \\ p_{02} & = & u_2\, p_2 - v_{21}\, p_1\, x_2^{d_2}\,, & p_{02} \in K_0[x_1, x_2]\,, \\ & \vdots & & \\ p_{0n} & = & u_n\, p_n - (v_{n1}\, p_1 + \cdots + v_{n,n-1}\, p_{n-1})\, x_n^{d_n}\,, & p_{0n} \in R_0\,. \end{array} \tag{3.2}$$

For each $1 \leq k \leq n$, the polynomials p_{0k} have the same leading variable x_k and the same degree d_k in x_k as p_k; they all have initials equal to 1 (the polynomials are said to be *monic*). Denote $A_0 = \{p_{01}, \ldots, p_{0n}\}$. The ideal generated by A_0 is equal to $\mathfrak{A}_0$. The above observation is summarized in the following proposition.

Proposition 7 *Assume A is a regular chain. Then, the ideal $\mathfrak{A}_0$ admits a basis A_0 made of polynomials $p_{01}, \ldots, p_{0n}$ such that the polynomials p_{0k} have the same leading variable x_k and the same degree d_k in x_k as p_k, and have initials all equal to* 1.

In (3.1), the polynomials u_k are inverses of the initials i_k. Inverses can be computed by means of the extended Euclidean algorithm. Indeed, using the pseudo-codes given in Figures 3.1, page 30 and 3.2, page 31, the regular chain condition can easily be turned into an algorithm that decides whether a triangular system is a regular chain.

3.5 Membership Testing to the Ideal

The two next propositions are easy and do not even require A to be triangular.

Proposition 8 *Let f and be any polynomial of R and denote $g = \mathsf{prem}(f, A)$. Then*

$$\deg(g, x_k) \;<\; \deg(p_k, x_k) \quad (1 \leq k \leq n)\,. \tag{3.3}$$

Moreover, there exists a power product h_f of initials of A and polynomials $v_1, v_2, \ldots, v_n$ such that

$$h_f\, f \;=\; g + v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n\,. \tag{3.4}$$

3.5.1 $\mathbf{a} \Rightarrow \mathbf{b}$

Proposition 9 *Let f be any polynomial of R. If $\mathsf{prem}(f, A) = 0$ then f is zero in $R/\mathfrak{A}$.*

Proof By Formula (3.4) of Proposition 8. □

The following proposition is more difficult. Combined with the above one, it proves $\mathbf{a} \Rightarrow \mathbf{b}$.

Proposition 10 *Assume A is a regular chain and let f be any polynomial of R. If f is zero in $R/\mathfrak{A}$ then $\mathsf{prem}(f, A)$ is the zero polynomial.*

Proof Denote $g = \mathsf{prem}(f, A)$. Assume f is zero in $R/\mathfrak{A}$. Then g is zero in $R/\mathfrak{A}$ and in $R_0/\mathfrak{A}_0$.

There exists a short proof for readers who know Gröbner bases: in R_0, the triangular set A_0 defined in Proposition 7 is a Gröbner basis, w.r.t. the lexicographic ordering $x_1 < \cdots < x_n$, of the ideal $\mathfrak{A}_0$, since the leading monomials are disjoint. See [6, 2, 9, Proposition 4 "Buchberger's First

Criterion" and Theorem 3, page 101]. Condition (3.3) implies that g is irreducible by A_0. Then g must be zero, as a polynomial. See [6, 2, 6, Corollary 2, page 80].

Here is another proof, which avoids the Gröbner bases theory. We assume g is not the zero polynomial and seek a contradiction. Since $g \in \mathfrak{A}_0$, there exists a formula

$$g = \underbrace{v_1\, p_{01} + v_2\, p_{02} + \cdots + v_k\, p_{0k}}_{\mathscr{F}} .$$

To any such formula $\mathscr{F}$, one may associate an index $j(\mathscr{F})$ defined as the highest index j such that x_j occurs in some v_i or some p_{0i}. This index is well defined since g is not zero. And we must have $j \geq k$. Among all possible formulas $\mathscr{F}$, let us consider one, such that $j(\mathscr{F})$ is minimal. Let us denote $j = j(\mathscr{F})$ for short, $d = \deg(p_{0j}, x_j)$ and $p_{0j} = x_j^d + q_j$. In the polynomials v_i of $\mathscr{F}$, let us substitute every occurence of x_j^d by $p_{0j} - q_j$ yielding another formula

$$g = \underbrace{w_1\, p_{01} + w_2\, p_{02} + \cdots + w_\ell\, p_{0\ell}}_{\mathscr{F}'} \quad (w_\ell \neq 0)$$

such that $\deg(w_i, x_j) < d$ for $1 \leq i \leq \ell$. We must have $\ell = j$ since $j(\mathscr{F}) = j(\mathscr{F}')$. Since $\deg(w_i, x_j) < d$ and $\deg(p_{0i}, x_j) = 0$ for $i < j$ and $w_j \neq 0$, we must have $\deg(g, x_j) \geq d$. This contradiction with Condition (3.3) proves that g must be the zero polynomial. □

3.5.2 b ⇒ a

Example. The following triangular set A is not a regular chain since the initial $t_1\, x_1 - 1$ of p_2 has a non-unit gcd with p_1. It is thus not regular in $R/(p_1) : i_1^\infty$.

```
> p1 := t[1]*x[1]^2 - x[1];
                                        2
                          p1 := t[1] x[1]  - x[1]

> p2 := (t[1]*x[1]-1)*x[2]^3 - x[1]*x[2] + t[1];
                                            3
                 p2 := (t[1] x[1] - 1) x[2]  - x[1] x[2] + t[1]

> gcdex (t[1]*x[1]-1, p1, x[1]);
                                      1
                                x[1] - ----
                                     t[1]
```

Since ideal $\mathfrak{A}$ is saturated by all the initials of the triangular set, it contains the quotient x_1 of p_1 by $t_1\, x_1 - 1$, viewed as polynomials in x_1. However, this quotient is not reduced to zero by A because its degree in x_1 is strictly less than the one of p_1. In summary: if **a** does not hold then **b** may not hold either.

Proposition 11 proves **b** ⇒ **a** by the very same argument, formulated in a more general way. The ideal $\mathfrak{A}$ is assumed to be proper for simplicity. According to Proposition 6, this is not a restriction for proving **b** ⇒ **a**.

Proposition 11 *Let A be triangular set of R such that $\mathfrak{A}$ is proper, and $1 \leq k < n$ be an index such that the regular chain condition is satisfied up to k and i_{k+1} is not regular in $R/(p_1, \ldots, p_k) : (i_1 \cdots i_k)^\infty$. Then there exists some $f \in \mathfrak{A}$ such that* $\mathsf{prem}(f, A) \neq 0$.

Proof Denote $\mathfrak{A}_k = (p_1, \ldots, p_k) : (i_1 \cdots i_k)^\infty$. Let $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be an irredundant primary representation of $\mathfrak{A}_k$ and $\mathfrak{p}_\ell = \sqrt{\mathfrak{q}_\ell}$ be its associated prime ideals. Since i_{k+1} is not regular in $R/\mathfrak{A}_k$, there exists an index $1 \leq j \leq r$ such that $i_{k+1} \in \mathfrak{p}_1, \ldots, \mathfrak{p}_j$ and $i_{k+1} \notin \mathfrak{p}_{j+1}, \ldots, \mathfrak{p}_r$ Denote $\mathfrak{B}_k = \mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_r$ (the intersection is not empty for $\mathfrak{A}$ is proper). We have $\mathfrak{B}_k = \mathfrak{A}_k : i_{k+1}^\infty$ by [9, IV, 10, Theorem 17, page 225]. Denote $R_k = K[t_1, \ldots, t_m, x_1, \ldots, x_k]$. By Proposition 4, there exists some nonzero polynomial $f \in \mathfrak{B}_k \cap R_k$. Choose $f \notin \mathfrak{A}_k$. Since $f \in R_k$ we have $\mathsf{prem}(f, A_k) = \mathsf{prem}(f, A)$. Since $f \notin \mathfrak{A}_k$ we have $\mathsf{prem}(f, A_k) \neq 0$ (Proposition 9). Since $f \in \mathfrak{B}_k \subset \mathfrak{A}$, the proposition is proved. □

3.6 Regularity Testing modulo the Ideal

In the examples above, we have tested the regularity of the initial of p_2 modulo the ideal defined by p_1 by means of a gcd computation, through the Euclidean algorithm. The gcd and the resultant of two polynomials are quite related. From a theoretical point of view, the resultant has the advantage of being a determinant: the determinant of the Sylvester matrix defined by the polynomials under consideration. As such, it is defined for polynomials over general rings.

Example. The following computations, combined to the fact that a zero resultant indicates a common factor (Theorem 1, page 9), prove $x_1 - 1$ is regular in $R/(p_1) : i_1^\infty$.

```
> with (LinearAlgebra):
> p1 := t[1]*x[1]^2 - x[1];
                                        2
                          p1 := t[1] x[1]  - x[1]

> S := SylvesterMatrix (x[1]-1,p1,x[1]);
                                [ 1      -1     0]
                                [                ]
                           S := [ 0       1    -1]
                                [                ]
                                [t[1]    -1     0]

> Determinant (S);
                                  -1 + t[1]
```

The following computations prove that $t_1\, x_1 - 1$ is a zero-divisor.

```
> S := SylvesterMatrix (t[1]*x[1]-1,p1,x[1]);
                               [t[1]     -1      0]
                               [                 ]
                          S := [ 0      t[1]    -1]
                               [                 ]
                               [t[1]     -1      0]

> Determinant (S);
                                        0
```

Proposition 12 *Let f be a polynomial and A be a triangular set of R. Then there exists polynomials $u, v_1, v_2, \ldots, v_n$ of R such that*

$$u\, f \quad = \quad \mathsf{res}(f, A) + v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n \tag{3.5}$$

Proof Apply n times the fact that the resultant of two polynomials is in the ideal generated by these polynomials (Theorem 3, page 11). □

3.6.1 c ⇒ a

In this section, the ideal $\mathfrak{A}$ is assumed to be proper, for simplicity. According to Proposition 6, this is not a restriction for proving **c** ⇒ **a**.

Proposition 13 *Let f be a polynomial and A be a triangular set of R such that $\mathfrak{A}$ is a proper ideal. If $\mathsf{res}(f, A) \neq 0$ then f is regular in $R/\mathfrak{A}$.*

Proof Take Formula (3.5) in $R/\mathfrak{A}$. We have $u\, f = \mathsf{res}(f, A)$. Since $\mathsf{res}(f, A) \in K[t_1, \ldots, t_m]$, by Proposition 4, it is a regular element of $R/\mathfrak{A}$, thus so is f. □

Combined with Proposition 13, the following Proposition 14 proves that **c** ⇒ **a**.

Proposition 14 *Let A be a triangular set of R such that $\mathfrak{A}$ is a proper ideal. Assume that, for any f regular in $R/\mathfrak{A}$, we have $\mathsf{res}(f, A) \neq 0$. Then A is a regular chain.*

Proof Let $1 \leq k \leq n$ be an index. The initial i_k of p_k is regular in $R/\mathfrak{A}$, since $\mathfrak{A}$ is saturated by the product of its initials. See [9, IV, 6, Corollary 3 to Theorem 11, page 214; and 10, Theorem 17, page 225]. Thus by assumption, $\mathsf{res}(i_k, A) \neq 0$. Let us decompose $\mathsf{res}(i_k, A) = \mathsf{res}(r_k, \{p_1, \ldots, p_{k-1}\})$ where $r_k = \mathsf{res}(i_k, \{p_k, \ldots, p_n\})$. Then $\mathsf{res}(r_k, \{p_1, \ldots, p_{k-1}\}) \neq 0$. Thus r_k is regular in $R/(p_1, \ldots, p_{k-1}){:}(i_1 \cdots i_{k-1})^\infty$ by Proposition 13. Since i_k does not depend on $x_k, \ldots, x_n$, the polynomial r_k is a power of i_k. Thus i_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. Thus A is a regular chain. □

3.6.2 a ⇒ c

In the sequel, A is a regular chain. We thus prefer to work with the monic triangular set A_0 of R_0 as defined in Proposition 7. The following proposition provides a theoretical justification.

Proposition 15 *Let f be a polynomial, A be a regular chain of R, and A_0 be the monic triangular set of R_0, defined in Proposition 7. Then there exists polynomials $u, v_1, v_2, \ldots, v_n$ of R_0 such that*

$$u\, f \quad = \quad \mathsf{res}(f, A) + v_1\, p_{01} + v_2\, p_{02} + \cdots + v_n\, p_{0n} \tag{3.6}$$

Proof Solving system (3.2) w.r.t. $p_1, p_2, \ldots, p_n$ and replacing them by their values in (3.5) provides the sought formula. □

Combined with Proposition 16, Proposition 13 proves **a** ⇒ **c**.

Proposition 16 *Let f be a polynomial and A be a regular chain of R. If $\mathsf{res}(f, A) = 0$ then f is a zero-divisor in $R/\mathfrak{A}$.*

Proof The Proposition holds if f is zero. Assume f is nonzero.

Let A_0 and R_0 and $\mathfrak{A}_0$ as in Proposition 7. We assume $\mathsf{res}(f, A_0) = 0$ and prove that f is a zero-divisor in $R_0/\mathfrak{A}_0$, i.e. that there exists an associated prime ideal of $\mathfrak{A}_0$ which contains f. See [9, IV, 6, Corollary 3 to Theorem 11, page 214].

The proof is by induction on n.

Basis: the case $n = 1$. Then $\mathsf{res}(f, A_0) = \mathsf{res}(f, p_{01}, x_1)$. If it is zero then f and p_{01} have a common factor (Theorem 1, page 11). This common factor provides at least one associated prime ideal of $\mathfrak{A}_0$ containing f.

General case: $n > 1$. Denote $R'_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_{n-1}]$, $A'_0 = \{p_{01}, \ldots, p_{0,n-1}\}$, $\mathfrak{A}'_0$ the ideal (A'_0) in R'_0 and $g = \mathsf{rem}(f, p_{0n}, x)$. By Theorem 2 we have $\mathsf{res}(g, A_0) = \pm\,\mathsf{res}(f, A_0)$. Since $\mathsf{res}(f, A_0) = 0$, we have $\mathsf{res}(g, A_0) = 0$. Decompose $\mathsf{res}(g, A_0) = \mathsf{res}(r, A'_0)$ where $r = \mathsf{res}(g, p_{0n}, x_n)$. We have $\mathsf{res}(r, A'_0) = 0$. The induction hypothesis applies: there exists an associated prime ideal $\mathfrak{p}'$ of $\mathfrak{A}'_0$ which contains r. Denote φ the canonical ring homomorphism $R'_0 \to R'_0/\mathfrak{p}'$, so that $\varphi(r) = 0$. Since $\deg(g, x_n) < \deg(p_{0n}, x_n)$ and p_{0n} is monic, Theorem 4 applies and we have $\mathsf{res}(\varphi(g), \varphi(p_{0n}), x_n) = 0$. The two polynomials $\varphi(g)$ and $\varphi(p_{0n})$ have coefficients in $R'_0/\mathfrak{p}'$, which is a domain. Apply Theorem 1: the polynomials $\varphi(g)$ and $\varphi(p_{0n})$ have a common factor. Thus $\varphi(f)$ and $\varphi(p_{0n})$ have a common factor. This factor defines at least one prime ideal $\mathfrak{p}$ of R_0 such that $f \in \mathfrak{p}$, $\mathfrak{A}_0 \subset \mathfrak{p}$ and $\mathfrak{p}' = \mathfrak{p} \cap R'_0$. Since $\dim \mathfrak{A}_0 = 0$, the prime ideal $\mathfrak{p}$ is an associated prime of $\mathfrak{A}_0$. Thus f is a zero-divisor in $R_0/\mathfrak{A}_0$. □

3.7 Concluding Remarks

The concept of a *regular chain* was introduced in [7].

It was much developed in the mid 1990's in the team of Daniel Lazard [8, 1]. Since then, huge developments (algebra and computer science), undertaken by the group of Marc Moreno Maza at ORCCA, led to the MAPLE package `RegularChains`[1].

This chapter owes a lot to [5], [3] and [4].

Bibliography

[1] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza. On the Theories of Triangular Sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

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

[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, François Lemaire, and Alexandre Sedoglavic. On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains. In *Proceedings of Computer Algebra in Scientific Computing, LNCS 6885*, pages 61–72, Kassel, Germany, 2011. `http://hal.archives-ouvertes.fr/hal-00599440`.

[5] Changbo Chen, François Lemaire, Marc Moreno Maza, and Wei Pan. Comprehensive Triangular Decompositions. In *Proceedings of CASC'07*, pages 73–101, 2007.

[6] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms. An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer Verlag, New York, 2nd edition, 1996.

[1] The first version of `RegularChains` was written by François Lemaire.

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

[8] 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.

[9] 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.

```
function AlgebraicInverseNonZero (f, A)
Parameters
  A = {p_1, ..., p_n} is a regular chain in K_0[x_1, ..., x_n], and only involves monic polynomials
  f is a polynomial in K_0[x_1, ..., x_n], which does not lie in the ideal (A)
Result
  an inverse of f in K_0[x_1, ..., x_n]/(A) or the exception "inversion of a zero-divisor"
begin
  if f ∈ K_0 then
the polynomial f, which does not belong to (A), cannot be zero
    return 1/f
  else
    let x_k be the leading variable of f
    u := ExtendedEuclideanAlgorithm (f, p_k, x_k, A)
one has u_1 f + u_2 p_k = u_3  mod (A)
    if u_3 = 1 then
one has u_1 f = 1  mod (A)
      return u_1
    else
the polynomial u_3 divides p_k and is different from p_k since f does not lie in A
      raise "inversion of a zero-divisor": u_3
    fi
  fi
end
```

Figure 3.1: The `AlgebraicInverseNonZero` function.

function `ExtendedEuclideanAlgorithm` (f, g, x_k, A)
Parameters
  $A = \{p_1, \ldots, p_n\}$ *is a regular chain in* $K_0[x_1, \ldots, x_n]$ *and only involves monic polynomials*
  f, g *are polynomials in* $K_0[x_1, \ldots, x_n]$ *; their leading coeff. w.r.t.* x_k *do not lie in the ideal* (A)
Result
  a vector $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ *of polynomials in* $K_0[x_1, \ldots, x_n]$*, such that, in* $K_0[x_1, \ldots, x_n]/(A)$*,*
    the relationship $\mathbf{u}_1 f + \mathbf{u}_2 g = \mathbf{u}_3$ *holds,*
    the polynomial $\mathbf{u}_3$ *is a common divisor of* f *and* g*,*
    the leading coefficient of $\mathbf{u}_3$ *w.r.t.* x_k *is* 1
  or the exception "inversion of a zero-divisor"
begin
  $\mathbf{u} := (1, 0, f)$
  $\mathbf{v} := (0, 1, g)$
the property $\mathbf{u}_1 f + \mathbf{u}_2 g = \mathbf{u}_3 \mod (A)$ *is a loop invariant*
the set of common divisors of $\mathbf{u}_3$ *and* $\mathbf{v}_3$ *modulo* (A) *is another loop invariant*
  while $\mathbf{v}_3 \neq 0$ do
    let $\imath$ be the leading coefficient of $\mathbf{v}_3$ w.r.t. x_k
    $\bar{\imath} :=$ `AlgebraicInverseNonZero` $(\imath, A)$
compute the remainder componentwise
    $\mathbf{v} := \mathsf{rem}(\bar{\imath}\,\mathbf{v}, A)$
the leading coefficient of $\mathbf{v}_3$ *w.r.t.* x_k *is now* 1
    $q := \mathsf{quo}(\mathbf{u}_3, \mathbf{v}_3, x_k)$
    $\mathbf{t} := \mathbf{v}$
    $\mathbf{v} := \mathsf{rem}(\mathbf{u} - q\,\mathbf{v}, \{p_1, \ldots, p_{k-1}\})$
if $\mathbf{v}_3$ *is nonzero then, its leading coefficient w.r.t.* x_k *does not lie in* (A)
    $\mathbf{u} := \mathbf{t}$
  od
the polynomial $\mathbf{u}_3$ *is a common divisor of* $\mathbf{u}_3$ *and* 0*, hence a common divisor of* f *and* g
  return $\mathbf{u}$
end

Figure 3.2: The `ExtendedEuclideanAlgorithm` function.

Chapter 4

Lazard's Lemma

This chapter provides a complete proof of Proposition 17 (Lazard's Lemma). It relies on Chapter 2 only.

4.1 Informal Introduction

Let us load the `DifferentialAlgebra` MAPLE package and consider again the introductory example of Chapter 2.

```
> with (DifferentialAlgebra):
> R := DifferentialRing(derivations = [x,y], blocks = [[v,u]]);
                              R := differential_ring
```

Let us assign to `p1`, `p2`, `p3` the three differential polynomials which were assigned to `sys` in Chapter 2.

```
> p1 := u[x]^2-4*u;
                                        2
                                p1 := u[x]  - 4 u

> p2 := u[x,y]*v[y]-u+1;
                            p2 := u[x, y] v[y] - u + 1

> p3 := v[x,x]-u[x];
                                p3 := v[x, x] - u[x]
```

Let us compute again a regular differential chain from these three differential polynomials (which are three generators of some differential ideal $\mathfrak{A}$) and display the chain elements.

```
> ideal := RosenfeldGroebner([p1,p2,p3],R);
                      ideal := [regular_differential_chain]

> ideal := ideal[1]:
> Equations(ideal, solved);
                                -u[x] u[y] u + u[x] u[y]      2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u,
                                            u
```

```
        2
    u[y]  = 2 u]
```

We notice that, if we apply an elimination algorithm such as `RosenfeldGroebner` over *powers* of the three generators of $\mathfrak{A}$, we obtain the very same regular differential chain.

```
> jdeal := RosenfeldGroebner([p1^2,p2^3,p3^2],R);
                      jdeal := [regular_differential_chain]

> jdeal := jdeal[1]:
> Equations (jdeal,solved);
                                -u[x] u[y] u + u[x] u[y]      2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u,
                                          u

        2
    u[y]  = 2 u]
```

I stated a similar[1] observation in my PhD memoir (see [1, Section 5.2]). Daniel Lazard, who was one my PhD referees, wrote me back two weeks before my PhD defense, that he thought that the ideals defined by the output of the algorithm were radical ideals. A first (incomplete) proof of this remark was published in [2, Lemma 2]. It is today often called Lazard's Lemma.

4.2 Why are Radical Ideals Important

An ideal is said to be *radical* if it is equal to its radical [6, III, 7, Definition 2, page 147]. A radical ideal of a ring S is thus an ideal $\mathfrak{B}$ such that, for any $f \in S$, we have $f \in \mathfrak{B}$ whenever some power f^d of f belongs to $\mathfrak{B}$.

Radical ideals are important because of the Hilbert Nullstellensatz [6, VII, 3, Theorem 14, page 164], recalled below.

Theorem 9 *(The Hilbert Nullstellensatz)*

Let K be a field. If $f_1, f_2, \ldots, f_q$ are polynomials in $K[x_1, x_2, \ldots, x_n]$ and if f vanishes at every common zero of $f_1, f_2, \ldots, f_q$ (in an algebraically closed extension $\bar{K}$ of K), then there exists an exponent ρ and polynomials $a_1, a_2, \ldots, a_n$ in $K[x_1, x_2, \ldots, x_n]$ such that

$$f^\rho \;=\; a_1\, f_1 + a_2\, f_2 + \cdots + a_n\, f_n\,. \tag{4.1}$$

Formula (4.1) just expresses that f belongs to the radical of the ideal $\mathfrak{B}$ generated by $f_1, f_2, \ldots, f_q$. The converse implication of the theorem is obvious: if $f \in \sqrt{\mathfrak{B}}$ then f vanishes at every common zero of $f_1, f_2, \ldots, f_q$ (in any field extension of K, not necessarily algebraically closed).

[1] In my PhD memoir, the version of `RosenfeldGroebner` was much simpler than the one implemented in the MAPLE package. In particular, the output was made of Gröbner bases rather than regular differential chains, which were not yet defined in 1994. The observation still holds, however.

4.3 The Chinese Remainder Theorem

By consistency w.r.t. the rest of these lecture notes, we would like to rely on Zariski and Samuel *Commutative Algebra*. Their formulation of the Chinese Remainder Theorem, through direct sums, may look unusual for many readers. We thus feel the need of summarizing their approach. Let us start with a small example and consider the polynomial

$$p = \underbrace{(x^2-2)}_{p_1}\underbrace{(x-1)}_{p_2}$$

in the polynomial ring $K[x]$. The gcd of the two irreducible factors p_1 and p_2 is 1. Indeed, we even have, by the extended Euclidean algorithm, a Bézout identity (as one says in France) between the two factors:

$$\begin{aligned} u\,p_1 + v\,p_2 &= 1\,, \\ u &= -1\,, \\ v &= x+1\,, \end{aligned}$$

which permits to solve the following problem: given any pair of polynomials f_1, f_2, find a polynomial f such that:

$$\begin{aligned} f &= f_1 \mod (x^2-2)\,, \\ f &= f_2 \mod (x-1)\,. \end{aligned}$$

Multiply the first equation by $v\,p_2$, the second one by $u\,p_1$, add termwise and use the Bézout identity:

$$f = v\,p_2\,f_1 + u\,p_1\,f_2 \mod (p)\,. \tag{4.2}$$

It is not difficult to strengthen the above statements and end up with the following isomorphim of rings, which is the classical formulation of the Chinese Remainder Theorem:

$$K[x]/(p) = K[x]/(p_1) \times K[x]/(p_2)\,.$$

The Cartesian product on the right hand-side is endowed with a ring structure: ring operations are performed componentwise.

There exists another way to present the above construct. It is the one adopted in [6]. Let us denote $S = K[x]/(p)$ and $\mathfrak{B}_i$ the ideal generated by p_i in S for $i = 1, 2$. The fact that the gcd of the two polynomials is 1 implies that the ideals $\mathfrak{B}_i$ are comaximal, i.e. that their sum is equal to the whole ring [6, III, 13, page 176]. The intersection of two comaximal ideals is equal to their product [6, III, 13, Theorem 31, page 177]. In S, the ideal (p) becomes (0). Taking all these remarks into account, we have

$$\begin{aligned} (0) &= \mathfrak{B}_1 \cap \mathfrak{B}_2\,, \\ S &= \mathfrak{B}_1 + \mathfrak{B}_2\,. \end{aligned}$$

The above conditions actually imply that the sum is direct, which means that every element f of S has a unique representation as a sum of one element of $\mathfrak{B}_1$ and one element of $\mathfrak{B}_2$ [6, III, 12, page 164]. Back to our example, this decomposition is given by (4.2):

$$f = \underbrace{v\,p_2\,f_1}_{\mathfrak{B}_2} + \underbrace{u\,p_1\,f_2}_{\mathfrak{B}_1}\,.$$

The following more general definition comes from [6, III, 13, Definition 1, page 174]. Recall that an ideal of a ring S is a subring of S. A ring S is said to be a *direct sum* of the ideals $S_1, S_2, \ldots, S_r$ if $S = S_1 + S_2 + \cdots + S_r$ and $S_i \cap \sum_{j \neq i} S_j = (0)$ for $1 \leq i \leq r$. One writes $S = S_1 \oplus S_2 \oplus \cdots \oplus S_r$.

When this holds, $S_i\, S_j = (0)$ for $i \neq j$. This comes from the fact that $S_i\, S_j \subset S_i \cap S_j \subset S_i \cap \sum_{j \neq i} S_j$, which is equal to (0) by definition of direct sums.

The following theorem is a shortened version of [6, III, 13, Theorem 32, page 178]. It is a formulation of the Chinese Remainder Theorem.

Theorem 10 *Let S be a ring with identity. Let $\mathfrak{B}_1, \ldots, \mathfrak{B}_r$ be ideals such that $(0) = \cap_i \mathfrak{B}_i$ and $\mathfrak{B}_i + \mathfrak{B}_j = S$ for $i \neq j$. If we define $S_i = \cap_{j \neq i} \mathfrak{B}_j$ for $1 \leq i \leq n$, then $S = S_1 \oplus \cdots \oplus S_r$ with $S_i \simeq S/\mathfrak{B}_i$.*

Theorem 11 is an incomplete formulation of [6, III, 13, Theorem 30, page 175] which essentially states that in a ring which is a direct sum, addition and multiplication are performed summandwise.

Theorem 11 *Let S be a ring with identity. Let $S_1, S_2, \ldots, S_r$ be subrings such that $S = S_1 + S_2 + \cdots + S_r$ and $S_i\, S_j = (0)$ for $i \neq j$. Then each S_i is an ideal and the sum is direct. If $a_i, b_i \in S_i$ for $1 \leq i \leq r$, then $(a_1 + a_2 + \cdots + a_r) + (b_1 + b_2 + \cdots + b_r) = (a_1 + b_1) + \cdots + (a_r + b_r)$ and $(a_1 + a_2 + \cdots + a_r)\,(b_1 + b_2 + \cdots + b_r) = a_1\, b_1 + \cdots + a_r\, b_r$. If $\mathfrak{B}$ is an ideal in S, there exists a decomposition $\mathfrak{B} = \mathfrak{B}_1 \oplus \cdots \oplus \mathfrak{B}_r$, where $\mathfrak{B}_i$ is an ideal in S_i; this decomposition is unique. The residue class ring $S/\mathfrak{B} \simeq S/\mathfrak{B}_1 \oplus \cdots \oplus S/\mathfrak{B}_r$.*

Notice that direct sums are associative i.e. that if S is a direct sum of S_i and each S_i is a direct sum of S_{ij} then S is the direct sum of the S_{ij}, taken together [6, III, 12, page 164]. Notice also that if $S = S_1 \oplus \cdots \oplus S_r$ then $S[x] = S_1[x] \oplus \cdots \oplus S_r[x]$.

4.4 The Result

The ingredients of the proof of Lazard's Lemma are then the following ones:

1. An ideal $\mathfrak{B}$ of a ring S is radical if and only if the total quotient ring of $S/\mathfrak{B}$ does not contain any nilpotent element.

2. A direct sum of fields does not contain any nilpotent element (because fields have no nilpotent elements and, in direct sums, operations are performed summandwise).

3. If an ideal $\mathfrak{B}$ is an intersection of maximal ideals of a ring S then $S/\mathfrak{B}$ is a direct sum of fields (by Theorem 10, the fact that maximal ideals are pairwise comaximal, and that the residue class ring by a maximal ideal is a field [6, III, 8, Theorem 10, page 150]).

4. If p is a polynomial in $K[x]$ and $s = \partial p/\partial x$ is its separant, then the ideal $(p) : s^\infty$ is generated by the product of the irreducible simple factors of p. It is the intersection of the maximal ideals generated by each of these factors.

5. If $S = S_1 \oplus \cdots \oplus S_r$ and p is a polynomial in $S[x]$, so that $p = p_1 + \cdots + p_r$, then the separant of p can be taken summandwise i.e. $\partial p/\partial x = \partial p_1/\partial x + \cdots + \partial p_r/\partial x$.

Actually, all the idea of the proof consists in applying the well-known property 4 above in a context where it is not supposed to apply. Let us enter details. The ring $K[x]$ is unique factorization domain. Consider a polynomial $p = f^d\, g$ with f irreducible and $f \wedge g = 1$. Then the separant of p is $s = p' = d\, f^{d-1}\, f'\, g + f^d\, g'$ and we see that $f^{d-1} \mid s$ i.e. if f is not simple then f is a common factor of p and s and will be factored out by the saturation. In order to show that the saturation does not factor out simple factors, we need to show that f^d does not divide the separant, i.e. that f does not divide $f'\, g$. In a unique factorization domain, Gauss Lemma applies: $f \mid f'\, g$ and $f \mid f\, f'$ thus f divides their gcd $(f'\, g \wedge f\, f') = (f \wedge g)\, f' = f'$. In the case of Lazard's Lemma, the polynomial rings involve zero-divisors. They cannot be unique factorization domains and Gauss Lemma is not supposed to apply. However, they are direct sums of unique factorization domains ...

Proposition 17 *(Lazard's Lemma)*

Let $A = \{p_1, \ldots, p_n\}$ be a triangular system of $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$, such that x_i is the leading variable of p_i for $1 \leq i \leq n$. Let h denote the product of the separants of A and $\mathfrak{A} = (A) : h^\infty$. Then $\mathfrak{A}$ is radical. Moreover, if $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{A}$ then $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$.

Proof The last sentence of the Proposition is a corollary to Proposition 4. We thus only need to prove that $\mathfrak{A}$ is radical.

Denote $\mathfrak{A}_0$ the ideal $(A) : h^\infty$ in the ring $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. By Proposition 4, the rings R_0 and R have the same total quotient ring. We thus only need to prove that $\mathfrak{A}_0$ is radical.

We prove by induction on n that $R_0/\mathfrak{A}_0$ is a direct sum of fields. This ring can be constructed incrementally as S_n defined by:

$$S_0 = K(t_1, \ldots, t_m)\,, \quad S_i = S_{i-1}[x_i]/(p_i) : s_i^\infty\,,$$

where $s_i = \partial p_i / \partial x_i$ is the separant of p_i.

The basis $n = 0$ is trivial.

Assume S_{n-1} is a direct sum of fields $K_1 \oplus \cdots \oplus K_r$. Then S_n is isomorphic to the direct sum $(1 \leq j \leq r)$ of the rings $K_j[x_n]/(p_n) : s_n^\infty$.

Thus, in $K_j[x_n]$, the ideal $(p_n) : s_n^\infty$ is generated by the product of the irreducible simple factors of p_n. It is thus the intersection of the maximal ideals $\mathfrak{m}_\ell$ generated by these factors. According to the Chinese Remainder Theorem, $K_j[x_n]/(p_n) : s_n^\infty$ is isomorphic to the direct sum of the fields $K_j[x_n]/\mathfrak{m}_\ell$. Since direct sums are associative the ring S_n is a direct sum of fields. □

4.5 Concluding Remarks

The sketch of proof of Proposition 17 is the one of Daniel Lazard with two differences: 1) the original version was formulated using product of fields instead of direct sums of fields (I have switched to direct sums because it is the presentation of [6] but the two formulations are completely equivalent); 2) the original proof was incomplete because it implicitly assumed that the nonzero elements of $K[t_1, \ldots, t_m]$ are nonzero divisors (the gap is filled by Proposition 4).

The first complete proof of Proposition 17 is due to Sally Morrison [3, 4].

Proposition 17 is formulated for non-differential ideals. Combined to Rosenfeld's Lemma [5, Lemma], it has important consequences for differential ideals.

Bibliography

[1] François Boulier. *Étude et implantation de quelques algorithmes en algèbre différentielle.* PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, 1994. `http://tel.archives-ouvertes.fr/tel-00137866`.

[2] 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`.

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

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

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

[6] 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.

Chapter 5

Rosenfeld's Lemma

Regular differential chains are particular cases of triangular sets of differential polynomials which satisfy Rosenfeld's Lemma. This chapter aims at proving Proposition 22 (Rosenfeld's Lemma).

5.1 Informal Introduction

Rosenfeld's Lemma is an analogue, in differential algebra, of the Theorem of the Gröbner bases theory which states that, when all S-polynomials are reduced to zero, we have a Gröbner basis. It is interesting to notice that Rosenfeld's Lemma is earlier than the Gröbner bases theory (1959 vs 1965) and contains, up to some encoding, the Gröbner basis Theorem (see concluding remarks).

It is also earlier than the regular chains theory, which was developed in the 1990's. However, the ideals it deals with are saturated ideals. This cannot have been motivated by the issues and results studied in the three first chapters of these notes. Here is a part (probably) of an explanation.

Let $p_1 \in K[x_1]$ and $p_2 = s_2\, x_2 + q_2$ with $s_2, q_2 \in K[x_1]$ be two polynomials. Assume $f \in (p_1, p_2) \cap K[x_1]$. Then $s_2\, f \in (p_1)$ (see below) and we see a saturated ideal naturally arising since $f \in (p_1) : s_2^\infty$. Why do we have $s_2\, f \in (p_1)$? For an informal introduction, we may just consider an example. Since $f \in (p_1, p_2)$, there exists a formula (say)

$$f \;=\; (2\, x_1 + x_2)\, p_1 + x_1^2\, p_2\,.$$

The x_2 occuring in the first factor bothers us. Let us rewrite it using p_2. Precisely, let us perform the substitution

$$x_2 \;=\; \frac{p_2 - q_2}{s_2}.$$

We obtain a formula

$$f \;=\; \left(2\, x_1 + \frac{p_2 - q_2}{s_2}\right) p_1 + x_1^2\, p_2$$

that yields another formula, by clearing denominators:

$$s_2\, f \;=\; (2\, x_1\, s_2 + p_2 - q_2)\, p_1 + x_1^2\, s_2\, p_2.$$

Let us arrange it and collect terms rather w.r.t. p_2 than w.r.t. p_1. We obtain

$$s_2\, f \;=\; (2\, x_1\, s_2 - q_2)\, p_1 + \underbrace{(x_1^2\, s_2 + p_1)}_{=0}\, p_2.$$

The indeterminate x_2 does not occur in the left hand-side nor in the first summand of the right hand-side. Therefore, the factor in front of p_2 must be zero.

In differential algebra, differential polynomials such as p_2 naturally occur: all proper derivatives of differential polynomials have this shape. In this context, the indeterminate x_2 is a leading derivative and s is a separant.

In the ordinary differential case, the above argument is sufficient to prove Rosenfeld's Lemma. This is actually done by Ritt in [4, II, 12, page 30].

In the case of partial derivatives, the above process raises a specific difficulty, suggested (rather than illustrated) by the following example. Consider the differential system

$$\begin{aligned} u_x &= v\,, \\ u_y &= 0\,, \end{aligned}$$

and assume leading derivatives occur on the left hand-sides of equations. Differentiate the first equation w.r.t. y, the second w.r.t. x and subtract: the differential polynomial v_y belongs to the differential ideal generated by the two differential polynomials. However, it would not be reduced to zero by them (we will make this statement more precise below). This situation is very close to the one encountered in the Gröbner bases theory. It is solved by Rosenfeld's Lemma.

5.2 Basic Elements of Differential Algebra

Let U be a finite set of *differential indeterminates* u_k and $\{\delta_1, \ldots, \delta_m\}$ be a set of *derivations* i.e. unary operations which obey the following rules

$$\delta(a+b) = \delta(a) + \delta(b)\,, \quad \delta(a\,b) = \delta(a)\,b + a\,\delta(b)$$

and which commute pairwise i.e. such that

$$\delta_i\,\delta_j\,a = \delta_j\,\delta_i\,a\,.$$

Derivations generate a commutative multiplicative monoid Θ of derivation operators $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$. Any derivation operator whose *order* $a_1 + \cdots + a_m$ is different from zero is said to be *proper*. The monoid Θ acts on the set of differential indeterminates, giving the *derivatives* $\theta\, u$. The infinite set of derivatives is naturally denoted $\Theta\, U$.

Differential polynomials are nothing but polynomials in $K[\Theta\, U]$. Differential polynomials can be differentiated, which means that they belong to an algebraic structure which is a ring endowed with derivations. Such rings are called *differential rings*. The ground field K of differential polynomials is a *differential field*. Using Ritt's notation, the differential polynomial ring is denoted $R = K\{U\}$.

Example. First one defines a differential polynomial ring with two derivations $\delta_1 = \delta_x$, $\delta_2 = \delta_y$ and two differential indeterminates v and u.

```
> with (DifferentialAlgebra):
> with (Tools):
> R := DifferentialRing(derivations = [x,y], blocks = [[v,u]]);
                              R := differential_ring
```

The three variables `p[1]`, `p[2]` and `p[3]` are assigned three differential polynomials. Derivation operators occur as indices. For instance, `u[x,y]` stands for $\theta\, u$ with $\theta = \delta_x\, \delta_y$.

```
> p[1],p[2],p[3] := u[x]^2-4*u, u[x,y]*v[y]-u+1, v[x,x]-u[x];
                                 2
     p[1], p[2], p[3] := u[x]  - 4 u, u[x, y] v[y] - u + 1, v[x, x] - u[x]
```

Differential algebra is an abstract theory. However, it is often helpful to interpret abstract derivations as derivations, in the usual sense, w.r.t. some independent variables x and y and differential indeterminates as functions $u(x, y)$ and $v(x, y)$ of these two variables. The following command interprets `p[2]` as an equation with partial derivatives.

```
> NormalForm (p[2], notation=diff, R);
                  /  2          \
                  | d           | /d         \
                  |----- u(x, y)| |-- v(x, y)| - u(x, y) + 1
                  \dy dx        / \dy        /
```

Derivations act on differential polynomials. Here is $\delta_x\, p_2$.

```
> Differentiate (p[2], x, R);
                   u[x, x, y] v[y] + v[x, y] u[x, y] - u[x]
```

Regular differential chains are particular cases of regular chains i.e. of triangular systems. In order to generalize this notion of triangularity to the differential context, we need to be able to associate a *leading derivative*, denoted $\mathrm{ld}\, p$, to any differential polynomial p (not in K). This is classically achieved by fixing a total ordering over the set of derivatives $\Theta\, U$ and defining the *leading derivative* of p as the highest derivative occuring in p, w.r.t. the ordering. The following definition of leading derivatives has the advantage to hold for objects more complicated than polynomials, such as rational fractions of differential polynomials:

$$\mathrm{ld}\, p \;=\; \max_{v \in \Theta U} v \mid \frac{\partial p}{\partial v} \neq 0 \cdot$$

Total orderings on $\Theta\, U$ satisfying the two following conditions are called *rankings*. See [3, I, 8, page 75].

1. $u \leq \theta\, u$ for all $u \in U$, $\theta \in \Theta$;
2. $\theta\, u < \theta'\, u' \Rightarrow \varphi\theta\, u < \varphi\theta'\, u'$ for all $u, u' \in U$ and $\theta, \theta', \varphi \in \Theta$.

Proposition 18 *Assume $\Theta\, U$ is ordered by a ranking and consider any differential polynomial $p \in R \setminus K$. Then, for any proper derivation operator $\theta \in \Theta$, we have $\mathrm{ld}\, \theta\, p = \theta\ \mathrm{ld}\, p$, the degree of $\theta\, p$ w.r.t. its leading derivative is 1 and the initial of $\theta\, p$ (which is the leading coefficient of $\theta\, p$ w.r.t. its leading derivative), is the separant of p i.e. the differential polynomial*

$$s_p \;=\; \frac{\partial p}{\partial\, \mathrm{ld}\, p} \cdot$$

Example. In the MAPLE package, each mathematical differential polynomial ring is endowed with a ranking, which is defined by playing with the list of blocks argument of the `DifferentialRing` function. In our case, the ranking is

$$\cdots > v_{xx} > v_{xy} > v_{yy} > u_{xx} > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u\,.$$

The following commands extract the leading derivatives, initials and separants of our three differential polynomials.

```
> LeadingDerivative ([p[1],p[2],p[3]], R);
                            [u[x], u[x, y], v[x, x]]

> Initial ([p[1],p[2],p[3]], R);
                                  [1, v[y], 1]

> Separant ([p[1],p[2],p[3]], R);
                                [2 u[x], v[y], 1]
```

One can also check a few claims of Proposition 18.

```
> LeadingDerivative (Differentiate (p[1], x, R), R);
                                   u[x, x]

> Initial (Differentiate (p[1], x, R), R);
                                   2 u[x]
```

The following proposition permits us to write proofs by (possibly transfinite) induction on derivatives ordered by rankings. See [3, I, 17, Lemma 15, page 49].

Proposition 19 *Every ranking is a well-ordering (i.e. every strictly decreasing sequence of derivatives is finite).*

Proof This is essentially Dickson's Lemma.

By induction on the number of derivations m.

Basis: if $m = 1$ the Proposition is obvious.

General case: $m \geq 2$. Induction hypothesis: the Proposition holds for less than m derivations. We assume the existence of an infinite strictly decreasing sequence of derivatives and seek a contradiction. Since the number of differential indeterminates is finite, this sequence contains an infinite strictly decreasing sequence of derivatives $(\theta_i\, u)$ of the same differential indeterminate u. Because of the first axiom of rankings, the corresponding sequence (θ_i) satisfies Property (P): $\theta_i \nmid \theta_j$ for all $1 \leq i < j$. Denote $\theta_i = \delta_1^{a_{1i}}\, \delta_2^{a_{2i}} \cdots \delta_m^{a_{mi}}$ and $\theta_i^* = \delta_2^{a_{2i}} \cdots \delta_m^{a_{mi}}$. Now, every infinite sequence of nonnegative integers contains an infinite increasing subsequence. Thus (θ_i) contains an infinite subsequence such that the sequence (a_{1i}) is increasing. Thus the corresponding subsequence of (θ_i^*) must satisfy Property (P). This contradiction with the induction hypothesis proves the Proposition. □

In the sequel, each time we consider the leading derivative, the initial or the separant of some differential polynomial p, it is implicitly assumed that 1) $\Theta\, U$ is endowed with a ranking anf 2) $p \notin K$.

A differential polynomial f is said to be *partially reduced* (according to Kolchin's terminology [3, I, 9, page 77]) w.r.t. a differential polynomial p if f does not depend on any proper derivative of the leading derivative of p. Thanks to Proposition 18, given any differential polynomial f and any set $A = \{p_1, p_2, \ldots, p_n\}$ of differential polynomials of R, the pseudoremainder $\mathsf{prem}(f, \Theta^* A)$ (where Θ^* denotes the set of proper derivation operators) is partially reduced w.r.t. A. In principle, this pseudo-remainder is defined as in Chapter 3. Entering in details, it is obtained by computing a sequence $f = f_0, f_1, \ldots, f_\ell = g$ of differential polynomials such that $f_{k+1} = \mathsf{prem}(f_k, \theta\, p, \mathrm{ld}\,\theta\, p)$ where $p \in A$ and $\theta \in \Theta^*$. The traditional strategy consists in choosing a pair (θ, p) such that the leading derivative of $\theta\, p$ is the highest derivative among all the proper derivatives of the leading derivatives of A occuring in f_k. Whatever the strategy, the sequence of f_k is finite (Proposition 19). According to formula (3.4), page 25, there exists some power product h_f of separants of A such that

$$h_f\, f \quad = \quad g \mod [A] \tag{5.1}$$

where $[A]$, the *differential ideal* of R generated by A, is the set of all finite linear combinations of derivatives of elements of A, with differential polynomials of R as coefficients i.e. the ideal $(\Theta\, A)$. In the proof of Rosenfeld's Lemma, we will need to be even more precise and stress the fact that the pseudodivision process only requires derivatives of A whose leading derivatives are less than or equal to that of f:

$$h_f\, f \quad = \quad g \mod (\theta\, p \mid \mathrm{ld}\,\theta\, p \leq \mathrm{ld}\, f)\,. \tag{5.2}$$

The differential polynomial g is called the *partial remainder* of f by A. Of course, one may also reduce g by the elements of A without differentiating them. In that case, Formulas (5.1) and (5.2) still hold, provided that h_f denotes a power product of separants and initials of A. The new differential polynomial g is then called the *full remainder* of f by A. See [4, I, 6, pages 5-7] or [3, I, 9, pages 77-81].

Example. For legibility, let us precompute a few derivatives of p_1.

```
> p[1];
                                      2
                                  u[x]  - 4 u

> py[1] := Differentiate (p[1], y, R);
                       py[1] := 2 u[x, y] u[x] - 4 u[y]

> pyy[1] := Differentiate (py[1], y, R);
                                                          2
             pyy[1] := 2 u[x, y, y] u[x] + 2 u[x, y]  - 4 u[y, y]
```

Let us now partially reduce $f_0 = \theta\, u$ with $\theta = \delta_x\, \delta_y^2$. To clarify the process, we compute the power of the separants and the pseudoquotients involved in the pseudoreduction.

```
> f[0] := u[x,y,y]:
> f[1] := prem (f[0], pyy[1], u[x,y,y], 'h1', 'q1'):
> 'f[1]' = f[1], 'h1' = h1, 'q1' = q1;
                                  2
              f[1] = -2 u[x, y]  + 4 u[y, y], h1 = 2 u[x], q1 = 1
```

```
> f[2] := prem (f[1], py[1], u[x,y], 'h2', 'q2'):
> 'f[2]' = f[2], 'h2' = h2, 'q2' = q2;
                2                    2              2
f[2] = 16 u[x]  u[y, y] - 32 u[y] , h2 = 4 u[x] , q2 = -4 u[x, y] u[x] - 8 u[y]
```

The differential polynomial f_2 is partially reduced w.r.t. p_1. However, it is not fully reduced. Thus if we perform one more reduction step, we get the full remainder f_3.

```
> f[3] := prem (f[2], p[1], u[x], 'h3', 'q3'):
> 'f[3]' = f[3], 'h3' = h3, 'q3' = q3;
                              2
           f[3] = -32 u[y]  + 64 u[y, y] u, h3 = 1, q3 = 16 u[y, y]
```

It is now possible to make Formula (5.2) explicit, over this example.

```
> expand (h1*h2*h3*f[0] - h2*h3*q1*pyy[1] - h3*q2*py[1] - q3*p[1] - f[3]);
                                        0
```

5.3 The Result

Rosenfeld's Lemma reduces the differential ideal membership problem to a non-differential one. In order to achieve this goal, we first require triangular sets A of R to have elements pairwise partially reduced. This property implies that

$$A \;=\; \{p_1, \ldots, p_n\}$$

is finite (order the polynomials by decreasing leading derivatives and apply Proposition 19). In the ordinary differential case ($m = 1$), this property implies moreover that A does not contain two differential polynomials whose leading derivatives are derivatives of the same differential indeterminate. However, if $m \geq 2$, this is not true anymore and A may involve *critical pairs*.

Definition 2 *A set $\{p_1, p_2\}$ of differential polynomials of $R \setminus K$ is said to form a* critical pair *if the leading derivatives $\theta_1\, u$ of p_1 and $\theta_2\, u$ of p_2 are derivatives of some same differential indeterminate u.*

If the least common multiple θ_{12} of θ_1 and θ_2 is different from both θ_1 and θ_2, one defines the Δ-polynomial associated to the pair as

$$\Delta(p_1, p_2) \;=\; s_1 \frac{\theta_{12}}{\theta_2}\, p_2 - s_2 \frac{\theta_{12}}{\theta_1}\, p_1\,, \tag{5.3}$$

where s_1, s_2 are the separants of p_1, p_2.

Formula (5.3) is built in order to annihilate the leading terms, both equal to $\pm s_1\, s_2\, \theta_{12}\, u$, of the two derivatives of p_1, p_2. Therefore,

Proposition 20 *Either $\Delta(p_1, p_2) \in K$ or it has a leading derivative <u>strictly</u> less than $\theta_{12}\, u$.*

Example. Our set of differential polynomials defines a single critical pair (the two first ones) with $\theta_1 = \delta_x$ and $\theta_2 = \delta_x \, \delta_y$. However $\theta_{12} = \theta_2$ so that the Δ-polynomial is not defined, according to the above definition. In order to see a Δ-polynomial, we may consider the critical pair $\{\delta_x \, p_1, \, p_2\}$. Then we have $\theta_1 = \delta_x^2$, $\theta_2 = \delta_x \, \delta_y$ and $\theta_{12} = \delta_x^2 \, \delta_y$. We may observe that the Δ-polynomial depends on derivatives strictly less than $\theta_{12} \, u$ only.

```
> px[1] := Differentiate(p[1], x, R);
                        px[1] := 2 u[x, x] u[x] - 4 u[x]

> DeltaPolynomial (px[1], p[2], R);
                                                                        2
     v[x, y] u[x, y] u[x] - u[x, x] u[x, y] v[y] + 2 u[x, y] v[y] - u[x]
```

If A is a triangular set of pairwise partially reduced differential polynomials, then a Δ-polynomial is associated to any critical pair of A.

Before stating the following definition, recall that if $\mathfrak{A}$ is an ideal (possibly differential) and h is any differential polynomial of R, then the *saturation* of $\mathfrak{A}$ by h is the ideal (differential, if so is $\mathfrak{A}$)

$$\mathfrak{A} : h^\infty \quad = \quad \{ f \in R \mid \exists \, d \geq 0 \, , \ f^d \in \mathfrak{A} \} \, .$$

Definition 3 *Let A be a triangular set of pairwise partially reduced differential polynomials of R and h be the product of its initials and separants. A critical pair $\{p_1, p_2\} \subset A$ is said to be* solved *if*

$$\Delta(p_1, p_2) \quad \in \quad (\theta \, p \mid p \in A \, , \ \mathrm{ld} \, \theta \, p < \theta_{12} \, u) : h^\infty \, . \tag{5.4}$$

In Formula (5.4) the inequality is strict (if it were large, every critical pair would be solved).

Proposition 21 *(the algorithmic criterion)*
Let A be a triangular set of pairwise partially reduced differential polynomials of R and $\{p_1, p_2\} \subset A$ be a critical pair. If

$$\mathsf{prem}(\Delta(p_1, p_2), \Theta \, A) \quad = \quad 0$$

then the critical pair is solved.

Proof If $\mathsf{prem}(\Delta(p_1, p_2), \Theta \, A) = 0$ then $\Delta(p_1, p_2)$ belongs to the ideal stated in Formula (5.2) (with a large inequality, w.r.t. the leading derivative of the Δ-polynomial). However, this leading derivative is strictly less than θ_{12} (Proposition 20), so that Formula (5.4) holds. □

Definition 4 *A triangular set of pairwise partially reduced differential polynomials is said to be* coherent *if all its critical pairs are solved.*

Our set S of three differential polynomials defines a differential ideal (the radical of the differential ideal generated by these differential polynomials). This set is triangular but its elements are not pairwise partially reduced. It turns out that the ideal defined by S can be represented by a single regular differential chain A. In the following commands, the call to `RosenfeldGroebner` computes A from S and the ranking. Regular differential chains satisfy the hypotheses of Rosenfeld's Lemma. In particular, they are triangular sets of differential polynomials pairwise partially reduced.

```
> ideal := RosenfeldGroebner([p[1],p[2],p[3]],R):
> A := Equations (ideal[1]);
                                                                    2
A := [v[x, x] - u[x], 4 v[y] u - u[x] u[y] u + u[x] u[y], u[x]  - 4 u,

        2
    u[y]  - 2 u]

> LeadingDerivative (A, R);
                          [v[x, x], v[y], u[x], u[y]]
```

The two critical pairs defined by A are solved (Proposition 21). The calls to `DifferentialPrem` perform Ritt reduction. Each call returns a sequence h, r where h is the power product of initials and separants involved in the reduction process and r is the remainder. One can observe that remainders are zero. The set A is thus coherent.

```
> DifferentialPrem (DeltaPolynomial (A[1], A[2], R), A, R);
                                    2     3  2
                              16 u[x]  u[y]  u , 0

> DifferentialPrem (DeltaPolynomial (A[3], A[4], R), A, R);
                                     1, 0
```

Proposition 22 *(Rosenfeld's Lemma)*
Let A be a triangular set of pairwise partially reduced differential polynomials of R and h be the product of its initials and separants. If all critical pairs of A are solved (i.e. if A is coherent), then every differential polynomial $f \in [A] : h^\infty$, which is partially reduced w.r.t. A belongs to $(A) : h^\infty$.

Proof By transfinite induction.

Since $f \in [A] : h^\infty$, there exists a power product h_f of separants and initials of A and finitely many differential polynomials $b_{\varphi,i}$ such that

$$h_f\, f \;=\; \underbrace{\sum_{\varphi\in\Theta}\sum_{i=1}^{n} b_{\varphi,i}\,\varphi\, p_i}_{(\mathscr{F})} \;.$$

We assume $f \notin (A) : h^\infty$ and seek a contradiction. Formula $(\mathscr{F})$ then involves proper derivatives of leading derivatives of A. Let $v(\mathscr{F})$ be the lowest one w.r.t. the ranking. Among all possible formulas $(\mathscr{F})$, choose one such that $v(\mathscr{F})$ is minimal. This derivative does exist since rankings are well-orderings. We seek another formula $(\mathscr{F}')$ such that $v(\mathscr{F}') < v(\mathscr{F})$. This contradiction with the minimality hypothesis will prove the Proposition.

Denote $v(\mathscr{F}) = \theta\, u$ and assume that $\theta\, u$ is a proper derivative of the leading derivtaives $\theta_1\, u, \ldots, \theta_k\, u$ of the differential polynomials $p_1, \ldots, p_k \in A$ (renumbering if needed). Denote $(\theta/\theta_1)\, p_1 = s_1\, \theta\, u + r_1$. Apply over $(\mathscr{F})$ the substitution

$$\theta\, u \;=\; \frac{(\theta/\theta_1)\, p_1 - r_1}{s_1}$$

and multiply by a suitable power of the separant s_1 in order to clear denominators. Denote $\gamma_j = \theta/\operatorname{lcm}(\theta_1, \theta_j)$ for $2 \leq j \leq k$. One obtains the following formula, where c, d_j and lines (5.6) and (5.7) involve derivatives strictly less than $v(\mathscr{F})$ only:

$$\begin{aligned} s_1^\alpha\, h_f\, f &= c\,\frac{\theta}{\theta_1}\,p_1 && (5.5)\\ &+ \sum_{j=2}^{k} d_j\,\Delta(\gamma_j\,p_1,\,\gamma_j\,p_j) && (5.6)\\ &+ \sum_{\varphi\in\Theta}\sum_{j=1}^{n} e_{\varphi,j}\,\varphi\,p_j. && (5.7) \end{aligned}$$

The leading derivative of $s_i^\alpha\, h\, f$ is itself strictly less than $v(\mathscr{F})$. Thus $v(\mathscr{F})$ only shows up as leading derivative of $(\theta/\theta_1)\,p_1$. The differential polynomial c is thus identically zero.

In the ordinary differential case, the sum (5.6) is empty and (5.7) provides the sought formula $(\mathscr{F}')$.

Let us address the partial case ($m = 2$). All critical pairs $\{p_1, p_j\}$ are supposed to be solved. According to Proposition 23, all critical pairs $\{\gamma_j\,p_1, \gamma_j\,p_j\}$ are also solved. Multiplying again, possibly, both sides of the formula by a suitable power product of initials and separants of A, one sees that (5.6) belongs to the ideal generated by the elements of $\Theta\,A$ whose leading derivative is strictly less than $v(\mathscr{F})$. The sum of (5.6) and (5.7) provides the sought formula $(\mathscr{F}')$. □

The following Proposition actually is a technical lemma, used in the proof of Proposition 22.

Proposition 23 *Let A be a triangular set of pairwise partially reduced differential polynomials of R, $\{p_1, p_2\} \subset A$ be a solved critical pair and $\gamma \in \Theta$ a derivation operator. Then the critical pair $\{\gamma\,p_1, \gamma\,p_2\}$ is solved.*

Proof By induction on the order of γ.

First observe that

$$\Delta(\gamma\,p_1, \gamma\,p_2) = s_1\,\frac{\gamma\,\theta_{12}}{\theta_2}\,p_2 - s_2\,\frac{\gamma\,\theta_{12}}{\theta_1}\,p_1\,.$$

Basis: if the order is zero then $\{\gamma\,p_1, \gamma\,p_2\} = \{p_1, p_2\}$ is solved.

General case. Decompose $\gamma = \delta\,\lambda$ with δ a single derivation. Assume inductively that $\{\lambda\,p_1, \lambda\,p_2\}$ is solved. Denote $\varphi = \lambda\,\theta_{12}$ and $\theta = \delta\,\varphi = \gamma\,\theta_{12}$. By the induction hypothesis, there exists a power product of initials and separants h_d of A such that

$$h_d\,\Delta(\lambda\,p_1, \lambda\,p_2) \in (\mu\,p \mid \operatorname{ld}\mu\,p < \varphi\,u)$$

Differentiate this expression by δ and multiply again by h_d. One gets a sum

$$(\delta\,h_d)\,h_d\,\Delta(\lambda\,p_1, \lambda\,p_2) + h_d^2\,\delta\,\Delta(\lambda\,p_1, \lambda\,p_2)$$

which belongs to $(\mu\,p \mid \operatorname{ld}\mu\,p < \theta\,u)$, and whose first summand belongs to $(\mu\,p \mid \operatorname{ld}\mu\,p < \varphi\,u)$. Since $\varphi\,u < \theta\,u$, one sees that the second summand belongs to $(\mu\,p \mid \operatorname{ld}\mu\,p < \theta\,u)$. Develop this second

summand:

$$h_d^2\,\delta\,\Delta(\lambda\,p_1,\,\lambda\,p_2) = h_d^2\,\delta\left\{s_1\,\frac{\varphi}{\theta_2}\,p_2 - s_2\,\frac{\varphi}{\theta_1}\,p_1\right\} \quad (5.8)$$

$$= h_d^2\left\{(\delta\,s_1)\frac{\varphi}{\theta_2}\,p_2 - (\delta\,s_2)\frac{\varphi}{\theta_1}\,p_1\right\} \quad (5.9)$$

$$+ h_d^2\left\{s_1\,\frac{\theta}{\theta_2}\,p_2 - s_2\,\frac{\theta}{\theta_1}\,p_1\right\}. \quad (5.10)$$

The differential polynomials $(\varphi/\theta_i)\,p_i$ on line (5.9) belong to $(\mu\,p \mid \mathrm{ld}\,\mu\,p < \varphi\,u)$. Thus, the expression on line (5.10), which is nothing but $h_d^2\,\Delta(\gamma\,p_1,\,\gamma\,p_2)$, lies also in this ideal. The critical pair $\{\gamma\,p_1,\,\gamma\,p_2\}$ is thus solved. □

5.4 Concluding Remarks

Rosenfeld's Lemma appears in [5, Lemma]. It improves an earlier (flawed?) version by Seidenberg [6, Theorem 6]. A generalized version is available in [3, III, 8, pages 135-138] but Kolchin's version does not clearly appear to be algorithmic.

The presentation of Rosenfeld's Lemma owes a lot to [1, Section 7.3], which also involves a fixed formulation of Seidenberg's variant.

Proposition 22 is formulated for ideals saturated by the separants and the initials of A. Actually, the theorem can be formulated for ideals saturated by the separants only, provided that one updates accordingly the definition of solved critical pairs. In that case however, Proposition 21 (the algorithmic criterion) does not hold anymore but can be replaced by a partial remainder computation, followed by a Gröbner basis reduction.

Every polynomial system can be encoded as a linear PDE system, in one differential indeterminate, with constant coefficients. With this encoding, Rosenfeld's Lemma implies that a polynomial system which reduces to zero all its S-polynomials is a Gröbner basis [2, 2, 9, Theorem 3, page 101].

Bibliography

[1] 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`.

[2] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics. Springer Verlag, New York, 2nd edition, 1996.

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

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

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

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

Chapter 6

The Differential Nullstellensatz

This section aims at proving Propositions 24 and 25.

6.1 Informal Introduction

We reconsider the example of Chapter 10 and focus on a point which introduces this chapter. See Chapter 10 for more details.

We start with the following chemical reaction system. It describes the transformation of a substrate S into a product P, in the presence of some enzyme E. An intermediate complex C is formed. The symbols k_1, k_{-1}, k_2 denote reaction rates and are considered as parameters.

$$E + S \underset{k_{-1}}{\overset{k_1}{\rightleftarrows}} C \xrightarrow{k_2} E + P\,. \tag{6.1}$$

Let us first build the deterministic model of (6.1) using the mass-action law. The four functions correspond to the concentrations of the corresponding chemical species.

```
> with (LinearAlgebra):
> X := <E(t), S(t), C(t), P(t)>:
> V := <k[1]*E(t)*S(t), k[-1]*C(t), k[2]*C(t)>:
> N := <<-1, -1, 1, 0> | <1, 1, -1, 0> | <1, 0, -1, 1>>:
> X, N, V;
                  [E(t)]  [-1     1     1]
                  [    ]  [              ]  [k[1] E(t) S(t)]
                  [S(t)]  [-1     1     0]  [              ]
                  [    ], [              ], [  k[-1] C(t)  ]
                  [C(t)]  [ 1    -1    -1]  [              ]
                  [    ]  [              ]  [  k[2] C(t)   ]
                  [P(t)]  [ 0     0     1]
```

Here is a first formulation of the dynamical system.

```
> madm := map (diff, X, t) = N . V;
                  [d      ]
                  [-- E(t)]
                  [dt     ]
                  [       ]
                  [d      ]   [-k[1] E(t) S(t) + k[-1] C(t) + k[2] C(t)]
                  [-- S(t)]   [                                         ]
                  [dt     ]   [      -k[1] E(t) S(t) + k[-1] C(t)      ]
         madm := [       ] = [                                         ]
                  [d      ]   [k[1] E(t) S(t) - k[-1] C(t) - k[2] C(t) ]
                  [-- C(t)]   [                                         ]
                  [dt     ]   [               k[2] C(t)                 ]
                  [       ]
                  [d      ]
                  [-- P(t)]
                  [dt     ]
```

Here, we would like to study what happens if we assume moreover that the rate change of the complex $C(t)$ is zero.

```
> with(DifferentialAlgebra);
```

Let us now define a differential polynomial ring, endowed with the ranking

$$(\text{the derivatives of } C, E, P, S) \gg (\text{the parameters } k_1, k_{-1}, k_2)\,.$$

```
> R :=  DifferentialRing
      (blocks = [[C,E,P,S], [k[1](),k[-1](),k[2]()]], derivations = [t]);
                            R := differential_ring
```

Let us now add to `madm` the hypothesis that $C(t)$ is a constant, obtaining a new system called `madm_approx`.

```
> madm_approx :=
   [ seq (lhs (madm) [i] = rhs (madm) [i], i = 1 .. Dimension (X)),
     diff (C(t),t) = 0 ];
```

In the simplification process, we do not want to discuss the possible vanishing of any expression depending on the three parameters: we want the simplification to be "generic". The algebraic way to formulate this consists in moving the three parameters in the ground field of the equations. Indeed, in a field, every quantity which is not zero is invertible, and cannot vanish.

```
> Field := field (generators = [k[1],k[-1],k[2]]);
                Field := field(generators = [k[1], k[-1], k[2]])
```

Let us now simplify the system over the ground field `Field`.

```
> ideal := RosenfeldGroebner (madm_approx, R, basefield = Field);
       ideal := [regular_differential_chain, regular_differential_chain]

> Equations (ideal);
          d        d                       d        d
        [[-- E(t), -- P(t), C(t), S(t)], [-- P(t), -- S(t), C(t), E(t)]]
          dt       dt                      dt       dt
```

We have thus got two cases, represented by two regular differential chains. This is a nice example since the two chains are very simple and obviously define prime differential ideals which are not included in each other. The intersection is thus irredundant (Proposition 24 below).

How did we end up with these two cases? Actually, the hypothesis $\dot{C}(t) = 0$ simplifies one of the equations and yields $k_1\,E(t)\,S(t) - k_{-1}\,C(t) - k_2\,C(t) = 0$. Differentiating this equation (the two sides are the zero function and the derivative of the zero function is the zero function), taking the hypothesis into account, and dividing by k_1, which is a ground field element, we get $E(t)\,\dot{S}(t) + \dot{E}(t)\,S(t) = 0$. At this stage, the simplifier has solved the equation w.r.t. its leading derivative, which is $\dot{E}(t)$, and has viewed it as

$$\dot{E}(t) \quad \rightarrow \quad -\frac{E(t)\,\dot{S}(t)}{S(t)}$$

provided that $S(t) \neq 0$. Separately, it has considered the case $S(t) = 0$ in order not to loose any solution: It has split cases.

This chapter is all about the correspondence between the solution sets (the algebraic varieties) and the equation sets (the differential ideals). As long as we do not split cases, it is easy: the hypothesis $\dot{C}(t) = 0$ can be restated as $\dot{C}(t) \in \mathfrak{A}$ where $\mathfrak{A}$ is the differential ideal generated by `madm_approx`. Observe we have differentiated one differential polynomial without leaving $\mathfrak{A}$ since the ideal is differential.

The analysis of the splitting requires more theory. What is clear, is that it preserves the (differential) algebraic variety V of the input system. Denoting V_1 and V_2 the solution sets (one of them is not an algebraic variety since it involves an inequation) after the splitting, we see that

$$V \quad = \quad V_1 \cup V_2\,. \tag{6.2}$$

Let us denote $I(V)$ the differential ideal of the differential polynomials which annihilate over V (define similarly $I(V_1)$ and $I(V_2)$). We would like to translate the union of varieties (6.2) as an intersection of ideals

$$I(V) \quad = \quad I(V_1) \cap I(V_2)\,. \tag{6.3}$$

In order to have $I(V) = \mathfrak{A}$, we will require $\mathfrak{A}$ to be a radical differential ideal (Proposition 25). We will also need to give formulas for $I(V_1)$ and $I(V_2)$. This is achieved by Proposition 26.

6.2 In Commutative Algebra

The Lasker-Nöther Theorem (Theorem 5, page 17) states that, in a Nötherian ring R, every ideal $\mathfrak{a}$ can be represented by an irredundant primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. Irredundant means that, for $i \neq j$, 1) $\mathfrak{q}_i \not\subset \mathfrak{q}_j$ and 2) $\mathfrak{q}_i \cap \mathfrak{q}_j$ is not primary. The prime ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are the *associated* prime ideals of $\mathfrak{a}$. The associated primes of $\mathfrak{a}$ which contain no other associated prime are said to be *isolated*. The ones which are not isolated are said to be *imbedded*. See [8, IV, 4-5, pages 208-212].

The associated prime ideals of $\mathfrak{a}$ play an important role since an element $f \in R$ is a zero-divisor in $R/\mathfrak{a}$ if and only if f belongs to the union of the associated prime ideals of $\mathfrak{a}$ [8, IV, 6, Corollary 3 to Theorem 11, page 214].

If R is a polynomial ring in finitely many indeterminates, over a field K then R is Nötherian, which means that $\mathfrak{a}$ is generated by a finite set $p_1, \ldots, p_n$ of polynomials. In this context, the above theorems can be interpreted in terms of solutions of the polynomial system

$$p_1 = \cdots = p_n = 0\,.$$

Indeed, provided that we seek solutions of $\mathfrak{a}$ in non-fixed overfields of the ground field K, a polynomial f belongs to $\sqrt{\mathfrak{a}}$ if and only if vanishes on every solution of the polynomial system.

Proof The implication $\Rightarrow$ is clear: every solution of the polynomial system annihilates the whole ideal $\mathfrak{a}$. Since solutions are sought in fields, which are particular cases of domains, $f^d = 0$ implies that $f = 0$.

The implication $\Leftarrow$ may be proved by means of the Lasker-Nöther Theorem. We assume $f \notin \sqrt{a}$ and we prove that the polynomial system admits a solution that does not annihilate f. The ideal $\sqrt{a}$ is the intersection of the isolated associated prime ideals of $\mathfrak{a}$. Since $f \notin \sqrt{a}$, there exists at least one isolated associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ such that $f \notin \mathfrak{p}$. The field of fractions K' of $R/\mathfrak{p}$ is a field extension of K. Let $x_1, \ldots, x_r$ denote the indeterminates of R. The image of the vector $(x_1, \ldots, x_r)$ by the canonical ring homomorphism $K \to K'$ provides the desired solution. □

To simplify statements and avoid non-fixed overfields, one may go a bit further and inject K' in the field of the complex numbers. We then obtain Hilbert Nullstellensatz [8, VII, 3, Theorem 14, page 164].

The overfield K' thus depends on the solution under consideration. Here is a basic example. Consider the equation $x^2 - 2 = 0$ in $\mathbb{Q}[x]$. The idea consists in looking for a solution in $\mathbb{Q}(\sqrt{2})$ rather than in $\mathbb{C}$. Formally, $(x^2 - 2)$ is a prime (even a maximal) ideal of $\mathbb{Q}[x]$. The field K' is the residue class ring $\mathbb{Q}[x]/(x^2 - 2)$. The solution $x = \sqrt{2}$ is the image of x by the canonical ring homomorphism $\mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2 - 2)$. Indeed, what is $\sqrt{2}$? Almost nothing but a symbol x such that $x^2 - 2 = 0$.

The isolated associated prime ideals of $\mathfrak{a}$ correspond to the irreducible components of the algebraic variety of the polynomial system [8, VII, 3, Corollary 3 to Theorem 14, page 167].

6.3 In Differential Algebra

Let $R = K\{U\}$ be a differential polynomial ring where K is a differential field of characteristic zero, U is a finite set of differential indeterminates u_k, endowed with a finite set of derivations $\{\delta_1, \ldots, \delta_m\}$. Let Θ denote the multiplicative monoid of derivation operators, generated by the m derivations. See Section 5.2, page 39, for more details.

The differential polynomial ring $R = K[\Theta\, U]$ is a polynomial ring in infinitely many indeterminates (the *derivatives*). It is thus not Nötherian and the Lasker-Nöther Theorem needs not hold. Indeed, we only have a weak form at our disposal (Proposition 25).

An ideal $\mathfrak{A}$ of R is said to be *differential* if $\theta\, f \in \mathfrak{A}$ whenever $f \in \mathfrak{A}$, for any differential polynomial $f \in R$ and any derivation operator $\theta \in \Theta$. The radical of a differential ideal is a radical differential ideal (or *perfect* in Ritt's terminology). A prime differential ideal is a differential ideal which is prime. If $A \subset R$, then one denotes $[A]$ the differential ideal generated by A.

We are now ready to state [6, I, 16, Theorem; and 17, page 16].

Proposition 24 *Every radical differential ideal $\mathfrak{A}$ of R has a representation as an irredundant finite intersection of prime differential ideals $\mathfrak{A} = \cap_{i=1}^{r} \mathfrak{P}_i$. Irredundant means that if $i \neq j$ then $\mathfrak{P}_i \not\subset \mathfrak{P}_j$.*

By analogy with the commutative algebra case, we will call the differential prime ideals $\mathfrak{P}_i$ the *associated* differential prime ideals of $\mathfrak{A}$ (the *essential prime divisors* in Ritt's terminology).

There does not seem to be any mention of primary differential ideals in classical books, though the study of differential ideals such as $[y^p]$ [6, I, 21, page 16] is probably related to such a concern.

Proposition 24 implies the following differential Nullstellensatz [6, II, 7, Theorem of zeros, page 27].

Proposition 25 *(differential Nullstellensatz)*

Let $p_1, \ldots, p_n$ be differential polynomials of $R = K\{U\}$ and $\mathfrak{A}$ be the radical of the differential ideal that they generate. Then a differential polynomial f belongs to $\mathfrak{A}$ if and only if it vanishes over every solution of the system of differential polynomial equations $p_1 = \cdots = p_n = 0$, taken in some non-fixed differential field extension K' of K.

In principle, the proof is exactly the same as in commutative algebra.

In the non-differential case, we have used the Lasker-Nöther Theorem to conclude that, if $f \notin \sqrt{a}$ then there exists an associated prime ideal of $\mathfrak{a}$ which does not contain f. In the differential case, one may use Proposition 24 for the same purpose.

A notion which may seem unclear to some readers is that, if $\mathfrak{P}$ is a differential prime ideal of R then $R/\mathfrak{P}$ is a differential ring. A clear explanation is given in [6, II, 6, page 26]: a residue class ring $S/\mathfrak{a}$ is the set of the equivalence classes w.r.t. the equivalence relation modulo the ideal $\mathfrak{a}$. This set is endowed with a ring structure by defining the sum and the product of two classes. If a lies in a class A and b lies in a class B then the sum of the two classes $A + B$ is defined as the class which contains the sum $a + b$ (the product is defined likewise). And it is a classical exercise to prove, using the definition of ideals, that $A + B$ depends on A and B and not on the arbitrary elements $a \in A$ and $b \in B$. If $\mathfrak{a}$ is differential, one can similarly define the derivative of a class and thereby endow $S/\mathfrak{a}$ of a differential ring structure.

6.4 The Splitting Case Mechanism

Proposition 26 *Let $p_1, \ldots, p_n$ be differential polynomials of $R = K\{U\}$ and $\mathfrak{A}$ be the radical of the differential ideal that they generate. Let h be any differential polynomial.*

Then the solution set V of $p_1 = \cdots = p_n = 0$ is the union $V = V_1 \cup V_2$ of the solution sets V_1 of $p_1 = \cdots = p_n = h = 0$, and V_2 of $p_1 = \cdots = p_n = 0$, $h \neq 0$.

Moreover, the set $\mathfrak{A}_1$ of the differential polynomials which annihilate over V_1 is the radical differential ideal $\sqrt{[\mathfrak{A} \cup \{h\}]}$, the set $\mathfrak{A}_2$ of the differential polynomials which annihilate over V_2 is the radical differential ideal $\mathfrak{A} : h^\infty$, and we have $\mathfrak{A} = \mathfrak{A}_1 \cap \mathfrak{A}_2$.

Proof The fact that $V = V_1 \cup V_2$ is obvious.

The fact that $\mathfrak{A}_1 = \sqrt{[\mathfrak{A} \cup \{h\}]}$ is a consequence of Proposition 25.

By Proposition 25, the differential polynomials that annihilate over V_2 have the form $h^d f$ with $d \geq 0$ and $f \in \mathfrak{A}$. They thus belong to $\mathfrak{A}_2 = \mathfrak{A} : h^\infty$. By definition of the saturation, $\mathfrak{A}_2$ is the intersection of the associated differential prime ideals of $\mathfrak{A}$ which do not contain h (one defines the

empty intersection to be the whole ring). Since it is an intersection of prime differential ideals, it is a radical differential ideal.

The equivalence between $V = V_1 \cup V_2$ and $\mathfrak{A} = \mathfrak{A}_1 \cap \mathfrak{A}_2$ is classical. In the commutative algebra context, see [8, VII, 3, page 160]. □

6.5 Formal Power Series Solutions

Assume $u(x)$ is an analytic function. The following formula is well-known:

$$u(x) \quad = \quad u(0) + \dot{u}(0)\, x + \ddot{u}(0)\, \frac{x^2}{2} + \cdots$$

It generalizes to functions of m independent variables $x_1, \ldots, x_m$. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ is a derivation operator, denote $x^\theta = x_1^{a_1} \cdots x_m^{a_m}$ and $\theta! = a_1! \cdots a_m!$. Then

$$u(x) = \sum (\theta\, u)(0)\, \frac{x^\theta}{\theta!}\cdot$$

Let $\mathfrak{A}$ be a radical differential ideal of R. Let us view every derivative of any differential indeterminate as a non-differential indeterminate and seek a solution of $\mathfrak{A}$ in, say, the field of the complex numbers. Such a solution provides a map $\varphi : \Theta U \to \mathbb{C}$. Now, if we interpret $\varphi(\theta\, u)$ as $(\theta\, u)(0)$ and the derivations δ_k as partial derivatives w.r.t. x_k, for $1 \leq k \leq m$, then the vector $(\bar{u}_1, \ldots, \bar{u}_n)$ (see below) provides a solution of $\mathfrak{A}$ has a tuple of formal power series.

$$\bar{u}_k(x) = \sum \varphi(\theta\, u_k)\, \frac{x^\theta}{\theta!}\cdot$$

Example. Let us consider the differential equation $\dot{u}^3 - 27\, u^2$, which admits $u(x) = (x + c)^3$ as a solution.

```
> with (DifferentialAlgebra):
> with (Tools):

> p := u[x]^3-27*u[]^2;
                                        3          2
                              p := u[x]  - 27 u[]
```

Let us assign to `ideal` the regular differential chain that it defines.

```
> R := DifferentialRing (derivations = [x], blocks = [u]):
> ideal := PretendRegularDifferentialChain ([p], R);
                        ideal := regular_differential_chain
```

Let us assign to `ThetaU` the following list of derivatives

```
> ThetaU := [seq (Differentiate (u,x^i,R,notation=tjet), i = 0..4)];
           ThetaU := [u[], u[x], u[x, x], u[x, x, x], u[x, x, x, x]]
```

and to `L` some of the differential polynomials that must be annihilated by any solution φ.

```
> L := [seq (Differentiate (p,x^i,R), i = 0..3)];
          3         2                2
L := [u[x]  - 27 u[] , 3 u[x, x] u[x]  - 54 u[x] u[],

                     2           2                                  2
    3 u[x, x, x] u[x]  + 6 u[x, x]  u[x] - 54 u[x, x] u[] - 54 u[x] ,

                       2
    3 u[x, x, x, x] u[x]  + 18 u[x, x, x] u[x, x] u[x] - 54 u[x, x, x] u[]

              3
     + 6 u[x, x]  - 162 u[x, x] u[x]]
```

In order to obtain a solution φ, a simple method consists in computing the *normal forms* of the derivatives of `ThetaU` w.r.t. the regular differential chain.

```
> NF_ThetaU := NormalForm (ThetaU, ideal);
                                                    2
                                                 u[x]
                NF_ThetaU := [u[], u[x], 2/3 -----, 6, 0]
                                                  u[]
```

These normal forms depend on two symbols `u[]` and `u[x]` but any value given to these symbols must annihilate `p`. We thus cannot choose both of them freely. A convenient possibility consists in assigning c^3 to `u[]` and $3\,c^2$ to `u[x]`.

```
> phi := [seq (ThetaU[i] = subs (u[]=c^3, u[x]=3*c^2, NF_ThetaU[i]), i=1..5)];
phi :=
            3            2
    [u[] = c , u[x] = 3 c , u[x, x] = 6 c, u[x, x, x] = 6, u[x, x, x, x] = 0]
```

Let us double check that `phi` actually is a non-differential solution of the polynomial equations of `L`.

```
> subs (phi, L);
                                  [0, 0, 0, 0]
```

In order to form the formal power series solution (which turns out to be a polynomial, here), let us assign a generic formal power series to `generic_u`

```
> generic_u := add (u[x$(i-1)]*x^(i-1)/(i-1)!, i = 1..5);
generic_u :=
                       2               3                    4
    u[] + x u[x] + 1/2 x  u[x, x] + 1/6 x  u[x, x, x] + 1/24 x  u[x, x, x, x]
```

and replace the derivatives by the values listed in `phi`. We have got our differential solution.

```
> ubar := subs (phi, generic_u);
                              3        2      2      3
                    ubar := c  + 3 x c  + 3 x  c + x

> factor (ubar);
                                       3
                                 (c + x)
```

6.6 Concluding Remarks

This chapter owes a lot to [2].

Under some conditions, formal power series solutions provide analytic solutions. This is nicely explained in [6, 7]. See also [5, 4] which give the most general rankings ensuring the analyticity of the power series solutions of orthonomic systems, with analytic initial conditions.

The method for computing formal power series solutions permits to expand solutions for initial values that do not annihilate the initials and the separants of the regular differential chain, i.e. for regular initial values. The case of initial values that annihilate some initials or separants is much more complicated and the general problem: given a regular differential chain and an expansion point, does there exist a formal power series solution of the regular differential chain, centered at that point, is undecidable (a decision algorithm would solve Hilbert's tenth problem). See [3, Theorem 4.11] for the key result and [1, 6.1.5, page 100] for the application to regular differential chains.

Bibliography

[1] 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`.

[2] 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.

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

[4] François Lemaire. Les classements les plus généraux assurant l'analycité des systèmes orthonomes pour des conditions initiales analytiques. In Victor G. Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *proceedings of Computer Algebra in Scientific computation 2002*, pages 207–219, Yalta, Ukraine, 2002. Institüt für Informatik, Technische Universität München.

[5] François Lemaire. *Contribution à l'algorithmique en algèbre différentielle*. PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, January 2002. (in French).

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

[7] Abraham Seidenberg. Some basic theorems in differential algebra (characteristic p arbitrary). *Trans. Amer. Math. Soc.*, 73:174–190, 1952.

[8] 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.

Chapter 7

Regular Differential Chains

This chapter aims at proving Proposition 29. First we recall some basic elements of differential algebra. For more details, see Section 5.2, page 39.

Let $R = K\{U\}$ be a differential polynomial ring where K is a differential field of characteristic zero, U is a finite set of differential indeterminates u_k, endowed with a finite set of derivations $\{\delta_1, \ldots, \delta_m\}$. Let Θ denote the multiplicative monoid of derivation operators, generated by the m derivations. Assume the infinite set of derivatives $\Theta\, U$ is ordered w.r.t. a ranking, so that the leading derivative, the initial and the separant of any differential polynomial of $R \setminus K$ are well defined.

Recall that a differential polynomial f is said to partially reduced w.r.t. a differential polynomial p if f does not depend on any proper derivative of the leading derivative of p. In the sequel, A denotes a triangular set of n differential polynomials of $R \setminus K$, pairwise partially reduced. If f is any differential polynomial, then $\mathsf{prem}(f, \Theta\, A)$ denotes the full remainder of f by all the derivatives of A.

In the case $m \geq 2$, the set A may involve critical pairs i.e. pairs $\{p_1, p_2\} \subset A$ such that the leading derivatives $\theta_1\, u$ of p_1 and $\theta_2\, u$ of p_2 are derivatives of some same differential indeterminate u. Define $\theta_{12} = \mathrm{lcm}(\theta_1, \theta_2)$ and the Δ-polynomial associated to the pair as

$$\Delta(p_1, p_2) \quad = \quad s_1 \, \frac{\theta_{12}}{\theta_2} \, p_2 - s_2 \, \frac{\theta_{12}}{\theta_1} \, p_1 \, ,$$

where s_1, s_2 are the separants of p_1, p_2. The critical pair is said to be solved if

$$\mathsf{prem}(\Delta(p_1, p_2), \Theta\, A) \quad = \quad 0$$

The set A is said to be coherent if all its critical pairs are solved.

Let h denote the product of the initials and the separants of A. Distinguish the differential ideal $[A] : h^\infty$, which is the ideal generated by $\Theta\, A$, saturated by h

$$[A] : h^\infty \quad = \quad \{f \in R \mid \exists\, d \geq 0\, , \ f^d \in (\Theta\, A)\}$$

from the non-differential ideal $(A) : h^\infty$, which is the ideal generated by A, saturated by h

$$(A) : h^\infty \quad = \quad \{f \in R \mid \exists\, d \geq 0\, , \ f^d \in (A)\}\, .$$

Definition 5 *A triangular set A of pairwise partially reduced differential polynomials of R is said to be a* regular differential chain *if it satisfies the following conditions:*

a *the initial i_k of p_k is regular in $R/(p_1,\ldots,p_{k-1}):(i_1\cdots i_{k-1})^\infty$ for $2\leq k\leq n$ (algorithmic regular chain criterion);*

b *the separant s_k of p_k is regular in $R/(A):(i_1\cdots i_n)^\infty$ for $1\leq k\leq n$;*

c *A is coherent, i.e. all critical pairs of A are solved (meaningful only if $m\geq 2$).*

Condition **a** implies that A is a regular chain (Proposition 5). Condition **b** implies that $(A):(i_1\cdots i_n)^\infty = (A):h^\infty$ hence that the regular chain A can be used for recognizing zero and zero-divisors in $R/(A):h^\infty$. Condition **c** implies that A satisfies the hypotheses of Proposition 22 (Rosenfeld's Lemma). Last observe that, since h contains the separants of A as factors, the ideal $(A):h^\infty$ satisfies the hypotheses of Proposition 17 (Lazard's Lemma).

7.1 Important Properties

This section is actually a sequence of Propositions listing the properties of regular differential chains. Many propositions are split in two parts, in order to separate the properties implied by Rosenfeld and Lazard Lemmas from the ones implied by the regular chain condition.

Proposition 27 *Let A be a coherent triangular set of pairwise partially reduced differential polynomials of R, f be a differential polynomial of R and $g=\mathsf{prem}(f,\Theta^* A)$, where Θ^* denotes the set of proper derivation operators.*

Then f is zero in $R/[A]:h^\infty$ if and only if g is zero in $R/(A):h^\infty$.

Proof The differential polynomial is zero in $R/[A]:h^\infty$ if and only if g is zero in $R/[A]:h^\infty$. The partial remainder g is partially reduced w.r.t. A. By Rosenfeld Lemma (Proposition 22), g is zero in $R/[A]:h^\infty$ if and only if g is zero in $R/(A):h^\infty$. □

Proposition 28 *Let A be a regular differential chain, h be the product of the initials and separants of A and f be a differential polynomial of R.*

Then $\mathsf{prem}(f,\Theta A)=0$ if and only if f is zero in $R/[A]:h^\infty$.

Proof The implication $\Rightarrow$ is clear.

In order to prove the implication $\Leftarrow$, let us consider some $f\in[A]:h^\infty$ and denote $g=\mathsf{prem}(f,\Theta A)$ (the full remainder of f by A). Since g is partially reduced w.r.t. A, Proposition 22 (Rosenfeld's Lemma) applies and $g\in(A):h^\infty$. Since $g=\mathsf{prem}(g,A)$ and A is a regular chain and $(A):(i_1\cdots i_n)^\infty=(A):h^\infty$, we have $g=0$ (Proposition 5). □

The following Proposition is sometimes called the "lifting of Lazard's Lemma" to differential algebra. It relies on the notion of associated differential prime ideal of a radical differential ideal, introduced in Proposition 24, page 53.

Proposition 29 *Let A be a coherent triangular set of pairwise partially reduced differential polynomials of R, h be the product of its initials and separants and R_1 be the ring of the differential polynomials partially reduced w.r.t. A.*

Then the differential ideal $[A]{:}h^\infty$ is radical and there is a one-to-one correspondence between the associated differential prime ideals $\mathfrak{P}_1,\ldots,\mathfrak{P}_r$ of $[A]:h^\infty$ and the associated prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ of the non-differential ideal $(A):h^\infty$ of R_1. The correspondence is given by $\mathfrak{p}_i=\mathfrak{P}_i\cap R_1$ for $1\leq i\leq r$.

Proof Let f be a differential polynomial such that $f^d \in [A] : h^\infty$ for some $d \geq 0$. Let $g = \mathsf{prem}(f, \Theta^* A)$ where Θ^* denotes the set of all proper derivation operators (so that g is the partial remainder of f by A). Then $g^d \in [A] : h^\infty$. Since g is partially reduced w.r.t. A, Proposition 22 (Rosenfeld's Lemma) applies and $g^d \in (A) : h^\infty$. Since h contains each separant of A as a factor, Proposition 17 (Lazard's Lemma) applies and $g \in (A) : h^\infty$. Therefore, $g \in [A] : h^\infty$ and so does f. The differential ideal $[A] : h^\infty$ is thus radical.

The intersection of a prime ideal of R and the subring $R_1 \subset R$ is a prime ideal of R_1. Therefore, $(A) : h^\infty = \cap_{i=1}^r \mathfrak{p}_i$ where $\mathfrak{p}_i = \mathfrak{P}_i \cap R_1$ is prime for $1 \leq i \leq r$. We thus only need to prove that none of the $\mathfrak{p}_i$ is redundant. We assume $\mathfrak{p}_1$ is redundant and we seek a contradiction by proving that $\mathfrak{P}_1$ is redundant too. Let $f \in \cap_{i=1}^r \mathfrak{P}_i$ and $g = \mathsf{prem}(f, \Theta^* A)$. We have $g \in \cap_{i=2}^r \mathfrak{p}_i$ hence $g \in (A) : h^\infty$ since we have assumed $\mathfrak{p}_1$ is redundant. Therefore, $g \in [A] : h^\infty$, so does f and $\mathfrak{P}_1$ is redundant. □

The following Propositions deal with the notion of zero-divisors in differential residue class rings. Some explanations are provided in Chapter 1.

Proposition 30 *Let A be a coherent triangular set of pairwise partially reduced differential polynomials of R, h be the product of its initials and separants, f be a differential polynomial of R and $g = \mathsf{prem}(f, \Theta^* A)$, where Θ^* denotes the set of proper derivation operators.*

Then f is a zero-divisor in $R/[A] : h^\infty$ if and only if g is a zero-divisor in $R/(A) : h^\infty$.

Proof Let R_1 the ring of the differential polynomials partially reduced w.r.t. A, $\mathfrak{P}$ an associated differential prime of $[A] : h^\infty$ and $\mathfrak{p} = \mathfrak{P} \cap R_1$. By Proposition 29, the prime ideal $\mathfrak{p}$ is an associated prime ideal of $(A) : h^\infty$.

The differential polynomial $f \in \mathfrak{P}$ if and only if $g \in \mathfrak{p}$.

The differential polynomial f is a zero-divisor in $R/[A] : h^\infty$ if and only if f belongs to an associated differential prime ideal of $[A] : h^\infty$.

The differential polynomial g is a zero-divisor in $R/(A) : h^\infty$ if and only if g belongs to an associated prime ideal of $(A) : h^\infty$. □

The following Proposition relies on the notion of iterated resultant, which is introduced in Chapter 3. In the case $m \geq 2$, the set ΘA is not triangular so that the differential polynomial of ΘA to be used for computing a resultant needs not be uniquely defined. In such a case, pick any of the possible differential polynomials.

Proposition 31 *Let A be a regular differential chain, h be the product of the initials and separants of A and f be a differential polynomial of R.*

Then $\mathsf{res}(f, \Theta A) = 0$ if and only if f is a zero-divisor in $R/[A] : h^\infty$.

Proof Decompose $\mathsf{res}(f, \Theta A) = \mathsf{res}(g, A)$ where $g = \mathsf{res}(f, \Theta^* A)$ and Θ^* is the set of proper derivation operators.

Since all elements of $\Theta^* A$ have leading degrees equal to 1, we have $g = \pm\, \mathsf{prem}(f, \Theta^* A)$ (see Corollary 1, page 10). By Proposition 30, f is a zero-divisor in $R/[A] : h^\infty$ if and only if g is a zero-divisor in $R/(A) : h^\infty$. By Proposition 5, page 23 and the fact that $(A) : h^\infty = (A) : (i_1 \cdots i_n)^\infty$, the differential polynomial g is a zero-divisor in $R/(A) : h^\infty$ if and only if $\mathsf{res}(g, A) = 0$. □

7.2 Concluding Remarks

It seems that the term "regular differential chain" was introduced for the first time in [2], by analogy with the regular chains studied in Chapter 3.

There is a relationship with the notion of *characteristic set*, a notion introduced by Ritt [3, I, 5, page 5], then by Kolchin in a restricted case [1, I, 10, page 81]. Let R be a differential polynomial ring endowed with a ranking. Characteristic sets are particular cases of *autoreduced sets* (a notion introduced by Kolchin [1, I, 9, page 77]) i.e. sets of pairwise fully reduced differential polynomials. According to Ritt, a characteristic set of a set $E \subset R$ is an autoreduced subset of E which is minimal, in some sense, among all autoreduced subsets of E. The minimality condition is somewhat complicated but ensures the following target property: if C is a characteristic set of E and f is a nonzero differential polynomial, fully reduced w.r.t. C, then the characteristic sets of $E \cup \{f\}$ are smaller than C. If A is a regular differential chain, then its elements need not be pairwise fully reduced but it is always possible to reduce them without changing their leading derivatives nor their leading degrees. The resulting set is both a regular differential chain and a characteristic set (in Ritt and Kolchin sense) of the differential ideal $[A] : h^\infty$, where h denotes the product of the initials and separants of A. In summary, a regular differential chain A has the same leading derivatives and leading degrees than any characteristic set of the differential ideal $[A] : h^\infty$.

Bibliography

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

[2] François Lemaire. *Contribution à l'algorithmique en algèbre différentielle.* PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, January 2002. (in French).

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

Chapter 8

Normal Forms

Let $R = K\{U\}$ be a differential polynomial ring where K is a differential field of characteristic zero, U is a finite set of differential indeterminates u_k, endowed with a finite set of derivations $\{\delta_1, \ldots, \delta_m\}$. Let Θ denote the multiplicative monoid of derivation operators, generated by the m derivations. Assume the infinite set of derivatives $\Theta\, U$ is ordered w.r.t. a ranking, so that the leading derivative, the initial and the separant of any differential polynomial of $R \setminus K$ are well defined.

Recall that a differential polynomial f is said to partially reduced w.r.t. a differential polynomial p if f does not depend on any proper derivative of the leading derivative of p. In the sequel, A denotes a triangular set of n differential polynomials of $R \setminus K$, pairwise partially reduced. If f is any differential polynomial, then $\mathsf{prem}(f, \Theta\, A)$ denotes the full remainder of f by all the derivatives of A.

According to Definition 5, page 57, a triangular set A of pairwise partially reduced differential polynomials of R is said to be a *regular differential chain* if it satisfies the following conditions:

a the initial i_k of p_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$ for $2 \leq k \leq n$ (algorithmic regular chain criterion);

b the separant s_k of p_k is regular in $R/(A) : (i_1 \cdots i_n)^\infty$ for $1 \leq k \leq n$;

c A is coherent, i.e. all critical pairs of A are solved (meaningful only if $m \geq 2$).

We have not recalled the definition of the *coherence*, which does not play any role in this chapter. See Definition 4, page 44.

Let A be a regular differential chain. Let $\mathfrak{A} = [A] : h^\infty$ (the differential ideal generated by A, saturated by h) where h is the product of the initials and separants of A. Then, given any $f \in R$, we have $\mathsf{prem}(f, \Theta\, A) = 0$ if and only if f is zero in $R/[A] : h^\infty$ (Proposition 28) and $\mathsf{res}(f, \Theta\, A) = 0$ if and only if f is a zero-divisor in $R/[A] : h^\infty$ (Proposition 31).

The regular differential chain A permits to compute *normal forms* of differential polynomials of R and, more generally of differential fractions with denominators regular in $R/[A] : h^\infty$.

Split the set $\Theta\, U$ of the derivatives into $L = \mathrm{ld}\, A$ (the leading derivatives of A) and $N = \Theta\, U \setminus \Theta\, L$ (the set of the derivatives of $\Theta\, U$ which are not derivatives of any element of L). Then $K[N \cup L]$ is the ring of the differential polynomials partially reduced w.r.t. A.

Definition 6 *Let A be a regular differential chain, $L = \mathrm{ld}\, A$ and $N = \Theta U \setminus \Theta L$. Let a be a nonzero differential polynomial of R. An* inverse *of a is any fraction f/g of nonzero differential polynomials such that $f \in K[N \cup L]$ and $g \in K[N]$ and $a\, f = g$ in $R/\mathfrak{A}$.*

Proposition 32 *Let A be a regular differential chain, $L = \mathrm{ld}\, A$ and $N = \Theta U \setminus \Theta L$. Let a be a nonzero differential polynomial of R. A differential polynomial $a \in R$ admits an inverse if and only if a is regular in $R/\mathfrak{A}$.*

Proof Let $b = \mathsf{prem}(a, \Theta^* A)$ be the partial remainder of a by A (where Θ^* is the set of proper derivation operators). By Proposition 30, a is regular in $R/\mathfrak{A}$ if and only if b is regular in $R/\mathfrak{A}$. Moreover, there exists a power product h_a of separants of A such that $h_a\, a = b \mod [A]$. Observe $h_a \in K[N \cup L]$. Let now $g = \mathsf{res}(b, A) = \mathsf{res}(b, \Theta A)$ since b is partially reduced w.r.t. A. By Proposition 31, b is regular in $R/\mathfrak{A}$ if and only if $g \neq 0$. Observe $g \in K[N]$. Using Proposition 12, page 27, we see that there exists a differential polynomial $u \in K[N \cup L]$ such that $u\, b = g \mod (A)$. Therefore a is regular in $R/\mathfrak{A}$ if and only if there exists a differential polynomial $f = h_a\, u \in K[N \cup L]$ and a nonzero differential polynomial $g \in K[N]$ such that $a\, f = g \mod [A]$ i.e. an inverse f/g of a. □

The proof of the above Proposition actually provides an algorithm for computing an inverse of a whenever it exists. One may also use the algorithm `AlgebraicInverseNonZero` given in Figure 3.1, page 30, instead of computing the resultant. A feature of this variant is that the inverse computation may fail even if the inverse exists, exhibiting a factorization of some element of A.

Definition 7 *Let A be a regular differential chain, $L = \mathrm{ld}\, A$ and $N = \Theta U \setminus \Theta L$. Let a/b be a differential fraction, with b regular in $R/\mathfrak{A}$. A* normal form *of a/b modulo A is any differential fraction f/g such that*

1 *f is fully reduced with respect to A ;*

2 *g belongs to $K[N]$ (and is thus regular in $R/\mathfrak{A}$),*

3 *$a/b = f/g$ in $R/\mathfrak{A}$.*

Proposition 33 *Let a/b be a differential fraction, with b regular in $R/\mathfrak{A}$. The normal form f/g of a/b exists and is unique. In particular,*

4 *a is zero in $R/\mathfrak{A}$ if and only if its normal form is zero ;*

5 *f/g is a canonical representative of the residue class of a/b in the total quotient ring of $R/\mathfrak{A}$.*

Moreover,

6 *each irreducible factor of g divides the denominator of an inverse of b, or of some initial or separant of A .*

Proof One first proves the uniqueness of the normal form. Assume f'/g' is another normal form of a/b. Then, by **3**, $f/g = f'/g'$ in $R/\mathfrak{A}$, which implies that $f\, g' - f'\, g$ is zero in $R/\mathfrak{A}$. By **1** and **2**, we have $\mathsf{prem}(f\, g' - f'\, g, \Theta A) = f\, g' - f'\, g$. By Proposition 28 we then have $f\, g' - f'\, g = 0$. The two fractions are thus equal.

function NF $(a/b,\ A)$
Parameters
a/b *is a differential fraction with* $a,\ b \in R$.
$A = \{p_1, \ldots, p_n\}$ *is a regular differential chain, defining a differential ideal* $\mathfrak{A}$.
Result
the normal form of a/b *modulo* A *or an error.*
begin
$z_\mathrm{b}/t_\mathrm{b} :=$ an inverse of b modulo A
$(f_{n+2},\ g_{n+2}) := (z_\mathrm{b}\, a,\ t_\mathrm{b})$
$z_i/t_i :=$ an inverse of each separant s_i of A
using Ritt's partial reduction algorithm, compute $d_1, \ldots, d_n \in \mathbb{N}$ and
$$r_{n+1} \in K[N \cup L] \text{ such that } s_1^{d_1} \cdots s_n^{d_n}\, f_{n+2} \equiv r_{n+1} \mod \mathfrak{A}$$
$f_{n+1} := z_1^{d_1} \cdots z_n^{d_n}\, r_{n+1}$
$g_{n+1} := t_1^{d_1} \cdots t_n^{d_n}\, g_{n+2}$
denote $v_i = \mathrm{ld}\, p_i$ $(1 \leq i \leq n)$ and assume $v_n > \cdots > v_1$
for ℓ from n to 1 by -1 do
$r_\ell :=$ prem$(f_{\ell+1},\ p_\ell,\ v_\ell)$
let i_ℓ denote the initial of p_ℓ
let $d_\ell \in \mathbb{N}$ be such that $i_\ell^{d_\ell}\, f_{\ell+1} \equiv r_\ell \mod (p_\ell)$
$z_\ell/t_\ell :=$ an inverse of i_ℓ modulo A
$f_\ell := z_\ell^{d_\ell}\, r_\ell$
$g_\ell := t_\ell^{d_\ell}\, g_{\ell+1}$
od
return f_1/g_1
the rational fraction may be reduced by means of a gcd computation
of multivariate polynomials over the field K
end

Figure 8.1: The NF function.

The NF algorithm in Figure 8.1 returns a fraction. To prove the existence of the normal form, it is sufficient to prove that the fraction returned by the NF algorithm in Figure 8.1 satisfies **1**, **2** and **3**.

1. The differential polynomial r_{n+1} is a partial remainder. It is thus partially reduced with respect to A. The differential polynomials $z_1, \ldots, z_n$ lie in $K[N \cup L]$ i.e. are partially reduced w.r.t. A. Thus f_{n+1} is partially reduced w.r.t. A. Let now $n \geq \ell \geq 1$ be a loop index. Assume $f_{\ell+1}$ is partially reduced w.r.t. A and $\deg(f_{\ell+1},\ v_k) < \deg(p_k,\ v_k)$ for each $n \geq k > \ell$. Consider the sequence of instructions of the loop body. After the pseudodivision, we have $\deg(r_\ell,\ v_\ell) < \deg(p_\ell,\ v_\ell)$. Moreover, since $\deg(i_\ell,\ v_\ell) = 0$, we have $\deg(z_\ell,\ v_\ell) = 0$. Thus f_ℓ is partially reduced w.r.t. A and, using the fact that p_ℓ does not depend on $v_{\ell+1}, \ldots, v_n$, one has $\deg(f_\ell,\ v_k) < \deg(p_k,\ v_k)$ for each $n \geq k \geq \ell$. Putting the above argument in an inductive proof, one sees that $f = f_1$ is partially reduced w.r.t. A and $\deg(f_1,\ v_k) < \deg(p_k,\ v_k)$ for each $n \geq k \geq 1$ i.e. that f is fully reduced w.r.t. A.

2. One actually proves **6**, which implies **2**. All the differential polynomials g_i are products of

denominators of inverses of b and of the initials and separants of A. They belong to $K[N]$. The final reduction may simply remove some factors of g_1.

3. At the beginning of the function, $a/b = f_{n+2}/g_{n+2}$ in $R/\mathfrak{A}$. After the partial reduction step,

$$\frac{a}{b} \;=\; \frac{f_{n+2}\, s_1^{d_1} \cdots s_n^{d_n}\, z_1^{d_1} \cdots z_n^{d_n}}{g_{n+2}\, s_1^{d_1} \cdots s_n^{d_n}\, z_1^{d_1} \cdots z_n^{d_n}} \quad \text{in } R/\mathfrak{A}\,.$$

Simplify $s_1^{d_1} \cdots s_n^{d_n}\, f_{n+2}$ as r_{n+1} and each product $s_i\, z_i$ as t_i. One sees that $a/b = f_{n+1}/g_{n+1}$ in $R/\mathfrak{A}$. Let now $n \geq \ell \geq 1$ be a loop index, consider the sequence of instructions of the loop body and assume that $a/b = f_{\ell+1}/g_{\ell+1}$ in $R/\mathfrak{A}$. After the pseudodivision step,

$$\frac{a}{b} \;=\; \frac{f_{\ell+1}\, i_\ell^{d_\ell}\, z_\ell^{d_\ell}}{g_{\ell+1}\, i_\ell^{d_\ell}\, z_\ell^{d_\ell}} \quad \text{in } R/\mathfrak{A}\,.$$

Simplify $i_\ell^{d_\ell}\, f_{\ell+1}$ as r_ℓ and each product $i_\ell\, z_\ell$ as t_ℓ. One sees that $a/b = f_\ell/g_\ell$ in $R/\mathfrak{A}$. Putting the above argument in an inductive proof, **3** is proved.

This concludes the proof of the existence of the normal form. One proceeds with the three last points.

4. It follows from the uniqueness, **3** and the fact that 0 is a normal form.

5. It follows from **3** and the uniqueness of normal forms.

6. It was proved in **2**, above. □

Proposition 34 *Let a/b and a'/b' be two differential fractions with b and b' regular in $R/\mathfrak{A}$. Denote f/g and f'/g' their normal forms. Then*

(i) $\mathtt{NF}\left(\dfrac{a}{b} + \dfrac{a'}{b'}\,,\, A\right) = \dfrac{f}{g} + \dfrac{f'}{g'}\,,$

(ii) $\mathtt{NF}\left(\dfrac{a}{b} \cdot \dfrac{a'}{b'}\,,\, A\right) = \mathtt{NF}\left(\dfrac{f}{g} \cdot \dfrac{f'}{g'}\,,\, A\right),$

(iii) $\mathtt{NF}\left(\theta\left(\dfrac{a}{b}\right),\, A\right) = \mathtt{NF}\left(\theta\left(\dfrac{f}{g}\right),\, A\right)$ *for each derivation operator θ. Moreover, each irreducible factor of the denominator of this rational differential fraction divides the denominator of an inverse of b, or of some initial or separant of A.*

Proof **(i)**. The differential fraction on the right hand-side is $(f\, g' + f'\, g)/(g\, g')$. The numerator is reduced w.r.t. A and the denominator $g\, g' \in K[N]$. It is thus a normal form. Equality follows from the uniqueness.

(ii). It follows from Definition 7, **3** and the uniqueness normal forms.

(iii). The first statement follows from Definition 7, **3** and the uniqueness of normal forms. The second statement follows from Proposition 33, **6**. □

8.1 Concluding Remarks

This chapter owes a lot to [1] and [2].

Bibliography

[1] 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.

[2] François Boulier, François Lemaire, and Alexandre Sedoglavic. On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains. In *Proceedings of Computer Algebra in Scientific Computing, LNCS 6885*, pages 61–72, Kassel, Germany, 2011. `http://hal.archives-ouvertes.fr/hal-00599440`.

Chapter 9

The RosenfeldGroebner Algorithm

The version described here is quite close to the one implemented in the BLAD libraries [1], which is called by the `RosenfeldGroebner` function of the MAPLE package. The algorithm first computes *regular differential systems* (Definition 8), which are differential systems of polynomial equations and inequations $A = 0$, $S \neq 0$ over which Proposition 22 (Rosenfeld's Lemma) and Proposition 17 (Lazard's Lemma) apply. The set A is then converted into regular chains (hence regular differential chains), by a non-differential algorithm.

Let $R = K\{U\}$ be a differential polynomial ring where K is a differential field of characteristic zero, U is a finite set of differential indeterminates u_k, endowed with a finite set of derivations $\{\delta_1, \ldots, \delta_m\}$. Let Θ denote the multiplicative monoid of derivation operators, generated by the m derivations. Assume the infinite set of derivatives $\Theta\, U$ is ordered w.r.t. a ranking, so that the leading derivative, the initial and the separant of any differential polynomial of $R \setminus K$ are well defined.

Recall that a differential polynomial f is said to partially reduced w.r.t. a differential polynomial p if f does not depend on any proper derivative of the leading derivative of p. In the sequel, A denotes a triangular system of differential polynomials of $R \setminus K$, pairwise partially reduced. If f is any differential polynomial, then $\mathsf{prem}(f, \Theta\, A)$ denotes the full remainder of f by all the derivatives of A.

In the case $m \geq 2$, the set A may involve critical pairs i.e. pairs $\{p_1, p_2\} \subset A$ such that the leading derivatives $\theta_1\, u$ of p_1 and $\theta_2\, u$ of p_2 are derivatives of some same differential indeterminate u. Define $\theta_{12} = \mathrm{lcm}(\theta_1, \theta_2)$ and the Δ-polynomial associated to the pair as

$$\Delta(p_1, p_2) \quad = \quad s_1 \, \frac{\theta_{12}}{\theta_2} \, p_2 - s_2 \, \frac{\theta_{12}}{\theta_1} \, p_1 \, ,$$

where s_1, s_2 are the separants of p_1, p_2. The critical pair is said to be solved if

$$\mathsf{prem}(\Delta(p_1, p_2), \Theta\, A) \quad = \quad 0$$

The set A is said to be coherent if all its critical pairs are solved.

Definition 8 *(regular differential system)*
A regular differential system *is a system $A = 0$, $S \neq 0$ of differential polynomial equations and inequations of R such that*

- *A is a triangular set of differential polynomials, pairwise partially reduced;*

- *S contains the initials and separants of A and only involves differential polynomials partially reduced w.r.t. A;*
- *A is coherent i.e. all critical pairs of A are solved (meaningful only if $m \geq 2$).*

The following proposition collects some important properties of regular differential systems.

Proposition 35 *Let $A = 0$, $S \neq 0$ be a regular differential system, h denote the product of the elements of S and f be any differential polynomial of R. Then*

1. *the ideal $(A) : h^\infty$ is radical;*
2. *the differential ideal $[A] : h^\infty$ is radical;*
3. *The differential polynomial f is zero in $R/[A] : h^\infty$ if and only if $\mathsf{prem}(f, \Theta^* A)$ is zero in $R/(A) : h^\infty$, where Θ^* denotes the set of all proper derivation operators;*
4. *The differential polynomial f annihilates over every solution of the regular differential system if and only if $f \in [A] : h^\infty$.*

Since A is not a regular chain, it is possible that $[A] : h^\infty = R$. This is the case if and only if $(A) : h^\infty = R$ (by Rosenfeld's Lemma). If this happens, the system is said to be *inconsistent*.

9.1 An Ordinary Differential Example

Consider the following system of the differential polynomial ring $R = \mathbb{Q}\{u, v\}$ endowed with a single derivation δ_x.

$$(\Sigma_1) \qquad u_{xx} + v = 0, \quad u_x^2 + v = 0.$$

Let us fix the ranking such that $u \gg v$ which eliminates u and its derivatives. Leading derivatives are then u_{xx} and u_x. The first equation is not partially reduced w.r.t. the second one. To reduce it, proceed as follows: differentiate twice the second equation

$$2\, u_x\, u_{xx} + v_x = 0$$

and replace u_{xx} by $-v_x/(2\, u_x)$ in the first one, which yields

$$-\frac{v_x}{2\, u_x} + v = 0.$$

Then replace the first equation by the reduced one or, more precisely, by its numerator. Let us split cases, pose that $u_x \neq 0$ and consider separately the solutions of (Σ_1) which annihilate u_x. One gets

$$(\Sigma_2) \qquad u_{xx} + v = 0, \quad u_x^2 + v = 0, \quad u_x = 0$$

and

$$(\Sigma_3) \qquad 2\, v\, u_x - v_x = 0, \quad u_x^2 + v = 0, \quad u_x \neq 0.$$

Consider (Σ_2). Plug the third equation in the second one and its first derivative in the first equation. One gets $v = 0$. This system then simplifies to a regular differential system

$$(\Sigma_4) \qquad u_x = 0, \quad v = 0$$

whose solutions are $u(x) = c$ and $v(x) = 0$, where c is an arbitrary constant. System (Σ_4) is a regular differential chain. Let us now come back to (Σ_3). The two first equations have the same leading derivtaive. This system is thus not triangular. Let us apply Ritt's reduction algorithm as follows: replace u_x by $v_x/(2\,v)$ in the second equation. This gives

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

Take the numerator, provided that $v \neq 0$ and consider separately the solutions of (Σ_3) which annihilate v. One gets a new splitting.

$$(\Sigma_5) \qquad 2\,v\,u_x - v_x = 0, \quad u_x^2 + v = 0, \quad v = 0, \quad u_x \neq 0$$

and

$$(\Sigma_6) \qquad 2\,v\,u_x - v_x = 0, \quad v_x^2 + 4\,v^3 = 0, \quad u_x \neq 0, \quad v \neq 0.$$

Consider (Σ_5). Simplifying, one gets

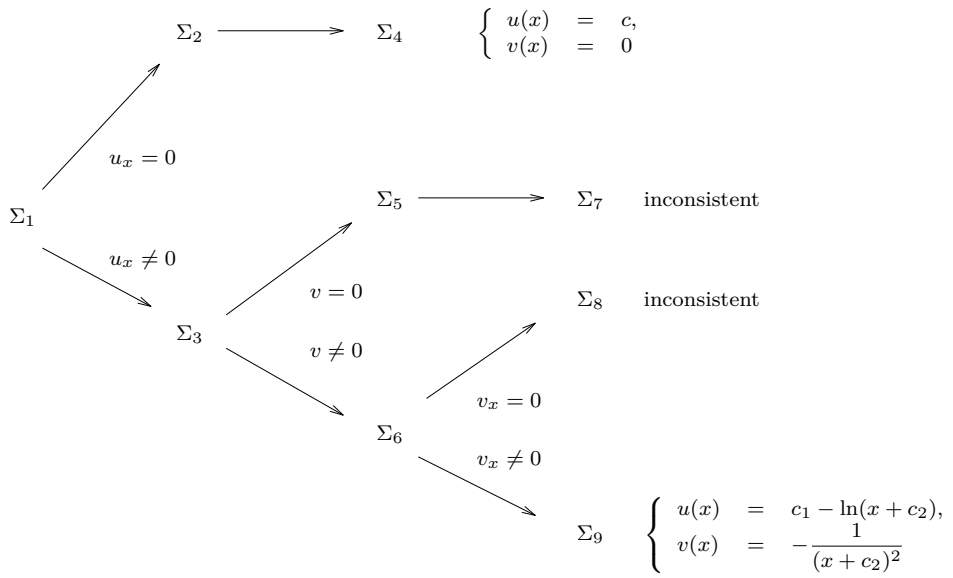
$$(\Sigma_7) \qquad u_x^2 = 0, \quad v = 0, \quad u_x \neq 0.$$

It is a regular differential system. An algorithm such as `regCharacteristic` can then be applied. By means of a gcd computation between $u_x^2 = 0$ and $u_x \neq 0$, it proves that the system is inconsistent. Come back to (Σ_6). It is not yet a regular differential system because the separant $2\,v_x$ of the second equation does not belong to the inequation set. Perform another splitting and consider separately the solutions of (Σ_6) which annihilate v_x from the ones which do not annihilate it. One gets

$$(\Sigma_8) \qquad 2\,v\,u_x - v_x = 0, \quad v_x^2 + 4\,v^3 = 0, \quad v_x = 0, \quad u_x \neq 0, \quad v \neq 0.$$

$$(\Sigma_9) \qquad 2\,v\,u_x - v_x = 0, \quad v_x^2 + 4\,v^3 = 0, \quad v_x \neq 0, \quad u_x \neq 0, \quad v \neq 0.$$

Argumenting as for (Σ_7), one sees that (Σ_8) is inconsistent. System (Σ_9) is a regular differential system. Its equation set even forms a regular differential chain. We can then drop the inequation $u_x \neq 0$ which is not an initial nor a separant of the chain. The solutions of (Σ_9) are $u(x) = c_1 - \ln(x + c_2)$ and $v(x) = -1/(x + c_2)^2$ where c_1 and c_2 are arbitrary constants. Here is a summary of the computations.



Every solution of (Σ_1) is a solution of (Σ_4) or of (Σ_9) and conversely. By Proposition 26, we have

$$\sqrt{[u_{xx}+v,\, u_x^2+v]} = [u_x,\, v] \cap [2\,v\,u_x - v_x,\; v_x^2 + 4\,v^3] : (v\,v_x)^\infty.$$

By Proposition 28, a differential polynomial f belongs to $\sqrt{[\Sigma_1]}$ if and only if it is reduced to zero by both (Σ_4) and (Σ_9). This is the case for $f = v_{xx} + 6\,v^2$.

9.2 An Example with Partial Derivatives

Consider the system $\{f_1,\, f_2,\, f_3\}$ from the differential polynomial ring $\mathbb{Q}\{u, v\}$ endowd with the two derivations δ_x and δ_y.

$$(\Sigma_1) \qquad u_y^2 - 4\,u = 0, \quad u_x - v_x\,u = 0, \quad v_y = 0.$$

Let us fix the following ranking:

$$\cdots > u_{xx} > u_{xy} > u_{yy} > v_{xx} > v_{xy} > v_{yy} > u_x > u_y > v_x > v_y > u > v.$$

The leading derivatives are then u_y, u_x and v_y. The system is then triangular and its elements are pairwise partially reduced. Is it coherent? The two first equations form a critical pair $\{f_1,\, f_2\}$. Form

$$\Delta(f_1,\, f_2) = 2\,u\,u_y\,v_{xy} + 2\,u_y^2\,v_x - 4\,u_x.$$

Reduce it by (Σ_1). One gets a fourth equation $f_4 = u\,v_x = 0$ that we add to the system:

$$(\Sigma_2) \qquad u_y^2 - 4\,u = 0, \quad u_x - v_x\,u = 0, \quad v_y = 0, \quad u\,v_x = 0.$$

The former critical pair $\{f_1,\, f_2\}$ is now solved. However, the new critical pair $\{f_3,\, f_4\}$ arises. Before forming the Δ-polynomial, let us split cases on the initial of f_4 and consider separately the solutions of (Σ_2) which annihilate u from the ones which do not annihilate it. One gets

$$(\Sigma_3) \qquad u_y^2 - 4\,u = 0, \quad u_x - v_x\,u = 0, \quad v_y = 0, \quad u\,v_x = 0, \quad u = 0$$

and

$$(\Sigma_4) \qquad u_y^2 - 4\,u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u \neq 0.$$

System (Σ_3) simplifies to

$$(\Sigma_5) \qquad v_y = 0, \quad u = 0$$

which constitutes a regular differential system and, even, a regular differential chain. Its solutions are $u(x,\, y) = 0$ and $v(x,\, y) = \varphi(x)$ where $\varphi(x)$ is an arbitrary function of x.

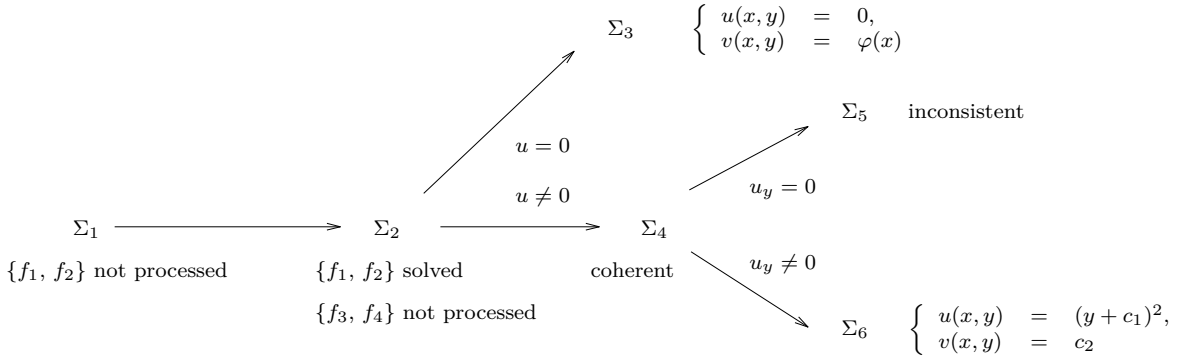
Consider system (Σ_4). The critical pair $\{f_1,\, f_2\}$ is solved. The critical pair $\{f_3,\, f_4\}$ is solved also since $\Delta(f_3,\, f_4) = 0$. This system is thus coherent. It is not yet a regular differential system for the separant u_y of f_1 does not belong to the inequation set. Let us split cases:

$$(\Sigma_5) \qquad u_y^2 - 4\,u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u_y = 0, \quad u \neq 0$$

and

$$(\Sigma_6) \qquad u_y^2 - 4\,u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u_y \neq 0, \quad u \neq 0.$$

System (Σ_5) is inconsistent. The new equation $u_y = 0$ permits to simplify the first one and obtain $u = 0$, which contradicts the inequation $u \neq 0$. The system (Σ_6) is a regular differential system. Its equation set form a regular differential chain. An algorithm such as `regCharacteristic` permits to prove that the inequation $u \neq 0$, which is not an initial or a separant of the chain, is regular modulo the ideal defined by the chain. It is thus discarded. The solutions of (Σ_6) are $u(x, y) = (y + c_1)^2$ and $v(x, y) = c_2$ where c_1 and c_2 are arbitrary constants. Here is a summary of the computations.



Every solution of (Σ_1) is a solution of (Σ_3) or of (Σ_6), and conversely. As in the ordinary case, we have

$$\sqrt{[u_y^2 - 4\,u,\, u_x - v_x\,u,\, v_y]} = [u,\, v_y] \cap [u_y^2 - 4\,u,\, u_x,\, v_y,\, v_x] : (u_y)^\infty.$$

One also sees that u and v_x do not belong to the radical of the differential ideal generated by Σ_1 while their product does. This ideal is thus not prime.

9.3 Pseudo-Code

The following function gathers as input a system of differential polynomial equations and inequations $A_0 = 0,\ S_0 \neq 0$ as well as a ranking $\mathscr{O}$. It returns a list of regular differential chains $A_1, \ldots, A_t$ such that (denoting h_0 the product of elements of S_0 and h_k the product of the initials and separants of A_k, for $1 \leq k \leq t$)

$$\sqrt{[A_0] : h_0^\infty} \quad = \quad [A_1] : h_1^\infty \cap \cdots \cap [A_t] : h_t^\infty\,.$$

When still being processed a system is a quadruple $\langle A,\, D,\, P,\, S\rangle$ where A is (somewhat) the set of the already processed equations, D is the set of critical pairs to be processed, P is the set of the equations to process and S is the set of the inequations.

The function relies on two sub-algorithms: the function `complete`, given afterwards and the function `regCharacteristic`, which transforms a regular differential system as a possibly empty intersection of differential ideals presented by regular differential chains. This function is completely non-differential. It relies on the ideas sketched in Chapter 3 and is detailed in [3].

Splittings are handled through a list `toDo` of quadruples to be processed and a liste `Done` of regular differential chains. The two insertions of quadruples performed before `complete` is called correspond to splittings. The first one correspond to the case of the vanishing of the initial of f. The second one corresponds to the case of the non-vanishing of the initial, and the vanishing of the separant. The `complete` function covers the case of the non-vanishing of both the initial and the separant of f.

```
function RosenfeldGroebner (A_0, S_0, 𝒪)
begin
  toDo := [⟨∅, ∅, A_0, S_0⟩]
  Done := []
  while toDo is not empty do
    Pick a quadruple ⟨A, D, P, S⟩ from toDo
    if D = P = ∅ then
      Make all elements of A pairwise partially reduced
      if this operation did not change leading derivatives nor leading degrees then
        Make the elements of S partially reduced w.r.t. A
        Append to Done the regular differential chains obtained by applying
                    regCharacteristic over A = 0, S ≠ 0
      fi
    else
      if P ≠ ∅ then
        Pick a differential polynomial f from P
      else
        Pick a critical pair {p_1, p_2} from D
        f := Δ(p_1, p_2)
      fi
      g := prem(f, Θ A)
      if g = 0 then
        Append ⟨A, D, P, S⟩ to toDo
      elif g ∉ K
        Let v be the leading derivative, d the leading degree,
                    i the initial and s the separant of g
        g_i := g − i v^d
        g_s := d g − v s
        Append ⟨A, D, P ∪ {i, g_i}, S⟩ to toDo
        Append ⟨A, D, P ∪ {s, g_s}, S ∪ {i}⟩ to toDo
        Append complete (⟨A, D, P, S⟩, g) to toDo
      fi
    fi
  od
  return Done
end
```

9.3.1 The `complete` Subalgorithm

The `complete` function inserts the new equation $g \notin K$ in the list A. We want to keep the set of leading derivatives of A pairwise partially reduced. We thus remove from A every differential polynomial f whose leading derivative is a derivative of the one of g. Removed equations are not lost: they are elements of critical pairs of D. Observe that, according to Definition 2, page 43, some of the critical pairs may not define a Δ-polynomial. In the implementation of the `RosenfeldGroebner` (and in the MAPLE package), the definition of Δ-polynomials was generalized to cover this case.

```
function complete (⟨A, D, P, S⟩, f)
begin
  Ā := the union of {g} and the set of the elements of A whose leading derivatives
            are not a derivative of the one of g
  D̄ := the union of D and the set of all critical pairs that can be formed between g
            and any element of A
  P̄ := P
  S̄ := the union of S and the initial and the separant of g
  return ⟨Ā, D̄, P̄, S̄⟩
end
```

9.3.2 The `regCharacteristic` Subalgorithm

It is a non-differential algorithm essentially applying the ideas given in Chapter 3 and, in particular, the algorithms given in Figures 3.1, page 30 and 3.2, page 31.

The input is a regular differential system $A_0 = 0$, $S_0 \neq 0$. The output is a possibly empty set of regular differential chains $A_1, \ldots, A_r$ such that

$$(A_0) : h_0^\infty \quad = \quad \cap_{i=1}^r (A_i) : h_i^\infty$$

where h_0 is the product of the elements of S_0 and h_i is the product of the initials and separants of A_i for $1 \leq i \leq r$. The algorithm ultimately relies on Proposition 4. Denote $A_0 = \{p_1, \ldots, p_n\}$. All computations are performed in $R_0 = K_0[x_1, \ldots, x_n]$ where x_i is the leading derivative of p_i and K_0 is the field obtained by moving all other derivatives in the ground field of the equations.

The algorithm builds a sequence of sets $(\mathscr{F}_i)$ as follows. Initially, $\mathscr{F}_0 = \{(A_0 = 0, S_0 \neq 0)\}$. Assume $\mathscr{F}_i = \{(A_1 = 0, S_1 \neq 0), \ldots, (A_t = 0, S_t \neq 0)\}$. Two cases may arise:

1. each A_i is monic and each S_i is empty, for $1 \leq i \leq t$. Then, after clearing denominators, return $\{A_1, \ldots, A_t\}$;

2. there exists some $A = 0$, $S \neq 0$ in $\mathscr{F}_i$ such that A contains some non-monic polynomial or S is not empty. Then apply one of the rules **R1** or **R2** over $A = 0$, $S \neq 0$, giving a possibly empty set $\bar{\mathscr{F}}$. Define $\mathscr{F}_{i+1} = \mathscr{F}_i \setminus \{(A = 0, S \neq 0)\} \cup \bar{\mathscr{F}}$.

R1: try to make a polynomial monic. This rule applies if there exists some non-monic polynomial $p_k \in A$ such that $p_1, \ldots, p_{k-1} \in A$ are monic. Three cases may arise:

1. the initial of p_k is zero in $R_0/(p_1, \ldots, p_{k-1})$ (see Proposition 5). Then $\bar{\mathscr{F}} = \varnothing$;

2. an inverse of the initial of p_k in $R_0/(p_1, \ldots, p_{k-1})$ could be computed by the algorithm `AlgebraicInverseNonZero` given in Figure 3.1. Then $\bar{\mathscr{F}} = \{(A' = 0, S \neq 0)\}$ where A' is obtained from A by making p_k monic, using the inverse;

3. the algorithm `AlgebraicInverseNonZero` raised the exception "inversion of a zero-divisor" and returned a triple (j, f, g) such that $1 \leq j < k$ and $p_j = f\,g$ in $R_0/(p_1, \ldots, p_{j-1})$. Then $\bar{\mathscr{F}} = \{(A_f, S \neq 0), (A_g, S \neq 0)\}$ where $A_f = A \setminus \{p_j\} \cup \{f\}$ and $A_g = A \setminus \{p_j\} \cup \{g\}$.

R1: try to get rid of an inequation. This rule applies if there exists some $s \in S$ such that the leading variable of s is x_k and $p_1, \ldots, p_k \in A$ are monic. Three cases may arise:

1. s is zero in $R_0/(p_1, \ldots, p_k)$ (see Proposition 5). Then $\bar{\mathscr{F}} = \varnothing$;
2. an inverse of s in $R_0/(p_1, \ldots, p_k)$ could be computed by the algorithm `AlgebraicInverseNonZero` given in Figure 3.1. Then $\bar{\mathscr{F}} = \{(A = 0,\ S' \neq 0)\}$ where $S' = S \setminus \{s\}$;
3. the algorithm `AlgebraicInverseNonZero` raised the exception "inversion of a zero-divisor" and returned a triple (j, f, g) such that $1 \leq j < k$ and $p_j = f\,g$ in $R_0/(p_1, \ldots, p_{j-1})$. Then $\bar{\mathscr{F}} = \{(A_f,\ S \neq 0),\ (A_g,\ S \neq 0)\}$ where $A_f = A \setminus \{p_j\} \cup \{f\}$ and $A_g = A \setminus \{p_j\} \cup \{g\}$.

Proposition 36 *The `regCharacteristic` algorithm terminates.*

Proof If all inverse computations succeed, the termination is clear. Each time a zero-divisor is exhibited, the triangular set A is split in two triangular sets, obtained by replacing a polynomial of A by two polynomials with strictly lower leading degrees. Cases can thus only be split finitely many times. □

9.3.3 Termination Proof

Proposition 37 *The `RosenfeldGroebner` function terminates.*

Proof Every infinite locally finite tree involves a branch of infinite length (König's Lemma). Locally finite means that finitely many edges start from each node.

The function builds a locally finite tree of quadruples. It is thus sufficient to prove that no branch has infinite length.

The call to `complete` modifies A. Using essentially the arguments developed in Proposition 19, page 41 (Dickson's Lemma), it is possible to prove that it can only be called finitely many times. This function is the only one to enlarge D. In all branches of the tree, the list D thus remains finite and we can slightly cheat, assume D does not exist and that all Δ-polynomials are present in P from the beginning.

The two other operations which are likely to generate a quadruple consist in extracting a differential polynomial f from P and to replace them by at most two differential polynomials which have either lower leading derivative or same leading derivative and lower leading degree than f. By Proposition 19, these operations can only be performed finitely many times.

Eventually, the `regCharacteristic` algorithm is performed finitely many times. Each call terminates by Proposition 36. □

9.4 Concluding Remarks

This chapter owes a lot to [2, chapter 9]. The `regCharacteristic` algorithm is borrowed from [3].

An analogue of Buchberger's second criterion to avoid useless critical pairs does exist. Some further efficient criteria are presented in [2, section 9.5].

By applying a primary decomposition algorithm over each regular differential chain, one would obtain a representation of the radical of the differential ideal defined by the input system as a finite intersection of prime differential ideals. However, this intersection does not need to be irredundant

and the problem of computing an irredundant decomposition is theoretically wide open. See[1] [4, IV, 9, page 166].

In non-differential algebra, the principal ideal theorem permits to cut some branches in the splitting tree. Indeed, if the input system involves n equations then every regular chain that involves more than n equations is necessarily redundant. The argument is a dimension-theoretic one. In differential algebra, we only know that if the input system involves a single equation, then every regular differential chain that involves more than one equation is necessarily redundant [4, IV, 14, Theorem 5, page 185]. This result is part of the Low Power Theorem. See [5, III, 1, page 57] or [4, IV, 15, Theorem 6, page 187]. The general case is wide open and is one of the questions for investigation stated by Ritt [5, Appendix, 10, page 178]. In the MAPLE package, the interface of the `RosenfeldGroebner` function permits the user to assume the conjecture holds. By default, the conjecture is assumed not to hold.

Bibliography

[1] François Boulier. The BLAD libraries. `http://www.lifl.fr/~boulier/BLAD`.

[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. 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`.

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

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

[1] Kolchin's book mentions *characteristic sets* and *autoreduced sets*. A characteristic set of a prime differential ideal $\mathfrak{P}$ is a regular differential chain A such that $\mathfrak{P} = [A] : h^\infty$ where h is the product of the initials and separants of A. An autoreduced set is a particular case of a triangular set of pairwise partially reduced differential polynomials.

Chapter 10

The Henri-Michaelis-Menten Formula

Final models do not require any deep ideal theory but intermediate, temporary models do.

In this chapter, one considers models designed as systems of parametric — every model is parametric — ordinary differential equations. Final models, the ones which occur in books, are usually very simple, from an ideal-theoretic point of view. However, on the long path leading to the final model, the modeler may need to study the consequences of various hypotheses, which can sometimes be formulated as equations. The investigation of these intermediate, temporary models, that book readers usually do not see, may actually require a much more intrincated ideal theory.

This chapter develops such an example. It owes a lot to [3]. It shows that the famous Henri-Michaelis-Menten formula [4, 7] can be obtained by encoding the hypotheses which lead to it as differential equations and simplifying them through a differential elimination process.

We start with the following chemical reaction system. It describes the transformation of a substrate S into a product P, in the presence of some enzyme E. An intermediate complex C is formed.

$$E + S \underset{k_{-1}}{\overset{k_1}{\rightleftarrows}} C \xrightarrow{k_2} E + P\,. \tag{10.1}$$

It is interesting to note that a chemical reaction system may be endowed with at least eight dynamics: the state space may be discrete or continuous, the time may be discrete or continuous, and the evolution rules may be deterministic or stochastic. See [8]. These eight dynamics have something in common, which is provided by a graph such as (10.1) and could be summarized in the stoichiometry matrix of the system. See [5] for more details on the informations that can be extracted from the stoichiometry matrix.

In this chapter, we focus on the case of a continuous state space, continuous time, and deterministic evolution (the deterministic model). The symbols k_1, k_{-1}, k_2 then denote reaction rates and are considered as parameters.

The sought Henri-Michaelis-Menten formula is Formula (10.2). It features two parameters $V_{\max}$ and K which are rational functions of k_1, k_{-1}, k_2.

$$\frac{\mathrm{d}S}{\mathrm{d}t}(t) = -\frac{V_{\max}\, S(t)}{K + S(t)} \tag{10.2}$$

Let us first build the deterministic model of (10.1) using the mass-action law. The four functions correspond to the concentrations of the corresponding chemical species. The matrix `N` is the stoichiometry matrix.

```
> with (LinearAlgebra):
> X := <E(t), S(t), C(t), P(t)>:
> V := <k[1]*E(t)*S(t), k[-1]*C(t), k[2]*C(t)>:
> N := <<-1, -1, 1, 0> | <1, 1, -1, 0> | <1, 0, -1, 1>>:
> X, N, V;
                    [E(t)]  [-1     1     1]
                    [    ]  [              ]  [k[1] E(t) S(t)]
                    [S(t)]  [-1     1     0]  [              ]
                    [    ], [              ], [  k[-1] C(t)  ]
                    [C(t)]  [ 1    -1    -1]  [              ]
                    [    ]  [              ]  [  k[2] C(t)   ]
                    [P(t)]  [ 0     0     1]
```

Here is a first formulation of the dynamical system.

```
> madm := map (diff, X, t) = N . V;
                  [d      ]
                  [-- E(t)]
                  [dt     ]
                  [       ]
                  [d      ]   [-k[1] E(t) S(t) + k[-1] C(t) + k[2] C(t)]
                  [-- S(t)]   [                                        ]
                  [dt     ]   [      -k[1] E(t) S(t) + k[-1] C(t)      ]
          madm := [       ] = [                                        ]
                  [d      ]   [k[1] E(t) S(t) - k[-1] C(t) - k[2] C(t) ]
                  [-- C(t)]   [                                        ]
                  [dt     ]   [               k[2] C(t)                ]
                  [       ]
                  [d      ]
                  [-- P(t)]
                  [dt     ]
```

This is a final model. The differential ideal generated by these polynomial differential equations is prime. Differential algebra is not useful here.

10.1 An Overly Simplifying Assumption

For a while, one could read in the *Wikipedia* that the Henri-Michaelis-Menten formula could be obtained by assuming that the rate change of the complex $C(t)$ is zero. In the web page, the authors started to use this assumption in their proof and then carefully forgot it, because it actually leads to a useless system.

The `RosenfeldGroebner` function permits to represent the radical $\mathfrak{A}$ of the differential ideal generated by a given input system as a finite intersection of differential ideals, presented by regular differential chains. By the differential Nullstellensatz (Proposition 25, page 53), $\mathfrak{A}$ can be viewed as the set of all the equations that are consequences of the input system.

```
> with(DifferentialAlgebra);
```

Let us now define a differential polynomial ring, endowed with the ranking

$$(\text{the derivatives of } C, E, P, S) \gg (\text{the parameters } k_1, k_{-1}, k_2)\,.$$

```
> R :=  DifferentialRing
      (blocks = [[C,E,P,S], [k[1](),k[-1](),k[2]()]], derivations = [t]);
                              R := differential_ring
```

Let us now add to `madm` the hypothesis that $C(t)$ is a constant, obtaining a new system called `madm_approx`.

```
> madm_approx :=
   [ seq (lhs (madm) [i] = rhs (madm) [i], i = 1 .. Dimension (X)),
     diff (C(t),t) = 0 ];

                d
madm_approx := [-- E(t) = -k[1] E(t) S(t) + k[-1] C(t) + k[2] C(t),
                dt

    d
    -- S(t) = -k[1] E(t) S(t) + k[-1] C(t),
    dt

    d                                                       d
    -- C(t) = k[1] E(t) S(t) - k[-1] C(t) - k[2] C(t), -- P(t) = k[2] C(t),
    dt                                                      dt

    d
    -- C(t) = 0]
    dt
```

In the simplification process, we do not want to discuss the possible vanishing of any expression depending on the three parameters: we want the simplification to be "generic". The algebraic way to formulate this consists in moving the three parameters in the ground field of the equations. Indeed, in a field, every quantity which is not zero is invertible, and cannot vanish.

```
> Field := field (generators = [k[1],k[-1],k[2]]);
                Field := field(generators = [k[1], k[-1], k[2]])
```

Let us now simplify the system over the ground field `Field`.

```
> ideal := RosenfeldGroebner (madm_approx, R, basefield = Field);
       ideal := [regular_differential_chain, regular_differential_chain]
```

We have got two cases, represented by two regular differential chains. The two chains are very simple and obviously define prime differential ideals which are not included in each other. The intersection is thus irredundant (Proposition 24, page 53).

```
> Equations (ideal);
          d        d                        d        d
        [[-- E(t), -- P(t), C(t), S(t)], [-- P(t), -- S(t), C(t), E(t)]]
          dt       dt                       dt       dt
```

A differential polynomial belongs to the differential ideal $\mathfrak{A}$ generated by `madm_approx` if and only if it belongs to both its associated differential prime ideals. We thus see that $S(t)\,E(t) \in \mathfrak{A}$ while $S(t)$, $E(t) \notin \mathfrak{A}$. With less algebraic words, the equations of `madm_approx` imply that $C(t) = 0$ and that, either $S(t) = 0$ or $E(t) = 0$.

This is afterwards easy to understand: if $C(t)$ were not zero, then it would tend to zero and would thus not be a constant. We thus need $C(t)$ to be zero and to remain zero. Then the reaction labelled by k_1 must not fire. This implies that either $S(t) = 0$ or $E(t) = 0$.

Obviously, our assumption leads to overly simplified models. It is however a nice example of a naturally occuring intermediate, temporary model, generating a non-prime differential ideal.

10.2 The Right Approximation

It relies on the idea that the set of reactions can be split into two subsets: the set of the fast reactions and the one of the slow reactions. Here, the fast reactions are the ones labelled with k_1, k_{-1}. The slow reaction is the third one, labelled with k_2.

The first step consists in simplifying (10.1) by forgetting everything about the dynamics of the fast reactions, except that they exist i.e. that there is some conservation of the flow (quite interesting: we are somehow coming back to the part of the dynamics which is common to the eight dynamics). This we encode by representing this unknown flow by a new unknown function $F_1(t)$. We then obtain the following reaction system where $F_1(t)$ has the dimension of a flow.

$$E + S \underset{-F_1(t)}{\overset{F_1(t)}{\rightleftarrows}} C \xrightarrow{k_2} E + P\,.$$

The second step consists in restricting this generalized dynamics to the algebraic variety defined by the fast reactions of (10.1), if there were no slow reactions, i.e. to the variety defined by the algebraic equation

$$k_1\, E(t)\, S(t) - k_{-1}\, C(t) \;\; = \;\; 0\,.$$

Together, the two steps lead to the following system (a DAE, actually):

```
> sys := [
           diff(E(t),t) = - F[1](t) + k[2]*C(t),
           diff(S(t),t) = - F[1](t),
           diff (C(t),t) = - k[2]*C(t) + F[1](t),
           diff (P(t),t) = k[2]*C(t),
           0 = k[1]*E(t)*S(t) - k[-1]*C(t)
         ];

        d                                  d
sys := [-- E(t) = -F[1](t) + k[2] C(t), -- S(t) = -F[1](t),
        dt                                 dt

    d                                  d
    -- C(t) = -k[2] C(t) + F[1](t), -- P(t) = k[2] C(t),
    dt                                 dt

    0 = k[1] E(t) S(t) - k[-1] C(t)]
```

We are now going to simplify `sys` by eliminating the unknown flow $F_1(t)$. We thus choose a ranking such as

$$(\text{the derivatives of } F_1) \gg (\text{the derivatives of } C, E, P, S) \gg (\text{the parameters})\,.$$

```
> R := DifferentialRing
        (blocks = [F[1], [C,E,P,S], [k[1](),k[-1](),k[2]()]],
         derivations = [t]);
                              R := differential_ring
```

As above, we want the simplification to be generic. We thus move the parameters to the base field of the equations.

```
> Field := field (generators = [k[1],k[-1],k[2]]);
                  Field := field(generators = [k[1], k[-1], k[2]])
```

The simplification process represents the differential ideal defined by `sys` as an intersection of three differential ideals, presented by regular differential chains.

```
> ideal := RosenfeldGroebner (sys, basefield = Field, R);
ideal := [regular_differential_chain, regular_differential_chain,

    regular_differential_chain]
```

Here are their equations, in "solved" form i.e. with leading derivatives on the left hand-sides.

```
> Equations (ideal, solved);
                          2     2
              -E(t) S(t)  k[1]  k[2] - E(t) S(t) k[1] k[-1] k[2]
[[F[1](t) = - ----------------------------------------------------,
                                    %1

                  2          2
    d         E(t)  S(t) k[1]  k[2]  d         E(t) S(t) k[1] k[2]
    -- E(t) = ----------------------, -- P(t) = --------------------,
    dt                 %1            dt                k[-1]

                        2     2
    d           E(t) S(t)  k[1]  k[2] + E(t) S(t) k[1] k[-1] k[2]
    -- S(t) = - ----------------------------------------------------,
    dt                                  %1

           E(t) S(t) k[1]
    C(t) = --------------],
                k[-1]

                  d                                  k[-1]
    [F[1](t) = 0, -- P(t) = 0, C(t) = 0, E(t) = - -----, S(t) = 0],
                  dt                                 k[1]

                  d                                            k[-1]
    [F[1](t) = 0, -- P(t) = 0, C(t) = 0, E(t) = 0, S(t) = - -----]]
                  dt                                           k[1]

                                                 2
%1 := E(t) k[1] k[-1] + S(t) k[1] k[-1] + k[-1]
```

The first component is the interesting one since it corresponds to a nonzero flow. The differential equation which gives the evolution of the substrate $S(t)$ does not exactly look like the Michaelis-Menten formula. To get the real formula, one needs to take into account some "minor" hypotheses. We then introduce new constants for initial values and the two constants K and $V_{\max}$, leading to an extended differential polynomial ring.

```
> R := DifferentialRing
         (blocks = [F[1], [E,C,P,S],
                    [k[1](),k[-1](),k[2](),C0(),E0(),P0(),S0(),K(),Vmax()]],
          derivations = [t]);
                              R := differential_ring
```

Some algebraic relations hold among the parameters: initial values which are supposed to be zero and relations just meant to rename constants.

```
> relations_among_params :=
     Tools:-PretendRegularDifferentialChain
       ([P0 = 0, C0 = 0, K = k[-1]/k[1], Vmax = k[2]*E0], R);
              relations_among_params := regular_differential_chain
```

As above, we move parameters in the base field of the equations. This time, however, this field is defined by generators and relations.

```
> Field := field
      (generators = [k[1],k[-1],k[2],C0,E0,P0,S0,K,Vmax],
       relations = relations_among_params);
Field := field(generators = [k[1], k[-1], k[2], C0, E0, P0, S0, K, Vmax],

    relations = regular_differential_chain)
```

We also need two linear conservation laws (that could have been automatically extracted from the stoichiometry matrix).

```
> conservation_laws :=
       [E(t) + C(t) = E0 + C0,
        S(t) + C(t) + P(t) = S0 + C0 + P0];
conservation_laws := [E(t) + C(t) = E0 + C0, S(t) + C(t) + P(t) = S0 + C0 + P0]
```

We are now ready to simplify the whole system.

```
> ideal := RosenfeldGroebner
              ([ op(sys), op(conservation_laws) ],
               R, basefield = Field);
                     ideal := [regular_differential_chain]
```

Let us pick the formula which gives the evolution of $S(t)$.

```
> formula := Equations (ideal[1], solved, leader=diff(S(t),t));
                                              2
                           d              S(t)  Vmax + S(t) K Vmax
              formula := [-- S(t) = - ----------------------------]
                           dt                2                        2
                                    S(t)  + 2 S(t) K + E0 K + K
```

Not yet! One still needs to neglect the term $K\,E_0$, assuming $S_0 \gg E_0$.

```
> formula := normal (subs (K*E0=0, formula));
                                    d           S(t) Vmax
                        formula := [-- S(t) = - ---------]
                                    dt          S(t) + K
```

The formula can also be obtained by looking for the equation which gives the evolution of $P(t)$.

```
> NormalForm (diff (P(t),t), ideal[1]);
                                    S(t) Vmax
                                    ---------
                                    S(t) + K
```

10.3 Concluding Remarks

The example of the Henri-Michaelis-Menten equation is actually connected to the well-known quasi-steady state approximation technique, which belongs to the singular perturbation theory and is related to the Tikhonov Theorem. See [6] for details. The quasi-steady state approximation of a dynamical system is not an algorithmic method in general, since 1) it requires the knowledge of the fast and slow variables of the system and 2) these variables may need to be obtained through some change of coordinates from the model variables. However, in the particular case of dynamical systems arising from chemical reaction systems endowed with the mass-action law, the process is algorithmic, provided that reaction sets are split into two sets: the fast and the slow reactions. Observe reactions are not variables. As far as we know, this important fact was noticed first in [9]. Our contribution consisted in noticing that the whole symbolic treatment could be achieved by differential elimination. We could then apply the overall method for approximating rigorously more complicated models featuring genetic clocks [2, 1]. The approximated models were then simple enough to permit the study of their Hopf bifurcations.

Bibliography

[1] François Boulier, Marc Lefranc, François Lemaire, and Pierre-Emmanuel Morant. Applying a rigorous quasi-steady state approximation method for proving the absence of oscillations in models of genetic circuits. In K. Horimoto et al., editor, *Proceedings of Algebraic Biology 2008*, number 5147 in LNCS, pages 56–64. Springer Verlag Berlin Heidelberg, 2008.

[2] François Boulier, Marc Lefranc, François Lemaire, Pierre-Emmanuel Morant, and Aslı Ürgüplü. On proving the absence of oscillations in models of genetic circuits. In K. Horimoto H. Anai and T. Kutsia, editors, *Proceedings of Algebraic Biology 2007*, volume 4545 of *LNCS*, pages 66–80. Springer Verlag Berlin Heidelberg, 2007. `http://hal.archives-ouvertes.fr/hal-00139667`.

[3] François Boulier, François Lemaire, Michel Petitot, and Alexandre Sedoglavic. Chemical Reaction Systems, Computer Algebra and Systems Biology. In Vladimir Gerdt et al., editor, *Proceedings of Computer Algebra in Scientific Computing, LNCS 6885*, pages 73–87, Kassel, Germany, 2011. `http://hal.archives-ouvertes.fr/hal-00603290`.

[4] Victor Henri. *Lois générales de l'Action des Diastases*. Hermann, Paris, 1903.

[5] Steffen Klamt and Jörg Stelling. Stoichiometric and Constraint-based Modeling. In Zoltan Szallasi, Jörg Stelling, and Vipul Periwal, editors, *System Modeling in Cellular Biology: From Concepts to Nuts and Bolts*, pages 73–96. Cambridge, Massachussets: The MIT Press, 2006.

[6] Petar Kokotovic, Hassan K. Khalil, and John O'Reilly. *Singular Perturbation Methods in Control: Analysis and Design*. Classics in Applied Mathematics 25. SIAM, 1999.

[7] Leonor Michaelis and Maud Menten. Die kinetik der invertinwirkung. *Biochemische Zeitschrift*, 49:333–369, 1973. Partial translation in english on `http://web.lemoyne.edu/~giunta/menten.html`.

[8] Péter Érdi and János Tóth. *Mathematical models of chemical reactions: theory and applications of deterministic and stochastic models*. Princeton University Press, 1989.

[9] Vincent Van Breusegem and George Bastin. Reduced order dynamical modelling of reaction systems: a singular perturbation approach. In *Proceedings of the 30th IEEE Conference on Decision and Control*, pages 1049–1054, Brighton, England, December 1991.

Chapter 11

Parameter Estimation

This section borrows quite some material from [4, 1].

11.1 The Problem

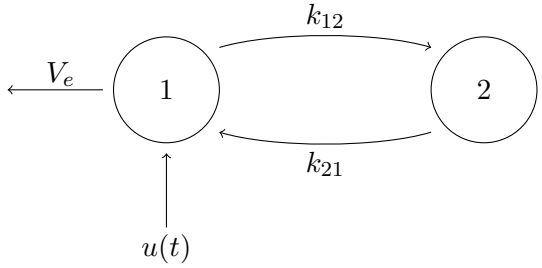


Figure 11.1: A two-compartment model featuring three parameters.

The academic two-compartment model depicted in Figure 11.1 is a close variant of [7, (1), page 517] endowed with an input $u(t)$. Compartment 1 represents the blood system and compartment 2 represents some organ. Both compartments are supposed to have unit volumes. The function $u(t)$, which has the dimension of a flow, represents a medical drug, injected in compartment 1. The drug diffuses between the two compartments, following linear laws: the proportionality constants are named k_{12} and k_{21}. The drug exits compartment 1, following a law of Michaelis-Menten type. Such a law indicates a hidden enzymatic reaction. In general, it depends on two constants V_e and k_e. For the sake of simplicity, it is assumed that $k_e = 1$. The state variables in this system are $x_1(t)$ and $x_2(t)$. They represent the concentrations of drug in each compartment. This information is sufficient to write the two first equations of the mathematical model (11.1). The last equation of (11.1) states that the output, denoted $y(t)$, is equal to $x_1(t)$. This means that only $x_1(t)$ is observed: some numerical data are available for $x_1(t)$ but not for $x_2(t)$. The problem addressed here then consists in estimating the three parameters k_{12}, k_{21} and V_e from these data and the

knowledge of $u(t)$.

$$\begin{aligned} \dot{x}_1(t) &= -k_{12}\, x_1(t) + k_{21}\, x_2(t) - \frac{V_e\, x_1(t)}{1 + x_1(t)} + u(t)\,, \\ \dot{x}_2(t) &= k_{12}\, x_1(t) - k_{21}\, x_2(t)\,, \\ y(t) &= x_1(t)\,. \end{aligned} \tag{11.1}$$

11.2 The Input-Output Equation

Differential algebra provides an algebraic framework for polynomial differential systems. Differential systems involving rational fractions, such as (11.1), are theoretically easily handled since there is a straightforward method to convert them into polynomial form. Observe that differential algebra imposes a restriction which is important to us, since it reduces its applicability to control theory: the solutions of the systems under study are supposed to belong to integral domains (e.g. an equation such as $u(t)\, v(t) = 0$ would imply that $u(t) = 0$ or $v(t) = 0$) and must be differentiable infinitely many times. See Chapter 6. The input $u(t)$ of (11.1) must then be smooth. One cannot study the case of a piecewise constant function $u(t)$ without leaving the realm of differential algebra.

Subtract right-hand sides from left-hand sides of (11.1). Multiply the first equation by its denominator and state that this latter is nonzero. One obtains a system of three differential polynomial equations and one inequation:

$$p_1 = p_2 = p_3 = 0\,, \qquad 1 + x_1 \neq 0\,. \tag{11.2}$$

The left-hand sides of (11.2) belong to the differential polynomial ring

$$R = \mathbb{Q}(k_{12}, k_{21}, V_e)\{y, x_1, x_2\}\,.$$

The three symbols y, x_1, x_2 are the differential indeterminates. To this system, one associates the differential ideal

$$\mathfrak{A} = [p_1, p_2, p_3] : (1 + x_1)^\infty.$$

The ideal $\mathfrak{A}$ is defined as the ideal of R generated by the three differential polynomials and their derivatives up to any order, saturated by the multiplicative family generated by $1 + x_1$. This means that if any differential polynomial of the form $(1 + x_1)\, g$ belongs to $\mathfrak{A}$, then g itself belongs to $\mathfrak{A}$. It can be proved that $\mathfrak{A}$ is a prime (hence radical) differential ideal[1].

```
> restart;
> with (DifferentialAlgebra):
> with (Tools):
```

Let us assign the input system to `syst`.

[1]The primality of $\mathfrak{A}$ can be established, roughly speaking, as follows: if it were not prime, one of the three differential polynomials p_1, p_2, p_3 (viewed as univariate polynomials in their leading derivatives) could be factorized. This cannot happen because their leading degrees are 1.

```
> syst := [
    diff (x1(t),t) = - k12*x1(t) + k21*x2(t) - Ve*x1(t)/(1+x1(t)) + u(t),
    diff (x2(t),t) =   k12*x1(t) - k21*x2(t),
               y(t) =       x1(t) ];

         d                                      Ve x1(t)
syst := [-- x1(t) = -k12 x1(t) + k21 x2(t) - --------- + u(t),
         dt                                     1 + x1(t)

    d
    -- x2(t) = k12 x1(t) - k21 x2(t), y(t) = x1(t)]
    dt
```

Let us assign to `R` a differential polynomial ring endowed with the ranking

$$(\text{the derivatives of } y) \gg (\text{those of } x_1, x_2) \gg (\text{those of } u) \gg (\text{the parameters})\,.$$

The parentheses following the parameters in the last block indicate that these symbols are parameters.

```
> R := DifferentialRing (derivations = [t],
                         blocks = [y,[x1,x2],u,[k12(),k21(),Ve()]]);
                             R := differential_ring
```

The call to `RosenfeldGroebner` below does not transform the equations of `syst`. It only aims at letting the package determine that 1) the input system already is a regular differential chain with respect to the above ranking and 2) the differential ideal defined by the input system is prime.

```
> ideal := RosenfeldGroebner (syst, R);
                      ideal := [regular_differential_chain]
```

Let us assign to `ideal` the first element of the returned list.

```
> ideal := ideal [1]:
```

In order to compute the input-output equation, let us now assign to `io_R` the same mathematical differential polynomial ring as `R`, but endowed with the following ranking

$$(\text{the derivatives of } x_1, x_2) \gg (\text{the derivatives of } y, u) \gg (\text{the parameters})\,, \tag{11.3}$$

```
> io_R := DifferentialRing (derivations = [t],
                            blocks = [[x1,x2],[y,u],[k12(),k21(),Ve()]]);
                           io_R := differential_ring
```

The following call to `RosenfeldGroebner` does perform a differential elimination task: it computes another regular differential chain, defining the same prime differential ideal $\mathfrak{A}$, with respect to the ranking (11.3). The `RosenfeldGroebner` function applies here the algorithm presented in [3], which develops an idea initially stated in [6]: it avoids splitting cases since $\mathfrak{A}$ is prime and a regular differential chain is already known, which permits to recognize zero in $R/\mathfrak{A}$.

```
> io_ideal := RosenfeldGroebner (ideal, io_R);
                     io_ideal := regular_differential_chain
```

Here are the defining equations of `io_ideal`. The leading derivatives, with respect to the ranking, appear on the left hand sides of the equations. For legibility, the raw output of the command is pretty-printed. This pretty-printing operation could possibly be performed automatically, by means of the algorithm described in [2] and implemented by François Lemaire, but is not yet well integrated to the MAPLE package. I thus do not want to give the corresponding commands. We may however expect the software to systematically provide an output close to the following one in the future.

```
> Equations (io_ideal, solved);
  [+ some pretty-printing]
```

$$[x1(t) = y(t),\ x2(t) = \frac{Ve}{k21} - \frac{Ve}{k21\ (1 + y(t))} + \frac{y(t)\ k12 - u(t)}{k21} + \int\int \frac{y(t)}{k21}]$$

$$\frac{d^2}{dt^2} y(t) =$$

$$-k21\ Ve + u(t)\ k21 + \frac{k21\ Ve}{1 + y(t)} + \int\left[(-k12 - k21)\ y(t) + u(t) + \frac{Ve}{1 + y(t)}\right]$$

The third equation of `io_ideal` is the input-output equation of the dynamical system under study. It can be used to prove the global structural identifiability of the dynamical system. It may also be used to estimate the unknown parameters from the knowledge of $y(t)$ and $u(t)$, by means of numerical methods. See [5, 1] and references therein for more details.

11.3 Numerical Estimation

Bibliography

[1] François Boulier, Anja Korporal, François Lemaire, Wilfrid Perruquetti, Adrien Poteaux, and Rosane Ushirobira. An Algorithm for Converting Nonlinear Differential Equations to Integral Equations with an Application to Parameter Estimation from Noisy Data. In *LNCS 8660: Proceedings of Computer Algebra and Scientific Computing (CASC) 2014*, pages 28–43, Warsaw, Poland, 2014.

[2] François Boulier, Joseph Lallemand, François Lemaire, Georg Regensburger, and Markus Rosenkranz. Additive normal forms and integration of differential fractions. *Journal of Symbolic Computation*, 2016. To appear.

[3] François Boulier, François Lemaire, and Marc Moreno Maza. Computing differential characteristic sets by change of ordering. *Journal of Symbolic Computation*, 45(1):124–149, 2010. doi:10.1016/j.jsc.2009.09.04.

[4] François Boulier, François Lemaire, Markus Rosenkranz, Rosane Ushirobira, and Nathalie Verdière. *On Symbolic Approaches to Integro-Differential Equations*. 2016. (submitted).

[5] Lilianne Denis-Vidal, Ghislaine Joly-Blanchard, and Céline Noiret. System identifiability (symbolic computation) and parameter estimation (numerical computation). In *Numerical Algorithms*, volume 34, pages 282–292, 2003.

[6] François Ollivier. *Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*. PhD thesis, École Polytechnique, Palaiseau, France, 1990.

[7] Nathalie Verdière, Lilianne Denis-Vidal, Ghislaine Joly-Blanchard, and Dominique Domurado. Identifiability and Estimation of Pharmacokinetic Parameters for the Ligands of the Macrophage Mannose Receptor. *Int. J. Appl. Math. Comput. Sci.*, 15(4):517–526, 2005.