Elimination theory in codimension one and applications

Laurent Busé

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Elimination theory in codimension one and applications

Laurent Busé

N° ????

June 2006

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--????--FR+ENG

Elimination theory in codimension one and applications

Laurent Busé

Thème SYM — Systèmes symboliques
Projet Galaad

Rapport de recherche n° ???? — June 2006 — 47 pages

Abstract: In these notes, we present a general framework to compute the codimension one part of the elimination ideal of a system of homogeneous polynomials. It is based on the computation of the so-called MacRae's invariants that we will obtain by means of determinants of complexes. Our approach mostly uses tools from commutative algebra. We begin with some basics on elimination theory and then introduce the MacRae's invariant and the so-called determinants of complexes. The rest of these notes illustrates our approach through two important examples: the Macaulay's resultant of n homogeneous polynomials in n variables and the computation of an implicit equation of a parameterized hypersurface using syzygies.

Key-words: Elimination theory, homogeneous polynomial systems, resultants, determinants of complexes, computational algebra, implicitization of rational hypersurfaces.

Notes of lectures given at the CIMPA-UNESCO-IRAN school in Zanjan, Iran, July 9-22 2005.

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : +33 4 92 38 77 77 — Télécopie : +33 4 92 38 77 65

Théorie de l'élimination en codimension un et applications

Résumé : Dans ces notes, nous présentons une approche algébrique pour calculer la partie de codimension un d'un idéal d'élimination d'un système de polynômes homogènes. Elle repose principalement sur le calcul d'invariants dits de MacRae que nous obtiendrons en termes de déterminants de complexes. Dans un premier temps des résultats essentiels de la théorie de l'élimination sont rappelés puis les invariants de MacRae et les déterminants de complexes sont introduits. Le reste de ces notes illustre cette approche au travers de deux exemples: le résultant de Macaulay de n polynômes homogènes en n variables puis le calcul de l'équation implicite d'une hypersurface paramétrée en utilisant les syzygies de cette paramétrisation.

Mots-clés : Théorie de l'élimination, systèmes de polynômes homogènes, résultants, déterminants de complexes, calcul formel, implicitation d'hypersurfaces rationnelles.

In these notes, we present a general framework to compute the codimension one part of the elimination ideal of a system of homogeneous polynomials. It is based on the so-called MacRae's invariants that can be obtained by means of determinants of complexes. Our approach mostly uses tools from commutative algebra and is inspired by the works of Jean-Pierre Jouanolou [22, 23, 25] (see also [31] for a similar point of view).

We begin with some basics on elimination theory. Then, in section 2, we introduce the MacRae's invariant and the so-called determinants of complexes that will allow us to compute this invariant. The rest of these notes illustrates our approach through two examples: the Macaulay's resultant of n homogeneous polynomials in n variables and the computation of an implicit equation of a parameterized hypersurface using syzygies. The first one is treated in section 3 where we follow the monograph [22]. The second one, treated in section 4, report on joint works with Marc Chardin and Jean-Pierre Jouanolou [7, 4, 8]. All along the way, we will recall some tools from commutative algebra and algebraic geometry which may be useful for other purposes.

Contents

Throughout these notes, all rings will be assumed to be non-trivial commutative rings with an identity element.

1 General framework

Let A be a ring. We consider the graded polynomial ring $A[X_1,\ldots,X_n]$, with $\deg(X_i)=1$ for all i, and denote by $\mathfrak{m}$ its irrelevant homogeneous ideal $\mathfrak{m}:=(X_1,\ldots,X_n)$. We suppose given a finitely generated homogeneous ideal $I:=(f_1,\ldots,f_r)\subset\mathfrak{m}$ of $A[X_1,\ldots,X_n]$ and put $B:=A[\mathbf{X}]/I$ which is naturally a graded $A[\mathbf{X}]$-module (the grading is with respect to the variables $X_1,\ldots,X_n$).

Observe that $f_1,\ldots,f_r$ are polynomials in the variables $X_1,\ldots,X_n$ with coefficients in the ring A. Thus, A may be seen as the ring of the parameters of the polynomial system $f_1=\cdots=f_r=0$ from which we want to *eliminate* the variables $X_1,\ldots,X_n$. With a geometric point of view, we consider the incidence scheme (remember that B is graded w.r.t. the X_i's)

$$\mathrm{Proj}(B)\subset\mathbb{P}^{n-1}_A:=\mathrm{Proj}(A[X_1,\ldots,X_n])$$

(this A-schemes inclusion is induced by the surjective map $A[X_1,\ldots,X_n]\to B$) and want to "compute" the image of its canonical projection on $\mathrm{Spec}(A)$. It turns out that this image is closed and has a natural scheme structure (see e.g. [13, §V.1.1]); its definition ideal is

$$\begin{aligned}
\mathfrak{A} &:= \mathrm{Ker}\left(A=\Gamma(\mathrm{Spec}(A),\mathcal{O}_{\mathrm{Spec}(A)})\xrightarrow{can}\Gamma(\mathrm{Proj}(B),\mathcal{O}_{\mathrm{Proj}(B)})\right)\subset A\\
&= \mathrm{Ker}\left(A\to\prod_{i=1}^{n}B_{(X_i)}\right)\\
&= \{s\in A:\exists k\in\mathbb{N}\text{ such that }\mathfrak{m}^k s=_B 0\}=(I:_{A[\mathbf{X}]}\mathfrak{m}^\infty)\cap A\\
&= (I:_{A[\mathbf{X}]}\mathfrak{m}^\infty)_0=H^0_{\mathfrak{m}}(B)_0.
\end{aligned}$$

(the second equality is because a section $s\in\Gamma(\mathrm{Proj}(B),\mathcal{O}_{\mathrm{Proj}(B)})$ is uniquely determined by its restrictions to all the open sets $D^+(X_i)$, $i=1,\ldots,n$). Recall that

$$H^0_{\mathfrak{m}}(B):=\bigcup_{k\in\mathbb{N}}(0:_B\mathfrak{m}^k)=\{P\in B:\exists k\in\mathbb{N}\text{ such that }\mathfrak{m}^kP=0\}. \tag{1.1}$$

All these considerations can be summarized in the following famous

Theorem 1.1 (Elimination theorem) *Let $\mathbb{K}$ be a field and suppose given a ring morphism $\rho:A\to\mathbb{K}$ (often called a specialization map). Then, the following statements are equivalent:*

(i) $\rho(\mathfrak{A})=0$.

(ii) *There exists an extension $\mathbb{L}$ of $\mathbb{K}$ (i.e. $\mathbb{L}$ is both a $\mathbb{K}$-algebra and a field) and a non-trivial zero*[1] *of I in $\mathbb{L}^n$.*

[1] A zero of the ideal I in $\mathbb{K}^n$ is an element $\xi\in\mathbb{K}^n$ such that $\phi(P)(\xi)=0$ for all $P\in I$, where $\phi:=\rho\otimes_A A[\mathbf{X}]:A[\mathbf{X}]\to\mathbb{K}[\mathbf{X}]$ is the extension of the map ρ to polynomials in the X_i's. The element $(0,\ldots,0)\in\mathbb{K}^n$ is called the trivial zero, since it is always a zero of I in $\mathbb{K}^n$ as soon as I is graded and $\rho(I\cap A)=0$. We straightforwardly extend these notations to any extension field $\mathbb{L}$ of $\mathbb{K}$ using the inclusion $\mathbb{K}\subset\mathbb{L}$.

(iii) *The ideal I possesses a non-trivial zero in $\overline{\mathbb{K}}^n$, where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$.*

Proof. This relatively old result has become an elementary result of the schemes theory; see e.g. [17, chapter II, theorem 4.9]. A more classical proof can be found in [16]. □

Therefore, we deduce that *the elimination process which we consider consists in the computation of the 0^{th} graded part of the 0^{th} local cohomology module of B.*

Observe that $(I : \mathfrak{m}^\infty)/I \simeq H^0_{\mathfrak{m}}(B)$ through the canonical map $A[\mathbf{X}] \to B$, and therefore that this local cohomology module is linked to the *saturation* of the ideal I (our system of polynomial equations) w.r.t. the ideal generated by the variables $X_1, \ldots, X_n$ we would like to eliminate. By the way, we recall that $\mathrm{Proj}(B) = \mathrm{Proj}(B/H^0_{\mathfrak{m}}(B))$ (which is easily seen in the open sets $D^+_{X_i}$, $i = 1, \ldots, n$): $B/H^0_{\mathfrak{m}}(B)$ is called the saturated module of B.

We now turn to a description of $\mathfrak{A}$ in terms of annihilators. For all couple $(\nu, t) \in \mathbb{N}^2$ we define the A-linear map

$$\Theta_{\nu,t} : B_\nu \to \mathrm{Hom}_A(B_t, B_{t+\nu}) : b \mapsto (c \mapsto b.c).$$

By (1.1), it follows immediately that for all $\nu \in \mathbb{N}$ we have

$$H^0_{\mathfrak{m}}(B)_\nu = \bigcup_{t \in \mathbb{N}} \mathrm{Ker}(\Theta_{\nu,t}). \tag{1.2}$$

Moreover, for all $(\nu, t) \in \mathbb{N}^2$ we have $\mathrm{Ker}(\Theta_{\nu,t}) \subset \mathrm{Ker}(\Theta_{\nu,t+1})$. Indeed, the multiplication $B_1 \otimes B_n \to B_{n+1}$ being surjective, if $b \in \mathrm{Ker}(\Theta_{\nu,t})$ then $b.c = 0$ for all $c \in B_{t+1+\nu}$ since $c = c_1 \otimes c_n$ and $bc_n = 0$ by hypothesis.

Therefore, noting that $\mathrm{ann}_A(B_t) = \mathrm{Ker}(\Theta_{0,t})$ for all $t \in \mathbb{N}$ (remember that $A \cap I = 0$ which implies that $B_0 = A$), we obtain that

$$\mathfrak{A} := H^0_{\mathfrak{m}}(B)_0 = \bigcup_{t \geq 0} \mathrm{ann}_A(B_t). \tag{1.3}$$

where $\mathrm{ann}_A(B_t) \subset \mathrm{ann}_A(B_{t+1})$ for all $t \in \mathbb{N}$. Thus, it would be very useful to know if this ascending chain of annihilators stops at some point (which is automatic if A is noetherian) and especially at which level.

Proposition 1.2 *Let $\eta \in \mathbb{N}$ be such that $H^0_{\mathfrak{m}}(B)_\eta = 0$. Then, for all integer $t \geq 0$ we have*

$$\mathrm{ann}_A(B_\eta) = \mathrm{ann}_A(B_{\eta+t}) = H^0_{\mathfrak{m}}(B)_0 =: \mathfrak{A}.$$

Proof. Let $(\nu, t) \in \mathbb{N}^2$. It is easy to check that if $a \in \mathrm{ann}_A(B_{\nu+t})$ then $aB_\nu \subset \mathrm{Ker}(\Theta_{\nu,t})$. In particular, since we know that $\mathrm{ann}_A(B_\nu) \subset \mathrm{ann}_A(B_{\nu+t})$, the equality $\mathrm{Ker}(\Theta_{\nu,t}) = 0$ implies that $\mathrm{ann}_A(B_\nu) = \mathrm{ann}_A(B_{\nu+t})$. But by hypothesis $H^0_{\mathfrak{m}}(B)_\eta = 0$. Therefore $\mathrm{Ker}(\Theta_{\eta,t}) = 0$ for all $t \in \mathbb{N}$ by (1.2), which concludes the proof with (1.3). □

This proposition shows that once the smallest integer η such that $H^0_{\mathfrak{m}}(B)_\eta = 0$ (such an integer is often called the saturation index of B) is computed, then the eliminant ideal $\mathfrak{A}$ is nothing but $\mathrm{ann}_A(B_\eta)$. In the case where this ideal is principal, then one can get both η and $\mathrm{ann}_A(B_\eta)$ from a finite free resolution of B: the purpose of these notes is to present and illustrate such a technique, providing on the way the necessary tools.

2 The MacRae's invariant

Let A be a ring. The MacRae's invariant, that will be denoted $\mathfrak{S}(M)$, of a A-module M under suitable assumptions is constructed as an ideal of A which describes the codimension one part of the support of M. It first appears in this form in [29]. In our (quick!) exposition we will mainly follow the very nice treatment given by Northcott in [30] for the existence and properties of this interesting invariant. To compute it, we will use a technique which goes back to Cayley and is called nowadays the *determinant of a complex*. We will follow notes from Demazure [11] for this point, but this subject has been treated in different places and at different levels: see for instance [14, 15], or [23] and [27] for very general settings.

2.1 Notation and preliminaries

2.1.1 The Fitting invariants.

If $\phi : F \to G$ is a map of free A-modules, then the ideal $\det_\nu(\phi)$, where $\nu \in \mathbb{Z}$, is the image of the map $\wedge^\nu F \otimes \wedge^\nu G^* \to A$ induced by $\wedge^\nu \phi$ (where G^* stands for the dual module of G, i.e. $\mathrm{Hom}_A(G, A)$). Choosing bases for the free modules F and G, then ϕ is represented by a matrix and we see that $\det_\nu(\phi)$ is generated by the determinants of all the $\nu \times \nu$-minors of this matrix, its so-called ν^{th} determinantal ideal. Hereafter we make the convention that the 0×0-matrix has determinant 1; this implies in particular that $\det_\nu(\phi) = A$ for all $\nu \leq 0$.

Proposition 2.1 *Let M be a finitely generated A-module and let $\phi : F \to G \to M \to 0$ and $\phi' : F' \to G' \to M \to 0$ be two finite free presentations of M. Then, for all $\nu \in \mathbb{N}$ we have*

$$\det_{\mathrm{rank}(G)-\nu}(\phi) = \det_{\mathrm{rank}(G')-\nu}(\phi').$$

Proof. See [30, §3.1] and [12, §20.2]. □

We can thus define the following invariants of a finitely generated A-module:

Definition 2.2 *Let M be a finitely generated A-module. Then, by choosing any presentation $\phi : F \to G \to M \to 0$ of M, we define, for all $i \in \mathbb{N}$, the ν^{th} Fitting invariant of M to be the ideal*

$$\mathfrak{F}_\nu(M) := \det_{\mathrm{rank}(G)-\nu}(\phi).$$

The Fitting invariant $\mathfrak{F}_0(M)$ will be often denoted $\mathfrak{F}(M)$ and called the initial Fitting invariant of M.

Here are some useful properties of these invariants:

Proposition 2.3 *Let M be a finitely generated A-module.*

(i) *The fitting invariants of M form an increasing sequence*

$$\mathfrak{F}(M) := \mathfrak{F}_0(M) \subseteq \mathfrak{F}_1(M) \subseteq \mathfrak{F}_2(M) \subseteq \dots$$

Furthermore, if M can be generated by q elements, then $\mathfrak{F}_q(M) = A$.

(ii) *Given any map $A \to R$ of rings, we have, for all $\nu \in \mathbb{N}$,*

$$\mathfrak{F}_\nu(M \otimes_A R) = (\mathfrak{F}_\nu(M))R.$$

(iii) *For every $\nu \in \mathbb{N}^*$ we have $\operatorname{ann}(M)\mathfrak{F}_\nu(M) \subseteq \mathfrak{F}_{\nu-1}(M)$. Moreover, if M can be generated by q elements, then*

$$\operatorname{ann}(M)^q \subseteq \mathfrak{F}(M) \subseteq \operatorname{ann}(M).$$

(iv) *If M is finitely presented[2], then each of its Fitting invariants is a finitely generated ideal of A.*

Proof. Again, we refer the reader to [30, §3.1] and [12, §20.2]. □

We end this paragraph with the very useful McCoy's lemma:

Lemma 2.4 (McCoy) *Let $\phi : M \to N$ be a morphism between two finite free A-modules of rank m and n respectively. Then ϕ is injective if and only if $0 :_A \det_m(\phi) = 0$. Moreover, when this is the case we have $m \leq n$.*

Proof. See [30, theorem 6 and 8] or [36, theorem A.6.3]. □

2.1.2 The Euler characteristic.

As we will see, this invariant has the property, among many others, to characterize those A-modules which have trivial annihilators.

Proposition 2.5 *Let M be a A-module. Given two finite free resolutions of M*

$$0 \to F_n \to F_{n-1} \to \dots \to F_1 \to F_0 \to M \to 0,$$
$$0 \to F'_m \to F'_{m-1} \to \dots \to F'_1 \to F'_0 \to M \to 0,$$

[2] We will say that a A-module M is finitely presented if it is finitely generated and if its first module of syzygies is also finitely generated.

we have

$$\sum_{i=0}^{n}(-1)^i \mathrm{rank}(F_i) = \sum_{j=0}^{m}(-1)^j \mathrm{rank}(F'_j).$$

In particular, if $0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to 0$ *is an exact sequence of finite free modules then* $\sum_{i=0}^{n}(-1)^i \mathrm{rank}(F_i) = 0$.

Proof. See [30, chapter 2, theorem 19 and 20]. The last point follows immediately from the first one by taking $M = 0$. □

Definition 2.6 *Let* M *be a* A*-module admitting a finite free resolution*

$$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0.$$

Then we define the Euler Characteristic *of* M *as*

$$\mathrm{Char}(M) := \sum_{i=0}^{n}(-1)^i \mathrm{rank}(F_i).$$

The Euler characteristic of M is always a non-negative integer [30, §4.3]. The following theorem, due to Vasconcelos, characterizes those modules for which the Euler Characteristic has the value zero (modules which will be of particular interest for us, as we will see later on).

Theorem 2.7 *Let* M *be a* A*-module having a finite free resolution of finite length. Then, the Euler characteristic of* M *is a non-negative integer and*

(i) $\mathrm{Char}(M) > 0$ *if and only if* $\mathrm{ann}_A(M) = 0$,

(ii) $\mathrm{Char}(M) = 0$ *if and only if* $\mathrm{ann}_A(M) \neq 0$ *if and only if* $0 :_A \mathrm{ann}_A(M) = 0$.

Proof. See [34] for the original proof or [30, chapter 4, theorem 12]. Note that, in the case where A is noetherian, the point (ii) is also equivalent to the fact that $\mathrm{ann}_A(M)$ contains a non-zero divisor. □

2.2 Definition and properties

We are now ready to define the MacRae's invariant of a A-module M having a finite free resolution of finite length and Euler characteristic zero. We start with the particular case of interest where M have a finite free resolution of length one.

Lemma 2.8 *Let* M *be a* A*-module having a finite free resolution of length one,*

$$0 \to F_1 \to F_0 \to M \to 0, \tag{2.1}$$

and Euler characteristic zero. Then the initial Fitting ideal $\mathfrak{F}(M)$ *is a principal ideal generated by a non-zero-divisor, that is to say* $0 :_A \mathfrak{F}(M) = 0$.

Proof. By hypothesis we have $r := \mathrm{rank}(F_1) = \mathrm{rank}(F_0)$ and $\mathfrak{F}(M)$ is obviously a principal ideal: choosing bases for F_1 and F_0 respectively, $\mathfrak{F}(M)$ is generated by the determinant of the matrix of the map $F_1 \to F_0$ in these bases. Then the rest of the lemma is a consequence of the McCoy's lemma 2.4. □

Following Northcott [30], let us call *elementary modules* those modules satisfying the hypotheses of the above lemma. The initial Fitting ideal of such modules is thus an invertible integral ideal[3] generated by a non-zerodivisor. We will call it the MacRae's invariant of M and will denote it by $\mathfrak{S}(M)$. Observe that if A is a graded ring, M is a graded A-module and (2.1) a graded free resolution, then $\mathfrak{S}(M)$ is an homogeneous ideal and we have graded isomorphisms (of degree zero)

$$\mathfrak{S}(M) \simeq \bigwedge^{\max} F_0^* \otimes_A \bigwedge^{\max} F_1 \simeq A(-d)$$

where d denotes the degree of the determinant of the map $F_1 \to F_0$ and $\bigwedge^{\max}(-)$ denotes the highest non-zero exterior power.

Suppose now given a A-module M such that there exists an exact sequence of finite length

$$0 \to K_n \to K_{n-1} \to \cdots \to K_1 \to K_0 \to M \to 0$$

where the A-modules K_i, $i = 0, \ldots, n$, are all elementary; we will refer to such sequences as *finite elementary resolutions* of M. Then we associate it the invertible fractional ideal

$$\mathfrak{S}(M) := \prod_{i=0}^{n} \mathfrak{F}(K_i)^{(-1)^i} = \mathfrak{F}(K_0)\mathfrak{F}(K_1)^{-1}\mathfrak{F}(K_2)\mathfrak{F}(K_3)^{-1}\ldots$$

and call it the MacRae's invariant of M. Observe that this notation encapsulates correctly the case where M is itself an elementary module, since $0 \to M = M \to 0$ is then an elementary resolution of M. Moreover, as indicated by the notation, the formation of $\mathfrak{S}(M)$ does not depend on the choice of the finite elementary resolution. This and two other properties of the MacRae's invariant are gathered in the following proposition.

Proposition 2.9 *Let M be a A-module having a finite elementary resolution. Then, we have the following properties :*

[3] Let S be the multiplicative closed subset of the ring A whose elements are the non-zerodivisors of A and set $Q = A_S$, the full ring of fractions of A (if A is a domain, then $Q := \mathrm{Frac}(A)$). We recall that a *fractional ideal* of A is a A-submodule I of Q such that there exists a non-zerodivisor $a \in A$ with the property $aI \subset A$ and an *integral ideal* of A is just an ordinary ideal of A (a fractional ideal with $a = 1_A$). Moreover, a fractional ideal I is said to be *invertible* is there exists a fractional ideal J such that $IJ = JI = A$. If such an ideal J exists, then it is unique and denoted by I^{-1}. For example, if a is a non-zerodivisor of A, then aA is an invertible fractional (even integral) ideal whose inverse if $a^{-1}A$.

(i) *Suppose given two finite elementary resolutions of* M*:*

$$0 \to K_n \to K_{n-1} \to \cdots \to K_1 \to K_0 \to M \to 0$$
$$0 \to L_m \to L_{m-1} \to \cdots \to L_1 \to L_0 \to M \to 0.$$

Then, we have the equality

$$\prod_{i=0}^{n} \mathfrak{F}(K_i)^{(-1)^i} = \prod_{j=0}^{m} \mathfrak{F}(L_i)^{(-1)^i}.$$

(ii) *If we have an exact sequence* $0 \to M' \to M \to M'' \to 0$ *of* A*-modules, where* M' *and* M'' *have also finite elementary resolutions, then* $\mathfrak{S}(M) = \mathfrak{S}(M')\mathfrak{S}(M'')$.

(iii) *Let* S *be a multiplicative closed subset of* A*. Then the* A_S*-module* M_S *has an finite elementary resolution and* $\mathfrak{S}(M)A_S = \mathfrak{S}(M_S)$.

(iv) The fractional ideal $\mathfrak{S}(M)$ *of* A *is actually an integral ideal of* A*. Moreover, it is a principal ideal generated by a non-zerodivisor such that* $\mathfrak{F}(M) \subseteq \mathfrak{S}(M)$ *and it is the smallest one with this property: if* I *is a principal ideal of* A *such that* $\mathfrak{F}(M) \subseteq I$*, then* $\mathfrak{S}(M) \subseteq I$.

Proof. See [30, §3.6 and §6.2]. □

Remark 2.10 *Note that the property (iv) implies that any generator of the MacRae's invariant of* M *may serve as a* greatest common divisor *(gcd for short) of any set of generators of the initial Fitting invariant of* M*. In particular, when* A *is UFD,* $\mathfrak{S}(M)$ *is generated by the gcd of a set of generators of* $\mathfrak{F}(M)$.

The property of admitting a finite elementary resolution for a A-module may seem quite intricate. The following result links this property to the existence of the much more commonly used finite free resolutions.

Proposition 2.11 *If* M *is an* A*-module, then the three following statements are equivalent:*

(i) M *admits a finite elementary resolution.*

(ii) M *admits a finite free resolution and* $\mathrm{Char}(M) = 0$.

(iii) M *admits a finite free resolution and* $\mathrm{ann}(M)$ *contains a non-zero divisor.*

Proof. We refer the reader to [30, chapter 3, theorem 23]. Note that the equivalence between (ii) and (iii) is given by theorem 2.7. Moreover, in the following section we will show, with a constructive approach, that (ii) implies (i); this is the only result that we will use in the sequel of these notes. □

As a consequence of this proposition, *the MacRae's invariant of a A-module M admitting a finite free resolution and having Euler characteristic zero is defined* in an obvious way (by taking an elementary resolution). In the following section we will see how we can effectively compute this MacRae's invariant from such a finite free resolution.

2.3 A constructive approach

From now on, we assume that the ring A *is a domain* and we suppose given a A-module M which admits a finite free resolution of length $n \geq 1$

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \to F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0 \tag{2.2}$$

and such that $\mathrm{Char}(M) = \sum_{i=0}^{n}(-1)^i r_i = 0$, where we put $r_i := \mathrm{rank}(F_i)$ for all $i = 0, \ldots, n$. We decompose the complex $F_\bullet$ from the left to the right as follows.

We put $F_n^{(1)} = F_n$ and $F_n^{(0)} = 0$. Since the map $\phi_n : F_n \to F_{n-1}$ is injective, we deduce from the McCoy's lemma that

- F_{n-1} splits into $F_{n-1}^{(0)} \oplus F_{n-1}^{(1)}$ where these two free modules have rank r_n and $r_{n-1} - r_n$ respectively,
- the matrix of ϕ_n is of the form $\begin{pmatrix} c_n \\ d_n \end{pmatrix}$ with $\det(c_n) \neq 0$.

Now, since the restricted map c_n is bijective over $\mathrm{Frac}(A)$ and since $\mathrm{Im}(d_n) = \mathrm{Ker}(d_{n-1})$, we deduce that

- F_{n-2} splits into $F_{n-2}^{(0)} \oplus F_{n-2}^{(1)}$ where these two free modules have rank $r_{n-1} - r_n$ and $r_{n-2} - r_{n-1} + r_n$ respectively,
- the matrix of ϕ_{n-1} is of the form $\begin{pmatrix} a_{n-1} & c_{n-1} \\ b_{n-1} & d_{n-1} \end{pmatrix}$ with $\det(c_{n-1}) \neq 0$.

We can continue this way and obtain, for all $i = 0, \ldots, n$, that

- F_i splits into $F_i^{(0)} \oplus F_i^{(1)}$ where these two free modules have rank $\sum_{j=0}^{n-i-1}(-1)^j r_{i+1+j}$ and $\sum_{j=0}^{n-i}(-1)^j r_{i+j}$ respectively,
- the matrix of ϕ_i $(i \geq 1)$ is of the form $\begin{pmatrix} a_i & c_i \\ b_i & d_i \end{pmatrix}$ with $\det(c_i) \neq 0$.

Note that since $\mathrm{Char}(M) = \sum_{j=0}^{n}(-1)^j r_j = 0$, such a decomposition must end with a matrix of ϕ_1 of the form $\begin{pmatrix} a_1 & c_1 \end{pmatrix}$ with $\det(c_1) \neq 0$, whereas we started with a matrix of ϕ_n of the form $\begin{pmatrix} c_n & d_n \end{pmatrix}^t$. It is of course possible to decompose the complex $F_\bullet$ is a similar way from the right to the left.

Proposition 2.12 *With the above notation, we have*

$$\mathfrak{S}(M) = \frac{\det(c_1)\det(c_3)\dots}{\det(c_2)\det(c_4)\dots}.A = \left(\prod_{i=1}^{n} \det(c_i)^{(-1)^{i-1}}\right).A \subset A.$$

Moreover, if A is graded, M is a graded A-module and (2.2) is a graded free resolution, then we have graded isomorphisms

$$\mathfrak{S}(M) \simeq \bigotimes_{i=0}^{n} \left(\bigwedge^{r_i} F_i\right)^{\otimes(-1)^{i+1}} \simeq A(-d)$$

where d denotes the degree of $\prod_{i=1}^{n} \det(c_i)^{(-1)^{i-1}} \in A$ and $(-)^{\otimes(-1)} := (-)^*$, the dual module.

Proof. We start by building a new complex a finite free modules

$$0 \to F_n^{(1)} \xrightarrow{\psi_n} F_n^{(1)} \oplus F_{n-1}^{(1)} \xrightarrow{\psi_{n-1}} \cdots \to F_2^{(1)} \oplus F_1^{(1)} \xrightarrow{\psi_1} F_1^{(1)} \oplus F_0^{(1)} \to 0 \qquad (2.3)$$

where, for all integer $i = 1, \dots, n$, the map ψ_i are defined by the matrix $\begin{pmatrix} 0 & \mathrm{Id} \\ 0 & 0 \end{pmatrix}$, where Id denotes the identity matrix of the suitable size. This complex is obviously exact (and not only acyclic). Now, we construct a morphism $\delta_\bullet$ of complexes from this new complex (2.3) to the resolution (2.2) of M as follows:

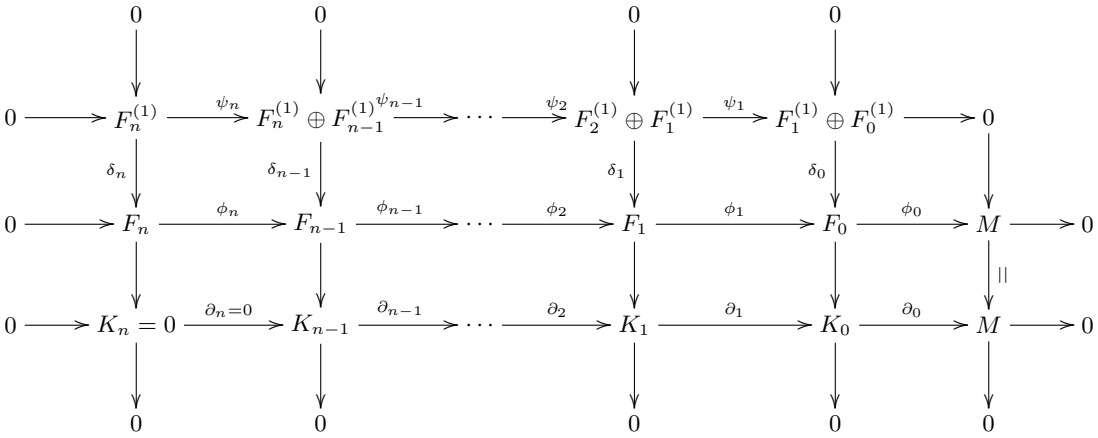
- $\delta_n := \mathrm{Id}$ from $F_n^{(1)} = F_n$ to F_n,
- for $i = 0, \dots, n-1$, the map $\delta_i : F_{i+1}^{(1)} \oplus F_i^{(1)} \to F_i = F_i^{(0)} \oplus F_i^{(1)}$, is explicitly defined by the square (!) matrix $\begin{pmatrix} c_{i+1} & 0 \\ d_{i+1} & \mathrm{Id} \end{pmatrix}$.

To ensure that $\delta_\bullet$ is a morphism of complexes we have to check that, for all integer $i = 1, \dots, n$, we have $\phi_i \circ \delta_i = \delta_{i-1} \circ \psi_i$. Indeed,

$$\begin{pmatrix} a_i & c_i \\ b_i & d_i \end{pmatrix} \begin{pmatrix} c_{i+1} & 0 \\ d_{i+1} & \mathrm{Id} \end{pmatrix} = \begin{pmatrix} 0 & c_i \\ 0 & d_i \end{pmatrix} = \begin{pmatrix} c_i & 0 \\ d_i & \mathrm{Id} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{Id} \\ 0 & 0 \end{pmatrix}$$

since $\phi_i \circ \phi_{i+1} = 0$ for all integer $i = 1, \dots, n-1$.

Now, since $\det(c_i) \neq 0$ for all $i = 1, \dots, n$ we deduce that δ_i, with $i = 0, \dots, n$ is injective (again by the McCoy's lemma). Therefore, for all $i = 0, \dots, n$ we can define the A-module $K_i := \mathrm{Coker}(\delta_i)$ which is an elementary module. Moreover, for all $i = 1, \dots, n$, the map $\phi_i : F_i \to F_{i-1}$ induces a map $\partial_i : K_i \to K_{i-1}$ and we obtain a third complex $(K_\bullet, \partial_\bullet)$. In addition, the surjective map $\phi_0 : F_0 \to M$ induces a surjective map $\partial_0 : K_0 \to M$. Let us summarize the situation with the following commutative diagram:



From the above constructions we get that all the columns and both first top lines in this diagram are exact. This implies that the third line is also exact (use for instance a classical long exact sequence of homology) and therefore that the complex $(K_\bullet, \partial_\bullet)$ is a finite elementary resolution of M. By definition of the MacRae's invariant of M, we deduce that (observe that $\mathfrak{F}(K_n) = \mathfrak{F}(0) = A$)

$$\mathfrak{S}(M) = \mathfrak{F}(K_0)\mathfrak{F}(K_1)^{-1}\mathfrak{F}(K_2)\cdots\mathfrak{F}(K_{n-1})^{(-1)^{n-1}} = \prod_{i=0}^{n-1}\mathfrak{F}(K_i)^{(-1)^i}.$$

But by construction, we have for all $i = 0, \ldots, n-1$, an exact sequence

$$0 \to F_{i+1}^{(1)} \oplus F_i^{(1)} \xrightarrow{\delta_i = \begin{pmatrix} c_{i+1} & 0 \\ d_{i+1} & \mathrm{Id} \end{pmatrix}} F_i = F_i^{(0)} \oplus F_i^{(1)} \to K_i \to 0 \tag{2.4}$$

from we deduce that $\mathfrak{F}(K_i) = \det(c_{i+1}).A$, which completes the proof of the first assertion.

Now assume that A, M and (2.2) are graded. Then it is easy to see that the new complex (2.3) is also graded, as well as the above big commutative diagram. It follows that we have for all $i = 0, \ldots, n-1$, graded isomorphisms

$$\mathfrak{F}(K_i) \simeq \overset{\max}{\bigwedge}(F_{i+1}^{(1)} \oplus F_i^{(1)}) \otimes \overset{\max}{\bigwedge}(F_i)^{\otimes(-1)}$$

We deduce the following graded isomorphisms

$$\begin{aligned}
\mathfrak{S}(M) &\simeq \bigotimes_{i=0}^{n-1}\left(\bigwedge^{\max}(F_{i+1}^{(1)}\oplus F_i^{(1)})\otimes\bigwedge^{\max}(F_i)^{\otimes(-1)}\right)^{\otimes(-1)^i}\\
&\simeq \bigotimes_{i=0}^{n-1}\left(\bigwedge^{\max}(F_{i+1}^{(1)}\oplus F_i^{(1)})\right)^{\otimes(-1)^i}\bigotimes_{i=0}^{n-1}\left(\bigwedge^{r_i}F_i\right)^{\otimes(-1)^{i+1}}\\
&\simeq \bigotimes_{i=0}^{n-1}\left(\bigwedge^{\max}(F_{i+1}^{(1)}\oplus F_i^{(1)})\right)^{\otimes(-1)^i}\bigotimes\left(\bigwedge^{\max}F_n^{(1)}\right)^{\otimes(-1)^n}\bigotimes_{i=0}^{n}\left(\bigwedge^{r_i}F_i\right)^{\otimes(-1)^{i+1}}\\
&\simeq \bigotimes_{i=0}^{n-1}\left(\bigwedge^{\max}F_{i+1}^{(1)}\right)^{\otimes(-1)^i}\bigotimes_{i=0}^{n}\left(\bigwedge^{\max}F_i^{(1)}\right)^{\otimes(-1)^i}\bigotimes_{i=0}^{n}\left(\bigwedge^{r_i}F_i\right)^{\otimes(-1)^{i+1}}\\
&\simeq \bigotimes_{i=0}^{n}\left(\bigwedge^{r_i}F_i\right)^{\otimes(-1)^{i+1}}
\end{aligned}$$

(observe that $F_0^{(1)}=0$ by the construction of the decomposition of the complex (2.2)). □

2.3.1 $\mathfrak{S}(M)$ as a greatest common divisor

We know that $\mathfrak{S}(M)$ is the smallest principal ideal which contains the initial Fitting ideal $\mathfrak{F}(M)$; in other words, $\mathfrak{S}(M)$ is the *codimension one part of* $\mathfrak{F}(M)$. It follows from proposition 2.3(iii) that the associated primes of $\mathfrak{F}(M)$ are exactly the associated primes of $\mathrm{ann}_A(M)$. More precisely, if A is a UFD ring and if $P_1,\ldots,P_r$ denote the irreducible factors of a gcd of a system of generators of $\mathfrak{F}(M)$, then $P_1^{e_1}P_2^{e_2}\ldots P_r^{e_r}$ is a generator of $\mathfrak{S}(M)$ where e_i denotes the "multiplicity" of $\mathfrak{S}(M)$ over $A/(P_i)$. We refer the reader to [17, chapter I, proposition 7.4] or [28, chapter V, §2] for the concept of multiplicity for modules.

3 The Macaulay's resultant

The Macaulay's resultant corresponds to the situation presented in section 1 where $r=n$, that is to say when the number of homogeneous polynomials equals the number of homogeneous variables one wants to eliminate. In such case, the resultant (or eliminant) ideal turns out to be principal and one of its generator can be obtained as a MacRae's invariant (under suitable hypotheses). The purpose of this section is to prove these results. But before, we need to introduce important tools from homological algebra.

3.1 Koszul and Čech complexes

In this section, we quickly review two standard constructions of homological algebra: the Koszul and Čech complexes. We will use them very often in the rest of these notes. Of course, there are many places where one can learn about them.

3.1.1 The Koszul complex.

Let A be a ring. For any element $x \in A$ we define its *homological Koszul complex* as the complex

$$K_\bullet(x) := 0 \to K_1(x;A) = A \xrightarrow{(x)} K_0(x;A) = A \to 0,$$

where the only non-zero map is the multiplication by x in A. Now, given a sequence $\mathbf{x} := (x_1, \ldots, x_n)$ of n elements, its homological Koszul complex is

$$K_\bullet(\mathbf{x}) := K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n).$$

Another way, may be more explicit, to define this Koszul complex is as follows: let $K_i(\mathbf{x})$ be the exterior power $\wedge^i(A^n)$. Then, if $\{e_1, \ldots, e_n\}$ denotes the canonical basis of A^n, $K_0(\mathbf{x}) = A$ and for all $p \in \mathbb{N}^*$

$$K_p(\mathbf{x}) = \bigoplus_{1 \le i_1 < \cdots < i_p \le n} A e_{i_1} \wedge \cdots \wedge e_{i_p}.$$

Moreover, the differential map $d_p : K_p(\mathbf{x}) \to K_{p-1}(\mathbf{x})$ sends a basis element $e_{i_1} \wedge \cdots \wedge e_{i_p}$ to

$$d_p(e_{i_1} \wedge \cdots \wedge e_{i_p}) := \sum_{k=1}^{p} (-1)^{k+1} x_{i_k} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_k}} \wedge \cdots \wedge e_{i_p}.$$

It is immediate to check that this defines a complex, that is to say that $d_{p-1} \circ d_p = 0$ for all p.

If M is a A-module, then we define the homological Koszul complex of the sequence $\mathbf{x}$ over M by $K_\bullet(\mathbf{x}; M) := K_\bullet(\mathbf{x}) \otimes_A M = K_\bullet(\mathbf{x}; A) \otimes_A M$. For all integer p we will denote by $H_p(\mathbf{x}; M)$ the p^{th} homology A-module of the Koszul complex $K_\bullet(\mathbf{x}; M)$.

Proposition 3.1 *With the above notation,*

(i) *The ideals* $\mathrm{ann}_A(M)$ *and* $(\mathbf{x})$ *of* A *annihilates all the homology modules of the Koszul complex* $K_\bullet(\mathbf{x}; M)$.

(ii) *If* $\mathbf{x}$ *is a* M*-regular sequence*[4]*, then* $H_p(\mathbf{x}; M) = 0$ *for all* $p \ge 1$.

[4] this means that for all $i = 1, \ldots, n$ the element x_i is not a zero-divisor in $M/(x_1, \ldots, x_{i-1})M$.

Proof. For the first point, it suffices to check that for all integers $p \geq 0$ and $j = 1, \ldots, n$, and all $x \in K_p(\mathbf{x}; M)$ we have

$$d_{p+1}\sigma_p^j(x) + \sigma_{p_1}^j d_p(x) = x_j x,$$

where the map $\sigma_p^j : K_p(\mathbf{x}; M) \to K_{p+1}(\mathbf{x}; M)$ sends the basis element $e_{i_1} \wedge \cdots \wedge e_{i_p}$ to the element $e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_p}$.

To prove the second statement, we proceed by induction on n. If $n = 1$, then we have $H_1(x_1; M) = \mathrm{Ker}(M \xrightarrow{\times x1} M) = 0$. Now, assume that we have proved (ii) for all integer $1, \ldots, t-1$ and put $\mathbf{x}' := (x_1, \ldots, x_{n-1})$. It is easy to check that we have the following exact sequence of complexes:

$$0 \to K_\bullet(\mathbf{x}'; M) \hookrightarrow K_\bullet(\mathbf{x}; M) \xrightarrow{\pi} K_\bullet(\mathbf{x}'; M)[-1] \to 0$$

where $K_\bullet[-1]$ is the "left translation" of $K_\bullet$ (i.e. $K_p[-1] := K_{p-1}$ and $d_p[-1] := d_{p-1}$) and the A-linear map π sends a basis element $e_{i_1} \wedge \cdots \wedge e_{i_p}$ to $e_{i_1} \wedge \cdots \wedge e_{i_{p-1}}$ if $i_p = n$, or 0 otherwise. This exact sequence gives rise to the long exact sequence of homology groups (we leave to the reader the explicitation of the connecting map)

$$\cdots \to H_p(\mathbf{x}'; M) \xrightarrow{\times(-1)^p x_n} H_p(\mathbf{x}'; M) \to H_p(\mathbf{x}; M) \to H_{p-1}(\mathbf{x}; M) \to \cdots$$

which immediately shows, with the inductive hypothesis, that $H_p(\mathbf{x}; M) = 0$ for all $p > 1$. To finish the proof, we examine the right end of the long exact sequence:

$$0 = H_1(\mathbf{x}'; M) \to H_1(\mathbf{x}; M) \to H_0(\mathbf{x}'; M) \xrightarrow{\times x_n} H_0(\mathbf{x}'; M) \to \cdots$$

Since $\mathbf{x}$ is assumed to be a M-regular sequence, then the map on the right is injective and it follows that $H_1(\mathbf{x}; M) = 0$. □

Remark 3.2 *The statement (ii) becomes an equivalence in the graded or local case. More precisely, if either*

- *A is a graded ring, M is a graded A-module of finite type and all the x_i's are homogeneous element with positive degree,*
- *A is a local noetherian ring $(A, \mathfrak{m})$ and for all $i = 1, \ldots, n$ we have $x_i \in \mathfrak{m}$,*

then $\mathbf{x}$ is a M-regular sequence if and only if $H_p(\mathbf{x}; M) = 0$ for all $p \geq 1$, if and only if $H_1(\mathbf{x}; M) = 0$. As a corollary, this proves that, under the same assumptions, $\mathbf{x}$ is a regular sequence independently of the order of its elements.

Note that if A is a graded ring, then the Koszul complex $K_\bullet(\mathbf{x}; M)$ inherits straightforwardly of this grading. For instance, if A is a $\mathbb{Z}$-graded ring and the elements $x_1, \ldots, x_n$

are homogeneous of degree $d_1, \ldots, d_n$, respectively, then the Koszul complex is graded by $K_0(\mathbf{x}; A) = A(0)$ and, for all $p \geq 1$,

$$K_p(\mathbf{x}; A) = \bigoplus_{1 \leq i_1 < \cdots < i_p \leq n} A(-d_{i_1} - \cdots - d_{i_p}).$$

Here, $A(\nu)$ denotes the twist by ν of A, i.e. $A(\nu)_t = A_{\nu+t}$ for all $(\nu, t) \in \mathbb{Z}^2$.

3.1.2 Generic polynomials.

Let k be a ring and $P_1, \ldots, P_s$ be the homogeneous generic polynomials of degree $d_1, \ldots, d_s$, respectively, in the homogeneous variables $X_1, \ldots, X_n$:

$$P_i(X_1, \ldots, X_n) := \sum_{|\alpha| = d_i} U_{i,\alpha} X^\alpha \in C := k[U_{i,\alpha} : i = 1, \ldots, s, |\alpha| = d_i][X_1, \ldots, X_n].$$

Lemma 3.3 *If $s \leq n$ then $P_1, \ldots, P_s$ is a regular sequence in the ring C.*

Proof. For all $i = 1, \ldots, s$ we distinguish the particular coefficient $\mathcal{E}_i := U_{i,(0,\ldots,0,d_i,0,\ldots,0)}$ of the monomial $X_i^{d_i}$ of the polynomial P_i. Then, all the remaining coefficients $U_{i,\alpha}$ form a regular sequence, and $P_i \equiv \mathcal{E}_i X_i^{d_i}$ in the corresponding quotient $k[\mathcal{E}_1, \ldots, \mathcal{E}_n][X_1, \ldots, X_n]$. Now, in this quotient it is easy to see that the polynomials $F_i = X_i - \mathcal{E}_i$, $i = 1, \ldots, s$, form a regular sequence. The corresponding quotient is then isomorphic to $k[X_1, \ldots, X_n]$ where $P_i \equiv X_i^{d_i+1}$, $i = 1, \ldots, s$. These later form also obviously a regular sequence. We conclude by using remark 3.2 which says that being a regular sequence does not depend on the order of the elements. □

Corollary 3.4 *Grading the polynomial ring C with $\deg(U_{i,\alpha}) = 0$ and $\deg(X_j) = 1$, the Koszul complex $K_\bullet(P_1, \ldots, P_s; C)$ provides, for all $s \leq n$, a finite free resolution of $C/(P_1, \ldots, P_s)$.*

In other words, we have the exact sequence

$$0 \to C(-d_1 - \cdots - d_s) \xrightarrow{d_s} \cdots \xrightarrow{d_3} \bigoplus_{1 \leq i < j \leq s} C(-d_i - d_j) \xrightarrow{d_2} \bigoplus_{i=1}^{s} C(-d_i) \xrightarrow{d_1} C \to \frac{C}{(P_1, \ldots, P_s)} \to 0.$$

In particular, the kernel of d_1 equals the image of d_2; therefore $(h_1, \ldots, h_s) \in \mathrm{Ker}(d_1)$ if and only if there exists $(\ldots, F_{i,j}, \ldots) \in \bigoplus_{1 \leq i < j \leq s} C(-d_i - d_j)$ such that $d_2(\ldots, F_{i,j}, \ldots) = (h_1, \ldots, h_s)$, that is to say if and only if

$$M \begin{pmatrix} P_1 \\ \vdots \\ P_s \end{pmatrix} = \begin{pmatrix} h_1 & \cdots & h_s \end{pmatrix}$$

where M is a skew-symmetric matrix (i.e. ${}^tM = -M$), namely $M := (F_{i,j})_{1 \leq i,j \leq s}$ (this last equivalence is easily checked by noting that $d_2(F_{i,j} e_i \wedge e_j) = F_{i,j} f_j e_i - F_{i,j} f_i e_j$).

3.1.3 The Čech complex.

Let A be a ring, $\mathbf{x} := (x_1, \ldots, x_n)$ a sequence of elements in A and M a A-module. The Čech complex of $\mathbf{x}$ over M is the cohomological complex $\mathcal{C}^\bullet(\mathbf{x}; M)$ whose terms are defined by

$$\mathcal{C}^0(\mathbf{x}; M) := M \text{ and } \mathcal{C}^p(\mathbf{x}; M) := \bigoplus_{1 \leq i_1 < \cdots < i_p \leq n} M_{x_{i_1} x_{i_2} \ldots x_{i_p}} \text{ for all } p = 1, \ldots, n.$$

The differentials $d^p : \mathcal{C}^p(\mathbf{x}; M) \to \mathcal{C}^{p+1}(\mathbf{x}; M)$ are defined by

$$d^0(m) = \sum_{i=1}^{p} \frac{m}{1} \text{ and } d^p(m_{i_1 \ldots i_p}) = \sum_{k \notin \{i_1, \ldots, i_p\}} (-1)^{t(k)} \phi_k(m_{i_1 \ldots i_p}),$$

where $i_{t(k)} < k < i_{t(k)+1}$ and $\phi_k(m_{i_1 \ldots i_p}) \in M_{x_{i_1} \ldots x_k \ldots x_n}$. One easily checks that $d^{p+1} \circ d^p = 0$, that is to say that $\mathcal{C}^\bullet(\mathbf{x}; M)$ is a complex.

For all integer p we will denote by $\check{H}^p(\mathbf{x}; M)$ the p^{th} cohomology A-modules of the Čech complex $\mathcal{C}^\bullet(\mathbf{x}; M)$.

Proposition 3.5 *With the above notation, the radical of the ideal* $(\mathbf{x})$ *of* A *annihilates all the cohomology modules* $\check{H}^i(\mathbf{x}; M)$ *of the Čech complex* $\mathcal{C}^\bullet(\mathbf{x}; M)$.

Proof. See [2, §3.5]. □

When the ring A is $\mathbb{Z}$-graded, M is a graded A-module and each element x_i is homogeneous of degree d_i, then the Čech complex is canonically graded by putting $\deg(\frac{m}{(x_{i_1} \ldots x_{i_p})^\alpha}) := \deg(m) - \alpha(d_{i_1} + \cdots + d_{i_p})$ (the differentials d^p are thus all of degree zero).

3.1.4 Local cohomology

Again, let A be a ring, I be an ideal of A generated by a sequence $\mathbf{x} := (x_1, \ldots, x_n)$ and M be a A-module.

Definition 3.6 *The* p^{th} *local cohomology* A*-module with support in* I *is the* p^{th} *cohomology* A*-module* $\check{H}^i(\mathbf{x}; M)$ *of the Čech complex* $\mathcal{C}^\bullet(\mathbf{x}; M)$. *It will be denoted by* $H^p_I(M)$.

Observe that we have, by definition,

$$H^0_I(M) = \{m \in M \text{ such that } \exists \nu \in \mathbb{N} : x_i^\nu m = 0 \text{ for all } i = 1, \ldots, n\}.$$

By the proposition 3.5 we deduce immediately that all the local cohomology modules $H^p_I(M)$ have their support contained in $V(I)$, which explains the name given to these modules. From the definition, it follows that the functor $H^p_I(-)$ commutes to sums and localization. We also get, given a short exact sequence of A-modules $0 \to M' \to M \to M'' \to 0$, a long exact sequence of local cohomology

$$0 \to H^0_I(M') \to H^0_I(M) \to H^0_I(M'') \to H^1_I(M') \to H^1_I(M) \to \cdots$$

Proposition 3.7 *Let t be an integer such that $1 \leq t \leq n$ and define the sequence $\mathbf{x}_t$ as $(x_1, \ldots, x_t)$. If $\mathbf{x}_t$ is a M-regular sequence then $H^p_I(M) = 0$ for all integer p such that $0 \leq p \leq t-1$.*

Proof. We proceed by induction on t. If $t = 1$, then for any $m \in H^0_I(M)$ there exists an integer ν such that $a_1^\nu m = 0$ which implies, since by hypothesis a_1 (and hence a_1^ν) is not a zero divisor in M, that $m = 0$. Now assume that this property is proved for all integer s such that $s-1 < t$. If $\mathbf{x}_s$ is a M-regular sequence, then a fortiori the sequence $(x_2, \ldots, x_s)$ is a M/x_1M-regular sequence from we deduce, using the inductive hypothesis, that $H^p_I(M/x_1M) = 0$ for all $0 \leq p \leq s-2$. The exact sequence of A-modules $0 \to M \xrightarrow{\times x_1} M \to M/x_1M \to 0$ yields the long exact sequence of local cohomology

$$0 \to H^0_I(M) \xrightarrow{\times x_1} \cdots \to H^{s-2}_I(M/x_1M) \to H^{s-1}_I(M) \xrightarrow{\times x_1} H^{s-1}_I(M) \to \cdots$$

which shows, using the inductive hypothesis, that the multiplication map by x_1 in $H^{s-1}_I(M)$ is injective. But since x_1 annihilates this local cohomology module, this later must be 0. □

Note that the local cohomology modules are canonically graded when A is graded and M is a graded A-module since in this case we already observed that the Čech complex is itself graded. Moreover, the definition of local cohomology modules in terms of the cohomology modules of the associated Čech complex yields immediately the well-known exact sequence

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to \bigoplus_{\nu \in \mathbb{Z}} \Gamma(\mathrm{Proj}(A), \widetilde{M}(\nu)) \to H^1_{\mathfrak{m}}(M) \to 0 \tag{3.1}$$

since we may identify $\Gamma(\mathrm{Proj}(A), \widetilde{M}(\nu))$ with $\mathrm{Ker}(\mathcal{C}^1 \xrightarrow{d^1} \mathcal{C}^2)$ (the "gluing conditions"; see [17, §II.5] for the definition of rings of sections).

In order to put our definition into practice we compute the local cohomology modules of the graded ring $A = k[X_1, \ldots, X_n]$ (seen as a graded A-module), where k is a ring, with support in the ideal $\mathfrak{m} = (X_1, \ldots, X_n)$. By the above proposition we know that all these modules are zero except $H^n_{\mathfrak{m}}(A)$. We claim that

$$H^n_{\mathfrak{m}}(A) \simeq \frac{1}{X_1 \ldots X_n} k[X_1^{-1}, \ldots, X_n^{-1}].$$

In particular, $H^n_{\mathfrak{m}}(A)_\nu = 0$ as soon as $\nu > -n$.

Indeed, an element in $H^n_{\mathfrak{m}}(A)$ is the class of an element in $A_{X_1 \ldots X_n}$ modulo the image of the differential $d^{n-1} : \oplus_{i=1}^n A_{X_1 \ldots \widehat{X_i} \ldots X_n} \to A_{X_1 \ldots X_n}$. Since d^{n-1} is k-linear, we just have to determine the class of a monomial $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ where $\alpha_i \in \mathbb{Z}$ for all $i = 1, \ldots, n$. But such a monomial is in the image of d^{n-1} if and only if there exists at least one integer $i \in \{1, \ldots, n\}$ such that $\alpha_i \geq 0$. Therefore the k-linear map

$$\phi : H^n_{\mathfrak{m}}(A) \to \frac{1}{X_1 \ldots X_n} k[X_1^{-1}, \ldots, X_n^{-1}] : \overline{X_1^{\alpha_1} \ldots X_n^{\alpha_n}} \mapsto \begin{cases} X_1^{\alpha_1} \ldots X_n^{\alpha_n} & \text{if } \alpha_i < 0 \ \forall i \\ 0 & \text{otherwise} \end{cases}$$

identifies $H^n_{\mathfrak{m}}(A)$ to $D := \frac{1}{X_1 \dots X_n} k[X_1^{-1}, \dots, X_n^{-1}]$ (giving it a structure of A-module in the same time). Moreover, since D is canonically graded, we have a perfect pairing[5]

$$A_m \times D_{-m-n} \to D_{-n} = k : (X^\alpha, X^\beta) \mapsto X^{\alpha+\beta}$$

which induces the duality

$$A_m \xrightarrow{\sim} D_{-n-m} : X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mapsto X_1^{-\alpha_1-1} \cdots X_n^{-\alpha_n-1}.$$

Finally, we mention that the local cohomology modules are usually defined as the right derived functors of the functor $H^0_I(-)$, assuming that the base ring is noetherian. It turns out that our definition of the local cohomology modules encapsulates the usual one, that is to say it corresponds to the usual one as soon as the ring A is assumed to be noetherian (see e.g. [2, §3.5] or [36, theorem A.8.3]).

3.2 Definition of the resultant

We take again the setting of the section 1 but assume now that the ring A is the universal ring of coefficients of the polynomials $f_1, \dots, f_r$. More precisely, we suppose given $r \geq 1$ homogeneous polynomials of positive degrees $d_1, \dots, d_r$, respectively (always in the variables $X_1, \dots, X_n$, all assumed to have weight 1),

$$f_i(X_1, \dots, X_n) = \sum_{|\alpha|=d_i} U_{i,\alpha} X^\alpha, \quad i = 1, \dots, r.$$

We put $A := k[U_{i,\alpha} : i = 1, \dots, r, |\alpha| = d_i]$ where k denotes a *UFD ring*. Then $f_i \in C := A[X_1, \dots, X_n]$ for all $i = 1, \dots, r$. As in the section 1, we consider the ideal $I := (f_1, \dots, f_r) \subset C$, as well as the graded quotient ring $B := C/I$ and put $\mathfrak{A} := H^0_{\mathfrak{m}}(B)_0$. The aim of this paragraph is to prove the

Theorem 3.8 *If $r = n$ then the ideal $\mathfrak{A}$ is a prime and principal ideal of A, the universal coefficient ring over the UFD ring k. Moreover, it has a unique generator, denoted* $\mathrm{Res}(f_1, \dots, f_n)$ *and called the* resultant *of $f_1, \dots, f_n$, such that*

$$\mathrm{Res}(X_1^{d_1}, \dots, X_n^{d_n}) = 1 \in k.$$

[5] Let R be an arbitrary non-zero commutative ring. A *bilinear form* or *bilinear pairing* $f : M \times N \to K$ is a multi-linear function with the additional property: for all $a \in R, m \in M, n \in N$ we have $f(am, n) = f(m, an) = af(m, n)$. There is a canonical bijection between such bilinear pairings and morphisms of R-modules $M \otimes_R N \to K$. Moreover, there is also a canonical bijection between bilinear pairing $f : M \times N \to R$ and morphisms of R-modules $F : M \to \mathrm{Hom}_R(N, R) : m \mapsto f(m, -)$.

We say that a bilinear pairing $f : M \times N \to K$ is *non-degenerated* if $f(m, n) = 0$ for all $n \in M$ (resp. $m \in M$) implies $m = 0$ (resp. $n = 0$). If $f : M \times N \to R$ is a non-degenerated pairing then clearly $F : M \to \mathrm{Hom}_R(N, R)$ is injective; so if M and N are finite free R-modules, the existence of a non-degenerated pairing f implies that $\mathrm{rank}(M) = \mathrm{rank}(N)$ (for f is non-degenerated implies that $g : N \times M \to R$ defined by $g(n, m) = f(m, n)$ is also a non-degenerated paring and hence that $G : N \to \mathrm{Hom}_R(M, R)$ is also injective).

We say that $f : M \times N \to R$ is a *perfect* pairing if it is non-degenerated and if the corresponding (injective) morphism $F : M \to \mathrm{Hom}_R(N, R)$ is an isomorphism.

We will closely follow the "preuve élémentaire" given by Jouanolou in [22]. Before going further into details, we point out that this theorem holds without any hypothesis on the ring k (except for the unicity of the normalized generator which requires that k is a reduced ring); we refer the interested reader to the monograph [22] for more details and many more properties of the resultant.

First introduced by Hurwitz, *inertia forms* reveal a powerful tool to study the resultant ideals, notably in the case $r = n$. We recall that $\mathfrak{m} := (X_1, \ldots, X_n) \subset C$, and that r and n are *a priori* two distinct integers.

Definition 3.9 *The ideal of inertia forms of the ideal I with respect to the ideal $\mathfrak{m}$ is*

$$\mathrm{TF}_{\mathfrak{m}}(I) := \bigcup_{t\geq 0}(I :_C \mathfrak{m}^t) = \{f \in C : \exists \nu \in \mathbb{N}\ \mathfrak{m}^\nu f \subset I\} = \pi^{-1}(H^0_{\mathfrak{m}}(B)) \subset C,$$

where π denotes the canonical projection $C \to B = C/I \to 0$.

Observe that $\mathrm{TF}_{\mathfrak{m}}(I)$ is an homogeneous ideal of C and that $\mathfrak{A} = \mathrm{TF}_{\mathfrak{m}}(I)_0 \subset A$. We give hereafter some properties of these inertia forms.

Lemma 3.10 *Let j be any fixed integer in $\{1, \ldots, n\}$, then*

$$\mathrm{TF}_{\mathfrak{m}}(I) = \bigcup_{t\geq 0}(I :_C X_j^t) = \{f \in C : \exists \nu \in \mathbb{N}\ X_j^\nu f \subset I\} = \mathrm{Ker}(C \to B_{X_j}). \tag{3.2}$$

Moreover, $\mathrm{TF}_{\mathfrak{m}}(I)$ is a prime ideal of C (and therefore $\mathfrak{A}$ is a prime ideal of A).

Proof. Let j be fixed in $\{1, \ldots, n\}$. For all $i = 1, \ldots, r$ we distinguish the particular coefficient $\mathcal{E}_i := U_{i,(0,\ldots,0,d_i,0,\ldots,0)}$ of the polynomial f_i which can be rewritten in $C[X_j^{-1}]$ as

$$f_i = X_j^{d_i}(\mathcal{E}_i + \sum_{\alpha\neq(0,\ldots,0,d_i,0,\ldots,0)} U_{i,\alpha}X^\alpha X_j^{-d_i}).$$

Then we easily get the isomorphism of k-algebras

$$\begin{aligned} B_{X_j} &\xrightarrow{\sim} k[U_{l,\alpha} : U_{l,\alpha} \neq \mathcal{E}_i][X_1, \ldots, X_n][X_j^{-1}] \\ \mathcal{E}_i &\mapsto \mathcal{E}_i - \frac{f_i}{X_j^{d_i}} = -\sum_{\alpha\neq(0,\ldots,0,d_i,0,\ldots,0)} U_{i,\alpha}X^\alpha X_j^{-d_i} \end{aligned} \tag{3.3}$$

from we deduce that X_i is not a zero divisor in B_{X_j} for all couple $(i,j) \in \{1, \ldots, n\}^2$. It follows that we successively obtain, for any couple $(i,j) \in \{1, \ldots, n\}^2$, the equalities

$$\mathrm{Ker}(C \to B_{X_i}) = \mathrm{Ker}(C \to B_{X_iX_j}) = \mathrm{Ker}(C \to B_{X_jX_i}) = \mathrm{Ker}(C \to B_{X_j})$$

which prove the claimed description of $\mathrm{TF}_{\mathfrak{m}}(I)$. Moreover, since k is a domain, it follows that the B_{X_j}'s are also domains and thus that $\mathrm{TF}_{\mathfrak{m}}(I)$ is a prime ideal of C. □

Proposition 3.11 (Hurwitz) *If $r < n$ then $\mathrm{TF}_{\mathfrak{m}}(I) = I$.*

Proof. We just have to prove that $\mathrm{TF}_{\mathfrak{m}}(I) \subset I$, the other inclusion being obvious. By the above lemma 3.10, we need to prove that for all $f \in C$ such that there exists $s \in \mathbb{N}$ such that $X_n^s f \in I$ then $f \in I$. This property is evident if $s = 0$ and an easy inductive argument shows that if we prove it for $s = 1$ the property is true for any $s \in \mathbb{N}$ (since $X_n^k f = X_n(X_n^{k-1} f)$).

Thus, let $f \in C$ such that $X_n f = h_1 f_1 + \cdots + h_r f_r \in I \subset C$. By specializing X_n to 0 we deduce that $\overline{h}_1 \overline{f}_1 + \cdots + \overline{h}_r \overline{f}_r = 0$, where the $\overline{f}_i$'s are generic homogeneous polynomials in $n-1$ variables. Therefore, by lemma 3.3 they form a regular sequence in $A[X_1, \ldots, X_{n-1}]$ and by corollary 3.4, the Koszul complex $K_\bullet(\overline{f}_1, \ldots, \overline{f}_r; A[X_1, \ldots, X_{n-1}])$ is acyclic. From the remark following this corollary 3.4 we deduce that there exists a skew-symmetric matrix M (i.e. ${}^t M = -M$), such that

$$\begin{pmatrix} \overline{h}_1 & \overline{h}_2 & \cdots & \overline{h}_r \end{pmatrix} = M \begin{pmatrix} \overline{f}_1 \\ \vdots \\ \overline{f}_r \end{pmatrix}.$$

Now, define the polynomials $g_1, \ldots, g_r \in A[X_1, \ldots, X_n]$ such that

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_r \end{pmatrix} = M \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}.$$

Since M is skew-symmetric, it is easy to check that $\sum_{i=1}^n g_i f_i = 0$. Moreover, for all $i = 1, \ldots, r$, since $\overline{g}_i = \overline{h}_i$ we deduce that there exists a polynomial l_i such that $h_i - g_i = X_n l_i$. Consequently, we have

$$X_n f = (g_1 + X_n l_1) f_1 + \cdots + (g_r + X_n l_r) f_r = \sum_{i=1}^n g_i f_i + X_n \sum_{i=1}^n l_i f_i$$

which implies that $f = \sum_{i=1}^n l_i f_i \in A[X_1, \ldots, X_n]$ (for X_n is not a zero divisor), i.e. $f \in I$. □

Corollary 3.12 *Assume that $r = n$ and let $f \in \mathrm{TF}_{\mathfrak{m}}(I) \subset A[X_1, \ldots, X_n]$. Then either $f \in I = (f_1, \ldots, f_n)$ or f depends on all the coefficients of each polynomials $f_1, \ldots, f_n$.*

Proof. Let us denote by $U := U_{i,\alpha}$ a coefficient of the polynomial f_i for some $i \in \{1, \ldots, n\}$; we put $g_i = f_i - U X^\alpha$. We assume that there exists $f \in \mathrm{TF}_{\mathfrak{m}}(I)$ independent of U and we will prove that $f \in I$.

Since $f \in \mathrm{TF}_{\mathfrak{m}}(I)$, we know that $X_n^l f = \sum_{i=1}^n h_i f_i \in A[X_1, \ldots, X_n]$ for some $l \in \mathbb{N}$. Consider the k-algebra morphism

$$\begin{array}{rcl} A[X_1, \ldots, X_n] & \xrightarrow{\varphi} & A[X_1, \ldots, X_n]_{X_1 X_2 \ldots X_n} \\ U & \mapsto & -g_i / X^\alpha \\ U_{j,\beta} & \mapsto & U_{j,\beta} \text{ if } (j,\beta) \neq (i,\alpha) \\ X_j & \mapsto & X_j. \end{array}$$

Since $\varphi(f_i) = 0$, we have

$$\varphi(X_n^l f) = H_1 f_1 + \cdots + H_{i-1} f_{i-1} + H_{i+1} f_{i+1} + \cdots + H_n f_n \in A[X_1, \ldots, X_n]_{X_1 \ldots X_n}.$$

But $X_1 \ldots X_n$ is not a zero-divisor in $A[X_1, \ldots, X_n]_{X_1 \ldots X_n}$ and $\varphi(X_n^l f) = X_n^l f$, so there exists a monomial X^β such that

$$X^\beta \varphi(X_n^l f) = X^\beta X_n^l f = G_1 f_1 + \cdots + G_{i-1} f_{i-1} + G_{i+1} f_{i+1} + \cdots + G_n f_n \in A[X_1, \ldots, X_n],$$

that is to say that $f \in \mathrm{TF}_{\mathfrak{m}}(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ (up to a certain extension of the coefficient ring). We conclude that $f \in I$ by the proposition 3.11. □

Proof of theorem 3.8. First, observe that $\mathfrak{A} \neq 0$ since

$$\mathrm{Proj}(k[X_1, \ldots, X_n]/(X_1^{d_1}, \ldots, X_n^{d_n})) = \emptyset.$$

Now, choose a coefficient $U := U_{i,\alpha}$ and define the polynomial ring A' such that $A = A'[U]$ (note that A' is also a UFD ring). Since $I \cap A = 0$, we deduce from corollary 4.4 that all non-zero $f \in \mathfrak{A}$ has a positive degree as a polynomial in U, i.e. $\deg_U(f) \geq 1$. Let $s \geq 1$ be the minimum such degree among all non-zero element $f \in \mathfrak{A}$.

We claim that there exists a *prime* element $R \in \mathfrak{A}$ such that $\deg_U(R) = s$. Indeed, let $f \neq 0 \in \mathfrak{A}$ such that $\deg_U(f) = s$. Since A' is a UFD ring, there exists a decomposition $f = q_1 \ldots q_t$ where q_j are primes in $A'[U]$. But since $\mathfrak{A}$ is a prime ideal by lemma 3.10, we deduce that there exists $j \in \{1, \ldots, t\}$ such that $q_j \in \mathfrak{A}$. Moreover, we have $1 \leq \deg_U(q_j) \leq \deg_U(f) = s$, and by the definition of s we get that $\deg_U(q_j) = s$, which implies that the element $R := q_j$ is as claimed.

We now show the above element R generates $\mathfrak{A}$. Indeed, since A' has no zero-divisor, for all $g \in \mathfrak{A}$ we have

$$\lambda g = uR + v \text{ with } \lambda \in A' \text{ and } \begin{cases} v = 0 \\ \text{or} \\ \deg_U(v) < s. \end{cases}$$

It follows that $v = \lambda g - uR \in \mathfrak{A}$. If $v \neq 0$, then $\deg_U(v) \geq 1$ by proposition 4.4, and thus $\deg_U(v) \geq s$ by the definition of s; this gives a contradiction. Therefore, $\lambda g = uR$. Moreover, $\lambda \in A'$ which does not contain U, so R divides g.

Finally, R is unique up to multiplication by an invertible element of A', hence of k. This element is fixed to $1 \in k$ by the normalization given in this theorem. □

3.3 The resultant as a MacRae's invariant

The aim of this section is to prove that the resultant ideal of n homogeneous polynomial in n homogeneous variables, which we proved that it is principal, is the MacRae's invariant of certain graded parts of a Koszul complex. As a byproduct, we obtain an algorithm to compute the resultant $\mathrm{Res}(f_1, \ldots, f_n)$ either as an alternating product of determinants or a gcd of some determinants of some maximal minors of a single matrix.

Lemma 3.13 *For all integer* $\nu \geq \eta := d_1 + \cdots + d_n - n + 1$ *we have* $H^0_{\mathfrak{m}}(B)_\nu = 0$.

Proof. The proof of this lemma consists in a standard use of two spectral sequences associated to the double complex

$$\begin{array}{ccccccccccc}
0 & \to & \mathcal{C}^0_{\mathfrak{m}}(\wedge^n E) & \xrightarrow{d_n} & \cdots & \xrightarrow{d_2} & \mathcal{C}^0_{\mathfrak{m}}(\wedge^1 E) & \xrightarrow{d_1} & \mathcal{C}^0_{\mathfrak{m}}(C) & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & \mathcal{C}^1_{\mathfrak{m}}(\wedge^n E) & \to & \cdots & \to & \mathcal{C}^1_{\mathfrak{m}}(\wedge^1 E) & \to & \mathcal{C}^1_{\mathfrak{m}}(C) & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & \mathcal{C}^n_{\mathfrak{m}}(\wedge^n E) & \to & \cdots & \to & \mathcal{C}^n_{\mathfrak{m}}(\wedge^1 E) & \to & \mathcal{C}^n_{\mathfrak{m}}(C) & \to & 0
\end{array}$$

where E denotes the graded free A-module $E := \oplus_{i=1}^n C(-d_i)$. The first row is the Koszul complex associated to the sequence $f_1, \ldots, f_n$, and its columns are Čech complexes. We know that $K_\bullet(f_1, \ldots, f_n; C)$ is acyclic and also that $H^i_{\mathfrak{m}}(C) = 0$ if $i \neq n$. Examining the two filtrations by rows and by columns we deduce that, among other properties,

$$H^0_{\mathfrak{m}}(B) \simeq \mathrm{Ker}\left(H^n_{\mathfrak{m}}(\wedge^n E) \to H^n_{\mathfrak{m}}(\wedge^{n-1} E)\right) \tag{3.4}$$

which is a graded isomorphism. By the computation we did at the end of section 3.1.4, we know that $H^n_{\mathfrak{m}}(C)_\nu = 0$ for all integer $\nu > -n$. Therefore, since

$$H^n_{\mathfrak{m}}(\wedge^n E)_\nu = H^n_{\mathfrak{m}}(C(-d_1 - \cdots - d_n))_\nu = H^n_{\mathfrak{m}}(C)_{\nu - d_1 - \cdots - d_n},$$

it follows that $H^0_{\mathfrak{m}}(B)_\nu = 0$ for all integer $\nu > d_1 + \cdots + d_n - n$. □

Corollary 3.14 *For all integer* $\nu \geq \eta$ *we have* $\mathrm{ann}_A(B_\nu) = \mathfrak{A} = (\mathrm{Res}(f_1, \ldots, f_n)) \subset A$.

Proof. It is an immediate consequence of the proposition 1.2 and the above lemma 3.13. □

As a consequence, we obtain that the initial Fitting ideal of the A-module B_ν, for all $\nu \geq \eta$, satisfies

$$\mathfrak{A}^{\binom{\nu+n-1}{n-1}} \subset \mathfrak{F}(B_\nu) \subset \mathfrak{A},$$

which implies that $\mathfrak{F}(B_\nu)$ and $\mathfrak{A} = (\mathrm{Res}(f_1, \ldots, f_n))$ have the same radical (as ideals in A). More precisely, $\mathfrak{A}$ is the unique *minimal prime* ideal containing $\mathfrak{F}(B_\nu)$. Moreover, it turns out that it contains it with "multiplicity" one in the sense that

$$\mathrm{length}_{A/\mathfrak{A}A}(B_\nu) = \mathrm{length}_{A_{\mathfrak{A}}/\mathfrak{A}A_{\mathfrak{A}}}((B_\nu)_{\mathfrak{A}}) = 1$$

(note that B_ν has a canonical structure of $A/\mathfrak{A}A$-module)[6]. This is the content of the following theorem. We first need the preliminary

[6] From a more geometric point of view, this property means that the projection $\mathrm{Proj}(B) \to \mathrm{Spec}(A/\mathfrak{A})$ is birational

Lemma 3.15 *For all integer $j = 1, \ldots, n$ and any couple (α, β) of multi-index such that $|\alpha| = |\beta| = d_j$, we have*

$$X^\alpha \frac{\partial R}{\partial U_{j,\beta}} - X^\beta \frac{\partial R}{\partial U_{j,\alpha}} \in \mathrm{TF}_{\mathfrak{m}}(I)$$

where $R := \mathrm{Res}(f_1, \ldots, f_n) \in A$.

Proof. By definition, there exists a monomial X^γ and polynomials c_i, $i = 1, \ldots, n$, in $A[\mathbf{X}]$ such that $X^\gamma R = \sum_{i=1}^n c_i f_i$. By computing the derivative with respect to $U_{j,\alpha}$ and to $U_{j,\beta}$ one gets both equalities

$$X^\gamma \frac{\partial R}{\partial U_{j,\alpha}} = c_j X^\alpha + \sum_{l=1}^n \frac{\partial c_l}{\partial U_{j,\alpha}} f_l \quad \text{and} \quad X^\gamma \frac{\partial R}{\partial U_{j,\beta}} = c_j X^\beta + \sum_{l=1}^n \frac{\partial c_l}{\partial U_{j,\beta}} f_l.$$

We deduce easily that

$$X^\gamma \left(X^\alpha \frac{\partial R}{\partial U_{j,\beta}} - X^\beta \frac{\partial R}{\partial U_{j,\alpha}} \right) \in (f_1, \ldots, f_n)$$

and conclude by using lemma 3.10. □

Theorem 3.16 *For all integer $\nu \geq \eta$ we have*

$$\mathfrak{S}(B_\nu) = \mathfrak{A} = (\mathrm{Res}(f_1, \ldots, f_n)) \subset A.$$

Proof. First, observe that by the behavior of MacRae's invariants and resultants under base changes, it is sufficient to prove this formula in the case where $k = \mathbb{Z}$.

We know that $\mathfrak{S}(B_\nu)$ is the smallest minimal prime (equivalently principal) ideal containing $\mathfrak{F}(B_\nu)$. Therefore, the claimed result will be proved if we show that (recall that Fitting ideals and MacRae's invariants are stable under localization)

$$\mathfrak{F}(B_\nu)_{\mathfrak{A}} = \mathfrak{A} A_{\mathfrak{A}}.$$

To prove this, we put, for simplicity, $R := \mathrm{Res}(f_1, \ldots, f_n)$ and denote by $\mathcal{E}_{j,l}$ the coefficient of the monomial $X_l X_n^{d_j - 1}$ in the polynomial f_j, for all couple $(i, j) \in \{1, \ldots, n\}$:

$$f_j(X_1, \ldots, X_n) := \cdots + \mathcal{E}_{j,1} X_1 X_n^{d_j - 1} + \mathcal{E}_{j,2} X_2 X_n^{d_j - 1} + \cdots + \mathcal{E}_{j,n} X_n^{d_j}.$$

From now on, let us fix the integer j. Consider the ideal of the quotient ring $A/\mathfrak{A}$

$$J := \left(\overline{\frac{\partial R}{\partial \mathcal{E}_{j,1}}}, \overline{\frac{\partial R}{\partial \mathcal{E}_{j,2}}}, \ldots, \overline{\frac{\partial R}{\partial \mathcal{E}_{j,n}}} \right) \subset A/\mathfrak{A}.$$

We can define a graded morphism (of degree zero) of A-algebras by

$$\begin{array}{rcl} \Theta : C := A[\mathbf{X}] & \to & \mathfrak{R} := A/\mathfrak{A} \oplus J \oplus J^2 \oplus \cdots \\ X_i & \mapsto & 0 \oplus \overline{\dfrac{\partial R}{\partial \mathcal{E}_{j,i}}} \oplus 0 \oplus \cdots \end{array}$$

which is clearly surjective.

We claim that there exists an integer j such that $\frac{\partial R}{\partial \mathcal{E}_{j,n}} \neq 0$. Indeed, by lemma 3.15 we know that for all j and all multi-index α such that $|\alpha| = d_j$ we have

$$X^{\alpha}\frac{\partial R}{\partial \mathcal{E}_{j,n}} - X_n^{d_j}\frac{\partial R}{\partial U_{j,\alpha}} \in \mathrm{TF}_{\mathfrak{m}}(I).$$

Therefore, if $\frac{\partial R}{\partial \mathcal{E}_{j,n}} = 0$ for all j, then $\frac{\partial R}{\partial U_{j,\alpha}} = 0$ for all j and all α which is impossible since $R \neq 0$ (we are in characteristic zero).

Now, one may assume that the integer j we chose to define $\mathfrak{R}$ is such that $\frac{\partial R}{\partial \mathcal{E}_{j,n}} \neq 0$. Then we claim that Θ induces a graded isomorphism $A[\mathbf{X}]/\mathrm{TF}_{\mathfrak{m}}(I) \simeq \mathfrak{R}$ (note that $A[\mathbf{X}]/\mathrm{TF}_{\mathfrak{m}}(I) = B/H^0_{\mathfrak{m}}(B)$). Indeed, let $F(\mathbf{X})$ be a homogeneous polynomial in $A[\mathbf{X}]$ of degree $d \geq 0$ such that $F \in \mathrm{Ker}(\Theta)$, i.e. such that

$$F\left(\frac{\partial R}{\partial \mathcal{E}_{j,1}}, \ldots, \frac{\partial R}{\partial \mathcal{E}_{j,n}}\right) \in \mathfrak{A}.$$

We easily derive from lemma 3.15 that

$$X_n^d F\left(\frac{\partial R}{\partial \mathcal{E}_{j,1}}, \ldots, \frac{\partial R}{\partial \mathcal{E}_{j,n}}\right) - \left(\frac{\partial R}{\partial \mathcal{E}_{j,n}}\right)^d F(X_1, \ldots, X_n) \in \mathrm{TF}_{\mathfrak{m}}(I),$$

which implies in our case that

$$\left(\frac{\partial R}{\partial \mathcal{E}_{j,n}}\right)^d F(X_1, \ldots, X_n) \in \mathrm{TF}_{\mathfrak{m}}(I).$$

But by hypothesis, $0 \neq \overline{\frac{\partial R}{\partial \mathcal{E}_{j,n}}} \in A/\mathfrak{A} \hookrightarrow B/H^0_{\mathfrak{m}}(B)$. Since $B/H^0_{\mathfrak{m}}(B)$ is a domain, we deduce that $\frac{\partial R}{\partial \mathcal{E}_{j,n}}$ is not a zero-divisor in $A[\mathbf{X}]/\mathrm{TF}_{\mathfrak{m}}(I)$, and therefore that $F \in \mathrm{TF}_{\mathfrak{m}}(I)$.

Finally, since $B/H^0_{\mathfrak{m}}(B) \simeq \mathfrak{R}$ (a graded isomorphism), we deduce, by localization at $\mathfrak{A}$, that

$$\left(B/H^0_{\mathfrak{m}}(B)\right)_{\mathfrak{A}} \simeq \bigoplus_{\mathbb{N}} A_{\mathfrak{A}}/\mathfrak{A}A_{\mathfrak{A}}$$

(again a graded isomorphism) since $J_{\mathfrak{A}} = A_{\mathfrak{A}}/\mathfrak{A}A_{\mathfrak{A}}$. Therefore, since $H^0_{\mathfrak{m}}(B)_{\nu} = 0$ as soon as $\nu \geq \eta$, we obtain that $(B_{\nu})_{\mathfrak{A}} \simeq A_{\mathfrak{A}}/\mathfrak{A}A_{\mathfrak{A}}$ for all $\nu \geq \eta$. Since $\mathfrak{A}$ is principal, we get $\mathfrak{F}(B_{\nu})_{\mathfrak{A}} = \mathfrak{A}A_{\mathfrak{A}}$, for all $\nu \geq \eta$. □

This theorem implies that the Macaulay's resultant can be computed as the determinant of certain graded parts of the Koszul complex $K_{\bullet}(f_1, \ldots, f_n; A[\mathbf{X}])$, as well as the gcd of the maximal minors of its first map (see section 2.3.1). Another consequence is that we can determine the degree, more precisely the multi-degree of the resultant of the polynomials $f_1, \ldots, f_n$.

To do this, observe that the Koszul $K_\bullet(f_1,\dots,f_n;A[\mathbf{X}])$ is $\mathbb{N}^{n+1}$-graded: it is graded with respect to the coefficients of each polynomial f_i, the $U_{i,\alpha}$'s, for $i=1,\dots,n$, and with respect to the variables $X_1,\dots,X_n$. We put

$$E := A(-1,0,\dots,0;-d_1)[\mathbf{X}] \oplus A(0,-1,0,\dots,0;-d_2)[\mathbf{X}] \oplus \cdots \oplus A(0,\dots,0,-1;-d_n)[\mathbf{X}]$$

so that $K_\bullet(f_1,\dots,f_n;A[\mathbf{X}])$ is of the form

$$K_n := \wedge^n(E) \to \cdots \to K_2 := \wedge^2(E) \to K_1 := \wedge^1(E) \simeq E \xrightarrow{(f_1,\dots,f_n)} K_0 := A[\mathbf{X}](0,\dots,0;0).$$

The theorem 3.16 says that for all integer $\nu \geq \eta := d_1+\cdots+d_n-n+1$ then the ν^{th} graded part of $K_\bullet(f_1,\dots,f_n;A[\mathbf{X}])$, seen as a complex $\mathbb{N}$-graded in the X_i's, has determinant $\mathfrak{S}(B_\nu)=\mathfrak{A}$ which is a principal ideal generated by the element $\mathrm{Res}(f_1,\dots,f_n)$. Therefore, by proposition 2.12 we have a canonical graded isomorphism of A-modules $\mathfrak{A} \simeq A(-\delta_1,\dots,-\delta_n)$ where, for all $i=1,\dots,n$,

$$\delta_i := \sum_{J\subset\{1,\dots,n\}\setminus\{i\}} (-1)^{|J|} \binom{\nu - d_i - \sum_{j\in J} d_j + n - 1}{n-1} \in \mathbb{Z}.$$

The following simple lemma helps to give a more compact formula for these integers.

Lemma 3.17 *Let $n, r_1,\dots,r_p$ be a list of positive integers and consider the formal series $S(T) := \prod_{i=1}^p (1-T^{r_i})/(1-T)^n \in \mathbb{Z}[[T]]$. Then, for all integer $\nu \geq 0$, we have*

$$S(T)_{|T^\nu} = \sum_{J\subset\{1,\dots,p\}} (-1)^{|J|} \binom{\nu - \sum_{j\in J} r_j + n - 1}{n-1} \in \mathbb{Z}$$

where $S(T)_{|T^\nu}$ denotes the coefficients of T^ν in $S(T)$, with the convention $\binom{q}{n-1}=0$ if $q<0$.

Proof. It suffices to develop $S(T)$ as

$$S(T) = \prod_{i=1}^p (1-T^{r_i}) \times \frac{1}{(1-T)^n} = \Big(\sum_{J\subset\{1,\dots,p\}} (-1)^{|J|} T^{\sum_{j\in J} r_j}\Big) \times \Big(\sum_{s\geq 0} \binom{s+n-1}{n-1} T^s\Big)$$

and compute the coefficient of the monomial T^ν. □

We deduce that δ_i is the coefficient of $T^{\nu-d_i}$ in the series $\frac{\prod_{j=1,j\neq i}^n (1-T^{d_i})}{(1-T)^n}$ for any integer $\nu \geq \eta$. Defining the polynomial

$$H(T) := \prod_{j=1,j\neq i}^n (1+T+\cdots+T^{d_i-1}) = \sum_{s=0}^{-d_i+d_1+\cdots+d_n-n+1} N_s T^s \in \mathbb{Z}[T],$$

we have $S(T) = H(T)/(1-T)$, that is to say $S(T) = H(T) \times (\sum_{s\geq 0} T^s)$. It follows that, since $\nu - d_i \geq \eta - d_i = \deg(H)$, we obtain $\delta_i = \sum_{s=0}^{\deg(H)} N_s = H(1) = \frac{d_1 d_2 \ldots d_n}{d_i}$ and therefore deduce that we have a graded isomorphism

$$(\mathrm{Res}(f_1, \ldots, f_n)) \simeq A(-d_2 \cdots d_n, \ldots, -\frac{d_1 d_2 \cdots d_n}{d_i}, \ldots, -d_1 d_2 \cdots d_{n-1}).$$

3.4 Complement: multivariate subresultants

Given n homogeneous polynomials $f_1, \ldots, f_n$ in n variables $X_1, \ldots, X_n$ of degree $d_1, \ldots, d_n$ respectively, we have just seen that their resultant is a generator of the MacRae's invariant of a graded part of the quotient algebra B of degree greater or equal to $\eta := d_1 + \cdots + d_n - n + 1$. A natural question is then to ask what kind of invariants, if any, are associated to the graded parts of B of degree smaller than η. This question leads us to the so-called *multivariate subresultants*, as defined by Chardin in [10]. We hereafter give a quick overview of the definition and some basic properties of these interesting eliminant polynomials, even if they are not really invariants of the input polynomials. The following can be seen as a direct extension of the techniques we used to define the Macaulay's resultants.

Let k be a UFD ring. We suppose given s generic homogeneous polynomials in n variables, such that $n \geq s \geq 1$, of positive degree $d_1, \ldots, d_s$ respectively

$$f_i(X_1, \ldots, X_n) := \sum_{|\alpha| = d_i \geq 1} U_{i,\alpha} X^\alpha, \ i = 1, \ldots, s.$$

We put $A := k[U_{i,\alpha} : i = 1, \ldots, s, |\alpha| = d_i]$ the universal coefficient ring over k, $C := A[X_1, \ldots, X_n]$, $\mathfrak{m} := (X_1, \ldots, X_n)$ and $B := C/(f_1, \ldots, f_s)$. Both C and B are naturally graded modules by setting $\deg(X_i) = 1$ for all $i = 1, \ldots, n$.

Suppose given an integer $\nu \geq 0$. From lemma 3.4 we know that the Koszul complex $K_\bullet(f_1, \ldots, f_s; C)$ is a graded finite free resolution of C-modules of the quotient algebra B. We deduce that its ν^{th} graded part is also a finite free resolution of A-modules of B_ν. Therefore,

$$\mathrm{Char}(B_\nu) = \sum_{J \subset \{1,\ldots,s\}} (-1)^{|J|} \binom{\nu - \sum_{j\in J} d_j + n - 1}{n-1} = S(T)_{|T^\nu}$$

where $S(T) := \prod_{i=1}^s (1 - T^{d_i})/(1-T)^n$, the last equality following from lemma 3.17. Therefore, we deduce that $\mathrm{Char}(B_\nu) = 0$ only if $d_1 + \cdots + d_s \geq n$ and $\nu \geq d_1 + \cdots + d_s - n + 1$ (for instance, if $s = n$ then $\mathrm{Char}(B_\nu) = 0$ only if $\nu \geq \eta := d_1 + \cdots + d_n - n + 1$). It follows that in some cases the MacRae's invariant of B_ν does not exists. To get ride of this difficulty we consider another associated module.

Suppose given an integer $\nu \geq 0$ and a set $\mathcal{S}$ of $\mathrm{Char}(B_\nu)$ homogeneous polynomial of degree ν in $k[X_1, \ldots, X_n]$ that we assume to be free in B_ν over A. We denote by $\langle \mathcal{S} \rangle_A$

the free A-submodule of B_ν with basis $\mathcal{S}$ and consider the A-module $M_\nu := B_\nu/\langle\mathcal{S}\rangle_A$. It admits a natural finite free resolution of A-modules, namely the ν^{th} graded part of the Koszul complex $K_\bullet(f_1,\ldots,f_s;C)$ whose last map on the right is co-restricted to $C_\nu/\langle\mathcal{S}\rangle_A$. It follows that the Euler characteristic of M_ν is zero and that it possesses a MacRae's invariant.

Definition 3.18 *We define the $\mathcal{S}$-subresultant of the polynomial $f_1,\ldots,f_s$, and we will denote it by $\Delta_{\mathcal{S}}(f_1,\ldots,f_s)$, or simply $\Delta_{\mathcal{S}}$, as a generator of the principal ideal $\mathfrak{S}(M_\nu)$. It is defined up to an invertible element in k; in particular, in the universal case $k=\mathbb{Z}$ it is uniquely defined up to a sign.*

As a consequence of the definition of $\Delta_{\mathcal{S}}$, we know that $\Delta_{\mathcal{S}}$ is a gcd of a system of generators of $\mathfrak{F}(M_\nu)$. We are now going to explicit its link with the annihilator of $\mathrm{ann}_A(M_\nu)$. But before, observe that if $s=n$ and $\nu\geq\eta$ then $\mathcal{S}$ must be the empty set and $\Delta_{\{\emptyset\}}$ is nothing but the resultant of the polynomials $f_1,\ldots,f_n$ (up to an invertible element in $k^\times$). The following proposition, pointed out to me by Jean-Pierre Jouanolou in a personal communication, may be seen as the main property of the multivariate subresultants.

Proposition 3.19 *Assume that k is a noetherian UFD ring and that B_ν is A-torsion free. Then the ideal $\mathrm{ann}_A(M_\nu)$ is a principal ideal of A.*

Proof. We will denote hereafter by P the set of prime ideals of A which are minimal among the non-zero prime ideals of A, that is to say the set of prime ideals of height one. We will prove that the set $\mathrm{Ass}_A(M_\nu)$ of associated primes of the A-module M_ν is contained in P.

Let K be the fraction field of A and consider the K-vector space $V := B_\nu\otimes_A K$. Observe that its dimension equals $\mathrm{Char}(B_\nu)$ which is exactly the rank of the free A-module $\langle\mathcal{S}\rangle_A$. Since B_ν is A-torsion free, we deduce that the canonical map $B_\nu\to V$ is injective (actually its kernel is exactly the A-torsion of B_ν) and hence induces an injective map $M_\nu\hookrightarrow V/\langle\mathcal{S}\rangle_A$. Therefore $\mathrm{Ass}_A(M_\nu)\subset\mathrm{Ass}_A(V/\langle\mathcal{S}\rangle_A)$ and we claim that $\mathrm{Ass}_A(V/\langle\mathcal{S}\rangle_A)\subset P$, where we note that $V := B_\nu\otimes_K = \langle\mathcal{S}\rangle_A\otimes K =: \langle S\rangle_K$ (remember that $\langle\mathcal{S}\rangle_A$ is a free A-submodule of V whose rank is just the dimension of V over $K := \mathrm{Frac}(A)$).

To see this, consider the map

$$V\to\bigoplus_{\mathfrak{p}\in P}\frac{V}{\langle\mathcal{S}\rangle_{A_\mathfrak{p}}} : x\mapsto(\ldots,\overline{x}^{\mathfrak{p}},\ldots) \tag{3.5}$$

where $\langle\mathcal{S}\rangle_{A_\mathfrak{p}} := \langle\mathcal{S}\rangle_A\otimes_A A_\mathfrak{p}$. Remark that since A is a UFD ring (and hence a Krull ring) then for any $x\in V$ we have $\overline{x}^{\mathfrak{p}}=0$ for all $\mathfrak{p}\in P$ except for a finite number of such prime ideal in P (see e.g. [1, VII §1 n° 2, théorème 4]). The kernel of (3.5) is clearly $\cap_{\mathfrak{p}\in P}\langle S\rangle_{A_\mathfrak{p}}$ which equals $\langle S\rangle_A$ because $A=\cap_{\mathfrak{p}\in P}A_\mathfrak{p}$ (since A is a Krull ring, see again [1, VII §1 n° 2, théorème 4]) and $\langle S\rangle_A$ is a free A-module. Therefore we deduce that

$$\mathrm{Ass}_A(M_\nu)\subset\mathrm{Ass}_A(V/\langle S\rangle_A)\subset\cup_{\mathfrak{p}\in P}\mathrm{Ass}_A(V/\langle S\rangle_{A_\mathfrak{p}}).$$

Now, let us pick a prime ideal $\mathfrak{p}\in P$. If $V/\langle S\rangle_{A_\mathfrak{p}}=0$ then $\mathrm{Ass}_A(V/\langle S\rangle_{A_\mathfrak{p}})=\emptyset$. So assume that $V/\langle S\rangle_{A_\mathfrak{p}}\neq 0$ and let $0\neq\mathfrak{q}\in\mathrm{Ass}_A(V/\langle S\rangle_{A_\mathfrak{p}})$ (observe that $V/\langle S\rangle_A$ is torsion).

Since any element of $A \setminus \mathfrak{p}$ is invertible in $A_{\mathfrak{p}}$, it is clear that $\mathfrak{q} \subset \mathfrak{p}$ and we conclude that $\mathrm{Ass}_A(V/\langle S \rangle_{A_{\mathfrak{p}}}) = \{\mathfrak{p}\}$.

We have just proved that $\mathrm{Ass}_A(M_\nu) \subset P$. But since M_ν is a A-module of finite type we deduce that $A/\mathrm{ann}_A(M_\nu) \subset M_\nu^s$. Indeed, let $m_1, \ldots, m_s$ be a system of generators of M and denote by $\mathfrak{p}_i := \mathrm{ann}_A(m_i)$ for all i. Then we clearly have $\mathrm{ann}_A(M_\nu) = \cap_{i=1}^s \mathfrak{p}_i$ and hence the kernel of the canonical map

$$A \to \oplus_{i=1}^s Am_i : a \mapsto (am_1, \ldots, am_i, \ldots, am_s)$$

equals $\mathrm{ann}_A(M_\nu)$. It follows that $A/\mathrm{ann}_A(M_\nu) \subset M_\nu^s$ since Am_i is a submodule of M_ν for all $i = 1, \ldots, s$. Therefore, we obtain that $\mathrm{Ass}_A(A/\mathrm{ann}_A(M_\nu)) \subset \cup_{i=1}^s \mathrm{Ass}_A(M_\nu) \subset P$. Since we assumed that A is a noetherian UFD ring, this implies that $\mathrm{ann}_A(M_\nu)$ is a principal ideal of A (see [1, VII, §1, n° 7, proposition 10 and §3, n° 2, théorème 1]). □

It appears that the absence of A-torsion of certain graded part of the quotient algebra B is a key point in the existence of the subresultants $\Delta_{\mathcal{S}}$. The following lemma, taken from [21, proposition 2.12] (see also [23, proposition 3.1.6.]), characterizes those graded parts of B without A-torsion.

Lemma 3.20 *The A-module B_ν is torsion free if either $1 \leq s < n$ or $s = n$ and $\nu < \eta := d_1 + \cdots + d_n - n + 1$.*

Proof. Assume first that $s < n$. From lemma 3.10 and proposition 3.11 we deduce that $I := (f_1, \ldots, f_s)$ is a prime ideal of C. Therefore $B = C/I$ is a domain and hence B_ν is A-torsion free (remember that k is a domain) for any integer ν.

We now turn to the second case which is much more intricate; we assume that $s = n$ and we want to prove that B_ν is A-torsion free for all integer ν such that $0 \leq \nu < \eta$. We first claim that for all integer ν such that $0 \leq \nu < \eta$ the pairing of A-modules

$$B_\nu \times B_{\eta-1-\nu} \to B_{\eta-1} : (x, y) \to xy \tag{3.6}$$

is non-degenerated. Indeed, let $x \in B_\nu$ such that $xB_{\eta-1-\nu} = 0$. Then it is clear that $\mathfrak{m}^{\eta-1-\nu}x = 0$ in B_ν. So we deduce that $x \in H^0_{\mathfrak{m}}(B)_\nu$ and more precisely that x is in the kernel of the canonical map

$$H^0_{\mathfrak{m}}(B)_\nu \to \mathrm{Hom}_A(B_{\eta-1-\nu}, H^0_{\mathfrak{m}}(B)_{\eta-1}) : x \mapsto (b \mapsto xb).$$

We want to prove that this kernel is zero. From the computation we did at the end of the section 3.1.4, we know that $H^0_{\mathfrak{m}}(C)_{-n} \simeq A$ an that we have isomorphisms (coming from the perfect duality)

$$H^0_{\mathfrak{m}}(C)_{-m-n} \xrightarrow{\sim} \mathrm{Hom}_A(C_m, H^0_{\mathfrak{m}}(C)_{-n}) : x \mapsto (c \mapsto xc)$$

for all relative integer $m \in \mathbb{Z}$. We thus deduce that

$$H^0_{\mathfrak{m}}(C)_{\nu-d_1-\cdots-d_n} = H^0_{\mathfrak{m}}(C)_{(\nu-\eta+1)-n} \xrightarrow{\sim} \mathrm{Hom}_A(C_{\eta-1-\nu}, H^0_{\mathfrak{m}}(B)_{\eta-1}).$$

But in the proof of lemma 3.13, we shown that

$$H^0_{\mathfrak{m}}(B)_\nu \simeq \mathrm{Ker}\left(H^n_{\mathfrak{m}}(C)_{\nu-d_1-\cdots-d_n} \xrightarrow{{}^t(f_1,\ldots,f_n)} \oplus_{i=1}^n H^n_{\mathfrak{m}}(C)_{\nu-d_1-\cdots-d_n+d_i}\right).$$

Therefore, we have

$$H^0_{\mathfrak{m}}(B)_\nu \simeq \{u \in \mathrm{Hom}_A(C_{\eta-1-\nu}, H^0_{\mathfrak{m}}(B)_{\eta-1})) \text{ s.t. } u(xf_i) = 0\, \forall j = 1,\ldots,n \text{ and } \forall x \in C_{\eta-1-\nu}\}$$

which shows that $H^0_{\mathfrak{m}}(B)_\nu \simeq \mathrm{Hom}_A(B_{\eta-1-\nu}, H^0_{\mathfrak{m}}(B)_{\eta-1}))$.

The paring (3.6) is hence non-degenerated. It follows that for all integer ν such that $0 \leq \nu < \eta$ we have a canonical inclusion

$$B_\nu \hookrightarrow \mathrm{Hom}_A(B_{\eta-1-\nu}, B_{\eta-1})$$

which implies that B_ν is A-torsion free if $B_{\eta-1}$ is so. Therefore, to complete the proof it only remains to prove that $B_{\eta-1}$ is A-torsion free. To do this, consider the exact sequence

$$0 \to H^0_{\mathfrak{m}}(B)_{\eta-1} \to B_{\eta-1} \to Q_{\eta-1} := B_{\eta-1}/H^0_{\mathfrak{m}}(B)_{\eta-1} \to 0.$$

Since $H^0_m(B)_{\eta-1} \simeq A$ we deduce that for any ideal K of A we have an exact sequence

$$0 \to H^0_K(A) \to H^0_K(B_{\eta-1}) \to H^0_K(Q_{\eta-1}).$$

But since A is a domain $H^0_K(A) = 0$ for all ideal K. Moreover, $\mathfrak{A}$ annihilates $Q_{\eta-1}$ (one immediately check that $\mathfrak{A}B_{\eta-1} \subset H^0_{\mathfrak{m}}(B)_{\eta-1}$ since $\mathfrak{A} = H^0_{\mathfrak{m}}(B)_0$), and hence $H^0_K(Q_{\eta-1})$, so we deduce that $\mathfrak{A}H^0_K(B)_{\eta-1} = 0$ and therefore that

$$H^0_K(B_{\eta-1}) \subset H^0_{\mathfrak{A}}(B)_{\eta-1}.$$

It turns out that $H^0_{\mathfrak{A}}(B)_{\eta-1} = 0$: this is a consequence of the proof of the theorem 3.16 (see [23, lemme 3.1.5] for the details). □

Corollary 3.21 *Assume that $s < n$ or $s = n$ and $\nu < \eta$. Then, $\Delta_{\mathcal{S}} \in \mathrm{ann}_A(M_\nu)$. Moreover the prime divisors of $\Delta_{\mathcal{S}}$ are the same of the prime divisors of any generator of $\mathrm{ann}_A(M_\nu)$. In particular if Δ_S is prime then $(\Delta_{\mathcal{S}}) = \mathrm{ann}_A(M_\nu)$.*

Proof. These are immediate consequences of the properties of MacRae's invariants. □

Corollary 3.22 ([10], theorem 2) *Let $\mathbb{K}$ be a field and $\rho : A \to \mathbb{K}$ a map of rings (a specialization map). Then we have*

$$\rho(\Delta_{\mathcal{S}}) \neq 0 \iff \langle S\rangle_A + (\rho(f_1),\ldots,\rho(f_s))_\nu = k[X_1,\ldots,X_n]_\nu.$$

Let us compute the multi-degree of $\Delta_{\mathcal{S}}$ in the coefficients of each polynomials $f_1, \ldots, f_s$. To do this, we use the fact that $\Delta_{\mathcal{S}}$ is a generator of the MacRae's invariant $\mathfrak{S}(M_\nu)$ and we proceed as for the case of resultants: (see the end of section 3.3). A straightforward extension of the computations we made at the end of section 3.3 show immediately that we have a graded isomorphism

$$(\Delta_{\mathcal{S}}) \simeq A(-S(T)_{|T^{\nu-d_1}}, \ldots, -S(T)_{|T^{\nu-d_i}}, \ldots, -S(T)_{|T^{\nu-d_n}}),$$

where $S(T) := \prod_{i=1}^{s}(1-T^{d_i})/(1-T)^n$.

We end this paragraph by emphasizing that the irreducibility of the multivariate subresultants seems to be a difficult problem. For now, it is only proved in [5] that $\Delta_{\mathcal{S}}$ is a prime element of A if $k = \mathbb{Z}$ and if $\nu > \eta - \min_i\{d_i\}$ (there is an example showing that this inequality is sharp, that is to say that there exists a reducible subresultant with $\nu = \eta - \min_i\{d_i\}$). Point out that in [9] it is proved that the A-module M_ν is $\mathbb{Z}$-torsion free, i.e. $\mathrm{Tor}_1^{\mathbb{Z}}(M_\nu, N) = 0$ for any $\mathbb{Z}$-module N (it is actually proved in [9] that $\mathrm{Tor}_1^{\mathbb{Z}}(M_\nu, \mathbb{Z}/p\mathbb{Z}) = 0$ for any prime integer p, which is sufficient to get the claimed result), if $\nu \geq \eta - \min_i\{d_i\}$.

4 Implicitization of rational hypersurfaces in a projective space

Let k be a field and A be a $\mathbb{N}$-graded k-algebra. Suppose given two integers $n \geq 2$, $d \geq 1$ and for all $i = 1, \ldots, n$ an element $f_i \in A_d$. Then, the k-algebra morphism

$$\begin{array}{rcl} h : k[T_1, \ldots, T_n] & \to & A \\ T_i & \mapsto & f_i \end{array} \tag{4.1}$$

gives rise to a k-schemes morphism

$$\begin{array}{rcl} \lambda : \mathrm{Proj}(A) & \to & \mathbb{P}_k^{n-1} \\ x & \mapsto & (f_1(x) : f_2(x) : \cdots : f_n(x)) \end{array} \tag{4.2}$$

whose closed image (the smallest k-scheme containing the image) is defined by the ideal $\mathrm{Ker}(h)$, that is to say that this closed image is $\mathrm{Proj}(k[\mathbf{T}]/\mathrm{Ker}(h)) = \mathrm{Proj}(k[\mathbf{T}]/\mathrm{Ker}(h)^{sat}) \subset \mathbb{P}_k^{n-1}$. Recall that an ideal of $k[\mathbf{T}]$ defines a closed subscheme in $\mathbb{P}_k^{n-1}$ up to saturation. In particular, the biggest ideal defining the closed image of λ is $\mathrm{Ker}(h)^{sat} := \mathrm{Ker}(h) :_{k[\mathbf{T}]} (\mathbf{T})^\infty$.

If we assume that A is a domain of dimension $n-1$ and that the parameterization map λ is generically finite onto its image, then it turns out that the ideal $\mathrm{Ker}(h)$ is a *prime* and *principal* ideal of $k[\mathbf{T}]$, that is to say that the closed image of λ is an irreducible hypersurface in $\mathbb{P}_k^{n-1}$. Indeed, it is a prime ideal because we have a canonical inclusion $k[\mathbf{T}]/\mathrm{Ker}(h) \hookrightarrow A$ and A is a domain, and it is a principal ideal because $\dim(k[\mathbf{T}]/\mathrm{Ker}(h)) = \dim(A) = n-1$ (since λ is generically finite [12, chapter 9]) and the well-known property saying that a

codimension one ideal in a factorial ring is a principal ideal. Consequently, any generator of $\mathrm{Ker}(h)$ will be called an *implicit equation* of the closed image of λ.

The aim of this last part is to provide techniques to "compute" such a closed image as a MacRae's invariant when A is the polynomial ring $k[X_1, \ldots, X_{n-1}]$. However, since some of the results can be stated for more general rings we will often precise the hypothesis we require on the ring A.

4.1 The degree formula

We always suppose that k is a field and we denote by C the polynomial ring $k[X_1, \ldots, X_r]$ which is $\mathbb{N}$-graded by putting $\deg(X_i) = 1$ for all $i = 1, \ldots, r$. Our concern here is to give a formula for the degree of the closed image of λ (which will be a hypersurface) providing

- the ring A is a $\mathbb{N}$-graded k-algebra of the form C/J, where J is a homogeneous prime ideal of C,
- $\mathrm{Proj}(A/I)$ is a zero-dimensional scheme (possibly empty), where I denotes the ideal $(f_1, \ldots, f_n) \subset A$,
- λ is generically finite onto its image (meaning that $\mathrm{Proj}(A)$ and the image of λ have the same dimension).

In order to state this formula we need to recall quickly the notions of algebraic and geometric multiplicities and state some useful properties. We refer the interested reader to [2] for a detailed treatment of this subject.

4.1.1 Geometric multiplicity.

For all $\mathbb{Z}$-graded finite C-module M one defines the *Hilbert series* of M:

$$\mathrm{H}_M(T) = \sum_{\nu \in \mathbb{Z}} \mathrm{length}_k(M_\nu) T^\nu = \sum_{\nu \in \mathbb{Z}} \dim_k(M_\nu) T^\nu.$$

If δ denotes the Krull dimension of M, there exists a unique polynomial $L_M(T)$ such that $L_M(1) \neq 0$ and

$$\mathrm{H}_M(T) = \sum_{\nu \in \mathbb{Z}} \dim_k(M_\nu) T^\nu = \frac{L_M(T)}{(1-T)^\delta}.$$

The number $L_M(1)$ is an invariant of the module M called the *multiplicity* of M; we will denote it by $\mathrm{mult}(M) := L_M(1)$. Another way to obtain this invariant is the *Hilbert polynomial* of M, denoted $\mathrm{P}_M(X)$. It is a polynomial of degree $\delta - 1$ such that $\mathrm{P}_M(\nu) = \dim_k(M_\nu)$ for all sufficiently large $\nu \in \mathbb{N}$. The Hilbert polynomial is of the form

$$\mathrm{P}_M(X) = \frac{a_{\delta-1}}{(\delta-1)!} X^{\delta-1} + \ldots + a_0,$$

and we have the equality $\text{mult}(M) = L_M(1) = a_{\delta-1}$.

Such a definition of multiplicity for M is called a *geometric* multiplicity and is also often called the degree of M because of its geometric meaning. Indeed, let J be a graded ideal of C and consider the quotient ring $R = C/J$. If δ denotes the dimension of R then the subscheme $\text{Proj}(R)$ of $\mathbb{P}_k^{n-1}$ is of dimension $\delta - 1$. The degree of $\text{Proj}(R)$ over $\mathbb{P}_k^{n-1}$ is defined to be the number of points obtained by cutting out $\text{Proj}(R)$ by $\delta - 1$ generic linear forms. To be more precise, if $l_1, \ldots, l_{\delta-1}$ are generic linear forms of $\mathbb{P}_k^{n-1}$, then the scheme $S = \text{Proj}(R/(l_1, \ldots, l_{\delta-1}))$ is finite and we set

$$\deg_{\mathbb{P}_k^{r-1}}(\text{Proj}(R)) := \dim_k \Gamma(S, \mathcal{O}_S) = \dim_k \left(\frac{R_\nu}{(l_1, \ldots, l_{\delta-1})_\nu} \right)$$

for all sufficiently large ν. It turns out that this geometric degree equals the multiplicity of R, i.e. we have

$$\deg_{\mathbb{P}_k^{r-1}}(\text{Proj}(R)) = \text{mult}(R) = L_M(1) = a_{d-1}.$$

To see it, just observe that the exact sequence

$$0 \to R(-1) \xrightarrow{\times l_1} R \to R/(l_1) \to 0$$

shows that $\text{H}_{R/(l_1)}(T) = (1-T)\text{H}_R(T) = L_M(T)/(1-T)^{\delta-1}$. The above equality is then obtain with an easy recursion.

4.1.2 Algebraic multiplicity.

Let $(R, \mathfrak{m})$ be a local noetherian ring and $M \neq 0$ a finite R-module. Let $I \subset \mathfrak{m}$ be an ideal of R such that there exists an integer t satisfying $\mathfrak{m}^t M \subset IM$ (any such ideal is called a definition ideal of M), the numerical function $\text{length}(M/I^\nu M)$ is a polynomial function for sufficiently large values of $\nu \in \mathbb{N}$. This polynomial, denoted $\text{S}_M^I(X)$, is called the *Hilbert-Samuel* polynomial of M with respect to I. It is of degree $\delta = \dim(M)$ and of the form:

$$\text{S}_M^I(X) = \frac{e(I, M)}{\delta!} X^\delta + \textit{terms of lower powers in } X.$$

The algebraic multiplicity of I in M is the number $e(I, M)$ appearing in this polynomial. With such a definition of algebraic multiplicity one can define the algebraic multiplicity of a zero-dimensional subscheme as follows: let J be a graded ideal of a $\mathbb{N}$-graded ring R, then if $T = \text{Proj}(R/J)$ is a finite subscheme of $\text{Proj}(R)$, its algebraic multiplicity is

$$e(T, \text{Proj}(R)) = e(J^\sharp, R^\sharp) = \sum_{t \in T} e(J_t^\sharp, \mathcal{O}_{\text{Proj}(R),t}) = \sum_{t \in T} e(J_t, R_t).$$

4.1.3 The degree formula.

We recall that if λ is assumed to be generically finite onto its image, then the function field of $\text{Proj}(A)$ is a finite extension field of the function field of the image of λ and its degree is

called *the degree of* λ (note that we abuse notation since we should say "the degree of the co-restriction of λ to its image"). More precisely, the fields inclusion is explicitly given by

$$0 \to \mathrm{Frac}(k[\mathbf{T}]/\mathrm{Ker}(h)) \hookrightarrow \mathrm{Frac}(A) : T_i \mapsto f_i.$$

Theorem 4.1 *Suppose that k is a field and that A is a $\mathbb{N}$-graded k-algebra of the form $k[X_1, \ldots, X_r]/J$, where J is a prime homogeneous ideal and each X_i is of degree one. Denote by δ the dimension of A and let $I = (f_1, \ldots, f_n)$ be an ideal of A such that each f_i is of degree $d \geq 1$. Then, if $T = \mathrm{Proj}(A/I)$ is finite over k, the number*

$$d^{\delta-1}\deg_{\mathbb{P}^{r-1}_k}(\mathrm{Proj}(A)) - e(T, \mathrm{Proj}(A))$$

equals

$$\begin{cases} \deg(\lambda).\deg_{\mathbb{P}^{n-1}_k}(H) & \text{if } \lambda \text{ is generically finite} \\ 0 & \text{if } \lambda\text{is not generically finite,} \end{cases}$$

where H denotes the closed image of λ.

Proof. The proof (we know) of this theorem is quite technical and beyond the scope of these notes. We refer the interested reader to [7, theorem 2.5] and also to [33, theorems 6.4 and 6.6]. □

4.2 Link with blow-up algebras

In this section, we assume that k is a ring and A is a $\mathbb{N}$-graded k-algebra such that $k = A_0$. We again consider the k-algebra morphism

$$\begin{array}{rccc} h: & k[T_1, \ldots, T_n] & \longrightarrow & A \\ & T_i & \mapsto & f_i, \end{array}$$

where all the f_i's are supposed to have the same degree $d \geq 1$. We will focus on two blow-up algebras associated to the ideal $I := (f_1, \ldots, f_n)$ of A, the Rees algebra $\mathrm{Rees}_A(I)$ and the symmetric algebra $\mathrm{Sym}_A(I)$, and show their close relation with the ideal $\mathrm{Ker}(h)$ of $k[T_1, \ldots, T_n]$.

4.2.1 The Rees algebra.

The Rees algebra of A with respect to the ideal I is the graded A-algebra

$$\mathrm{Res}_A(I) := A \oplus I \oplus I^2 \oplus I^3 \oplus \cdots$$

Introducing a new indeterminate Z, this algebra is classically obtained as the image of the A-algebra morphism

$$\begin{array}{rccc} \beta: A[T_1, \ldots, T_n] & \longrightarrow & A[Z] \\ T_i & \mapsto & f_i Z. \end{array}$$

In other words, $\mathrm{Rees}_A(I) \simeq A[\mathbf{T}]/\mathrm{Ker}(\beta)$ as bi-graded[7] $A[\mathbf{T}]$-modules. Moreover, we have the following simple description in the extended ring $A[\mathbf{T}, Z]$:

$$\mathrm{Ker}(\beta) = (T_1 - f_1 Z, T_2 - f_2 Z, \ldots, T_n - f_n Z) \cap A[\mathbf{T}]. \tag{4.3}$$

Proposition 4.2 *With the above notation,* $\mathrm{Ker}(h) = \mathrm{Ker}(\beta) \cap k[\mathbf{T}]$. *Moreover, if J is an ideal of A such that $H^0_J(A) = 0$, then we have* $\mathrm{Ker}(\beta) = \mathrm{Ker}(\beta) :_{A[\mathbf{T}]} J^\infty$, *and therefore*

$$\mathrm{Ker}(h) = \mathrm{Ker}(\beta) \cap k[\mathbf{T}] = (\mathrm{Ker}(\beta) :_{A[\mathbf{T}]} J^\infty) \cap k[\mathbf{T}].$$

Proof. Let $P \in k[\mathbf{T}]$ such that $\beta(P) = P(f_1 Z, f_2, Z, \ldots, f_n Z) = 0$ in $A[Z]$. By specializing Z to 1 we deduce that $P \in \mathrm{Ker}(h)$. Now, let $P \in \mathrm{Ker}(h)$. Since $\mathrm{Ker}(h)$ is a homogeneous ideal on may assume that P is homogeneous of degree $n \geq 0$. Then we have

$$\beta(P) = P(f_1 Z, f_2 Z, \ldots, f_n Z) = Z^n P(f_1, f_2, \ldots, f_n) = 0.$$

Regarding the second part of the proposition, we only have to prove that $\mathrm{Ker}(\beta) :_{A[\mathbf{T}]} J^\infty \subset \mathrm{Ker}(\beta)$ since the other inclusion is immediate. Let $P \in A[\mathbf{T}]$ such that there exist $n \in \mathbb{N}$ with the property $J^n P \subset \mathrm{Ker}(\beta)$. Then, we deduce that

$$J^n P(f_1 Z, f_2 Z, \ldots, f_n Z) = 0 \in A[Z].$$

But $H^0_J(A[Z]) = H^0_J(A)[Z] = 0$ by hypothesis, and it follows that $P(f_1 Z, f_2 Z, \ldots, f_n Z) = 0$ in $A[Z]$. □

Let us point out two consequences of this proposition. First, If we see $\mathrm{Ker}(\beta)$ as a graded A-module, then $\mathrm{Ker}(\beta)_0 = \mathrm{Ker}(h)$. It follows that one may obtain a generator of $\mathrm{Ker}(h)$, in the case it is principal, from certain minimal systems of generators for $\mathrm{Ker}(\beta)$. For instance, assume that $A = k[X_1, \ldots, X_{n-1}]$ and that $f_1, \ldots, f_n$ define a rational hypersurface in $\mathrm{Proj}(k[\mathbf{T}])$. Then, Gröbner basis computations on the ideal (4.3) with a lex-order satisfying $X_1 > X_2 > \cdots > X_{n-1} > Z$ will return a minimal system of generators of $\mathrm{Ker}(\beta)$ containing a unique element in $k[\mathbf{T}]$ which is an implicit equation of this hypersurface. Second, always under the previous assumptions on the ring A, regarding $\mathrm{Rees}_A(I)$ as a A-graded module we easily see that $H^0_{\mathfrak{m}}(\mathrm{Rees}_A(I)) = (\mathrm{Ker}(\beta) :_{A[\mathbf{T}]} \mathfrak{m}^\infty)/\mathrm{Ker}(\beta) = 0$ as soon as $H^0_{\mathfrak{m}}(A) = 0$ where $\mathfrak{m} = (X_1, \ldots, X_{n-1})$. Therefore, using section 1 we deduce immediately that for all $\nu \in \mathbb{N}$ we have

$$\mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Rees}_A(I)_\nu) = \mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Rees}_A(I)_0) = \mathrm{Ker}(\beta) \cap k[\mathbf{T}] = \mathrm{Ker}(h).$$

Although the Rees algebra has this very nice property, there is a significant drawback: in general, there is no known "universal" resolution of this algebra. We thus turn to its closer related blow-up algebra:

[7] there is a grading coming from A and another grading coming from the T_i's, setting $\deg(T_i) = 1$ for all $i = 1, \ldots, n$

4.2.2 The symmetric algebra.

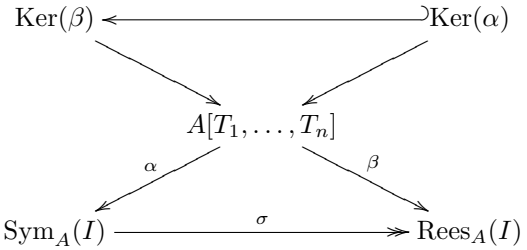
This well-known algebra can be described by the surjective morphism of A-algebras

$$\begin{array}{rcl} \alpha : A[T_1, \ldots, T_n] & \longrightarrow & \mathrm{Sym}_A(I) \to 0 \\ T_i & \mapsto & f_i, \end{array}$$

whose kernel is described by

$$\mathrm{Ker}(\alpha) = \{T_1 g_1 + \ldots + T_n g_n \text{ such that } g_i \in A[\mathbf{T}] \text{ and } \sum_{i=1}^{n} f_i g_i = 0\}.$$

The symmetric algebra of I appears naturally by its link with the Rees algebra of I (see for instance [35]). We have the following commutative diagram



where σ denotes the canonical map from $\mathrm{Sym}_A(I)$ to $\mathrm{Rees}_A(I)$. In fact the quotient $\mathrm{Ker}(\beta)/\mathrm{Ker}(\alpha)$ has been widely studied as it gives a measure of the difficulty in examining the Rees algebra of I. We recall that the ideal I is said to be of *linear type* if the canonical map σ is an isomorphism.

Lemma 4.3 *Let J be an ideal of A such that the ideal I is of linear type outside $V(J)$ then*

$$\mathrm{Ker}(\alpha) :_{A[\mathbf{T}]} J^\infty = \mathrm{Ker}(\beta) :_{A[\mathbf{T}]} J^\infty.$$

If moreover $H^0_J(A) = 0$ then $\mathrm{Ker}(\beta) = \mathrm{Ker}(\alpha) :_{A[\mathbf{T}]} J^\infty$.

Proof. The first assertion comes by definition: if I is of linear type outside $V(J)$ then the $A[\mathbf{T}]$-module $\mathrm{Ker}(\beta)/\mathrm{Ker}(\alpha)$ is supported in $V(J)$, that is

$$J.A[\mathbf{T}] \subset \sqrt{J.A[\mathbf{T}]} \subset \sqrt{\mathrm{ann}_{A[\mathbf{T}]}(\mathrm{Ker}(\beta)/\mathrm{Ker}(\alpha))},$$

which implies $\mathrm{Ker}(\alpha) :_{A[\mathbf{T}]} J^\infty = \mathrm{Ker}(\beta) :_{A[\mathbf{T}]} J^\infty$. The second statement is a consequence of the first one and proposition 4.2. □

We are now in position to state the key result of our approach to the implicitization problem.

Proposition 4.4 *Assume that k is a field and A is the polynomial ring $k[X_1, \ldots, X_{n-1}]$. Let η be an integer such that $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0$ for all $\nu \geq \eta$, where $\mathrm{Sym}_A(I)$ is seen as a graded A-module. Then*

$$\mathrm{Ker}(h) \supseteq \mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Sym}_A(I)_\nu) \quad \textit{for all} \quad \nu \geq \eta.$$

Moreover, if the ideal I is of linear type outside $V(\mathfrak{m})$, where $\mathfrak{m} = (X_1, \ldots, X_{n-1})$, then

$$\mathrm{Ker}(h) = \mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Sym}_A(I)_\nu) \quad \textit{for all} \quad \nu \geq \eta.$$

Proof. This is a consequence on the discussion and properties developed in the general setting of section 1 with $B := \mathrm{Sym}_A(I)$ regarded as a graded A-module (we want to eliminate the X_i's). By proposition 1.2, the hypothesis $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0$ for all $\nu \geq \eta$ implies that, for all $\nu \geq \eta$,

$$\mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Sym}_A(I)_\nu) = \mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Sym}_A(I)_\eta) = H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_0.$$

Now, proposition 4.2 shows, since $H^0_{\mathfrak{m}}(A) = 0$, that $\mathrm{Ker}(h) = (\mathrm{Ker}(\beta) :_{k[\mathbf{T}]} \mathfrak{m}^\infty) \cap k[\mathbf{T}]$. Since we always have $\mathrm{Ker}(\alpha) \subseteq \mathrm{Ker}(\beta) \subseteq A[\mathbf{T}]$, we deduce that

$$\mathrm{Ker}(h) = (\mathrm{Ker}(\beta) :_{k[\mathbf{T}]} \mathfrak{m}^\infty) \supseteq (\mathrm{Ker}(\alpha) :_{k[\mathbf{T}]} \mathfrak{m}^\infty) = H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_0.$$

If moreover I is assumed to be of linear type outside $V(\mathfrak{m})$ then lemma 4.3 implies that

$$(\mathrm{Ker}(\beta) :_{k[\mathbf{T}]} \mathfrak{m}^\infty) = (\mathrm{Ker}(\alpha) :_{k[\mathbf{T}]} \mathfrak{m}^\infty),$$

which completes the proof. □

Under the hypotheses of this proposition, we deduce that for all $\nu \geq \eta$ the MacRae's invariant $\mathfrak{S}(\mathrm{Sym}_A(I)_\nu)$ equals $\mathrm{Ker}(h)$ up to a certain power. The purpose of the following section is to provide of finite free resolution of $\mathrm{Sym}_A(I)_\nu$ that will be used to compute a generator of this MacRae's invariant, i.e. an implicit equation of our parameterized hypersurface image of λ.

4.3 Approximation complexes

In this section we give the definition and some basic properties of the *approximation complexes*. These complexes was introduced in [32] and systematically developed in [18] and [19]. At their most typical, they are projective resolutions of the symmetric algebras of ideals and allow an in-depth study of the canonical morphism $\sigma : \mathrm{Sym}_A(I) \to \mathrm{Rees}_A(I)$, where I is an ideal of a given ring A. In what follows we only develop (sometimes without proof) those properties that directly affect the applications we are interested in. For a complete treatment on the subject we refer the reader to the previously cited articles.

4.3.1 Definition.

Let A be a ring and J be an ideal of A generated by r elements $a_1, \ldots, a_r$ (which we will often abbreviate with the bold letter $\mathbf{a}$). Let also $\mathbf{T} := (T_1, \ldots, T_r)$ be a sequence of new indeterminates. To both applications

$$u : A[T_1, \ldots, T_r]^r \xrightarrow{(a_1,\ldots,a_r)} A[T_1, \ldots, T_r] : (b_1, \ldots, b_r) \mapsto \sum_{i=1}^{r} b_i a_i,$$

$$v : A[T_1, \ldots, T_r]^r \xrightarrow{(T_1,\ldots,T_r)} A[T_1, \ldots, T_r] : (b_1, \ldots, b_r) \mapsto \sum_{i=1}^{r} b_i T_i,$$

we can associate both Koszul complexes $K(\mathbf{a}; A[\mathbf{T}])$ and $K(\mathbf{T}; A[\mathbf{T}])$ with respective differentials $d_{\mathbf{a}}$ and $d_{\mathbf{T}}$. One can easily check that these differentials satisfy the property $d_{\mathbf{a}} \circ d_{\mathbf{T}} + d_{\mathbf{T}} \circ d_{\mathbf{a}} = 0$, and therefore there exists three complexes, the so-called *approximation complexes*, which we denote

$$\begin{aligned} \mathcal{Z}_\bullet &= (\operatorname{Ker} d_{\mathbf{a}}, d_{\mathbf{T}}) \\ \mathcal{B}_\bullet &= (\operatorname{Im} d_{\mathbf{a}}, d_{\mathbf{T}}) \\ \mathcal{M}_\bullet &= (H_\bullet(K(\mathbf{a}; A[\mathbf{T}])), d_{\mathbf{T}}). \end{aligned}$$

The $\mathcal{Z}$-complex ends with the sequence $\operatorname{Ker}(u) \xrightarrow{v} A[T_1, \ldots, T_r] \to 0$. Since by definition

$$v(\operatorname{Ker}(u)) = \left\{ \sum_{i=1}^{r} b_i T_i \;\text{ such that }\; \sum_{i=1}^{r} b_i a_i = 0 \right\},$$

we deduce that

$$H_0(\mathcal{Z}) = \frac{A[T_1, \ldots, T_r]}{v(\operatorname{Ker}(u))} \simeq \operatorname{Sym}_A(J).$$

A similar argument applied to the $\mathcal{M}$-complex shows that

$$H_0(\mathcal{M}) \simeq \operatorname{Sym}_{A/J}(J/J^2).$$

More generally, one can check that $v(\operatorname{Ker}(u))$ annihilates the homology modules (over $A[\mathbf{T}]$) of $\mathcal{Z}, \mathcal{B}$ and $\mathcal{M}$ which are therefore modules over $\operatorname{Sym}_A(J)$. These homology modules have the following interesting property, which is probably one of the most important of the approximation complexes:

Proposition 4.5 *The homology modules of $\mathcal{Z}, \mathcal{B}$ and $\mathcal{M}$ do not depend on the generating set chosen for the ideal J.*

Proof. See proposition 3.2.6 and corollary 3.2.7 of [35] or [20, §3]. □

4.3.2 Proper sequences and an acyclicity criterion.

The acyclicity of the complex $\mathcal{Z}_\bullet$ bears a striking resemblance to that of an ordinary Koszul complex, with the role of regular sequences (see proposition 3.1 and attached remark 3.2) being played by the so-called proper sequences (see [20, §6]).

Definition 4.6 *Let A be a ring and suppose given a sequence $x_1, \ldots, x_r$ of elements in R. This sequence is called a* proper sequence *if*

$$x_{i+1} H_j(x_1, \ldots, x_i; A) = 0 \quad \text{for } i = 0, \ldots, r-1 \text{ and } j > 0,$$

where $H_j(x_1, \ldots, x_i; A)$ denotes, as in section 3.1, the j^{th} homology group of the Koszul complex $K_\bullet(x_1, \ldots, x_i; A)$.

Theorem 4.7 *Let A be a ring and I be an ideal of A. Consider the following statements:*

(i) *I is generated by a proper sequence,*

(ii) *the complex $\mathcal{Z}(I)_\bullet$ is acyclic.*

Then (i) implies (ii). Moreover, if A is a local noetherian ring $(A, \mathfrak{m}, k)$ with infinite residue field, then (i) and (ii) are equivalent. The same holds if A is a graded ring, where $A_0 = k$ is an infinite field and $\mathfrak{m}$ is its irrelevant ideal, which is finitely generated as an A_1-algebra and such that all $x_i \in \mathfrak{m}$ is a homogeneous element of positive degree.

Proof. This is proved in [20]. The first assertion is the theorem 12.5 (the ambient ring A does not need to be noetherian, which is the framework of [20], for that particular property), and the second assertion is the theorem 12.9. □

We use the above acyclicity criterion to derive the following one which is well suited for the application to the implicitization problem that we have in mind. However, we need to recall the

Proposition 4.8 *Let A be a ring and $\mathbf{x} := (x_1, \ldots, x_n)$ a sequence in A generating a proper ideal I in A. If $y_1, \ldots, y_m$ is a A-regular sequence generating and ideal J contained in the ideal I then*

$$H_{n+1-i}(\mathbf{x}; A) = 0 \quad \textit{for all} \quad i = 1, \ldots, m, \quad \textit{and}$$

$$H_{n-m}(\mathbf{x}; A) \simeq \mathrm{Ext}^m_A(A/I, A) \simeq \mathrm{Hom}_A(A/I, A/J) \simeq (J : I)/J.$$

Proof. See for instance theorem 1.6.16 in [2]. □

Proposition 4.9 *Let k be an infinite field and define $A := k[X_1, \ldots, X_{n-1}]$ and $\mathfrak{m} := (X_1, \ldots, X_{n-1})$. Suppose given an ideal $I = (f_1, \ldots, f_n)$ of A such that $\mathcal{P} := \mathrm{Proj}(A/I)$ is finite, then the following statements are equivalent.*

(i) $\mathcal{Z}_\bullet$ *is acyclic,*

(ii) $\mathcal{Z}_\bullet$ *is acyclic outside* $V(\mathfrak{m})$*,*

(iii) *the ideal* I *can be generated by a proper sequence,*

(iv) *the projective scheme* $\mathcal{P}$ *can be locally generated by a proper sequence in* $\mathrm{Proj}(A)$*,*

(v) *the projective scheme* $\mathcal{P}$ *can be locally generated by* $n-1$ *equations in* $\mathrm{Proj}(A)$*.*

Proof.

Clearly (i)⇒(ii) and (iii)⇒(iv); moreover, by theorem 4.7 we have (i)⇔(iii) and (ii)⇔(iv). Therefore, it remains to show, for instance, that (iv)⇒(v)⇒(iii).

Proving that (iv) implies (v) is clearly a local property at each point $\mathfrak{p} \in \mathcal{P}$. So let $(R, \mathfrak{p})$ be a local Cohen-Macaulay ring (observe that A is Cohen-Macaulay) of dimension $n-2$ and with infinite residue field. Suppose given an ideal $I \subset \mathfrak{p}$ of codimension (and hence depth) at least $n-2$ which can be generated by a proper sequence. Then, one may find a generating proper sequence $g_1, \ldots, g_n$ such that the sequence $g_1, \ldots, g_{n-2}$ is R-regular. Therefore, by proposition 4.8 and the definition 4.6 of a proper sequence, g_n must annihilates

$$H_1(g_1, \ldots, g_{n-1}; R) \simeq ((g_1, \ldots, g_{n-2}) : (g_1, \ldots, g_{n-1}))/(g_1, \ldots, g_{n-2}).$$

Now, since the ideal $(g_1, \ldots, g_{n-1})$ is unmixed (it is $\mathfrak{p}$-primary) then, by [36, proposition 3.2.3 and corollary 3.2.2], we know that the annihilator of $H_1(g_1, \ldots, g_{n-1}; R))$ is exactly $(g_1, \ldots, g_{n-1})$ itself. It follows that $g_n \in (g_1, \ldots, g_{n-1})$.

Now, assume (v). Since k is infinite and the support of $\mathcal{P}$ is finite, one can find a sequence of homogeneous elements $(g_1, \ldots, g_n)$ in A generating I such that the sequence $g_1, \ldots, g_{n-1}$ defines $\mathcal{P}$, that is to say that $((g_1, \ldots, g_{n-1}) : \mathfrak{m}^\infty) = (I : \mathfrak{m}^\infty)$ in A, and such that $g_1, \ldots, g_{n-2}$ is a A-regular sequence (and hence $g_1, \ldots, g_{n-1}$ is a proper sequence). It follows that $g_n \in ((g_1, \ldots, g_{n-1}) : \mathfrak{m}^\infty)$ (since it is obviously in $(I : \mathfrak{m}^\infty)$) and to conclude the proof, we need to show that g_n annihilates $H_1(g_1, \ldots, g_{n-1}; A)$. But as before, we have

$$\begin{aligned} H_1(g_1, \ldots, g_{n-1}; A) &\simeq \mathrm{Ext}_A(A/(g_1, \ldots, g_{n-1}), A) \simeq \mathrm{Ext}_A(A/((g_1, \ldots, g_{n-1}) : \mathfrak{m}^\infty), A) \\ &\simeq ((g_1, \ldots, g_{n-2}) : ((g_1, \ldots, g_{n-1}) : \mathfrak{m}^\infty))/(g_1, \ldots, g_{n-2}) \end{aligned}$$

(we can saturate the ideal $(g_1, \ldots, g_{n-1})$ thanks to the Exts properties; see [36, end of the proof of proposition 3.2.3]) and from [36, proposition 3.2.3 and corollary 3.2.2] we get that its annihilator is exactly $((g_1, \ldots, g_{n-1}) : \mathfrak{m}^\infty)$ (which is an unmixed ideal). □

Remark 4.10 *In the above proposition, note that conditions (i), (ii) and (v) are unaffected by extension of the base field. Therefore, the equivalence of these three assertions remains true if we drop the hypothesis that the field* k *is infinite.*

4.4 Implicitization by means of linear syzygies

It is now time to gather the various results we obtained in the above sections. Recall that we started from the rational map λ (4.2) whose image lives in $\mathbb{P}_k^{n-1}$ and which is canonically associated to a k-algebra morphism h (4.1) from $k[\mathbf{T}]$ to A. *From now on we will assume that A is the polynomial ring $A := k[X_1, \ldots, X_{n-1}]$ ($n \geq 3$) so that the closed image of λ is an irreducible hypersurface $\mathcal{H}$ in $\mathbb{P}_k^{n-1}$.*

Let us denote by I the ideal of A generated by the homogeneous polynomials $f_1, \ldots, f_n \in A$, all assumed to have degree $d \geq 1$, defining the rational parameterization λ. Recall that $\mathrm{Ker}(h) \subset k[\mathbf{T}]$ is the defining ideal of $\mathcal{H}$ in $\mathbb{P}_k^{n-1}$. In the previous sections, we proved that

- $\mathrm{Ker}(h)$ is a principal and prime ideal of $k[\mathbf{T}]$,
- There exists an integer η such that for all integer $\nu \geq \eta$ we have

$$\mathrm{Ker}(h) \supseteq \mathrm{ann}_{k[\mathbf{T}]}(\mathrm{Sym}(I)_\nu)$$

  with equality if I is of linear type outside $V(\mathfrak{m})$ (see proposition 4.4).
- $\mathcal{Z}_\bullet(I)$ is a projective bi-graded resolution of $\mathrm{Sym}(I)$ as soon as $\mathrm{Proj}(A/I)$ is finite and locally defined by at most $n-1$ equations.

All the ingredient are given to obtain an implicit equation of $\mathcal{H}$, that is to say a generator of the ideal $\mathrm{Ker}(h)$, as a MacRae's invariant of a certain graded parts of a $\mathcal{Z}$-approximation complex. In this aim, we will hereafter always assume that *k is a field* and that the projective scheme $\mathrm{Proj}(A/I)$ *is finite and locally defined by at most $n-1$ equations* - this means that the ideal I defines only a finite number of isolated points, possible zero, in $\mathbb{P}_k^{n-2}$ and that at each such point is locally generated by at most $n-1$ equations.

4.4.1 Bound on the saturation index.

We need to provide an upper bound of the saturation index of $\mathrm{Sym}(I)$ with respect to the graduation of A, that is a bound on the integer η such that $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0$ for all $\nu \geq \eta$. We recall that if M is a $\mathbb{N}$-graded module over a $\mathbb{N}$-graded ring then its initial degree is $\mathrm{indeg}(M) := \min\{\nu \in \mathbb{N} : M_\nu \neq 0\}$.

Lemma 4.11 *We define the integer*

$$\eta := (n-2)(d-1) - \mathrm{indeg}(I :_A \mathfrak{m}^\infty) \in \mathbb{N}.$$

Then, for all integer $\nu \geq \eta$ we have $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0$.

Proof. This lemma can be proved very similarly to lemma 3.13 but is much more technical. We refer the reader to [4]. □

4.4.2 The main theorem.

We are now ready to state the central result of this part. We recall that for each point $\mathfrak{p} \in \mathcal{P} := \mathrm{Proj}(A/I)$, often called a *base point* of the parameterization λ, we two multiplicities:

- the "degree", that we will denote by $d_{\mathfrak{p}}$, which $\dim_{A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}} A_{\mathfrak{p}}/I_{\mathfrak{p}}$
- the "multiplicity" which equals $e(I_{\mathfrak{p}}, R_{\mathfrak{p}})$ as defined in paragraph 4.1.2.

Moreover, we always have $e_{\mathfrak{p}} \geq d_{\mathfrak{p}}$ and this inequality is an equality if and only if $\mathfrak{p}$ can be generated by a regular sequence[8] (see [2, corollary 4.5.10]).

Theorem 4.12 *With the above notation, for all integer $\nu \geq \eta$ we have*

$$\mathrm{Ker}(h)^{\deg(\lambda)} \supseteq \mathfrak{S}(\mathrm{Sym}_A(I)_\nu) = \mathfrak{S}(\mathrm{Sym}_A(I)_\eta) \simeq k[\mathbf{T}](-d^{n-2} + \sum_{\mathfrak{p}\in \mathrm{Proj}(A/I)} d_{\mathfrak{p}})$$

where the last isomorphism is a graded isomorphism of $k[\mathbf{T}]$-modules. Moreover, the three following statements are equivalents

(i) $\mathrm{Proj}(A/I)$ *is locally of linear type,*

(ii) $\mathrm{Proj}(A/I)$ *is locally a complete intersection.*

(iii) *the above inclusion is an equality*

Sketch of proof. We refer the reader to [7] and [4] for a complete proof of this theorem that we will only outline.

We already know that $\mathfrak{S}(\mathrm{Sym}_A(I)_\nu)$ is contained in $\mathrm{Ker}(h)$ for all $\nu \geq \eta$. To prove that it is actually contained is $\mathrm{Ker}(h)^{\deg(\lambda)}$ we need to prove that

$$\mathrm{length}((\mathrm{Sym}_A(I)_\nu)_{\mathrm{Ker}(h)}) \geq \deg(\lambda) = \mathrm{length}((\mathrm{Rees}_A(I)_\nu)_{\mathrm{Ker}(h)})$$

where the last equality comes (implicitly) from the degree formula stated in theorem, but this is a consequence of the additivity of the length.

To compute the degree of a generator of $\mathfrak{S}(\mathrm{Sym}_A(I)_\nu)$, that we will denote by δ, we will use the formula given in proposition 2.12. We saw that the $\mathcal{Z}$-approximation complex associated to I is a projective resolution of $\mathrm{Sym}_A(I)$. By shifting correctly the $\mathcal{Z}_i$'s, it is actually a bi-graded resolution of $\mathrm{Sym}_A(I)$, the first grading being w.r.t. the grading in the X_i's and the second grading w.r.t.the T_i's; it is of the form

$$0 \to \mathcal{Z}_{n-1}((n-1)d; -(n-1)) \to \cdots \to \mathcal{Z}_2(2d; -2) \to \mathcal{Z}(d; -1) \to \mathcal{Z}_0(0,0) = A[\mathbf{T}]$$

(remember that its differentials are linear in the T_i's and that $\mathcal{Z}_i \hookrightarrow A[\mathbf{T}](-id; 0)$ for all $i \geq 0$). Therefore, taking the degree $\nu \geq \eta$ part of this complex with respect to the grading in

[8] One also often says that the base point $\mathfrak{p}$ is locally a complete intersection

the X_i's, on get a finite *linear* free resolution of $k[\mathbf{T}]$-modules of $\mathrm{Sym}_A(I)_\nu$ from we deduce that

$$\delta := \sum_{i=1}^{n-1}(-1)^{i+1} i \dim_k((Z_i)_{\nu+id}).$$

We have canonical graded exact sequences, $i = 0, \ldots, n-1$,

$$0 \to Z_{i+1} \to K_{i+1} \to B_i(-d) \to 0$$

and

$$0 \to B_i \to Z_i \to H_i \to 0$$

which shows that δ can be expressed in terms of the Hilbert polynomials of the K_i's and the H_i's. The contribution of the K_i's only depends on n and d, and hence equals to d^{n-2} (for $\nu \gg 0$) as it is the case when $\mathcal{P}$ is empty (in such case $\mathrm{Sym}_A(I)$ is of linear type and there is no base points; see [7, theorem 5.2]). The contribution of the H_i's only comes from Z_1 and Z_2 since $H_i = 0$ for all $i \geq 3$ and an easy computation shows that it is

$$(H_0)_{\nu+d} - 2((H_1)_{\nu+2d} - (H_0)_{\nu+2d}).$$

As $\deg H_1 = 2\deg\mathcal{P}$ (one may use for example that $(H_0)_\nu - (H_1)_\nu + (H_2)_\nu = 0$ for $\nu \gg 0$ and that $H_2 \simeq \omega_{R/I}$, the canonical module, up to a degree shift), this contribution is equal to $-\deg\mathcal{P} = -\sum_{\mathfrak{p}\in\mathcal{P}} d_\mathfrak{p}$ for $\nu \gg 0$.

We now turn to the proof of the equivalence of the three statements (i), (ii) and (iii). Let $X := \mathrm{Proj}(\mathrm{Rees}_A(I)) \subseteq Y := \mathrm{Proj}(\mathrm{Sym}_A(I)) \subset \mathbb{P}^{n-1} \times \mathbb{P}^n$. If $\mathcal{P}$ is locally of linear type, then $X = Y$, so that, by comparing degrees (see (4.4)), $\mathfrak{S}(\mathrm{Sym}_A(I)) = \mathrm{Ker}(h)^{\deg(\lambda)}$, $d_p = e_p$ for any $p \in \mathcal{P}$ and $\mathcal{P}$ is locally a complete intersection. So we just proved that $(i) \to (iii) \to (ii)$. The fact that (ii) implies (i) follows from standard properties of the $\mathcal{M}$-approximation complex, as proved in [7, first lines of the proof of theorem 5.7] □

Recall that we know from theorem 4.1 that

$$\mathrm{Ker}(h)^{\deg(\lambda)} \simeq k[\mathbf{T}](-d^{n-2} + \sum_{\mathfrak{p}\in\mathrm{Proj}(A/I)} e_p) \tag{4.4}$$

where the last isomorphism is again a graded isomorphism. It follows that when computing $\mathfrak{S}(\mathrm{Sym}_A(I)_\eta)$ as the determinant of the η^{th}-graded part of $\mathcal{Z}_\bullet$ we get an implicit equation of $\mathcal{H}$ to the power $\deg(\lambda)$ times an extraneous homogeneous element of degree $\sum_{\mathfrak{p}\in\mathrm{Proj}(A/I)} e_\mathfrak{p} - d_\mathfrak{p}$ (which equals zero as soon as the base points are locally complete intersection).

References

[1] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 5 à 7. [Commutative algebra. Chapters 5–7], Reprint.

[2] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[3] Laurent Busé. Resultants of determinantal varieties. *J. Pure Appl. Algebra*, 193(1-3):71–97, 2004.

[4] Laurent Busé and Marc Chardin. Implicitizing rational hypersurfaces using approximation complexes. J. Symbolic Computation (to appear) and math.AG/0301238.

[5] Laurent Busé and Carlos D'Andrea. On the irreducibility of multivariate subresultants. *C. R. Math. Acad. Sci. Paris*, 338(4):287–290, 2004.

[6] Laurent Busé, Mohamed Elkadi, and Bernard Mourrain. Using projection operators in computer aided geometric design. In *Topics in algebraic geometry and geometric modeling*, volume 334 of *Contemp. Math.*, pages 321–342. Amer. Math. Soc., Providence, RI, 2003.

[7] Laurent Busé and Jean-Pierre Jouanolou. On the closed image of a rational map and the implicitization problem. *J. Algebra*, 265(1):312–357, 2003.

[8] Marc Chardin. Implicitization using approximation complexes. To appear and math.AC/0503180.

[9] Marc Chardin. Sur l'indépendance linéaire de certains monômes modulo des polynômes génériques. *C. R. Acad. Sci. Paris Sér. I Math.*, 319(10):1033–1036, 1994.

[10] Marc Chardin. Multivariate subresultants. *J. Pure Appl. Algebra*, 101(2):129–138, 1995.

[11] Michel Demazure. Une définition constructive du résultant. Preprint of the "Notes Informelles de Calcul Formel", `http://www.gage.polytechnique.fr/notes/1984-1994.html`, may 1984.

[12] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[13] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[14] Hans-Bjørn Foxby. The MacRae invariant. In *Commutative algebra: Durham 1981 (Durham, 1981)*, volume 72 of *London Math. Soc. Lecture Note Ser.*, pages 121–128. Cambridge Univ. Press, Cambridge, 1982.

[15] I. M. Gel'fand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[16] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. A first course.

[17] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[18] J. Herzog, A. Simis, and W. V. Vasconcelos. Approximation complexes of blowing-up rings. *J. Algebra*, 74(2):466–493, 1982.

[19] J. Herzog, A. Simis, and W. V. Vasconcelos. Approximation complexes of blowing-up rings. II. *J. Algebra*, 82(1):53–83, 1983.

[20] J. Herzog, A. Simis, and W. V. Vasconcelos. Koszul homology and blowing-up rings. In *Commutative algebra (Trento, 1981)*, volume 84 of *Lecture Notes in Pure and Appl. Math.*, pages 79–169. Dekker, New York, 1983.

[21] J. P. Jouanolou. Singularités rationnelles du résultant. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 183–213. Springer, Berlin, 1979.

[22] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2):117–263, 1991.

[23] Jean-Pierre Jouanolou. Aspects invariants de l'élimination. *Adv. Math.*, 114(1):1–174, 1995.

[24] Jean-Pierre Jouanolou. Résultant anisotrope, compléments et applications. *Electron. J. Combin.*, 3(2):Research Paper 2, approx. 91 pp. (electronic), 1996. The Foata Festschrift.

[25] Jean-Pierre Jouanolou. Formes d'inertie et résultant: un formulaire. *Adv. Math.*, 126(2):119–250, 1997.

[26] Amit Khetan. Exact matrix formula for the unmixed resultant in three variables. *J. Pure Appl. Algebra*, 198(1-3):237–256, 2005.

[27] Finn Faye Knudsen and David Mumford. The projectivity of the moduli space of stable curves. I. Preliminaries on "det" and "Div". *Math. Scand.*, 39(1):19–55, 1976.

[28] Ernst Kunz. *Introduction to commutative algebra and algebraic geometry*. Birkhäuser Boston Inc., Boston, MA, 1985. Translated from the German by Michael Ackerman, With a preface by David Mumford.

[29] R. E. MacRae. On an application of the Fitting invariants. *J. Algebra*, 2:153–169, 1965.

[30] D. G. Northcott. *Finite free resolutions*. Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 71.

[31] Günter Scheja and Uwe Storch. *Regular sequences and resultants*, volume 8 of *Research Notes in Mathematics*. A K Peters Ltd., Natick, MA, 2001.

[32] A. Simis and W. V. Vasconcelos. The syzygies of the conormal module. *Amer. J. Math.*, 103(2):203–224, 1981.

[33] Aron Simis, Bernd Ulrich, and Wolmer V. Vasconcelos. Codimension, multiplicity and integral extensions. *Math. Proc. Cambridge Philos. Soc.*, 130(2):237–257, 2001.

[34] Wolmer V. Vasconcelos. Annihilators of modules with a finite free resolution. *Proc. Amer. Math. Soc.*, 29:440–442, 1971.

[35] Wolmer V. Vasconcelos. *Arithmetic of blowup algebras*, volume 195 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1994.

[36] Wolmer V. Vasconcelos. *Computational methods in commutative algebra and algebraic geometry*, volume 2 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman.

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399