A Short Contribution to the Theory of Regular Chains

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

A Short Contribution to the Theory of Regular Chains

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

Abstract. This paper contains short contributions to the theory of regular chains which follow a recent JSC paper by the same authors. These contributions apply to both the nondifferential and the differential context. They deal with the computation of normal forms and with the membership problem to ideals defined by regular chains.

1. Introduction

This paper investigates consequences of the recent [5] which contains important characterizations of regular chains in the nondifferential case [5, Theorem 21] and in the differential one [5, Theorem 37]. This paper: 1) improves an algorithm for computing the normal form of a differential fraction f/g (f and g being two differential polynomials) modulo a regular differential chain A, which was presented in [4, Figure 2]; 2) provides a new proof of the well-known fact that regular chains decide membership to the ideals that they define, which highlights the main theoretical argument underlying this result; 3) extends some results of [5].

Our new normal form algorithms are better than the former versions for two reasons: 1) they succeed in computing normal forms whenever these ones exist (see Section 2.2.1 for examples); and 2) they are conceptually simpler, though their simplicities hide subtleties (see Section 2.2.2).

The main computational tool involved in this paper is the resultant of a polynomial w.r.t. a regular chain (which is a triangular set of polynomials with good properties). The main recent theoretical argument involved in our proofs is the implication $1 \Rightarrow 4$ of [5, Theorem 21] (recalled as Theorem 1 in this paper):

> *Let A be a regular chain, $\mathfrak{a}$ the ideal that it defines and f be a polynomial of some polynomial ring R. Then, f is regular in $R/\mathfrak{a}$ if and only if the resultant of f w.r.t. A is not zero.*

Non expert readers may wonder about the novelty of the above quotation since seemingly similar statements can be found in earlier papers. Indeed, the above statement already appears in [6, Theorem 1]. It was formerly proved, in the zerodimensional case, in [7, Lemma 4]. As far as we know, the first occurrence of a similar statement is [16, Corollary 4, page 150] but its exact relationship with more recent works is difficult to clarify since it is formulated in terms of *proper ascending chains*. A formulation in terms of *regular zeros* occurs in [15, Proposition 5.1.5]. Deciding the regularity of a polynomial w.r.t. a regular chain is also a much studied problem. A careful survey on this question can be found in [5, Section 8].

Non expert readers may also wonder about the relevance of the above quotation. Indeed, the membership test to the ideal $\mathfrak{a}$ defined by a triangular set A, by means of the pseudoremainder algorithm, seems much more important. Actually, this membership test was established by Ritt in [13], in the easy case of a *prime* ideal $\mathfrak{a}$. In the case of an ideal $\mathfrak{a}$ which is not prime, this membership test only holds for regular chains — not for general triangular sets (Proposition 11). We believe

This work has been supported by the bilateral project ANR-17-CE40-0036 and DFG-391322026 SYMBIONT..

that any proof for this membership test to $\mathfrak{a}$ first requires to secure a nontrivial regularity property equivalent to the above quotation. In particular, we believe that many formerly published proofs are — if not flawed — at least implicitly using a nontrivial argument. For more details on this point, we refer to [5, Section 8]. Our new proof of Proposition 9 aims at highlighting the key role of the above quotation.

The paper is organized as follows. The nondifferential case is addressed in Section 2. Classical results are recalled in Section 2.1. Then the new normal form algorithms are presented in Section 2.2. In particular, Algorithms 1 and 2 as well as Propositions 4 and 7 are new results. The new proof of the membership test is given in Section 2.3. The differential case is addressed in Section 3. Classical results are recalled in Section 3.1. Then the new normal form algorithms are presented in Section 3.2. In particular, Algorithms 3, 4 and 5 as well as Propositions 16 and 18 are new results. Proposition 16 is notably important since it completes [5, Theorem 37].

2. The Nondifferential Case

2.1. Classical Results

In this section, $A = \{p_1, \ldots, p_n\}$ denotes a subset of the polynomial ring $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ which is triangular in the sense that $\deg(p_k, x_k) > 0$ and $\deg(p_k, x_\ell) = 0$ for all indices $1 \leq k \leq n$ and $k < \ell \leq n$. Denote i_k the initial of p_k i.e. the leading coefficient of p_k w.r.t. x_k, for $1 \leq k \leq n$. Let f and g be two polynomials of $S[x]$, where S is a unitary ring of characteristic zero:

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

If f or g is zero, then the resultant of f and g is taken to be zero. Assume that f and g are nonzero and that at least one of them has positive degree. Then, the resultant of f and g, denoted $\mathrm{res}(f, g, x)$, 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 [2, 4.2, page 105].

Definition 1. *Let A be a possibly empty triangular set and $f \in R$. The* resultant of f by A, *denoted* $\mathrm{res}(f, A)$, *is defined as follows:*

1. *if $A = \varnothing$ then $\mathrm{res}(f, A) = f$;*
2. *if $A = \{p_1, \ldots, p_n\}$ then $\mathrm{res}(f, A) = \mathrm{res}(\mathrm{res}(f, p_n, x_n), \{p_1, \ldots, p_{n-1}\})$.*

The following Proposition is an easy consequence of basic properties of resultants. See [15, Lemma 4.3.2]. Observe it is algorithmic, thanks to extended versions of algorithms for computing pseudo-remainder subresultant sequences. See [8].

Proposition 1. *Let f be a polynomial and A be a triangular set of R. Then there exist polynomials $u, v_1, v_2, \ldots, v_n$ of R such that*

$$u\, f \quad = \quad \mathrm{res}(f, A) + v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n\,. \tag{1}$$

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

Notation. To each (non necessarily triangular) set A of polynomials of $R \setminus K$, one associates the ideal $\mathrm{sat}\,(A) = (A) : (i_1 \cdots i_n)^\infty$ which will often be denoted $\mathfrak{a}$. Similarly, if A', A_k, $\bar{A}$ are subsets of $R \setminus K$, the ideals $\mathrm{sat}\,(A')$, $\mathrm{sat}\,(A_k)$, $\mathrm{sat}\,(\bar{A})$ will be denoted $\mathfrak{a}'$, $\mathfrak{a}_k$, $\bar{\mathfrak{a}}$.

Definition 2. *A triangular set is said to be a* regular chain *if the initial i_k of p_k is regular (i.e. a non zerodivisor) in $R/\mathrm{sat}\,(p_1, \ldots, p_{k-1})$ for $2 \leq k \leq n$.*

The following characterization is [5, Theorem 21].

Theorem 1. *Let A be a triangular set. The following conditions are equivalent:*

1. *A is a regular chain;*
2. *for each $2 \leq \ell \leq n$ and each $1 \leq k \leq n$ we have $\mathrm{res}(i_\ell, \{p_k, \ldots, p_n\})$ regular in $R/\mathfrak{a}$;*

3. *for each* $2 \leq \ell \leq n$ *we have* $\mathrm{res}(i_\ell, A) \neq 0$*;*
4. *for each* $f \in R$*,* f *is regular in* $R/\mathfrak{a}$ *if and only if* $\mathrm{res}(f, A) \neq 0$*;*
5. *for each* $f \in R$*,*

$$f \text{ is regular in } R/\mathfrak{a}$$
$$\Updownarrow$$
$$\text{for each } 1 \leq k \leq n,\ \mathrm{res}(f, \{p_k, \ldots, p_n\}) \text{ is regular in } R/\mathfrak{a}.$$

Normal forms of rational fractions modulo regular chains are defined and studied in [4, Definition 5.1, Proposition 5.2], in the framework of differential algebra. In the nondifferential context, these results can be restated by the following definition and proposition.

Definition 3. *Let* A *be a regular chain and* f/g *be a rational fraction with* g *regular in* $R/\mathfrak{a}$*. A rational fraction* p/q *is said to be a* normal form of f/g modulo A *if it satisfies:*

1. $\deg(p, x_k) < \deg(p_k, x_k)$ *for* $1 \leq k \leq n$*;*
2. $q \in K[t_1, \ldots, t_m]$*;*
3. f/g *and* p/q *are equal in the total ring of fractions of* $R/\mathfrak{a}$*.*

Proposition 2. *Let* A *be a regular chain and* f/g *be a rational fraction with* g *regular in* $R/\mathfrak{a}$*. The normal form of* f/g *modulo* A *exists and is unique.*

An algorithm for computing the normal form of a rational fraction is given in [4, Figure 2]. This algorithm relies on the computation of the inverse of a polynomial modulo a regular chain. The following definition and proposition restate [4, Definition 4.1 and Proposition 4.3].

Definition 4. *Let* A *be a regular chain and* g *be a nonzero polynomial of* R*. An* inverse of g modulo A *is any rational fraction* p/q *such that* $q \neq 0$*,* $q \in K[t_1, \ldots, t_m]$ *and* $g\,p = q$ *in* $R/\mathfrak{a}$*.*

Proposition 3. *Let* A *be a regular chain and* g *be a nonzero polynomial of* R*. The polynomial* g *is regular in* $R/\mathfrak{a}$ *if and only if it admits an inverse modulo* A*.*

2.2. A New Normal Form Algorithm

Algorithm 1, respectively 2, computes the normal form of a polynomial, respectively a rational fraction, modulo a regular chain A. These algorithms are new. Their proofs essentially rely on the following Proposition, which actually provides an algorithm for computing inverses, since it relies on Proposition 1, which is itself of algorithmic nature.

Proposition 4. *Let* A *be a regular chain and* g *be a regular element of* $R/\mathfrak{a}$*. Let* u *be a polynomial such that* $u\,g = \mathrm{res}(g, A)$ *in* $R/\mathfrak{a}$*. Then* $u/\mathrm{res}(g, A)$ *is an inverse of* g *modulo* A*.*

Proof. The existence of u is guaranteed by Proposition 1. The fact that $\mathrm{res}(g, A) \in K[t_1, \ldots, t_m]$ is an easy property of the iterated resultant. The fact that $\mathrm{res}(g, A) \neq 0$ follows from the regularity of g and the implication $1 \Rightarrow 4$ of Theorem 1. □

Algorithm 1: `NFpoly`(f, A)

input : a polynomial f, and $A = \{p_1, \ldots, p_n\}$ a regular chain
output: the normal form of f modulo A

if *A is empty* **then**
  return f
else
  compute $i_n^\alpha\, f = \bar{f} + v_n\, p_n$; `/* by computing` $\bar{f} = \mathrm{prem}(f, p_n, x_n)$ `*/`
  compute u/r an inverse of i_n modulo A ; `/* Proposition 4 */`
  return $(1/r^\alpha) \times$ `NFpoly`$(u^\alpha \bar{f}, \{p_1, \ldots, p_{n-1}\})$;
end

Algorithm 2: $\mathtt{NF}(f/g, A)$

input : a fraction f/g, and a regular chain $A = \{p_1, \ldots, p_n\}$ with g regular in $R/\mathfrak{a}$
output: the normal form of f/g modulo A
1 compute u/r an inverse of g modulo A ; /* Proposition 4 */
2 **return** $(1/r) \times \mathtt{NFpoly}(uf, A)$

2.2.1. Improvement Compared to the Former Version. As pointed out in [4, Appendix A], the normal form algorithm of [4] may fail to compute a normal form (in some cases where it exists), because of the failure of the function used for computing inverses modulo regular chains. Consider the regular chain

$$A = \{p_3 := x_3 - x_2 - x_1\,,\ p_2 := x_2^2 - x_1^3\,,\ p_1 := (x_1 - 1)\,(x_1 + 1)\,(x_1^2 - 2)\}$$

from [4, Appendix A, Example 4] and consider the polynomial $g = (x_1 - 1)\,x_2 + 1$. The polynomial g is invertible in $R/\mathfrak{a}$ since $\mathrm{res}(g, \{p_2, p_1\}) = 45$. Moreover, the inverse of g in $R/\mathfrak{a}$ is easily deduced from the following formula:

$$\begin{aligned} -3\,(2\,x_1 + 3)\,(2\,x_1^2 + 1)\,(x_1\,x_2 - x_2 - 1)\,g = 45 - (12\,x_1^3 + 18\,x_1^2 + 6\,x_1 + 9)\,(x_1 - 1)^2\,p_2 \\ - (12\,x_1^4 - 6\,x_1^3 + 18\,x_1^2 - 3\,x_1 + 18)\,p_1. \end{aligned}$$

Thus, using our new algorithm, we have

$$\mathrm{NF}(1/g, A) = -\frac{(2\,x_1 + 3)\,(2x_1^2 + 1)\,(x_1\,x_2 - x_2 - 1)}{15}.$$

However, calling [4, NF]$(1/g, A)$ yields an error for the following reason: a call to Algorithm [4, Inverse](g, A) triggers a call to Algorithm [4, AlgebraicInverseNonZero](g, A), which itself triggers a call to Algorithm [4, ExtendedEuclideanAlgorithm](g, p_2, x_2, A) which fails since the initial of g (which is $x_1 - 1$) is not invertible in $R/\mathfrak{a}$.

2.2.2. Caveats. The simplicity of the new algorithms hide subtleties, detailed below. The following proposition is [5, Proposition 23].

Proposition 5. *Let A be a regular chain of R and A' be a nonempty subset of A. Then A' is a regular chain. Moreover, every $f \in R$ which is regular in $R/\mathfrak{a}$ is regular in $R/\mathfrak{a}'$.*

It is tempting to try to generalize this proposition as follows: "*Let f/g be a fraction with g regular in $R/\mathfrak{a}$. Then* $\mathrm{NF}(f/g, A) = \mathrm{NF}(\mathrm{NF}(f/g, A'), A)$". Unfortunately, this generalization is false. A counterexample is suggested by the Remark following [5, Proposition 17]. Take

$$p_1 = (x_1 - 1)(x_1 - 3)\,, \quad p_2 = x_2 - 10\,x_1\,, \quad p = x_1 + x_2 - 31\,.$$

Take $A = \{p_1, p_2\}$, $A' = \{p_1\}$ and $f/g = 1/p$. Both A and A' are regular chains. We have

$$\mathrm{NF}\left(\frac{f}{g}, A\right) = \frac{11\,x_1 - 13}{40} \quad \text{and} \quad \mathrm{NF}\left(\frac{f}{g}, A'\right) = \frac{x_2 - x_1 - 27}{(x_2 - 28)\,(x_2 - 30)}.$$

However, $\mathrm{res}((x_2 - 28)\,(x_2 - 30), A) = 0$, proving that this polynomial is a zerodivisor in $R/\mathfrak{a}$ by the implication $1 \Rightarrow 4$ of Theorem 1. Thus $\mathrm{NF}(\mathrm{NF}(f/g, A'), A)$ is not defined. In this example, the fact that $\deg(p_1, x_1) > 1$ is important, the next propositions (the second one is new) show.

Proposition 6. *Let g be a polynomial and f be a polynomial such that* $\deg(f, x) = 1$. *Denote* $n = \deg(g, x)$ *and* $r = \mathrm{prem}(g, f, x)$. *Then* $\mathrm{res}(g, f, x) = (-1)^n\,r$.

Proof. By [2, Lemma 4.17, page 107] we have $\mathrm{res}(g, f, x) = (-1)^n\,\mathrm{res}(f, r, x)$. Since $\deg(f, x) = 1$ we have $\deg(r, x) = 0$. Thus the Sylvester matrix defined by f and r has dimension 1×1 and involves r as single element. Thus $\mathrm{res}(f, r, x) = r$ and the Proposition is proved. □

Proposition 7. *Let A be a regular chain, $p_k \in A$ be such that* $\deg(p_k, x_k) = 1$ *and g be a polynomial of R. Then g is regular in $R/\mathfrak{a}$ if and only if* $\mathrm{res}(g, p_k, x_k)$ *is regular in $R/\mathfrak{a}$.*

Proof. Let $r = \mathrm{prem}(g, p_k, x_k)$ denote the pseudoremainder of g by p_k and $n = \deg(g, x_k)$. By Proposition 6, we have $\mathrm{res}(g, p_k, x_k) = (-1)^n\, r$.

We claim that g is regular in $R/\mathfrak{a}$ if and only if r is so. Let $\mathfrak{p}$ be any associated prime ideal of $\mathfrak{a}$. There exists a power h of the initial of p_k such that $h\, g = r \pmod{\mathfrak{p}}$. Since $\mathfrak{a}$ is saturated by the initials of A, we have $h \notin \mathfrak{p}$ hence $g \in \mathfrak{p}$ if and only if $r \in \mathfrak{p}$. By [17, IV, 7, Corollary 3 to Theorem 10], the claim and the proposition are proved. □

2.3. The Membership Problem

All propositions stated in this section are well-known: the only difficult one is Proposition 9, which already appears in [1, $(i) \Rightarrow (iii)$]. Another proof is given in [9, Theorem 5.13]. The originality of this section is the proof of that Proposition which involves a single nontrivial argument: the implication $1 \Rightarrow 4$ of Theorem 1.

Proposition 8. *Let A be a triangular set and f be any polynomial of R. Denote $g = \mathrm{prem}(f, A)$. Then*

$$\deg(g, x_k) \quad < \quad \deg(p_k, x_k) \quad (1 \leq k \leq n)\,. \tag{2}$$

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

$$h\, f \quad = \quad g + v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n\,. \tag{3}$$

Proposition 9. *Assume A is a regular chain and f is any polynomial of R. If $f \in \mathfrak{a}$ then* $\mathrm{prem}(f, A) = 0$.

Proof. Observe that if $\mathfrak{a} = (0)$ then the proposition holds so that we only need to consider the case $\mathfrak{a} \neq (0)$. Observe also that, if $f \in \mathfrak{a}$ then $\mathrm{prem}(f, A) \in \mathfrak{a}$. Thus, if $f \in \mathfrak{a}$ is such that $\mathrm{prem}(f, A) \neq 0$ then there exists such a polynomial f reduced w.r.t. A i.e. such that $\deg(f, x_k) < \deg(p_k, x_k)$ for all $1 \leq k \leq n$. We thus assume that there exists a nonzero polynomial $f \in \mathfrak{a}$ which is reduced w.r.t. A and seek a contradiction.

Since $f \in \mathfrak{a}$, there exist nonnegative integers $\alpha_1, \ldots, \alpha_n$ and polynomials $v_1, \ldots, v_n$ such that

$$i_1^{\alpha_1} \cdots i_n^{\alpha_n}\, f \quad = \quad v_1\, p_1 + v_2\, p_2 + \cdots + v_n\, p_n\,. \tag{4}$$

For $1 \leq k \leq n$, denote $r_k = \mathrm{res}(i_k, A)$ and u_k a polynomial such that $u_k\, i_k = r_k \pmod{\mathfrak{a}}$, according to Proposition 1. Multiply both sides of (4) by $u_1^{\alpha_1}\, u_2^{\alpha_2} \cdots u_n^{\alpha_n}$ and denote $h_f = r_1^{\alpha_1} \cdots r_n^{\alpha_n}$. Since the initials i_k are regular in $R/\mathfrak{a}$, their resultants r_k are different from zero by the implication $1 \Rightarrow 4$ of Theorem 1. Thus there exists a nonzero element $h \in K[t_1, \ldots, t_m]$ (one may take $h = h_f$) and polynomials $w_1, \ldots, w_n$ not all zero, such that

$$h\, f \quad = \quad \underbrace{w_1\, p_1 + w_2\, p_2 + \cdots + w_n\, p_n}_{\mathscr{F}}\,. \tag{5}$$

To any such formula $\mathscr{F}$, one associates the index $j(\mathscr{F})$ defined as

$$j(\mathscr{F}) \quad = \quad \max\{\ell \in \mathbb{N} \mid \exists\, k \in [1, n]\,,\ \deg(w_k\, p_k, x_\ell) > 0\}\,. \tag{6}$$

The index j is well defined since the polynomials w_k are not all zero. The definition of j implies that $w_{j+1} = \cdots = w_n = 0$. Moreover, since $x_{j+1}, \ldots, x_n$ appear nowhere in the right hand side of (5), they cannot appear either in the left hand side so that f is free of $x_{j+1}, \ldots, x_n$. Last observe that $j > 1$ since, otherwise, $\deg(f, x_1)$ would be greater than or equal to $\deg(p_1, x_1)$, which would contradict the assumption that f is reduced w.r.t. A.

Denote $\mathscr{E}$ the set of all possible pairs $(f, \mathscr{F})$, where $f \in \mathfrak{a}$ is a nonzero polynomial reduced w.r.t. A and there exists some nonzero $h \in K[t_1, \ldots, t_m]$ such that (5) holds. Our assumptions imply that $\mathscr{E}$ is not empty. Among all possible pairs $(f, \mathscr{F}) \in \mathscr{E}$, fix one such that $j = j(\mathscr{F})$ is minimal and denote $d = \deg(p_j, x_j)$.

Denote $w'_k = \mathrm{prem}(w_k, p_j, x_j)$ for $1 \leq k < j$. There exist nonnegative integers β_k and polynomials q_k such that

$$i_j^{\beta_k}\, w_k \quad = \quad w'_k + q_k\, p_j\,, \quad (1 \leq k < j)\,. \tag{7}$$

Denote $\varrho = \max(\beta_1, \ldots, \beta_{j-1})$. Multiply both sides of (5) by i_j^ϱ and recall that $w_{j+1} = \cdots = w_n = 0$. One gets a formula:

$$i_j^\varrho \, h \, f \quad = \quad i_j^\varrho \, w_1 \, p_1 + \cdots + i_j^\varrho \, w_{j-1} \, p_{j-1} + i_j^\varrho \, w_j \, p_j \, . \tag{8}$$

Denote $\varrho_k = \varrho - \beta_k$ for $1 \leq k < j$. From (7) and (8) one gets:

$$\begin{aligned} i_j^\varrho \, h \, f &= i_j^{\varrho_1} \, (i_j^{\beta_1} \, w_1) \, p_1 + \cdots + i_j^{\varrho_{j-1}} \, (i_j^{\beta_{j-1}} \, w_{j-1}) \, p_{j-1} + i_j^\varrho \, w_j \, p_j \, , & (9) \\ &= i_j^{\varrho_1} \, (w_1' + q_1 \, p_j) \, p_1 + \cdots + i_j^{\varrho_{j-1}} \, (w_{j-1}' + q_{j-1} \, p_j) \, p_{j-1} + i_j^\varrho \, w_j \, p_j \, , & (10) \\ &= \underbrace{i_j^{\varrho_1} \, w_1'}_{w_1''} \, p_1 + \cdots + \underbrace{i_j^{\varrho_{j-1}} \, w_{j-1}'}_{w_{j-1}''} \, p_{j-1} + \underbrace{(i_j^\varrho \, w_j + i_j^{\varrho_1} \, q_1 \, p_1 + \cdots + i_j^{\varrho_{j-1}} \, q_{j-1} \, p_{j-1})}_{w_j''} \, p_j \, . & (11) \end{aligned}$$

We have $\deg(w_k'', x_j) < d$ for $1 \leq k < j$ and $\deg(i_j^\varrho \, h \, f) < d$. Thus $w_j'' = 0$.

The initial i_j does not depend on $x_j, \ldots, x_n$. Thus Proposition 1 permits us to express the resultant r_j as

$$u_j \, i_j \quad = \quad r_j + z_1 \, p_1 + \cdots + z_{j-1} \, p_{j-1} \, , \tag{12}$$

where $u_j, z_1, \ldots, z_{j-1}$ are polynomials which do not depend on $x_j, \ldots, x_n$. Multiplying both sides of (11) by u_j^ϱ, one gets

$$(u_j \, i_j)^\varrho \, h \, f \quad = \quad u_j^\varrho \, w_1'' \, p_1 + \cdots + u_j^\varrho \, w_{j-1}'' \, p_{j-1} \, . \tag{13}$$

Plugging (12), one gets

$$(r_j + z_1 \, p_1 + \cdots + z_{j-1} \, p_{j-1})^\varrho \, h \, f \quad = \quad u_j^\varrho \, w_1'' \, p_1 + \cdots + u_j^\varrho \, w_{j-1}'' \, p_{j-1} \, . \tag{14}$$

The polynomials $u_j, z_1, \ldots, z_{j-1}$ are free of x_j. The polynomials $f, w_1'', \ldots, w_{j-1}''$ have degree in x_j less than d. The polynomials r_j, h are nonzero elements of $K[t_1, \ldots, t_m]$. Denote $h' = r_j^\varrho \, h$. Expanding the left hand side of (14) and distributing over the right hand side (there may be many different ways to perform this operation), one eventually gets a formula

$$h' \, f \quad = \quad w_1''' \, p_1 + \cdots + w_{j-1}''' \, p_{j-1} \tag{15}$$

where h' is a nonzero element of $K[t_1, \ldots, t_m]$ and the w_k''' are polynomials such that $\deg(w_k''', x_j) < d$ for $1 \leq k < j$. All polynomials occurring in (15) are free of $x_{j+1}, \ldots, x_n$.

Let now e be some degree ($0 \leq e < d$). Denote f_e the coefficient of x_j^e in f and $w_{k,e}'''$ the coefficient of x_j^e in w_k''', for $1 \leq k < j$. Since the polynomials $p_1, \ldots, p_{j-1}$ are free of x_j, the following formula holds for each degree $0 \leq e < d$. Since f is nonzero, the formula holds for some e such that f_e is nonzero.

$$h' \, f_e \quad = \quad \underbrace{w_{1,e}''' \, p_1 + \cdots + w_{j-1,e}''' \, p_{j-1}}_{\mathscr{F}'} \, . \tag{16}$$

Formula (16) implies in particular that $h' \, f_e \in \mathfrak{a}$. Since h' is a nonzero element of $K[t_1, \ldots, t_m]$, it is a regular element of $R/\mathfrak{a}$, by the implication $1 \Rightarrow 4$ of Theorem 1 and the fact that $\mathrm{res}(h', A) = h'$. Thus $f_e \in \mathfrak{a}$. Since f_e is a coefficient of a polynomial f reduced w.r.t. A, it is reduced w.r.t. A also. The pair $(f_e, \mathscr{F}')$ thus belongs to $\mathscr{E}$ and is such that $j(\mathscr{F}') < j(\mathscr{F})$. This contradiction with the minimality of $j(\mathscr{F})$ proves that $\mathscr{E}$ must be empty and concludes the proof of the proposition. □

The two following Propositions already appear in [1, Theorem 6.1]. Their proofs are elementary.

Proposition 10. *Let A be a triangular set of R. Assume that for each polynomial $f \in R$ we have* $\mathrm{prem}(f, A) = 0$ *if $f \in \mathfrak{a}$. Then A is a regular chain.*

Proof. Since $\mathrm{prem}(f, A) = 0$ for each $f \in \mathfrak{a}$ and $\mathrm{prem}(1, A) \neq 0$, the ideal $\mathfrak{a}$ is proper.

Denote $R_\ell = K[t_1, \ldots, t_m, x_1, \ldots, x_\ell]$ and $\mathfrak{a}_\ell = \mathrm{sat}\,(p_1, \ldots, p_\ell)$ for each $1 \leq \ell \leq n$.

We assume the regular chain condition is satisfied up to index $k < n$ but not at index $k+1$ i.e. i_ℓ is regular in $R/\mathfrak{a}_{\ell-1}$ for each $2 \leq \ell \leq k$ and i_{k+1} is a zerodivisor in $R/\mathfrak{a}_k$. We prove that there exists some $f \in \mathfrak{a}$ such that $\mathrm{prem}(f, A) \neq 0$.

Denote $\mathfrak{b}_k = \mathfrak{a}_k : i_{k+1}^\infty = (p_1, \ldots, p_k) : (i_1 \cdots i_{k+1})^\infty$. Since i_{k+1} is a zerodivisor in $R/\mathfrak{a}_k$ we have $\mathfrak{a}_k \subsetneq \mathfrak{b}_k$. Thus there exists some $f \in \mathfrak{b}_k$, $f \notin \mathfrak{a}_k$. Since the defining polynomials of $\mathfrak{a}_k$ and $\mathfrak{b}_k$ belong to R_k, we may assume $f \in R_k$.

Since $f \notin \mathfrak{a}_k$, we have $\mathrm{prem}(f, A_k) \neq 0$ (Proposition 8). Since $f \in R_k$, we have $\mathrm{prem}(f, A_k) = \mathrm{prem}(f, A)$. Since $f \in \mathfrak{b}_k \subset \mathfrak{a}$, the Proposition is proved. □

The following proposition completes [5, Theorem 21].

Proposition 11. *Let A be a triangular set. The following conditions are equivalent:*

1. *A is a regular chain;*
6. *for each $f \in R$, $f \in \mathfrak{a}$ if and only if* $\mathrm{prem}(f, A) = 0$.

Proof. First observe that, for any set A, if $\mathrm{prem}(f, A) = 0$ then $f \in \mathfrak{a}$ (Proposition 8). The implication $1 \Rightarrow 6$ is then Proposition 9. The converse implication is Proposition 10. □

3. The Differential Case

3.1. Classical Results

Reference books are the ones of Ritt and Kolchin [13, 11].

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. Let Θ denote the multiplicative monoid of derivative operators, generated by the derivations and $\Theta^* \subset \Theta$ the set of proper derivative operators. Assume the infinite set of derivatives ΘU is ordered w.r.t. a ranking [11, I, 8, page 75] so that, given any differential polynomial $f \in R \setminus K$, its leading derivative $\mathrm{ld}\, f$ (called *leader* by Kolchin), its initial and its separant, which is the partial derivative of f w.r.t. its leading derivative, are well defined.

In the sequel, we will have to consider sets of differential polynomials as particular cases of sets of plain polynomials, in order to apply the results of Section 2. By a *triangular set* of differential polynomials $\{p_1, \ldots, p_n\}$ we mean a set of differential polynomials of $R \setminus K$ having pairwise distinct leading derivatives. In order to apply the results of the former sections and fit to their notations, we assume moreover that $\mathrm{ld}\, p_1 < \mathrm{ld}\, p_2 < \cdots < \mathrm{ld}\, p_n$. These leading derivatives then correspond to the variables $x_1, x_2, \ldots, x_n$. In particular, the numbering of the x is imposed by the ranking. The other derivatives occurring in the differential polynomials correspond to $t_1, \ldots, t_m$.

This being understood, there is no ambiguity in a statement such as "the triangular set A of differential polynomials is a regular chain". Similarly, if f is any differential polynomial, the differential polynomial $\mathrm{res}(f, A)$ is well defined, by means of the iterated resultant.

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 v of p [11, I, 9, page 77]. It is said to be *fully reduced* w.r.t. p if, in addition, $\deg(f, v) < \deg(p, v)$. If f is any element and A is any subset of $R \setminus K$, thanks to the pseudo-remainder algorithm, it is easy to compute a differential polynomial g, partially reduced w.r.t. A (i.e. w.r.t. each element of A) and such that $h\, f = g \pmod{[A]}$ where $[A]$ denotes the differential ideal generated by A in R and h is some power product of separants of A. The differential polynomial g is called a *partial remainder* of f by A. It is as well easy to compute a differential polynomial g, fully reduced w.r.t. A and such that $h\, f = g \pmod{[A]}$ where h is some power product of initials and separants of A. The differential polynomial g is called a *full remainder* of f by A. See [11, I, 9] or [13, I, 6].

Consider a triangular set A of differential polynomials of R. Let L denote the set of leading derivatives of A and $N = \Theta U \setminus \Theta L$ the possibly infinite set of the elements of ΘU which are not derivatives of any element of L (the derivatives "under the stairs" of A). Then $K[N \cup L] \subset R$ is the ring of the differential polynomials partially reduced w.r.t. A.

Uppercase gothic letters denote differential ideals while lowercase ones denote nondifferential ones. In particular, we denote $\mathfrak{A}$ the differential ideal $[A] : h^\infty$ of R where h denotes the product of the

initials and separants of A. We denote $\mathfrak{a} = \mathrm{sat}\,(A)$ the nondifferential ideal of R defined by A, viewed as a plain triangular set.

The concept of a squarefree regular chain actually is a nondifferential one. Intuitively, its relevance in the definition of regular differential chains (see below) comes from the fact the separant of a differential polynomial f is the initial of any proper derivative of f.

Definition 5. *A regular chain A is said to be* squarefree *if, for each $1 \leq k \leq n$, the separant s_k of p_k is regular in $R/\mathfrak{a}$.*

Definition 6. *A triangular set A of pairwise partially reduced differential polynomials is said to be* coherent *if, for each pair $\{p_1, p_2\}$ of polynomials of A whose leading derivatives $\theta_1 u, \theta_2 u$ are the derivatives of some common differential indeterminate $u \in U$, we have $\Delta(p_1, p_2) \in \mathrm{sat}\,(A')$ where $\theta_{12} = \mathrm{lcm}(\theta_1, \theta_2)$, $A' = \{p \in \Theta A \mid \mathrm{ld}\, p < \theta_{12} u\}$ and, denoting s_1 and s_2 the separants of p_1 and p_2,*

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

The pairs considered in the above definition may exist only if the number of derivations is greater than or equal to 2. Thus, in the ordinary differential case, every triangular set A of pairwise partially reduced differential polynomials is coherent.

Definition 7. *A triangular set A of pairwise partially reduced differential polynomials is said to be a regular differential chain if it is a coherent squarefree regular chain.*

The following characterization is [5, Theorem 37].

Theorem 2. *Let A be a triangular set of differential polynomials pairwise partially reduced. The following conditions are equivalent:*

1. *A is a regular differential chain;*
2. *A is coherent and, for each $1 \leq \ell \leq n$ and each $1 \leq k \leq n$ we have $\mathrm{res}(i_\ell, \{p_k, \ldots, p_n\})$ and $\mathrm{res}(s_\ell, \{p_k, \ldots, p_n\})$ regular in $R/\mathfrak{a}$;*
3. *A is coherent and $\mathrm{res}(i_\ell, A) \neq 0$ and $\mathrm{res}(s_\ell, A) \neq 0$ for each $1 \leq \ell \leq n$;*
4. *for each $f \in R$,*

$$f \text{ is regular in } R/\mathfrak{A}$$
$$\Updownarrow$$
for any triangular finite subset $A' \subset \Theta A$ such that $\mathrm{res}(f, A') \in K[N \cup L]$, $\mathrm{res}(f, A') \neq 0$.

The next proposition is [5, Proposition 35]. It is an easy corollary to Rosenfeld's Lemma [14].

Proposition 12. *Let A be a regular differential chain. Then $\mathfrak{A} \cap K[N \cup L] = \mathfrak{a} \cap K[N \cup L]$.*

The following proposition is well known. Its first statement is a particular case of a result proved in [3, 12, 10]. The second statement goes back to [13, I, 16; and IX, page 166].

Proposition 13. *Let A be a regular differential chain. Then $\mathfrak{A}$ is a radical differential ideal. In particular, it is a finite intersection of differential prime ideals $\mathfrak{A} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_r$, which is unique if it is minimal.*

The remaining part of this section is dedicated to normal forms. The following proposition restates [4, Definition 5.1 and Proposition 5.2].

Definition 8. *Let A be a regular differential chain and f/g be a fraction of differential polynomials with g regular in $R/\mathfrak{A}$. A fraction p/q of differential polynomials is said to be a* normal form of f/g modulo A *if it satisfies:*

1. *p is fully reduced w.r.t. A;*
2. *$q \in K[N]$;*
3. *f/g and p/q are equal in the total ring of fractions of $R/\mathfrak{A}$.*

Proposition 14. *Let A be a regular differential chain and f/g be a fraction of differential polynomials with g regular in $R/\mathfrak{A}$. The normal form of f/g modulo A exists and is unique.*

The next definition and proposition are [4, Definition 4.1, Proposition 4.3 and Proposition 5.1].

Definition 9. *Let A be a regular differential chain and g be a nonzero differential polynomial of R. An* inverse of g modulo A *is any fraction p/q of differential polynomials such that $p \in K[N \cup L]$, q is a nonzero element of $K[N]$ and $g\,p = q$ in $R/\mathfrak{A}$.*

Proposition 15. *Let A be a regular differential chain and g be a differential polynomial of R. Then g admits an inverse modulo A if and only if it is regular in $R/\mathfrak{A}$.*

3.2. A New Normal Form Algorithm

The following proposition is new and completes Theorem 2.

Proposition 16. *Let A be a regular differential chain. Then,*

5. *for each $f \in R$,*

$$f \text{ is a zerodivisor in } R/\mathfrak{A}$$
$$\Updownarrow$$
$$\text{for any triangular finite subset } A' \subset \Theta A \text{ such that } \operatorname{res}(f, A') \in K[N],\ \operatorname{res}(f, A') = 0.$$

Proof. First observe that there exists a triangular finite subset A' of ΘA such that $\operatorname{res}(f, A') \in K[N]$. Its finiteness follows from the fact that rankings are well-orderings [11, I, 8].

The bottom-up implication. Assume that, for any triangular finite subset $A' \subset \Theta A$ such that $\operatorname{res}(f, A') \in K[N]$ we have $\operatorname{res}(f, A') = 0$. Then f is a zerodivisor in $R/\mathfrak{A}$ by the implication $1 \Rightarrow 4$ of Theorem 2.

The top-down implication. Let A' be a triangular finite subset of ΘA such that $\operatorname{res}(f, A') \in K[N]$. Assume f is a zerodivisor in $R/\mathfrak{A}$. Then there exists some differential polynomial $g \notin \mathfrak{A}$ such that $f\,g \in \mathfrak{A}$.

Since $\mathfrak{A}$ is radical, it is a finite, minimal, intersection of differential prime ideals $\mathfrak{A} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_r$ by Proposition 13. Since f is a zerodivisor in $R/\mathfrak{A}$, renumbering the $\mathfrak{P}_i$ if needed, there exists some index $1 \leq s \leq r$ such that $f \in \mathfrak{P}_i$ if and only if $1 \leq i \leq s$. The differential polynomial g thus satisfies: 1) $g \in \mathfrak{P}_j$ for all $s < j \leq r$; and 2) $g \notin \mathfrak{P}_i$ for some $1 \leq i \leq s$.

Let $\bar{g}$ denote a full remainder of g by A (one may take $\bar{g} = \operatorname{prem}(g, A')$). For each $1 \leq i \leq r$, we have $g \in \mathfrak{P}_i$ if and only if $\bar{g} \in \mathfrak{P}_i$. In particular, $\bar{g} \notin \mathfrak{A}$ hence is nonzero. Consider now the resultant $r = \operatorname{res}(f, A')$. We have $r \in \mathfrak{P}_i$ for $1 \leq i \leq s$ by Proposition 1.

The product $r\,\bar{g} \in \mathfrak{P}_i$ for each $1 \leq i \leq r$ hence it belongs to $\mathfrak{A}$. Since $\bar{g} \in K[N \cup L]$ and $r \in K[N]$, we have $r\,\bar{g} \in \mathfrak{A} \cap K[N \cup L]$. Thus, by Proposition 12, $r\,\bar{g} \in \mathfrak{a}$, in some finitely generated polynomial subring of $K[N \cup L]$. Since A is a regular chain, we have $\operatorname{prem}(r\,\bar{g}, A) = 0$, by Proposition 9. Since $r \in K[N]$ and $\bar{g}$ is reduced w.r.t. A, the product $r\,\bar{g}$ is reduced w.r.t. A i.e. $\operatorname{prem}(r\,\bar{g}, A) = r\,\bar{g}$. Since $\bar{g} \neq 0$, we must have $r = 0$. □

Proposition 17. *Let g be a differential polynomial of R and f be a differential polynomial of $R \setminus K$ with leading derivative v.*

Then for any derivative operator $\theta \in \Theta^*$ we have $\operatorname{res}(g, \theta f, \theta v) = \pm \operatorname{prem}(g, \theta f, \theta v)$. In particular, there exists a power h of the separant of f such that $h\,g = \pm \operatorname{res}(g, \theta f, \theta v) \pmod{(\theta f)}$.

Proof. Since θ is a proper operator, θf has leading derivative θv, degree one in θv and the separant of f as leading coefficient w.r.t. θv. The Proposition then follows from Propositions 6 and 8. □

The following proposition is new and provides an algorithm for computing the inverse of a differential polynomial which is regular in $R/\mathfrak{A}$, since it relies on Proposition 1, which is itself of algorithmic nature.

Proposition 18. *Let A be a regular differential chain and g be a differential polynomial of R. Let A' be a triangular subset of ΘA such that $\operatorname{res}(g, A') \in K[N]$. Then*

1. *g is regular in $R/\mathfrak{A}$ if and only if* $\operatorname{res}(g, A') \neq 0$*;*
2. *there exists a differential polynomial $u \in K[N \cup L]$ such that $u\,g = \operatorname{res}(g, A')$ in $R/\mathfrak{A}$;*
3. *if g is regular in $R/\mathfrak{A}$, then $u/\operatorname{res}(g, A')$ is an inverse of g modulo A.*

Proof. Assume g is regular in $R/\mathfrak{A}$. Then $\operatorname{res}(g, A') \neq 0$ by the implication $1 \Rightarrow 4$ of Theorem 2. Conversely, assume g is a zerodivisor in $R/\mathfrak{A}$. Then $\operatorname{res}(g, A') = 0$ by Proposition 16. The first item is thus proved.

The existence of a differential polynomial u such that $u\,g = \operatorname{res}(g, A')$ in $R/\mathfrak{A}$ follows from Proposition 1. The fact that $u \in K[N \cup L]$ comes from the fact that the iterated resultant by A' can be decomposed into elementary resultants, either by elements of A, or by proper derivatives of elements of A. The polynomial u is the product of polynomials (say) u_i arising from these elementary resultant computations. In the first case, $u_i \in K[N \cup L]$; in the second case, u_i is a separant of some element of A, by Proposition 17, hence belongs also to $K[N \cup L]$. The second item is thus proved.

The third item follows from Definition 9 and the two former items. □

Algorithms 3 and 4 provide algorithms for computing the normal form of a differential fraction, which are directly derived from the theoretical construction achieved so far. In Algorithm 3, the inverse computations at lines 8 and 11 require the simple nondifferential Proposition 4 because the elements of A are pairwise partially reduced. In Algorithm 4, the differential polynomial g need not be partially reduced with respect to A. The inverse computation at line 1 thus requires the differential process described in Proposition 18.

Algorithm 3: `NFpoly_diff` (f, A)

input : a differential polynomial f and a differential regular chain A
output: the normal form of f modulo A

```
1  if f is fully reduced w.r.t. A then
2  |  return f
3  else
4  |  among all the derivatives of the leading derivatives of the elements of A which actually
   |   occur in f, let w be the highest, w.r.t. the ranking ;
5  |  let p_k ∈ A, with leading derivative v_k be such that w = θ v_k for some θ ∈ Θ ;
6  |  if θ = 1 then
7  |  |  compute i_k^α f = f̄ + q p_k ;                    /* f̄ = prem(f, p_k, v_k) */
8  |  |  compute u/r an inverse of i_k modulo A ;          /* Proposition 4 */
9  |  else
10 |  |  compute s_k^α f = f̄ + q (θ p_k) ;                /* f̄ = prem(f, θ p_k, θ v_k) */
11 |  |  compute u/r an inverse of s_k modulo A ;          /* Proposition 4 */
12 |  end
13 |  return (1/r^α) × NFpoly_diff (u^α f̄, A)
14 end
```

Algorithm 4: `NF_diff` $(f/g, A)$

input : a differential fraction f/g, and a differential regular chain A with g regular in $R/\mathfrak{A}$
output: the normal form of f/g modulo A

```
1  compute u/r an inverse of g modulo A ;                 /* Proposition 18 */
2  return (1/r) × NFpoly_diff(u f, A)
```

Algorithm 5 provides an alternative method for computing the normal form of a differential fraction, which takes advantage of the fact that one can start with a partial reduction step then proceed with Algorithm 2.

Algorithm 5: `NF_diff_v2` $(f/g, A)$

input : a differential fraction f/g, and A a differential regular chain with g regular in $R/\mathfrak{A}$
output: the normal form of f/g modulo A

1 compute $h_f\, f = \bar{f} \pmod{[A]}$ where h_f denotes a power product of separants of A
; `/* ` $\bar{f}$ `is a partial remainder of` f `by` A `*/`
2 compute $h_g\, g = \bar{g} \pmod{[A]}$ where h_g denotes a power product of separants of A
; `/* ` $\bar{g}$ `is a partial remainder of` g `by` A `*/`
3 **return** $\mathtt{NF}\left(\dfrac{h_g\,\bar{f}}{h_f\,\bar{g}}, A\right)$

4. Conclusion

In this paper, we have provided new and conceptually simple algorithms for computing normal forms of fractions modulo regular chains, in both the nondifferential and the differential case. We have also provided a new proof of the membership test to ideals defined by regular chains, which highlights the main non trivial argument underlying this well known result. However, one cannot exclude the existence of a completely elementary proof, which would actually lead to a simplified general theory of regular chains.

References

[1] Aubry, P., Lazard, D., Moreno Maza, M.: On the Theories of Triangular Sets. Journal of Symbolic Computation **28**, 105–124 (1999)

[2] Basu, S., Pollack, R., Roy, M.F.: Algorithms in Real Algebraic Geometry, Algorithms and Computation in Mathematics, vol. 10. Springer Verlag (2003)

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

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

[5] Boulier, F., Lemaire, F., Poteaux, A., Moreno Maza, M.: An Equivalence Theorem for Regular Differential Chains. Journal of Symbolic Computation **93**, 34–55 (2019), `hal.archives-ouvertes.fr/hal-01391768`

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

[7] Chen, C., , Golubitsky, O., Lemaire, F., Moreno Maza, M., Pan, W.: Comprehensive Triangular Decompositions. In: Proceedings of CASC'07. pp. 73–101 (2007)

[8] Ducos, L.: source of the axiom package `prs.spad` (1999), `http://www-math.sp2mi.univ-poitiers.fr/~ducos/src/travaux.html`

[9] Hubert, É.: Notes on triangular sets and triangulation–decomposition algorithm I: Polynomial Systems. Symbolic and Numerical Scientific Computing 2001 pp. 243–158 (2003)

[10] Hubert, É.: Notes on triangular sets and triangulation–decomposition algorithm II: Differential Systems. Symbolic and Numerical Scientific Computing 2001 pp. 40–87 (2003)

[11] Kolchin, E.R.: Differential Algebra and Algebraic Groups. Academic Press, New York (1973)

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

[13] Ritt, J.F.: Differential Algebra, American Mathematical Society Colloquium Publications, vol. 33. American Mathematical Society, New York (1950)

[14] Rosenfeld, A.: Specializations in differential algebra. Trans. Amer. Math. Soc. **90**, 394–407 (1959)

[15] Wang, D.: Elimination Methods. Springer Verlag, Wien New York (2001)

[16] Yang, L., Zhang, J.: Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Artificial Intelligence in Mathematics pp. 147–156 (1994), 1991 version available at `streaming.ictp.trieste.it/preprints/P/91/006.pdf`

[17] Zariski, O., Samuel, P.: Commutative Algebra. Van Nostrand, New York (1958), Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag

François Boulier
Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France `pro.univ-lille.fr/francois-boulier`
e-mail: `francois.boulier@univ-lille.fr`

François Lemaire
Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France `pro.univ-lille.fr/francois-lemaire`
e-mail: `francois.lemaire@univ-lille.fr`

Marc Moreno Maza
Univ. Western Ontario, ORCCA, N6A 3K7, London, Ontario, Canada
e-mail: `moreno@csd.uwo.ca`

Adrien Poteaux
Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France `pro.univ-lille.fr/adrien-poteaux`
e-mail: `adrien.poteaux@univ-lille.fr`