# Well known theorems on triangular systems and the $D^5$ principle

François Boulier    François Lemaire    Marc Moreno Maza

**Abstract**

The theorems that we present in this paper are very important to prove the correctness of triangular decomposition algorithms. The most important of them are not new but their proofs are. We illustrate how they articulate with the $D^5$ principle.

## Introduction

This paper presents the proofs of theorems which constitute the basis of the triangular systems theory: the equidimensionality (or unmixedness) theorem for which we give two formulations (Theorems 1.1 and 1.6) and Lazard's lemma (Theorem 2.1). The first section of this paper is devoted to the proof of the equidimensionality theorem. Our proof is original since it covers in the same time the ideals generated by triangular systems saturated by the set of the initials of the system (i.e. of the form $(A) : I_A^\infty$) and those saturated by the set of the separants of the system (i.e. of the form $(A) : S_A^\infty$). The former type of ideal naturally arises in polynomial problems while the latter one naturally arises in the differential context. Our proof shows also the key role of Macaulay's unmixedness theorem [24, chapter VII, paragraph 8, Theorem 26]. Its importance in the context of triangular systems was first demonstrated by Morrison in [14] and published in [15]. In her papers, Morrison aimed at completing the proof of Lazard's lemma provided in [3, Lemma 2]. Thus Morrison only considered the case of the ideals of the form $(A) : S_A^\infty$, which are the ideals w.r.t. which Lazard's lemma applies. The case of the ideals of the form $(A) : I_A^\infty$ was addressed in [2]. The proof of [2, Theorem 5.1] involves the same gap as that given in [3, Lemma 2]. It was fixed in [1]. The proof provided in [1] does not explicitly use Macaulay's theorem but relies on the properties of regular sequences in Cohen–Macaulay rings, which are the rings in which Macaulay's theorem applies.

What is this gap in the proofs mentioned above ? Among all the indeterminates the elements of a triangular system $A$ depend on, denote $t_1, \ldots, t_m$ the ones which are not main indeterminates. The proofs given in [2, Theorem 5.1] and in [3, Lemma 2] rely implicitly on the assumption that the non zero polynomials which only depend on $t_1, \ldots, t_m$ are not zero divisors modulo the ideal defined by $A$. This assumption is indeed true but certainly deserves a specific proof.

In the case of the ideals of the form $(A) : I_A^\infty$, let's mention the equidimensionality result of [19] which is not sufficient since it does not solve the problem of the embedded associated prime ideals of $(A):I_A^\infty$. In the case of the ideals of the form $(A):S_A^\infty$, there is a simple proof [16, 4] which unfortunately does not seem to generalize to the ideals of the form $(A):I_A^\infty$.

The second section of this paper is devoted to the proof of Lazard's lemma. This lemma was communicated by Lazard to the first author a few days before his PhD defense in 1994, with a sketch of proof. The proof given here is very close to the original one. As stated above, Lazard's lemma was first published in [3] but its first complete proof is due to Morrison [14, 15]. Among the few other proofs published afterwards, let's mention the ones given in [18, 4, 8, 17].

In the remaining sections, we show how the equidimensionality theorem and Lazard's lemma apply to the so called "regular chains" [11, 9, 23, 2]. We last recall a few basic algorithms which carry out a generalization of the "$D^5$" principle [6] for regular chains and which implictly rely on the equidimensionality theorem. Historically, the "$D^5$" principle suggests to compute modulo zero dimensional ideals presented by triangular systems as if these ideals were prime (whenever a zero divisor is exhibited, the ideal is split). It is its generalization to non zero dimensional ideals which requires the equidimensionality theorem.

Throughout this paper, $K$ denotes a commutative field of characteristic zero.

# 1 The equidimensionality theorem

In the polynomial ring $R = K[x_1, \ldots, x_n, t_1, \ldots, t_m]$, we consider a polynomial system $A = \{p_1, \ldots, p_n\}$. We assume that $\deg(p_i, x_i) > 0$ and $\deg(p_i, x_k) = 0$ for all $1 \leq i \leq n$ and $i < k \leq n$ i.e. that $A$ is a triangular system w.r.t. to at least one ordering such that $x_1 < \cdots < x_n$ and that the $x$ indeterminates are precisely the main indeterminates of the elements of $A$. The initial of a polynomial $p_i$ is the leading coefficient of $p_i$, viewed as a univariate polynomial in $x_i$. The separant of $p_i$ is the polynomial $\partial p_i / \partial x_i$.

In the following, $h$ denotes either the product of the initials of all the elements of $A$ or the product of the separants of all the elements of $A$.

We are concerned by the properties of the ideal $\mathfrak{A} = (A) : h^\infty$ which is the set of all the polynomials $f \in R$ such that, for some nonnegative integer $r$ and some $\lambda_1, \ldots, \lambda_n \in R$ we have $h^r f = \lambda_1 p_1 + \cdots + \lambda_r p_r$. When $h$ is the product of the initials of the elements of $A$, the ideal $\mathfrak{A}$ is often denoted $(A) : I_A^\infty$ in the literature. When $h$ is the product of the separants, the ideal $\mathfrak{A}$ is often denoted $(A) : S_A^\infty$.

In general, the ideal $\mathfrak{A}$ may be the trivial ideal $R$ (take $A = \{x_1, x_1 x_2\}$). We assume this is not the case.

Denote $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$ the polynomial ring obtained by "moving the $t$ indeterminates in the base field" of $R$ and $\mathfrak{A}_0$ the ideal $(A) : h^\infty$ in the ring $R_0$. Denote $M$ the multiplicative family generated by the nonzero elements of $K[t_1, \ldots, t_m]$ so that $R_0 = M^{-1} R$. The elements of $R_0/\mathfrak{A}_0$, which is isomorphic to $(M/\mathfrak{A})^{-1}(R/\mathfrak{A})$, have the form $a/b$ where $a \in R/\mathfrak{A}$ and $b \in M/\mathfrak{A}$. In this section, we prove the following theorem.

**Theorem 1.1.** *An element $a \in R/\mathfrak{A}$ is zero (respectively regular[1]) if and only if every element $a/b \in R_0/\mathfrak{A}_0$ is zero (respectively regular).*

[1] regular = not a zero divisor.

**Proposition 1.2.** *To prove Theorem 1.1, it is sufficient to prove that every element of $M/\mathfrak{A}$ is regular.*

*Proof.* This is a very classical proposition. If every element of $M/\mathfrak{A}$ is regular then $R_0/\mathfrak{A}_0$, is a subring of the total ring of fractions of $R/\mathfrak{A}$ [24, chapter IV, paragraph 9]. The proposition then follows [24, chapter I, paragraph 19, Corollary 1]. □

Let us recall the Lasker–Noether theorem [24, chapter IV, Theorems 4 and 6].

**Theorem 1.3.** *(Lasker–Noether theorem)*
*In a noetherian ring, every ideal is a finite intersection of primary ideals. Every representation of an ideal $\mathfrak{A}$ as an intersection of primary ideals can be minimized by removing on the one hand the redundant primary ideals and by grouping on the other hand the primary ideals whose intersection is itself primary. The so obtained minimal primary decomposition of $\mathfrak{A}$ is not uniquely defined. However, the number of its components and the radicals of its components (the so called "associated prime ideals" of $\mathfrak{A}$) are uniquely defined.*

All the rings considered in this section are noetherian.

**Proposition 1.4.** *To prove Theorem 1.1, it is sufficient to prove that no associated prime ideal of $\mathfrak{A}$ meets $M$.*

*Proof.* According to [24, chapter IV, paragraph 6, Corollary 3], if $M$ does not meet any associated prime ideal of $\mathfrak{A}$ then every element of $M/\mathfrak{A}$ is regular. Theorem 1.1 then follows from Proposition 1.2. □

Recall the definition of the dimension of an ideal.

**Definition 1.5.** The dimension $\dim \mathfrak{p}$ of a prime ideal $\mathfrak{p}$ of a polynomial ring $R$ with coefficients in a field $K$ is the transcendence degree of the fraction field of $R/\mathfrak{p}$ over $K$. The dimension $\dim \mathfrak{B}$ of an ideal $\mathfrak{B}$ of $R$ is the maximum of the dimensions of the associated prime ideals of $\mathfrak{B}$.

The rest of this section is completely dedicated to the proof of the following theorem which admits Theorem 1.1 as a corollary. This reformulation of Theorem 1.1 is often convenient for writing proofs.

**Theorem 1.6.** *The associated prime ideals of $\mathfrak{A}$ have dimension $m$ and do not meet $M$.*

In order to apply Macaulay's unmixedness theorem, one needs to get rid of the saturation by $h$. For this, one may use the Rabinowitsch trick [20, section 16.5]. One introduces some new indeterminate $x_{n+1}$ and a new polynomial $p_{n+1} = h\,x_{n+1} - 1$. One denotes $A'$ the triangular system of $R' = R[x_{n+1}]$ obtained by adjoining $p_{n+1}$ to $A$. One denotes $\mathfrak{A}'$ the ideal $(A')$ of $R'$. Consider the two following canonical ring homomorphisms:

$$R \xrightarrow{\ \phi\ } h^{-1}\,R \simeq R'/(p_{n+1}) \xleftarrow{\ \pi\ } R'.$$

The isomorphism $h^{-1}R \simeq R'/(p_{n+1})$ is classical [7, Exercise 2.2, page 79]: every element of $R$ corresponds to itself, $x_{n+1}$ corresponds to $h^{-1}$. If $\mathfrak{B}$ is an ideal of $R$, one denotes $h^{-1}\mathfrak{B}$ or $(\phi\mathfrak{B})$ the ideal of $h^{-1}R$ generated by $\phi\mathfrak{B}$. If $\mathfrak{B}'$ is an ideal of $R'$ then $\pi\mathfrak{B}'$ is an ideal of $\pi R' = R'/(p_{n+1})$.

**Lemma 1.7.** *The ideal $\mathfrak{A}'$ is proper. If $\mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_r$ is a minimal primary decomposition of $\mathfrak{A}'$ then $\phi^{-1}(\pi\mathfrak{q}'_1) \cap \cdots \cap \phi^{-1}(\pi\mathfrak{q}'_r)$ is a minimal primary decomposition of $\mathfrak{A}$.*

*Proof.* We use the notations of extensions and contractions defined in [24, chapter IV, paragraph 8], w.r.t. the ring homomorphism $\phi$ so that $(\phi\mathfrak{A}) = \mathfrak{A}^e$. The ideal $\pi\mathfrak{A}'$ is equal to the ideal $\mathfrak{A}^e$ since both ideals admit a same generating family: $A$. By [24, chapter IV, Theorem 15 (a)] we have $\mathfrak{A} = \mathfrak{A}^{ec}$ since $\mathfrak{A} = \mathfrak{A} : h^\infty$. Therefore, since $\mathfrak{A}$ is assumed to be proper, so are $\mathfrak{A}^e$ and $\mathfrak{A}'$.

Consider now a minimal primary decomposition $\mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_r$ of $\mathfrak{A}'$. According to [24, chapter IV, paragraph 5, Remark concerning passage to a residue class ring], $\pi\mathfrak{q}'_1 \cap \cdots \cap \pi\mathfrak{q}'_r$ is a minimal primary decomposition of $\pi\mathfrak{A}' = \mathfrak{A}^e$. Since $\mathfrak{A} = \mathfrak{A}^{ec}$, by [24, chapter IV, Theorem 15 (b) and a comment just above this theorem], the associated prime ideals of $\mathfrak{A}$ do not meet $M$. By [24, chapter IV, Theorem 17] the intersection $\phi^{-1}(\pi\mathfrak{q}'_1) \cap \cdots \cap \phi^{-1}(\pi\mathfrak{q}'_r)$ is a minimal primary decomposition of $\mathfrak{A}$. □

**Proposition 1.8.** *To prove Theorem 1.6, it is sufficient to prove that the associated prime ideals of $\mathfrak{A}'$ have dimension $m$ and do not meet $M$.*

*Proof.* Let $\mathfrak{p}'$ be an associated prime ideal of $\mathfrak{A}'$ and $\mathfrak{p} = \phi^{-1}(\pi\mathfrak{p}')$ the corresponding associated prime ideal of $\mathfrak{A}$ according to Lemma 1.7. Let $a$ be an element of the subring $R$ of $R'$. Then $a \in \mathfrak{p}'$ if and only if $a/1 \in \pi\mathfrak{p}'$ and $a/1 \in \pi\mathfrak{p}'$ if and only if $a \in \mathfrak{p}$. Therefore, if $\mathfrak{p}'$ does not meet $M$ then $\mathfrak{p}$ does not either and $\dim \mathfrak{p} \geq m$. If moreover $\dim \mathfrak{p}' = m$ then $x_1, \ldots, x_n$ must depend algebraically on $t_1, \ldots, t_m$ modulo $\mathfrak{p}'$ hence they depend algebraically on $t_1, \ldots, t_m$ modulo $\mathfrak{p}$ and $\dim \mathfrak{p} \leq m$. Combining both inequalities, one concludes that $\dim \mathfrak{p} = m$. □

One distinguishes two sorts of prime ideals associated to an ideal $\mathfrak{A}$: the isolated or minimal ones and the embedded or imbedded ones. An embedded associated prime ideal of $\mathfrak{A}$ is an associated prime of $\mathfrak{A}$ which contains another associated prime ideal of $\mathfrak{A}$. In the context of polynomial rings, its algebraic variety is included (embedded) in that of the associated prime ideal that it contains. One thus sees that, at least in the context of polynomial rings, it is much easier to get informations on the minimal associated prime ideals (they correspond to the irreducible components of the algebraic variety of the ideal [24, chapter VII, paragraph 3, Corollary 3 to Hilbert's Nullstellensatz]) than on the embedded associated prime ideals, which have no such simple geometric meaning (see however [7, section 3.8] for a geometric interpretation of embedded primes). In our case, the problem of the minimal associated prime ideals is easily solved by Lemma 1.10. The problem of the embedded associated prime ideals is solved by a difficult theorem: Macaulay's unmixedness theorem. Recall Krull's principal ideal theorem [24, chapter VII, Theorem 22].

**Theorem 1.9.** *(principal ideal theorem)*

*If a proper ideal $\mathfrak{A}$ of a ring $R = K[x_1, \ldots, x_n]$ admits a generating family formed of $k$ elements ($1 \leq k \leq n$) then $\dim \mathfrak{A} \geq n - k$.*

Let us come back to our study of the ideal $\mathfrak{A}'$ of $R'$.

**Lemma 1.10.** *The dimension of $\mathfrak{A}'$ is $m$. Moreover, none of the $m$–dimensional associated prime ideal of $\mathfrak{A}'$ meets $M$.*

*Proof.* Consider an associated prime ideal $\mathfrak{p}'$ of $\mathfrak{A}'$.

First consider the case of $h$ being the product of the initials of the elements of $A$. Then none of these initials belongs to $\mathfrak{p}'$ (otherwise $\mathfrak{p}'$, which contains $h\,x_{n+1} - 1$ would also contain 1). Thus $x_1, \ldots, x_{n+1}$ are algebraically dependent on $t_1, \ldots, t_m$ over $K$ in $R'/\mathfrak{p}'$ (the polynomials of $A'$ cannot degenerate at all).

Consider now the case of $h$ being the product of the separants of the elements of $A$. Let $p_\ell = a_d\, x_\ell^d + \cdots + a_1\, x_\ell + a_0$ be any element of $A'$. Since its separant $s_\ell = d\, a_d\, x_\ell^{d-1} + \cdots + a_1$ does not belong to $\mathfrak{p}'$, at least one of the coefficients $a_d, \ldots, a_1$ does not belong to it. Thus $x_1, \ldots, x_{n+1}$ are algebraically dependent on $t_1, \ldots, t_m$ over $K$ in $R'/\mathfrak{p}'$ (the polynomials of $A'$ cannot completely degenerate).

In both cases, $x_1, \ldots, x_{n+1}$ are algebraically dependent on $t_1, \ldots, t_m$ over $K$ in $R'/\mathfrak{p}'$. One then concludes, first that $\dim \mathfrak{p}' \leq m$ hence $\dim \mathfrak{A}' \leq m$, second that if $\dim \mathfrak{p}' = m$ then $\mathfrak{p}' \cap M = \emptyset$. The ideal $\mathfrak{A}'$ admits a basis made of $n + 1$ elements in a polynomial ring in $n + m + 1$ indeterminates. According to the principal ideal theorem, $\dim \mathfrak{A}' \geq m$. Combining both inequalities, one concludes that $\dim \mathfrak{A}' = m$. $\square$

Let us recall Macaulay's unmixedness theorem [24, chapter VII, Theorem 26].

**Theorem 1.11.** *(Macaulay's unmixedness theorem)*

*If a proper ideal $\mathfrak{A}$ of a polynomial ring $R = K[x_1, \ldots, x_n]$ admits a basis made of $k$ elements ($1 \leq k \leq n$) and if $\dim \mathfrak{A} = n - k$ then all its associated prime ideals have dimension $n - k$.*

The following proposition, combined to Proposition 1.8, concludes the proof of Theorem 1.6 hence that of Theorem 1.1.

**Proposition 1.12.** *The associated prime ideals of $\mathfrak{A}'$ have dimension $m$ and do not meet $M$.*

*Proof.* The ideal $\mathfrak{A}'$ admits a basis made of $n+1$ elements in a polynomial ring in $n+m+1$ indeterminates. According to Lemma 1.10, its dimension is $m$. According to Macaulay's unmixedness theorem, all its associated prime ideals have dimension $m$. According to Lemma 1.10 again, none of these prime ideals meets $M$. $\square$

Let us state a few easy corollaries to Theorem 1.1.

**Corollary 1.13.** *The minimal primary decomposition of $\mathfrak{A}$ is uniquely defined.*

*Proof.* By Theorem 1.6, the ideal $\mathfrak{A}$ has no embedded associated prime ideal. The corollary then follows [24, chapter IV, paragraph 5, Theorem 8]. $\square$

**Corollary 1.14.** *Theorems 1.1 and 1.6 hold if $\mathfrak{A}$ is replaced by any ideal $(A) : S^\infty$ where $S$ is any subset of $R$ containing $h$, provided that $(A) : S^\infty$ is proper.*

*Proof.* The ideal $(A) : S^\infty$ is the intersection of the primary components of $(A) : h^\infty$ which do not meet the multiplicative family generated by $S$. Since the primary components of $(A) : h^\infty$ do not meet $M$, the primary components of $(A) : S^\infty$ do not meet $M$ either and, Theorem 1.6 holds for this ideal also. Theorem 1.1 follows from Theorem 1.6 and Proposition 1.4. □

**Corollary 1.15.** *Every regular element of $R_0/\mathfrak{A}_0$ is invertible.*

*Proof.* Still a well known theorem. By Theorem 1.6, the ideal $\mathfrak{A}_0$ has dimension zero. By [24, chapter VII, paragraph 7], the associated prime ideals of $\mathfrak{A}_0$ are maximal. The ideal $\mathfrak{A}_0$ is thus contained in finitely many prime ideals. There is a bijection [24, chapter III, Theorem 7] between the ideals of $R_0$ which contain $\mathfrak{A}_0$ and the ideals of $R_0/\mathfrak{A}_0$. This bijection maps prime ideals to prime ideals [24, chapter III, Theorem 11]. The ring $R_0/\mathfrak{A}_0$ thus involves only finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ which are the associated primes of $(0)$. Assume $a \in R_0/\mathfrak{A}_0$ is regular. By [24, chapter IV, paragraph 6, Corollary 3], the element $a$ belongs to none of the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. The ideal generated by $a$ must contain 1 since it would otherwise have associated prime ideals all different from $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and there are no such prime ideals. Thus there exists some $\bar{a} \in R_0/\mathfrak{A}_0$ such that $a\,\bar{a} = 1$ and $a$ is invertible. □

**Corollary 1.16.** *Let $1 \leq i \leq n$ be an index. Denote $A_i = \{p_1, \ldots, p_i\}$. If $h$ is the product of the initials of $A$, denote $h_i$ the product of the initials of the elements of $A_i$ otherwise, denote $h_i$ the product of the separants of the elements of $A_i$. Denote $\mathfrak{A}_i = (A_i) : h_i^\infty$. Let $a \in R$ be any polynomial. If $a$ is regular in $R_i/\mathfrak{A}_i$ then $a$ is regular in $R/\mathfrak{A}$.*

*Proof.* Denote $R_{0,i} = K(t_1, \ldots, t_m)[x_1, \ldots, x_i]$ and $\mathfrak{A}_{0,i} = (A_i) : h_i^\infty$ in $R_{0,i}$. Assume $a$ is regular in $R_i/\mathfrak{A}_i$. Then, by Theorem 1.1 and Corollary 1.15, there exists some $\bar{a} \in R_{0,i}$ such that $a\,\bar{a} - 1 \in \mathfrak{A}_{0,i}$. Since $R_{0,i} \subset R_0$ and $\mathfrak{A}_{0,i} \subset \mathfrak{A}_0$, we have $a\,\bar{a} - 1 \in \mathfrak{A}_0$ and $a$ is invertible in $R_0/\mathfrak{A}_0$. By Theorem 1.1 again, $a$ is regular in $R/\mathfrak{A}$. □

## 2 Lazard's lemma

In this section, we keep the notations of section 1 but we restrict ourselves to the case of $h$ being the product of the separants of the elements of $A$. The ideal $\mathfrak{A} = (A) : h^\infty$ is often denoted $(A) : S_A^\infty$ in the literature. It is assumed to be proper.

**Theorem 2.1.** *(Lazard's lemma)*
*The ideal $\mathfrak{A}$ is radical.*
*The minimal prime ideals of $\mathfrak{A}$ have dimension $m$ and do not meet $M$.*

Before proceeding, let us consider the basic case of a system $A$ made of a single polynomial $p_1 = t_1\,(x_1 - 1)^3\,(x_1 - 2)$. Then the separant $h = t_1\,(x_1 - 1)^2\,(4\,x_1 - 7)$ involves as a factor the polynomial $t_1$ which does not depend on $x_1$ and the multiple factor $(x_1 - 1)$

of $p_1$. The ideal $\mathfrak{A}$ is generated by $(x_1 - 2)$ and satisfies Theorem 2.1. Observe that the theorem would not hold in the case of $h$ being the product of the initials of $A$ only. In that case, the ideal $\mathfrak{A}$, which would be generated by $(x_1 - 1)^3 (x_1 - 2)$ would not be radical.

The second statement of Lazard's lemma follows from Theorem 1.6. One just needs to prove that $\mathfrak{A}$ is radical i.e. that $R/\mathfrak{A}$ does not involve any nilpotent[2] element.

**Proposition 2.2.** *To prove Theorem 2.1, it is sufficient to prove that $\mathfrak{A}_0$ is radical.*

*Proof.* Assume $\mathfrak{A}_0$ is radical. Then $R_0/\mathfrak{A}_0$ does not involve any nilpotent element [24, chapter IV, Theorem 10 and Corollary] hence $R/\mathfrak{A}$ does not either by Theorem 1.1 and $\mathfrak{A}$ is radical. $\square$

In the rest of this section, we prove that $\mathfrak{A}_0$ is radical by proving that $R_0/\mathfrak{A}_0$ is isomorphic to a direct product of fields. Since a direct product of fields does not involve any nilpotent element, the ideal $\mathfrak{A}_0$ is radical and the proof of Lazard's lemma is complete.

Indeed, if $R_1, \ldots, R_k$ are rings then one denotes $S = R_1 \times \cdots \times R_k$ their direct product. Elements of $S$ are tuples with $k$ components. Given any two elements $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ of $S$ one defines $a + b$ as $(a_1 + b_1, \ldots, a_k + b_k)$ and $a\, b$ as $(a_1\, b_1, \ldots, a_k\, b_k)$. In the ring $S$, zero is equal to $(0, \ldots, 0)$ and one is equal to $(1, \ldots, 1)$. If the rings $R_i$ do not involve any nilpotent element then $S$ does not either. This is the case in particular when the rings $R_i$ are fields. See [24, chapter III, paragraph 13] for an equivalent formulation based on direct sums. The following theorem is a generalization of the Chinese Remainder Theorem. See [24, chapter III, paragraph 13, Theorem 32] or [7, Exercise 2.6, page 79].

**Theorem 2.3.** *(Chinese Remainder Theorem)*

*If $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ are ideals of $R$ such that $\mathfrak{A}_i + \mathfrak{A}_j = R$ whenever $i \neq j$ then the ring $R/(\mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_k)$ is isomorphic to the direct product $(R/\mathfrak{A}_1) \times \cdots \times (R/\mathfrak{A}_k)$.*

The proposition below concludes the proof of Theorem 2.1. The scheme of its proof is the original scheme of proof communicated by Daniel Lazard.

**Proposition 2.4.** *The ring $R_0/\mathfrak{A}_0$ is isomorphic to a direct product of fields.*

*Proof.* The ring $R_0/\mathfrak{A}_0$ can be constructed incrementally. It is isomorphic to the ring $S_n$ defined by:

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

The proof is an induction on $n$.

The basis $n = 0$ is trivial.

Assume $S_{n-1}$ is a direct product of fields $K_1 \times \cdots \times K_r$. Then $S_n$ is isomorphic to the direct product of the rings $K_j[x_n]/(p_n) : s_n^\infty$ for all $1 \leq j \leq r$. In the formula above one assimilates the polynomials $p_n$ and $s_n$ with their images by the canonical ring homomorphisms, noticing that the image of the separant of $p_n$ in each $K_j[x_n]$ is the separant of the image of $p_n$ in this ring.

[2] A nilpotent element of a ring $R$ is a nonzero element of $R$ a power of which is zero.

Therefore, in each $K_j[x_n]$, the ideal $(p_n) : s_n^\infty$ is generated by the product of the simple irreducible 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, each $K_j[x_n]/(p_n) : s_n^\infty$ is isomorphic to the direct product of the fields $K_j[x_n]/\mathfrak{m}_\ell$. Since direct products are associative, the ring $S_n$ itself is a direct product of fields. $\square$

**Corollary 2.5.** *Theorem 2.1 holds if $\mathfrak{A}$ is replaced by any ideal $(A) : S^\infty$ where $S$ is any subset of $R$ containing the separants of the elements of $A$, provided that $(A) : S^\infty$ is proper.*

*Proof.* The ideal $(A) : S^\infty$ is the intersection of the primary components of $\mathfrak{A}$ which do not meet the multiplicative family generated by $S$. Since $\mathfrak{A}$ is radical, its primary components are prime ideals [24, chapter IV, Theorem 5]. Thus the primary components of $(A) : S^\infty$ are prime ideals and $(A) : S^\infty$ is radical. The dimension properties shared by all the associated prime ideals of $\mathfrak{A}$ also hold for all the associated prime ideals of $(A) : S^\infty$. $\square$

# 3 Regular chains

We consider the polynomial ring $R = K[x_1, \ldots, x_n, t_1, \ldots, t_m]$. We assume that the $m + n$ indeterminates are ordered according to some total ordering $\mathscr{O}$. Let $p$ be any polynomial of $R \setminus K$. The greatest indeterminate w.r.t. $\mathscr{O}$ among the indeterminates $p$ depends on is called the *main indeterminate* of $p$. We consider a *triangular* system $A = \{p_1, \ldots, p_n\}$ of $R$ i.e. a polynomial system whose elements have distinct main indeterminates. Renaming the indeterminates if necessary, we assume that the main indeterminate of $p_i$ is $x_i$ for each $1 \leq i \leq n$. The multiplicative family $M$, the initials and the separants of the elements of $A$ are then defined as in section 1.

Fix some $1 \leq i \leq n$. Denote $A_i$ the system $\{p_1, \ldots, p_i\}$. Denote $h_i$ the product of the initials of the elements of $A_i$. Denote $R_i$ the ring $K[t_1, \ldots, t_m, x_1, \ldots, x_i]$. Denote $R_{0,i}$ the ring $K(t_1, \ldots, t_m)[x_1, \ldots, x_i]$. Denote $\mathfrak{A}_i$ the ideal $(A_i) : h_i^\infty$ of $R$ and $\mathfrak{A}_{0,i}$ the ideal $(A_i) : h_i^\infty$ of $R_{0,i}$. Denote $R_0 = R_{0,n}$ and $\mathfrak{A} = \mathfrak{A}_n$.

**Definition 3.1.** The system $A$ is a *regular chain* if, for each $2 \leq i \leq n$, the initial of $p_i$ is regular in the ring $R_{i-1}/\mathfrak{A}_{i-1}$. Assume $A$ is a regular chain. Then $A$ is said to be *squarefree* if, for each $1 \leq i \leq n$, the separant of $p_i$ is regular in $R_i/\mathfrak{A}_i$.

The above definition is not exactly the same as that of [2, Definition 4.1] but they are strictly equivalent. The difference is that, in [2], the $t$ indeterminates greater than $x_i$ would have been withdrawn from the rings $R_{i-1}$ and $R_i$. This change is not important for the elements of $A_i$ do not depend on the $t$ indeterminates greater than $x_i$ and, by [24, chapter I, paragraph 16, Theorem 6], if $\bar{R}$ is a ring, $a$ is one of its elements and $x$ is an indeterminate over it then $a$ is zero (respectively regular) if and only if it is zero (respectively regular) in the ring $\bar{R}[x]$. The following results are corollaries to Theorems 1.1 and 2.1.

**Corollary 3.2.** *The system $A$ is a* regular chain *if, for each $2 \leq i \leq n$, the initial of $p_i$ is invertible in the ring $R_{0,i-1}/\mathfrak{A}_{0,i-1}$. Assume $A$ is a regular chain. Then $A$ is squarefree if, for each $1 \leq i \leq n$, the separant of $p_i$ is invertible in $R_{0,i}/\mathfrak{A}_{0,i}$.*

*Proof.* It is an immediate corollary of Theorem 1.1 (enlarging the set of the $t$ indeterminates with the $x$ indeterminates which are not needed). $\square$

**Corollary 3.3.** *Assume $A$ is a squarefree regular chain. Then $\mathfrak{A}$ is radical. Its minimal prime ideals have dimension $m$ and do not meet $M$.*

*Proof.* By Corollary 1.16 and the definition of squarefreeness, the separants of the elements of $A$ are regular in $R/\mathfrak{A}$. The corollary follows from Corollary 2.5. $\square$

## 3.1 Splittings

In this section, we provide two propositions which permit to justify many algorithms carrying out the "$D^5$" principle for triangular systems [6]. We keep the notations of section 3 and we assume that $A$ is a regular chain. Let $1 \le i \le n$ be an index. Assume that there exists a factorization $p_i = b\,c$ in $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$ such that $0 < \deg(b, x_i)$, $\deg(c,\, x_i) < \deg(p_i, x_i)$. For each $1 \le j \le n$, denote $B_j = A_j$ if $j < i$ otherwise denote $B_j = (A_j \setminus \{p_i\}) \cup \{b\}$. Denote $B = B_n$. For each $1 \le j \le n$, denote $h_{b,j}$ the product of the initials of the elements of $B_j$ and $\mathfrak{B}_j$ the ideal $(B_j) : h_{b,j}^{\infty}$ of $R$ and $\mathfrak{B}_{0,j}$ the ideal $(B_j) : h_{b,j}^{\infty}$ of $R_{0,j}$. Replacing $b$ by $c$ in the formulas, define $C$ and for each $1 \le j \le n$, define $C_j$, $h_{c,j}$, $\mathfrak{C}_j$ and $\mathfrak{C}_{0,j}$ Denote $\mathfrak{B}_0 = \mathfrak{B}_{0,n}$ and $\mathfrak{C}_0 = \mathfrak{C}_{0,n}$.

**Proposition 3.4.** *The triangular sets $B$ and $C$ are regular chains. For each $1 \le j \le n$ we have $\mathfrak{A}_j \subset \mathfrak{B}_j$ and $\mathfrak{A}_j \subset \mathfrak{C}_j$.*

*Proof.* We focus on the set $B$. The arguments for $C$ are similar. Since $0 < \deg(b, x_i) < \deg(p_i, x_i)$, the set $B$ is triangular. For each $1 \le j < i$ we have $A_j = B_j$ thus $\mathfrak{A}_j = \mathfrak{B}_j$ and $B$ is a regular chain up to index $i-1$. In the ring $R_{0,i-1}$, the initial of $p_i$ is the product of the initials of $b$ and $c$. Since $A$ is a regular chain, the initial of $p_i$ is invertible in $R_{0,i-1}/\mathfrak{A}_{0,i-1}$. Therefore, the initial of $b$ is invertible in $R_{0,i-1}/\mathfrak{B}_{0,i-1}$. By Corollary 3.2, the set $B$ is a regular chain up to index $i$ and $\mathfrak{A}_i \subset \mathfrak{B}_i$. Let $i < j \le n$ be an index. We have $\mathfrak{A}_j \subset \mathfrak{B}_j$. Thus the initial of $p_j$, which is invertible in $R_{0,j-1}/\mathfrak{A}_{0,j-1}$, is also invertible in $R_{0,j-1}/\mathfrak{B}_{0,j-1}$. By Corollary 3.2, the set $B$ is a regular chain up to any index and $\mathfrak{A}_j \subset \mathfrak{B}_j$. $\square$

We have proved that $\mathfrak{A} \subset \mathfrak{B} \cap \mathfrak{C}$. In general the equality does not hold because of possible common factors of $b$ and $c$. In the particular case of squarefree regular chains, $b$ and $c$ have no common factors and the equality holds, the following proposition shows.

**Proposition 3.5.** *Assume $A$ is squarefree. Then so are $B$, $C$ and we have $\mathfrak{A} = \mathfrak{B} \cap \mathfrak{C}$. Moreover, the sets of the minimal prime ideals of $\mathfrak{B}$ and $\mathfrak{C}$ form a partition of the set of the minimal prime ideals of $\mathfrak{A}$.*

*Proof.* First we prove that $B$ and $C$ are squarefree regular chains. As in the above proof, we focus on $B$. By Proposition 3.4, the set $B$ is a regular chain. Assume $A$ is squarefree. Let $1 \le j < i$ be an index. Since $A_j = B_j$, the separant of $p_j$ is regular in $R_j/\mathfrak{B}_j$ and $B$ is a squarefree regular chain up to index $i-1$. Denote $s_i$, $s_b$ and $s_c$ the separants of $p_i$, $b$ and $c$. We have $s_i = s_b\,c + s_c\,b$. Let us prove that $s_b$ is regular in $R_i/\mathfrak{B}_i$. Since $A$ is squarefree, $s_i$

is invertible in $R_{0,i}/\mathfrak{A}_{0,i}$. By Proposition 3.4, for each $1 \leq j \leq n$ we have $\mathfrak{A}_j \subset \mathfrak{B}_j$ thus $s_i$ is also invertible in $R_{0,i}/\mathfrak{B}_{0,i}$. Then, using the fact that $b \in B_i$ we see that $s_b\, c$, hence $s_b$, is invertible in $R_{0,i}/\mathfrak{B}_{0,i}$. By Corollary 3.2, the set $B$ is a squarefree regular chain up to index $i$. Let $i < j \leq n$ be an index. Using again the fact that $\mathfrak{A}_j \subset \mathfrak{B}_j$, we see that the separant of $p_j$ is regular in $R_j/\mathfrak{B}_j$. Thus $B$ is a squarefree regular chain up to any index.

Similar statements prove that $C$ is a squarefree regular chain.

By Corollary 3.3, the ideals $\mathfrak{B}$ and $\mathfrak{C}$ are radical. They are equal to the intersections of their minimal prime ideals by [24, chapter IV, Theorem 5]. To conclude the proof of the proposition, it is thus sufficient to prove that the sets of the minimal prime ideals of $\mathfrak{B}$ and $\mathfrak{C}$ form a partition of the set of the minimal prime ideals of $\mathfrak{A}$. Denote $V$, $V_b$ and $V_c$ the sets of zeros of $\mathfrak{A}_0$, $\mathfrak{B}_0$ and $\mathfrak{C}_0$ in the algebraic closure of $K(t_1, \ldots, t_m)$. Since these ideals have dimension zero, these sets are finite. The minimal prime ideals of $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ have dimension $m$ and do not meet $M$. Therefore, by [24, chapter IV, Theorem 15(d)], the ring homomorphism $R \to R_0$ provides a bijection between the minimal prime ideals of $\mathfrak{A}$ (respectively $\mathfrak{B}$, $\mathfrak{C}$) and those of $\mathfrak{A}_0$ (respectively $\mathfrak{B}_0$, $\mathfrak{C}_0$) hence, using [24, chapter VII, paragraph 3, Corollary 2], a bijection between the minimal prime ideals of $\mathfrak{A}$ (respectively $\mathfrak{B}$, $\mathfrak{C}$) and the elements of $V$ (respectively $V_b$, $V_c$). It is thus sufficient to prove that $V_b$ and $V_c$ form a partition of $V$. The cardinal $|V|$ of $V$ is the product $\prod_{j=1}^{n} \deg(p_j,\, x_j)$. Similar statements hold for $V_b$ and $V_c$. Since $\deg(p_i,\, x_i) = \deg(b,\, x_i) + \deg(c,\, x_i)$ we see first that $|V| = |V_b| + |V_c|$. Second, we have $V_b \subset V$ and $V_c \subset V$. Third, $V_b \cap V_c$ is empty for a common zero of $\mathfrak{B}$ and $\mathfrak{C}$ would annihilate $s_i = s_b\, c + s_c\, b$ which is invertible. Therefore $V = V_b \cup V_c$, the sets $V_b$ and $V_c$ form a partition of $V$ and the proposition is proved. □

### 3.2 The $D^5$ principle for triangular systems

In this section, we provide the scheme of many algorithms carrying out the "$D^5$" principle for triangular systems. More efficient algorithms can be found in [13, 12]. See also [22, 21, 5]. The triangular set $A$ is assumed to be a regular chain.

**Definition 3.6.** For every $a \in R$ we define the pseudoremainder of $a$ by $A$ as

$$\mathrm{prem}(a,\, A) \underset{\mathrm{def}}{=} \mathrm{prem}(\ldots \mathrm{prem}(\mathrm{prem}(a,\, p_n,\, x_n),\, p_{n-1},\, x_{n-1}) \ldots,\, p_1,\, x_1).$$

The pseudoremainder algorithm is based on [24, chapter I, paragraph 16, Theorem 9]. It is defined in [10, volume 2, page 407]. The next proposition is proved in [2, Theorem 6.1].

**Proposition 3.7.** *For every $a \in R$ we have $a \in \mathfrak{A}$ if and only if* $\mathrm{prem}(a,\, A) = 0$.

The parameter $a$ of *algebraic_inverse* denotes an element of $R$. The function returns an inverse of $a$ in $R_0/\mathfrak{A}_0$ or fails. If it succeeds then $a$ is proved invertible in $R_0/\mathfrak{A}_0$ hence regular in $R/\mathfrak{A}$ by Theorem 1.1. The function thus implicitly relies on the equidimensionnality theorem. If it fails by encountering a zero divisor, it exhibits a nontrivial factorization of some element $p_i$ of $A$. The exhibited factorization might allow some calling function to split $A$ as two regular chains by using Proposition 3.4. Observe that the function may fail even if $a$ is regular in $R/\mathfrak{A}$ for it checks the regularity of many different elements of $R/\mathfrak{A}$.

```
function algebraic_inverse (a, A)
begin
  if a ∈ K(t_1, ... , t_m) then
    if a ≠ 0 then
      1/a
    else
      the inverse computation fails (inversion of zero)
    endif
  else
    let x_i be the main indeterminate of a
    (u_1, u_2, u_3) := extended_Euclid (a, p_i, x_i, A)
    if u_3 ≠ 1 then
      the inverse computation fails (inversion of a zero divisor): u_3 is a factor of p_i
    else
      u_1
    endif
  endif
end
```

Here is the generalization of the extended Euclidean algorithm called by *algebraic_inverse*. The main indeterminate of the two polynomials $a$ and $b$ is $x_i$. The polynomials $a$ and $b$ are viewed as polynomials in $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$. The function fails or returns a triple $U = (u_1,\, u_2,\, u_3)$ of elements of $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$ satisfying a Bézout identity in the ring $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$ i.e. a relation $u_1\, a + u_2\, b = u_3$. A proof that $U$ satisfies a Bézout identity can be designed by using the two following loop invariants (i.e. properties which hold each time the loop condition is evaluated). These loop invariants are natural generalizations of the very classical loop invariants of the basic extended Euclidean algorithm:

- $u_1\, a + u_2\, b = u_3$ and $v_1\, a + v_2\, b = v_3$ in $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$ ;
- the set of the common divisors of $u_3$ and $v_3$ is equal to the set of the common divisors of $a$ and $b$.

Observe that the second invariant is stated without using the word "gcd" which would be controversial in this context for the ring $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$ is not a UFD. A definition of the gcd in this context is however provided in [13]. Observe that the function needs to recognize zero in $R_{0,i-1}/\mathfrak{A}_{0,i-1}$ in order to evaluate the loop condition and to determine the degree of $u_3$ after the loop execution. This is achieved by Proposition 3.7. The function also needs to check the regularity of the leading coefficient of $v_3$ before performing the Euclidean division. This can be achieved using *algebraic_inverse*.

```
function extended_Euclid (a, b, x_i, A)
begin
  U := (1, 0, a)
```

$V := (0,\, 1,\, b)$
while $v_3 \neq 0$ do
  $q :=$ the quotient of the Euclidean division of $u_3$ by $v_3$ in $(R_{0,i-1}/\mathfrak{A}_{0,i-1})[x_i]$
  $T := V$
  $V := U - q\,V$
  $U := T$
done
$c :=$ the coefficient of $x_i^{\deg(u_3,\, x_i)}$ in $u_3$
return *algebraic_inverse* $(c, A)\, U$
end

## References


[1] Philippe Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Univ. Paris VI, 1999.

[2] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[3] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *proceedings of ISSAC'95*, pages 158–166, Montréal, Canada, 1995.

[4] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. Technical report, Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, 1997. (ref. IT306, december 1998 version published in the habilitation thesis of Michel Petitot).

[5] Driss Bouziane, Abdelillah Kandri Rody, and Hamid Maârouf. Unmixed–Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *Journal of Symbolic Computation*, 31:631–649, 2001.

[6] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In *Proceedings of EUROCAL85, vol. 2*, volume 204 of *Lecture Notes in Computer Science*, pages 289–290. Springer Verlag, 1985.

[7] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer Verlag, 1995.

[8] Évelyne Hubert. Factorization free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4,5):641–662, 2000.

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

[10] Donald Erwin Knuth. *The art of computer programming.* Addison–Wesley, 1966. Second edition.

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

[12] Marc Moreno Maza. On Triangular Decompositions of Algebraic Varieties. Technical report, NAG, 2000. (presented at the MEGA2000 conference, submitted to the JSC).

[13] Marc Moreno Maza and Renaud Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Proceedings of AAECC11*, pages 365–382. Springer Verlag, 1995.

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

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

[16] François Ollivier. A proof of Lazard's lemma. private communication, october 1998.

[17] Brahim Sadik. Une note sur les algorithmes de décomposition en algèbre différentielle. *Comptes Rendus de l'Académie des Sciences*, 330:641–646, 2000.

[18] Josef Schicho and Ziming Li. A construction of radical ideals in polynomial algebra. Technical report, RISC, Johannes Kepler University, Linz, Austria, august 1995.

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

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

[21] Dongming Wang. Decomposing polynomial systems into simple systems. *Journal of Symbolic Computation*, 25:295–314, 1998.

[22] Wu Wen Tsün. On the foundation of algebraic differential geometry. *Mechanization of Mathematics, research preprints*, 3, 1987.

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

[24] Oscar Zariski and Pierre Samuel. *Commutative Algebra*. Van Nostrand, New York, 1958.

François Boulier
LIFL, Université Lille I, 59655 Villeneuve d'Ascq, France
boulier@lifl.fr, http://www.lifl.fr/~boulier

François Lemaire
LIFL, Université Lille I, 59655 Villeneuve d'Ascq, France
lemaire@lifl.fr, http://www.lifl.fr/~lemaire

Marc Moreno Maza
ORCCA, University of Western Ontario, London, N6A 5B7 Canada
moreno@orcca.on.ca, http://www.csd.uwo.ca/~moreno