Notes on Triangular Sets and Triangulation-Decomposition Algorithms I: Polynomial Systems

Evelyne Hubert

INRIA - Projet CAFE
2004 route des lucioles BP 93
F-06902 Sophia Antipolis
Evelyne.Hubert@inria.fr

Abstract. This is the first in a series of two tutorial articles devoted to triangulation-decomposition algorithms. The value of these notes resides in the uniform presentation of triangulation-decomposition of polynomial and differential radical ideals with detailed proofs of all the presented results.We emphasize the study of the mathematical objects manipulated by the algorithms and show their properties independently of those. We also detail a selection of algorithms, one for each task. We address here polynomial systems and some of the material we develop here will be used in the second part, devoted to differential systems.

1 Introduction

The natural representation of a tower of separable field extensions is a triangular set having some irreducibility properties. Those special triangular sets, called characteristic sets, therefore provide a natural representation for prime ideals in polynomial rings. That idea was in fact first fully developed by J.F.Ritt [Rit32, Rit50] in the context of differential algebra. Ritt gave an algorithm to represent the radical ideal generated by a finite set of polynomials as an intersection of prime ideals defined by their characteristic sets. For want of effectiveness and realistic implementations the irreducibility requirements were to disappear both in the representation of field extensions and of radical ideals.

What we call a triangulation-decomposition algorithm is an algorithm that computes a representation of the radical ideal generated by a finite set of polynomials as an intersection of ideals defined by triangular sets. Many triangulation-decomposition algorithms in fact provide a zero decomposition: the variety defined by a set of polynomials is decomposed into quasi-varieties. To be general, the quasi-varieties are described by a triangular system of equations and a set of inequations. Application or algorithm requirements lead to output systems and decomposition with more or less specific properties, [Wan99] presents quite a few options. Bridges between different approaches have been proposed in [ALMM99, AMM99, Del00a, Del01].

Zero decomposition algorithms were investigated and developed for application to geometry theorem proving starting with the work of Wu in the late seventies [Wu78]. Books devoted to the field include [Wu94, Cho88, CGZ94, Wu00]. As for field representation, the D5 system [DDD85, Duv87] was designed to work with algebraic numbers without factorization. Its extension to the dynamical closure system D7 [GD94, Del99, Del00b] is intended to work with towers of extensions. A side product of the D7 system is a zero decomposition algorithm. Last but not least, triangular forms of systems of polynomials are very amenable to resolution. Triangulation-decomposition of polynomial systems are therefore naturally applicable to solving polynomial systems with finite number of solutions [Laz92, MMR95] and parametric systems [GC92, Sch00]. In the case of polynomial system with a variety of positive dimension the decomposition computed is *strongly* unmixed dimensional [Laz91, MM97, Sza98, Aub99]. It therefore gives an excellent description of the variety and can be relatively easily refined into an irreducible decomposition. Solving polynomial system with triangulation-decomposition is particularly adequate when the solution set has relevant components of different dimensions, as is the case of the classification problem solved in [FMM01]. Triangulation-decomposition has also proved adequate for solving positive dimensional systems over the reals [ARSED00]. Also, elementary-algebraic systems [Ric99, BJ01] can be attacked with this technique.

The first focus of this paper is a thorough study of ideals defined by triangular sets. Many of the presented results are either assumed or disseminated in the literature. We will give full proofs to all those results. The second focus will be on Kalkbrener's algorithm. That algorithm was first presented in [Kal93] in a very synthetic and highly recursive way. Our presentation owes to the presentation of [Aub99].

The basic idea of working with triangular sets is to consider multivariate polynomials as univariate polynomial in a distinguished variable, the *leader*. We want to treat systems of polynomials recursively as univariate polynomials. The *reduction* of one polynomial by another will be pseudo-division.

Triangular sets are sets of polynomials with distinct leaders. We look at the ideals they define outside of some singularity sets, given by the *initials* of the polynomials, i.e. the leading coefficients of the polynomials when considered as univariate polynomial in the leader. These ideals have excellent properties: they are unmixed dimensional and the non leading variables give a transcendence basis for all associated primes (see Section 4). Thanks to that structure, we can associate a product of fields to a triangular set in a natural way.

Some specific triangular sets, called *regular chains* (Section 5), are amenable to computations. This is because the cutback of the ideal defined is given by the cutback of the regular chain. Computations can thus be lead recursively in a univariate way. Regular chains give the ideal they define a membership test, as well as a zero-divisor test (Section 8).

Of course, not every ideal can be written as the ideal defined by a regular chain. Our final goal is to give an algorithm that writes the radical ideal generated by some finite set of polynomials as an intersection of (radicals of) *characterizable ideals.* Characterizable ideals can be defined intrinsically and are given by regular chains.

For the zero-divisor test or the decomposition into characterizable ideals, there is an interesting notion coming in, the *pseudo-gcd.* This is a generalization of the gcd of univariate polynomial over a field to the case of univariate polynomials over a product of fields. In our case, we consider univariate polynomials with coefficients taken modulo the ideal defined by a triangular set.

The paper is organized as follow. In Section 2 we shall review some definitions and basic properties on polynomial rings. We in particular give a series of results about zero-divisors. We conclude the section with a simple example of a splitting procedure of a product of fields. This serves as an introduction to one of the two main components of Kalkbrener's algorithm. In Section 3 we review pseudo-division and its property and the definition of pseudo-gcd, as in [Aub99] . After the pseudo-gcd definition, we give an algorithm to compute a pseudo-gcd assuming we are given a splitting procedure. That provides an introduction to the second main component of Kalkbrener's algorithm. In Section 4 triangular sets together with the fundamental properties of the ideals they define are detailed. In Section 5, we define regular chain, review the notion of characteristic set of Ritt and give the equivalence of [ALMM99] between the two approaches. For the characterizable ideals they define we exhibit canonical representatives. Section 6 defines characteristic decompositions and makes the link between irredundant decompositions and decomposition of a product fields. Before the algorithmic part of the article, we assemble in Section 7 a number of results about the radical of an ideal defined by a triangular set. These results are of use to construct the radical of a characterizable ideal and in differential algebra [Hub02]. Section 8 gives the two components of Kalkbrener's algorithm, one to split and one to compute the pseudo-gcd. These components are then applied in Section 9 to provide a characteristic decomposition algorithm. A further application will be given in [Hub02] for the algebraic part of a decomposition algorithm in differential algebra.

2 Preliminaries and notations in commutative algebra

We recall here some basic definitions and results in commutative algebra and take the opportunity to set up some notations. The notions we shall expand on are saturation ideal, zero divisors and product of fields. All of these are central in the techniques of triangular sets and in Kalkbrener's algorithm. Other notions can be found for instance in [Eis94].

2.1 Ideals, saturation and equidimensionality

In this section and the following, $\mathcal{R}$ is a Noetherian ring. Let H be a subset of $\mathcal{R}$. We denote by H^∞ the minimal subset of $\mathcal{R}$ that contains 1 and H and is stable by multiplication and division i.e. $a, b \in H^\infty \;\Leftrightarrow\; ab \in H^\infty$. When H consists of a unique element h we will write h^∞ instead of $\{h\}^\infty$.

Let I be an ideal of $\mathcal{R}$. We define the saturation of I by a subset H of $\mathcal{R}$ as $I : H^\infty = \{q \in \mathcal{R} \mid \exists\, h \in H^\infty \text{ s.t. } h\,q \in I\}$. $I \subset I : H^\infty$ and $I : H^\infty$ is an ideal. Consider $H^{-1}\,\mathcal{R}$ the localization of $\mathcal{R}$ at H^∞. Let $H^{-1}\,I$ be the extension of I in $H^{-1}\,\mathcal{R}$. When $0 \notin H^\infty$, $I : H^\infty = H^{-1}\,I \,\cap\, \mathcal{R}$.

If P is a primary ideal of $\mathcal{R}$, $P : H^\infty$ is either equal to P or $\mathcal{R}$ according to whether $H \cap \sqrt{P}$ is empty or not. This has the following consequence.

Proposition 2.1. *Let J be an ideal of $\mathcal{R}$, and H a subset of $\mathcal{R}$. $J : H^\infty$ is the intersection of those primary components of J the radical of which have an empty intersection with H.*

We shall see that the ideals defined by triangular sets that are central in our approach are *unmixed dimensional*. The following definition is taken from [Vas98].

Definition 2.2. *Let $\mathcal{R}$ be a Noetherian ring. An ideal I in $\mathcal{R}$ is equidimensional if all its minimal primes have the same codimension. An ideal I in $\mathcal{R}$ is unmixed dimensional, if all its associated prime have the same codimension.*

An ideal that is unmixed dimensional is equidimensional and has no embedded primes. Therefore, the set of primary components is uniquely determined. Every zero-dimensional ideal is unmixed dimensional.

We note (F) the ideal generated by a non empty subset F of $\mathcal{R}$. For an ideal I of $\mathcal{R}$, we note $\sqrt{I}$ the radical of I that is $\sqrt{I} = \{r \in \mathcal{R} \mid \exists \alpha \in \mathbb{N} \text{ s.t. } r^\alpha \in I\}$, which is a radical ideal. $\sqrt{(F)}$ will be noted $\langle F \rangle$.

2.2 Zero divisors

In Kalkbrener's algorithm, deciding if an element is a zero divisor modulo the ideal defined by a triangular set is a central figure. We set up some notations that will enable us to describe the algorithms in a more compact way. We review also a number of results that will be useful, in particular Gauss lemma.

We shall see that to a triangular set is naturally associated a product of fields. Computing modulo the ideal defined by a triangular set amounts to compute over this product of fields. We review some of the features of product of fields and their natural construction with the Chinese remainder theorem.

Given a ring $\mathcal{R}$, $\mathfrak{Zd}(\mathcal{R})$ will denote the set consisting of 0 and the zero divisors of $\mathcal{R}$. The total quotient ring of $\mathcal{R}$, that is the localization of $\mathcal{R}$ at $\mathcal{R} \setminus \mathfrak{Zd}(\mathcal{R})$ will be written $\mathfrak{Q}(\mathcal{R})$.

Let I be an ideal in $\mathcal{R}$. An element p of $\mathcal{R}$ is said to be

- invertible modulo I if its canonical image in $\mathcal{R}/I$ is a unit.
- a zero divisor modulo I if its canonical image in $\mathcal{R}/I$ is a zero divisor. By extension we write $p \in \mathfrak{Zd}(\mathcal{R}/I)$ or $p \in \mathfrak{Zd}(I)$ for short.

Note that an element of $\mathcal{R}$ is invertible modulo an ideal I iff it is invertible modulo the radical, $\sqrt{I}$. An element p of $\mathcal{R}$ is a zero divisor modulo an ideal I

iff p belongs to an associated prime of I. Thus, when I a unmixed dimensional $\mathfrak{Zd}(I) = \mathfrak{Zd}(\sqrt{I})$.

The following theorem is Gauss lemma [Eis94, Exercise 3.4]. It gives a practical test for a univariate polynomial to be a zero divisor. A weak version of this lemma is traditionally used in the literature on triangular sets: the test is made on the leading coefficient only. We will use it in its generality.

Theorem 2.3. *Consider a polynomial $f \in \mathcal{R}[x]$ and note C_f the ideal in $\mathcal{R}$ generated by the coefficients of f (the* content *of f). Then $f \in \mathfrak{Zd}(\mathcal{R}[x]) \quad \Leftrightarrow C_f \subset \mathfrak{Zd}(\mathcal{R})$.*

2.3 Product of fields

The Chinese Remainder Theorem [Eis94, Exercise 2.6] is a major tool in constructing product of rings - and thus of fields.

Theorem 2.4. *Let $Q_1, \ldots, Q_r$ be ideals in $\mathcal{R}$ such that $Q_i + Q_j = \mathcal{R}$ for all $i \neq j$. Then*

$$\mathcal{R}/\left(\bigcap_{i=1}^{r} Q_i\right) \cong \prod_{i=1}^{r} \mathcal{R}/Q_i.$$

When the Q_i are maximal ideals in $\mathcal{R}$, $\mathcal{R}/\left(\bigcap_{i=1}^{r} Q_i\right)$ is isomorphic to a product of fields. In particular, the quotient of $\mathcal{R}$ by a zero dimensional radical ideal is isomorphic to a product of fields.

Lemma 2.5. *Let $\mathcal{R}$ be a ring isomorphic to a product of fields. The total quotient ring of $\mathcal{R}$, $\mathfrak{Q}(\mathcal{R})$, is equal to $\mathcal{R}$.*

This is easily seen as a nonzero element of $\mathcal{R}$ that is not a zero divisor is a unit.

2.4 A splitting procedure

We shall pause here to introduce on a simple case the concept of splitting that comes into Kalkbrener's algorithm. Let $\mathcal{K}$ be a field and c a square-free univariate polynomial over $\mathcal{K}$, say in $\mathcal{K}[\lambda]$. Assume $c = \prod_{i=1}^{r} c_i$ is a decomposition into irreducible factors. By the Chinese remainder theorem $\mathcal{R} = \mathcal{K}[\lambda]/(c)$ is isomorphic to the product of the fields $\mathcal{K}_i = \mathcal{K}[\lambda]/(c_i)$.

To work over $\mathcal{R}$, i.e. modulo the algebraic condition on λ, one can factor c and work over each $\mathcal{K}_i$. Beside factorization, this implies repeating the same computation for several components. Instead, at each step of a computation, we can group the components where the same computation are done. We only need to distinguish the components on which an element is a unit from the components on which it is zero.

Given an element p in $\mathcal{K}[\lambda]$ it is possible to *split* $\mathcal{R}$ into two products of fields, $\mathcal{R}_0$ and $\mathcal{R}_1$, in such a way that the natural projection of p on $\mathcal{R}_0$ is zero while the projection on $\mathcal{R}_1$ is a unit. If $g_0 = \gcd(p,c)$ and $g_1 = \frac{c}{g_0}$ then we can just take $\mathcal{R}_0 = \mathcal{K}[\lambda]/(g_0)$ and $\mathcal{R}_1 = \mathcal{K}[\lambda]/(g_1)$. If $g_0, g_1 \notin \mathcal{K}$ then $\mathcal{R} \cong \mathcal{R}_0 \times \mathcal{R}_1$.

When c is not square-free we consider $\mathcal{R} = \mathcal{K}[\lambda]/\langle c\rangle$. We can take $\mathcal{R}_0 = \mathcal{K}[\lambda]/\langle g_0\rangle$, where $g_0 = \gcd(p,c)$. But now p and $g_1 = \frac{c}{g_0}$ may have common factors, in which case p is not a unit in $\mathcal{K}[\lambda]/\langle g_1\rangle$. Consider the sequence starting with g_1 s.t. $g_{k+1} = \frac{g_k}{\gcd(p,g_k)}$. For some k, $g_{k+1} \in \mathcal{K}$. We can then take $\mathcal{R}_1 = \mathcal{K}[\lambda]/\langle g_k\rangle$ so that $\mathcal{R} = \mathcal{R}_0 \times \mathcal{R}_1$.

3 Univariate polynomials over a ring

The basic reduction step in the triangular set techniques is pseudo division. We review briefly the properties of such an operation. We then introduce the notion of pseudo-gcd that was defined in [Aub99] to put a mathematical frame on Kalkbrener's algorithm. The pseudo-gcd (or pgcd) of a non empty set of univariate polynomials over a ring is the generalization of gcd in a principal ideal ring, i.e. the generator of the ideal. It is well defined over a product of fields. We shall show how to compute a pseudo-gcd over a product of fields when we have a splitting algorithm. This is a fairly simple extension of Euclid's algorithm. Kalkbrener's algorithm evolves on this basic idea.

3.1 Pseudo division

Let $\mathcal{R}[x]$ be a ring of univariate polynomials with coefficients in the ring $\mathcal{R}$. For a polynomial $p \in \mathcal{R}[x]$ we will note

- $\deg(p,x)$ the degree of p in x
- $\mathsf{lcoeff}(p,x)$ the coefficient of $x^{\deg(p,x)}$ in p (the leading coefficient).
- $\mathsf{tail}(p,x) = p - \mathsf{lcoeff}(p,x)\, x^{\deg(p,x)}$.

Let $p,q \in \mathcal{R}[x]$, $q \neq 0$, $d = \deg(p,x)$, $e = deg(q,x)$ and $c = \mathsf{lcoeff}(q,x)$. The pseudo-remainder of p w.r.t. q is defined as the unique polynomial $\bar{p}$ such that $\deg(\bar{p},x) < \deg(q,x)$ and $c^{d-e+1}\,p \equiv \bar{p} \mod (q)$ when $d \geq e$, p otherwise [GCL92, vzGG99]. A sparse pseudo-remainder is usually defined by taking a power of c as small as possible. One can be slightly more general and define a sparse pseudo-remainder of p with respect to q to be a polynomial r of degree in x strictly lower than that of p for which there exists $h \in c^\infty$ s.t. $h\,p \equiv r \mod (q)$. An equality $h\,p = aq + r$ where $p,q,a,r \in \mathcal{R}[x]$, $\deg(r,x) < \deg(q,x)$ and $h \in \mathsf{lcoeff}(q,x)^\infty$ is called a pseudo-division relationship (of p by q). We will write $r = \mathsf{srem}(p,q,x)$ and $a = \mathsf{squo}(p,q,x)$, though these two quantities depend on the algorithm used to compute them. We nonetheless have a kind of uniqueness property.

Proposition 3.1. *Let $f,g \in \mathcal{R}[x]$ such that $\mathsf{lcoeff}(g,x) \notin \mathfrak{Zd}(\mathcal{R})$. Assume $h\,f = q\,g + r$ and $h'\,f = q'\,g + r'$ are two pseudo division relationships. Let $\bar{h}, \bar{h}' \in \mathsf{lcoeff}(g,x)^\infty$ be chosen so that $\bar{h}\,h = \bar{h}'\,h'$. Then $\bar{h}\,q = \bar{h}'\,q'$ and $\bar{h}\,r = \bar{h}'\,r'$*

Proof. Indeed $\bar{h}\,h\,f = \bar{h}\,(q\,g + r)$ and $\bar{h}'\,h'\,f = \bar{h}'\,(q'\,g + r')$. Therefore $(\bar{h}\,q - \bar{h}'\,q)\,g = \bar{h}'\,r' - \bar{h}\,r$. The right hand side is of degree strictly less than $\deg(g, x)$. Since $\mathsf{lcoeff}(g, x)$ is not a zero divisor, it follows that $(\bar{h}\,q - \bar{h}'\,q)$ is zero and so is $(\bar{h}'\,r' - \bar{h}\,r)$.

It follows that the pseudo remainder is zero iff all the sparse pseudo remainders are zero. The following property is shown in a similar way.

PROPOSITION 3.2. *Let $f, g \in \mathcal{R}[x]$ be such that $\mathsf{lcoeff}(g, x) \notin \mathfrak{Z}\mathfrak{d}(\mathcal{R})$. The polynomial g divides f in $\mathfrak{Q}(\mathcal{R})[x]$ iff $\mathsf{srem}(f, g, x) = 0$.*

3.2 Pseudo-gcd over a product of fields

The notion of pseudo-gcd is present in [Laz91, Kal93, MMR95] We reproduce here the definition given in [Aub99].

DEFINITION 3.3. *Let $\mathcal{R}$ be a ring isomorphic to a product of fields and F a non-empty subset of $\mathcal{R}[x]$. The pseudo-gcd of F over $\mathcal{R}$ is a set of pairs $\{(\mathcal{R}_1, g_1), \ldots, (\mathcal{R}_r, g_r)\}$ such that*

- *$(F) = (g_i)$ in $\mathcal{R}_i[x]$, $1 \le i \le r$.*
- *$\mathcal{R}_1, \ldots, \mathcal{R}_r$ are isomorphic to products of fields and $\mathcal{R} \cong \mathcal{R}_1 \times \ldots \times \mathcal{R}_r$.*

The existence of a pseudo-gcd is secured by the existence of a gcd over each field that is a component of $\mathcal{R}$.

We shall expand here on the generalization of Euclid's algorithm over a product of fields as it is a good introduction to Kalkbrener's algorithm. Assume that we have for a product of fields $\mathcal{R}$ the procedures

- $\mathsf{is\text{-}zero}$ that decides if an element of $\mathcal{R}$ is zero
- $\mathsf{is\text{-}zerodivisor}$ that decides if an element of $\mathcal{R}$ is a zero divisor
- split that splits $\mathcal{R}$ according to a zerodivisor p into $\mathcal{R}_0$ and $\mathcal{R}_1$ s.t. $\mathcal{R} \cong \mathcal{R}_0 \times \mathcal{R}_1$ and $p = 0$ in $\mathcal{R}_0$ while p is a non zero divisor in $\mathcal{R}_1$.

In Section 2.4, we saw for $\mathcal{R} = \mathcal{K}[\lambda]/\langle c\rangle$, c a polynomial in $\mathcal{K}[\lambda]$, how to write these procedures. One can rework Euclid's algorithm to compute the pseudo-gcd of two polynomials in $\mathcal{R}[x]$. It will work with the following property:

PROPOSITION 3.4. *Let $f, g \in \mathcal{R}[x]$ be such that $\mathsf{lcoeff}(g, x) \notin \mathfrak{Z}\mathfrak{d}(\mathcal{R})$. The ideals (f, g) and $(\mathsf{srem}(f, g, x), g)$ are equal when considered as ideals in $\mathfrak{Q}(\mathcal{R})[x]$.*

Recall that $\mathfrak{Q}(\mathcal{R}) = \mathcal{R}$ when $\mathcal{R}$ is a product of fields and so $(f, g) = (\mathsf{srem}(f, g, x), g)$ in $\mathcal{R}[x]$. In the general pgcd algorithm of Section 8.1 we will nonetheless have a slightly stronger result that needs this statement.

The following algorithm computes the pgcd of two univariate polynomials over $\mathcal{R}$. It is described in MAPLE style. As we shall often do in algorithm description, $\mathcal{S}$ is a set of tuples that await more computations while $\mathcal{G}$ contains data for which the computation is over. The command pop returns one element of a set and removes it from that set. Tuples are noted with parenthesis to fit mathematical notation rather than the MAPLE list construction with brackets.

Algorithm 3.5. *pgcd*
Input:

- $\mathcal{R}$ *a ring that is isomorphic to a product of fields.*
- p *and* q *polynomials in* $\mathcal{R}[x]$.

Output: *A pgcd* $\{(\mathcal{R}_1, g_1), \ldots, (\mathcal{R}_r, g_r)\}$ *of* p *and* q *over* $\mathcal{R}$.

$\mathcal{S} := \{(\mathcal{R}, p, q)\}$;
$\mathcal{G} := \emptyset$;
while $\mathcal{S} \neq \emptyset$ *do*
  $(\mathcal{Q}, a, b) :=$ *pop* $(\mathcal{S})$;
  if $b = 0$ *then*
    $\mathcal{G} := \mathcal{G} \cup \{(\mathcal{Q}, a)\}$;
  else
    $c :=$ *lcoeff*(b, x);
    if *is-zero*$(\mathcal{Q}, c)$ *then*
      $\mathcal{S} := \mathcal{S} \cup \{(\mathcal{Q}, a, \mathit{tail}(b, x))\}$;
    elif *is-zerodivisor*$(\mathcal{Q}, c)$ *then*
      $\mathcal{Q}_0, \mathcal{Q}_1 :=$ *split* $(\mathcal{Q}, c)$;
      $\mathcal{S} := \mathcal{S} \cup \{(\mathcal{Q}_0, a, \mathit{tail}(b, x)), (\mathcal{Q}_1, b, \mathit{srem}(a, b, x))\}$;
    else
      $\mathcal{S} := \mathcal{S} \cup \{(\mathcal{Q}, b, \mathit{srem}(a, b, x))\}$;
    fi;
return(G);

Together with what was presented in Section 2.4 we can now compute the pgcd of two polynomials in $(\mathcal{K}[\lambda]/\langle c\rangle)[x]$. The procedure can be made more efficient by using subresultant sequences [AK93, Del00c].

4 Multivariate polynomials with a recursive univariate viewpoint

We shall see multivariate polynomials as univariate polynomials in a distinguished variable. The coefficients are multivariate polynomials. Triangular sets are the basic objects of our approach. They define ideals with specific structure to which we associate products of fields.

4.1 Vocabulary for multivariate polynomials

Consider the polynomial ring $\mathcal{K}[X]$ where X is a set of ordered variables. The order on the indeterminates is called a *ranking* in the line of the terminology introduced by Ritt. A side effect is to avoid possible confusion with the term ordering used in Gröbner bases theory. For $x \in X$ we write $X_{>x}$, and respectively $X_{<x}$, the set of variables greater, and respectively lower, than x in X. We denote also $X_{\leq x} = X_{<x} \cup \{x\}$. When we write $\mathcal{K}[X][y]$ for $\mathcal{K}[X \cup \{y\}]$ it will be understood that $\forall x \in X,\ x < y$.

Let p be a polynomial in $\mathcal{K}[X] \setminus \mathcal{K}$. The *leader* and the *initial* of p are respectively the highest ranking variable appearing in p and the coefficient of its highest power in p. They will be noted $\mathsf{lead}(p)$ and $\mathsf{init}(p)$. If d is the degree of p in its leader, the rank of p is the term $\mathsf{rank}(p) = \mathsf{lead}(p)^d$.

The ranking on X induces a pre-order[1] on the polynomials of $\mathcal{K}[X]$. An element $q \in \mathcal{K}[X] \setminus \mathcal{K}$ is said to have higher rank (or to *rank higher*) than p when its leader, $\mathsf{lead}(q)$, has higher rank than $\mathsf{lead}(p)$ or when $\mathsf{lead}(p) = \mathsf{lead}(q)$ and the degree in this common leader is bigger in q than in p. In that case we write $\mathsf{rank}(q) > \mathsf{rank}(p)$.

A polynomial q is *reduced w.r.t.* p if the degree of q in $\mathsf{lead}(p)$ is strictly less than the degree of p in $\mathsf{lead}(p)$.

4.2 Triangular sets

From now on we consider a polynomial ring $\mathcal{K}[X]$ endowed with a ranking.

DEFINITION 4.1. *A subset of $\mathcal{K}[X]$ is a triangular set if it has no element in $\mathcal{K}$ and the leaders of its elements are pairwise different.*

A triangular set cannot have more elements than X but can be the empty set. Let $a_1, a_2, \ldots, a_r$ be the elements of a triangular set A such that $\mathsf{lead}(a_1) < \mathsf{lead}(a_2) < \ldots < \mathsf{lead}(a_r)$. We shall write $A = a_1 \vartriangle a_2 \vartriangle \ldots \vartriangle a_r$. We will also use the small triangle $\vartriangle$ to construct triangular sets by mixing polynomials a and triangular sets A, B in the following ways:

- $a \vartriangle A$ denotes the triangular set $A \cup \{a\}$ if a is such that $\mathsf{lead}(a)$ ranks lower than the leader of any element of A
- $A \vartriangle a$ denotes the triangular set $A \cup \{a\}$ if a is such that $\mathsf{lead}(a)$ ranks higher than the leader of any element of A
- $A \vartriangle B$ denotes the triangular set $A \cup B$ if the leader of any element of A ranks less than the leader of any element of B.

For a triangular set A in $\mathcal{K}[X]$ we note $\mathfrak{L}(A)$ and I_A the sets of the leaders and of the initials of the elements of A. We will also note $\mathfrak{T}(A) = X \setminus \mathfrak{L}(A)$ the set of the non leading variables of A. For $x \in X$ we define A_x to be the element of A with leader x if there is any, 0 otherwise. $A_{<x} = A \cap \mathcal{K}[X_{<x}]$, $A_{\leq x} = A \cap \mathcal{K}[X_{\leq x}]$ and $A_{>x} = A \setminus (A_{\leq x})$. $A_{<x}$ can be considered as a triangular set of $\mathcal{K}[X]$ or as a triangular set of $\mathcal{K}[X_{<x}]$.

A polynomial p is said to be reduced with respect to a triangular set A if for all x in $\mathfrak{L}(A)$ we have $\deg(p, x) < \deg(A_x, x)$. The pseudo division algorithm can be extended to compute the *reduction* of a polynomial in $\mathcal{K}[X]$ with respect to A.

[1] We take the convention that a pre-order is a relation that is reflexive, transitive and connex [BW93]. Therefore the difference with an order is that $a \leq b$ and $b \leq a$ does not imply $a = b$.

Lemma 4.2. *Let A be a non empty triangular set and p a polynomial in $\mathcal{K}[X]$. There exists $h \in I_A^\infty$ and $r \in \mathcal{K}[X]$ reduced w.r.t. A such that $h\,p \equiv r \mod (A)$. We will write $r = \mathsf{red}(p, A)$.*

The pair (h, r) is not unique but in our use, any such pair will do. If $A = a_1 \vartriangle \ldots \vartriangle a_m$ we can take

$$\mathsf{red}(p, A) = \mathsf{srem}(\ldots \mathsf{srem}(\mathsf{srem}(p, a_m, u_m), a_{m-1}, u_{m-1}), \ldots, a_1, u_1)\ ,$$

where $u_i = \mathsf{lead}(a_i)$.

Note that if $\mathsf{red}(p, A) = 0$ then $p \in (A) : I_A^\infty$. The best we can expect to represent with a non empty triangular set A of $\mathcal{K}[X]$ is the ideal $(A) : I_A^\infty$. For readability in some equation we note $\mathcal{I}(A) = (A) : I_A^\infty$ and $\mathcal{R}(A) = \sqrt{\mathcal{I}(A)} = \langle A \rangle : I_A^\infty$. For the empty set we take as a convention that $\mathcal{I}(\emptyset) = \mathcal{R}(\emptyset) = (0)$. A triangular set is said to be *consistent* if $1 \notin (A) : I_A^\infty$.

At some points we shall extend the coefficient field to the rational function field in the non leading variables $\mathfrak{T}(A)$ of A. We will write $\mathcal{K}_A = \mathcal{K}(\mathfrak{T}(A))$ and consider the ring of polynomials $\mathcal{K}_A[\mathfrak{L}(A)]$. If $\mathfrak{L}(A)$ is ordered according to the ranking on $\mathcal{K}[X]$ then A is a triangular set in $\mathcal{K}_A[\mathfrak{L}(A)]$. For a consistent triangular set A we furthermore define $\mathfrak{R}(A)$ the ring $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]\ /\ \mathcal{R}(A)$. We shall see that this ring is isomorphic to a product of fields (Proposition 4.7).

4.3 Ideals defined by triangular sets

In this section we examine the properties of the ideal $\mathcal{I}(A) = (A) : I_A^\infty$ defined by a triangular set A. They are unmixed dimensional and all the associated prime share the same transcendence basis, as stated in Theorem 4.4. There are several references for that theorem or its related results [GC92, Kal93, Sza98, Aub99, Hub00]. We also study the cutback properties of ideals defined by triangular sets. Indeed the basic operations on triangular sets is to extend or cut them shorter.

Lemma 4.3. *Let A be a triangular set in $\mathcal{K}[X]$. Let $a \in \mathcal{K}[X][x]$ be of strictly positive degree in x and $h = \mathsf{init}(a)$. Then*

$$(\mathcal{I}(A) : h^\infty + (a)) : h^\infty = \mathcal{I}(A \vartriangle a) \quad \text{and} \quad \mathcal{I}(A \vartriangle a) \cap \mathcal{K}[X] = \mathcal{I}(A) : h^\infty$$

Proof. We prove the first equality. Since $h \in I_{A \vartriangle a}$, it follows that $\mathcal{I}(A) : h^\infty \subset \mathcal{I}(A \vartriangle a)$ and thus $((a) + \mathcal{I}(A) : h^\infty) : h^\infty \subset \mathcal{I}(A \vartriangle a)$.

Let $p \in \mathcal{I}(A \vartriangle a)$. There exist $\bar{h} \in h^\infty$, $k \in I_A^\infty$ and $\bar{q} \in \mathcal{K}[X][x]$ such that $\bar{h}\,k\,p = \bar{q}\,a \mod (A)$. Since $\bar{h}\,k \notin \mathfrak{Zd}(\mathcal{I}(A) : h^\infty)$, p is divisible by a in $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(A) : h^\infty)[x]$. By Proposition 3.2 there exists $h' \in h^\infty$ and $q' \in \mathcal{K}[X]$ such that $h'\,p = q'\,a \mod \mathcal{I}(A) : h^\infty$. Thus $p \in (\mathcal{I}(A) : h^\infty + (a)) : h^\infty$.

For the second equality assume $p \in \mathcal{I}(A \vartriangle a) = (\mathcal{I}(A) : h^\infty + (a)) : h^\infty$. There exists $h' \in h^\infty, q \in \mathcal{K}[X][x]$ such that $h'\,p - q\,a \in \mathcal{I}(A) : h^\infty$, and therefore all the coefficients of the powers of x in $h'\,p - q\,a$ belong to $\mathcal{I}(A) : h^\infty$. Since $h = \mathsf{init}(a)$ is not a zero divisor modulo $\mathcal{I}(A) : h^\infty$, if $p \in \mathcal{K}[X]$ then $q = 0$. Thus $\mathcal{I}(A \vartriangle a) \cap \mathcal{K}[X] \subset \mathcal{I}(A) : h^\infty$ and the other inclusion is immediate from what precedes.

Intuitively this shows that if $\mathcal{I}(A):h^\infty \neq (1)$, a is not a zero divisor modulo $\mathcal{I}(A):h^\infty$ and therefore the dimension of $\mathcal{I}(A \vartriangle a)$ is one less then the dimension of $\mathcal{I}(A)$. Nonetheless an iterative proof of the dimension properties of the ideal defined by a triangular set is not easy. Conversely, the following fundamental property of the ideal $\mathcal{I}(A)$ allows us to understand better the iterative properties of triangular sets.

THEOREM 4.4. *Let A be a consistent triangular set of $\mathcal{K}[X]$. $\mathcal{I}(A)$ is unmixed dimensional of codimension the cardinal of A. Furthermore $\mathfrak{T}(A)$ forms a transcendence basis for each associated prime of $\mathcal{I}(A)$.*

Proof. Let us note $A = a_1 \vartriangle \ldots \vartriangle a_m$ and let u_i denote the leader of a_i. Each a_i introduces the new variable, u_i. Consider the localization $L_A = I_A^{-1}\mathcal{K}[X]$. We note $I_A^{-1}(A)$ the ideal generated by A in L_A. By the principal ideal theorem [Eis94, Theorem 10.2], $I_A^{-1}(A)$ has at most codimension m. Considered as a univariate polynomial in u_i, a_i has one of its coefficient, its initial, invertible in L_A. By Gauss lemma (Lemma 2.3) a_i can not divide zero modulo $I_A^{-1}(a_1, \ldots, a_{i-1})$. It follows that $a_1, \ldots, a_n$ is a L_A-regular sequence. $I_A^{-1}(A)$ has depth greater or equal to m. As L_A is Cohen-Macaulay $I_A^{-1}(A)$ has codimension m and therefore is unmixed dimensional [Eis94, Proposition 18.14 and 18.9]

As $\mathcal{I}(A) = (I_A^{-1}(A)) \cap \mathcal{K}[X]$, an associated prime of $\mathcal{I}(A)$ is the intersection with $\mathcal{K}[X]$ of an associated prime of $I_A^{-1}(A)$. They all have codimension n and there is no embedded prime [Eis94, Exercise 9.4].

Let P be a minimal prime of $\mathcal{I}(A)$. It contains no initial of the elements of A. Therefore all the elements of $\mathfrak{L}(A)$ are algebraic over $\mathfrak{T}(A)$ modulo P. Considering dimensions, $\mathfrak{T}(A)$ provides a transcendence basis for P.

It follows that $\mathfrak{Jd}(\mathcal{I}(A)) = \mathfrak{Jd}(\mathcal{R}(A))$ and we will simply write $\mathfrak{Jd}(A)$.

PROPOSITION 4.5. *Let A be a consistent triangular set of $\mathcal{K}[X]$ and $x \in X$. Assume P is a minimal prime of $\mathcal{I}(A)$. $P \cap \mathcal{K}[X_{\leq x}]$ is a minimal prime of $\mathcal{I}(A_{\leq x})$.*

Proof. Obviously $\mathcal{I}(A_{\leq x}) \subset \mathcal{I}(A)$ in $\mathcal{K}[X]$. Therefore $\mathcal{I}(A_{\leq x}) \subset \mathcal{I}(A) \cap \mathcal{K}[X_{\leq x}]$ in $\mathcal{K}[X_{\leq x}]$. Let P be a minimal prime of $\mathcal{I}(A)$ in $\mathcal{K}[X]$. $P \cap \mathcal{K}[X_{\leq x}]$ is a prime ideal that contains $\mathcal{I}(A_{\leq x})$. It must contain a minimal prime P' of $\mathcal{I}(A_{\leq x})$. Now $P \cap \mathcal{K}[X_{\leq x}]$ admits $\mathfrak{T}(A) \cap X_{\leq x} = \mathfrak{T}(A_{\leq x})$ as a transcendence basis; It has codimension the cardinal of $\mathfrak{L}(A) \cap X_{\leq x} = \mathfrak{L}(A_{\leq x})$. Theorem 4.4 applies to $A_{\leq x}$ in $\mathcal{K}[X_{\leq x}]$. Thus P and P' have the same dimension. They must be equal.

This property admits generally no converse implication. Some minimal prime of $\mathcal{I}(A_{\leq x})$ are not obtained as the intersection with $\mathcal{K}[X_{\leq x}]$ of a minimal prime of $\mathcal{I}(A)$. Lemma 5.8 gives a sufficient condition for this to happen.

EXAMPLE 4.6. *In $\mathbb{Q}[x, y]$ with $x < y$, consider the triangular set $A = x^2 - 1 \vartriangle (x+1)\,y - 1$. We have $\mathcal{I}(A) = (x-1, 2\,y-1)$ while $\mathcal{I}(A_{\leq x}) = (x-1) \cap (x+1)$.*

4.4 Product of fields associated to a triangular set

The association of a product of fields to a *normalized* triangular set was introduced and used in [Laz91, MM97, Aub99]. This association allows us to define a pseudo-gcd *modulo* a triangular set. Here, to introduce a product of fields we shall use the easy correspondence between positive dimension and dimension zero when dealing with ideals defined by triangular sets.

Let A be a triangular set of $\mathcal{K}[X]$. A can be considered as a triangular set in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$. The ideals will be subscripted by $\mathcal{K}$ or by $\mathcal{K}_A = \mathcal{K}(\mathfrak{T}(A))$ to indicate where they are taken when confusion can arise

By Theorem 4.4 $\mathfrak{T}(A)$ is a transcendence basis of each associated prime of $\mathcal{I}(A)$ so that $\mathcal{I}(A)_{\mathcal{K}_A}$ is a zero dimensional ideal of $\mathcal{K}_A[\mathfrak{L}(A)]$ and $\mathcal{I}(A)_{\mathcal{K}_A} \cap \mathcal{K}[X] = \mathcal{I}(A)_{\mathcal{K}}$. Similarly, $\mathcal{R}(A)_{\mathcal{K}_A}$ is a zero dimensional radical ideal of $\mathcal{K}_A[\mathfrak{L}(A)]$ and $\mathcal{R}(A)_{\mathcal{K}_A} \cap \mathcal{K}[X] = \mathcal{R}(A)_{\mathcal{K}}$. The construction of the product of fields associated to A is then an immediate consequence of the Chinese remainder theorem.

PROPOSITION 4.7. *Let A be a consistent triangular set. The ring $\mathfrak{R}(A) = \mathcal{K}_A[\mathfrak{L}(A)] \,/\, \mathcal{R}(A)_{\mathcal{K}_A}$ is isomorphic to a product of fields.*

Proof. $\mathcal{R}(A)_{\mathcal{K}_A}$ is a zero dimensional radical ideal of $\mathcal{K}_A[\mathfrak{L}(A)]$. Let $P_1, \ldots, P_r$ be the associated primes of $\mathcal{R}(A)_{\mathcal{K}_A}$. They are maximal ideals and therefore the $\mathcal{K}_A[\mathfrak{L}(A)] \,/P_i$ are fields. By application of Theorem 2.4, $\mathcal{K}_A[\mathfrak{L}(A)] \,/\, \mathcal{R}(A)_{\mathcal{K}_A} \cong \mathcal{K}_A[\mathfrak{L}(A)] \,/P_1 \times \ldots \times \mathcal{K}_A[\mathfrak{L}(A)] \,/P_r$.

We shall see that when the triangular set is a regular chain, the product of fields defined is computable in the sense that an element can be tested to be a zero divisor and we can write a splitting algorithm. As we have seen in Section 3.2 we can thus write a pseudo-gcd algorithm over $\mathfrak{R}(A) = \mathcal{K}_A[\mathfrak{L}(A)] \,/\, \mathcal{R}(A)$.

Note that $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)] \,/\, \mathcal{R}(A)$ is equal to its total field of fraction (Proposition 2.5). Therefore $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)] \,/\, \mathcal{R}(A) = \mathfrak{Q}\,(\mathcal{K}[X] \,/\, \mathcal{R}(A))$. For ideals defined by triangular sets, we thus obtain the same product of field as [Aub99]. The benefit of the present presentation is that we control the elements we invert, namely only the elements in $\mathcal{K}[\mathfrak{T}(A)]$.

5 Regular chains and characterizable ideals

Chains are special kinds of triangular set that allow the definition of characteristic set of an ideal. That notion of characteristic set was introduced by J.F. Ritt [Rit30, Rit50]. He defined them as *chains* that are minimal w.r.t. to a certain pre-order. The chains of Ritt are the *autoreduced sets* of Kolchin. The *chains* we define are less restrictive but only slightly.

Characterizable ideals were introduced in [Hub00]. They are ideals that are well defined by their characteristic sets. Ritt and Kolchin made use of the fact that dimension of prime ideals could be read on their characteristic set and that membership to prime ideals could be tested by reduction w.r.t. any of their characteristic set. Characterizable ideals is a wider class of ideals that have those two properties.

Regular chains were introduced by Kalkbrener [Kal93]. It is close to the definition of regular set of [MM97] These definitions were shown to be equivalent in [ALMM99]. The definition we give is equivalent, we only avoid the use of tower of simple extensions.

We show that characterizable ideals are in fact ideals defined by regular chains. Say it otherwise: regular chains are characteristic sets of characterizable ideals. That result appeared in [ALMM99]. Thus, the approach through characteristic sets allows to define characterizable ideals intrinsically while the regular chain approach allow us to construct characterizable ideals.

5.1 Characteristic sets

The ranking on X induces a pre-order[2] on the set of triangular sets of $\mathcal{K}[X]$. Let $A = a_1 \vartriangle \ldots \vartriangle a_r$ and $B = b_1 \vartriangle \ldots \vartriangle b_s$ be triangular sets. A is said to have lower rank than B when there exists k, $0 \leq k \leq r, s$, such that $\mathsf{rank}(a_i) = \mathsf{rank}(b_i)$ for all $1 \leq i \leq k$ and either $k = r < s$ or $\mathsf{rank}(a_k) < \mathsf{rank}(b_k)$. If this is the case, we write $\mathsf{rank}(A) < \mathsf{rank}(B)$.

If $A = B \vartriangle C$ then $\mathsf{rank}(A) < \mathsf{rank}(B)$ reflecting the inclusion of ideals $(B) \subset (A)$. In particular, if B is the empty set and A is not then $\mathsf{rank}(A) < \mathsf{rank}(B)$.

Recall that a relation on a set M is well founded if every non empty subset of M has a minimal element for this relation. This is equivalent to the fact that there is no infinite decreasing sequence in M. See for instance [BW93, Chapter 4].

THEOREM 5.1. *The pre-order on triangular sets is well founded.*

Proof. Assume that the variables are indexed by increasing rank from 1 to n. The rank of a triangular set $A = a_1 \vartriangle \ldots \vartriangle a_r$ can be modeled by an element $(i_1, d_1, \ldots, i_n, d_n)$ of $\mathbb{N}^{2n}$ where, for $j \leq r$ i_j and d_j are respectively index of the leader of a_j and the degree of a_j in its leader while for $j > r$ $i_j = n + 1$ and $d_j = 0$. The pre-order on the triangular set is given by the lexicographic order in $\mathbb{N}^{2n}$ and that latter is well founded.

This property allows us to show termination of algorithms and to show that every ideal admits a characteristic set. But for this purpose we need to consider chains and not simply triangular sets. Indeed one can extend a triangular set included in an ideal to a lower rank one still included in the ideal.

EXAMPLE 5.2. *Consider the ideal $I = (x, y)$ in $\mathbb{Q}[x, y, z]$. $x \vartriangle y$ is a triangular set in I as is $x \vartriangle y \vartriangle xz$ which has lower rank. This latter is nonetheless useless in discriminating I.*

DEFINITION 5.3. *A subset of $\mathcal{K}[X]$ is an* autoreduced set *if any of its element is reduced w.r.t. the others.*

A triangular set A in $\mathcal{K}[X]$ is a chain *if for all $x \in \mathfrak{L}(A)$, the rank of $\mathsf{red}(A_x, A_{<x})$ is equal to the rank of A_x.*

[2] A pre-order is a relation that is reflexive, transitive and connex. The difference with an order is that $a \leq b$ and $b \leq a$ does not imply $a = b$.

An autoreduced set must be a triangular set. The important fact behind the definition of a chain is that to any chain we can associate an autoreduced set B with the same rank. We just take $B = \{\mathsf{red}(A_x, A_{<x}) \mid x \in \mathfrak{L}(A)\}$. Unfortunately the definition of chain above depends on the choice of the pseudo-division algorithm used, as illustrated in the example below. It is nonetheless practical to be able to define characteristic sets of ideals that are not necessarily autoreduced. Autoreduced sets have been replaced by *weak ascending chains* [CG90] or *fine* triangular sets [Wan93], i.e. triangular sets such that $\forall x \in \mathfrak{L}(A)$ $\mathsf{red}(\mathsf{init}(A_x), A_{<x}) \neq 0$, in Wu-Ritt type of triangulation-decomposition algorithm. Nonetheless, it is not always possible to associate an autoreduced set to a fine triangular set while keeping the same rank. It is indeed possible that $\mathsf{red}(\mathsf{init}(A_x), A_{<x}) \neq 0$ but that $\mathsf{red}(A_x, A_{<x})$ does not have the same rank as A_x. We give an example.

Example 5.4. *In $\mathbb{Q}[x, y, z]$ with ranking $x < y < z$ consider*

- *$A = x^2 \vartriangle xy-1 \vartriangle xz+y$. Then $\mathsf{red}(\mathsf{init}(A_z), A_{<z}) = x \neq 0$ but $\mathsf{red}(A_z, A_{<z}) = 1$.*
- *$A = x^2 - x \vartriangle xy - 1 \vartriangle (x-1)z + xy$. If sparse pseudo-division is used then A is a chain as $\mathsf{red}(A_z, A_{<z}) = (x-1)z + 1$. If pseudo-division is used then A is not a chain as $\mathsf{red}(A_z, A_{<z}) = x$.*

Definition 5.5. *Let I be a proper ideal in $\mathcal{K}[X]$. A chain A contained in I is a characteristic set of I if one of the following equivalent conditions holds:*

1. *A is of minimal rank among the chains contained in I.*
2. *there is no non zero element of I reduced w.r.t. A.*
3. *$\forall q \in I,\ \mathsf{red}(q, A) = 0$.*

We shall make explicit the equivalences in the definition.

1. $\Rightarrow$ **2.** Assume that there is a nonzero element p in I reduced w.r.t. A. Let $x = \mathsf{lead}(p)$ and consider $B = A_{<x} \vartriangle p$. B is a chain in I of lower rank than A. This contradicts the hypothesis on A.

2. $\Rightarrow$ **1.** Assume there exists a chain B in I of rank lower than A. We can assume that B is an autoreduced set. Let $A = a_1 \vartriangle \ldots \vartriangle a_s$ and $B = b_1 \vartriangle \ldots \vartriangle b_r$ and k, $0 \leq k \leq r, s$, such that $\mathsf{rank}(b_i) = \mathsf{rank}(a_i)$ for all $i \leq k$ and $\mathsf{rank}(b_{k+1}) < \mathsf{rank}(a_{k+1})$ or $k = s$. As b_k is reduced w.r.t. $b_1 \vartriangle \ldots \vartriangle b_{k-1}$ it is reduced w.r.t. A. That cannot be the case.

2. $\Leftrightarrow$ **3.** is immediate to write down.

From Point 3. in this definition we deduce that if A is a characteristic set of an ideal I of $\mathcal{K}[X]$ then $(A) \subset I \subset (A) : I_A^\infty$. From Point 1. and Theorem 5.1 we deduce that every ideal in $\mathcal{K}[X]$ admits a characteristic set and all the characteristic sets of a given ideal (for a given ranking) have the same rank.

The example below illustrate the fact that a chain A is not obviously a characteristic set of $(A) : I_A^\infty$.

Example 5.6. *In $\mathbb{Q}[x, y]$ endowed with a ranking $x < y$ consider, the chain $A = (x-1)\,y - 1 \vartriangle x^2 - 1$. Note that $(x+1) \in (A) : I_A^\infty$ though it is reduced w.r.t. A.*

5.2 Regular chains

The idea behind the definition of regular chains is that a generic zero of $\mathcal{R}(A_{<x})$ can be extended to a generic zero of $\mathcal{R}(A_{\leq x})$. This is expressed in Proposition 5.8 by the fact that any associated prime of $\mathcal{R}(A_{<x})$ does not disapear as in Example 4.6 but is always the cutback of an associated prime of $\mathcal{R}(A)$.

DEFINITION 5.7. *Let A be a triangular set in $\mathcal{K}[X]$. A is a regular chain if for all $x \in \mathfrak{L}(A)$, $\mathsf{init}(A_x)$ is not a zero divisor modulo $\mathcal{I}(A_{<x})$.*

A regular chain is a chain according to Definition 5.3. Indeed, if $\mathsf{rank}(\mathsf{red}(A_x, A_{<x}))$ were different from $\mathsf{rank}(A_x)$ that would imply that $\mathsf{init}(A_x) \in \mathcal{R}(A_{<x})$. If A is a regular chain, the ideal $\mathcal{I}(A)$ is not trivial and the properties of triangular sets apply. Namely

- $\mathcal{I}(A)$ is unmixed dimensional; it has no embedded prime; its set of primary components is unique.
- $\mathfrak{T}(A)$ is a transcendence basis of each associated prime of $\mathcal{I}(A)$.
- $\mathfrak{Zd}(\mathcal{I}(A)) = \mathfrak{Zd}(\mathcal{R}(A))$ and we write $\mathfrak{Zd}(A)$.

Furthermore, by Lemma 4.3, if $A \vartriangle a$ is a regular chain in $\mathcal{K}[X]$ then $(\mathcal{I}(A)+(a)) : h^\infty = \mathcal{I}(A \vartriangle a)$.

PROPOSITION 5.8. *Let C be a regular chain in $\mathcal{K}[X]$ and $x \in X$. $C_{\leq x}$ is a regular chain in $\mathcal{K}[X_{\leq x}]$ and*

- $\mathcal{I}(C) \cap \mathcal{K}[X_{\leq x}] = \mathcal{I}(C_{\leq x})$
- *the associated primes of $\mathcal{I}(C_{\leq x})$ are the intersections with $\mathcal{K}[X_{\leq x}]$ of the associated primes of $\mathcal{I}(C)$.*

Proof. The first point is an immediate consequence of Proposition 4.3 since $\mathsf{init}(C_x) \notin \mathfrak{Zd}(\mathcal{I}(C_{\leq x}))$. Together with Theorem 4.5, we can thus say that the set of the minimal primes of $\mathcal{I}(C_{\leq x})$ in $\mathcal{K}[X_{\leq x}]$ is equal to the set of the intersections with $\mathcal{K}[X_{\leq x}]$ of the minimal primes of $\mathcal{I}(C)$.

That implies that an element $p \in \mathcal{K}[X_{\leq x}]$ belongs to $\mathfrak{Zd}(C)$ if and only if $p \in \mathfrak{Zd}(C_{\leq x})$. We can choose $q \in \mathcal{K}[X_{\leq x}]$ s.t. $p\,q \in \mathcal{I}(C)$. With this property we can write without confusion, for any regular chain C, $\mathfrak{Zd}(C_{\leq x})$ to mean $\mathfrak{Zd}(C_{\leq x})$ or $\mathfrak{Zd}(C) \cap \mathcal{K}[X_{\leq x}]$ since these two sets are equal in $\mathcal{K}[X_{\leq x}]$ and can be extended to $\mathcal{K}[X]$. Note nonetheless that two different minimal primes of $\mathcal{I}(C)$ can have the same intersection with $\mathcal{K}[X_{\leq x}]$.

EXAMPLE 5.9. *In $\mathbb{Q}[x, y]$ where $x < y$ consider the triangular set $A = x \vartriangle y^2 - 1$. We have $\mathcal{R}(A) = \langle x, y-1 \rangle \cap \langle x, y+1 \rangle$. Both the minimal primes contract to $\langle x \rangle$ on $\mathcal{K}[x]$.*

5.3 Characterizable ideals

Ritt and Kolchin made high use of the fact that if A is a characteristic set of a prime ideal P then $P = (A) : I_A^\infty$ and therefore $p \in P \Leftrightarrow \mathsf{red}(p, A) = 0$. We introduce the very useful wider class of ideals having this property. We give an intrinsic definition and an explicit construction of those ideals.

Definition 5.10. *An ideal I of $\mathcal{K}[X]$ is characterizable if for a characteristic set A of I we have $I = (A) : I_A^\infty$. A is said to characterize I.*

Note that if I is a characterizable ideal characterized by A then $p \in I \Leftrightarrow \mathsf{red}(p, A) = 0$. Prime ideals are characterizable for any ranking but not all primary ideals are characterizable as illustrated in Example 5.11. Characterizable ideals that are not prime do exist but that depends then on the ranking (see Example 5.12). From Theorem 4.4 we see that characterizable ideals have specific dimension properties. A natural question would be to determine if an ideal given by its generators is characterisable. An answer in terms of Gröbner basis is given in [Hub00] for zero dimensional ideals and extended in [CH01] to ideals of positive dimension.

Example 5.11. *In $\mathbb{Q}[x, y]$ consider the primary ideal $I = (x^2, x\,y, y^2)$. The generators given here form a reduced Gröbner basis for the lexicographical term ordering $x < y$. Thus a chain of minimal rank in I according to a ranking $x < y$ is given by $A = x^2 \vartriangle x\,y$. A is thus a characteristic set of I but note that $(A) : I_A^\infty = (1) \neq I$. I is not characterizable.*

Example 5.12. *Consider $I = (y^3 - y, 2\,x - y^2 + 2)$ in $\mathbb{Q}[x, y]$. The generators of I given above form a reduced Gröbner basis G for the lexicographical term order where $y < x$. G is also an autoreduced set and therefore it is a characteristic set of I for the ranking $y < x$. We have $I = (G) = (G) : I_G^\infty$ and thus I is characterizable for the ranking $y < x$.*

The Gröbner basis of I for the lexicographical order $x < y$ is $G' = \{2\,x^2 + 3\,x + 1, 2\,x\,y + y, y^2 - 2\,x - 2\}$. Therefore $A = 2\,x^2 + 3\,x + 1 \vartriangle 2\,x\,y + y$ is a characteristic set of I for the ranking $x < y$. We can check that $I \neq (A) : I_A^\infty$ so that I is not characterizable for the ranking $x < y$.

The following equivalence was proved in [ALMM99, Theorem 6.1] but a related result appears in [Kol73, Lemma 13, Section 0.14]. It shows that characterizable ideals are in fact ideals defined by regular chains.

Theorem 5.13. *Let A be a chain in $\mathcal{K}[X]$. A is consistent and A is a characteristic set of $(A) : I_A^\infty$ if and only if A is a regular chain.*

Proof. We first show by induction that if A is a regular chain then $\mathcal{I}(A)$ contains no nonzero element reduced w.r.t. A. This is true for the empty chain which is the only chain of $\mathcal{K}$. Assume this hypothesis is true for all the regular chains of $\mathcal{K}[X]$. Let A be a regular chain of $\mathcal{K}[X][x]$. $A_{<x}$ is a regular chain of $\mathcal{K}[X]$ and $\mathcal{I}(A) \cap \mathcal{K}[X] = \mathcal{I}(A_{<x})$ (Lemma 5.8).

Let $p \in \mathcal{K}[X][x]$ belong to $\mathcal{I}(A)$ and be reduced w.r.t A. We can assume further that $\deg(p,x) > 0$, since otherwise $p \in \mathcal{I}(A) \Leftrightarrow p \in \mathcal{I}(A_{<x})$. If $x \notin \mathfrak{L}(A)$, the coefficients of p being considered as a polynomial in x must belong to $\mathcal{I}(A_{<x})$; they are also reduced w.r.t. $A_{<x}$ and therefore must be zero by induction hypothesis; p is equal to zero. Assume now $x \in \mathfrak{L}(A)$. Since $\mathcal{I}(A) = (\mathcal{I}(A_{<x}), A_x) : \mathsf{init}(A_x)$ there exists $h \in \mathsf{init}(A_x)^\infty$ and $q \in \mathcal{K}[X]$ such that $h\,p \equiv q\,A_x \mod \mathcal{I}(A_{<x})$. If q were non zero, the degree in x of p would be greater or equal to the one of A_x, contradicting thus the hypothesis that p is reduced w.r.t. A. It must be that $q = 0$; therefore p belongs to $\mathcal{I}(A_{<x}) : h^\infty = \mathcal{I}(A_{<x})$ and therefore its coefficients when considered as a polynomials in x belong to $\mathcal{I}(A_{<x})$. The coefficients being reduced w.r.t $A_{<x}$, they must be zero by induction hypothesis. We have thus proved that if A is a regular chain, $1 \notin (A) : I_A^\infty$ and A is a characteristic set of $\mathcal{I}(A)$.

Assume now A is not a regular chain. We shall prove that it is not a characteristic set of $\mathcal{I}(A)$. There exists $x \in X$ such that $\mathsf{init}(A_x) \in \mathfrak{Z}\mathfrak{d}(A_{<x})$. Select the smallest such x. $A_{<x}$ is a regular chain so that it is a characteristic set of $\mathcal{I}(A_{<x})$ by the first part of the proof. There exists $q \in \mathcal{K}[X_{<x}]$, $q \notin \mathcal{I}(A_{<x})$ such that $q\,\mathsf{init}(A_x) \in \mathcal{I}(A_{<x})$. Let $r = \mathsf{red}(q, A_{<x})$; r is nonzero since $q \notin \mathcal{I}(A_{<x})$ and $A_{<x}$ is a characteristic set of this ideal. We have $r\,\mathsf{init}(A_x) \in \mathcal{I}(A_{<x})$ and therefore $r \in \mathcal{I}(A)$, while r is reduced w.r.t. A. Thus either $1 \in (A) : I_A^\infty$ or A is not a characteristic set of $\mathcal{I}(A)$.

Assume A is a regular chain in $\mathcal{K}[X]$. Playing with definitions and Theorem 5.13, we have:

- $\mathcal{I}(A)$ is a characterizable ideal characterized by A
- $p \in \mathcal{I}(A) \Leftrightarrow \mathsf{red}(p, A) = 0$.

We shall show now that the definition of characterizable differential ideals is independent of the characteristic set chosen in Definition 5.10.

Proposition 5.14. *Let I be a characterizable ideal. Any characteristic set of I characterizes I.*

Proof. Note first that if A is a characteristic set of an ideal I in $\mathcal{K}[X]$ then $A_{<x}$ is a characteristic set of $I \cap \mathcal{K}[X_{<x}]$ for any $x \in X$. We prove the proposition by induction on X.

In $\mathcal{K}$, (0) is the only characterizable ideal and the only chain is the empty set. Assume the proposition is true in $\mathcal{K}[X]$. Let I be a characterizable ideal in $\mathcal{K}[X][x]$: there exists a regular chain C such that $I = \mathcal{I}(C)$. Then $C_{<x}$ is a regular chain and a characteristic set of $\mathcal{I}(C_{<x})$ in $\mathcal{K}[X]$. Let A be another characteristic set of I; A and C have the same rank. $A_{<x}$ is a characteristic set of $I \cap \mathcal{K}[X] = \mathcal{I}(C_{<x})$. By induction hypothesis, $A_{<x}$ is a regular chain characterizing $I \cap \mathcal{K}[X]$. Thus $I \cap \mathcal{K}[X] = \mathcal{I}(A_{<x}) = \mathcal{I}(C_{<x})$.

We shall show that A is a regular chain. If $x \notin \mathfrak{L}(A)$ then $I = \mathcal{I}(C_{<x})$ and the result comes from the induction hypothesis. Assume now $x \in \mathfrak{L}(A)$. Since $A_x \in I = (\mathcal{I}(C_{<x}), C_x) : \mathsf{init}(C_x)^\infty$, there exists $h \in \mathsf{init}(C_x)^\infty$ such that

$h\,A_x \equiv q\,C_x \mod \mathcal{I}(C_{<x})$, where $q \in \mathcal{K}$ since the degrees in x of A_x and C_x are equal. If $q = 0$ then $A_x \in \mathcal{I}(C_{<x}) : h^\infty = \mathcal{I}(C_{<x}) = I \cap \mathcal{K}[X]$: the coefficients of A_x all belong to $I \cap \mathcal{K}[X]$ and therefore are reduced to zero by $A_{<x}$ which is a characteristic set of $I \cap \mathcal{K}[X]$. This contradicts the fact that A is a chain. Thus $q \in \mathcal{K} \setminus \{0\}$. Equating the leading coefficients on both side of the pseudo-division relationship, we have that $h\,\mathsf{init}(A_x) \equiv q\,\mathsf{init}(C_x) \mod \mathcal{I}(C_{<x})$. Thus $\mathsf{init}(A_x)$ cannot divide zero modulo $\mathcal{I}(C_{<x})$. Since $\mathcal{I}(A_{<x}) = \mathcal{I}(C_{<x})$, A is a regular chain.

Furthermore, A being a characteristic set of I we have $A \subset \mathcal{I}(C) \subset \mathcal{I}(A)$ and thus $\mathcal{I}(A) = \mathcal{I}(C) : I_A^\infty = \mathcal{I}(C)$ since $I_{A_{<x}}$ and $\mathsf{init}(A_x)$ are not zero divisor of $\mathcal{I}(C)$.

5.4 Canonical representatives of characterizable ideals

We shall exhibit canonical representatives of characterizable ideals. These canonical representatives are taken in what we call Gröbner chains. They appear as *p-chain* in [GC92] for their relevance in deciding for which parameters there is a (regular) zero. In [BL00], where they are called *strongly normalized triangular sets*, they serve the purpose of computing normal forms of (differential) polynomials modulo a (differential) characterizable ideal. The name owes to Proposition 5.16 that makes the link between the characteristic set approach to represent ideals and the Gröbner bases approach.

Definition 5.15. *A triangular set A such that $\forall x \in \mathfrak{L}(A)$, $\mathsf{init}(A_x) \in \mathcal{K}[\mathfrak{T}(A)]$ is a* Gröbner chain. *A Gröbner chain is* reduced *if it is an autoreduced set such that none of its element has factors in $\mathcal{K}[\mathfrak{T}(A)]$.*

Theorem 4.4 shows that, for a triangular set A in $\mathcal{K}[X]$, $\mathcal{K}[\mathfrak{T}(A)]$ contains no zero divisor modulo $\mathcal{I}(A)$. Therefore a Gröbner chain is a regular chain.

Proposition 5.16. *A (reduced) Gröbner chain A in $\mathcal{K}[X]$ is a (reduced) Gröbner basis in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$ according to the lexicographical term order on $\mathfrak{L}(A)$ induced by the ranking on X.*

Proof. The leading terms have no common divisors. According to the first Buchberger criterion the S-polynomials are reduced to zero.

Proposition 5.17. *Every characterizable ideal in $\mathcal{K}[X]$ admits a (unique) characteristic set that is a (reduced) Gröbner chain.*

Proof. Let I be a characterizable ideal. There exists A, a regular chain, such that $I = \mathcal{I}(A)$. For all $y \in \mathfrak{L}(A)$ we define q_y and r_y as follow. If $\mathsf{init}(A_y) \in \mathcal{K}[\mathfrak{T}(A)]$ then $q_y = 1$ and $r_y = 0$. Otherwise since $\mathcal{I}(A_{<y})_{\mathcal{K}_{A_{<y}}}$ is a zero dimensional ideal in $\mathcal{K}(A_{<y})[\mathfrak{L}(A_{<y})]$ and $\mathsf{init}(A_y) \notin \mathfrak{Zd}(A_{<y})$ there exists $q_y \in \mathcal{K}[X_{<y}]$ and $u_y \in \mathcal{K}[\mathfrak{T}(A_{<y})]$ such that $q_y\,\mathsf{init}(A_y) = u_y + r_y$ where $r_y \in \mathcal{I}(A_{<y})$. Let $C = \Delta_{y\in\mathfrak{L}(A)}(q_y\,A_y - r_y\,\mathsf{init}(A_y)\,\mathsf{rank}(A_y))$. C is a Groebner chain. It characterizes I as $C \subset I$ and $\mathsf{rank}(C) = \mathsf{rank}(A)$.

The uniqueness of the second point owes to the canonical properties of reduced and minimal Gröbner bases.

Given a regular chain A it is possible to compute the canonical Gröbner chain of the characterizable ideal defined. First, one can think of making the proof constructive by a generalization of the extended Euclidean algorithm [GC92, MM97, BL00]. The algorithm of [MM97, BL00] might require nonetheless to split the ideal[3]. Alternatively, we can use Buchberger algorithm. Indeed the desired Gröbner chain is the Gröbner basis of (A) in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$ w.r.t. the lexicographical term order induced by the ranking on $\mathfrak{L}(A)$. This works thanks to the following proposition derived from [Aub99].

Proposition 5.18. *If A is a regular chain then the ideal $(A) : I_A^\infty$ is equal to the ideal (A) in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$.*

Proof. Assume $A = a_1 \vartriangle \ldots \vartriangle a_r$ and note $y_1, \ldots, y_r$ the leaders of $a_1, \ldots, a_r$. The proof works by induction. $\mathsf{init}(a_1) \in \mathcal{K}_A$ so that $(a_1) : \mathsf{init}(a_1)^\infty = (a_1)$. Assume that $\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k) = (a_1, \ldots, a_k)$.

Since $\mathsf{init}(a_k) \notin \mathfrak{Z}\mathfrak{d}(a_1 \vartriangle \ldots \vartriangle a_k)$ and $\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k)$ is a zero dimensional ideal in $\mathcal{K}_A[y_1, \ldots, y_k]$ there exists $q \in \mathcal{K}_A[y_1, \ldots, y_k]$ such that $q\,\mathsf{init}(a_{k+1}) \equiv 1 \mod \mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k)$. If p belongs to $\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_{k+1})$ that is equal to $(\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k) + (a_{k+1})) : \mathsf{init}(a_{k+1})^\infty$ then there exists $e \in \mathbb{N}$ s.t. $\mathsf{init}(a_{k+1})^e p \in (\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k) + (a_{k+1}))$. Premultiplying by q^e we obtain that $p \in (\mathcal{I}(a_1 \vartriangle \ldots \vartriangle a_k) + (a_{k+1}))$ so that by induction hypothesis $p \in (a_1, \ldots, a_{k+1})$.

The latter proposition entails that if a polynomial p does not belong to $\mathfrak{Z}\mathfrak{d}(A)$, where A is a regular chain, then p is a unit modulo (A) in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$ and therefore (A, p) contains an element in $\mathcal{K}[\mathfrak{T}(A)]$. Those properties are in fact definitions for a polynomial to be *invertible w.r.t. A* in [MKRS98, BKRM01].

6 Decomposition into characterizable ideals

In Section 9 we shall see that we can compute for any finite set of polynomials a decomposition of the radical of the ideal generated by these polynomials into characterizable ideals. This provides a membership test to this radical ideal. It also provides a *strongly* unmixed dimensional decomposition. We define here characteristic decomposition and make the link to decomposition of product of fields.

Let $J, J_1, \ldots, J_r$ be radical ideals such that the equality $J = J_1 \cap \ldots \cap J_r$ holds. This equality defines a decomposition of J and the J_i are called the component of J (in this decomposition). The decomposition is *irredundant* if the sets of prime components of the J_i gives a partition of the set of prime components of J. In other words, if P is a minimal prime of J, there exists a unique i such that $J_i \subset P$.

The following proposition is then trivial but useful.

Proposition 6.1. *Let J be a radical ideal in $\mathcal{K}[X]$. If $J = J_1 \cap \ldots \cap J_r$ is an irredundant decomposition then $\mathfrak{Z}\mathfrak{d}(J) = \mathfrak{Z}\mathfrak{d}(J_1) \cup \ldots \cup \mathfrak{Z}\mathfrak{d}(J_r)$.*

[3] Personal communication of F. Lemaire

Definition 6.2. *Let J be a non trivial radical ideal in $\mathcal{K}[X]$. A set of regular chains $\mathcal{C} = \{C_1, \ldots, C_r\}$ defines a characteristic decomposition of J if*

$$\sqrt{I} = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r) \text{ i.e. } \sqrt{I} = \langle C_1 \rangle : I_{C_1}^{\infty} \cap \ldots \cap \langle C_r \rangle : I_{C_r}^{\infty}.$$

We take as convention that the empty set is a characteristic decomposition of $J = \mathcal{K}[X]$.

Proposition 6.3. *Let A be a consistent triangular set of $\mathcal{K}[X]$. If $\mathcal{R}(A) = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r)$ is an irredundant characteristic decomposition then $\mathfrak{L}(A) = \mathfrak{L}(C_1) = \ldots = \mathfrak{L}(C_r)$.*

Proof. By Theorem 4.4, $\mathfrak{T}(A)$ is a basis of transcendence of all the associated prime of $\mathcal{R}(A)$ and thus of all the associated primes of $(C_i) : I_{C_i}^{\infty}$ while, for $1 \leq i \leq r$, $\mathfrak{T}(C_i)$ is a basis of transcendence of the associated primes of $(C_i) : I_{C_i}^{\infty}$. Thus $\mathfrak{T}(A)$ and $\mathfrak{T}(C_i)$ have the same cardinal and it is sufficient to prove that $\mathfrak{L}(A) \subset \mathfrak{L}(C)$. For $1 \leq i \leq r$, no element of I_A is a zero divisor of $(C_1) : I_{C_1}^{\infty}$. Assume there exists $x \in \mathfrak{L}(A)$ such that $x \notin \mathfrak{L}(C_i)$. Then $\{A_x\} \cup C_i$ is a regular chain lower then C_i in $(C_i) : I_{C_i}^{\infty}$. This contradicts the fact that C_i is a characteristic set of $(C_i) : I_{C_i}^{\infty}$. The conclusion follows: $\mathfrak{L}(A) \subset \mathfrak{L}(C)$.

The same way we can consider A as a triangular set in $\mathcal{K}_A[\mathfrak{L}(A)]$ we can also consider the C_i as regular chains in $\mathcal{K}_A[\mathfrak{L}(A)]$. An irredundant decomposition of $\mathcal{R}(A)$ provides in fact a decomposition of the product of fields associated to A. Recall we defined $\mathfrak{R}(A) = \mathcal{K}_A[\mathfrak{L}(A)]/\mathcal{R}(A)$ which is equal to $\mathfrak{Q}\left(\mathcal{K}[X]/\mathcal{R}(A)\right)$.

Proposition 6.4. *Let A be a consistent triangular set of $\mathcal{K}[X]$. Assume $\mathcal{R}(A) = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r)$ is an irredundant characteristic decomposition in $\mathcal{K}[X]$. Then $\mathcal{R}(A)_{\mathcal{K}_A} = \mathcal{R}(C_1)_{\mathcal{K}_A} \cap \ldots \cap \mathcal{R}(C_r)_{\mathcal{K}_A}$ is an irredundant characteristic decomposition in $\mathcal{K}_A[\mathfrak{L}(A)]$ and $\mathfrak{R}(A) \cong \mathfrak{R}(C_1) \times \ldots \times \mathfrak{R}(C_r)$.*

Proof. We have $\mathfrak{L}(A) = \mathfrak{L}(C_1) = \ldots = \mathfrak{L}(C_r)$. Thus $A, C_1, \ldots, C_r$ can be considered as triangular sets in $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$ and we overline them when we consider them as such. Let $\bar{P}$ be an associated prime of $\mathcal{R}(\bar{A})_{\mathcal{K}_A}$. If $\bar{P}$ contained $\mathcal{R}(\bar{C}_i)$ and $\mathcal{R}(\bar{C}_j)$ for $i \neq j$ then $\bar{P} \cap \mathcal{K}[X]$ would contain $\mathcal{R}(\bar{C}_i) \cap \mathcal{K}[X] = \mathcal{R}(C_i)$ and $\mathcal{R}(\bar{C}_j) \cap \mathcal{K}[X] = \mathcal{R}(C_j)$. Since $\bar{P} \cap \mathcal{K}[X]$ is a prime component of $\mathcal{R}(A)$ and the decomposition $\mathcal{R}(A) = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r)$ is irredundant this is not possible. Therefore $\mathcal{R}(\bar{A}) = \mathcal{R}(\bar{C}_1) \cap \ldots \cap \mathcal{R}(\bar{C}_r)$ is irredundant.

The radical ideals $\mathcal{R}(\bar{C}_i)_{\mathcal{K}_A}$ are zero dimensional and have no prime divisor in common. They are thus comaximal: $\mathcal{R}(\bar{C}_i) + \mathcal{R}(\bar{C}_j) = \mathcal{K}_A[\mathfrak{L}(A)]$. By the Chinese remainder theorem (Theorem 2.4) we have that

$$\mathcal{K}_A[\mathfrak{L}(A)]/\mathcal{R}(\bar{A}) \cong \mathcal{K}_A[\mathfrak{L}(A)]/\mathcal{R}(\bar{C}_1) \times \ldots \times \mathcal{K}_A[\mathfrak{L}(A)]/\mathcal{R}(\bar{C}_r)$$

The converse property is in fact also true. If $\mathcal{R}(\bar{A}) = \mathcal{R}(\bar{C}_1) \cap \ldots \cap \mathcal{R}(\bar{C}_r)$ is an irredundant characteristic decomposition in $\mathcal{K}_A[\mathfrak{L}(A)]$ then it can be *lifted* to the irredundant characteristic decomposition $\mathcal{R}(A) = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r)$ in $\mathcal{K}[X]$ where a C_i is obtained from $\bar{C}_i$ by cleaning the denominators and the factors in $\mathcal{K}[\mathfrak{T}(A)]$ (see [Hub00]).

7 Radical ideals defined by triangular sets

In this section, we generalize to triangular sets the following properties for $p \in \mathcal{K}[x]$:

- $q = \frac{p}{\gcd(p, \frac{\partial p}{\partial x})}$ is squarefree and $\sqrt{(p)} = (q)$ (Theorem 7.1).
- p is squarefree iff $\gcd(p, \frac{\partial p}{\partial x}) = 1$ (Corollary 7.3).
- $(p) : (\frac{\partial p}{\partial x})^\infty$ is radical (Theorem 7.5).

Some of these results can be found in [Laz91, BLOP95, BLOP97, SL98, Mor99, Del99, Aub99, Hub00]. They can be proved by applying the Jacobian criterion for regularity (see [Eis94, Chapter 16] and [Vas98, Chapter 5]).

Let p be an element of $\mathcal{K}[X]$. The *separant* of p is the derivative of p w.r.t. its leader: $\mathsf{sep}(p) = \frac{\partial p}{\partial \mathsf{lead}(p)}$. Thus if $x = \mathsf{lead}(p)$ and we can write $p = a_d x^d + \ldots + a_1 x + a_0$ then $\mathsf{sep}(p) = d a_d x^{d-1} + \ldots + a_1$. For a triangular set A in $\mathcal{K}[X]$ we denote S_A the set formed up by the separants of the elements of A and H_A the set of the initials and separants of the elements of A.

Theorem 7.1. *Let A be a triangular set in $\mathcal{K}[X]$. Let s be the product of the separants of the elements of A. $\mathcal{R}(A) = \mathcal{I}(A) : s$. In other words $\sqrt{(A) : I_A^\infty} = \{p \in \mathcal{K}[X] \mid s\, p \in (A) : I_A^\infty\}$.*

Proof. As seen in Theorem 4.4, $\mathcal{I}(A)$ and $\mathcal{R}(A)$ have no zero divisor in $\mathcal{K}[\mathfrak{T}(A)]$. It follows that $\mathcal{I}(A)_{\mathcal{K}} = \mathcal{I}(A)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ and $\mathcal{R}(A)_{\mathcal{K}} = \mathcal{R}(A)_{\mathcal{K}_A} \cap \mathcal{K}[X]$.

Consider A as a triangular set of $\mathcal{K}_A[\mathfrak{L}(A)]$. The Jacobian ideal of (A) is generated by s. By [Vas98, Theorem 5.4.2.], $(A)_{\mathcal{K}_A} : s = \sqrt{(A)}_{\mathcal{K}_A}$. Thus $\mathcal{I}(A)_{\mathcal{K}_A} : s = \mathcal{R}(A)_{\mathcal{K}_A}$. Taking the intersection with $\mathcal{K}[X]$ we have the equality announced.

This gives us a way to construct $\mathcal{R}(A)$ that will be used in Section 9. It also gives a criterion for $\mathcal{I}(A)$ to be radical: $\mathcal{I}(A)$ is radical if and only if no separant of the elements of A is a zero divisor modulo $\mathcal{I}(A)$. This criterion motivates the following definition and gives the corollary after it.

Definition 7.2. *A regular chain C in $\mathcal{K}[X]$ is squarefree if $S_C \cap \mathfrak{Zd}(C) = \emptyset$ i.e. no separant of C is a zero divisor modulo $\mathcal{I}(C)$.*

Corollary 7.3. *If C is a regular chain of $\mathcal{K}[X]$ then $(C) : I_C^\infty$ is radical if and only if C is squarefree.*

Note nonetheless that the radical of a characterizable ideal is not always characterizable. The example below is taken from [Aub99, Section 4.5].

Example 7.4. *In $\mathcal{K}[x, y]$ consider $A = x^2 - x \,\triangle\, y^2 - x$. A is a regular chain of $\mathcal{K}[x, y]$. We have $\mathcal{I}(A) = (A)$. A Gröbner basis of $\mathcal{R}(A) = \sqrt{(A)}$ for a lexicographical term oder satisfying $x < y$ is given by $G = \{x^2 - x, (x-1)\, y, y^2 - x\}$. We can extract from it the characteristic set $B = x^2 - x \,\triangle\, (x-1)\, y$ of $\mathcal{R}(A)$. It is not a regular chain. Thus $\mathcal{R}(A)$ is not characterizable.*

The following theorem is central in constructive differential algebra. It was first enunciated in [BLOP95] and named there after one of the coauthors, D. Lazard. The second part of the statement appeared already in [Kol73]. It shows that we have similar dimension properties whether we saturate by the initials or by the separants.

Theorem 7.5. *Let A be a triangular set of $\mathcal{K}[X]$. $(A):S_A^\infty$ is a radical ideal. If it is non trivial, $(A):S_A^\infty$ is unmixed dimensional and $\mathfrak{L}(A)$ is the set of leaders of the characteristic set of any associated prime of $(A):S_A^\infty$.*

Proof. The principal ideal theorem [Eis94, Theorem 10.2] implies that no associated prime of (A) has codimension bigger than $\mathrm{card}(A)$. The product s of the separants of A is a maximal minor of the Jacobian matrix $\frac{\partial A}{\partial X}$. Let P be a prime ideal that does not contain s. The rank of the Jacobian matrix modulo P is maximal and equal to $\mathrm{card}(A)$. By [Eis94, Theorem 16.9] the localization of $\mathcal{K}[X]/(A)$ at P is an integral ring and the codimension of $(A)_P$ is $\mathrm{card}(A)$. Thus P contains a single primary component of (A) and that component is prime and of codimension $\mathrm{card}(A)$.

$(A):S_A^\infty$ is the intersection of the primary components of (A) the radical of which does not contain s. From what precedes, these components have to be prime and of codimension $\mathrm{card}(A)$. Therefore $(A):S_A^\infty$ is the intersection of prime ideals and so is radical.

We are left to show that $\mathfrak{L}(A) \subset \mathfrak{L}(C)$ for any characteristic set C of P. For any $x \in \mathfrak{L}(A)$, $\mathsf{sep}(A_x) \notin P$. Thus one of the coefficients of a positive power of x in A_x does not belong to P. As any characteristic set of P must reduce A_x to zero, it must contain an element with leader x.

The theorem and its corollary is obviously true if we replace S_A by any set H that contains S_A. The case $H = H_A$ is of special use in differential algebra (see [Hub02]). The relationship between $(A):I_A^\infty$, $(A):S_A^\infty$ and $(A):H_A^\infty$ for regular chains is made explicit below.

Proposition 7.6. *If A is a regular chain in $\mathcal{K}[X]$ then $(A):H_A^\infty = (A):S_A^\infty$. If A is a squarefree regular chain then $(A):I_A^\infty = (A):S_A^\infty$.*

Proof. Assume A is a regular chain and $a \in A$. In $\mathcal{K}(\mathfrak{T}(A))[\mathfrak{L}(A)]$, $(A) = (A):I_A^\infty$ (Proposition 5.18). Any prime ideal of $\mathcal{K}[X]$ that contains A and $\mathsf{init}(a)$, for some $a \in A$, must contain an element in $\mathcal{K}[\mathfrak{T}(A)]$. This is the case of no associated prime of $(A):S_A^\infty$. Thus $\mathsf{init}(a)$ is not a zero divisor of $(A):S_A^\infty$ and the equality of ideals $(A):H_A^\infty = (A):S_A^\infty$ follows. If A is a squarefree regular chain we furthermore have that $(A):I_A^\infty = (A):H_A^\infty$.

8 Kalkbrener's pseudo-gcd and splitting algorithm

In Section 3.2 we saw that computing a pgcd over $\mathcal{K}[\lambda]/\langle c\rangle$ relied on a splitting algorithm for $\mathcal{K}[\lambda]/\langle c\rangle$. In Section 2.4 we saw how to write the splitting algorithm for $\mathcal{K}[\lambda]/\langle c\rangle$ in terms of a gcd over $\mathcal{K}$. We shall show how to generalize this process to compute a pgcd over the product of fields $\mathfrak{R}(C) = \mathfrak{Q}\left(\mathcal{K}[X]/\mathcal{R}(C)\right) = \mathcal{K}_C[\mathfrak{L}(C)]/\mathcal{R}(C)$ associated to a regular chain C.

The algorithms are presented in [Kal93, Kal98] in a very synthetic and highly recursive way. Improvements in view of an efficient implementation are presented in [Aub99]. The present presentation owes to the presentation of Aubry: the recursive calls are limited so that one sees better where the work is done. We shall give complete proofs that lead to a sharper description of the outputs.

The two procedures we shall describe, pgcd and split, work in interaction and recursively. Basically, $\mathsf{pgcd}(\mathcal{K}[X][x], *, *)$ calls $\mathsf{split}(\mathcal{K}[X], *, *)$ which in turn calls $\mathsf{pgcd}(\mathcal{K}[X], *, *)$.

The input of split consist of a regular chain C and a polynomial f. It then returns a pair of set $(\mathcal{Z},\mathcal{U})$ s.t. $\mathcal{R}(C) = \bigcap_{A\in\mathcal{Z}\cup\mathcal{U}} \mathcal{R}(A)$ is an irredundant characteristic decomposition and $f \in \mathcal{I}(A)$, $\forall A \in \mathcal{Z}$ while $f \notin \mathfrak{Z}\mathfrak{d}(A)$, $\forall A \in \mathcal{U}$. We thus have a splitting $\mathfrak{R}(C) \cong \mathfrak{R}_{\mathcal{Z}} \times \mathfrak{R}_{\mathcal{U}}$ where $\mathfrak{R}_{\mathcal{Z}} = \prod_{A\in\mathcal{Z}} \mathfrak{R}(A)$ and $\mathfrak{R}_{\mathcal{U}} = \prod_{A\in\mathcal{U}} \mathfrak{R}(A)$ so that the projection of f on $\mathfrak{R}_{\mathcal{Z}}$ is zero while the projection of f on $\mathfrak{R}_{\mathcal{U}}$ is a unit.

As for pgcd, it computes a pseudo-gcd over some product of field $\mathfrak{R}(C)$ defined by a regular chain. The pgcd computed has additional properties. In fact the output description of these algorithms are sharper in this paper than in [Kal93]. This nicely avoids extraneous complications in the proofs and the application to characteristic decomposition. We shall also make explicit that no redundancy nor multiplicities are introduced in the computations. If we start with a squarefree regular chain, the output regular chains will all be squarefree. Also, it may happen that the output consists of squarefree regular chains even if the input regular chain is not squarefree.

Termination and correctness: One will easily check that if $X = \emptyset$, $\mathsf{split}(\mathcal{K}, \emptyset, f)$ decides if $f = 0$ or not and $\mathsf{pgcd}(\mathcal{K}[x], \emptyset, F)$ computes the gcd of (F) over $\mathcal{K}$. The proof of pgcd and split is inductive. Assuming that $\mathsf{pgcd}(\mathcal{K}[X_{\leq y}], *, *)$ is correct and terminates, for all $y \in X$, we shall prove that $\mathsf{split}(\mathcal{K}[X], *, *)$ is correct. Assuming that $\mathsf{split}(\mathcal{K}[X], *, *)$ is correct, we shall prove that $\mathsf{pgcd}(\mathcal{K}[X][x], *, *)$ is correct.

An intermediate algorithm $\mathsf{relatively\text{-}prime}$, that is a direct application of pgcd, generalizes the recursion presented at the end of Section 2.4 in the case c is not squarefree. It is used in the splitting algorithm split.

Conventions: We shall describe accurately the output of the algorithms and their properties. Correctness of the algorithms and their outputs will be proved by exhibiting invariants for the loops of the algorithms. These invariants are also useful to understand what goes on in the algorithm. We shall need to name precisely one property of the output of an algorithm. For that purpose we number the output properties. We will refer to the i^{th} property of the output of an algorithm, say pgcd, by $\mathsf{pgcd.i}$.

The algorithms are described in Maple style but we use parentheses to denote ordered tuples. We make use of sets $\mathcal{S}$ to stack the data awaiting more computations. The command pop chooses one of those, removes it from the set and returns it. The set $\mathcal{C}$, $\mathcal{U}$, $\mathcal{Z}$ contains the data for which computation is completed.

8.1 Pseudo-gcd algorithm

This algorithm is no different than the one given in Section 3.2 only more specific. The product of fields are replaced by regular chains defining them and we use a more specific output of the splitting algorithm.

ALGORITHM 8.1. **pgcd**
INPUT:

- $\mathcal{K}[X][x]$ *a ring of polynomials.*
- C *a regular chain in* $\mathcal{K}[X]$
- F *a subset of* $\mathcal{K}[X][x]$ *s.t.* $F \not\subset \{0\}$.

OUTPUT: *A set of pairs* $\{(A_1, g_1), \ldots, (A_r, g_r)\}$ *such that*

1. $\mathcal{R}(C) = \mathcal{R}(A_1) \cap \ldots \cap \mathcal{R}(A_r)$ *is an irredundant characteristic decomposition.*
2. $\mathcal{I}(C) \subset \mathcal{I}(A_i)$, $1 \leq i \leq r$.
3. $(F) = (g_i)$ *in* $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(A_i))[x]$.
4. $g_i \in (F) + \mathcal{I}(A_i)$.
5. $g_i = 0$ *or* lcoeff(g_i, x) *does not belong to* $\mathfrak{Zd}(A_i)$.

```
C := ∅;
S := { (C, F) } ;
while S ≠ ∅ do
   (B, G) := pop( S );
   g := an element of G  of lowest degree in  x;
   G := G \ {g};
   (Z,U) := split(K[X], B, lcoeff(g, x));
   if Z ≠ ∅ then
      G' := G ∪ {tail(g, x)};
      if G' ⊂ {0} then
         C := C ∪ {(A, 0) | A ∈ Z} ;
      else
         S := S ∪ {(A, G' \ {0}) | A ∈ Z} ;
      fi;
   fi
   if U ≠ ∅ then
      G' := {srem(f, g, x) | f ∈ G};
      if G' ⊂ {0} then
         C := C ∪ {(A, g) | A ∈ U};
      else
         S := S ∪ {(A, G' ∪ {g}) | A ∈ U};
      fi;
```

fi;
od;
return ($\mathcal{C}$) ;

It is also possible (recommended) to reduce the sets G' by A, or only some element of A, before inserting the pairs $[A, G']$ in $\mathcal{S}$.

Termination: The algorithm can be seen as constructing a tree with root (C, F). Each node has a finite number of sons. The sons of a node (B, G) are some (A, G') where either $G' \subset \{0\}$, in which case it is a leaf, or the sum of the degrees in x of the elements of G' is lower than for G. A path in the tree thus gives a sequence of strictly decreasing positive integers. Any path must be finite and therefore the tree is finite. If split $(\mathcal{K}[X], *, *)$ terminates, pgcd $(\mathcal{K}[X][x], *, *)$ terminates.

Correctness Assuming the correctness of split $(\mathcal{K}[X], *, *)$ we shall show that the while loop has the following invariants.

I1 $\mathcal{R}(C) = \bigcap_{(A,g)\in\mathcal{C}} \mathcal{R}(A) \cap \bigcap_{(A,G)\in\mathcal{S}} \mathcal{R}(A)$ is an irredundant characteristic decomposition.
I2 $\mathcal{I}(C) \subset \mathcal{I}(B)$ for all $(B, G) \in \mathcal{S}$,
I2' $\mathcal{I}(C) \subset \mathcal{I}(A)$ for all $(A, g) \in \mathcal{C}$,
I3 $(F) = (G)$ in $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(A))[x]$ for all $(A, G) \in \mathcal{S}$
I3' $(F) = (g)$ in $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(A))[x]$ for all $(A, g) \in \mathcal{C}$
I4 $G \subset (F) + \mathcal{I}(A)$, for all $(A, G) \in \mathcal{S}$
I4' $g \in (F) + \mathcal{I}(A)$, for all $(A, g) \in \mathcal{C}$

The invariants are easily checked to be true before the loop. That I1 and I2 are preserved comes from Output 1 and 2 of split. I2' is a direct consequence of I2.

I3 is preserved because, if the selected $g \in G$ is such that

- $\mathsf{lcoeff}(g, x) = 0$ in $\mathcal{K}[X]/\mathcal{I}(B)$ then $g = \mathsf{tail}(g, x)$ in $\mathcal{K}[X]/\mathcal{I}(B)$.
- $\mathsf{init}(g) \notin \mathfrak{Z}\mathfrak{d}(B)$ so that $(f, g) = (\mathsf{srem}(f, g), g)$ in $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(B))[x]$, by Proposition 3.4.

I3' is a direct consequence of I3.

The set G in the algorithm starts from F and evolves by pseudo-division by an element in G or by setting to zero an element that belongs to $\mathcal{I}(A)$. I4 is thus preserved and I4' is a consequence of it.

8.2 Useful properties for splitting

This section contains the ingredients for the proof of the splitting algorithm. We first give the simple splits that can always be done on radical ideals and two properties to play with characteristic decompositions. We then give two additional properties of the outputs of the pgcd algorithm.

PROPOSITION 8.2. *Let F be a non empty subset of $\mathcal{K}[X]$. Then*

- $\langle (F) + (a\,b) \rangle = \langle (F) + (a) \rangle \cap \langle (F) + (b) \rangle$ *for any* $a, b \in \mathcal{K}[X]$.
- $\langle F \rangle = \langle F \rangle : H^\infty \cap \bigcap_{h \in H} \langle (F) + (h) \rangle$ *for any finite subset H of $\mathcal{K}[X]$.*

PROPOSITION 8.3. *Let $C \vartriangle c$ be a regular chain in $\mathcal{K}[X][x]$ s.t. $\mathit{lead}(c) = x$. Consider $b \in \mathcal{K}[X][x]$ s.t. $\deg(b,x) = \deg(c,x)$ and $h \in \mathcal{K}[X]$, $h \notin \mathfrak{Zd}(C)$ s.t. $h\,c \equiv b \mod \mathcal{I}(C)$. Then $\mathcal{I}(C \vartriangle c) = \mathcal{I}(C \vartriangle b)$.*

Proof. Let us note $h_c = \mathsf{init}(c)$ and $h_b = \mathsf{init}(b)$. Note that $h_b \equiv h\,h_c \mod \mathcal{I}(C)$. Therefore $h_b \notin \mathfrak{Zd}(C)$ and $C \vartriangle b$ is a regular chain. $\mathcal{I}(C \vartriangle b) = (\mathcal{I}(C) + (b)) : h_b^\infty = (\mathcal{I}(C) + (h\,c)) : (hh_c)^\infty$. We have $c \in (\mathcal{I}(C) + (h\,c)) : (hh_c)^\infty$ and $(\mathcal{I}(C) + (h\,c)) : (hh_c)^\infty \subset \mathcal{I}(C \vartriangle c)$ since $h \notin \mathfrak{Zd}(C \vartriangle c)$. The equality follows.

PROPOSITION 8.4. *Let $C \vartriangle c$ be a regular chain. Assume $\mathcal{R}(C) = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r)$ is an irredundant characteristic decomposition. Then $\mathcal{R}(C \vartriangle c) = \mathcal{R}(C_1 \vartriangle c) \cap \ldots \cap \mathcal{R}(C_r \vartriangle c)$ is an irredundant characteristic decomposition.*

Proof. Since the decomposition is irredundant, $\mathfrak{Zd}(C) = \mathfrak{Zd}(C_1) \cup \ldots \cup \mathfrak{Zd}(C_r)$. Thus $\mathsf{init}(c) \notin \mathfrak{Zd}(C_i)$, $1 \le i \le r$, so that $C_1 \vartriangle c, \ldots, C_r \vartriangle c$ are regular chains.

Obviously $\mathcal{R}(C \vartriangle c) \subset \mathcal{R}(C_i \vartriangle c)$, for $1 \le i \le r$. Let P be a minimal prime of $\mathcal{R}(C \vartriangle c)$. $P \cap \mathcal{K}[X]$ is a minimal prime of $\mathcal{R}(C)$ (Proposition 4.5). By the irredundancy of the decomposition of $\mathcal{R}(C)$, there exists a unique i, $1 \le i \le r$, such that $P \cap \mathcal{K}[X]$ contains $\mathcal{R}(C_i)$. P contains thus a unique $\mathcal{R}(C_i \vartriangle c) = (\mathcal{R}(C_i), c) : \mathsf{init}(c)^\infty$. Given the dimension of the minimal primes of $\mathcal{R}(C_i \vartriangle c)$ and $\mathcal{R}(C \vartriangle c)$ (Proposition 4.4), P is a minimal prime of $\mathcal{R}(C_i \vartriangle c)$. We have

$$\mathcal{R}(C \vartriangle c) \subset \mathcal{R}(C_1 \vartriangle c) \cap \ldots \cap \mathcal{R}(C_r \vartriangle c) \subset \bigcap_{P \text{ a minimal prime of } \mathcal{R}(C \vartriangle c)} P$$

We thus have proved that $\mathcal{R}(C \vartriangle c) = \mathcal{R}(C_1 \vartriangle c) \cap \ldots \cap \mathcal{R}(C_r \vartriangle c)$ is an irredundant characteristic decomposition.

Iterating the process we obtain the following result.

COROLLARY 8.5. *Let $A \vartriangle B$ be a regular chain and assume $\mathcal{R}(A) = \mathcal{R}(A_1) \cap \ldots \cap \mathcal{R}(A_r)$ is an irredundant characteristic decomposition. Then $\mathcal{R}(A \vartriangle B) = \mathcal{R}(A_1 \vartriangle B) \cap \ldots \cap \mathcal{R}(A_r \vartriangle B)$ is an irredundant characteristic decomposition.*

PROPOSITION 8.6. *Assume the pair (B,g) belongs to the output of pgcd $(\mathcal{K}[X][x], C, F)$. If $\deg(g,x) > 0$ then $B \vartriangle g$ is a regular chain and $((F) + \mathcal{I}(B)) : h^\infty = \mathcal{I}(B \vartriangle g)$, where $h = \mathit{init}(g)$.*

Proof. By pgcd.5, $\mathsf{init}(g) = \mathsf{lcoeff}(g,x) \notin \mathfrak{Zd}(B)$. Therefore $B \vartriangle g$ is a regular chain. From pgcd.3, $(F) = (g)$ in $\mathfrak{Q}(\mathcal{K}[X]/\mathcal{I}(B))[x]$. From Proposition 3.2 we have that for all $f \in F$ there exists $k \in h^\infty$ and $q \in \mathcal{K}[X][x]$ such that $k\,f = q\,g \mod \mathcal{I}(B)$. Therefore $F \subset (\mathcal{I}(B) + (g)) : h^\infty$. From pgcd.4, $(g) \subset (F) + \mathcal{I}(B)$. As $\mathcal{I}(B \vartriangle g) = (\mathcal{I}(B) + (g)) : h^\infty$, the equality follows.

PROPOSITION 8.7. *Let $C \vartriangle c$ be a regular chain in $\mathcal{K}[X][x]$ such that $\mathsf{lead}(c) = x$ and $f \in \mathcal{K}[X][x]$ such that $\deg(f, x) > 0$. Assume the pair (B, g) belongs to the output of $\mathsf{pgcd}(\mathcal{K}[X][x], C, \{f, c\})$. Then $B \vartriangle c$ is a regular chain, $g \neq 0$ and*

- *if $\deg(g, x) = 0$ then $f \notin \mathfrak{Zd}(B \vartriangle c)$ so that $\mathcal{I}(B \vartriangle c) : f^\infty = \mathcal{I}(B \vartriangle c)$.*
- *if $\deg(g, x) > 0$ then*
  1. *$\mathcal{R}(B \vartriangle c) : f^\infty = \langle \mathcal{R}(B) + (q) \rangle : (f\, h_q)^\infty$*
  2. *$\mathcal{I}(B \vartriangle c) \subset (\mathcal{I}(B) + (q)) : h_q^\infty$*

  where $q = \mathsf{squo}(c, g, x)$ and $h_q = \mathsf{lcoeff}(q, x) \notin \mathfrak{Zd}(B)$.

Proof. $B \vartriangle c$ is a regular chain by kpgcd.1 and Proposition 8.4. By pgcd.3, $g \neq 0$ since c can not be zero modulo $\mathcal{I}(B)$.

From pgcd.4, there exists $a \in \mathcal{K}[X][x]$ such that $g = a\, f \mod \mathcal{I}(B \vartriangle c)$. If f belongs to $\mathfrak{Zd}(B \vartriangle c)$ so does g. If $\deg(g, x) = 0$ then $g = \mathsf{lcoeff}(g, x) \notin \mathfrak{Zd}(B \vartriangle c)$ by pgcd.5. This proves the first point.

If $\deg(g, x) > 0$, $B \vartriangle g$ is a regular chain and $c \in \mathcal{I}(B \vartriangle g)$, as seen in Proposition 8.6. Let us write $h_g = \mathsf{init}(g)$. There exists $h \in h_g^\infty$ such that $h\, c \equiv q\, g \mod \mathcal{I}(B)$ where $q = \mathsf{squo}(c, g, x)$. We have $h\, \mathsf{init}(c) \equiv h_q\, h_g \mod \mathcal{I}(B)$ and therefore $h_q \notin \mathfrak{Zd}(B)$.

By Proposition 8.3 and Lemma 4.3, $\mathcal{I}(B \vartriangle c) = \mathcal{I}(B \vartriangle q\, g) = (\mathcal{I}(B) + (q\, g)) : (h_q\, h_g)^\infty$. We first have the inclusion property $\mathcal{I}(B \vartriangle c) \subset (\mathcal{I}(B) + (q)) : h_q^\infty$, since the latter ideal is equal to $\mathcal{K}[X][x]$ when $\deg(q, x) = 0$ and equal to $\mathcal{I}(B \vartriangle q)$ when $\deg(q, x) > 0$. Then, by Proposition 8.2 $\langle \mathcal{I}(B) + (q\, g) \rangle = \langle \mathcal{I}(B) + (q) \rangle \cap \langle \mathcal{I}(B) + (g) \rangle$ so that $\mathcal{R}(B \vartriangle c) = \langle \mathcal{I}(B) + (q) \rangle : (h_q\, h_g)^\infty \cap \mathcal{R}(B \vartriangle g)$ and consequently $\mathcal{R}(B \vartriangle c) : f^\infty = \langle \mathcal{I}(B) + (q) \rangle : (f\, h_q\, h_g)^\infty$. Reasoning on the degree of q again we conclude $\langle \mathcal{I}(B) + (q) \rangle : (f\, h_q\, h_g)^\infty = \langle \mathcal{I}(B) + (q) \rangle : (f\, h_q)^\infty$.

8.3 A sub-algorithm of the split

The relatively-prime algorithm presented is a sub-algorithm of split. It generalizes the recursion at the end of Section 2.2 when dealing with non squarefree polynomials. Its role is to compute an irredundant decomposition of the saturation of a characterisable ideal by a polynomial. The call of split to relatively-prime requires in fact to compute saturations of ideals of $\mathcal{K}[X][x]$ of the type $\langle \mathcal{I}(C) + (c) \rangle : \mathsf{lcoeff}(c, x)^\infty$ as it is possible that $\deg(c, x) = 0$.

ALGORITHM 8.8. **Krelatively-prime**
INPUT:

- *$\mathcal{K}[X][x]$ a ring of polynomials.*
- *C a regular chain of $\mathcal{K}[X]$*
- *$c \in \mathcal{K}[X][x]$ such that $\mathsf{lcoeff}(c, x) \notin \mathfrak{Zd}(C)$*
- *$f \in \mathcal{K}[X][x]$, $\deg(f, x) > 0$*

OUTPUT: *A set $\bar{\mathcal{C}}$ of regular chains in $\mathcal{K}[X][x]$ such that $\bar{\mathcal{C}}$ is empty if $(\mathcal{I}(C) + (c)) : \mathsf{lcoeff}(c, x)^\infty : f^\infty = \mathcal{K}[X][x]$ and otherwise*

1. *$\mathcal{R}(C \vartriangle c) : f^\infty = \bigcap_{A \in \bar{\mathcal{C}}} \mathcal{R}(A)$ is an irredundant characteristic decomposition*

2. $\mathcal{I}(C \vartriangle c) \subset \mathcal{I}(A),\ \forall A \in \bar{\mathcal{C}}$

$\mathcal{C} := \emptyset$;
$\mathcal{S} := \{(C, c)\}$;
while $\mathcal{S} \neq \emptyset$ *do*
  $(A, a) := pop(\mathcal{S})$;
  if $\deg(a, x) \neq 0$ *then*
    $G :=$ *pgcd* $(\mathcal{K}[X][x],\ A,\ \{a, f\})$;
    $\mathcal{C} := \mathcal{C} \cup \{(B, a) \mid (B, b) \in G$ *and* $\deg(b, x) = 0\}$;
    $\mathcal{S} := \mathcal{S} \cup \{(B, \mathsf{squo}(a, b, x)) \mid (B, b) \in G$ *and* $\deg(b, x) > 0\}$;
  fi;
od;
return ($\{A \vartriangle a \mid (A, a) \in \mathcal{C}$);

Note that if $\deg(c, x) = 0$ then $(\mathcal{R}(C) + (c)) : \mathsf{lcoeff}(c, x)^\infty = \mathcal{K}[X][x]$ and Krelatively-prime returns an empty set.

Termination: The degree in x is lower in $\mathsf{squo}(a, b, x)$ than in a, $\forall (B, b) \in G_0$. Termination is proved thanks to the same analogy to a tree as for pgcd.

Correctness We shall check that the following properties are invariants of the while loop. The correctness then follows.

I0 $\bigcap_{(A,a)\in\mathcal{C}\cup\mathcal{S}} \mathcal{R}(A)$ is an irredundant characteristic decomposition.
I1 $(\mathcal{I}(C) + (c)) : \mathsf{lcoeff}(c, x)^\infty \subset (\mathcal{I}(A) + (a)) : \mathsf{lcoeff}(a, x)^\infty$, for all $(A, a) \in \mathcal{S}$
I1' $\mathcal{I}(C \vartriangle c) \subset \mathcal{I}(A \vartriangle a)$, for all $(A, a) \in \mathcal{C}$
I2 $\mathsf{lcoeff}(a, x) \notin \mathfrak{Zd}(A)$, for all $(A, a) \in \mathcal{S}$
I2' $A \vartriangle a$ is a regular chain for all $(A, a) \in \mathcal{C}$
I3 $f \notin \mathfrak{Zd}(A \vartriangle a)$, for all $(A, a) \in \mathcal{C}$.
I4 $\langle \mathcal{I}(C) + (c) \rangle : (f\,\mathsf{lcoeff}(c, x))^\infty = \bigcap_{(A,a)\in\mathcal{S}} \langle \mathcal{I}(A) + (a) \rangle : (f\,\mathsf{lcoeff}(a, x))^\infty \cap \bigcap_{(A,a)\in\mathcal{C}} \mathcal{R}(A \vartriangle a)$

The invariants are satisfied before the while loop. Assume they are now true at the beginning of an iteration. If $\deg(a, x) = 0$ then $a = \mathsf{lcoeff}(a, x)$ and thus $1 \in \langle \mathcal{I}(A) + (a) \rangle : \mathsf{lcoeff}(a, x)^\infty$. Dropping this component does not affect I4. Nor does it affect I0, I1, I2, I2' and I3.

Let us consider the case $\deg(a, x) > 0$. This case can only happen when the input is such that $\deg(c, x) > 0$. By induction hypothesis on I2, $A \vartriangle a$ is a regular chain.

By pgcd.1 and Proposition 8.4, $\mathcal{R}(A) = \bigcap_{(B,b)\in G} \mathcal{R}(B)$ and $\mathcal{R}(A \vartriangle a) = \bigcap_{(B,b)\in G} \mathcal{R}(B \vartriangle a)$ are irredundant characteristic decompositions. I0 will be preserved. From pgcd.2, $\mathcal{I}(A) \subset \mathcal{I}(B)$.

Let (B, b) be an element of G. Note first that $b \neq 0$ since $a \notin \mathfrak{Zd}(A)$. If $\deg(b, x) = 0$, then $f \notin \mathfrak{Zd}(B \vartriangle a)$ by Proposition 8.7. The pair (B, a) is put in $\mathcal{C}$ so that I2' and I3 are preserved. From pgcd.2 we can say that $\mathcal{I}(A \vartriangle a) \subset \mathcal{I}(B \vartriangle a)$ and thus I1' is preserved by induction hypothesis on I1.

If $\deg(b, x) > 0$, by Proposition 8.7, $\mathcal{I}(B \vartriangle a) \subset (\mathcal{I}(B) + (q)) : h_{ab}^{\infty}$ and $\mathcal{R}(B \vartriangle a) : f^{\infty} = \langle \mathcal{R}(B) + (q_{ab}) \rangle : (f\, h_{ab})^{\infty}$, where $q_{ab} = \mathsf{squo}(a, b, x)$ and $h_{ab} = \mathsf{lcoeff}(q_{ab}, x) \notin \mathfrak{Zd}(B)$. On the one hand I1 and I2 are preserved and on the other hand we can write

$$\begin{aligned}\mathcal{R}(A \vartriangle a) : f^{\infty} &= \textstyle\bigcap_{(B,b)\in G} \mathcal{R}(B \vartriangle a) : f^{\infty} \\ &= \bigcap_{\substack{(B,b)\in G \\ \deg(b,x)=0}} \mathcal{R}(B \vartriangle a) \quad \cap \quad \bigcap_{\substack{(B,b)\in G \\ \deg(b,x)>0}} (\mathcal{R}(B) + (q_{ab})) : (f\, h_{ab})^{\infty} .\end{aligned}$$

That insures that I4 is preserved.

8.4 Splitting algorithm

In Section 2.4 we saw a way of splitting a product of field $\mathcal{K}[x]/\langle c \rangle$ according to a polynomial in $\mathcal{K}[x]$. The process relied on gcd computations over $\mathcal{K}$. The split algorithm we describe here is an extension to the product of field $\mathcal{K}(\mathfrak{T}(C))[\mathfrak{L}(C)]$ where C is a regular chain in $\mathcal{K}[X]$. It relies essentially on a pgcd algorithm and Gauss lemma Theorem 2.3 .

The algorithm split has the side effect of decreasing multiplicities. Take the simple case where we examine the splitting of $\mathcal{K}[x]/\langle c \rangle$, where $c = x(x+1)^r$ according to the polynomial $f = (x+1)^e$ where $e < r$. We will obtain $\mathcal{K}[x]/\langle c \rangle = \mathcal{K}[x]/\langle g_0 \rangle \times \mathcal{K}[x]/\langle x \rangle$ where $g_0 = (x+1)^e$ if $e < r$ and $g_1 = x$.

Algorithm 8.9. **split**
Input:

- $\mathcal{K}[X]$ *a polynomial ring*
- C *a regular chain of* $\mathcal{K}[X]$
- f *a polynomial in* $\mathcal{K}[X]$

Output: *A pair* $(\mathcal{Z}, \mathcal{U})$ *of sets of regular chains in* $\mathcal{K}[X]$ *such that*

1. $\mathcal{R}(C) = \bigcap_{A \in \mathcal{Z}\cup\mathcal{U}} \mathcal{R}(A)$ *is an irredundant characteristic decomposition.*
2. $\mathcal{I}(C) \subset \mathcal{I}(A)$, $\forall A \in \mathcal{Z} \cup \mathcal{U}$,
3. $f \in \mathcal{I}(A)$, $\forall A \in \mathcal{Z}$.
4. $f \notin \mathfrak{Zd}(A)$, $\forall A \in \mathcal{U}$.

```
if f = 0 then
  return( ({C}, ∅) );
elif f ∈ K then
  return((∅, {C}) );
fi;
x := lead(f);
```

if $x \notin \mathfrak{L}(C)$ *then*
F := *the set of coefficients of* f, *seen as a polynomial in* x;
$\mathcal{U} := \emptyset$; $\mathcal{Z} = \emptyset$;
$\mathcal{S} := \{ (C_{<x}, F) \}$;
while $\mathcal{S} \neq \emptyset$ *do*
$(B, E) :=$ *pop* $(\mathcal{S})$;
$g :=$ *pop*(E);
$(Z, U) :=$ *split* $(\mathcal{K}[X_{<x}], B, g)$;
$\mathcal{U} := \mathcal{U} \cup U$;
if $E = \emptyset$ *then*
$\mathcal{Z} := \mathcal{Z} \cup Z$;
else
$\mathcal{S} := \mathcal{S} \cup \{(A, E) \mid A \in Z\}$;
fi;
od;
else
c := *the element of* C *with leader* x;
$G :=$ *pgcd*$(\mathcal{K}[X_{<x}][x], C_{<x}, \{f, c\})$;
$\mathcal{Z} := \{A \vartriangle a \mid (A, a) \in G, \deg(a, x) > 0\}$;
$\mathcal{U} := \{A \vartriangle c \mid \exists a,\ (A, a) \in G, \deg(a, x) = 0\}$;
$\mathcal{U} := \mathcal{U} \cup \bigcup_{\substack{(A,a) \in G \\ \deg(a,x) > 0}}$ *relatively-prime*$(\mathcal{K}[X][x], A,$ *squo*$(c, a, x), f)$;
fi;
$\mathcal{Z} := \{A \vartriangle C_{>x} \mid A \in \mathcal{Z}\}$;
$\mathcal{U} := \{A \vartriangle C_{>x} \mid A \in \mathcal{U}\}$;
return($(\mathcal{Z}, \mathcal{U})$);

In the case $C_x = 0$, we use Gauss lemma. Consider for instance $C = x\,(x+1)\,(x+2)$ as a regular chain in $\mathcal{K}[x, y]$ and $f = x\,y^2 + (x+1)\,y + 1$. To decide if f is not a zero divisor one needs to decide if one its coefficients is not a zero divisor. A simple inspection leads us to the fact $f \notin \mathfrak{Zd}(C)$ since one of its coefficient belongs to $\mathcal{K}$. Therefore $(\emptyset, C)$ is a valid output. [Kal93] and [Aub99] use a weakened version of Gauss lemma. The successive initials of f are inspected. For the example presented here, split would be recursively called for x and then for $x+1$. The output would therefore be $(\emptyset, \{C_1, C_2, C_3\})$ leading to more components and therefore redundancies in the computations.

Termination Termination follows simply from termination of split$(\mathcal{K}[X_{<y}], *, *)$ and of pgcd$(\mathcal{K}[X_{<y}][y], *, *)$ for any $y \in X$.

Correctness We shall assume that split$(\mathcal{K}[X_{<y}], *, *])$ and pgcd$(\mathcal{K}[X_{<y}][y], *, *])$ is correct for any $y \in X$ and prove correctness for split$(\mathcal{K}[X], *, *])$. For that we need to prove that after the conditional branching if $x \notin \mathfrak{L}(C)$ then [...] else [...] we have:

- $\mathcal{R}(C_{\leq x}) = \bigcap_{A\in\mathcal{U}\cup\mathcal{Z}} \mathcal{R}(A)$ is an irredundant characteristic decomposition.
- $f \equiv 0 \mod \mathcal{I}(A),\ \forall A \in \mathcal{Z}$
- $f \notin \mathfrak{Zd}(A),\ \forall A \in \mathcal{U}$.

Indeed Proposition 5.8 and 8.4 allow then to conclude. There are two different cases according to whether or not $x = \mathsf{lead}(f)$ appears as a leader of an element of C.

The case $x \notin \mathfrak{L}(C)$

Then $\mathcal{K}[X][x]/\mathcal{I}(C_{\leq x}) = (\mathcal{K}[X]/\mathcal{I}(C_{<x}))[x]$. Thus, according to Gauss lemma (Theorem 2.3), $f \in \mathfrak{Zd}(C_{\leq x})$ if and only if F, the set of coefficients of f considered as a polynomial in x, is included in $\mathfrak{Zd}(C_{<x})$. The *while* loop inspects each coefficient in turn (in any order). It has the following invariants:

I0 $\mathcal{R}(C_{<x}) = \bigcap_{(A,E)\in\mathcal{S}} \mathcal{R}(A) \cap \bigcap_{A\in\mathcal{U}\cup\mathcal{Z}} \mathcal{R}(A)$ is an irredundant characteristic decomposition
I1 $\mathcal{I}(C_{<x}) \subset \mathcal{I}(A)$ for all $A \in \mathcal{Z}\cup\mathcal{U}$ and all $(A,E) \in \mathcal{S}$
I2 $F \setminus E \subset \mathcal{I}(A)$, for all $(A,E) \in \mathcal{S}$
I2' $F \not\subset \mathfrak{Zd}(A)$, for all $A \in \mathcal{U}$
I2" $F \subset \mathcal{I}(A)$, for $A \in \mathcal{Z}$

These invariants are obviously satisfied before the *while* loop. At each iteration I0 and I1 are kept true because of $\mathsf{split}.1$ and $\mathsf{split}.2$ on $\mathcal{K}[X_{<x}]$. I2 is easily seen to be kept true since $\mathcal{S}$ is augmented with the components modulo which the element of F treated is 0. I2' and I2" are consequences of I2 given how are augmented $\mathcal{Z}$ and $\mathcal{U}$.

The case $x \in \mathfrak{L}(C)$

Thanks to $\mathsf{pgcd}.1$, $\mathsf{pgcd}.2$ and Proposition 8.4 we have that $\mathcal{R}(C_{\leq x}) = \bigcap_{(A,a)\in G} \mathcal{R}(A \triangle c)$ is an irredundant characteristic decomposition and $\mathcal{I}(C_{\leq x}) \subset \mathcal{I}(A \triangle c), \forall (A,a) \in G$. For any pair $(A,a) \in G$, $a \neq 0$ because $c \neq 0 \mod \mathcal{I}(A)$.

For $(A,a) \in G$ such that $\deg(a,x) = 0$, $f \notin \mathfrak{Zd}(A \triangle c)$ by Proposition 8.7. That justifies the initialization of $\mathcal{U}$.

For (A,a) with $\deg(a,x) > 0$, $h_a = \mathsf{init}(a) = \mathsf{lcoeff}(a,x)$ does not belong to $\mathfrak{Zd}(A)$, by $\mathsf{pgcd}.5$. By $\mathsf{pgcd}.3$, $f \in \mathcal{I}(A \triangle a)$ which justifies the value given to $\mathcal{Z}$. Let $h_c = \mathsf{init}(c)$. We have $\mathcal{R}(A \triangle c) = \mathcal{R}(A \triangle c) : h_a^\infty = \langle \mathcal{I}(A) + (c,f)\rangle : (h_c h_a)^\infty \cap \mathcal{R}(A \triangle c) : f^\infty$ by Lemma 4.3 and Proposition 8.2. This decomposition is irredundant if $1 \notin \mathcal{R}(A \triangle c) : f^\infty$. Now $\langle \mathcal{I}(A) + (c,f)\rangle : (h_a)^\infty = \mathcal{R}(A \triangle a)$ by Proposition 8.6. Since $h_c \notin \mathfrak{Zd}(A \triangle a)$ the previous decomposition can be written $\mathcal{R}(A \triangle c) = \mathcal{R}(A \triangle a) \cap \mathcal{R}(A \triangle c) : f^\infty$. By Proposition 8.7, $\mathcal{R}(A \triangle c) : f^\infty = \langle \mathcal{I}(A) + (q)\rangle : (f\, h_q)^\infty$ and $\mathcal{I}(A \triangle c) \subset (\mathcal{I}(A) + (q)) : h_q^\infty$ where $q = \mathsf{squo}(c,a,x)$ and $h_q = \mathsf{lcoeff}(q,x)$. The output properties of $\mathsf{relatively\text{-}prime}$ allow to conclude.

9 Characteristic decomposition algorithm

A pseudo-gcd algorithm with respect to a characterizable ideal given by a regular chain can be applied to compute a characteristic decomposition of the radical ideal generated by a finite family of polynomials. After describing and proving the algorithm, we shall discuss the membership test it gives to the radical ideal as well as how to refine the characteristic decomposition obtained.

In the description of this algorithm again, $\mathcal{S}$ is a set containing the data awaiting more computations, while $\mathcal{C}$ is a set of data for which the computation is completed. An element $(\hat{F}, \check{F}, C)$ of $\mathcal{S}$, where $\hat{F}, \check{F}$ are subsets of $\mathcal{K}[X]$ and C is a regular chain, represents the radical ideal $\left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle$. $\check{F}$ correspond to the already considered polynomials of F, in the sense that $\check{F} \subset \mathcal{I}(C)$.

Algorithm 9.1. **decompose**
Input:

- $\mathcal{K}[X]$ *a polynomial ring*
- F *a nonempty set of polynomials in* $\mathcal{K}[X]$

Output: *A set* $\mathcal{C}$ *of regular chains such that*

- $\mathcal{C}$ *is empty if* $\langle F \rangle = \mathcal{K}[X]$.
- $\langle F \rangle = \bigcap_{C \in \mathcal{C}} \mathcal{R}(C)$ *otherwise.*

$\mathcal{C} := \emptyset$;
$\mathcal{S} := \{(F, \emptyset, \emptyset)\}$;
while $\mathcal{S} \neq \emptyset$ *do*
  $(\hat{F}, \check{F}, C) :=$ *pop* $(\mathcal{S})$;
  if $\hat{F} \subset \{0\}$ *then*
    $\mathcal{C} := \mathcal{C} \cup \{C\}$
  elif $\hat{F} \cap \mathcal{K} \neq \emptyset$
    $x := \min\{y \in X \mid \hat{F} \cap \mathcal{K}[X_{\leq y}] \neq \emptyset\}$;
    $F_x := \hat{F} \cap \mathcal{K}[X_{\leq x}]$;
    $G :=$ *pgcd* $(\mathcal{K}[X_{<x}][x], C, F_x)$;
    $S_0 := \{(\hat{F} \setminus F_x, \check{F} \cup F_x, B) \mid (B, 0) \in G\}$;
    $S_1 := \{(\hat{F} \cup \check{F} \cup B \cup \{g\}, \emptyset, \emptyset) \mid (B, g) \in G,\ \deg(g, x) = 0,\ g \neq 0\}$;
    $S_2 := \{(\hat{F} \setminus F_x, \check{F} \cup F_x, B \vartriangle g) \mid (B, g) \in G,\ \deg(g, x) > 0\}$;
    $S_2' := \{(\hat{F} \cup \check{F} \cup B \cup \{\mathit{init}(g)\}, \emptyset, \emptyset) \mid (B, g) \in G,\ \deg(g, x) > 0\}$;
    $\mathcal{S} := \mathcal{S} \cup S_0 \cup S_1 \cup S_2 \cup S_2'$
  fi;
od;
return($\mathcal{C}$ *);*

Note the following difference with the versions of [Kal93, Aub99]: the regular chains computed up to a point are reintroduced in the components of S_1 and S_2' where the computation basically starts over. Computations are then easier if there is already a triangular set to start with.

Termination We can visualize the algorithm as constructing a tree with root $(F, \emptyset, \emptyset)$. A node is given by a 3-tuple $(\hat{F}, \check{F}, C)$. A son of a node $(\hat{F}, \check{F}, C)$ is an element of the constructed sets S_0, S_1, S_2 or S_2'. A leaf is an element $(\emptyset, *, *)$.

For convenience, we shall introduce a dummy variable x_0 that we assume to be lower than all the variables of X. We write $\bar{X} = X \cup \{x_0\}$. We extend each 3-tuple $(\hat{F}, \check{F}, C)$ to a 4-tuple $(\hat{F}, \check{F}, C, y)$ where y is such that $C \subset \mathcal{K}[\bar{X}_{\leq y}]$ and $\hat{E} \cap \mathcal{K}[\bar{X}_{\leq y}] = \emptyset$. The root is now $(F, \emptyset, \emptyset, x_0)$.

A son $(\hat{F}, \check{F}, C, y)$ of a node $(\hat{E}, \check{E}, B, x)$ falls into one of the two following categories

Type 1: It is such that $\hat{F} \cup \check{F} = \hat{E} \cup \check{E}$ and $y > x$. This is the case of the 4-tuples in S_0 and S_2.

Type 2: $\check{F} = \emptyset$, $C = \emptyset$ and $y = x_0$. This is the case of the 4-tuples in S_1 and S_2'. Their main property is that the ideal generated by the set $(\hat{E} \cup \check{E}) \cap \mathcal{K}[\bar{X}_{<y}] = \check{E} \cap \mathcal{K}[\bar{X}_{<y}]$ is strictly included in the ideal generated by the set $(\hat{F} \cup \check{F}) \cap \mathcal{K}[\bar{X}_{<y}] = \hat{F} \cap \mathcal{K}[\bar{X}_{<y}]$. Indeed we introduce in $\hat{F}$ g or $\mathsf{init}(g)$ and we shall see in the correctness part of the proof that they do not belong to $(\check{E}) \subset \mathcal{I}(B)$. We also have $\hat{E} \cup \check{E} \subset \hat{F} \cup \check{F}$.

Assume that there is an infinite path in the tree. Since the set $\bar{X}$ is finite, there will be on this path an infinite sequence of nodes $(\hat{F}_i, \emptyset, \emptyset, x_0)$ of type 2 with a father having the same y as 4th component. This sequence defines a strictly increasing sequence of ideals in $\mathcal{K}[\bar{X}_{<y}]$, namely the ideals $(\hat{F}_i \cap \mathcal{K}[\bar{X}_{<y}])$. This contradicts the fact that $\mathcal{K}[\bar{X}_{<y}]$ is Noetherian.

Correctness We shall show that the while loop has the following invariants.

I0 $F \subset \hat{F} \cup \check{F}$ and $\check{F} \subset \mathcal{I}(C)$, for all $(\hat{F}, \check{F}, C) \in \mathcal{S}$

I1 $\langle F \rangle = \bigcap_{(\hat{F}, \check{F}, C) \in \mathcal{S}} \left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle \cap \bigcap_{C \in \mathcal{C}} \mathcal{R}(C)$

We first give a couple of easy properties that are used implicitly in the proof.

Proposition 9.2. *Let I and J be ideals in a ring $\mathcal{K}[X]$. $\sqrt{I + J} = \sqrt{I + \sqrt{J}}$.*

Proposition 9.3. *Let $I_0, I_1, \ldots, I_r$ be ideals in a ring $\mathcal{K}[X]$. Then $\sqrt{I_0 + \bigcap_{j=1}^{r} I_j} = \bigcap_{k=1}^{r} \sqrt{I_0 + I_k}$.*

I0 and I1 are obviously true before the while loop. Assume that they are true at the beginning of a new iteration treating the tuple $(\hat{F}, \check{F}, C)$. If $\hat{F} \subset \{0\}$ then $\left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle = \mathcal{R}(C)$. If $\hat{F} \cap \mathcal{K} \setminus \{0\}$ then $\left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle = \mathcal{K}[X]$ and the component can be dropped. We assume from now on that $\hat{F} \cap \mathcal{K} = \emptyset$.

By $\mathsf{pgcd}.1$ and $\mathsf{pgcd}.2$, $\check{F} \subset \mathcal{I}(C) \subset \mathcal{I}(B)$ and

$$\left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle = \bigcap_{(B,g) \in G} \left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle. \tag{1}$$

Take $(B, g) \in G$. There are three cases according to whether $g = 0$, $\deg(g, x) = 0$ or $\deg(g, x) > 0$. We examine these three cases separately.

If $g = 0$, we know that $F_x \subset \mathcal{I}(B)$ by pgcd.3. Thus

$$\left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle = \left\langle (\hat{F} \setminus F_x) + \mathcal{I}(B) \right\rangle \tag{2}$$

If $\deg(g, x) = 0$ but $g \neq 0$, from pgcd.4, $g \in (F_x) + \mathcal{I}(B)$. By induction hypothesis on I0 we thus obtain

$$\langle F \rangle \subset \left\langle (\hat{F} \cup \check{F}) + (g) + (B) \right\rangle \subset \left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle \tag{3}$$

If $\deg(g, x) > 0$, let $h_g = \mathsf{init}(g) = \mathsf{lcoeff}(g, x)$. Thanks to Proposition 8.2

$$\begin{aligned} &\left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle = \left\langle (\hat{F} \setminus F_x) + (F_x) + \mathcal{I}(B) \right\rangle \\ &= \left\langle (\hat{F} \setminus F_x) + \langle (F_x) + \mathcal{I}(B) \rangle : h_g^\infty \right\rangle \cap \left\langle (\hat{F} \setminus F_x) + \langle (F_x) + \mathcal{I}(B) + (h_g) \rangle \right\rangle . \end{aligned} \tag{4}$$

By Proposition 8.6, $B \vartriangle g$ is a regular chain and $((F_x) + \mathcal{I}(B)) : h_g^\infty = \mathcal{I}(B \vartriangle g)$. Equation (4) becomes

$$\left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle = \left\langle (\hat{F} \setminus F_x) + \mathcal{I}(B \vartriangle g) \right\rangle \cap \left\langle (\hat{F}) + \mathcal{I}(B) + (h_g) \right\rangle \tag{5}$$

By induction hypothesis on I0, $F \subset \hat{F} \cup \check{F}$ and with pgcd.2, $\check{F} \subset \mathcal{I}(C) \subset \mathcal{I}(B)$. Thus

$$\langle F \rangle \subset \left\langle (\hat{F} \cup \check{F}) + (B) + (h_g) \right\rangle \subset \left\langle (\hat{F}) + \mathcal{I}(B) + (h_g) \right\rangle . \tag{6}$$

$\mathcal{S}$ is the set deprived from the tuple $\{(\hat{F}, \check{F}, C)\}$. With the induction hypothesis on I1 we can write

$$\langle F \rangle = \bigcap_{(\hat{E}, \check{E}, D) \in \mathcal{S}} \left\langle (\hat{E}) + \mathcal{I}(D) \right\rangle \cap \left\langle (\hat{F}) + \mathcal{I}(C) \right\rangle$$

With (1), (2) and (5) we can rewrite this equation as

$$\begin{aligned} \langle F \rangle = &\bigcap_{(\hat{E}, \check{E}, D) \in \mathcal{S}} \left\langle (\hat{E}) + \mathcal{I}(D) \right\rangle \cap \bigcap_{(B,0) \in G} \left\langle (\hat{F} \setminus F_x) + \mathcal{I}(B) \right\rangle \cap \bigcap_{\substack{(B,g) \in G \\ \deg(g,x) = 0}} \left\langle (\hat{F}) + \mathcal{I}(B) \right\rangle \\ \cap &\bigcap_{\substack{(B,g) \in G \\ \deg(g,x) > 0}} \left(\left\langle (\hat{F} \setminus F_x) + (B \vartriangle g) : I_{B \vartriangle g}^\infty \right\rangle \cap \left\langle (\hat{F}) + \mathcal{I}(B) + (h_g) \right\rangle \right) \end{aligned}$$

Intersecting both sides of this latter equation by $\left\langle (\hat{F} \cup \check{F}) + (g) + (B) \right\rangle$, for all $(B, g) \in G$ with $\deg(g, x) = 0, g \neq 0$, and $\left\langle (\hat{F} \cup \check{F}) + (B) + (h_g) \right\rangle$ for all

$(B,g) \in G$ with $\deg(g,x) > 0$, we obtain, thanks to (3) and (6),

$$
\begin{aligned}
\langle F\rangle = & \bigcap_{(\hat{E},\check{E},D)\in\mathcal{S}} \left\langle(\hat{E}) + \mathcal{I}(D)\right\rangle \cap \bigcap_{(B,0)\in G} \left\langle(\hat{F}\setminus F_x) + \mathcal{I}(B)\right\rangle \\
\cap & \bigcap_{\substack{(B,g)\in G\\ \deg(g,x)=0}} \left\langle(\hat{F}\cup\check{F}) + (g) + (B)\right\rangle \\
\cap & \bigcap_{\substack{(B,g)\in G\\ \deg(g,x)>0}} \left(\left\langle(\hat{F}\setminus F_x) + \mathcal{I}(B\vartriangle g)\right\rangle \cap \left\langle(\hat{F}\cup\check{F}) + (B) + (h_g)\right\rangle\right)
\end{aligned}
$$

This justifies that the elements pushed on the stack preserve the invariants I0 and I1.

Membership test With a characteristic decomposition, as computed by decompose, it is possible to test membership to the radical ideal generated by a finite set of polynomials. This is explained below. Nonetheless, since the decomposition is not always irredundant, it is not possible to give sufficient or necessary conditions for f to be invertible or a zero divisor modulo $\langle F\rangle$.

Consider a finite set of polynomials F in $\mathcal{K}[X]$ and compute its characteristic decomposition

$$\langle F\rangle = \mathcal{R}(C_1) \cap \ldots \cap \mathcal{R}(C_r).$$

For an element f of $\mathcal{K}[X]$, let $(\mathcal{Z}_i, \mathcal{U}_i)$ be the output of $\mathsf{split}(\mathcal{K}[X], C_i, f)$. For f to belong to $\langle F\rangle$ it is necessary and sufficient that all $\mathcal{U}_i$ be empty.

If in the characteristic decomposition all the regular chains C_i are squarefree, the test is simpler. In this case a necessary and sufficient condition for f to belong to $\langle F\rangle$ is that $\mathsf{srem}(f, C_i) = 0$ for all $1 \le i \le r$. In the next paragraph we show how to obtain a squarefree decomposition.

Refinement to squarefree regular chains It is possible to refine the output of decompose so that all the components are squarefree regular chains. In which case we have a decomposition that can be written

$$\langle F\rangle = \mathcal{I}(C_1) \cap \ldots \cap \mathcal{I}(C_r).$$

One way to proceed is to apply the following algorithm to each component of the output of decompose.

ALGORITHM 9.4. **sqrfree-decomposition**
INPUT:

- $\mathcal{K}[X]$ *a ring of polynomials.*
- C *a regular chain of* $\mathcal{K}[X]$

OUTPUT: *A non empty set* $\mathcal{C}$ *of squarefree regular chains in* $\mathcal{K}[X][x]$ *such that* $\mathcal{R}(C) = \bigcap_{A\in\mathcal{C}} \mathcal{I}(A)$ *is an irredundant characteristic decomposition*

$\mathcal{C} := \emptyset$;
$\mathcal{S} := \{(C, \emptyset)\}$;
while $\mathcal{S} \neq \emptyset$ *do*
  $(\hat{B}, \check{B}) := pop(\mathcal{S})$;
  if $\hat{B} = \emptyset$ *then*
    $\mathcal{C} := \mathcal{C} \cup \{C\}$;
  else
    $x :=$ *the lowest variable of* $\mathfrak{L}(\hat{B})$;
    $b :=$ *the element of* $\hat{B}$ *with leader* x;
    $G := \mathsf{pgcd}\ (\mathcal{K}[X][x], \check{B}, \{b, \mathsf{sep}(b)\})$;
    $\mathcal{S} := \mathcal{S} \cup \{(\hat{B}_{>x}, A \vartriangle \mathsf{squo}(c, a, x)) \mid (A, a) \in G\}$;
  fi;
od;
return $(\mathcal{C})$;

The main ingredient to prove that the following properties are invariants of the while loop is Theorem 7.1.

I1 $\check{B}$ is a squarefree regular chain, for all $(\hat{B}, \check{B}) \in \mathcal{S}$
I1' B is a squarefree regular chain, for all $B \in \mathcal{C}$
I2 $\mathcal{R}(C) = \bigcap_{(\hat{B},\check{B}) \in \mathcal{S}} \mathcal{R}(\check{B} \vartriangle \hat{B}) \cap \bigcap_{B \in \mathcal{C}} \mathcal{I}(B)$ is an irredundant characteristic decomposition.

References

[AK93] S. A. Abramov and K. Y. Kvashenko. The greatest common divisor of polynomials that depend on a parameter. *Vestnik Moskovskogo Universiteta. Seriya XV. Vychislitel′ naya Matematika i Kibernetika*, 2:65–71, 1993. translation in Moscow Univ. Comput. Math. Cybernet. 1993, no. 2, 59–64.

[ALMM99] P. Aubry, D. Lazard, and M. Moreno-Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28(1-2), 1999.

[AMM99] P. Aubry and M. Moreno-Maza. Triangular sets for solving polynomial systems: a comparative implementation of four methods. *Journal of Symbolic Computation*, 28(1-2):125–154, 1999.

[ARSED00] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. Technical report, INRIA, `http://www.inria.fr/rrrt/rr-3992.html`, 2000.

[Aub99] P. Aubry. *Ensembles triangulaires de polynomes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université de Paris 6, 1999.

[BJ01] A. M. Bellido and V. Jalby. Spécifications des algorithmes de triangulation de systèmes algébro-élémentaires. *C. R. Acad. Sci. Paris*, Ser. I(334):155–159, 2001.

[BKRM01] D. Bouziane, A. Kandri Rody, and H. Maârouf. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. *Journal of Symbolic Computation*, 31(6):631–649, 2001.

[BL00] F. Boulier and F. Lemaire. Computing canonical representatives of regular differential ideals. In C. Traverso, editor, *ISSAC*. ACM-SIGSAM, ACM, 2000.

[BLOP95] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A. H. M. Levelt, editor, *ISSAC'95*. ACM Press, New York, 1995.

[BLOP97] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL, 1997.

[BW93] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, 1993.

[CG90] S. C. Chou and X. S. Gao. Ritt-wu's decomposition algorithm and geometry theorem proving. In M. E. Stickel, editor, *10th International Conference on Automated Deduction*, number 449 in Lecture Notes in Computer Sicences, pages 207–220. Springer-Verlag, 1990.

[CGZ94] S. C. Chou, X. S. Gao, and J. Z. Zhang. *Machine proofs in geometry*. World Scientific Publishing Co. Inc., River Edge, NJ, 1994. Automated production of readable proofs for geometry theorems, With a foreword by Robert S. Boyer.

[CH01] T. Cluzeau and E. Hubert. Resolvent representation for regular differential ideals. Technical Report RR-4200, INRIA Sophia Antipolis, `http://www.inria.fr/rrrt/rr-4200.html`, 2001.

[Cho88] S. C. Chou. *Mechanical geometry theorem proving*. D. Reidel Publishing Co., Dordrecht, 1988. With a foreword by Larry Wos.

[DDD85] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *Proceedings of EUROCAL 85*, number 204 in Lecture Notes in Computer Science, pages 289–290. Springer-Verlag, 1985.

[Del99] S. Dellière. *Triangularisation de systèmes constructibles. Application à l'évaluation dynamique*. PhD thesis, Université de Limoges, 1999.

[Del00a] S. Dellière. D. M. Wang simple systems and dynamic constructible closure. Technical Report 16, Laboratoire d'Arithmétique, de Calcul Formel et d'Optimisation, Limoges, `http://www.unilim.fr/laco`, 2000.

[Del00b] S. Dellière. A first course to D7 with examples. `www-lmc.imag.fr/lmc-cf/Claire.Dicrescenzo/D7`, 2000.

[Del00c] S. Dellière. Pgcd de deux polynômes paramètres : approche par la clôture constructible dynamique et généralisation de la méthode de S. A. Abramov, K. Yu. Kvashenko. Technical Report RR-3882, INRIA, Sophia Antipolis, 2000. http://www.inria.fr/RRRT/RR-3882.html.

[Del01] S. Dellière. On the links between triangular sets and dynamic constructible closure. *J. Pure Appl. Algebra*, 163(1):49–68, 2001.

[Duv87] D. Duval. *Diverses questions relatives au calcul formel avec des nombres algébriques*. PhD thesis, Institut Fourier, Grenoble, 1987.

[Eis94] D. Eisenbud. *Commutative Algebra with a View toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag New York, 1994.

[FMM01] M. V. Foursov and M. Moreno Maza. On computer-assisted classification of coupled integrable equations. In *Proceedings of the 2001 international symposium on Symbolic and algebraic computation*, pages 129–136. ACM Press, 2001.

[GC92] X. S. Gao and S. C. Chou. Solving parametric algebraic sytems. In *ISSAC 92*, pages 335–341. ACM Press, New York, NY, USA, 1992.

[GCL92] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

[GD94] T. Gómez-Dîaz. *Quelques applications de l'valuation dynamique*. PhD thesis, Université de Limoges, 1994.

[Hub00] E. Hubert. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000.

[Hub02] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. II Differential systems. In this volume, 2002.

[Kal93] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15(2):143–167, 1993.

[Kal98] M. Kalkbrener. Algorithmic properties of polynomial rings. *Journal of Symbolic Computation*, 26(5):525–582, November 1998.

[Kol73] E. R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1973.

[Laz91] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete and Applied Mathematics*, 33:147–160, 1991.

[Laz92] D. Lazard. Solving zero dimensional algebraic systems. *Journal of Symbolic Computation*, 15:117–132, 1992.

[MKRS98] H. Maârouf, A. Kandri Rody, and M. Ssafini. Triviality and dimension of a system of algebraic differential equations. *Journal of Automated Reasoning*, 20(3):365–385, 1998.

[MM97] M. Moreno-Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques*. PhD thesis, Université Paris 6, 1997.

[MMR95] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, pages 365–382. Springer, Berlin, 1995.

[Mor99] S. Morrison. The differential ideal $[P]:M^\infty$. *Journal of Symbolic Computation*, 28(4-5):631–656, 1999.

[Ric99] D. Richardson. Weak Wu stratification in $\mathbf{R}^n$. *Journal of Symbolic Computation*, 28(1-2):213–223, 1999. Polynomial elimination—algorithms and applications.

[Rit30] J. F. Ritt. Manifolds of functions defined by systems of algebraic differential equations. *Transaction of the American Mathematical Society*, 32:569–598, 1930.

[Rit32] J. F. Ritt. *Differential Equations from the Algebraic Standpoint*. Amer. Math. Soc. Colloq. Publ., 1932.

[Rit50] J. F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium publications*. American Mathematical Society, 1950. Reprinted by Dover Publications, Inc (1966).

[Sch00] E. Schost. *Sur la rsolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.

[SL98] J. Schicho and Z. Li. A construction of radical ideals in polynomial algebra. Technical Report 98-17, RISC-Linz, 1998. `ftp://ftp.risc.uni-linz.ac.at/pub/techreports/1998/98-17.ps.gz`.

[Sza98] A. Szanto. *Computation with polynomial systems*. PhD thesis, Cornell University, 1998.

[Vas98] W. V. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 1998.

[vzGG99] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.

[Wan93] D. Wang. An elimination method for polynomial systems. *Journal of Symbolic Computation*, 16(2):83–114, August 1993.

[Wan98] D. Wang. Decomposing polynomial systems into simple systems. *Journal of Symbolic Computation*, 25(3):295–314, 1998.

[Wan99] D. Wang. *Elimination methods*. Texts and Monographs in Symbolic Computation. Springer-Verlag Wien, 1999.

[Wan00] D. Wang. Computing triangular systems and regular systems. *Journal of Symbolic Computation*, 30(2):221–236, 2000.

[Wu78] W. T. Wu. On the decision problem and the mechanization of theorem-proving in elementary geometry. *Sci. Sinica*, 21(2):159–172, 1978.

[Wu94] W. T. Wu. *Mechanical theorem proving in geometries*. Springer-Verlag, Vienna, 1994. Basic principles, Translated from the 1984 Chinese original by Xiao Fan Jin and Dong Ming Wang.

[Wu00] W. T. Wu. *Mathematics mechanization*. Kluwer Academic Publishers Group, Dordrecht, 2000. Mechanical geometry theorem-proving, mechanical geometry problem-solving and polynomial equations-solving.