An Equivalence Theorem For Regular Differential Chains

François Boulier, François Lemaire, Adrien Poteaux, Marc Moreno Maza

An Equivalence Theorem For Regular Differential Chains

François Boulier, * François Lemaire, Adrien Poteaux and

Univ. Lille, CNRS, Centrale Lille, UMR 9189 - CRIStAL -
Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France

Marc Moreno Maza

Univ. Western Ontario - ORCCA, N6A 3K7 London, Ontario, Canada

Abstract

The main result of this paper is a new characterization of regular differential chains, which are generalizations of Ritt's characteristic sets in differential algebra. An original presentation of a similar equivalence theorem for nondifferential regular chains is also provided.

Key words: Differential algebra, regular differential chain, characteristic set

1. Introduction

This paper summarizes in an equivalence Theorem (Theorem 26, page 17) the most important properties of *regular differential chains*, which are sets of differential polynomials that naturally arise in the elimination theory of *differential algebra*.

1.1. Relationship with Classical Differential Algebra

Differential algebra is an algebraic theory for systems of differential polynomials founded by Ritt (1932, 1950) and developed by Kolchin (1973). It has involved an elimination theory from its very beginning. Casual readers will find in Section 1.2 an academic example which illustrates its usefulness.

A regular differential chain is a concept very close to the one of a *characteristic set* of a differential ideal. Characteristic sets are introduced in Ritt (1932) already, under

* Corresponding author

Email addresses: {francois.boulier,francois.lemaire,adrien.poteaux}@univ-lille1.fr (François Lemaire, Adrien Poteaux and), moreno@csd.uwo.ca (Marc Moreno Maza).

the name *basic set*. The term *characteristic set* itself appears in (Ritt, 1950, Chapter I) where the nonconstructive argument that any set of differential polynomials has a characteristic set permits to prove the Ritt-Raudenbush Basis Theorem and then the fact that any radical differential ideal is a unique finite initersection of prime differential ideals. Characteristic sets are then used in (Ritt, 1950, Chapter V, Constructive Methods) as a major tool for an elimination theory.

In the remaining part of this section, we review a short set of the works which led from Ritt (1950) to the concept of regular differential chain and the ones which are strongly related to technical issues addressed by this paper. All of them essentially aim at generalizing Ritt's original ideas by fixing two important drawbacks: the use, by Ritt, of factorizations over towers of algebraic extensions of the base field of the equations; and the fact that the case of more than one derivation — the case of systems of partial differential equations — is not covered.

Seidenberg (1956) seems to be the first one to provide an elimination theory which is factorization free and covers the case of more than one derivation. However, the theory of *rankings* was not yet fully developed at this time and Seidenberg restricts himself to the case of pure elimination rankings. His methods do not compute characteristic sets: instead, they are decision procedures which gather as input a basis of a *differential ideal* $\mathfrak{A}$, a differential polynomial p and return a boolean indicating whether a power of p belongs to $\mathfrak{A}$. Their complexity is very high as pointed out by Grigoriev (1987).

Rosenfeld (1959) seems to be the first one to provide the algorithmic conditions (the so-called *coherence* property) that Ritt's characteristic sets would need to fulfill in order to apply in the case of more than one derivation. His Lemma is formulated using the modern concept of rankings.

Kolchin (1973) provides an impressive unified presentation of the earlier works of Ritt's school and generalizes many of them. Unfortunately, his presentation of Rosenfeld's Lemma hides the algorithmic nature of this important result.

Wu (1989) and his school popularized Ritt's theory of characteristic sets by describing many applications (though the term *characteristic set* has different meanings in the texts of Ritt and Wu). Wu does not address the case of more than one derivation. His work was later developed by many authors such as Wang (1996), more recently Gao et al. (2009) and many others.

Fliess (1989) pointed out the conceptual importance of differential algebra in the context of control theory. This seminal work motivated a renewal of interest for Ritt's characteristic sets in the case of a single derivation. See Ollivier (1990); Ljung and Glad (1994).

Boulier (1994) and Boulier et al. (1995) developed the first factorization free elimination method (the *RosenfeldGroebner* algorithm) for differential algebra which covers also the case of more than one derivation, by combining Seidenberg's idea of using Hilbert's Theorem of Zeros, Rosenfeld's Lemma and Gröbner bases for the eventual simplification of polynomial systems of equations and inequations returned by the differential procedure. The *RosenfeldGroebner* algorithm gathers as input a basis of a *differential ideal* $\mathfrak{A}$, a ranking and returns a decomposition of the radical of $\mathfrak{A}$ as an intersection of differential ideals that need not be prime but are radical, as stated by the so-called Lazard's Lemma (Boulier et al., 1995, Lemma 2). However, generalizing characteristic sets methods to nonprime ideals raises specific difficulties. In particular, it becomes much more important to understand the structure of the set of the zerodivisors in rings defined by

characteristic sets. It is this difficulty which makes the proof of (Boulier et al., 1995, Lemma 2) incomplete. Morrison (1995, 1999) was the first one to provide a complete proof, and to point out the relevance of Macaulay's unmixedness Theorem not only in this theory but also in related ones, such as most of the elimination theories relying on triangular sets. Ritt proved that every prime ideal has a characteristic set, which permits to decide membership to it, by means of some reduction process, based on the pseudodivision. The generalization to nonprime ideals led to the concept of *characterizable ideals*, introduced by Hubert (2000).

The concept of *regular chain* was introduced independently by Kalkbrener (1993); Chou and Gao (1993); Yang and Zhang (1994), as an alternative of Gröbner bases for the study of nondifferential polynomial ideals. It would be quite long to list all the works which developed this idea. Let us just cite Aubry et al. (1999), who summarized the important properties of regular chains in (Aubry et al., 1999, Theorem 6.1), with a proof which implicitly relies on Macaulay's unmixedness Theorem. In particular, it is proved that regular chains are (up to some irrelevant degree condition) characteristic sets, in the sense of Ritt, of the polynomial ideals that they define.

Lemaire (2002) then introduced the concept of *regular differential chain*, formulated a version of *RosenfeldGroebner* that returns them and proved that they are characteristic sets, in the sense of Ritt, of the differential polynomial ideals that they define.

1.2. An Academic Example

Regular differential chains are sets of differential polynomials returned by differential elimination procedures such as the `RosenfeldGroebner` function of the MAPLE `DifferentialAlgebra` package, which was developed by Boulier and Cheb-Terrab (2008) and followed an earlier package developed by Boulier and Hubert (1996). In order to motivate readers, here is a small academic example, carried out by the package.

The variable `sys` is assigned a system of polynomial PDE, in jet notation. 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. The symbol `u[x,y]` denotes the *derivative* $\frac{\partial^2 u(x,y)}{\partial x\, \partial y}$. In commutative algebra, polynomials belong to polynomial rings. In differential algebra, *differential polynomials* belong to *differential polynomial rings*. Such a differential polynomial ring is assigned to the `R` variable.

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

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]
```

The following command shows that there exists an elimination procedure (a close algorithm is detailed by Boulier (2006)) which takes as input 1) a set of differential polynomials, 2) a ranking. It returns a list of *regular differential chains* which provide many structural informations on the solutions of the input system of PDE.

```
> 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]
```

In particular, the computed regular differential chain permits to expand solutions of the initial system into formal power series, from given initial values. Initial values cannot be chosen freely. The constraints they must satisfy are provided by the regular differential chain: a property quite related to the issue of consistent initial values for numerically solving differential-algebraic equations.

```
> 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
```

Our example is very particular because all solutions are polynomials. Indeed, the above polynomials are solutions of our input system.

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

1.3. Novelty and Structure of This Paper

The main result of this paper is Theorem 26, which states equivalent conditions for a set of differential polynomials, to be a regular differential chain. Among these conditions, $\mathbf{a} \Rightarrow \mathbf{b}$ is known, $\mathbf{b} \Rightarrow \mathbf{a}$ was only published in Lemaire (2002) and deserves a

better exposition, while **a** $\Leftrightarrow$ **c** and **a** $\Leftrightarrow$ **d** are new. Theorem 26 relies on Theorem 13, which states equivalent conditions for a set of usual polynomials, to be a regular chain. These equivalent conditions are all known. However, some of the published proofs are incomplete, some other ones were only published in conference papers and/or rely on definitions which are not consistent with ours. For this reason, a complete set of proofs for Theorem 13 is provided. Our proofs are original since they completely avoid any reduction to the zerodimensional case.

This paper is organized as follows. Section 2 presents some algebraic preliminaries. Section 3 recalls two major Theorems on triangular sets. Section 4 then adapts two well-known algorithms (pseudodivision and resultant) to the context of triangular sets. Section 5 focuses on a particular class of triangular sets — the regular chains — and proves Theorem 13. So far, all presented notions are useful for differential algebra but not specific to it. In Section 6, basic notions of differential algebra are introduced. Last, Section 7 presents our main result.

2. Preliminaries

An element a of a ring R is a zerodivisor if there exists some nonzero $b \in R$ such that $a\,b = 0$. Therefore zero is a zerodivisor (Zariski and Samuel, 1958, I, 5, page 8). An element a which is not a zerodivisor of R is said to be a *regular* element of R.

Some propositions of this paper involve statements such as "a polynomial f is zero (or a zerodivisor) 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 zerodivisor in $R/\mathfrak{A}$" should actually be written "the image of f by the canonical ring homomorphism $R \to R/\mathfrak{A}$ is a zerodivisor" or, "f is a zerodivisor 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.

In this paper, 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

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

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 $h\,f \in \mathfrak{A} : h^\infty$. If $\mathfrak{q}$ is a *primary* ideal of a ring R (Zariski and Samuel, 1958, III, 9, page 152) and $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is its *associated prime ideal*, then $\mathfrak{q} : h^\infty = \mathfrak{q}$ if and only if $h \notin \mathfrak{p}$ and $\mathfrak{q} : h^\infty = R$ if $h \in \mathfrak{p}$. Therefore, in Nötherian rings, where every ideal $\mathfrak{A}$ has an irredundant representation $\mathfrak{A} = \cap_{i=1}^r \mathfrak{q}_i$ as an intersection of primary ideals (Zariski and Samuel, 1958, IV, 4, The Lasker-Nöther Theorem, page 208), the ideal $\mathfrak{A} : h^\infty$ is the intersection of the primary ideals $\mathfrak{q}_i$ such that $h \notin \sqrt{\mathfrak{q}_i}$. The ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are called the associated prime ideals of $\mathfrak{A}$ (Zariski and Samuel, 1958, IV, 5, page 211).

Therefore, since, in Nötherian rings, the set of the zerodivisors of $R/\mathfrak{A}$ is the union of the associated prime ideals of $\mathfrak{A}$ (Zariski and Samuel, 1958, IV, 6, Corollary 3 to Theorem 11, page 214), we see that

(1) $\mathfrak{A} : h^\infty = \mathfrak{A}$ if and only if h is a regular element of $R/\mathfrak{A}$;
(2) h is a regular element of $R/(\mathfrak{A} : h^\infty) = R/\mathfrak{A} : h^\infty$, provided that h is not zero in $R/\mathfrak{A}$;
(3) if all primary components of $\mathfrak{A}$ share some common property then all primary components of $\mathfrak{A} : h^\infty$ share also this property. We will meet two examples: 1) the case of $\mathfrak{A}$ being a radical ideal (all its primary components are prime) and 2) the case of $\mathfrak{A}$ being unmixed (all its associated prime ideals have the same dimension).

In Section 6, we will consider differential polynomial rings which contain *differential* ideals, i.e. ideals stable under derivation. Such a ring R is not Nötherian but every radical (called *perfect* by Ritt) differential ideal $\mathfrak{A}$ of R has an irredundant representation $\mathfrak{A} = \cap_{i=1}^r \mathfrak{p}_i$ as an intersection of prime differential ideals (Ritt, 1950, I, 16, page 13). Ritt calls these ideals the *essential prime divisors* of $\mathfrak{A}$. By analogy with commutative algebra, we will call them the *associated differential prime ideals* of $\mathfrak{A}$. If $\mathfrak{A}$ is not radical, the structure of the set of the zerodivisors of $R/\mathfrak{A}$ is not clear in general. However,

(1) the set of the zerodivisors of $R/\mathfrak{A}$ contains the union of the associated differential prime ideals of $\sqrt{\mathfrak{A}}$ (with equality if $\mathfrak{A}$ is radical) [1] ;
(2) $\mathfrak{A} : h^\infty = \mathfrak{A}$ if and only if h is a regular element of $R/\mathfrak{A}$;
(3) h is a regular element of $R/\mathfrak{A} : h^\infty$, provided that h is not zero in $R/\mathfrak{A}$.
(4) if $\mathfrak{A}$ is radical and all its associated differential prime ideals share some common property then $\mathfrak{A} : h^\infty$ is radical and all its associated differential prime ideals share this same property.

3. Triangular Sets

Let K be a commutative field of characteristic zero. We are concerned with a triangular set $A = \{p_1, \ldots, p_n\}$ in a polynomial ring $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. The set is triangular in the sense that each polynomial p_k introduces at least one variable, its *leading variable* x_k, which is such that $\deg(p_k, x_k) > 0$ and $\deg(p_k, x_{k+1}) = \cdots = \deg(p_k, x_n) = 0$ for each $1 \leq k \leq n$. The *initial* of p_k, denoted i_k, is the leading coefficient of p_k w.r.t. its leading variable; the *separant* of p_k is the polynomial $s_k = \partial p_k / \partial x_k$, for each $1 \leq k \leq n$.

The following Theorem is (Boulier et al., 2006, Theorem 1.6). It could mostly be viewed as a corollary to Macaulay's unmixedness Theorem, whose importance in the theory addressed in this paper was first pointed out by Morrison (1995, 1999).

Unmixed ideals are defined in (Zariski and Samuel, 1958, VII, 7, page 196). Without entering details, let us stress that if an ideal $\mathfrak{A}$ is unmixed (or equidimensional), then its algebraic variety is unmixed-dimensional. However, the converse is false. The theory addressed in this paper does require the ideal to be unmixed, not only its radical nor its variety.

The ideal $(A) : h^\infty$ mentioned in the next Theorem, is often denoted $(A) : I_A^\infty$, or $\mathrm{sat}(A)$, in the literature.

---

[1] Consider for instance the differential ideal $\mathfrak{A} = [u^2, u\,v]$ in some ordinary differential polynomial ring R, which is ideal of R generated by $u^2, u\,v, u\,\dot{u}, \dot{u}\,v + u\,\dot{v}, \ldots$ Its radical is the differential ideal $[u]$, which is its own unique associated differential prime ideal and one sees that u is a zerodivisor in $R/\mathfrak{A}$. However, the differential polynomial v also is a zerodivisor in $R/\mathfrak{A}$, though it does not belong to any associated differential prime ideal of $\sqrt{\mathfrak{A}}$.

Theorem 1. *Let A be a triangular set of $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ such that x_k is the leading variable of p_k for $1 \leq k \leq n$. Let h denote either the product of its initials or the product of its separants and $\mathfrak{A} = (A) : h^\infty$.*

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

Proof. Sketched. Consider $\mathfrak{A}' = (A, p_{n+1})$ in $R' = R[x_{n+1}]$ where $p_{n+1} = h\, x_{n+1} - 1$. Use the "principal ideal theorem" (Zariski and Samuel, 1958, 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 $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$. Use then Macaulay's unmixedness theorem (Zariski and Samuel, 1958, VII, 8, Theorem 26, page 203) in order to prove that all associated prime ideals of $\mathfrak{A}'$ are isolated. Last, use the behaviour of the irredundant primary decomposition of $\mathfrak{A}'$ under passage to residue class ring over $R'/(p_{n+1})$ (Zariski and Samuel, 1958, IV, 5, page 213) and contraction (with respect to the localization at h) (Zariski and Samuel, 1958, IV, 10, Theorem 17, page 225) to prove that these properties of $\mathfrak{A}'$ apply to $\mathfrak{A}$. □

The following Theorem was first published by Boulier et al. (1995) with an incomplete proof. The first complete proof is due to Morrison (1995, 1999). The scheme of proof is a close variant of the one originally suggested by Daniel Lazard.

Theorem 2. *(Lazard's Lemma)*

Let $A = \{p_1, \ldots, p_n\}$ be a triangular set of $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$, such that x_k is the leading variable of p_k for $1 \leq k \leq n$. 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 Theorem is a corollary to Theorem 1. We thus only need to prove that $\mathfrak{A}$ is radical. Denote $\mathfrak{A}_0$ the ideal $(A) : h^\infty$ in $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. We prove below that $R_0/\mathfrak{A}_0$ is a direct sum of fields, hence a ring which does not involve any nilpotent element and a ring equal to its own total quotient ring. By Theorem 1, the rings $R_0/\mathfrak{A}_0$ and $R/\mathfrak{A}$ have the same total quotient ring. Thus $R/\mathfrak{A}$ does not involve any nilpotent element and $\mathfrak{A}$ 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. The general case $n > 0$. 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 (Zariski and Samuel, 1958, III, 13, Theorem 32, page 178), $K_j[x_n]/(p_n) : s_n^\infty$ 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. Iterated Pseudodivision and Resultant

4.1. The Iterated Pseudodivision

Let R be a polynomial ring over a commutative field K of characteristic zero, $A = \{p_1, \ldots, p_n\}$ be a triangular set of R, with leading variables $x_1, \ldots, x_n$ and $\mathfrak{A} = (A) : h^\infty$ where h denotes the product of the initials of A.

One denotes $\mathrm{prem}(f, g, x)$ the pseudoremainder of a polynomial f, by a polynomial g such that $\deg(g, x) > 0$ (it is the polynomial $r(x)$ mentioned in (Zariski and Samuel, 1958, I, 17, Theorem 9, page 30)). One may now define the pseudoremainder of a polynomial f by a triangular set A as follows:

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

Lemma 3. *Let f and be any polynomial and $g = \mathrm{prem}(f, A)$. Then*

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

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

$$h_f\, f = g + v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n\,. \tag{2}$$

4.2. The Resultant of two Polynomials

The iterated resultant of a polynomial f by a triangular set A is defined, as expected, using the usual resultant of two polynomials. We first need to recall basic properties of this usual resultant in order to cover some cases which are usually not considered, such as one of the two polynomials being zero. Let f and g be two polynomials of $R[x]$, where R is a unitary ring of characteristic zero:

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

If f or g is zero, then the resultant of f and g is taken to be zero. Assume 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 has dimensions $(m + n) \times (m + n)$ and rows, from top down $x^{n-1}\, f, \ldots, x\, f, f, x^{m-1}\, g, \ldots, x\, g, g$. See (Basu et al., 2003, 4.2, page 105).

Lemma 4. *Assume f is nonzero and $n = 0$ (i.e. $g = b_0$). Then* $\mathrm{res}(f, g, x) = g^m$. *In particular, if $m = 1$ then* $\mathrm{res}(f, g, x) = g$.

Proof. Expand the determinant of the Sylvester matrix, which is diagonal. □

Lemma 5. *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* $\mathrm{res}(f, g, x) = 0$ *if and only if f and g have a common factor in $K[x]$.*

Proof. The Lemma is clear if f or g is zero. Otherwise, see (Basu et al., 2003, 4.2, Proposition 4.15, page 106). □

Lemma 6. *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* $\mathrm{res}(f, g, x) = \mathrm{res}(g, r, x) = 0$. *Otherwise,*

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

Proof. If f is zero then r is zero and both resultants are zero. Assume f is nonzero. If r is zero, then $\mathrm{res}(g, r, x) = 0$ 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 Lemma 5, we have $\mathrm{res}(f, g, x) = 0$. Assume f and r are nonzero. The proof is then essentially that of (Basu et al., 2003, 4.2, Lemma 4.17, page 107). □

Lemma 7. *Let R be a domain, f, g and h be polynomials in $R[x]$. Then* $\mathrm{res}(f\, g, h, x) = \mathrm{res}(f, h, x)\ \mathrm{res}(g, h, x)$.

Proof. The lemma obviously holds if any of the three polynomials is zero. Assume none of them is zero. Here is a scheme of proof for this well-known formula: 1) establish the formula which relates resultants to the roots of the input polynomials over the algebraic closure of R (Basu et al., 2003, 4.2, Theorem 4.16, page 107) 2) then follow (Cox et al., 2005, 3, Exercise 3, page 79). □

Lemma 8. *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* $\mathrm{res}(f, g, x) = u\, f + v\, g$.

Proof. See (Basu et al., 2003, 4.2, Proposition 4.18, page 108). □

The following Lemma generalizes (Basu et al., 2003, 4.2, Proposition 4.20, page 109) and deserves a proof.

Lemma 9. *Let f, g be two polynomials of $R[x]$ such that $m \geq n$. Let $\phi : R \to S$ be a ring homorphism, such that $\phi(a_m) \neq 0$. Extend ϕ to a ring homomorphism $R[x] \to S[x]$. Then there exists a nonnegative integer α such that* $\phi(\mathrm{res}(f, g, x)) = \phi(a_m)^\alpha\ \mathrm{res}(\phi(f), \phi(g), x)$.

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

Assume g and $\phi(g)$ are nonzero. If the ring homomorphism ϕ, which does not annihilate a_m, does not annihilate b_n either, then $S(f, g) = S(\phi(f), \phi(g))$ and the Lemma is proved. Assume $\deg(\phi(g)) = t < n$. Then the Sylvester matrix $S(\phi(f), \phi(g))$ appears as the $(m+t) \times (m+t)$ submatrix of $\phi(S(f, g))$ (Fig. 1) at the bottom-right corner. Developing the determinant of $\phi(S(f, g))$ w.r.t. its $n - t$ first columns, we see that $\phi(\mathrm{res}(f, g, x)) = \phi(a_m)^{n-t}\ \mathrm{res}(\phi(f), \phi(g), x)$. □

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

Fig. 1. The image by ϕ of the Sylvester matrix $S(f,g)$.

4.3. The Iterated Resultant

Let R be a polynomial ring over a commutative field K of characteristic zero, $A = \{p_1, \ldots, p_n\}$ be a triangular set of R, with leading variables $x_1, \ldots, x_n$. One defines the resultant of a polynomial f by a triangular set A as follows:

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

Proposition 10. *Let A be a triangular set and f, g be two polynomials.*
Then $\operatorname{res}(f\,g, A) = \operatorname{res}(f, A)\ \operatorname{res}(g, A)$.

Proof. By Lemma 7. □

Proposition 11. *Let f be a polynomial and A be a triangular set. Then there exist polynomials $u, v_1, v_2, \ldots, v_n$ such that*

$$u\,f = \operatorname{res}(f, A) + v_1\,p_1 + v_2\,p_2 + \cdots + v_n\,p_n\,. \tag{3}$$

Moreover, if f does not depend on $x_k, \ldots, x_n$ for some $1 \leq k \leq n$, then there exists a formula (3) *such that $u, v_1, \ldots, v_{k-1}$ do not depend on $x_k, \ldots, x_n$ and $v_k = \cdots = v_n = 0$.*

Proof. By Lemmas 8 and 4. □

Remark. If f does not depend on x_n then $\operatorname{prem}(f, A) = \operatorname{prem}(f, A \setminus \{p_n\})$. This is however not true for the resultant (Lemma 4). A question which then naturally arises is: what about defining it inductively as Chen et al. (2007) i.e. as $\overline{\operatorname{res}}(f, A)$ below?

$$\begin{cases}
\overline{\operatorname{res}}(f, A) = f & \text{if } f \in K[t_1, \ldots, t_m]\,, \\
\overline{\operatorname{res}}(f, A) = \overline{\operatorname{res}}(\operatorname{res}(f, p_n, x_n), A) & \text{if } \deg(f, x_n) > 0\,, \\
\overline{\operatorname{res}}(f, A) = \overline{\operatorname{res}}(f, A \setminus \{p_n\}) & \text{if } \deg(f, x_n) = 0\,.
\end{cases}$$

Though $\mathrm{res}(f, A) \neq \overline{\mathrm{res}}(f, A)$ in general, both have the same squarefree part. In the next sections, all Propositions relying on $\mathrm{res}(f, A)$ are only concerned with the possible vanishing of this resultant. These Propositions thus still hold if one replaces $\mathrm{res}(f, A)$ by $\overline{\mathrm{res}}(f, A)$. However, Proposition 10 does not.

5. Regular Chains

The concept of *regular chain* was introduced by Kalkbrener (1993); Chou and Gao (1993); Yang and Zhang (1994). It was much studied in the former team of Daniel Lazard and, more recently, in the group of Marc Moreno Maza. In Theorem 13, the equivalence $\mathbf{a} \Leftrightarrow \mathbf{b}$ was already proved in (Aubry et al., 1999, Theorem 6.1) (with a proof which implicitly assumes Theorem 1). The implication $\mathbf{a} \Rightarrow \mathbf{c}$ is proved in (Chen et al., 2007, Lemma 4) (with another definition of zerodivisors). The implication $\mathbf{c} \Rightarrow \mathbf{a}$ is proved in (Boulier et al., 2011, Lemma 5). The equivalence $\mathbf{a} \Leftrightarrow \mathbf{d}$ is proved in (Chen et al., 2007, Theorem 1). In order to establish our main result (Theorem 26) on sound bases, it is thus necessary to state Theorem 13, with a complete set of proofs, relying on coherent definitions. Observe also that our proofs are original in the sense that they completely avoid any reduction to the zerodimensional case.

Let R be a polynomial ring over a commutative field K of characteristic zero, $A = \{p_1, \ldots, p_n\}$ be a triangular set of R, with leading variables $x_1, \ldots, x_n$ and $\mathfrak{A} = (A) : h^\infty$ where h denotes the product of the initials of A.

Definition 12. A triangular set 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 $2 \leq k \leq n$.

Theorem 13. *Let A be a triangular set. The following conditions are equivalent:*
a *A is a regular chain;*
b *for any polynomial f, we have $\mathrm{prem}(f, A) = 0$ if and only if f is zero in $R/\mathfrak{A}$;*
c *for any polynomial f, we have $\mathrm{res}(f, A) = 0$ if and only if f is a zerodivisor in $R/\mathfrak{A}$;*
d *$\mathrm{res}(i_k, A) \neq 0$ for each $2 \leq k \leq n$.*

From now on, all Propositions aim at proving Theorem 13.

Proposition 14. *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 zerodivisor. Thus Condition **a** cannot hold. Moreover, if f is any nonzero element of $K[t_1, \ldots, t_m]$ then $\mathrm{prem}(f, A) \neq 0$ and $\mathrm{res}(f, A) \neq 0$. Thus Conditions **b** and **c** cannot hold either. □

5.1. Regularity Testing modulo the Ideal

5.1.1. $\mathbf{c} \Rightarrow \mathbf{a}$

Proposition 15. *Let f be a polynomial and A be a triangular set such that $\mathfrak{A}$ is a proper ideal. If $\mathrm{res}(f, A) \neq 0$ then f is regular in $R/\mathfrak{A}$.*

Proof. We have $u\, f = \mathrm{res}(f, A)$ in $R/\mathfrak{A}$ (Proposition 11) and $\mathrm{res}(f, A) \in K[t_1, \ldots, t_m]$. The proof then follows from Theorem 1. □

Proposition 16. *Let A be a triangular set such that $\mathfrak{A}$ is a proper ideal. Assume that, for any f regular in $R/\mathfrak{A}$, we have* $\mathrm{res}(f, A) \neq 0$. *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. Thus by assumption, $\mathrm{res}(i_k, A) \neq 0$. We need to show that i_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. Decompose $\mathrm{res}(i_k, A) = \mathrm{res}(r_k, \{p_1, \ldots, p_{k-1}\})$ where $r_k = \mathrm{res}(i_k, \{p_k, \ldots, p_n\})$. Then $\mathrm{res}(r_k, \{p_1, \ldots, p_{k-1}\}) \neq 0$. Thus, by Proposition 15, r_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. 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. □

In summary, let us assume Condition **c** holds. Then $\mathfrak{A}$ is proper by Proposition 14. Condition **c** implies, as a particular case, that the hypothesis of Proposition 16 is satisfied. Thus Condition **a** holds.

5.1.2. **a ⇒ c**

Proposition 17. *Let f be a polynomial and A be a regular chain. If* $\mathrm{res}(f, A) = 0$ *then f is a zerodivisor in $R/\mathfrak{A}$.*

Proof. The Proposition holds if f is zero. Assume f is nonzero and $\mathrm{res}(f, A) = 0$. The proof is by induction on n.

Basis: the case $n = 1$ (note $R = K[t_1, \ldots, t_m, x_1]$). Then $\mathrm{res}(f, A) = \mathrm{res}(f, p_1, x_1)$. Since this resultant is zero, f and p_1 have a common factor in $K(t_1, \ldots, t_m)[x_1]$, by Lemma 5. This factor provides, at least, one associated prime ideal of $\mathfrak{A}$ which contains f. Thus f is a zerodivisor in $R/\mathfrak{A}$.

General case: $n > 1$. Denote $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$, $A' = \{p_1, \ldots, p_{n-1}\}$ and $\mathfrak{A}'$ the ideal $(p_1, \ldots, p_{n-1}) : (i_1 \cdots i_{n-1})^\infty$ of R'. Denote $r = \mathrm{prem}(f, p_n, x_n)$. There exists a nonnegative integer α such that

$$i_n^\alpha f = q\, p_n + r\,, \quad \deg(r, x_n) < \deg(p_n, x_n)\,. \tag{4}$$

By Lemmas 6 and 7, we have $\mathrm{res}(f, A) = \pm\, \mathrm{res}(i_n, A)^\beta\ \mathrm{res}(r, A)$ for some nonnegative integer β. Since A is a regular chain, i_n is regular in $R'/\mathfrak{A}'$. Thus, by induction hypothesis, $\mathrm{res}(i_n, A') \neq 0$. By assumption $\mathrm{res}(f, A) = 0$. Thus $\mathrm{res}(r, A) = 0$.

Decompose now $\mathrm{res}(r, A) = \mathrm{res}(s, A')$ with $s = \mathrm{res}(r, p_n, x_n)$. Since $\mathrm{res}(r, A) = 0$ we have $\mathrm{res}(s, A') = 0$. Thus, by induction hypothesis, s is a zerodivisor in $R'/\mathfrak{A}'$. Thus there exists an associated prime ideal $\mathfrak{p}'$ of $\mathfrak{A}'$ such that $s \in \mathfrak{p}'$.

Denote ϕ the canonical ring homomorphism $R' \to R'/\mathfrak{p}'$. We have $\phi(\mathrm{res}(r, p_n, x_n)) = 0$, $\deg(r, x_n) < \deg(p_n, x_n)$ and $\phi(i_n) \neq 0$ since i_n is regular in $R'/\mathfrak{A}'$ by the regular chain condition. Moreover, the ring $R'/\mathfrak{p}'$ is a domain since $\mathfrak{p}'$ is prime. Thus Lemma 9 applies and $\mathrm{res}(\phi(r), \phi(p_n), x_n) = 0$. Thus $\phi(r)$ and $\phi(p_n)$ have a common factor in $K'[x_n]$ where K' denotes the field of fractions of $R'/\mathfrak{p}'$. This common factor provides [2], at least, one associated prime ideal $\mathfrak{p}$ of $\mathfrak{A}$ which contains r.

---

[2] Let M' be the multiplicative family formed by the nonzero elements of $R'/\mathfrak{p}'$ so that $K' = (R'/\mathfrak{p}')_{M'}$ (with the notation of (Zariski and Samuel, 1958, IV, 9, Quotient rings, page 221)). Denote ψ the canonical ring homomorphism $R'/\mathfrak{p}' \to K'$. We have (extending homomorphisms between ground rings to polynomial rings)

$$R \xrightarrow{\ \phi\ } R'/\mathfrak{p}'[x_n] \xrightarrow{\ \psi\ } K'[x_n]\,.$$

Thus $f \in \mathfrak{p}$, using (4) and the fact that $i_n \notin \mathfrak{p}$ since it is regular in $R/\mathfrak{A}$. Thus f is a zerodivisor in $R/\mathfrak{A}$. □

Corollary 18. *Let A be a regular chain and $1 \leq k \leq n$. Then the initial i_k is regular in $R/\mathfrak{A}$. In particular,* $\mathrm{res}(i_k, A) \neq 0$.

Proof. Since A is a regular chain, $r = \mathrm{res}(i_k, \{p_1, \ldots, p_{k-1}\})$ is different from zero, by Proposition 17. Since $\mathrm{res}(i_k, A)$ is a power of r, we have $\mathrm{res}(i_k, A) \neq 0$. Thus i_k is regular in $R/\mathfrak{A}$ by Proposition 15. □

In summary, assume Condition **a** holds. Then $\mathfrak{A}$ is proper by Proposition 14. Then Condition **c** holds by Propositions 15 and 17.

5.2. Membership Testing to the Ideal

5.2.1. **a ⇒ b**

Proposition 19. *Let f be any polynomial. If* $\mathrm{prem}(f, A) = 0$ *then f is zero in $R/\mathfrak{A}$.*

Proposition 20. *Assume A is a regular chain and let f be any polynomial. If f is zero in $R/\mathfrak{A}$ then* $\mathrm{prem}(f, A) = 0$.

Proof. Given any index $2 \leq \ell \leq n$, let $r_\ell = \mathrm{res}(i_\ell, A)$ and $u_\ell, v_{\ell,1}, v_{\ell,2}, \ldots, v_{\ell,\ell-1}$ be polynomials free of $x_\ell, \ldots, x_n$ such that, according to Proposition 11, we have

$$u_\ell \, i_\ell = r_\ell + v_{\ell,1} \, p_1 + v_{\ell,2} \, p_2 + \cdots + v_{\ell,\ell-1} \, p_{\ell-1} \, . \tag{5}$$

Since A is a regular chain, all resultants r_ℓ are nonzero, by Corollary 18.

We assume f is zero in $R/\mathfrak{A}$ and $g = \mathrm{prem}(f, A) \neq 0$ and we seek a contradiction. By Lemma 3, we have $\deg(g, x_\ell) < d_\ell = \deg(p_\ell, x_\ell)$ for $1 \leq \ell \leq n$. Since $g \in \mathfrak{A}$, there exists nonnegative integers $\alpha_1, \ldots, \alpha_n$ and polynomials $v_1, \ldots, v_n$ such that

$$i_1^{\alpha_1} \cdots i_n^{\alpha_n} \, g = v_1 \, p_1 + v_2 \, p_2 + \cdots + v_n \, p_n \, . \tag{6}$$

Multiply both sides of (6) by $u_1^{\alpha_1} \cdots u_n^{\alpha_n}$ and use (5). There exists some nonzero polynomial $h_g \in K[t_1, \ldots, t_m]$ (one may take $h_g = r_1^{\alpha_1} \cdots r_n^{\alpha_n}$), some index $1 \leq k \leq n$ and some polynomials $w_1, \ldots, w_k$ such that

$$h_g \, g = \underbrace{w_1 \, p_1 + w_2 \, p_2 + \cdots + w_k \, p_k}_{\mathscr{F}} \quad (w_k \neq 0) \, .$$

The ideal $\mathfrak{A}$ of R is mapped to the ideal $\mathfrak{A}/\mathfrak{p}' = (\phi(p_n)) : (\phi(i_1) \cdots \phi(i_n))^\infty$ of $R'/\mathfrak{p}'[x_n]$, which is itself mapped to the ideal $(\psi(\phi(p_n)))$ of $K'[x_n]$. The common factor between $\psi(\phi(p_n))$ and $\psi(\phi(r))$ generates an ideal whose associated prime ideals are extended ideals w.r.t. ψ. These ideals contain $\phi(r)$. Follow ψ^{-1}: the corresponding contracted ideals are associated prime ideals of $\mathfrak{A}/\mathfrak{p}'$ by (Zariski and Samuel, 1958, IV, 10, Theorem 17, page 225). Follow ϕ^{-1}: the associated prime ideals of $\mathfrak{A}/\mathfrak{p}'$ are the images by ϕ of associated prime ideals of $\mathfrak{A}$ by (Zariski and Samuel, 1958, IV, 5, Remark concerning passage to a residue class ring, page 213). These associated prime ideals of $\mathfrak{A}$ contain r.

Consider the set $\mathscr{E}$ — which depends on g — of all such formulas $\mathscr{F}$ which evaluate to some polynomial $h_g\, g \neq 0$ with $h_g \in K[t_1, \ldots, t_m]$. By the argument above, $\mathscr{E}$ is not empty. To any formula $\mathscr{F}$ of $\mathscr{E}$, associate the index $j(\mathscr{F})$ defined as the highest index j such that x_j occurs in some w_t or some p_t. Among all formulas $\mathscr{F}$ of $\mathscr{E}$, fix one such that $j(\mathscr{F})$ is minimal. For short, denote $j = j(\mathscr{F})$, $d = d_j$ and $p_j = i_j\, x_j^d + q_j$. In the polynomials $w_1, w_2, \ldots, w_k$ of $\mathscr{F}$, substitute $x_j^d \to (p_j - q_j)/i_j$. Multiply both sides of the equality by a suitable power i_j^α of the initial i_j to clear denominators. Use again (5): multiply both sides by u_j^α, replace $(u_j\, i_j)^\alpha$ on the left-hand side by r_j^α and update the right-hand side. One obtains another formula

$$r_j^\alpha\, h_g\, g = \underbrace{w'_1\, p_1 + w'_2\, p_2 + \cdots + w'_{k'}\, p_{k'}}_{\mathscr{F}'} \quad (w'_{k'} \neq 0)$$

that we may organize so that $\deg(w'_t, x_j) < d$ for $t < j$. The formula $\mathscr{F}'$ belongs to $\mathscr{E}$ thus $j(\mathscr{F}') \geq j$. The substitution we have just performed involves polynomials free of $x_j, \ldots, x_n$. Thus $j(\mathscr{F}') \leq j$ hence $j(\mathscr{F}') = j$.

We have $j(\mathscr{F}') \geq k'$ since $w'_{k'} \neq 0$.

Assume $j(\mathscr{F}') = k'$. Since $\deg(w'_t, x_j) < d$ and $\deg(p_t, x_j) = 0$ for $t < k' = j$ and $w'_{k'} = w'_j \neq 0$, we have $\deg(r_j^\alpha\, h_g\, g, x_j) \geq d$. This contradiction with the hypothesis $\deg(g, x_j) < d$ proves that the assumption cannot hold.

Assume $j(\mathscr{F}') > k'$. One may reorganize $\mathscr{F}'$ as

$$r_j^\alpha\, h_g\, g = \mathscr{F}_0 + \mathscr{F}_1\, x_j + \mathscr{F}_2\, x_j^2 + \cdots + \mathscr{F}_{d'}\, x_j^{d'}$$

for some $d' \geq 0$ so that each formula $\mathscr{F}_t$ is a linear combination of the polynomials $p_1, p_2, \ldots, p_{k'}$ with polynomial coefficients, all free of x_j. With other words, $j(\mathscr{F}_t) < j$ for $0 \leq t \leq d'$. Since g is nonzero, at least one of these $\mathscr{F}_t$ must evaluate to some nonzero polynomial hence belong to $\mathscr{E}$. This final contradiction with the minimality hypothesis of j completes the proof of the Proposition. □

In summary, assume Condition **a** holds. Then Condition **b** holds by Propositions 19 and 20.

5.2.2. **b ⇒ a**

Proposition 21. *Let A be a triangular set such that $\mathfrak{A}$ is proper. If* $\mathrm{prem}(f, A) = 0$ *for each $f \in \mathfrak{A}$ then A is a regular chain.*

Proof. We assume the existence of an index $1 \leq k < n$ such that the regular chain condition is satisfied up to k while i_{k+1} is not regular in $R/(p_1, \ldots, p_k) : (i_1 \cdots i_k)^\infty$. We prove the existence of a polynomial $f \in \mathfrak{A}$ such that $\mathrm{prem}(f, A) \neq 0$.

Let $\mathfrak{A}_k = (p_1, \ldots, p_k) : (i_1 \cdots i_k)^\infty$ and $\mathfrak{B}_k = \mathfrak{A}_k : i_{k+1}^\infty$. Since i_{k+1} is not regular in $R/\mathfrak{A}_k$, we have $\mathfrak{B}_k \neq \mathfrak{A}_k$. Since $\mathfrak{A}$ is proper, so is $\mathfrak{B}_k$. Let $R_k = K[t_1, \ldots, t_m, x_1, \ldots, x_k]$ and $\mathfrak{q}$ be a primary component of $\mathfrak{A}_k$. By Theorem 1, we have $\mathfrak{q} \cap R_k \neq (0)$. Thus there exists some $f \in R_k$ such that $f \in \mathfrak{B}_k$, $f \notin \mathfrak{A}_k$. Since $f \in R_k$ we have $\mathrm{prem}(f, A) = \mathrm{prem}(f, A_k)$. Since $f \notin \mathfrak{A}_k$, we have $\mathrm{prem}(f, A_k) \neq 0$ (Proposition 19). Since $\mathfrak{B}_k \subset \mathfrak{A}$, the proof is completed. □

In summary, assume Condition **b** holds. Then $\mathfrak{A}$ is proper, by Proposition 14. Thus Condition **b** implies, as a particular case, the hypotheses of Proposition 21. Thus Condition **a** holds, by Proposition 21.

5.3. $\mathbf{a} \Leftrightarrow \mathbf{d}$

The following Proposition concludes the proof of Theorem 13.

Proposition 22. *A triangular set A is a regular chain if and only if* $\mathrm{res}(i_k, A) \neq 0$ *for* $2 \leq k \leq n$.

Proof. Let $2 \leq k \leq n$ be an index. Recall $\mathrm{res}(i_k, A)$ is a power of $\mathrm{res}(i_k, \{p_1, \ldots, p_{k-1}\})$ since i_k does not depend on $x_k, \ldots, x_n$.

The implication $\Rightarrow$ follows from Corollary 18.

The implication $\Leftarrow$. Assume A is not a regular chain and let $2 \leq k \leq n$ be such that $\{p_1, \ldots, p_{k-1}\}$ is a regular chain while i_k is a zerodivisor in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. Then $\mathrm{res}(i_k, \{p_1, \ldots, p_{k-1}\}) = 0$ (Proposition 15) thus $\mathrm{res}(i_k, A) = 0$. □

5.4. Changing the Ordering

The following Proposition is involved in the proof of Proposition 33.

The notion of triangular set depends on some ordering on the variables. So far, this ordering has been fixed through the numbering of the variables x_k but we need a more general definition for the following Proposition.

Let an ordering be defined over the variables. Then x is the leading variable of some polynomial p if $\deg(p, x) > 0$ and $\deg(p, y) = 0$ for any variable $y > x$. Accordingly, it is more accurate to view triangular sets as triangular lists.

Proposition 23. *Let $A = [p_1, \ldots, p_n]$ be a regular chain w.r.t. any ordering such that $x_1 < \cdots < x_n$. Let be given a second ordering over the variables such that x_j keeps being the leading variable of p_j for $1 \leq j \leq n$. Let A' be the list of the p_j, by increasing leading variable, w.r.t. this new ordering.*

Then A' is a regular chain.

Proof. It is sufficient to assume that the second ordering only permutes two variables, of indices $1 \leq k < \ell \leq n$. We show A' is a regular chain by proving it satisfies Definition 12.

We do not need to address the case of the initials of the polynomials p_j such that $j < k$ or $j > \ell$ since the corresponding ideals $(p_1, \ldots, p_{j-1}) : (i_1 \cdots i_{j-1})^\infty$ are the same, w.r.t. both orderings.

Let $k \leq j \leq \ell$ be an index. The assumption that the new ordering preserves the leading variables of the elements of A implies that the initial i_j does not depend on x_k nor on x_ℓ. Using the fact that, if f does not depend on x_i, $\mathrm{res}(f, p_i, x_i) = f^{d_i}$, we see that $\mathrm{res}(i_j, A) = \mathrm{res}(i_j, A')$. The fact that A' is a regular chain then follows from Theorem 13. □

6. Differential Algebra Preliminaries

Reference books are the ones of Ritt (1950) and Kolchin (1973).

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 and Θ^* denote the set of the *proper* derivation operators. Assume the infinite set of derivatives $\Theta\, U$ is ordered w.r.t. a ranking (Kolchin, 1973, I, 8, page 75) so that, given any differential polynomial $f \in R \setminus K$, its leading derivative $\operatorname{ld} f$ (called *leader* by Kolchin), its initial and its separant $\partial f / \partial \operatorname{ld} f$ are well defined.

A differential polynomial f is said to be *partially reduced* w.r.t. a differential polynomial $p \notin K$ if f does not depend on any proper derivative of the leading derivative of p (Kolchin, 1973, I, 9, page 77). In the sequel, A denotes a triangular set of n differential polynomials of $R \setminus K$, pairwise partially reduced.

In the sequel, we need to define the pseudodivision and the resultant of a differential polynomial f by $\Theta\, A$.

The differential polynomial $g = \operatorname{prem}(f, \Theta\, A)$ (respectively $g = \operatorname{res}(f, \Theta\, A)$) is obtained by computing a sequence $f = f_0, f_1, \ldots, f_\ell = g$ of differential polynomials such that $f_{k+1} = \operatorname{prem}(f_k, \theta\, p, \operatorname{ld} \theta\, p)$ (respectively $f_{k+1} = \operatorname{res}(f_k, \theta\, p, \operatorname{ld} \theta\, p)$) where $p \in A$ and $\theta \in \Theta$. We apply the traditional strategy: choosing a pair (θ, p), which needs not be uniquely defined, 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. The sequence of f_k is finite, because rankings are well-orderings (Kolchin, 1973, I, 8, page 75).

The case of the resultant calls a specific remark, related to the comment following Proposition 11: if p is any differential polynomial of $R \setminus K$ and $\theta \in \Theta^*$, then the degree of $\theta\, p$ in its leading derivative is 1, which implies that, given any $f \in R$, there exists a finite subset $A' \subset \Theta\, A$ such that $\operatorname{res}(f, \Theta\, A) = \operatorname{res}(f, A')$. In particular, the resultant of f w.r.t. the infinite set $\Theta\, A$ is well-defined. Of course, the same property holds also for the pseudoremainder, but is more straightforward.

Let $f \notin K$ be any differential polynomial.

Then $\operatorname{prem}(f, \Theta^*\, A)$ denotes the *partial remainder* of f by A (Kolchin, 1973, I, 9, page 77). The result is a differential polynomial g, partially reduced w.r.t. A, such that, for some power product h_f of separants of A, we have $h_f\, f \equiv g \pmod{\mathfrak{B}}$, where $\mathfrak{B}$ stands for the ideal of R generated by all proper derivatives of A whose leading derivatives are less than or equal to the one of f.

Similarly, $\operatorname{prem}(f, \Theta\, A)$ denotes the (full) *remainder* of f by A (Kolchin, 1973, I, 9, page 79). The result is a differential polynomial g, partially reduced w.r.t. A, such that, for some power product h_f of initials and separants of A, we have

$$h_f\, f \equiv g \pmod{\mathfrak{B}}\,, \tag{7}$$

where $\mathfrak{B}$ stands for the ideal of R generated by all derivatives of A (not necessarily proper) whose leading derivatives are less than or equal to the one of f.

In the sequel, we will sometimes decompose $g = \operatorname{prem}(f, \Theta\, A)$ as $g = \operatorname{prem}(g^*, A)$ where $g^* = \operatorname{prem}(f, \Theta^*\, A)$ (this is actually Ritt and Kolchin way of presenting the full

remainder). Strictly speaking, both computations are not completely equivalent. However, relation (7) holds in both cases. This permits us to perform this abuse in all proofs which only rely on the existence of such a relation.

In the case $m \geq 2$, there may exist subsets $\{p_1, p_2\} \subset A$, called *critical pairs*, such that the leading derivatives $\theta_1\, u$ of p_1 and $\theta_2\, u$ of p_2 are derivatives of some common differential indeterminate u. Define $\theta_{12} = \mathrm{lcm}(\theta_1, \theta_2)$ (observe $\theta_{12} \neq \theta_1, \theta_2$ because of our assumptions on A) and the Δ-*polynomial* associated to the critical pair as $\Delta(p_1, p_2) = s_1 \frac{\theta_{12}}{\theta_2}\, p_2 - s_2 \frac{\theta_{12}}{\theta_1}\, p_1$ where s_1, s_2 are the separants of p_1, p_2. The critical pair is said to be *solved* if we have $\mathrm{prem}(\Delta(p_1, p_2), \Theta\, A) = 0$. The set A is said to be *coherent* if all its critical pairs are solved.

The following Theorem appears in (Rosenfeld, 1959, Lemma). It generalizes (Seidenberg, 1956, Theorem 6). A generalized version is available in (Kolchin, 1973, III, 8, pages 135-138) but Kolchin's version does not clearly appear to be algorithmic. The ideals $[A] : h^\infty$ and $(A) : h^\infty$ are denoted $[A] : H_A^\infty$ and $(A) : H_A^\infty$ by Kolchin.

Theorem 24. *(Rosenfeld's Lemma)*
Let A be a triangular set of pairwise partially reduced differential polynomials 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 $(A) : h^\infty$.

7. The Main Theorem

Lemaire (2002) introduced the definition of *regular differential chains* and proved the equivalence **a** $\Leftrightarrow$ **b** of Theorem 26. The other equivalences are new.

Definition 25. A triangular set A of pairwise partially reduced differential polynomials is said to be a *regular differential chain* if it satisfies the following conditions:
1 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 $2 \leq k \leq n$;
2 the separant s_k of p_k is regular in $R/(A) : (i_1 \cdots i_n)^\infty$ for $1 \leq k \leq n$;
3 A is coherent (meaningful only if $m \geq 2$).

In some other texts such as (Boulier and Lemaire, 2010, Definition 3.1), Condition **2** is replaced by: *the separant s_k of p_k is regular in $R/(A) : (i_1 \cdots i_k)^\infty$ for $1 \leq k \leq n$*, known also as *squarefree regular chain* condition. Both conditions are actually equivalent by Theorem 13 and the fact that $\mathrm{res}(s_k, A)$ is a power of $\mathrm{res}(s_k, \{p_1, \ldots, p_k\})$.

Theorem 26. *Let A be a triangular set of pairwise partially reduced differential polynomials, h be the product of its initials and separants and $\mathfrak{A} = [A] : h^\infty$. The following conditions are equivalent:*
a *A is a regular differential chain;*
b *for any differential polynomial f, we have $\mathrm{prem}(f, \Theta\, A) = 0$ if and only if f is zero in $R/\mathfrak{A}$;*
c *for any differential polynomial f, we have $\mathrm{res}(f, \Theta\, A) = 0$ if and only if f is a zerodivisor in $R/\mathfrak{A}$.*
d *$\mathrm{res}(i_k, A) \neq 0$ for each $2 \leq k \leq n$, $\mathrm{res}(s_k, A) \neq 0$ for each $1 \leq k \leq n$ and A is coherent.*

From now on, all Propositions aim at proving Theorem 26.

Proposition 27. *If a triangular set A of pairwise partially reduced differential polynomials satisfies any of Conditions* ***a****,* ***b*** *or* ***c*** *then the differential ideal $\mathfrak{A}$ is necessarily proper.*

Proof. If $\mathfrak{A} = R$ then every element of $R/\mathfrak{A}$ is zero and a zerodivisor. Thus the regular chain condition involved in Condition **a** cannot hold. Moreover, if f is any nonzero differential polynomial partially reduced w.r.t. A then $\mathrm{prem}(f, A) \neq 0$ and $\mathrm{res}(f, A) \neq 0$. Thus Conditions **b** and **c** cannot hold either. □

7.1. Membership Testing to the Ideal

Proposition 28. *Let A be any set of differential polynomials of $R \setminus K$, h be the product of its initials and separants and $\mathfrak{A} = [A] : h^\infty$. If $\mathrm{prem}(f, \Theta A) = 0$ then f is zero in $R/\mathfrak{A}$.*

7.1.1. **a ⇒ b**

Proposition 29. *Let A be a coherent triangular set of pairwise partially reduced differential polynomials, h be the product of its initials and separants, $\mathfrak{A} = [A] : h^\infty$, $\mathfrak{B} = (A) : h^\infty$, f be a differential polynomial and $g = \mathrm{prem}(f, \Theta^* A)$.*

Then f is zero in $R/\mathfrak{A}$ if and only if g is zero in $R/\mathfrak{B}$.

Proof. The differential polynomial is zero in $R/\mathfrak{A}$ if and only if g is zero in $R/\mathfrak{A}$. The partial remainder g is partially reduced w.r.t. A. By Theorem 24 (Rosenfeld Lemma), g is zero in $R/\mathfrak{A}$ if and only if g is zero in $R/\mathfrak{B}$. □

Proposition 30. *Let A be a regular differential chain, h be the product of its initials and separants, $\mathfrak{A} = [A] : h^\infty$ and f be a differential polynomial.*

If f is zero in $R/\mathfrak{A}$ then $\mathrm{prem}(f, \Theta A) = 0$.

Proof. Denote $\mathfrak{B}_1 = (A) : h^\infty$ and $\mathfrak{B}_2 = (A) : (i_1 \cdots i_n)^\infty$. Let us consider some $f \in \mathfrak{A}$ and denote $g = \mathrm{prem}(f, \Theta A)$ (the full remainder of f by A). Since g is partially reduced w.r.t. A, Theorem 24 (Rosenfeld's Lemma) applies and $g \in \mathfrak{B}_1$. Since the separants of A are regular in $R/\mathfrak{B}_2$, we have $\mathfrak{B}_1 = \mathfrak{B}_2$ thus $g \in \mathfrak{B}_2$. Since $g = \mathrm{prem}(g, A)$ and A is a regular chain, by Theorem 13, $g = 0$. □

In summary, assume Condition **a** holds. Then Condition **b** holds by Propositions 28 and 30.

7.1.2. **b ⇒ a**

Proposition 31. *Let A be a triangular set of pairwise partially reduced differential polynomials of R and h be the product of its initials and separants. Assume $\mathfrak{A} = [A] : h^\infty$ is proper.*

Assume that, for any f which is zero in $R/\mathfrak{A}$ we have $\mathrm{prem}(f, \Theta A) = 0$. Then A is a regular differential chain.

Proof. Denote R_1 the ring of the differential polynomials of R partially reduced w.r.t. A. Let $\mathfrak{A}_1 = \mathfrak{A} \cap R_1$, $\mathfrak{B}_1 = (A) : h^\infty$ and $\mathfrak{B}_2 = (A) : (i_1 \cdots i_n)^\infty$ be three ideals of R_1.

Consider some $f \in R_1$. If $\mathrm{prem}(f, A) = 0$ then $f \in \mathfrak{B}_2$. Conversely, if $f \in \mathfrak{B}_2$ then $f \in \mathfrak{A}$ and, by assumption, $\mathrm{prem}(f, \Theta A) = \mathrm{prem}(f, A) = 0$. Therefore, by Theorem 13, A is a regular chain and Condition **1** of Definition 25 holds.

All the Δ-polynomials that can be formed using A belong to $\mathfrak{A}$. They are thus reduced to zero by A through the pseudodivision process. Therefore A is coherent and Condition **3** of Definition 25 holds.

Thus Theorem 24 (Rosenfeld's Lemma) applies and $\mathfrak{A}_1 = \mathfrak{B}_1$.

Last, we prove Condition **2** by establishing that $\mathfrak{B}_1 = \mathfrak{B}_2$ (this is indeed sufficient for the separants of the elements of A which occur in h as factors, are regular in $R/\mathfrak{B}_1$). Let $f \in R_1$. Then $\mathrm{prem}(f, A) = \mathrm{prem}(f, \Theta A)$. Thus, combining the assumption and Proposition 28, we see, on the one hand, that $\mathrm{prem}(f, A) = 0$ if and only if $f \in \mathfrak{B}_1$. On the other hand, we have proven that A is a regular chain so that Theorem 13 applies and $\mathrm{prem}(f, A) = 0$ if and only if $f \in \mathfrak{B}_2$. Thus $\mathfrak{B}_1 = \mathfrak{B}_2$ and Condition **2** holds.

Thus A is a regular differential chain. □

In summary, assume Condition **b** holds. Then $\mathfrak{A}$ is proper by Proposition 27. Thus Condition **b** implies, as a particular case, the hypotheses of Proposition 31. Thus Condition **a** holds by Proposition 31.

7.2. Regularity Testing modulo the Ideal

In this section, we will sometimes consider finitely generated nondifferential ideals $\mathfrak{B}$ belonging to the polynomial ring R_1 of the differential polynomials partially reduced w.r.t. some given set A. In general R_1 is a polynomial ring in infinitely many indeterminates. It is thus not Nötherian. However, since the finite bases of $\mathfrak{B}$ only feature finitely many indeterminates, it is always possible, in proofs, to restrict further R_1 to some polynomial ring in finitely many indeterminates, hence to a Nötherian ring, in which the Lasker-Nöther Theorem applies. For simplicity, we will not explicitly perform this restriction. We will thus allow ourselves to apply the Lasker-Nöther Theorem to the finitely generated ideals $\mathfrak{B}$ of R_1.

The following Theorem is proved in Boulier et al. (2009).

Theorem 32. *Let A be a coherent triangular set of pairwise partially reduced differential polynomials, h be the product of its initials and separants, $\mathfrak{A} = [A] : h^\infty$, R_1 be the ring of the differential polynomials partially reduced w.r.t. A and $\mathfrak{B} = (A) : h^\infty$ in R_1.*

Then $\mathfrak{A}$ and $\mathfrak{B}$ are radical and there is a one-to-one correspondence between the associated differential prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathfrak{A}$ and the associated prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathfrak{B}$, given by $\mathfrak{p}_i = \mathfrak{P}_i \cap R_1$ for $1 \leq i \leq r$.

Proof. Since h contains each separant of A as a factor, Theorem 2 (Lazard's Lemma) applies and $\mathfrak{B}$ is radical.

Let f be a differential polynomial such that $f^d \in \mathfrak{A}$ for some $d \geq 0$. Let $g = \mathrm{prem}(f, \Theta^* A)$ where Θ^* denotes the set of all proper derivation operators (so that g is the partial remainder of f by A). Then $g^d \in \mathfrak{A}$. Since g is partially reduced w.r.t. A, Theorem 24 (Rosenfeld's Lemma) applies and $g^d \in \mathfrak{B}$. Since $\mathfrak{B}$ is radical, $g \in \mathfrak{B}$. Thus $g \in \mathfrak{A}$ and so does f. The differential ideal $\mathfrak{A}$ 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, $\mathfrak{B} = \cap_{i=1}^r \mathfrak{p}_i$ 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 $f \in \cap_{i=2}^r \mathfrak{P}_i$ be a differential polynomial and $g = \mathrm{prem}(f, \Theta^* A)$. Since $g \in R_1$, we have $g \in \cap_{i=2}^r \mathfrak{p}_i$ hence $g \in \mathfrak{B}$ since $\mathfrak{p}_1$ is redundant. Thus $f \in \mathfrak{A}$ by Proposition 29 and $\mathfrak{P}_1$ is redundant. □

Proposition 33. *Let A be a regular differential chain and A' be a triangular set of differential polynomials such that $A \subset A' \subset \Theta A$.*

Then A' is a regular chain.

Proof. Assume (easy case) that the leading derivatives of the elements of $A' \setminus A$ are all greater than the leading derivatives of A, w.r.t. the ranking. By the fact that the initials of $A' \setminus A$ are the separants of A, the fact that the regular chain is squarefree (Condition **2** of Definition 25) and Definition 12, one concludes that A' is a regular chain.

Assume now that some leading derivatives of $A' \setminus A$ are lower than some leading derivatives of A. Since A is differentially triangular and its elements are pairwise partially reduced, there exists another ordering on the leading derivatives of A', which does not change the leading derivatives of A', and belongs to the easy case. W.r.t. this other ordering, A' is a regular chain.

Therefore A' is a regular chain w.r.t. the ranking also, by Proposition 23. □

The following Theorem contains Theorems 24 and 32 as a special case, by taking $f = 0$.

Theorem 34. *Let A be a coherent triangular set of pairwise partially reduced differential polynomials, h be the product of its initials and separants and $\mathfrak{A} = [A] : h^\infty$.*

Let f be a differential polynomial, $A' \subset \Theta A$ be the union of A and the elements of ΘA involved in the computation of $\operatorname{res}(f, \Theta A)$. Let $R' \subset R$ be the smallest polynomial ring containing A' and $\mathfrak{A}' = (A') : h^\infty$ in R'.

Then $\mathfrak{A}' = \mathfrak{A} \cap R'$, both ideals are radical, and there is a one-to-one correspondence between the associated differential prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathfrak{A}$ and the associated prime ideals $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_r$ of $\mathfrak{A}'$, given by $\mathfrak{p}'_i = \mathfrak{P}_i \cap R'$ for $1 \leq i \leq r$.

Proof. The algorithm applied to compute $\operatorname{res}(f, \Theta A)$ ensures that A' is triangular. Thus Proposition 33 applies and A' is a regular chain.

Since h contains each separant of A' as a factor, Theorem 2 (Lazard's Lemma) applies and $\mathfrak{A}'$ is radical.

We have $\mathfrak{A}' \subset \mathfrak{A} \cap R'$. Consider some $f_2 \in \mathfrak{A} \cap R'$ and define $g_2 = \operatorname{prem}(f_2, A')$. The set A' contains enough differential polynomials to ensure that g_2 is partially reduced w.r.t. A. Thus $g_2 \in (A) : h^\infty$ by Theorem 24 (Rosenfeld's Lemma). Since $(A) : h^\infty \subset \mathfrak{A}'$ we have $g_2 \in \mathfrak{A}'$ hence $f_2 \in \mathfrak{A}'$. Thus $\mathfrak{A}' = \mathfrak{A} \cap R'$.

Using the same argument as in the proof of Theorem 32, this equality and the radicality of $\mathfrak{A}'$ imply that $\mathfrak{A}$ is radical.

The intersection of a prime ideal of R and the subring $R' \subset R$ is a prime ideal of R'. Therefore $\mathfrak{A}' = \cap_{i=1}^r \mathfrak{p}'_i$ where $\mathfrak{p}'_i = \mathfrak{P}_i \cap R'$ 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. Using Theorem 32 and the fact that $(A) : h^\infty \subset \mathfrak{A}'$ we see that $\mathfrak{P}_i \cap R' \neq (0)$ for $1 \leq i \leq r$. We may thus consider some nonzero $f_2 \in \cap_{i=2}^r \mathfrak{P}_i \cap R'$. Then $f_2 \in \cap_{i=2}^r \mathfrak{p}'_i$ hence $f_2 \in \mathfrak{A}'$ since $\mathfrak{p}'_1$ is redundant. Therefore $f_2 \in \mathfrak{A}$ and $\mathfrak{P}_1$ is redundant. □

7.2.1. **a ⇒ c**

Proposition 35. *Let A be a regular differential chain, h be the product of its initials and separants, $\mathfrak{A} = [A] : h^\infty$ and f be a differential polynomial.*

Then $\mathrm{res}(f, \Theta A) = 0$ *if and only if f is a zerodivisor in $R/\mathfrak{A}$.*

Proof. Let $A' \subset \Theta A$ be the union of A and the elements of ΘA involved in the computation of $\mathrm{res}(f, \Theta A)$ and $\mathfrak{A}' = (A') : h^\infty$.

The algorithm applied to compute $\mathrm{res}(f, \Theta A)$ ensures that A' is triangular. Thus Proposition 33 applies and A' is a regular chain. Thus Theorem 13 applies and we have $\mathrm{res}(f, \Theta A) = \mathrm{res}(f, A') = 0$ if and only if f is a zerodivisor in $R/\mathfrak{A}'$ i.e. if and only if f belongs to an associated prime ideal of $\mathfrak{A}'$. Thus, by Theorem 34, $\mathrm{res}(f, \Theta A) = 0$ if and only if f belongs to some associated differential prime ideal of $\mathfrak{A}$ i.e. is a zerodivisor in $R/\mathfrak{A}$. □

In summary, assume Condition **a** holds. Then Condition **c** holds also, by Proposition 35.

7.2.2. **c ⇒ a**

Proposition 36. *Let A be a triangular set of pairwise partially reduced differential polynomials and h be the product of its initials and separants. Assume $\mathfrak{A} = [A] : h^\infty$ is proper. Assume that, for any differential polynomial f, we have* $\mathrm{res}(f, \Theta A) = 0$ *if and only if f is a zerodivisor in $R/\mathfrak{A}$.*

Then A is a regular differential chain.

Proof. Denote R_1 the ring of the differential polynomials of R partially reduced w.r.t. A.

Let $\mathfrak{A}_1 = \mathfrak{A} \cap R_1$ and $\mathfrak{B}_2 = (A) : (i_1 \cdots i_n)^\infty$ be two ideals of R_1.

We first prove Condition **1** of Definition 25 holds, i.e. that A is a regular chain. Let $1 \leq k \leq n$ be an index. The initial i_k is regular in $R_1/\mathfrak{A}_1$ since $\mathfrak{A}_1 = \mathfrak{A}_1 : h^\infty$. We need to show that i_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. Decompose $\mathrm{res}(i_k, A) = \mathrm{res}(r_k, \{p_1, \ldots, p_{k-1}\})$ where $r_k = \mathrm{res}(i_k, \{p_k, \ldots, p_n\})$. By assumption, $\mathrm{res}(i_k, A) \neq 0$ thus $\mathrm{res}(r_k, \{p_1, \ldots, p_{k-1}\}) \neq 0$. Thus r_k is regular in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$ by Proposition 15. Since i_k does not depend on the leading derivatives of $p_k, \ldots, p_n$, 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 and Condition **1** holds.

Let $f, g \notin \mathfrak{A}$ such that $f\, g \in \mathfrak{A}$ so that f is a zerodivisor in $R/\mathfrak{A}$. Let $f' = \mathrm{prem}(f, \Theta^* A)$ and $g' = \mathrm{prem}(g, \Theta^* A)$ be their partial remainders w.r.t. A. Since $\mathfrak{A}$ is saturated by the separants of A, we have $f', g' \notin \mathfrak{A}$ and $f'\, g' \in \mathfrak{A}$. Therefore, if $f \in R_1$ is a zerodivisor in $R/\mathfrak{A}$ then it is a zerodivisor in $R_1/\mathfrak{A}_1$.

We now prove Condition **2** by establishing that the rings $R_1/\mathfrak{A}_1$ and $R_1/\mathfrak{B}_2$ have the same set of zerodivisors (this is indeed sufficient for the separants of the elements of A, which occur in h as factors, are regular in $R_1/\mathfrak{A}_1$).

Let $f \in R_1$. Then $\mathrm{res}(f, \Theta A) = \mathrm{res}(f, A)$. On the one hand, according to our assumptions, $\mathrm{res}(f, A) = 0$ if and only if f is a zerodivisor in $R_1/\mathfrak{A}_1$. On the other hand, we have proven that A is a regular chain so that Theorem 13 applies and $\mathrm{res}(f, A) = 0$ if and only if f is a zerodivisor in $R_1/\mathfrak{B}_2$. Thus $R_1/\mathfrak{A}_1$ and $R_1/\mathfrak{B}_2$ have the same set of zerodivisors, the separants of A are regular in $R_1/\mathfrak{B}_2$ and Condition **2** holds.

Last, we prove Condition **3** holds i.e. that A is coherent. We have just proven above that $R_1/\mathfrak{A}_1$ and $R_1/\mathfrak{B}_2$ have the same set of zerodivisors. This implies that they have the same set associated prime ideals by (Zariski and Samuel, 1958, IV, 6, Corollary 3 to Theorem 11, page 214). They thus have the same radical. Since Condition **2** holds, Theorem 2 (Lazard's Lemma) applies and $\mathfrak{B}_2$ is radical. Therefore, $\sqrt{\mathfrak{A}_1} = \mathfrak{B}_2$. Let Δ_{ij} be any Δ-polynomial of A and $f = \mathrm{prem}(\Delta_{ij}, \Theta\, A)$. We have $f \in \mathfrak{A}_1$ hence $f \in \mathfrak{B}_2$. Since $\mathrm{prem}(f, A) = f$ and A is a regular chain, Theorem 13 applies thus f is zero. Thus A is coherent and Condition **3** holds.

Thus A is a regular differential chain. □

In summary, assume Condition **c** holds. Then $\mathfrak{A}$ is proper by Proposition 27. Thus Condition **a** holds by Proposition 36.

7.3. **a ⇔ d**

The following Proposition concludes the proof of Theorem 26.

Proposition 37. *A triangular set A of pairwise partially reduced differential polynomials is a regular differential chain if and only if* $\mathrm{res}(i_k, A) \neq 0$ *for each* $2 \leq k \leq n$, $\mathrm{res}(s_k, A) \neq 0$ *for each* $1 \leq k \leq n$ *and A is coherent.*

Proof. Recall that, if there exists an index $1 \leq k \leq n$ such that f does not depend on the leading derivatives of $p_k, \ldots, p_n$, then $\mathrm{res}(f, A)$ is a power of $\mathrm{res}(f, \{p_1, \ldots, p_{k-1}\})$.

The implication ⇒. Assume A is a regular differential chain. Then A is a regular chain (Condition **1** of Definition 25) and $\mathrm{res}(i_k, A) \neq 0$ by Theorem 13. The separants of A are regular in $R/(A) : (i_1 \cdots i_n)^\infty$ (Condition **2** of Definition 25) hence $\mathrm{res}(s_k, A) \neq 0$ for each $1 \leq k \leq n$ by Theorem 13 again. Last, A is coherent (Condition **3** of Definition 25).

The implication ⇐. Assume A is not a regular differential chain. Then Condition **1**, **2** or **3** of Definition 25 must fail. If Condition **3** fails then A is not coherent. Assume Condition **3** holds for A. Then there exists some index $1 \leq k < n$ such that $\{p_1, \ldots, p_{k-1}\}$ satisfies Conditions **1** and **2** while $\{p_1, \ldots, p_k\}$ fails to satisfy one of them. If Condition **1** fails for $\{p_1, \ldots, p_k\}$ then $k \geq 2$ and i_k is a zerodivisor in $R/(p_1, \ldots, p_{k-1}) : (i_1 \cdots i_{k-1})^\infty$. Thus, by Theorem 13, applied over $\{p_1, \ldots, p_{k-1}\}$, we have $\mathrm{res}(i_k, \{p_1, \ldots, p_{k-1}\}) = 0$ hence $\mathrm{res}(i_k, A) = 0$. Assume Condition **1** holds for $\{p_1, \ldots, p_k\}$. Then Condition **2** must fail for $\{p_1, \ldots, p_k\}$ and by Theorem 13 again, applied over $\{p_1, \ldots, p_k\}$, we have $\mathrm{res}(s_k, \{p_1, \ldots, p_k\}) = 0$, hence $\mathrm{res}(s_k, A) = 0$. □

References

Aubry, P., Lazard, D., Moreno Maza, M., 1999. On the Theories of Triangular Sets. Journal of Symbolic Computation 28, 105–124.

Basu, S., Pollack, R., Roy, M.-F., 2003. Algorithms in Real Algebraic Geometry. Vol. 10 of Algorithms and Computation in Mathematics. Springer Verlag.

Boulier, F., 1994. Étude et implantation de quelques algorithmes en algèbre différentielle. Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, `http://tel.archives-ouvertes.fr/tel-00137866`.

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

Boulier, F., Cheb-Terrab, E., 2008. `DifferentialAlgebra`. Package of MapleSoft MAPLE standard library since MAPLE 14.

Boulier, F., Hubert, É., 1996. `diffalg`. Package of MapleSoft MAPLE standard library from MAPLE V to MAPLE 13.

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

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 2009. Computing representations for radicals of finitely generated differential ideals. Applicable Algebra in Engineering, Communication and Computing 20 (1), 73–121, (1997 Techrep. IT306 of the LIFL). URL `http://dx.doi.org/10.1007/s00200-009-0091-7`

Boulier, F., Lemaire, F., 2010. A Normal Form Algorithm for Regular Differential Chains. Mathematics in Computer Science 4 (2), 185–201, 10.1007/s11786-010-0060-3. URL `http://dx.doi.org/10.1007/s11786-010-0060-3`

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D^5 principle. In: Proceedings of Transgressive Computing 2006. Granada, Spain, pp. 79–91, `http://hal.archives-ouvertes.fr/hal-00137158`.

Boulier, F., Lemaire, F., Sedoglavic, A., 2011. On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains. In: Proceedings of Computer Algebra in Scientific Computing, LNCS 6885. Kassel, Germany, pp. 61–72, `http://hal.archives-ouvertes.fr/hal-00599440`.

Chen, C., Lemaire, F., Moreno Maza, M., Pan, W., 2007. Comprehensive Triangular Decompositions. In: Proceedings of CASC'07. pp. 73–101.

Chou, S.-C., Gao, X.-S., 1993. On the dimension of an arbitrary ascending chain. Chinese Bulletin of Science 38, 799–904.

Cox, D., Little, J., O'Shea, D., 2005. Using Algebraic Geometry, 2nd Edition. Vol. 185 of Graduate Texts in Mathematics. Springer Verlag, New York.

Fliess, M., 1989. Automatique et corps différentiels. Forum Math. 1, 227–238.

Gao, X.-S., Van Der Hoeven, J., Yuan, C. M., Zhang, G. L., 2009. Ritt-Wu's Characteristic Set Method for Differential-Difference Polynomial Systems. Journal of Symbolic Computation 44 (9), 1137–1163.

Grigoriev, D. Y., 1987. Complexity of quantifier elimination in the theory of ordinary differential equations. Vol. 378 of Lecture Notes in Computer Science. Springer Verlag, pp. 11–25.

Hubert, É., 2000. Factorization free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29 (4,5), 641–662.

Kalkbrener, M., 1993. A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. Journal of Symbolic Computation 15, 143–167.

Kolchin, E. R., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.

Lemaire, F., January 2002. Contribution à l'algorithmique en algèbre différentielle. Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, (in French).

Ljung, L., Glad, S. T., 1994. On global identifiability for arbitrary model parametrisations. Automatica 30, 265–276.

Morrison, S., december 1995. Yet another proof of Lazard's lemma. private communication.

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

Ollivier, F., 1990. Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité. Ph.D. thesis, École Polytechnique, Palaiseau, France.

Ritt, J. F., 1932. Differential equations from the algebraic standpoint. Vol. 14 of American Mathematical Society Colloquium Publications. American Mathematical Society, New York.

Ritt, J. F., 1950. Differential Algebra. Vol. 33 of American Mathematical Society Colloquium Publications. American Mathematical Society, New York.

Rosenfeld, A., 1959. Specializations in differential algebra. Trans. Amer. Math. Soc. 90, 394–407.

Seidenberg, A., 1956. An elimination theory for differential algebra. Univ. California Publ. Math. (New Series) 3, 31–65.

Wang, D., 1996. An elimination method for differential polynomial systems I. Systems Science and Mathematical Sciences 9 (3), 216–228.

Wu, W., 1989. On the foundation of algebraic differential geometry. Mechanization of Mathematics, research preprints 3, 2–27.

Yang, L., Zhang, J., 1994. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Artificial Intelligence in Mathematics, 147–156.

Zariski, O., Samuel, P., 1958. Commutative Algebra. Van Nostrand, New York, Also volumes 28 and 29 of the Graduate Texts in Mathematics, Springer Verlag.