The Resultant via a Koszul Complex

Marc Chardin

Équipe de Calcul Formel
Centre de Mathématiques
École Polytechnique
F–91128 Palaiseau cedex
e-mail : chardin@polytechnique.fr

Abstract. *As noticed by Jouanolou, Hurwitz proved in 1913 ([Hu]) that, in the generic case, the Koszul complex is acyclic in positive degrees if the number of (homogeneous) polynomials is less than or equal to the number of variables*[†]*. It was known around 1930 that resultants may be calculated as a Mc Rae invariant of this complex. This expresses the resultant as an alternate product of determinants coming from the differentials of this complex. Demazure explained in a preprint ([De]), how to recover this formula from an easy particular case of deep results of Buchsbaum and Eisenbud on finite free resolutions. He noticed that one only needs to add one new variable in order to do the calculation in a non generic situation.*

I have never seen any mention of this technique of calculation in recent reports on the subject (except the quite confidential one of Demazure and in an extensive work of Jouanolou, however from a rather different point of view). So, I will give here elementary and short proofs of the theorems needed—except the well-known acyclicity of the Koszul complex and the "Principal Theorem of Elimination"—and present some useful remarks leading to the subsequent algorithm. In fact, no genericity is needed (it is not the case for all the other techniques). Furthermore, when the resultant vanishes, some information can be given about the dimension of the associated variety.

As an illustration of this technique, we give an arithmetical consequence on the resultant : if the polynomials have integral coefficients and their reductions modulo a prime p defines a variety of projective dimension zero and degree d, then p^d divides the resultant.

I The tools

Let A be a noetherian and factorial domain, k its quotient field and $R = A[X_1, \ldots, X_n]$.

If $P_1, \ldots, P_n$ is a regular sequence of homogeneous polynomials in R, let I be the ideal generated by the P_i's, d_i the degree of P_i and $\mathbf{K}$ the associated Koszul complex:

$$\mathbf{K} \ : \ 0 \longrightarrow \bigwedge^n B \xrightarrow{\partial_n} \bigwedge^{n-1} B \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} \bigwedge^1 B \xrightarrow{\partial_1} R \longrightarrow 0$$

where B is the free R-module R^n equipped with the base $(e_1, \ldots, e_n)$ and the differentials ∂_p are defined by

$$\partial_p(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \sum_{s=1}^{p} (-1)^{s+1} P_{i_s} \ e_{i_1} \wedge \cdots \wedge \widehat{e_{i_s}} \wedge \cdots \wedge e_{i_p}.$$

If we introduce on the modules $K_p = \bigwedge^p B$ the natural graduation $\deg(e_{i_1} \wedge \cdots \wedge e_{i_p}) = d_{i_1} + \cdots + d_{i_p}$, this complex of A-modules **is graduated**, its differential is of degree zero, moreover, **up to the surjectivity of ∂_1 it is exact in all degrees** ([Se] IV Prop. 2, original proof in [Hu]).

We will write K_p^ν and ∂_p^ν for the degree ν parts of the modules and differentials.

[†] *at least in this generic case, the Koszul complex was thus known long before the general theory of Koszul complexes.*

Let us now recall a classical theorem from elimination theory:

Proposition 1.— *Let $A = \mathbf{Z}[U_{i,\alpha}]$ where the $U_{i,\alpha}$ are the algebraically independent coefficients of the generic homogeneous polynomials defined as $P_i = \sum_{|\alpha|=d_i} U_{i,\alpha} X^\alpha \in R = A[X_1, \dots, X_n]$ for $i = 1, \dots, n$.*

Then:

$$\mathrm{Ann}_A \left(R/(P_1, \dots, P_n)\right)_\nu = \mathrm{Res}(P_1, \dots, P_n)$$

if and only if $\nu > \sum_{i=1}^n (d_i - 1)$.

Proof. See [Jo2] §3.5 page 144.

We will now give the result we need from homological algebra.

If A is a noetherian factorial ring and M is a torsion A-module of finite type we will denote by $\mathrm{div}(M)$ the divisor associated to M:

$$\mathrm{div}(M) = \sum_{\mathcal{P} \in \mathrm{Ass}(M), h(\mathcal{P})=1} \mathrm{length}(M_{\mathcal{P}})\mathcal{P}$$

If I is an ideal of A, and $[I]$ the principal part of I (i.e. the gcd of generators of I), then $\mathrm{div}(R/I) = \sum_i e_i \mathcal{P}_i$ if $[I] = \prod_i \mathcal{P}_i^{e_i}$ is the decomposition into irreducible factors of the principal ideal $[I]$.

A good reference for theses concepts is [Bo] Chap. 7, §4.

Proposition 2.— *Let $\mathbf{C}$ be a complex of finitely generated free A-modules (A factorial and noetherian):*

$$\mathbf{C} \ : \ 0 \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \longrightarrow 0$$

and suppose that we have a decomposition $C_i = E_{i+1} \oplus E_i$, $E_0 = E_{n+1} = 0$, $\partial_p = \begin{pmatrix} a_p & \phi_p \\ b_p & c_p \end{pmatrix}$ where ϕ_p is an injective endomorphism of E_p.

Then the complex has only torsion homology, and we have:

$$\sum_i (-1)^i \mathrm{div}(H_i(\mathbf{C})) = \sum_i (-1)^i \mathrm{div}(\det \phi_{i+1}).$$

So if $H_i(\mathbf{C}) = 0$ for $i > 0$, the cokernel of ∂_1 being equal to $H_0(\mathbf{C})$, we have:

$$[\mathrm{Coker}(\partial_1)] = \prod_{i=1}^n (\det \phi_i)^{(-1)^{i+1}}.$$

Proof *(from Demazure's one).* The homology of $\mathbf{C} \otimes_A k$ is zero because ∂_i restricted to $E_i \otimes_A k$ is an automorphism. So $H(\mathbf{C})$ is torsion.

Let $\partial'_i = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}$, the complex $(\mathbf{C}, \partial')$ has zero homology and the application $f_n = id$, $f_i = \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix}$ for $i < n$ from C_i into himself defines a morphism from $(\mathbf{C}, \partial')$ to $(\mathbf{C}, \partial)$, as we have:

$$\partial_i \circ f_i = \begin{pmatrix} a_i & \phi_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix} = \begin{pmatrix} 0 & \phi_i \\ 0 & c_i \end{pmatrix} = \begin{pmatrix} \phi_i & 0 \\ c_i & I \end{pmatrix} \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} = f_{i-1} \circ \partial'_i.$$

f_i is into and $\mathrm{Coker}(f_i)$ can be identified with $\mathrm{Coker}(\phi_{i+1})$, so that we get the following diagram where the vertical sequences are exact:

$$\begin{array}{ccccccccccccc}
 & & & & 0 & & & & 0 & & 0 & & \\
 & & & & \uparrow & & & & \uparrow & & \uparrow & & \\
 & & 0 & \xrightarrow{\theta_n} & \mathrm{Coker}\phi_n & \xrightarrow{\theta_{n-1}} & \cdots & \xrightarrow{\theta_2} & \mathrm{Coker}\phi_2 & \xrightarrow{\theta_1} & \mathrm{Coker}\phi_1 & \rightarrow & 0 \\
 & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow & & \\
0 & \rightarrow & C_n & \xrightarrow{\partial_n} & C_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots & \xrightarrow{\partial_2} & C_1 & \xrightarrow{\partial_1} & C_0 & \rightarrow & 0 \\
 & & \uparrow f_n & & \uparrow f_{n-1} & & & & \uparrow f_1 & & \uparrow f_0 & & \\
0 & \rightarrow & C_n & \xrightarrow{\partial'_n} & C_{n-1} & \xrightarrow{\partial'_{n-1}} & \cdots & \xrightarrow{\partial'_2} & C_1 & \xrightarrow{\partial'_1} & C_0 & \rightarrow & 0 \\
 & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & & & 0 & & 0 & &
\end{array}$$

As we see, the complex of the cokernels have the same homology as $(\mathbf{C}, \partial)$, so we get:

$$\begin{aligned}\operatorname{div}(\operatorname{Coker}\ \phi_i) &= \operatorname{div}(\operatorname{Im}\ \theta_{i-1}) + \operatorname{div}(\ker\ \theta_{i-1}) \\ &= \operatorname{div}(\operatorname{Im}\ \theta_{i-1}) + \operatorname{div}(\operatorname{Im}\ \theta_i) + \operatorname{div}(H_{i-1}(\mathbf{C})).\end{aligned}$$

So the conclusion follows from the classical lemma ([Bo] Chap. 7, §4, n°6, corollary of prop. 13):

Lemma.—If ϕ is an injective endomorphism of a finitely generated free A-module M, we have:

$$\operatorname{div}(\operatorname{Coker}\ \phi) = \operatorname{div}(\det\ \phi)$$

Sketch of proof. Let $M' = \phi(M)$, $(e_i)_{i\in I}$ a base of M and P set of representatives of the irreducible elements of A. If $\mathcal{P} \in P$, $M'_{\mathcal{P}} \neq M_{\mathcal{P}}$ if and only if $\mathcal{P}$ divides $\det\phi$. So the two divisors have the same support. If we localize on such a $\mathcal{P}$, the ring $A_{\mathcal{P}}$ being principal, there exists two automorphisms ξ and ξ' of $M_{\mathcal{P}}$ such that $\xi \circ \phi \circ \xi'$ looks like $e_i \longmapsto \mathcal{P}^{d_i} e_i$, so $\det\phi = u\mathcal{P}^m$ with $m = \sum_i d_i$ and u a unit, and we have $M'_{\mathcal{P}} = \bigoplus_i \mathcal{P}^{d_i} A_{\mathcal{P}}$. The conclusion follows. ∎

Remarks.

1. The proposition 2 is also true if A is noetherian and integrally closed.

2. If the truncated Euler-Poincaré characteristics are positive (i.e. $\sum_{i=k}^{n-1}(-1)^{i-k}\operatorname{div} H_i(\mathbf{C})$ is effective), then $\Delta_k = \prod_{i=k}^{n-1}(\det\ \phi_{i+1})^{(-1)^{i-k}} \in A$ as

$$\sum_{i=k}^{n-1}(-1)^{i-k}\operatorname{div}\ (\det\ \phi_{i+1}) = \operatorname{div}\ (\operatorname{Im}\ \theta_k) + \sum_{i=k}^{n-1}(-1)^{i-k}\operatorname{div}\ (H_i(\mathbf{C})).$$

In particular, $\Delta_k \in A$ for $k \geq 0$ when $H_i(\mathbf{C}) = 0$ for $i > 0$.

If we have an exact sequence of finitely generated free A-modules of the form

$$0 \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$$

with $\sum(-1)^i \operatorname{Rank}_A(C_i) = 0$, then we may construct a decomposition of the C_i's in the following way:

• fix a base B_i for each C_i,

• choose a maximal non zero minor of ∂_n (there exists one because ∂_n is into). This choice splits B_{n-1} into two parts: $B_{n-1} = B'_n \cup B''_{n-1}$ where $\operatorname{card} B'_n = \operatorname{card} B_n$,

• the restriction of ∂_{n-i} to the module $A\langle B''_{n-i}\rangle$ is into so that we can iterate the process by choosing at each step a maximal minor of ∂_{n-i} restricted to $A\langle B''_{n-i}\rangle$, and therefore a decomposition $B_{n-i-1} = B'_{n-i-1} \cup B''_{n-i-1}$,

• the matrix of ∂_1 restricted to $A\langle B''_1\rangle$ is a square matrix because of the hypotheses on the ranks.

In the case of the Koszul complex of a complete intersection, the generating function for the rank of K_p^ν is

$$G(T_p, T_\nu) = \prod_{s=1}^{n} \frac{1 + T_\nu^{d_s} T_p}{1 - T_\nu},$$

so that the alternate sum of the ranks is equal to the coefficient of the degree ν term of $\prod_{s=1}^{n} \frac{1-T_\nu^{d_s}}{1-T_\nu}$ and therefore vanishes if and only if $\nu > \sum_i (d_i - 1)$.

II The Algorithm

From what we have seen above, we get the following algorithm to calculate the resultant of $P_1, \dots, P_n \in A[X_1, \dots, X_n]$ when A is a domain (all the operations are performed in A, because we *a priori* know that the divisions are exact):

(1) Put $\nu = \sum_{i=1}^n (\deg P_i - 1) + 1$ and calculate the matrices M_i of ∂_i^ν for the Koszul complex corresponding to the input polynomials.

(2) Put $i := n-1$, $\Delta_i = 1$.

(3) If M_i is not of maximal rank, $\mathrm{Res}(P_1, \dots, P_n) = 0$, end.

(4) Take a maximal submatrix M_i' of M_i with $D_i = \det M_i' \neq 0$, put $\Delta_{i-1} = D_i/\Delta_i$ and replace M_{i-1} by the minor of M_{i-1} obtained by erasing the columns corresponding to the lines which appears in M_i'.

(5) If $i > 1$ do $i := i-1$, and go to (3).

(6) $\Delta_0 = \pm \mathrm{Res}(P_1, \dots, P_n)$.

III Some remarks and an improvement of the algorithm

Remarks.

1. M_n is empty in degree $\nu = \sum_i (d_i - 1) + 1$.

2. It is clear that this algorithm works over any field (or domain) because:
• if one of the matrices is not of maximal rank the complex is not exact, so that the polynomials have a non trivial common zero and the resultant vanishes,
• if a determinant is not zero in one case, it is not zero in the generic case. So if a decomposition works in a specific case it works in the generic case and rises to the resultant.

3. If, **in the preceding algorithm**, $M_n, \dots, M_{i+1}$ are of maximal rank but M_i is not, there is no regular sequence of length $n-i+1$ constituted by elements of the ideal generated by the P_i's ([No] Chap. 8, Theorem 6, p. 371). So the dimension of the zero locus of the P_i's is at least i.

4. If A is any ring and the algorithm returns 0, then for every field k and every morphism $\varphi : A \longrightarrow k$, $\varphi(\mathrm{Res}(P_1, \dots, P_n)) = 0$; if the subring of A spanned by the coefficients of the P_i's is reduced this implies that the resultant is zero. So the algorithm gives the resultant over any reduced ring and returns 0 only if every specialization of the elements of A in any field (or domain) leads to a vanishing resultant.

5. It is easy to check that the alternate sum of the dimensions of the matrices M_i' (for $\nu = \sum_i (d_i - 1) + 1$ or bigger), is equal to the degree ν coefficient of $\frac{\partial G}{\partial T_p}(-1, T_\nu)$ and is therefore given by:

$$\begin{aligned}\frac{\partial G}{\partial T_p}(-1, T_\nu) &= \sum_{i=1}^n \left[\frac{T_\nu^{d_i}}{1 - T_\nu} \prod_{j \neq i} \frac{1 - T_\nu^{d_j}}{1 - T_\nu} \right] \\ &= \sum_{i=1}^n \Big[(T_\nu^{d_i} + T_\nu^{d_i+1} + \cdots) \prod_{j \neq i} (1 + T_\nu + \cdots + T_\nu^{d_j - 1}) \Big].\end{aligned}$$

From that we see that the resultant is an homogeneous polynomial in the coefficients of the generic polynomials of the expected total degree $\sum_{i=1}^n \prod_{j \neq i} d_j$.

6. For every i and every ν all the minors of the matrix M_k^ν of ∂_k^ν are homogeneous polynomials in the coefficients of the polynomials P_i's, because the entries of M_k^ν are either a coefficient of one of the P_i's or 0. Moreover theses polynomials are also homogeneous in the coefficients of each P_i.

Let us prove it, for example, for the coefficients of P_1. For this purpose, consider the partition of $S_k = \{e_{i_1} \wedge \cdots \wedge e_{i_k},\ 1 \leq i_1 < \cdots < i_k \leq n\}$ into $S_k' \cup S_k''$ where $S_k' = \{e_1 \wedge e_{i_2} \wedge \cdots \wedge e_{i_k},\ 2 \leq i_2 < \cdots i_k \leq n\}$ and $S_k'' = S_k - S_k'$.

If $e \in S_k'$, $\partial_k(e) = P_1 e'' + \sum_{k \geq 2} P_{i_k} e_k'$ with $i_k \geq 2$, $e'' \in S_{k-1}''$ and $e_k' \in S_{k-1}'$.

If $e \in S''_k$, $\partial_k(e) = \sum_{k\geq 1} P_{i_k} e''_k$ with $i_k \geq 2$ and $e''_k \in S''_{k-1}$.

So every submatrix N^ν_k of M^ν_k splits into four blocks (eventually empty):

$$N^\nu_k = \begin{pmatrix} \text{Coef. of} & 0 \\ P_i\text{'s } i>1 & \\ & \text{Coef. of} \\ \text{Coef. of } P_1 & P_i\text{'s } i>1 \end{pmatrix} = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

Suppose that A (resp. B and C) is an $m' \times n'$ (resp. $m'' \times n'$ and $m'' \times n''$) matrix. By a Laplace expansion we see that if $m' > n'$ we have $\det N^\nu_k = 0$ and if $m' \leq n'$ the determinant of N^ν_k is an homogeneous polynomial in the coefficients of P_1 of degree $n' - m' = m'' - n''$.

7. If the resultant is not zero, there exists a decomposition of the Koszul complex such that the determinant of the matrix M'_i does not depend of the coefficients of $P_{n-i+2}, \ldots, P_n$, because the fact that $P_1, \ldots, P_{n-i+1}$ is a regular sequence implies that $H^j(\mathbf{K}) = 0$ for $j \geq i$ independently of $P_{n-i+2}, \ldots, P_n$.

From the formula $\Delta_0\Delta_1 = D_1$ we see that, as the resultant actually depends on the coefficients of P_n and Δ_1 does not if we make an adapted decomposition, the resultant divides Δ_0 because of its irreducibility. As Δ_0 and the resultant have the same degree they must be equal up to a constant, the case $P_i = X_i^{d_i}$ shows that this constant is ± 1.

This shows that the algorithm produces the resultant, using only the classical definition of the resultant (see e.g. [Ma] or [Gr]) regardless to proposition 1.

An improvement of the algorithm.

From the two remarks above, we deduce that we can replace in the algorithm the matrix M^ν_i by the matrix $\hat{M}^\nu_i$ obtained from M^ν_i by replacing the coefficients of $P_{n-i+2}, \ldots, P_n$ by 0. Moreover, after this replacement, the matrix split into blocks and therefore the calculation is greatly simplified ; for example the maximal minor of $\hat{\partial}^\nu_{n-1}$ may always be chosen as the product of determinants of triangular submatrices of $\hat{\partial}^\nu_{n-1}$ and maximal minors of matrices representing $(A_1, A_2) \mapsto A_1P_1 + A_2P_2$ in some degrees.

On the other hand, after this substitution, if the algorithm stops before the calculation of D_1 you do not get any lower bound for the dimension of the associated variety.

IV An arithmetic consequence on the resultants

Let $P_1, \ldots, P_n$ be n homogeneous polynomials of $\mathbf{Z}[X_1, \ldots, X_n]$ and $r \in \mathbf{Z}$ their resultant. If p is a prime number, p divides r if and only if the reductions modulo p of these polynomials have a non trivial common zero in an algebraic closure of $\mathbf{F}_p$.

When the algebraic variety V_p associated to the reductions modulo p of the P_i's is of dimension zero and of degree d, we will prove that $v_p(r) \geq d$, where $v_p(r)$ is the p-adic valuation of r.

In this situation, it arrives that a bigger power of p divides r. Moreover, two n-tuples of polynomials with the same reductions modulo p may have different p-adic valuation of their resultants. However, an upper bound for the p-adic valuation of the resultant of the generic lifting of n homogeneous polynomials in $\mathbf{F}_p[X_1, \ldots, X_n]$ (with $\dim V_p = 0$) can be given. This bound is d when $n = 2$ but not in general. We will not be concern with this question here.

Let us fix some notations :

• $\mathbf{Z}[X_1, \ldots, X_n] \equiv \mathbf{Z}[\mathbf{X}]$ and $\mathbf{F}_p[X_1, \ldots, X_n] \equiv \mathbf{F}_p[\mathbf{X}]$.

• p is a prime number.

• $P_1, \ldots, P_n$ are n homogeneous polynomials in $\mathbf{Z}[\mathbf{X}]$ of respective degrees $d_1, \ldots, d_n$ and we will suppose, to avoid some trivial remarks, that they are not divisible by p.

• $\overline{P}_i$ is the image of P_i by the canonical homomorphism from $\mathbf{Z}[\mathbf{X}]$ to $\mathbf{F}_p[\mathbf{X}]$, V_p is the variety associated to the homogeneous ideal spanned by the polynomials $\overline{P}_i$ and d is the degree of V_p.

• $r \in \mathbf{Z}$ is the resultant of the P_i's.

• As before K_m^ν and ∂_m^ν are the homogeneous part of degree ν of K_m and ∂_m for the polynomials P_i with $A = \mathbf{Q}$ and, in a similar fashion, $\overline{K}_m^\nu$ and $\overline{\partial}_m^\nu$ with $A = \mathbf{F}_p$.

Our result is the following :

Proposition 3. *With the above notations, p^d divides r if $\dim V_p = 0$ and $\deg V_p = d$.*

As in remark 3 of section III, we notice that $\dim V_p = 0$ implies that $H_i(\overline{\mathbf{K}}) = 0$ for $i > 1$. And the proposition follows from two easy lemmas :

Lemma 1. *If $H_i(\overline{\mathbf{K}}) = 0$ for $i > 1$, the p-adic valuation of r is the minimum of the p-adic valuations of the maximal minors of ∂_1^ν for all ν strictly bigger than $\delta = \sum_{i=1}^n (d_i - 1)$.*

Proof. For all $\nu > \delta$, as $H_i(\overline{\mathbf{K}}^\nu) = 0$ for $i > 1$, the construction made in the algorithm (for the $\overline{P}_i$'s) gives for $m > 1$ some square submatrix M'_m of M_m (the matrix of ∂_m^ν) whose determinant is not divisible by p (because the matrix associated to $\overline{\partial}_m^\nu$ is the reduction mod p of M_m) and a square submatrix of maximal size M'_1 of M_1 such that $r = \pm \prod_{i=1}^n (\det M'_i)^{(-1)^{i+1}}$.

So the p-adic valuation of the resultant is the one of a maximal minor of ∂_1^ν, and this for all $\nu > \delta$. As the resultant divides all the maximal minors, the lemma follows. ∎

The corank of $\overline{\partial}_1^\nu$ is the Hilbert function of V_p in degree ν and therefore, for ν big enough, equal to the degree of V_p. It remains to show the elementary following lemma :

Lemma 2. *Let M be a square matrix with entries in $\mathbf{Z}$ whose reduction modulo p is a matrix of corank d, then p^d divides $\det M$.*

Proof. If $\overline{M}$ is the reduction modulo p of M, we can find two invertible matrices with entries in $\mathbf{F}_p$ such that : $A\overline{M}B = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$ where I is the identity of size $(n-d) \times (n-d)$. If we choose some liftings A' and B' of A and B in $\mathbf{Z}$, the determinant of the matrix $A'MB'$ has the same p-adic valuation as the one of M and is divisible by p^d as the last d lines of $A'MB'$ are divisible by p. ∎

Remark 1. We have just seen that, if V_p is of dimension zero, the p-adic valuation of r is the one of the gcd of the maximal non zero minors of the so called "Generalized Sylvester matrix", that is the matrix of the application $\partial_1^\nu : (A_1, \ldots, A_n) \longmapsto \sum_{i=1}^n A_i P_i$, written on the monomial bases, and in degree ν strictly bigger than $\sum_{i=1}^n (d_i - 1)$.

In particular, if, for all p, V_p is of dimension zero, the resultant is the gcd of the maximal non zero minors of this matrix, as in the generic case.

Remark 2. If $(P_1, \ldots, P_n)$ is a regular sequence on $\mathbf{Z}[\mathbf{X}]$ the homology modules $H_i(\mathbf{K})$ $(i > 0)$ are vanishing (they may have torsion even if the P_i's defines an empty variety). The classical exact sequence of ([Se] IV prop. 1) then implies that, for all prime p, $H_i(\overline{\mathbf{K}}) = 0$ for $i > 1$.

So, from the construction above, the p-adic valuation of r is the one of a maximal minor of ∂_1^ν for all ν big enough. Lemma 2 implies that the corank of $\overline{\partial}_1^\nu$, that is the Hilbert function of V_p, is bounded by $v_p(r)$ for all ν big enough.

So, for all p, V_p is either empty or of dimension zero.

V A specific decomposition and a possible application

We will now give an explicit decomposition of the modules K_p that we take from Demazurés note (Demazure told me that he found it in Van der Waerden's work), which gives a method to compute the resultant adding only one parameter. First a definition:

Definition.—*Given an n-tuple $(d_1, \ldots, d_n)$, a monomial $X_1^{i_1} \cdots X_n^{i_n}$ is called k-reduced if $i_s < d_s$ for all $s < k$. The set of k-reduced monomials will be denoted by $\Re_k$.*

This notion was known by Macaulay, it is the one he uses to define the "Macaulay minors" of the Sylvester matrix (see e.g. [Gr]).

In our situation k-reduced will mean k-reduced with respect to the n-tuple of the degrees of the P_i's. We will denote by V_i the free A-module $V_i = \bigoplus_{X^\alpha \in \Re_i} AX^\alpha \subseteq A[X_1, \ldots, X_n]$.

With this definition K_p splits into $K_p = K'_{p+1} \oplus K''_p$ with:

$$K''_p = \bigoplus_{i_1 < \cdots < i_p} V_{i_1}\, e_{i_1} \wedge \cdots \wedge e_{i_p}$$

$$K'_{p+1} = \bigoplus_{i_1 < \cdots < i_p} V^{\mathbf{c}}_{i_1}\, e_{i_1} \wedge \cdots \wedge e_{i_p}$$

where $V^{\mathbf{c}}_i$ is the free A-module spanned by the non-reduced monomials.

As the resultant is an universal object, the following lemma enables us to calculate the resultant with one added parameter:

Lemma.—*If $1 \leq p \leq n$ the composed application*

$$K''_p \hookrightarrow K_p \xrightarrow{\partial_p} K_{p-1} \xrightarrow{s} K'_p$$

where s is the canonical surjection, is a bijection for the regular sequence $P_i = X_i^{d_i}$.

Proof. See [De] p. 12 .

This lemma shows that, in this case, all the determinants coming from this decomposition equal ± 1; so, replacing every polynomials P_i by $P_i + \lambda X_i^{d_i}$, the associated determinants are monic polynomials in λ.

So the resultant is the constant term of a quotient two products of monic polynomials in λ that can be calculated by exact divisions which remain in $A[\lambda]$.

The idea of using a deformation parameter this way was also used by others, for example by Canny *et al.* (to compute the resultant using Macaulay formulas) or by Chistov & Grigoriev (among others) to determine the solutions of a zero dimensional variety.

Remark. With this decomposition, the matrix M'_i does not depend on the coefficients of $P_n, \ldots, P_{n-i+2}$ (see [De] p. 15), it gives an effective version of what we have said at the remark 7 of part III.

References

[Bo] N. Bourbaki, *Algèbre Commutative Chapitres 1 à 9*, Masson 1983 et 1985.

[De] M. Demazure, *Une définition constructive du résultant*, Notes Informelles de Calcul Formel **2**, prépublication du Centre de Mathématiques de l'École Polytechnique, 1984.

[Gr] W. Gröbner, *Modern Algebraische Geometrie*, Springer-Verlag, Wien und Innsbruck, 1949.

[Hu] A. Hurwitz, *Über die Trägheitsformen eines algebraischen Moduls*, Annali di Mathematica pura ed applicata (3) **20**, 1913, pp. 113–151.

[Jo1] J.-P. Jouanolou, *Le formalisme du résultant*, Advances in Mathematics, Vol. **90** N°**2**, December 1991 *(also edited as:* Publication de l'IRMA 417/P-234, Université de Strasbourg, 1990*)*.

[Jo2] J.-P. Jouanolou, *Aspects invariants de l'élimination*, Publication de l'IRMA 457/P-263, Université de Strasbourg, 1991.

[Jo3] J.-P. Jouanolou, *Formes d'inertie et résultant : un formulaire*, Publication de l'IRMA 499/P-288, Université de Strasbourg, 1992.

[Ma] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Stechert-Hafner Service Agency, New-York and London, 1964, *(Originally published in 1916 by Cambridge University Press)*.

[No] D.G. Northcott, *Lessons on Rings Modules and Multiplicities*, Cambridge University Press, 1968.

[Se] J.-P. Serre, *Algèbre locale et multiplicités*, Lectures Notes in Mathematics **11**, 1965.