J. Symbolic Computation (1999) **28**, 105–124
Article No. jsco.1998.0269
Available online at http://www.idealibrary.com on IDEAL®

On the Theories of Triangular Sets

PHILIPPE AUBRY[†§], DANIEL LAZARD[†¶] AND MARC MORENO MAZA[†‡‖]

[†] *LIP6, Université Paris 6, 4 Place Jussieu 75252 Paris Cedex 05, France*
[‡] *Computational Mathematics Group, NAG Ltd, Jordan Hill Rd, Oxford OX2 8DR, U.K.*

Different notions of triangular sets are presented. The relationship between these notions are studied. The main result is that four different existing notions of *good* triangular sets are equivalent.

1. Introduction

Triangular sets appear under various names in many papers concerning systems of polynomial equations. Ritt (1932) introduced them as characteristic sets. He described also an algorithm for solving polynomial systems by computing characteristic sets of prime ideals and factorizing in field extensions. Characteristic sets of prime ideals have good properties but factorization in algebraic extensions is, most of the time, too costly. In order to avoid factorizations, Wu's algorithm (Wu, 1986, 1987) computes characteristic sets of finite sets of polynomials which do not generate necessarily prime ideals. Wu's algorithm may produce redundant decompositions of varieties and may not discover their possible emptiness. Several authors continued and improved Wu's approach, mainly Chou and Gao (1990, 1991a, 1992), Gallo and Mishra (1990, 1991) and Wang (1992, 1993, 1995).

Kalkbrener (1991) and Yang and Zhang (1994) introduced particular triangular sets, called regular chains. Taking advantage of the good properties of regular chains, Kalkbrener presented also an algorithm for decomposing a variety into unmixed-dimensional non-empty components described as regular chains. In addition, Lazard (1991a) introduced the notion of normalized triangular sets which are special regular chains and he provided a method for uniquely decomposing the solution of a polynomial system as regular zeros of such normalized triangular sets. This avoids the problems resulting from the non-canonicity of Wu's and other decompositions. Following the work of Lazard (1992), an efficient alogrithm for solving zero-dimensional systems by means of normalized triangular sets is reported in Moreno Maza and Rioboo (1995). Wang (1998a) gave a generalization of the notion of a regular chain to pairs of polynomial sets (one set for equations and the other one for inequations) whose union is a triangular set, such pairs being called simple systems. He also presented an algorithm for solving polynomial systems by means of simple systems. The relationships between most of these algorithms and

[§] E-mail: aubry@calfor.lip6.fr
[¶] E-mail: lazard@calfor.lip6.fr
[‖] E-mail: marc@nag.co.uk

0747–7171/99/070105 + 20 $30.00/0

other methods for solving polynomial systems is discussed in the review paper of Lazard (1991b) while an experimental comparison of several methods for computing triangular decompositions is presented in Aubry and Moreno Maza (1997).

On the other hand, it has been remarked for a long time that field extensions of finite type are well represented as towers of simple transcendental or algebraic extensions, themselves represented by triangular sets. As irreducible varieties correspond to field extensions, solving polynomial systems may be viewed as equivalent to find the triangular sets corresponding to the fields associated to the components of the variety.

All these theories are very close together and the situation is rather confusing because many slightly different notions are used under the same (or, on the contrary, completely different) names by various authors. In this paper we are concerned with the clarification of this situation and we think that our main result is a step in this direction. More specifically we study the theoretical relationship between these various approaches to triangular sets, namely *characteristic set* (Ritt, 1932; Wu, 1984a), *regular chain* and *representation of a regular chain* (Kalkbrener, 1991), *tower of simple extensions* (Lazard, 1991a), *regular set* (Moreno Maza, 1997).

One can easily verify that if T is a reduced triangular set contained in a prime ideal $\mathcal{P}$, then the following conditions are equivalent:

(i) T is a regular chain whose representation is $\mathcal{P}$,
(ii) T is a regular set which describes a tower of field extension defining the field associated to $\mathcal{P}$,
(iii) $\mathcal{P}$ is the set of all polynomials reducible to 0 by T,
(iv) T is a Ritt characteristic set of $\mathcal{P}$.

It appears also that an ideal is naturally associated to any triangular set; we call it the saturated ideal. We review or define precisely all the above notions when the saturated ideal is not necessarily prime. We prove their main properties and study the relationship between them. Our main result is that, for a non-empty triangular set T, the following conditions are equivalent:

(i) T is a regular chain,
(ii) T is a regular set, which is the name we give for the generalization of triangular sets defining towers of field extensions,
(iii) the set of all polynomials reducible to 0 by T is the saturated ideal of T,
(iv) T is a Ritt characteristic set of its saturated ideal.

The paper is structured as follows. Section 2 consists mainly of standard preliminaries. In Section 3, we review Ritt characteristic sets and the way they are used in the algorithms of Ritt (1966), and Wu (1987). We also examine the relationship between Ritt characteristic sets and Gröbner bases. In fact Ritt characteristic sets may easily be deduced from lexicographical Gröbner bases. In Section 4, we study properties of regular chains and establish that the ideal associated to a regular chain (namely its representation) is the radical of the saturated ideal of T. In Section 5 we define regular sets and their associated tower of simple extensions. We give an isomorphism which shows the relation between the saturated ideal of a regular set and its tower. The very short Section 6 states precisely the above mentioned main result and proves it as a corollary of the preceding sections. Some natural results which appear in the paper may have been

stated earlier (or may easily be deduced from earlier work) but we have not always found the original sources. For this reason and for an easier reading, several results which are not new are given with self-contained proofs.

2. Preliminaries

2.1. TRIANGULAR SETS

In this section we define our notations related to multivariate polynomials and we recall the most general definition for triangular sets, as in Wang (1993) where they are called *triangular forms*. We present a terminology which is completely different from the one of Gröbner basis theory, even if the notions are similar, in order to avoid confusion when both theories are used simultaneously. Note also that the term of *initial* is standard in differential algebra.

NOTATION 2.1. Let $\mathbf{k}$ be a field and $x_1 < x_2 < \cdots < x_n$ be n ordered variables. For every i in the range $1 \ldots n$ we define $\mathbf{P}_i = \mathbf{k}[x_1, \ldots, x_i]$ to be the ring of multivariate polynomials in the variables $x_1, \ldots, x_i$ with coefficients in $\mathbf{k}$. We also put $\mathbf{P}_0 = \mathbf{k}$. Let $p \in \mathbf{P}_n$ with $p \notin \mathbf{k}$. We write $\mathsf{deg}(p, x_i)$ for the degree of p with respect to x_i.

DEFINITION 2.1. Let $p \in \mathbf{P}_n$ with $p \notin \mathbf{k}$. We call the *main variable* of p, denoted by $\mathsf{mvar}(p)$, the greatest variable $v \in \{x_1, \ldots, x_n\}$ such that $\mathsf{deg}(p, v) \neq 0$. Assuming $\mathsf{mvar}(p) = x_i$, let us regard p as a univariate polynomial in $\mathbf{P}_{i-1}[x_i]$. Thus, we can write $p = c{x_i}^d + r$, where $d = \mathsf{deg}(p, x_i)$, $c \in \mathbf{P}_{i-1}$, $r \in \mathbf{P}_i$ and $r \neq 0 \Rightarrow \mathsf{deg}(r, x_i) < d$. The quantities c, d and r are respectively called the *initial*, the *main degree* and the *tail* of p and denoted by $\mathsf{init}(p)$, $\mathsf{mdeg}(p)$ and $\mathsf{tail}(p)$. Finally, we call the *head* of p, denoted by $\mathsf{head}(p)$, the polynomial $p - \mathsf{tail}(p)$.

EXAMPLE 2.1. Assume $n \geq 3$ and let $p \in \mathbf{P}_n$. If $p = x_1x_3^2 - 2x_2x_3 + 1$, then we have $\mathsf{mvar}(p) = x_3$, $\mathsf{mdeg}(p) = 2$, $\mathsf{init}(p) = x_1$, $\mathsf{tail}(p) = -2x_2x_3 + 1$ and $\mathsf{head}(p) = x_1x_3^2$.

DEFINITION 2.2. A subset T of $\mathbf{P}_n$ is called a *triangular set* if no element of T lies in $\mathbf{k}$ and if for all $p, q \in T$ with $p \neq q$ we have $\mathsf{mvar}(p) \neq \mathsf{mvar}(q)$. A variable $v \in \{x_1, \ldots, x_n\}$ is called *algebraic* w.r.t. T if there exists $p \in T$ such that $v = \mathsf{mvar}(p)$. We denote by $\mathsf{algVar}(T)$ the set of all variables which are algebraic w.r.t. T.

EXAMPLE 2.2. Assume $n \geq 4$. The subset $T_1 = \{x_2^2 - x_1, x_1x_3^2 - 2x_2x_3 + 1, (x_2x_3 - 1)x_4 + x_2^2\}$ of $\mathbf{P}_n$ is a triangular set (whose algebraic variables are x_2, x_3, x_4) whereas the subset $T_2 = \{x_1^2x_2 + 1, x_1x_2^2 - 1\}$ of $\mathbf{P}_n$ is not a triangular set.

EXAMPLE 2.3. Let $p \in \mathbf{P}_n$. Let $\mathsf{iter}(p)$ be the subset of $\mathbf{P}_n$ recursively defined as follows: if $p \in \mathbf{R}$ then $\mathsf{iter}(p) = \emptyset$ otherwise $\mathsf{iter}(p) = \{p\} \cup \mathsf{iter}(\mathsf{init}(p))$.

Then $\mathsf{iter}(p)$ is a triangular set of $\mathbf{P}_n$ whose elements are called the *iterated initials* of p. For instance, with $p = (x_2x_3 - 1)x_4 + x_2^2$ we have $\mathsf{iter}(p) = \{x_2, x_2x_3 - 1, p\}$.

2.2. REDUCED TRIANGULAR SETS

In this section we first recall the partial ordering on the polynomials which is used in various algorithms dealing with triangular sets, and especially in the one of Ritt

(1966) and Wu (1987). The termination of this algorithm is also based on the notion of *reduced triangular sets* (Definition 2.5) called *chains* in Ritt (1966) and *ascending sets* in Wu (1987). To increase the efficiency of the Ritt–Wu algorithm, one may use the weaker notion of *initially reduced triangular sets* instead: see Moreno Maza (1997) for some examples. Moreover, initially reduced triangular sets appear in the output of the algorithm of Lazard (1991a) and Moreno Maza (1997) and in the connection between triangular sets and Gröbner bases (Theorem 3.3).

DEFINITION 2.3. Let $p, q \in \mathbf{P}_n$. We say that p is *smaller than q w.r.t. Ritt ordering* and we write $p \prec_r q$ if one of the following assertions holds:

(i) $p \in \mathbf{k}$ and $q \notin \mathbf{k}$,
(ii) $p, q \notin \mathbf{k}$ and $\mathsf{mvar}(p) < \mathsf{mvar}(q)$,
(iii) $p, q \notin \mathbf{k}$ and $\mathsf{mvar}(p) = \mathsf{mvar}(q)$ and $\mathsf{mdeg}(p) < \mathsf{mdeg}(q)$.

We say that p is *greater than q w.r.t. Ritt ordering* and we write $p \succ_r q$ if $q \prec_r p$. We say that p and q are *not comparable w.r.t. Ritt ordering* and we write $p \sim_r q$ if neither $p \prec_r q$ nor $p \succ_r q$ hold.

REMARK 2.1. For $p \in \mathbf{P}_n$ with $p \notin \mathbf{k}$ we have $\mathsf{init}(p) \prec_r p$ and $\mathsf{tail}(p) \prec_r p$. Note also that every decreasing chain w.r.t. the Ritt ordering starting at p breaks off after finitely many steps.

DEFINITION 2.4. Let $p, q \in \mathbf{P}_n$ with $q \notin \mathbf{k}$. We say that p is *reduced w.r.t. q in Ritt sense* and we write $\mathsf{red?}(p, q)$ if one of the following assertions holds:

(i) $p \prec_r q$,
(ii) $p \notin \mathbf{k}$ and $\mathsf{mvar}(p) > \mathsf{mvar}(q)$ and $\mathsf{red?}(\mathsf{init}(p), q)$ and $\mathsf{red?}(\mathsf{tail}(p), q)$.

For a subset T of $\mathbf{P}_n$ we say that p is *reduced w.r.t. T* and we write $\mathsf{red?}(p, T)$ if for every $t \in T$ the assertion $\mathsf{red?}(p, t)$ holds. We say that p is *initially reduced w.r.t. q* and we write $\mathsf{iRed?}(p, q)$ if one of the following assertions holds:

(i) $p \prec_r q$,
(ii) $p \notin \mathbf{k}$ and $\mathsf{mvar}(p) > \mathsf{mvar}(q)$ and $\mathsf{iRed?}(\mathsf{init}(p), q)$.

For a subset T of $\mathbf{P}_n$ we say that p is *initially reduced w.r.t. T* and we write $\mathsf{iRed?}(p, T)$ if for every $t \in T$ the assertion $\mathsf{iRed?}(p, t)$ holds.

PROPOSITION 2.1. *For $p, q \in \mathbf{P}_n$ with $q \notin \mathbf{k}$, the following assertions are equivalent:*

(i) $\mathsf{red?}(p, q)$,
(ii) $\mathsf{deg}(p, \mathsf{mvar}(q)) < \mathsf{mdeg}(q)$.

PROOF. The result is trivial if $p \prec_r q$. The general case is treated by induction on v^d, where $v = \mathsf{mvar}(p)$ and $d = \mathsf{mdeg}(p)$, using the Ritt ordering (see Remark 2.1).□

NOTATION 2.2. Let T be a triangular set of $\mathbf{P}_n$ and i be an integer in $\{1, \ldots, n\}$. If x_i is an algebraic variable w.r.t. T, we denote by T_{x_i} the polynomial in T whose main variable is x_i. We also define:

$$T_{x_i}^{-} = T \cap \mathbf{P}_{i-1} \qquad \text{and} \qquad T_{x_i}^{+} = \{t \in T \mid \mathsf{mvar}(t) > x_i\}.$$

DEFINITION 2.5. A triangular set T of $\mathbf{P}_n$ is called *reduced* (resp. *initially reduced*) if for every $v \in \mathsf{algVar}(T)$ we have $\mathsf{red?}(T_v,\ T_v^{-})$ (resp. $\mathsf{iRed?}(T_v,\ T_v^{-})$).

EXAMPLE 2.4. Assume $n \geq 4$. The subset T_1 (Example 2.2) of $\mathbf{P}_n$ is an initially reduced triangular set, but it is not reduced because of the tail of the third polynomial. The subset $T_3 = \{x_1(x_1 - 1), x_1^2 x_2 + 1\}$ of $\mathbf{P}_n$ is not initially reduced because of the initial of the second polynomial.

REMARK 2.2. Our notion of reduced triangular set is the same as in Ritt (1966) or Wu (1987). However, our notion of initially reduced triangular set is weaker than Wu's notion of *ascending set in the weak sense*, see p. 6 in Wu (1987). Indeed, a triangular set T has this latter property if for every $t \in T$, the head of t is reduced w.r.t. $T \setminus \{t\}$, whereas we only ask that for each polynomial p in $\mathsf{iter}(t) \setminus \{t\}$ such that there exists $q \in T$ with $\mathsf{mvar}(p) = \mathsf{mvar}(q)$ we have $\mathsf{red?}(p, q)$. Wu remarked that without any notion of reduction, his computations were frequently faster but may not terminate. Our notion of initially reduced triangular guarantees the termination of Wu's algorithm. Moreover, the efficiency of the corresponding implementation compares to the one which does not use any notion of reduction.

On the other hand, for the algorithm of Chou and Gao (1990) and the algorithm of Wang (1993) the following notion of *fine triangular sets*, which is weaker than the one of initially reduced triangular sets, is adequate. Moreover, fine triangular sets are crucial for the main result of this paper (Theorem 6.1).

NOTATION 2.3. Let $p, q \in \mathbf{P}_n$, with $q \notin \mathbf{k}$. We denote by $\mathsf{prem}(p, q)$ and $\mathsf{pquo}(p, q)$ the pseudo-remainder and the pseudo-quotient of p by q when interpreting them as univariate in $\mathsf{mvar}(q)$. Let $T \subseteq \mathbf{P}_n$ be a triangular set. If $T = \emptyset$ we define $\mathsf{prem}(p, T) = p$ otherwise we define $\mathsf{prem}(p, T) = \mathsf{prem}(\mathsf{prem}(p,\ T_v),\ T_v^{-})$ where v is the greatest variable of $\mathsf{algVar}(T)$. For instance, with $T_4 = \{x_1(x_1 - 1), x_1 x_2 - 1\}$ and $p = x_2^2 + x_1 x_2 + x_1^2$, we have

$$\mathsf{prem}(p, T) = \mathsf{prem}(\mathsf{prem}(p,\ T_{x_2}),\ T_{x_1}) = \mathsf{prem}(x_1^4 + x_1^2 + 1,\ T_{x_1}) = 2\ x_1 + 1.$$

DEFINITION 2.6. A triangular set T of $\mathbf{P}_n$ is called *fine* if it is not empty and if for every $v \in \mathsf{algVar}(T)$ we have $\mathsf{prem}(\mathsf{init}(T_v),\ T_v^{-}) \neq 0$.

2.3. SATURATED IDEALS AND REGULAR ZEROS

Triangular sets are deeply involved in polynomial system solving. In methods like those of Wu (1987), Wang (1993), Lazard (1991a) and Moreno Maza (1997), one has to consider

a particular subset of the affine variety associated to a triangular set (on an algebraic closure of $\mathbf{k}$), namely the *set of regular zeros*.

In the method of Kalkbrener, one has to consider a particular ideal associated with a triangular set, namely its *saturated ideal*. This concept of *saturated ideal* associated with a triangular set was first considered in Chou and Gao (1991b). However, the more general concept of *saturated ideal w.r.t. a multiplicatively closed subset of a ring* is standard in commutative algebra, see p. 90 in Bourbaki (1961).

To investigate triangular set properties, we recall these notions in this section.

NOTATION 2.4. For $F \subseteq \mathbf{P}_n$ we denote by $\langle F \rangle$ the ideal of $\mathbf{P}_n$ generated by F and by $\sqrt{\langle F \rangle}$ the radical of $\langle F \rangle$. For $h \in \mathbf{P}_n$ we denote by $\langle F \rangle : h$ the ideal quotient of $\langle F \rangle$ by h (i.e. the set of the polynomials $p \in \mathbf{P}_n$ such that $p\,h \in \langle F \rangle$). Let $T \subseteq \mathbf{P}_n$ be a triangular set. We denote by $\mathsf{red}_{\mapsto 0}(T)$ the subset of $\mathbf{P}_n$ defined as follows:

$$\mathsf{red}_{\mapsto 0}(T) = \{p \in \mathbf{P}_n \mid \mathsf{prem}(p, T) = 0\}.$$

PROPOSITION 2.2. *Let $p \in \mathbf{P}_n$ and $T = \{t_1, \ldots, t_\ell\}$ be a triangular set of $\mathbf{P}_n$. Let c_k be the initial of t_k. Then we have $\mathsf{red?}(\mathsf{prem}(p, T), T)$. Moreover, there exist integers $e_1, \ldots, e_\ell$ and polynomials $q_1, \ldots, q_\ell$ in $\mathbf{P}_n$ such that:*

$$c_1^{e_1} \cdots c_\ell^{e_\ell} p = q_1 t_1 + \cdots + q_\ell t_\ell + \mathsf{prem}(p, T).$$

PROOF. This statement is easily obtained by induction on ℓ and using Proposition 2.1. It appears in Wu (1984a) as the *remainder formula*.□

DEFINITION 2.7. Let $T \subseteq \mathbf{P}_n$ be a non-empty triangular set. Let h be the product of the initials of the polynomials in T. We call the *saturated ideal of T* the ideal of $\mathbf{P}_n$ denoted by $\mathsf{sat}(T)$ and defined as follows:

$$\mathsf{sat}(T) = \{p \in \mathbf{P}_n \mid (\exists n \in \mathbb{N})\ h^n p \in \langle T \rangle\}.$$

If $T = \emptyset$ we set $\mathsf{sat}(T) = \{0\}$.

PROPOSITION 2.3. *For any triangular set $T \subseteq \mathbf{P}_n$ we have:*

$$\mathsf{red}_{\mapsto 0}(T) \subseteq \mathsf{sat}(T).$$

The set $\mathsf{red}_{\mapsto 0}(T)$ is not necessarily an ideal of $\mathbf{P}_n$ and the previous inclusion is not necessarily an equality.

PROOF. The above inclusion is obviously obtained from Proposition 2.2. Let us now give a counter-example illustrating the fact that $\mathsf{red}_{\mapsto 0}(T)$ is not necessarily an ideal of $\mathbf{P}_n$. Assume $n \geq 2$ and consider the following triangular set $T_4 = \{x_1(x_1 - 1), x_1 x_2 - 1\}$. One can check that a lexicographical Gröbner basis of $\mathsf{sat}(T_4)$ is $\{x_1 - 1, x_2 - 1\}$. We define $p = (x_1 - 1)(x_1 x_2 - 1)$ and $q = -(x_1 - 1)x_1 x_2$. We see that $\mathsf{prem}(p, T_4) = \mathsf{prem}(q, T_4) = 0$. But we have $p + q = 1 - x_1$ and thus $(p + q) \notin \mathsf{red}_{\mapsto 0}(T_4)$.□

NOTATION 2.5. Let $\mathbf{K}$ be an algebraic closure of $\mathbf{k}$. For $F \subseteq \mathbf{P}_n$ we denote by $\mathbf{V}(F)$ the affine variety of $\mathbf{K}^n$ associated with F (i.e. the set of the points in $\mathbf{K}^n$ where every polynomial in F vanishes). For $W \subseteq \mathbf{K}^n$ we denote by $\overline{W}$ the Zariski closure of W w.r.t. $\mathbf{k}$ (i.e. the intersection of those $\mathbf{V}(F)$ containing W, for any $F \subseteq \mathbf{P}_n$).

DEFINITION 2.8. Let $T \subseteq \mathbf{P}_n$ be a non-empty triangular set. Let h be the product of the initials of the polynomials in T. We call the *regular zeros of* T the elements of the subset of $\mathbf{V}(T)$ denoted by $\mathbf{W}(T)$ and defined as follows:

$$\mathbf{W}(T) = \mathbf{V}(T) \setminus \mathbf{V}(h).$$

The triangular set T is called *consistent* if $\mathbf{W}(T) \neq \emptyset$, or, in other words, if $h \notin \sqrt{\langle T \rangle}$.

THEOREM 2.1. *For any non-empty triangular set* $T \subseteq \mathbf{P}_n$ *we have:*

$$\overline{\mathbf{W}(T)} = \mathbf{V}(\mathsf{sat}(T)).$$

PROOF. It is clear that $\overline{\mathbf{W}(T)} = \overline{\mathbf{V}(\sqrt{\langle T \rangle}) \setminus \mathbf{V}(h)}$. Thus, by Theorem 7, p. 193, in Cox *et al.* (1992), we have $\overline{\mathbf{W}(T)} = \mathbf{V}(\sqrt{\langle T \rangle} : h)$. Finally, one can check that for any positive integer $k > 0$ we have $\sqrt{\langle T \rangle} : h = \sqrt{\langle T \rangle} : h^k$ and thus $\sqrt{\langle T \rangle} : h = \sqrt{\mathsf{sat}(T)}$.□

3. Characteristic Sets

Ritt (1932) introduced the concept of a characteristic set of a finite or infinite set of differential polynomials; see p. 4 in Ritt (1966). One of his goals was to provide a method to solve systems of differential equations. A byproduct of that work is an algorithm for solving systems of algebraic equations by means of triangular sets, p. 95 in Ritt (1966). More precisely, given a finite subset F of $\mathbf{P}_n$, Ritt's algorithm computes characteristic sets $T_1, \ldots, T_\ell$ of prime ideals such that:

$$\mathbf{V}(F) = \cup_1^\ell \mathbf{W}(T_i).$$

Characteristic sets of prime ideals have good properties (see Theorem 3.3) but Ritt's process involves factorization in field extensions.

Wu (1986, 1987) used Ritt's work to provide an algorithm for solving systems of algebraic equations by means of triangular sets which only requires pseudo-remainder computations (i.e. no factorizations are needed). Wu's process is based on a procedure called CHRST-REM, see p. 3 in Wu (1987). Given a finite subset F of $\mathbf{P}_n$, this procedure computes a characteristic set T of a finite subset G of $\mathbf{P}_n$ such that $\langle F \rangle = \langle G \rangle$. But this T is not necessarily a characteristic set of $\langle F \rangle$. If F generates the unit ideal of $\mathbf{P}_n$, it is not always possible to discover it by using the procedure CHRST-REM. Moreover, the decompositions provided by Wu's algorithm (Wu, 1987) may be redundant. See Chapter 6 in Moreno Maza (1997) for some examples. However, Chou and Gao (1992) proved that Wu's algorithm provides a decomposition of an affine variety into unmixed-dimensional (or empty) components, and provided an algorithm for removing empty components.

Wu used the concept of characteristic set in a more general situation than Ritt did in his algorithm. But Wu did not give a precise definition for his case: in Wu (1987) a characteristic set is the result of algorithm CHRST-REM. The output of this algorithm depends on the ordering in which the input polynomials are being read. Taking into account the way algorithm CHRST-REM works, we propose the Definition 3.1 below for a characteristic set in the sense of Wu.

Wu characteristic set computations are based on Ritt ordering (see Definition 3.2) for reduced triangular sets. In view of our Theorem 6.1 we extend Ritt ordering defined for reduced triangular sets in p. 4 of Ritt (1966) to fine triangular sets. With this modification, we review Ritt definition for characteristic sets of ideals in $\mathbf{P}_n$ (Definition. 3.3) and

their basic properties (Proposition. 3.3, Theorem. 3.1). Until Remark 3.2, the content of this section is standard, but generally stated for reduced characteristic sets (Ritt, 1966), whereas we are concerned here with fine triangular sets. Then, we show how a Ritt characteristic set of an ideal $\mathcal{I}$ can easily be produced from a lexicographical Gröbner basis of $\mathcal{I}$ (Propositions 3.4, 3.5 and Theorem 3.2). Following Ritt (1966) we also investigate the case of prime ideals (Theorem 3.3).

NOTATION 3.1. Throughout this section F will denote a non-empty subset of non-null polynomials of $\mathbf{P}_n$.

DEFINITION 3.1. A non-empty subset T of $\langle F\rangle$ is a *Wu characteristic set* of F if one of the following conditions holds:

(i) $T = \{a\}$ for $a \neq 0$ in $\mathbf{k}$,
(ii) T is a triangular set and there exists a subset G of $\langle F\rangle$ such that $\langle F\rangle = \langle G\rangle$ and $G \subseteq \mathsf{red}_{\mapsto 0}(T)$.

PROPOSITION 3.1. *Let $T = \{t_1, \ldots, t_\ell\}$ be a triangular set of $\mathbf{P}_n$. We denote by c_k the initial of t_k. If T is a Wu characteristic set of F, then we have:*

(i) $\overline{\langle F\rangle} \subseteq \mathsf{sat}(T)$,
(ii) $\overline{\mathbf{W}(T)} \subseteq \mathbf{V}(F) \subseteq \mathbf{V}(T)$,
(iii) $\mathbf{V}(F) = \mathbf{W}(T) \cup \cup_1^l \mathbf{V}(F \cup \{c_k\})$,
(iv) If $\langle F\rangle$ is a prime ideal and if $\mathbf{W}(T) \neq \emptyset$ then we have $\mathbf{V}(F) = \overline{\mathbf{W}(T)}$.

PROOF. Property (i) is deduced from Proposition 2.3. Then, property (ii) results from (i) and Theorem 2.1. As (ii) holds, we clearly have:

$$\mathbf{W}(T) \cup \ \cup_1^l \mathbf{V}(F \cup \{c_k\}) \subseteq \mathbf{V}(F).$$

Conversely, because $\mathbf{W}(T) \subseteq \mathbf{V}(F) \subseteq \mathbf{V}(T)$, if a point $\zeta \in \mathbf{V}(F)$ does not belong to $\mathbf{W}(T)$, then it lies in one of the $\mathbf{V}(F \cup \{c_k\})$. Property (iv) follows easily from (iii).□

REMARK 3.1. Let F and T be as above. The triangular set T may be a Wu characteristic set of F even if F generates the unit ideal of $\mathbf{P}_n$. For instance, choose $F = T_1$ as in Example 2.2. In that case F is a Wu characteristic set of itself but we have $\langle F\rangle = \langle 1\rangle$.

DEFINITION 3.2. Let $T = \{t_1, \ldots, t_\ell\}$ and $S = \{s_1, \ldots, s_k\}$ be two fine triangular sets of $\mathbf{P}_n$. We say that T is *smaller than* S w.r.t. *Ritt ordering* and we write $T \prec_r S$ if one of the following conditions holds:

(i) $(\exists i \in \{1, \ldots, \min(k, \ell)\})\ (\forall j \in \{1, \ldots, i-1\})\ t_j \sim_r s_j$ and $t_i <_r s_i$,
(ii) $\ell > k$ and $(\forall j \in \{1, \ldots, k\})\ t_j \sim_r s_j$.

We say that T is *greater than* S w.r.t. *Ritt ordering* and we write $T \succ_r S$ if $S \prec_r T$. We say that T and S are *not comparable w.r.t. Ritt ordering* and we write $T \sim_r S$ if neither $T \prec_r S$ nor $T \succ_r S$ holds.

PROPOSITION 3.2. *Let $T = \{t_1, \ldots, t_\ell\}$ and $S = \{s_1, \ldots, s_k\}$ be two fine triangular sets of $\mathbf{P}_n$. Then the following assertions hold:*

(i) $T \sim_r S \iff l = k \text{and} (\forall j \in \{1, \ldots, k\}) t_j \sim_r s_j$,
(ii) $(\forall p \in \mathbf{P}_n \setminus \mathbf{k})$ $(\mathsf{red?}(p, T) \text{and} x_i = \mathsf{mvar}(p)) \Longrightarrow T_{x_i}^- \cup \{p\} \prec_r T$.

PROOF. This statement results obviously from Definitions 2.4 and 3.2.□

DEFINITION 3.3. A subset T of F is a *Ritt characteristic set* of F if one of the following conditions holds:

(i) $T = \{a\}$ for $a \neq 0$ in $\mathbf{k}$,
(ii) $F \cap \mathbf{k} \subseteq \{0\}$ and T is a minimal element for $\prec_r$ in $\mathcal{F}$, where $\mathcal{F}$ denotes the set of all fine triangular sets contained in F.

PROPOSITION 3.3. *Let T be a Ritt characteristic set of $\langle F \rangle$. Then T is a Wu characteristic set of F. Moreover, if T is a triangular set, then we have $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$.*

PROOF. The case $T \subset \mathbf{k}$ is trivial. So we assume that T is a triangular set. Thus we have $\langle F \rangle \cap \mathbf{k} = \{0\}$. Let $f \in \langle F \rangle$. We define $r = \mathsf{prem}(f, T)$. From (i) of Proposition 2.2 we get $r \in \langle F \rangle$. Assuming $r \neq 0$, we have $r \notin \mathbf{k}$ and r has a main variable v. From Proposition 3.2 and (ii) of Proposition 2.2 we have:

$$T_v^- \cup \{r\} \prec_r T.$$

This leads to a contradiction and shows that $r = 0$ and $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$.□

THEOREM 3.1. *Let T be a fine triangular set contained in $\langle F \rangle$. Then the following conditions are equivalent:*

(i) T is a Ritt characteristic set of $\langle F \rangle$,
(ii) $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$.

PROOF. From Proposition 3.3 we only need to prove that if T is not a Ritt characteristic set of $\langle F \rangle$ then there exists a polynomial $p \in \langle F \rangle$ such that $\mathsf{prem}(p, T) \neq 0$. Thus we assume that there exists a fine triangular set $S \subseteq \langle F \rangle$ such that $S \prec_r T$. We define $S = \{s_1, \ldots, s_k\}$ and $T = \{t_1, \ldots, t_\ell\}$. If S is not reduced, and because S is a fine triangular set, we can replace s_j by $\mathsf{prem}(s_j, \{s_1, \ldots, s_{j-1}\})$ for j in the range $2 \ldots k$ without violating any of the previous assumptions. We distinguish two cases.

First if $\ell < k$ and for all $j \in \{1, \ldots, \ell\}$ we have $t_j \sim_r s_j$, then let $p = s_{\ell+1}$. Note that $\mathsf{red?}(p, \{s_1, \ldots, s_\ell\})$. As for all $j \in \{1, \ldots, \ell\}$ we have $t_j \sim_r s_j$ we also obtain $\mathsf{red?}(p, \{t_1, \ldots, t_\ell\})$. Now if there exists $i \in \{1, \ldots, \min(k, \ell)\}$ such that $s_i \prec_r t_i$ and for all $j \in \{1, \ldots, i-1\}$ we have $t_j \sim_r s_j$, then let $p = s_i$. As above we have $\mathsf{red?}(p, \{t_1, \ldots, t_{i-1}\})$. As $p \prec_r t_i$ and as for $j \in \{i+1, \ldots, \ell\}$ we have $\mathsf{mvar}(p) \prec_r \mathsf{mvar}(t_j)$, we obtain $\mathsf{red?}(p, \{t_1, \ldots, t_\ell\})$. Finally, in both cases, we have found a polynomial $p \in \langle F \rangle$ such that $\mathsf{prem}(p, T) \neq 0$.□

REMARK 3.2. Computing Wu characteristic sets by means of Wu's procedure CHRST-REM is a hard task on some examples. Thus, in Wang (1992), the following weaker notion is used: a triangular set T contained in $\langle F \rangle$ is called a *medial set* of F if it is not greater w.r.t. Ritt ordering than any characteristic set of F. Of course, a Wu characteristic set of F and thus a Ritt characteristic set of $\langle F \rangle$ are medial sets of F.

3.1. characteristic sets and lexicographical Gröbner bases

NOTATION 3.2. From now on, we assume $\langle F\rangle \neq \mathbf{P}_n$. We define $\mathcal{I} = \langle F\rangle$. Let $\prec_{lex}$ be the lexicographical ordering on the monomials of $\mathbf{P}_n$ w.r.t the ordering $x_1 < \cdots < x_n$. Let $p \in \mathbf{P}_n$. We denote by $\mathsf{lm}(p)$ the leading monomial of p w.r.t. $\prec_{lex}$ and by $\mathsf{lc}(p)$ the corresponding leading coefficient in $\mathbf{k}$. Let G be the minimal Gröbner basis of $\mathcal{I}$ w.r.t. $\prec_{lex}$ such that for every $g \in G$ we have $\mathsf{lc}(p) = 1$. We define $\mathsf{lm}(G) = \{\mathsf{lm}(g) \mid g \in G\}$. Recall that if p lies in $\mathcal{I}$ then there exists $g \in G$ such that $\mathsf{lm}(g)$ divides $\mathsf{lm}(p)$. Let v be a variable in $\{x_1, \ldots, x_n\}$. Now, we define:

$$G_v = \{g \in G \mid \mathsf{mvar}(g) = v\} \qquad \text{and} \qquad G_v^- = \{g \in G \mid \mathsf{mvar}(g) < v\}.$$

Finally, we denote by $\mathsf{algVar}(G)$ the set of those variables v such that $G_v \neq \emptyset$.

DEFINITION 3.4. Let G be as above and let $\mathsf{algVar}(G) = \{y_1, \ldots, y_m\}$ with $y_1 < \cdots < y_m$. We call the *median set of* F and denote by $\mathcal{M}(F)$ the subset of G defined as follows:

(i) if $m = 1$ then $\mathcal{M}(F) = \{g_1\}$ where g_1 is the smallest polynomial in G_{y_1} w.r.t. $\prec_{lex}$,
(ii) if $m > 1$ then defining $T = \mathcal{M}(G_{y_m}^-)$ we distinguish two cases:
  (*a*) if $G_{y_m} \subseteq \mathsf{red}_{\mapsto 0}(T)$ then $\mathcal{M}(F) = T$,
  (*b*) if $G_{y_m} \not\subseteq \mathsf{red}_{\mapsto 0}(T)$ then $\mathcal{M}(F) = T \cup \{g_m\}$ where g_m is the smallest polynomial g in G_{y_m} w.r.t. $\prec_{lex}$ such that $\mathsf{prem}(g, T) \neq 0$.

EXAMPLE 3.1. Assume $n \geq 4$ and define $F = \{x_1x_2, x_2x_3, x_3x_4\}$. Then we have $G = F$ and $\mathcal{M}(F) = \{x_1x_2, x_3x_4\}$.

EXAMPLE 3.2. Assume $n \geq 4$ and define $F = \{x_2^2 - x_1, x_3^2 - 2x_2x_3 + x1, (x_3 - x_2)x_4\}$. Then we have $G = F$ and $\mathcal{M}(F) = G$. Note that $\mathbf{W}(\mathcal{M}(F)) = \emptyset$ because $(x_3 - x_2)$ lies in the radical of $G_{x_4}^-$.

REMARK 3.3. Even if F generates a radical ideal we may have $\mathbf{W}(\mathcal{M}(F)) = \emptyset$. Assume $n \geq 4$ and consider $F = \{x_1^2 - 2, x_2^2 - 2, (x_1 - x_2)x_3, (x_1 + x_2)x_4\}$. In this case we have $G = F \cup \{x_3x_4\}$ and $\mathcal{M}(F) = F$. We easily check that the product of the initials of F_{x_3} and F_{x_4} lies in the ideal generated by $F_{x_3}^-$. In order to avoid $\mathbf{W}(\mathcal{M}(F))$ being empty, one may assume that F generates a prime ideal (see Theorem 3.3).

PROPOSITION 3.4. *The median set $\mathcal{M}(F)$ is a non-empty triangular set such that*

$$\mathcal{M}(F) \subseteq \langle F\rangle \subseteq \mathsf{red}_{\mapsto 0}(\mathcal{M}(F)).$$

PROOF. Let $\mathcal{I}$ and G be as in Notation 3.2 and set $T = \mathcal{M}(F)$. Remark that T is not empty and that the first inclusion is trivial. Let us prove the second one. Suppose that there exists some $p \in \mathcal{I}$ such that $p \notin \mathsf{red}_{\mapsto 0}(\mathcal{M}(F))$. Let $r = \mathsf{prem}(p, T)$. Note that $r \in \mathcal{I}$. Thus, there exists $g \in G$ such that $\mathsf{lm}(r)$ is a multiple of $\mathsf{lm}(g)$. As $\mathsf{red?}(r, T)$ we have also $\mathsf{red?}(\mathsf{lm}(r), T)$ and $\mathsf{red?}(\mathsf{lm}(g), T)$. Let $v = \mathsf{mvar}(g)$. It follows from Definition 3.4 that either $g \in \mathsf{red}_{\mapsto 0}(T_v^-)$, or $g = T_v$, or $\mathsf{lm}(T_v) \prec_{lex} \mathsf{lm}(g)$. As $\mathsf{red?}(\mathsf{lm}(g), T)$ the last two cases are impossible. Suppose that the first one holds. Define $h = \mathsf{init}(g)$. Thus we have $\mathsf{prem}(h, T_v^-) = 0$ and one can check that there exists a polynomial $c \in \mathsf{iter}(h)$ such that $\mathsf{mvar}(c) \in \mathsf{algVar}(T_v^-)$ and $\mathsf{prem}(c, T_v^-) = 0$. Hence c and $\mathsf{lm}(g)$ are not reduced w.r.t. T_v^-. This contradicts Definition 3.4.□

PROPOSITION 3.5. *The median set $\mathcal{M}(F)$ is a fine triangular set.*

PROOF. Let $\mathcal{I}$ and G be as in Notation 3.2 and define $T = \mathcal{M}(F)$. Assume that for some $v \in \mathsf{algVar}(T)$ we have $\mathsf{prem}(\mathsf{init}(g_v), \mathcal{M}(F)) = 0$ and put $r = \mathsf{prem}(\mathsf{tail}(g_v),\ T_v^-)$. Then, one can check that:

$$\mathsf{prem}(g_v,\ T_v^-) = r.$$

As $T_v^- \cup \{g_v\} \subseteq \mathcal{I}$ we get $r \in \mathcal{I}$. Thus, by Proposition 3.4 we have $\mathsf{prem}(r, T) = 0$. As $\mathsf{red?}(r, T)$, in fact we have $r = 0$. Hence $\mathsf{prem}(g_v,\ T_v^-) = 0$. This contradicts the definition of $\mathcal{M}(F)$.□

THEOREM 3.2. *The median set $\mathcal{M}(F)$ is a Ritt characteristic set of $\langle F\rangle$.*

PROOF. This statement results from Theorem 3.1 and Propositions 3.4 and 3.5.□

PROPOSITION 3.6. *The median set $\mathcal{M}(F)$ is initially reduced.*

PROOF. Let $\mathcal{I}$ and G be as in Notation 3.2. We define $T = \mathcal{M}(F)$. Assume that T is not initially reduced. Thus, there exists $v \in \mathsf{algVar}(T)$ such that T_v is not initially reduced w.r.t. T_v^-. We choose v as small as possible. It is clear that $T_v^- \neq \emptyset$. As T is a fine triangular set, we have $\mathsf{prem}(\mathsf{init}(T_v),\ T_v^-) \neq 0$. Then by multiplying T_v by a product of the initials of T_v^- we can compute a polynomial $t \in \mathcal{I}$ such that $\mathsf{mvar}(t) = v$, the polynomial t is reduced w.r.t. T_v^- and $\mathsf{lm}(t) \prec_{lex} \mathsf{lm}(T_v)$. Consequently, due to the definition of T, the monomial $\mathsf{lm}(t)$ can be divided by one of those polynomials $g \in G_v$ such that $\mathsf{prem}(g,\ T_v^-) = 0$. This shows that t is not reduced w.r.t. T_v^- and leads to a contradiction.□

REMARK 3.4. Theorem 3.2 shows that every ideal $\mathcal{I}$ of $\mathbf{P}_n$ possesses a Ritt characteristic set and that such a set is not harder to compute than a lexicographical Gröbner basis of $\mathcal{I}$. Moreover, to check whether a subset C of $\mathcal{I}$ is a Ritt characteristic set of $\mathcal{I}$ it is sufficient to verify that C is a fine triangular set such that $C \sim_r \mathcal{M}(\mathcal{I})$. The following theorem shows that if F generates a prime ideal then $\mathcal{M}(F)$ is consistent and is easier to obtain than in the general case.

NOTATION 3.3. For $v \in \mathsf{algVar}(G)$, if $G_v \neq \emptyset$ we denote by g_v the smallest polynomial in G_v w.r.t. $\prec_{lex}$. We denote by T_G the triangular set whose elements are these polynomials g_v.

THEOREM 3.3. *If F generates a prime ideal in $\mathbf{P}_n$, then we have:*

(i) $\mathcal{M}(F) = T_G$,
(ii) $\langle F\rangle = \mathsf{sat}(\mathcal{M}(F))$,
(iii) $\mathbf{V}(F) = \overline{\mathbf{W}(\mathcal{M}(F))}$,
(iv) $\mathcal{M}(F)$ *is consistent.*

PROOF. Let $\mathcal{I}$ and G be as in Notation 3.2. For convenience, we simply write T instead of T_G. We first prove (i). Let $v \in \mathsf{algVar}(T)$. We shall verify that T_v is initially reduced w.r.t. T_v^-. Let us assume the contrary. So let h be in $\mathsf{iter}(T_v)$ with $w = \mathsf{mvar}(h)$. Let us

assume that $w \in \mathsf{algVar}(\ T_v^-)$ and that h is not reduced w.r.t. T_w. Thus there exist an integer e and two polynomials q and r such that:

$$\mathsf{init}(\ T_w)^e\, h = q\ T_w + r \qquad \text{and} \qquad r \prec_r T_w.$$

If $r = 0$ then $\mathsf{init}(\ T_w)^e h \in \mathcal{I}$. As $\mathcal{I}$ is a prime ideal, either $\mathsf{init}(\ T_w)$ or h would lie in $\mathcal{I}$. This is impossible: G is a minimal Gröbner basis and thus for every $g \in G$, no polynomial in $\mathsf{iter}(\mathsf{init}(g))$ can belong to $\mathcal{I}$. If $r \neq 0$ then we can reduce T_v w.r.t. T_w and obtain a polynomial $t \in \mathcal{I}$ such that $\mathsf{mvar}(t) = v$ and $\mathsf{lm}(t) \prec_{lex} \mathsf{lm}(\ T_v)$. As G is a minimal Gröbner basis of $\mathcal{I}$, and since T_v is the smallest polynomial in G with v as main variable, we are led to another contradiction. This completes the proof of (i). We now prove (ii). From Propositions 3.4 and 2.3 we only need to verify: $\mathcal{I} \supseteq \mathsf{sat}(T)$. Let $p \in \mathsf{sat}(T)$. There exists a product π of the initials of T such that πp lies in the ideal generated by T and thus in $\mathcal{I}$. We have already remarked that no initial of T could lie in $\mathcal{I}$. Thus, as $\mathcal{I}$ is a prime ideal, we have $p \in \mathcal{I}$. Point (iii) follows from (ii) and Theorem 2.1. Finally, point (iv) follows from (iii) because we have assumed $\mathcal{I} \neq \mathbf{P}_n$.□

4. Regular Chains

The concept of a *regular chain* was introduced independently by Yang and Zhang (1994) and Kalkbrener (1991). Regular chains also appear in Chou and Gao (1992). Regular chains are special fine triangular sets which are used by these authors to provide algorithms for computing unmixed-dimensional decompositions of algebraic varieties. Without using factorization, these decompositions have better properties than the ones produced by Wu's algorithm.

Kalkbrenner's original definition was based on the following remark. As every irreducible variety is uniquely determined by one of its generic points, varieties can be represented by describing the generic points of their irreducible components. These generic points are given in Kalkbrener (1991) by regular chains.

As varieties correspond to radical ideals and generic points to prime ideals, varieties can also be represented by describing their associated prime ideals. These associated prime ideals are given by regular chains in Kalkbrener (1998) where regular chains correspond to a particular case of *system of representations*. The Definition 4.1 below follows this second point of view.

Propositions 4.1 and 4.2 give a practical characterization of the *representation of a regular chain*. Propositions 4.3 and 4.4 give practical properties of the radical of the saturated ideal of a regular chain. Finally, Theorem 4.1 states the main result of this section: the representation of a regular chain is the radical of its saturated ideal. This result is close to Lemma 4.3 in Kalkbrener (1998) which is essentially an induction assertion for our theorem. As the context is not exactly the same we provide a self-contained proof.

Notation 4.1. Let $\mathbf{A}$ be a commutative Noetherian ring with units. We denote by $\mathbf{reg}(\mathbf{A})$ the multiplicatively closed subset of $\mathbf{A}$ consisting of the regular elements of $\mathbf{A}$ (i.e. the elements of $\mathbf{A}$ which are not zero-divisors). Then we denote by $\mathbf{fr}(\mathbf{A})$ the total quotient ring of $\mathbf{A}$ (i.e. the ring of fractions with numerators from $\mathbf{A}$ and denominators from $\mathbf{reg}(\mathbf{A})$). Let $\mathcal{I}$ be an ideal of $\mathbf{A}$. We denote by $\mathbf{A}/\mathcal{I}$ the residue class ring of $\mathbf{A}$ by $\mathcal{I}$, we denote by $\sqrt{\mathcal{I}}$ the radical of $\mathcal{I}$ and we denote by $\mathcal{I}[x]$ the ideal generated by $\mathcal{I}$ in $\mathbf{A}[x]$. For $h \in \mathbf{A}$ we denote by $\mathcal{I} : h^\infty$ the saturated ideal of $\mathcal{I}$ w.r.t. h (i.e. the set of the $a \in \mathbf{A}$ such that there exists a non-negative integer e with $h^e\, a \in \mathcal{I}$). For $p \in \mathbf{A}[x]$

we denote by $\overline{p}^{\mathcal{I}}$ the canonical image of p in $\mathbf{fr}(\mathbf{A}/\mathcal{I})[x]$. Finally, for any prime ideal $\mathcal{P}$ associated to $\mathcal{I}$, defining $\kappa = \mathbf{fr}(\ \mathbf{A}/\mathcal{P})$, we will write $\overline{p}^{\kappa}$ for $\overline{p}^{\mathcal{P}}$.

Remark 4.1. The following basic relations and properties will be useful in this section and in the next one. First note that $\sqrt{I[x]} = \sqrt{I}[x]$ and $(\mathcal{I} : h^{\infty})[x] = (\mathcal{I}[x]) : h^{\infty}$. Let $p \in \mathbf{A}[x]$ with $p \notin \mathbf{A}$. The polynomial $\overline{p}^{\mathcal{I}}$ is monic in $\mathbf{fr}(\mathbf{A}/\mathcal{I})[x]$ iff for any prime ideal $\mathcal{P}$ associated to $\mathcal{I}$ the initial of p does not belong to $\mathcal{P}$. See vol. 1, p.214 in Samuel and Zariski (1967). Assume from now on that $\overline{p}^{\mathcal{I}}$ is monic. Then we clearly have $\mathsf{deg}(p, x) = \mathsf{deg}(\overline{p}^{\mathcal{I}}, x)$. Moreover, giving another polynomial $r \in \mathbf{A}[x]$ with $r \notin \mathbf{A}$, if $\mathsf{deg}(r, x) < \mathsf{deg}(p, x)$ because we have $\mathsf{deg}(\overline{r}^{\mathcal{I}}, x) < \mathsf{deg}(\overline{p}^{\mathcal{I}}, x)$.

Example 4.1. Assume $n \geq 3$, let $\mathbf{k} = \mathbb{Q}$ the field of rational numbers. Let $T_5 = \{p_1, p_2\}$ where $p_1 = x_1^4 - 5\ x_1^2 + 6$ and $p_2 = \left(x_1^2 - 2\right)\ x_2^2 + \left(-2\ x_1^3 + 4\ x_1\right)\ x_2 + x_1^4 - 2\ x_1^2$. Let $\mathcal{I}$ be the ideal generated by T_5 in $\mathbf{P}_n$. We have the following primary decomposition:

$$\mathcal{I} = \langle x_1^2 - 3, (x_2 - x_1)^2 \rangle\ \cap\ \langle x_1^2 - 2 \rangle.$$

Thus the associated prime ideals of $\mathcal{I}$ are $\mathcal{P}_1 = \langle x_1^2 - 3, (x_2 - x_1) \rangle$ and $\mathcal{P}_2 = \langle x_1^2 - 2 \rangle$ so that we have $\sqrt{\mathcal{I}} = \mathcal{P}_1\ \cap\ \mathcal{P}_2$. Hence the associated fields of $\mathcal{I}$ are

$$\kappa_1 = \mathbf{fr}(\mathbb{Q}[x_1, x_2]/\mathcal{P}_1) = \mathbb{Q}(\sqrt{3}) \qquad \text{and} \qquad \kappa_2 = \mathbf{fr}(\mathbb{Q}[x_1, x_2]/\mathcal{P}_2) = \mathbb{Q}(\sqrt{2})(x_2).$$

Now let $p_3 = (x_1^2 - 2)\ x_3^4 + (x_2 - x_1)\ x_3^3 + (1 - x_1)\ x_3 + 1$ and put $h = \mathsf{init}(p_3)$. We have $\overline{h}^{\kappa_1} = 1$ and $\overline{h}^{\kappa_2} = 0$. This shows that $\overline{p}^{\mathcal{I}}$ is not monic in $\mathbf{fr}(\mathbf{A}/\mathcal{I})[x]$.

Notation 4.2. Let T be a triangular set of $\mathbf{P}_i$ and let $j \in \{1, \ldots, i\}$. From now on $\mathsf{Rep}_j(T)$ will denote an ideal of $\mathbf{P}_j$ and we define $\mathsf{Rep}_0(T) = \{0\}$. Then $\mathcal{K}_j(T)$ will denote the set of all fields $\kappa = \mathbf{fr}(\mathbf{P}_j/\mathcal{P})$, where $\mathcal{P}$ is a prime ideal associated to $\mathsf{Rep}_j(T)$. Finally we denote by $\mathsf{sat}_j(T)$ the saturated ideal of $T \cap \mathbf{P}_j$ in $\mathbf{P}_j$. Note from Remark 4.1 that if $x_i \notin \mathsf{algVar}(T)$ then we have $\mathsf{sat}_i(T) = \mathsf{sat}_{i-1}(T)[x_i]$.

Definition 4.1. We say that T is a *regular chain* in $\mathbf{P}_i$ whose *representation* is $\mathsf{Rep}_i(T)$ if one of the following conditions holds:

(i) $i = 0$ and the set T is empty,
(ii) $i > 0$, the set $T_{x_i}^{-}$ is a regular chain of $\mathbf{P}_{i-1}$ whose representation is $\mathsf{Rep}_{i-1}(T)$ such that one of both assertions holds:

(a) $x_i \notin \mathsf{algVar}(T)$ and for every $p \in \mathbf{P}_i$ we have:

$$p \in \mathsf{Rep}_i(T) \iff (\forall \kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^{-}))\ \ \overline{p}^{\kappa} = 0,$$

(b) $x_i \in \mathsf{algVar}(T)$, and for every $\kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^{-})$ we have $\overline{\mathsf{init}(\ T_{x_i})}^{\kappa} \neq 0$ and for every $p \in \mathbf{P}_i$ we have:

$$p \in \mathsf{Rep}_i(T) \iff (\forall \kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^{-}))\ \ \overline{p}^{\kappa} \in \sqrt{\langle\ \overline{T_{x_i}}^{\kappa} \rangle}.$$

Example 4.2. Assume $n \geq 3$ and let p_1, p_2, p_3 be as in Example 4.1. The set $\{p_1\}$ is clearly a regular chain in $\mathbf{P}_n$ whose representation is $\langle p_1 \rangle$. However, $\{p_1, p_2\}$ is not a regular chain in $\mathbf{P}_n$ because $\mathsf{init}(p_2)$ vanishes w.r.t. one of the prime ideals associated to

$\langle p_1 \rangle$. The two sets $C_1 = \{x_1^2 - 3, (x_2 - x_1)^2\}$ and $C_2 = \{x_1^2 - 2\}$ are regular chains whose representations are respectively $\mathcal{P}_1$ and $\mathcal{P}_2$. The set $C_1 \cup \{p_3\}$ is a regular chain because $\overline{h}^{\kappa_1} = 1$ where $h = \mathsf{init}(p_3)$ and its representation is $\langle x_1^2 - 3, x_2 - x_1, (x_3^2 - x_1)\ (x_3^2 + 1) \rangle$.

PROPOSITION 4.1. *Let T be a regular chain in $\mathbf{P}_i$. Then we have*

$$x_i \notin \mathsf{algVar}(T) \Longrightarrow \mathsf{Rep}_i(T) = \sqrt{\mathsf{Rep}_{i-1}(T)}[x_i].$$

PROOF. Let $p \in \mathbf{P}_i$ and let $\kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^-)$. The relation $\overline{p}^{\kappa} = 0$ means that every coefficient of p as a univariate polynomial in $\mathbf{P}_{i-1}[x_i]$ is null in κ. Thus $f \in \mathsf{Rep}_i(T)$ means that every coefficient of p as a univariate polynomial in $\mathbf{P}_{i-1}[x_i]$ lies in every prime ideal associated to $\mathsf{Rep}_{i-1}(T)$. Finally, the statement results from the fact that $\sqrt{\mathsf{Rep}_{i-1}(T)}$ is the intersection of the prime ideals associated to $\mathsf{Rep}_{i-1}(T)$.□

PROPOSITION 4.2. *Let T be a regular chain in $\mathbf{P}_i$. Then we have*

$$x_i \in \mathsf{algVar}(T) \quad \Longrightarrow \quad \mathsf{Rep}_i(T) = \{p \in \mathbf{P}_i \mid (\exists m \geq 0)\ \mathsf{prem}(p^m,\ T_{x_i}) \in \mathsf{Rep}_i(\ T_{x_i}^-)\}.$$

PROOF. Let $p \in \mathbf{P}_i$. We define $t = \ T_{x_i}$ and $h = \mathsf{init}(t)$. Let $e \geq 0$ be an integer. We define $r_e = \mathsf{prem}(p^e, t)$. Let δ_e be a non-negative integer and let $q_e \in \mathbf{P}_i$ such that:

$$h^{\delta_e} p^e = q_e t + r_e. \tag{4.1}$$

We first assume that $p \in \mathsf{Rep}_i(T)$. We prove that there exists an integer $m \geq 0$ such that $r_m \in \mathsf{Rep}_i(\ T_{x_i}^-)$. Let $\kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^-)$. By point (b) of Definition 4.1 there exists an integer $m \geq 0$ such that $(\overline{p}^{\kappa})^m$ lies in the ideal generated by $\overline{t}^{\kappa}$. By choosing an m big enough, we can take the same integer m for every prime ideal $\mathcal{P}$ associated to $\mathsf{Rep}_{i-1}(\ T_{x_i}^-)$. With the relation (4.1) we see that $\overline{r_m}^{\kappa}$ lies in the ideal generated by $\overline{t}^{\kappa}$. By Remark 4.1 it follows that $\overline{r_m}^{\kappa} = 0$. In the same way as in the proof of Proposition 4.1 we obtain:

$$r_m \in \sqrt{\mathsf{Rep}_{i-1}(\ T_{x_i}^-)}[x_i].$$

Finally, from the statement of the same proposition we are led to $r_m \in \mathsf{Rep}_i(\ T_{x_i}^-)$. Conversely, assume that there exists an integer $m \geq 0$ such that $r_m \in \mathsf{Rep}_i(\ T_{x_i}^-)$. We prove that $p \in \mathsf{Rep}_i(T)$. Let $\kappa \in \mathcal{K}_{i-1}(\ T_{x_i}^-)$. As $\overline{r_m}^{\kappa} = 0$, with the above relation (4.1), we see that $\overline{h^{\delta_m} p^m}^{\kappa} \in \langle \overline{t}^{\kappa} \rangle$. By point (b) of Definition 4.1, the element $\overline{h^{\delta_m}}^{\kappa}$ is invertible. Then it follows that $\overline{p}^{\kappa}$ lies in the radical of $\langle \overline{t}^{\kappa} \rangle$. Finally we obtain $p \in \mathsf{Rep}_i(T)$.□

PROPOSITION 4.3. *Let T be a non-empty triangular set of $\mathbf{P}_i$ with $x_i \in \mathsf{algVar}(T)$ and let $r \in \mathbf{P}_i$. We define $t = \ T_{x_i}$. We assume that the following assertions hold:*

(i) for every prime ideal $\mathcal{P}$ associated to $\mathsf{sat}_{i-1}(\ T_{x_i}^-)$ we have $\mathsf{init}(t) \notin \mathcal{P}$,
(ii) $r \in \mathsf{sat}_i(T)$,
(iii) $\mathsf{deg}(r, x_i) < \mathsf{mdeg}(t)$.

Then we have $r \in \sqrt{\mathsf{sat}_i(\ T_{x_i}^-)}$.

PROOF. We define $h = \mathsf{init}(t)$. We distinguish two cases. First we assume that $T_{x_i}^- = \emptyset$. From hypothesis (ii), there exists an integer $\delta \geq 0$ such that t divides $h^{\delta} r$. From hypothesis (iii), and because we are working in the integral domain $\mathbf{P}_{i-1}[x_i]$ we obtain

$r = 0$, which proves our claim. Now let us assume that $T_{x_i}^- \neq \emptyset$. We denote by h' the product of the initials of the polynomials in $T_{x_i}^-$. From hypothesis (ii), there exists an integer $\delta \geq 0$ and $q \in \mathbf{P}_i$ such that $(hh')^\delta r + qt$ lies in the ideal generated by $T_{x_i}^-$ in $\mathbf{P}_i$. Let $\mathcal{P}$ be a prime ideal associated to $\mathsf{sat}_{i-1}(T_{x_i}^-)$ and put $\kappa = \mathbf{fr}(\mathbf{P}_{i-1}/\mathcal{P})$. It is a classical remark that $h' \notin \mathcal{P}$. Thus, by hypothesis (i), the element $\overline{hh'}^\kappa$ is invertible. Therefore $\overline{t}^\kappa$ divides $\overline{r}^\kappa$. As we are working with univariate polynomials with coefficients in a field, hypothesis (iii) yields $\overline{r}^\kappa = 0$. Finally, the statement follows from Remark 4.1.□

PROPOSITION 4.4. *Let T be a non-empty triangular set of $\mathbf{P}_i$ with $x_i \in \mathsf{algVar}(T)$ and let $p \in \mathbf{P}_i$. We define $t = T_{x_i}$. We assume that for every prime ideal $\mathcal{P}$ associated to $\mathsf{sat}_{i-1}(T_{x_i}^-)$ we have $\mathsf{init}(t) \notin \mathcal{P}$. Then the following conditions are equivalent:*

(i) $p \in \sqrt{\mathsf{sat}_i(T)}$,
(ii) $(\exists m \geq 0) \mid \mathsf{prem}(p^m, t) \in \sqrt{\mathsf{sat}_i(T_{x_i}^-)}$.

PROOF. We first prove that $(i) \Rightarrow (ii)$. Let $m \geq 0$ be an integer such that $p^m \in \mathsf{sat}_i(T)$. As $t \in \mathsf{sat}_i(T)$, we clearly have $\mathsf{prem}(p^m, t) \in \mathsf{sat}_i(T)$. Then Proposition 4.3 applies with $r = \mathsf{prem}(p^m, t)$ and we obtain (ii). We now prove $(ii) \Rightarrow (i)$. Let $m \geq 0$ be an integer such that $\mathsf{prem}(p^m, t)$ lies in the radical of $\mathsf{sat}_i(T_{x_i}^-)$. If $T_{x_i}^-$ is empty we easily obtain (i). So we assume $T_{x_i}^- \neq \emptyset$. We denote by h' the product of the initials of the polynomials in $T_{x_i}^-$. There exists an integer $\delta \geq 0$ and $q \in \mathbf{P}_i$ such that $h^\delta p^m = qt + \mathsf{prem}(p^m, t)$. Let $\mathcal{I}$ be the ideal generated by T in $\mathbf{P}_i$. From (ii) we deduce $\mathsf{prem}(p^m, t) \in \sqrt{\mathcal{I} : h'^\infty}$. As $qt \in \mathcal{I}$ we obtain $h^\delta p^m \in \sqrt{\mathcal{I} : h'^\infty}$. As $\mathsf{sat}_i(T) = \mathcal{I} : (hh')^\infty$, it is easy to check that $p \in \sqrt{\mathsf{sat}_i(T)}$ and this completes the proof.□

THEOREM 4.1. *Let T be a regular chain in $\mathbf{P}_i$. Then we have*

$$\mathsf{Rep}_i(T) = \sqrt{\mathsf{sat}_i(T)}.$$

PROOF. We first assume $i = 0$. According to Definition 4.1, we have $T = \emptyset$ and $\mathsf{Rep}_i(T) = \{0\}$. On the other hand, from Definition 2.7, we have $\mathsf{sat}_i(T) = \{0\}$. As $\mathbf{P}_i$ is an integral domain, the result is obvious in that case. Now let $i > 0$. As $T_{x_i}^-$ is a regular chain, we can assume that the theorem is true for $i - 1$. If $x_i \notin \mathsf{algVar}(T)$, then the equality easily follows from Proposition 4.1, Remark 4.1 and the final remark in Notation 4.2. We now assume $x_i \in \mathsf{algVar}(T)$. From Proposition 4.2, we have

$$\mathsf{Rep}_i(T) = \{p \in \mathbf{P}_i \mid (\exists m \geq 0)\ \mathsf{prem}(p^m,\ T_{x_i}) \in \mathsf{Rep}_i(T_{x_i}^-)\}.$$

As $x_i \notin \mathsf{algVar}(T_{x_i}^-)$, we obtain from the previous case

$$\mathsf{Rep}_i(T_{x_i}^-) = \sqrt{\mathsf{sat}_i(T_{x_i}^-)}.$$

Finally, the conclusion follows from Proposition 4.4.□

PROPOSITION 4.5. *If T is a regular chain in $\mathbf{P}_i$, then T is consistent.*

PROOF. From Theorems 2.1 and 4.1, and from Hilbert theorem of zeros we only need to prove that $\mathsf{Rep}_i(T) \neq \mathbf{P}_i$. It follows from Propositions 4.1 and 4.2 that $1 \in \mathsf{Rep}_i(T)$ iff $1 \in \mathsf{Rep}_{i-1}(\ T^-_{x_i})$. Thus, as the statement is clear for $i = 0$, it also holds for any i.□

5. Towers of Simple Extensions

The notion of tower of simple extensions presented in this section generalize the usual notion of tower of field extensions. Towers of simple extensions and regular chains will appear in the final section as equivalent notions (Theorem 6.1). Moreover, the former concept is useful to present Lazard triangular sets (Lazard, 1991a) in a simple way. It is also convenient for presenting computations with multivariate polynomials modulo a regular chain as computations with univariate polynomials, especially when working with Lazard triangular sets (Moreno Maza, 1997).

Let us give first an idea of this notion, before introducing a precise definition (Definition 5.2). Given a tower of simple extensions, for $i = 1 \ldots n-1$, if $\mathbf{A}_{i-1}$ is a *floor* in this tower, the next floor $\mathbf{A}_i$ is built by applying one of the following rules:

(i) $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i])$,
(ii) there exists a non-constant and monic $t_i \in \mathbf{A}_{i-1}[x_i]$ such that $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i]/\langle t_i \rangle)$.

As $\mathbf{A}_0 = \mathbf{k}$, if each t_i is irreducible as a polynomial in $\mathbf{A}_{i-1}[x_i]$ then $\mathbf{A}_n$ is a field and there exists a prime ideal $\mathcal{P}$ in $\mathbf{P}_n$ such that $\mathbf{A}_n$ and $\mathbf{fr}(\mathbf{P}_n/\mathcal{P})$ are isomorphic. Conversely, let $\mathcal{P}$ be a prime ideal in $\mathbf{P}_n$ and let $\mathbf{A}_i = \mathbf{fr}(\mathbf{P}_i/\mathbf{P}_i \cap \mathcal{P})$. If ξ_i is the image of x_i in $\mathbf{A}_i$, then $\mathbf{A}_i = \mathbf{A}_{i-1}(\xi_i)$ is a simple field extension. Thus, there is a one-to-one correspondence between towers of field extensions (of $\mathbf{k}$ with n floors) and prime ideals (of $\mathbf{P}_n$). Therefore varieties can be represented by describing the towers of field extensions of their irreducible components. These towers of field extension are given in Lazard (1991a) by Lazard triangular sets.

More generally, Theorem 6.1 will state that towers of (ring) simple extension correspond to regular chains. In order to show it, we need to introduce an intermediate concept, namely the concept of a *regular set*. Regular sets are special fine triangular sets which naturally encode towers of simple extensions. Note that each one of the above t_i can be viewed as a polynomial in $\mathbf{P}_{i-1}[x_i]$ and that the set of the t_i is a triangular set.

Definition 5.1 presents the inverse construction: from a suitable triangular set to a tower of simple extensions. Proposition 5.1 is an important step to establish Theorem 6.1: it states that if T is a regular set in $\mathbf{P}_n$ then $\mathsf{sat}(T)$ and $\mathsf{red}_{\mapsto 0}(T)$ are the same objects. Finally, the main result of this section is Theorem 5.1: it can be viewed as an analogous result of Theorem 4.1 but stated for regular sets.

The results of this section appear in Moreno Maza (1997) and Proposition 5.1 is also established in Wang (1998b).

NOTATION 5.1. Let $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n$ be commutative rings with units such that $\mathbf{k} = \mathbf{A}_0$ and $\mathbf{A}_{i-1}$ is a sub-ring of $\mathbf{A}_i$ for $i \in \{1, \ldots, n\}$. Let x_{n+1} be an additional variable and put $\mathbf{P}_{n+1} = \mathbf{k}[x_1, \ldots, x_{n+1}]$. Let F_0 be the identity map of $\mathbf{P}_1$. Finally, for $i \in \{1, \ldots, n\}$, let F_i be an algebra homomorphism from $\mathbf{P}_{i+1}$ onto $\mathbf{A}_i[x_{i+1}]$ such that $F_i(x_{i+1}) = x_{i+1}$.

DEFINITION 5.1. Let T be a triangular set of $\mathbf{P}_i$. The set T is a *regular set* of $\mathbf{P}_i$ whose *associated map* is $(F_0, \ldots, F_i)$ and whose *associated tower of simple extensions* is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ if one of the following conditions holds:

(i) $i = 0$ and the set T is empty,
(ii) $i > 0$, the set $T_{x_i}^-$ is a regular set of $\mathbf{P}_{i-1}$ whose associated map is $(F_0, \ldots, F_{i-1})$ and whose associated tower of simple extensions is $(\mathbf{A}_0, \ldots, \mathbf{A}_{i-1})$ such that one of the two assertions holds:
   (*a*) $x_i \notin \mathsf{algVar}(T)$ and we have $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i])$ and for every $p \in \mathbf{P}_i$, the element $F_i(p)$ is the canonical image of $F_{i-1}(p)$ in $\mathbf{A}_i$,
   (*b*) $x_i \in \mathsf{algVar}(T)$, the element $F_{i-1}(\mathsf{init}(T_{x_i}))$ is a unit in $\mathbf{A}_{i-1}$, and we have $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i]/\langle t_i \rangle)$ and, for every $p \in \mathbf{P}_i$, the element $F_i(p)$ is the canonical image of $\overline{F_{i-1}(p)}^{\langle t_i \rangle}$ in $\mathbf{A}_i$ where t_i denotes $F_{i-1}(T_{x_i})$.

DEFINITION 5.2. The sequence $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ is called a *tower of simple extensions* of $\mathbf{k}$ (t.o.s.e. for short) if there exists a regular set of $\mathbf{P}_i$ whose associated tower of simple extensions is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$.

EXAMPLE 5.1. Assume $n \geq 4$. The subset T_1 (Example 2.2) is not a regular set of $\mathbf{P}_n$ whereas $T_{x_4}^-$ is one: as $F_2(T_{x_3}) = (x_1x_3 - 1)^2$ the element $F_2(\mathsf{init}(T_{x_4})) = (x_1x_3 - 1)$ is nilpotent in $\mathbf{A}_3$ where $(\mathbf{A}_0, \ldots, \mathbf{A}_n)$ denotes the associated t.o.s.e. of $T_{x_4}^-$.

REMARK 5.1. Let $T \subseteq \mathbf{P}_i$ be a regular set whose associated t.o.s.e. is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ and whose associated map is $(F_0, \ldots, F_i)$. For $0 \leq j \leq i$ and $x \in \mathbf{A}_j$, note that x is either a unit in $\mathbf{A}_j$ or a zero-divisor in $\mathbf{A}_j$. Moreover, if $j < i$ and if x is a unit in $\mathbf{A}_j$ then it is also a unit in $\mathbf{A}_{j+1}$. Proposition 5.2 characterizes the units of $\mathbf{A}_i$ whereas Proposition 5.1 characterizes the kernel of F_i, and, consequently the zero-divisors of $\mathbf{A}_i$.

PROPOSITION 5.1. *Let $T \subseteq \mathbf{P}_i$ be a regular set whose associated t.o.s.e. is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ and whose associated map is $(F_0, \ldots, F_i)$. Then, for every $p \in \mathbf{P}_i$ the following three conditions are equivalent:*

(i) $F_i(p) = 0$,
(ii) $\mathsf{prem}(p, T) = 0$,
(iii) $p \in \mathsf{sat}_i(T)$.

PROOF. We prove that the above assertions are equivalent by induction on i. We first assume $i = 0$. By virtue of Definition 5.1, we have $F_0(p) = 0 \iff p = 0$. Moreover, we have $T = \emptyset$ and thus $\mathsf{prem}(p, T) = 0 \iff p = 0$. On the other hand, we have $\mathsf{sat}_0(T) = \{0\}$ from Definition 2.7. It follows that the result is obvious in this case. Now let $i > 0$. As $T_{x_i}^-$ is a regular set, we can assume that the result is true for $i - 1$.

Following Definition 5.1, we distinguish two cases: $x_i \notin \mathsf{algVar}(T)$ and $x_i \in \mathsf{algVar}(T)$. First we assume $x_i \notin \mathsf{algVar}(T)$. From Definition 5.1, we obviously have

$$F_i(p) = 0 \iff F_{i-1}(p) = 0.$$

Regarding p as a univariate polynomial in $\mathbf{P}_{i-1}[x_i]$, we obtain by the induction hypothesis

$$F_{i-1}(p) = 0 \iff p \in \mathsf{sat}_{i-1}(\ T^-_{x_i})[x_i] \iff \mathsf{prem}(p,\ T^-_{x_i}) = 0.$$

As $\mathsf{sat}_i(T) = \mathsf{sat}_{i-1}(T)[x_i]$ we obtain the desired result.

Now we assume $x_i \in \mathsf{algVar}(T)$. We define $t = T_{x_i}$, $h = \mathsf{init}(t)$ and $r = \mathsf{prem}(p, t)$. From Definition 5.1 and Remark 5.1 the element $F_i(h)$ of $\mathbf{A}_i$ is a unit and we have $F_i(t) = 0$. Thus we easily obtain

$$F_i(p) = 0 \iff F_i(r) = 0.$$

From Definition 5.1 we have

$$F_i(r) = 0 \iff F_{i-1}(r) \in \langle F_{i-1}(t)\rangle.$$

As $\mathsf{deg}(r, x_i) < \mathsf{mdeg}(t)$ and since $F_{i-1}(t)$ is monic, we obtain from Remark 4.1

$$F_i(r) = 0 \iff F_{i-1}(r) = 0.$$

Regarding r as a univariate polynomial in $\mathbf{P}_{i-1}[x_i]$, we obtain by the induction hypothesis

$$F_{i-1}(r) = 0 \iff r \in \mathsf{sat}_{i-1}(\ T^-_{x_i})[x_i] \iff \mathsf{prem}(r,\ T^-_{x_i}) = 0.$$

As $\mathsf{prem}(p, T) = \mathsf{prem}(r,\ T^-_{x_i})$ we easily obtain

$$F_i(p) = 0 \iff \mathsf{prem}(p, T) = 0.$$

Thus, we have by Proposition 2.3

$$F_i(p) = 0 \Longrightarrow p \in \mathsf{sat}_i(T).$$

Conversely, assume $p \in \mathsf{sat}_i(T)$. We denote by h' the product of the initials of the polynomials in $T^-_{x_i}$. Thus there exists an integer $m \geq 0$ such that $(hh')^m p \in \langle T\rangle$. From Remark 5.1 the element $F_i(hh')$ is a unit in $\mathbf{A}_i$. Moreover, we have $(\forall t \in T)F_i(t) = 0$. Finally, we obtain

$$p \in \mathsf{sat}_i(T) \Longrightarrow F_i(p) = 0. \qquad \square$$

THEOREM 5.1. *Let $T \subseteq \mathbf{P}_i$ be a regular set whose associated t.o.s.e. is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ and whose associated map is $(F_0, \ldots, F_i)$. Then we have*

$$\mathbf{A}_i \cong \mathbf{fr}(\mathbf{P}_i/\mathsf{sat}_i(T)).$$

PROOF. If $i = 0$ the result is trivial. So, we assume $i > 0$. Recall that F_{i-1} is a surjective algebra homomorphism from $\mathbf{P}_i$ onto $\mathbf{A}_{i-1}[x_i]$ such that $F_{i-1}(x_i) = x_i$. From Proposition 5.1 we know that for $p \in \mathbf{P}_{i-1}$ we have

$$F_{i-1}(p) = 0 \iff p \in \mathsf{sat}_{i-1}(\ T^-_{x_i}).$$

Thus, the kernel of F_{i-1} is $\mathsf{sat}_{i-1}(\ T^-_{x_i})[x_i]$ and we have

$$\mathbf{A}_{i-1}[x_i] \cong \mathbf{P}_i/(\mathsf{sat}_{i-1}(\ T^-_{x_i})[x_i]).$$

If $x_i \notin \mathsf{algVar}(T)$, we know that $\mathsf{sat}_{i-1}(\ T^-_{x_i})[x_i] = \mathsf{sat}_i(T)$. Moreover, from Definition 5.1, we have $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i])$ Thus we obtain the desired isomorphism. The same conclusion easily follows if $x_i \in \mathsf{algVar}(T)$.□

PROPOSITION 5.2. *Let $T \subseteq \mathbf{P}_i$ be a regular set whose associated t.o.s.e. is $(\mathbf{A}_0, \ldots, \mathbf{A}_i)$ and whose associated map is $(F_0, \ldots, F_i)$. Let p be an element of $\mathbf{P}_i$. Then $F_i(p)$ is a unit in $\mathbf{A}_i$ iff for every prime ideal $\mathcal{P}$ associated to $\mathsf{sat}_i(T)$ we have $p \notin \mathcal{P}$.*

PROOF. From Remark 5.1 we know that $F_i(p)$ is a unit in $\mathbf{A}_i$ iff it is not a zero-divisor in $\mathbf{A}_i$. From Theorem 5.1 $F_i(p)$ is a zero-divisor in $\mathbf{A}_i$ iff the class of p in $\mathbf{P}_i/\mathsf{sat}_i(T)$ is a zero-divisor. Thus the statement follows from the following classical remark. For an ideal $\mathcal{I}$ in a Noetherian ring $\mathbf{A}$, for $x \in \mathbf{A}$, the class of x in $\mathbf{A}/\mathcal{I}$ is a zero-divisor iff there exists a prime ideal $\mathcal{P}$ associated with $\mathcal{I}$ such that x belongs to $\mathcal{P}$. See vol.1, p.214 in Samuel and Zariski (1967).□

6. The Main Result

THEOREM 6.1. *For any non-empty triangular set $T \subseteq \mathbf{P}_n$ the following four conditions are equivalent:*

(i) T *is a regular chain in* $\mathbf{P}_i$,
(ii) T *is a regular set in* $\mathbf{P}_i$,
(iii) $\mathsf{red}_{\mapsto 0}(T) = \mathsf{sat}_i(T)$,
(iv) T *is a Ritt characteristic set of* $\mathsf{sat}_i(T)$.

PROOF. From Proposition 5.2 and Theorem 4.1 we easily obtain $(i) \iff (ii)$. From Proposition 5.1 we have $(ii) \Rightarrow (iii)$. We now prove $(iii) \iff (iv)$. From Theorem 3.1 we have $(iv) \iff \mathsf{sat}_i(T) \subseteq \mathsf{red}_{\mapsto 0}(T)$. Thus together with Proposition 2.3 we obtain $(iii) \iff (iv)$. Finally we prove $(iii) \Rightarrow (ii)$. We assume that (iii) holds and that (ii) does not. We can assume that $T^-_{x_i}$ is a regular set in $\mathbf{P}_{i-1}$ and that T is not a regular set in $\mathbf{P}_i$. So let $(\mathbf{A}_0, \ldots, \mathbf{A}_{i-1})$ be the associated t.o.s.e. of $T^-_{x_i}$ and let $(F_0, \ldots, F_{i-1})$ be its associated map. We define $t = T_{x_i}$ and $h = \mathsf{init}(t)$. Thus we assume that $F_{i-1}(h)$ is a zero-divisor in $\mathbf{A}_{i-1}$. In other words, there exists $p \in \mathbf{P}_{i-1}$ such that $F_{i-1}(hp) = 0$ and $F_{i-1}(p) \neq 0$. From Proposition 5.1 we obtain

$$hp \in \mathsf{sat}_{i-1}(\ T^-_{x_i}) \qquad \text{and} \qquad \mathsf{prem}(p,\ T^-_{x_i}) \neq 0.$$

We define $r = \mathsf{prem}(p,\ T^-_{x_i})$. Note that we also have $hr \in \mathsf{sat}_{i-1}(\ T^-_{x_i})$ and then $r \in \mathsf{sat}_i(T)$. Consequently we have found a polynomial $r \in \mathbf{P}_{i-1}$ such that

$$r \in \mathsf{sat}_i(T) \qquad \text{and} \qquad r \notin \mathsf{red}_{\mapsto 0}(T).$$

This contradicts (iii).□

Acknowledgements

We would like to thank Dongming Wang, Mike Dewar and the referees for their helpful suggestions on an earlier version of this paper. The third author is also grateful to the European research project FRISCO † for supporting his work.

†A Framework for Integrated Symbolic/Numeric Computation. Esprit Scheme Project No. 21 024.

References

Aubry, P., Moreno Maza, M. (1997). Triangular sets for solving polynomial systems: a comparative implementation of four methods. *J. Symb. Comput.*, **28** 125–154

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the radical of a finitely generated differential ideal. In *Proceedings of ISSAC'95, Montréal, Canada*, pp. 158–166.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1997). Computing representations for radicals of finitely generated differential ideals. Technical Report, ref. IT–306, Université Lille I, 59655, Villeneuve d'Ascq, France.

Bourbaki, N. (1961). *Algèbre Commutative*, chapter 2. Paris, Herman.

Chou, S., Gao, X. (1990). Ritt–Wu's decomposition algorithm and geometry theorem proving. In *Proceedings CADE-10, Kaiserslautern, Germany,* pp. 202–220.

Chou, S., Gao, X. (1991a). Computations with parametric equations. In *Proceedings ISAAC'91, Bonn, Germany*, pp. 122–127.

Chou, S., Gao, X. (1991b). On the dimension of an arbitrary ascending chain. *Chin. Bull. Sci.*, **38**, 799–804.

Chou, S., Gao, X. (1992). Solving parametric algebraic systems. In *Proceedings ISAAC'92, Berkeley, CA*, pp. 335–341.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms*. New York, Springer-Verlag.

Gallo, G., Mishra, B. (1990). Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proceedings MEGA'90*, pp. 119–142.

Gallo, G., Mishra, B. (1991). Wu–Ritt characteristic sets and their complexity. In Goodman, J.E., Pollack, R. and Steiger, W., eds, *Discrete and Computational Geometry: Papers from the DIMACS Special Year*, volume 6, *Dimacs Series in Discrete Mathematics and Theoretical Computer Science*, pp. 111–136. American Mathematical Society and Association for Computing Machinery.

Kalkbrener, M. (1991). Three contributions to elimination theory. Ph.D. Thesis, Johannes Kepler University, Linz.

Kalkbrener, M. (1993). A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comput.*, **15**, 143–167.

Kalkbrener, M. (1998). Algorithmic properties of polynomial rings. *J. Symb. Comput.*, **26**, 525–581.

Lazard, D. (1991a). A new method for solving algebraic systems of positive dimension. *Discrete Appl. Math.*, **33**, 147–160.

Lazard, D. (1991b). Systems of algebraic equations (algorithms and complexity). In Eisenbud, D. and Robbiano, L., eds, *Cortona Proceedings*. Cambridge, Cambridge University Press.

Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symb. Comput.*, **15**, 117–132.

Moreno Maza, M. (1997). Calculs de Pgcd au-dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques. Ph.D. Thesis, Université Paris 6.

Moreno Maza, M., Rioboo, R. (1995). Polynomial gcd computations over towers of algebraic extensions. In Cohen G., Giusti M. and Mora T., eds, *Proceedings AAECC-11*, pp. 365–382. Berlin, Springer.

Ritt, J. (1932). *Differential Equations from an Algebraic Standpoint*, volume 14. New York, American Mathematical Society.

Ritt, J. (1966). *Differential Algebra*. New York, Dover Publications.

Samuel, P., Zariski, O. (1967). *Commutative Algebra*. D. Van Nostrand Company.

Wang, D. M. (1992). Some improvements on Wu's method for solving systems of algebraic equations. In Wen-Tsün, W. and Min-De, C., eds, *Proc. of the Int. Workshop on Math. Mechanisation, Beijing, China*. Institute of Systems Science, Academia Sinica.

Wang, D. M. (1993). An elimination method for polynomial systems. *J. Symb. Comput.*, **16**, 83–114.

Wang, D. M. (1995). An implementation of the characteristic set method in Maple. In Pfalzgraf, J. and Wang, D. M., eds, *Automated Practical Reasoning: Algebraic Approaches*, pp. 187–201. Wien, Springer.

Wang, D. M. (1998a). Decomposing polynomial systems into simple systems. *J. Symb. Comput.*, **25**, 295–314.

Wang, D. M. (1998b). *Elimination Methods*. Springer-Verlag, Wien, Springer-Verlag (in press).

Wu, W. T. (1984a). Basic principles of mechanical theorem proving in elementary geometries. *J. Syst. Sci. Math. Sci.*, **4**, 207–235.

Wu, W. T. (1984b). Some recent advances in mechanical theorem-proving of geometries. In Bledsoe, W. W. and Loveland, P.W., eds, *Automated Theorem Proving: After 25 Years*. Providence, RI, American Mathematical Society, pp. 235–241.

Wu, W. T. (1986). On zeros of algebraic equations—an application of Ritt principle. *Kexue Tongbao*, **31**, 1–5.

Wu, W. T. (1987). A zero structure theorem for polynomial equations solving. *MM Research Preprints*, **1**, 2–12.

Yang, L., Zhang, J. (1994). Searching dependency between algebraic equations: an algorithm applied to automated reasoning. In Johnson, J., McKee, S. and Vella, A., eds, *Artificial Intelligence in Mathematics*, pp. 147–156. Oxford, Oxford University Press.