An Introduction to TRAGHEITSFORMEN.

Abdallah Al-Amrani

An introduction to TRAGHEITSFORMEN.

Abd'allah AL AMRANI*

Université Louis Pasteur, Strasbourg I

Département de Mathématiques

7, rue René Descartes, 67084 STRASBOURG (France).

AMS Class. 13-14.

Key words : trägheitsform, jacobian, resultant.

* partially supported by the NSERC grant of L. ROBERTS. The hospitality of Queen's University is also gratefully acknowledged.

FOREWORD.

It is from Jean-Pierre JOUANOLOU that I learned what I know about elimination theory. I attended his courses (Strasbourg, Rabat), read his articles (Idéaux résultants, Le formalisme du résultant, Résultant anisotrope : compléments, and (partially) Aspects invariants de l'élimination), listened to his lectures...

But for me, his first course (Strasbourg, 1982-1983) remains, as well by its content as by its presentation, the most important. It was, in my opinion, a fundamental and simple way to be introduced to the subject : JOUANOLOU explained contributions by HURWITZ, MACAULAY, PERRON, POISSON (formula), MERTENS, ZARISKI, ... and by himself, using local cohomology and spectral sequences.

So it is not amazing that, if I am asked to explain elimination à la JOUANOLOU, I borrow heavily from his course, even though I do it in my own way.

Acknowledgments.

It is a pleasure for me to thank here Professor Leslie ROBERTS for his invitation, and for all the facilities he provided for me, during my stay at Queen's University : August-September, 1992. My thanks go also to Professor Paulo RIBENBOIM for his encouragement and his help, and to the colleagues who attended my talks and asked many fruitful questions.

Last, but not least, I would like to acknowledge the whole staff of Jeffery Hall who made me feel as if I were at home, in my own university at Strasbourg.

Kingston, Ontario

September 10th, 1992

CONTENTS

Before giving examples and the definition (*) of Trägheitsformen (= inertia forms), we fix some notation that will be used throughout this exposé.

I. NOTATION AND DATA.

Let $n, r, d_1, \cdots, d_r$ be integers ≥ 1. Let k be a commutative ring with 1, fixed as ground ring in the sequel. For each $i \in [r] := \{1, \cdots, r\}$, we consider a *generic* homogeneous polynomial of degree d_i, in n variables $X_1, \cdots, X_n$. It is denoted by $f_i = f_i(X_1, \cdots, X_n)$. Let I_i be the set of all $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ such that the weight $|\alpha| := \alpha_1 + \cdots + \alpha_n$ of α is equal to d_i. Then f_i can be written as

$$f_i = \sum_{\alpha \in I_i} U_{i,\alpha} X^\alpha \quad \text{where} \quad X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

The coefficients $U_{i,\alpha} (\alpha \in I_i)$ of the polynomial f_i are *indeterminates* over the ground ring k.

Let us make precise where the polynomials $f_1, \cdots, f_r$ live. Put

$$A = k\Big[U_{i,\alpha} | (i, \alpha) \in [r] \times \mathbb{N}^n \quad \text{such that} \quad |\alpha| = d_i\Big]$$

(A is the polynomial ring over k the indeterminates of which are the coefficients of the f_i's),

$$C = A[X_1, \cdots, X_n].$$

Hence the polynomials $f_1, \cdots, f_r$ are in C. The ring A is called the *universal coefficient ring.* The number of indeterminates in A is

$$N = \left[\begin{matrix} n + d_1 - 1 \\ d_1 \end{matrix}\right] + \cdots + \left[\begin{matrix} n + d_r - 1 \\ d_r \end{matrix}\right],$$

since the number of monomials X^β of degree d is equal to $\left[\begin{matrix} n + d - 1 \\ d \end{matrix}\right]$.

Notice that, if $i \in [r]$ is fixed, then, giving special values in k to the indeterminates $U_{i,\alpha} (\alpha \in I_i)$ we obtain from f_i any homogeneous polynomial g of degree d_i belonging to $k[X_1, \cdots, X_n]$. We say that g is obtained from f_i by *specialization*, and we will write $f_i \longmapsto g$ in this case. That explains why f_i is called generic.

(*) I will first give examples, *then* the definition!

Let us summarize the data and the vocabulary :

$$\begin{aligned}
k &= \text{ the ground ring,} \\
n &= \text{ the number of the variables } X_1, \cdots, X_n, \\
r &= \text{ the number of the (generic) polynomials } f_1, \cdots, f_r, \\
d_1, \cdots, d_r &= \text{ the degrees of the polynomials,} \\
A &= \text{ the universal coefficient ring } k[U_{i,\alpha}], \\
C &= \text{ the polynomial ring } A[X_1, \cdots, X_n].
\end{aligned}$$

II. EXAMPLES AND DEFINITION.

We first give examples of "Trägheitsformen" in the case $r = n$ (number of polynomials = number of variables).

1. Take $d_1 = \ldots = d_n = 1$, that is, the polynomials $f_1, \ldots, f_n$ are linear forms. Here we denote by U_{ij} the coefficients of f_i :

$$f_i = U_{i1}X_1 + \ldots + U_{in}X_n \, .$$

Consider the determinant $D = Det(f_1, \ldots, f_n) = |U_{ij}|$. Multiply the first column in D by X_1, and *then* add to it each j-th column multiplied by $X_j (2 \leq j \leq n)$. This gives

$$X_1 D = \begin{vmatrix} f_1 & U_{12} & \ldots & U_{1n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ f_n & U_{n2} & \ldots & U_{nn} \end{vmatrix}$$

Hence $X_1 D$ belongs to the ideal $(f_1, \cdots, f_n)$ of C. In the same way we have $X_i D \in (f_1, \cdots, f_n)$ for any i.

2. Consider the Jacobian of the polynomials $f_1, \cdots, f_n$

$$J = Jac(f_1, \cdots, f_n) = \left| \frac{\partial f_i}{\partial X_j} \right| .$$

As before, we multiply the first column in J by X_1, we add to it the $j - th$ column multiplied by X_j, for all $j \neq 1$, so that we obtain

$$X_1 J = \begin{vmatrix} d_1 f_1 & \frac{\partial f_1}{\partial X_2} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ d_n f_n & \frac{\partial f_n}{\partial X_2} & \cdots & \frac{\partial f_n}{\partial X_n} \end{vmatrix}$$

(because of the EULER identity). Hence, here again, we have $X_1 J \in (f_1, \cdots, f_n) \subset C$. Similarly one sees that $X_i J \in (f_1, \cdots, f_n)$, for all i.

Of course, the preceding example is a particular case of the Jacobian. Note that J is a homogeneous polynomial in C of degree

$$\delta = d_1 + \ldots + d_n - n.$$

The Jacobian J is defined by *differentiation* of the polynomials $f_1, \cdots, f_n$. We are now going to define an other "Jacobian", without use of any differentiation. It will be well-behaved in any characteristic, and it will have the same property, shown above, as J.

3. Each polynomial f_i can be decomposed in a *unique* way as follows :

$$(*) \qquad f_i = \sum_{j=1}^{n} X_j f_{ij} \quad , \qquad \text{with} \quad f_{ij} \in A[X_1, \cdots, X_j].$$

For example, if $n = 3$ and $d_i = 2$, we have

$$\begin{aligned} & V_1 X_1^2 + V_2 X_1 X_2 + V_3 X_1 X_3 + V_4 X_2^2 + V_5 X_2 X_3 + V_6 X_3^2 \\ & = X_1(V_1 X_1) + X_2(V_2 X_1 + V_4 X_2) + X_3(V_3 X_1 + V_5 X_2 + V_6 X_3) \end{aligned}$$

(Here we have denoted the coefficients $U_{i\alpha}$ by $V_\bullet$ for simplicity).

Let us call $\tilde{J}$ the following determinant

$$\tilde{J} = \tilde{J}ac(f_1, \cdots, f_n) := |f_{ij}| \; (1 \leq i, j \leq n).$$

The same argument as in **1.** and **2.** shows that

$$X_i \tilde{J} \in (f_1, \cdots, f_n), \quad \text{for all } i.$$

One uses *only* the definition $(*)$ of the f_{ij}'s. The degree of the homogeneous polynomial $\tilde{J}$ is δ. We will see later other reasons (besider the characteristic) why $\tilde{J}$ is the "good Jacobian". This is due to HURWITZ [H].

Now it is time to give the definition of a Trägheitsform.

4. DEFINITION *A polynomial φ in $C = A[X_1, \ldots, X_n]$ is called Trägheitsform (= inertia form), with respect to $f_1, \ldots, f_r$, if there exists an integer $s \geq 0$ such that*

$$(**) \qquad X^\alpha \varphi \in (f_1, \ldots, f_r) \text{ in } C, \text{ for all } \alpha \text{ with } |\alpha| = s.$$

(Here the integers n and r are arbitrary) ([1]).

Of course all the elements of the ideal $(f_1, \dots, f_r)$ are Trägheitsformen. We call them *trivial*. Sometimes the word Trägheitsform will be shorted to T.F.

In the case $r = n$, D, J and $\tilde{J}$ are examples of Trägheitsformen (**1.**, **2.**, **3.**). It will be shown in the sequel that if $r < n$, then all T.F. are trivial.

In the definition above, one can ask about the value of the smallest s which satisfies the property (**). This point will be discussed later.

The definition and the first study of Trägheitsformen go back to HURWITZ [H].

5. Link with local cohomology.

Consider the quotient ring

$$B = C/(f_1, \dots, f_r) \quad (\text{recall } C = A[X_1, \dots, X_n])$$

and call $\pi : C \to B$ the canonical map. Let $\mathcal{M}$ be the ideal $(X_1, \dots, X_n)$ in C. In particular B is a C-module via π. In the local cohomology theory $H^*_{\mathcal{M}}(B)$, the group $H^\circ_{\mathcal{M}}(B)$ can be defined by the equality

$$H^\circ_{\mathcal{M}}(B) = \{b \in B | \mathcal{M}^s.b = 0 \text{ in } B \text{ for some } \quad s \geq 0\}.$$

Now let

$$\mathcal{T} = \text{ the set of all T.F. in } C(w.r.t. f_1, \dots, f_r);$$

$\mathcal{T}$ is a homogeneous ideal of C.

Since $f_1, \dots, f_r$ are homogeneous, the ring B is graded, and $H^\circ_{\mathcal{M}}(B)$ is a *homogeneous* ideal in B. From the definitions we obtain

$$\mathcal{T} = \pi^{-1} H^\circ_{\mathcal{M}}(B)$$

and so

$$\mathcal{T}/(f_1, \dots, f_r) \xrightarrow{\sim} H^\circ_{\mathcal{M}}(B).$$

([1]) The symbol ه is the Arabic letter corresponding to H, written in an old way. Pronounce *ha* as in "have" or "haben" (German).

In other words, modulo trivial Trägheitsformen, $\mathcal{T}$ and $H^{\circ}_{\mathcal{M}}(B)$ are isomorphic. To simplify notation we put

$$\mathcal{B} = H^{\circ}_{\mathcal{M}}(B) \subset B.$$

Elements of $\mathcal{B}$ will also be called *Trägheitsformen.* So a Trägheitsform in B will be trivial if, and only if, it is zero.

6. Reduction of the definition. The definition of a T.F. can be simplified as follows :

PROPOSITION. — *Let φ be a polynomial in $C = A[X_1, \ldots, X_n]$. Then φ is a Trägheitsform if and only if there exist i, s such that $X_i^s \varphi \in (f_1, \ldots, f_r)$.*

Proof.— Assume we know that for *each* (i, j), X_i is not a zero-divisor in B_{X_j} (localization of B at X_j). Then, in the canonical commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B_{X_i} \\ \downarrow & & \downarrow \\ B_{X_j} & \longrightarrow & B_{X_i X_j} \end{array}$$

the maps $B_{X_i} \to B_{X_i X_j}$, $B_{X_j} \to B_{X_i X_j}$ are injective. Now suppose $X_l^s \varphi = 0$ in B for some (l, s). That is $\varphi = 0$ in B_{X_l}. Take any m between 1 and n. The preceding diagram shows that $\varphi = 0$ in $B_{X_l X_m}$ and hence $\varphi = 0$ in B_{X_m}. So $X_m^t \varphi = 0$ for some t. Substitute for t an integer large enough, if necessary, and obtain

$$X_m^t \varphi = 0 \text{ in } B, \text{ for some } t \text{ and for all } m.$$

Let q be an integer $\geq nt$. Then $X^\alpha \varphi = 0$ in B for all α such that $|\alpha| = q$. Hence φ is a T.F.

The assumption made at the beginning is a consequence of the following lemma. Although easy to see, this lemma will play an important rôle.

7. LEMMA. *Fix $i \in [n]$. Denote by V_j the coefficient of the monomial $X_i^{d_j}$ in f_j. Then consider the polynomial subring A_1 of A defined by the formula*

$$A = A_1[V_1, \ldots, V_r]$$

(*In other words* $A_1 = k[$all the coeff. of $f_1, \ldots, f_r$ except $V_1, \ldots, V_r]$).
There is an isomorphism of rings :

$$B_{X_i} \simeq A_1[X_1, \ldots, X_n, X_i^{-1}].$$

Proof.— Because of the importance of this lemma in the sequel, we are going to prove it in detail. We have canonical maps

$$A_1 \hookrightarrow A \hookrightarrow C = A[X_1, \ldots, X_n] \to B = C/(f_1, \ldots, f_r)$$

(Notice that $A \to B$ is *injective*). There is an A_1-algebra homomorphism

$$\begin{aligned} A_1[X_1, \ldots, X_n] &\to B \\ X_l &\mapsto \bar{X}_l. \end{aligned}$$

This induces a ring homomorphism

$$A_1[X_1, \ldots, X_n, X_i^{-1}] \to B_{X_i}.$$

Let us show that this map has an inverse. Write

$$g_j = f_j - V_j X_i^{dj} \quad (1 \leq j \leq r).$$

We have an A_1-algebra homomorphism

$$\begin{aligned} A = A_1[V_1, \ldots, V_r] &\to A_1[X_1, \ldots, X_n, X_i^{-1}] \\ V_j &\mapsto - g_j / X_i^{dj}. \end{aligned}$$

This yields an $A_1[X_1, \ldots, X_n]$-algebra homomorphism (in the obvious way)

$$C = A[X_1, \ldots, X_n] \to A_1[X_1, \ldots, X_n, X_i^{-1}],$$

which sends f_j to $0\,(1 \leq j \leq r)$. This gives a ring homomorphism $B \to A_1[X_1, \ldots, X_n, X_i^{-1}]$, which factorizes through B_{X_i}.
The remainder of the proof is clear.

8. Link with geometry(*)

We still (!) do not "know" how to solve a system of polynomial equations. This is, one must not forget, the first object of algebraic geometry. Since we have no *general formulas* for the solutions of polynomial systems, we could try at least to find *explicit* conditions for such solutions exist. This is the subject of elimination theory. So it is really difficult to imagine how elimation theory could be simply "eliminated" from algebraic geometry (cf. the introduction in [$J1$]).

Let us be more precise. First we take the complex numbers $\mathbb{C}$ as ground field, then we describe the corresponding situation for an arbitrary ground ring k. We keep the same notation and data as given in I.

a) Let $k = \mathbb{C}$. We consider *all* homogeneous polynomials of degrees $d_1, \ldots, d_r$ in $\mathbb{C}[X_1, \ldots, X_n]$. They are obtained from the generic ones $f_i = f_i((U_{i\alpha})_\alpha; X_1, \ldots, X_n)(1 \le i \le r)$ by specialization. So any polynomial, homogeneous of degree d_i, over $\mathbb{C}$, is of the form

$$f_i\big((u_{i\alpha})_\alpha; X_1, \ldots, X_n\big)\big(|\,\alpha| = d_i, u_{i\alpha} \in \mathbb{C}\big).$$

Take $(v_{i\alpha})_{i,\alpha} \in \mathbb{C}^N(1 \le i \le r, |\alpha| = d_i)$. We want to know when the homogeneous polynomials

$$(^*) \qquad f_1\big((v_{1\alpha})_\alpha; X_1, \ldots, X_n\big), \ldots, f_r\big((v_{r\alpha})_\alpha; X_1, \ldots, X_n\big) \in \mathbb{C}[X_1, \ldots, X_n]$$

have a non-trivial common zero $(x_1, \ldots, x_n) \in \mathbb{C}^n$. By homogeneity we can take $(x_1, \ldots, x_n)$ as a point in the projective space $P^{n-1}_{\mathbb{C}}$ over $\mathbb{C}$. Consider the ZARISKI closed subset

$$Z = \big\{\big((u_{i\alpha})_{i,\alpha}; x_1, \ldots, x_n\big) \in \mathbb{C}^N \times P^{n-1}_{\mathbb{C}} \mid f_i\big((u_{i\alpha})_\alpha; x_1, \ldots, x_n\big) = 0, 1 \le i \le r\big\}$$

of $\mathbb{C}^N \times P^{n-1}_{\mathbb{C}}$, and let $p : \mathbb{C}^N \times P^{n-1}_{\mathbb{C}} \to \mathbb{C}^N$ be the first projection. With respect to the topology induced by $\mathbb{C}$, p is clearly proper; hence $p(Z)$ is a closed subset of $\mathbb{C}^N$. The traditional "main theorem of elimination" [W] says that $p(Z)$ is a ZARISKI closed subset. That means there are polynomials

$$g_1, \ldots, g_s \in \mathbb{C}[U_{i\alpha} \mid 1 \le i \le r, |\alpha| = d_i] = A$$

so that

(*) This paragraph can be considered as an *introduction* to the study of Trägheitsformen. Unlike the other paragraphs, no details are given.

$$p(Z) = \{(u_{i\alpha})_{i,\alpha} \in \mathbb{C}^N \mid g_1(u_{i\alpha}) = \cdots = g_s(u_{i\alpha}) = 0\}.$$

One deduces that the polynomials $(*)$ above have a common root in $P_{\mathbb{C}}^{n-1}$ if, and only if, their coefficients $(v_{i\alpha})_{i\alpha}(1 \leq i \leq r, |\alpha| = d_i)$ constitute a common zero in $\mathbb{C}^N$ of $g_1, \ldots, g_s$.

It happens that these "polynomial conditions" g_i are *Trägheitsformen w.r.t.*$f_1, \ldots, f_r$ (loc.cit.). We will see that they "generate" all Trägheitsformen belonging to A. If $r = n$ (# polynomials = # variables), then $p(Z)$ can be defined by only one polynomial $g = g(U_{i\alpha})$, called "the" *resultant* of $f_1, \ldots, f_r$. All these notions will be made precise later (see the next part b) and V.).

In a less traditional form, the main theorem of elimination says that "a projective morphism is proper" [RB]. Since p is, by definition, projective, we see that $p(Z)$ is a closed subset of $\mathbb{C}^N$ for the ZARISKI topology.

b) Here the ground ring k is arbitrary, and one must be more careful and more precise. So we need the "language of schemes" introduced in [EGA]. See also [RB], [YB] ([1]).

Instead of $\mathbb{C}^N$, $P_{\mathbb{C}}^{n-1}$, $\mathbb{C}^N \times P_{\mathbb{C}}^{n-1}$, Z in a), we have here the following schemes (respectively)

$$\begin{array}{rlrl} E_k^N &= \mathrm{Spec(A)}, & A &= k[U_{i,\alpha} \mid 1 \leq i \leq r, |\alpha| = d_i] \\ P_k^{n-1} &= \mathrm{Proj}k[X_1, \ldots, X_n] & & \\ E_k^N \times P_k^{n-1} = P_A^{n-1} &= \mathrm{Proj(C)}, & C &= A[X_1, \ldots, X_n] \\ Z &= \mathrm{Proj(B)}, & B &= C/(f_1, \ldots, f_r) \end{array}$$

where Z is a closed subscheme of P_A^{n-1}. There is a natural commutative diagram

$$\begin{tikzcd} Z \arrow[r, hook] \arrow[dr, "p \mid Z"'] & P_A^{n-1} \arrow[d, "p"] \\ & E_k^N = \mathrm{Spec(A)} \end{tikzcd}$$

where $p, p \mid Z$ are, by definition, projective (hence proper) morphisms. The scheme-closed image of Z in E_k^N is defined by the ideal [EGAI]

([1]) RB is the *red* book, YB is the *yellow* book.

(**)
$$\mathcal{A} = \ker\big(A \to \Gamma(Z, \mathcal{O}_Z)\big)$$

where $\Gamma(Z, \mathcal{O}_Z)$ is the global sections of the scheme Z and the ring homomorphism $A \to \Gamma(Z, \mathcal{O}_Z)$ is the canonical one. Since $Z = \mathrm{Proj}(B)$ is covered by the standard open subsets $D^+(X_i)(1 \leq i \leq n)$, one deduces

$$\mathcal{A} = \ker(A \to \prod_{i=1}^{r} B_{(X_i)}),$$

with $B_{(X_i)}$ = the degree 0 homogeneous part of the $\mathbb{Z}$ -graded ring B_{X_i}. Therefore the proposition in **6.** above shows that $\mathcal{A}$ *is nothing else but the ideal of Trägheitsformen belonging to the ring A.*

What is the geometrical meaning of the other Trägheitsformen? With the notation of **5.**, we have

$$\mathcal{A} = A \cap H^{\circ}_{\mathcal{M}}(B)_{\circ}$$

$\big(H^{\circ}_{\mathcal{M}}(B)$ is a homogeneous ideal in B; its component of degree j is noted $H^{\circ}_{\mathcal{M}}(B)_j\big)$. Thus the relation $(**)$ is a particular case of the general fact

$$H^{\circ}_{\mathcal{M}}(B)_j = \ker\big[B_j \to \Gamma\big(Z, \mathcal{O}_Z(j)\big)\big]$$

This and other relations between the cohomologies $H^{*}_{\mathcal{M}}$ and $H^{*}\big(Z, \mathcal{O}_Z(j)\big)$ come from the properties of local cohomology and the computation of the cohomology of projective bundles. For more details, see [J2] **3.1.**.

In the following section we construct other examples of Trägheitsformen of degree 0 (i.e. belonging to A) in the case $r = n$. These are determinants which have been defined by MACAULAY and which generalize the well-known SYLVESTER determinant.

III. MACAULAY DETERMINANTS ([MA], [G]).

We assume $r = n$

1. Recall that $\delta = d_1 + \ldots + d_n - n$. Let t be an integer $\geq \delta + 1$, and put $E_t = \{\alpha \in \mathbb{N}^n \mid |\alpha| = t\}$. We are going to define a determinant $|a_{\alpha\beta}|(\alpha, \beta \in E_t)$, with entries in A. We order E_t lexicographically in a decreasing way $((t, 0, \ldots, 0) > (t-1, 1, 0, \ldots, 0) \ldots)$.

Let $\alpha \in E_t$. Since $|\alpha| \geq \delta + 1$, we can find a *minimal* integer $i(1 \leq i \leq n)$ such that $\alpha_i \geq d_i$. For any $\beta \in E_t$, put $a_{\alpha\beta}$ = the coeff. of X^α in the polynomial $\frac{X^\alpha}{X_i^{d_i}} \cdot f_i$ (Notice that $\frac{X^\alpha}{X_i^{d_i}} \cdot f_i$ is homogeneous of degree $|\alpha| = |\beta| = t$, and that $a_{\alpha\beta}$ may be equal to 0). Let us note

$$D(t) = \det[a_{\alpha\beta}](\alpha, \beta \in E_t) \in A.$$

ASSERTION. *The determinant $D(t)$ is a non-trivial Trägheitsform, homogeneous as polynomial in the coefficients of each f_i.*

Proof.— We operate on the columns of $D(t)$ as follows :

1) multiply the first column (the $n°$ of which is $(t, 0, \ldots, 0) \in E_t$) by X_1^t.
2) multiply each *other* column $n°\beta$ by X^β and add the result to the new first column.
3) now the first column has the following form

$$[f_{i(\alpha)} \cdot X^\alpha / X_{i(\alpha)}^{d_{i(\alpha)}}]_{\alpha \in E_t},$$

where $i(\alpha)$ is the minimal integer i such that $\alpha_i \geq d_i$ for a given $\alpha \in E_t$.

Now, expanding the new determinant with respect to the first colmn we see that

$$X_1^t D(t) \in (f_1, \ldots, f_n).$$

This shows that $D(t)$ is a T.F. by **II.6.**. Since $D(t) \in A$, to see that it is a non-trivial T.F., it is enough to check $D(t) \neq 0$. Let us specialize each f_i to $X_i^{d_i}$. Then $D(t)$ specializes to the determinant of the identity matrix ($f_{i(\alpha)} \cdot X^\alpha / X_{i(\alpha)}^{d_{i(\alpha)}} \mapsto X^\alpha$ for each $\alpha \in E_t$), that is $D(t) \mapsto 1$. So $D(t) \neq 0$.

Each row $n°\alpha$ in $D(t) = |a_{\beta\gamma}|$ contains only the coefficients of the polynomial $f_{i(\alpha)}$ and zeros. Hence $D(t)$ is homogeneous in the coefficients of f_j, for any fixed j (These coefficients appear effectively in $D(t)$: consider the row $n°\alpha \in E_t$ with $\alpha_i = d_i - 1$ for all $i \neq j$). The assertion is proved.

We will write $\deg_{f_i}$ for the degree of a polynomial in the coefficients of f_i (as indeterminates). Let us compute $\deg_{f_n}(D(t))$. From the preceding proof, last part, we have

$$\deg_{f_j}(D(t)) = \#\{\alpha \in E_t \mid i(\alpha) = j\}(1 \leq j \leq n).$$

But $i(\alpha) = n$ if, and only if, $0 \leq \alpha_1 \leq d_1 - 1, \ldots, 0 \leq \alpha_{n-1} \leq d_{n-1} - 1$.

Consequently

$$\boxed{\deg_{f_n}(D(t)) = d_1 \ldots d_{n-1}}$$

2. SYLVESTER determinant. Taking $t = \delta + 1$ in $n°1.$, one checks that the SYLVESTER determinant is equal to $D(\delta + 1)$ if $n = r = 2$. Indeed, in that case, the rows of $D(\delta + 1)$ are defined by the polynomials

$$X_1^{d_2-1} f_1, X_1^{d_2-2} X_2 f_1, \ldots, X_1 X_2^{d_2-2} f_1, X_2^{d_2-1} f_1,$$
$$X_1^{d_1-1} f_2, X_1^{d_1-2} X_2 f_2, \ldots, X_1 X_2^{d_1-2} f_2, X_2^{d_1-1} f_2.$$

From **1.** it is clear that

$$\deg_{f_1} D(\delta + 1) = d_2 \ , \ deg_{f_2} D(\delta + 1) = d_1.$$

3. Here we define other determinants similar to $D(t)$. In **1.** we have associated to a *sequence* of integers $(d_1, \ldots, d_n)$ a determinant $D(t)$, with $t \geq \delta + 1 = d_1 + \ldots + d_n - n + 1$ (by use of the polynomials $f_1, \ldots, f_n$). If we apply a permutation $\sigma \in S_n$ to the integers $(1, \ldots, n)$ and we do the same construction with the sequence $(f'_1, \ldots, f'_n) = (f_{\sigma(1)}, \ldots, f_{\sigma(n)})$, then we obtain a determinant $D^\sigma(t)$ (the integer δ does not change!)

By **1.**, *the determinants $D^\sigma(t)$ are non-trivial T.F., homogeneous w.r.t. the coefficients of each f_j, and*

$$\boxed{\deg_{f_i}(D^\sigma(t)) = d_1 \ldots d_n / d_i, \text{ if } i = \sigma(n).}$$

(Of course $D(t) = D^{id}(t)$).

These determinants $D^\sigma(t)$ have been constructed by MACAULAY to give an explicit formula for the "resultant" of the polynomials $f_1, \ldots, f_n$. We will call them MACAULAY determinants.

IV. THEOREM OF HURWITZ [H].

We first recall some facts about the KOSZUL complex.

1. Let R be a commutative ring with 1 and M an R-module. To any linear form $u : M \to R$, one associates a complex $K_\bullet(u; R)$ of R-modules

$$\begin{array}{ccccccccc} & & & & & M & & R & \\ & & & & & \| & & \| & \\ \ldots \to \wedge^{i+1}M & \to & \wedge^i M & \to \ldots \to & & \wedge^1 M & \to & \wedge^\circ M & \to 0 \\ & \theta_{i+1} & & & & & \theta_1 = u & & \end{array}$$

where the differentials are defined by the formula

$\theta_{i+1}(x_1 \wedge \ldots \wedge x_{i+1}) =$

$$\sum_{s=1}^{i+1}(-1)^{s+1}u(x_s) \cdot x_1 \wedge \ldots \wedge \hat{x}_s \wedge \ldots \wedge x_{i+1}(x_1, \ldots, x_{i+1} \in M)\ (^1)$$

If $M = R^p$ and $u(e_i) = a_i$, where $\{e_1, \ldots, e_p\}$ is the canonical basis of R^p, then $K_\bullet(u; R)$ is the KOSZUL complex defined by the sequence $(a_1, \ldots, a_p)$, usually denoted $K_\bullet(a_1, \ldots, a_p; R)$.

Assume R is a graded ring, with degrees in $\mathbb{N}$, and $a_1, \ldots, a_p$ are homogeneous elements in R. Then, taking

$$\deg(e_i) := \deg(a_i) \quad (1 \leq i \leq p),$$

we define a grading on the R-module R^p. More generally, the modules $\wedge^i R^p (1 \leq i \leq p)$ are graded by the formula

$$\deg(e_{j_1} \wedge \ldots \wedge e_{j_i}) = s_{j_1} + \ldots + s_{j_i}$$

where $s_t = \deg(a_t)$. In this case, $K_\bullet(a_1, \ldots, a_p; R)$ is a *graded complex* and one has

$$\wedge^i R^p = \oplus R[-s_{j_1} - \ldots - s_{j_i}]\ (1 \leq j_1 < \ldots < j_i \leq p);$$

the notation $R[q], q \in \mathbb{Z}$, means that the degrees are shifted by q in $R : R[q]$ is the R-module R, graded as follows

$$\left(R[q]\right)_t = R_{t+q} \quad ((\ )_t := \text{homogeneous part of degree } t).$$

---

(1) The symbol $\hat{a}$ means that a does not appear.

PROPOSITION [B] *(Paragraph 9, n°7) In the graded situation just described, with* $\deg(a_i) \geq 1 (1 \leq i \leq p)$, *one has*

$$(*) \qquad H_j\big(K_\bullet(a_1, \ldots, a_p; R)\big) = 0 \quad \text{for all } j \geq 1$$

if and only if $H_1\big(K_\bullet(a_1, \ldots, a_p; R)\big) = 0$.

In case of (*), we say that the complex $K_\bullet(a_1, \ldots, a_p; R)$ is *acyclic* except in degree 0 (1) The following remark will be useful for us.

REMARK. Here the KOSZUL complex is not necessarily graded. Consider the differential θ_2 of $K_\bullet(a_1, \ldots, a_p; R)$:

$$\begin{aligned} \theta_2 : \wedge^2 R^p &\longrightarrow \wedge^1 R^p = R^p \\ e_i \wedge e_j &\longmapsto a_i e_j - a_j e_i \end{aligned}$$

$\big(\{e_i \wedge e_j\}_{i<j}$ is a basis for the R-module $\wedge^2 R^p\big)$. Thus $\theta_2(e_i \wedge e_j) = E_{ij} \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_p \end{bmatrix}$, where E_{ij} is the *elementary* skew-symmetric matrix with 1 at the (j, i)-place. We deduce that $(b_1, \ldots, b_p) \in Im(\theta_2)$ if, and only if, there is a skew-symmetric matrix S (with 0's on the diagonal) such that

$$\begin{bmatrix} b_1 \\ \vdots \\ b_p \end{bmatrix} = S \begin{bmatrix} a_1 \\ \vdots \\ a_p \end{bmatrix}.$$

With the notation in **I.** and **II.**, we have the following statement.

2. HURWITZ THEOREM (1^{st} part).

a. *if* $r < n$, *then* $\mathcal{T} = (f_1, \ldots, f_r)$.
b. *if* $r \leq n$, *then* $H_1\big(K_\bullet(f_1, \ldots, f_r; C)\big) = 0$.

In other words, (a.) *says that, if the number of the generic polynomials is strictly less than the number of the variables, then there are only trivial Trägheitsformen;* (b.) *says that if the former number is less or equal to the second one, then the KOSZUL complex defined by the polynomials* $f_1, \ldots, f_r$ *is acyclic except in degree 0 (see Proposition in 1. above).*

Proof— To emphasize that the number of variables is n, we denote the assertions a. and b. by $a = a(n)$ and $b = b(n)$.

---

(1) If $\ldots \to L_{i+1} \to L_i \to \ldots$ is a complex, we say that L_i is its term of *degree i*.

Case $r = 1$

Since f_1 is not a zero-divisor in $C = A[X_1, \ldots, X_n]$ (f_1 is generic!), we have $H_1(K_\bullet(f_1; C)) = \ker(C \xrightarrow{\cdot f_1} C) = 0$. So (b.) is true. Let us show (a.). Take then $n > 1$. If p is a T.F., then

$$X_1^s p = g\, f_1 \text{ in } C, \text{ for some } s \text{ and some } g.$$

Now f_1 is generic in n variables, with $n \geq 2$. This implies that X_1^s divides g in C. So $p \in (f_1)$, as desired.

General case :

It is enough to show the two implications

$$\begin{aligned} &(i) \quad a(n) \Longrightarrow b(n), \\ &(ii) \quad b(n-1) \Longrightarrow a(n), \end{aligned}$$

since $b(1)$ is true ($n = 1, r \leq n \Longrightarrow r = 1!$).

The proof of the first implication uses induction on the number of the generic polynomials $f_1, \ldots, f_r$ involved.

Proof of (i). Suppose $a(n)$ is true. To prove $b(n)$ we can take $r \geq 2$. So let $2 \leq r \leq n$, and let us show that

$$H_1(K_\bullet(f_1, \ldots, f_r; C)) := \ker(\theta_1)/Im(\theta_2) = 0.$$

Consider an element $(g_1, \ldots, g_r) \in C^r$ such that

(1) $$g_1 f_1 + \ldots + g_r f_r = 0 (\text{i.e. } (g_1, \ldots, g_r) \in \ker(\theta_1), \text{ cf. } 1.)$$

LEMMA. *Put* $\bar{k} := k[U_{r,\alpha} \mid |\alpha| = d_r]$

$$\bar{A} := \bar{k}[U_{i,\alpha} \mid 1 \leq i \leq r-1, |\alpha| = d_i] = A\,,$$
$$\bar{C} := \bar{A}[X_1, \ldots, X_n] = C.$$

Then g_r is a Trägheitsform in $\bar{C}$ with respect to the generic polynomials $f_1, \ldots, f_{r-1}$ (over the ground ring $\bar{k}$).

Proof of the Lemma. Denote by $\bar{B}$ the ring $\bar{C}/(f_1, \ldots, f_{r-1})$. The relation (1) gives $\bar{g}_r \bar{f}_r = 0$ in $\bar{B}$. On the other hand, Lemma (7., II.) shows that

$$\bar{B}_{X_n} \simeq \bar{k}[\text{certain coeff. of } f_1, \ldots, f_{r-1}][X_1, \ldots, X_n, X_1^{-1}].$$

Hence $\bar{f}_r$ is not a zero-divisor in $\bar{B}_{X_n}$. We then obtain $\bar{g}_r = 0$ in $\bar{B}_{X_n}$, and so :

$$X_n^s \bar{g}_r = 0 \quad \text{in} \quad \bar{B}, \quad \text{for some integer } s \geq 0,$$

that is $X_n^s g_r \in (f_1, \ldots, f_{r-1})$ in $\bar{C} = C$. The lemma is proven, by Proposition (6., II.).

Now, in the situation of the lemma above, one has $r-1$ generic polynomials in n variables and $1 \leq r-1 < n$. Applying $a(n)$ to this case one obtains $g_r \in (f_1, \ldots, f_{r-1})$ in $\bar{C} = C$. In other words, one has an equality

$$g_r = \lambda_{r1} f_1 + \ldots + \lambda_{r,r-1} f_{r-1} \quad \text{in } C. \tag{2}$$

Substitute in (1) and get

$$h_1 f_1 + \ldots + h_{r-1} f_{r-1} = 0, \text{ with } h_i = g_i + \lambda_{r_i} f_r. \tag{3}$$

By induction on r, we have $H_1\big(K_\bullet(f_1, \ldots, f_{r-1}); \bar{C})\big) = 0$. Thus $(h_1, \ldots, h_{r-1})$ belongs to the image of the degree 2 differential in the complex $K_\bullet(f_1, \ldots, f_{r-1}; \bar{C})$. Using the remark in 1., one sees that there exists a skew-symmetric matrix $[\lambda_{ij}](1 \leq i, j \leq r-1)$ over $\bar{C} = C$ such that

$$\begin{bmatrix} h_1 \\ \vdots \\ h_{r-1} \end{bmatrix} = [\lambda_{ij}] \begin{bmatrix} f_1 \\ \vdots \\ f_{r-1} \end{bmatrix}.$$

If we take $\lambda_{rr} = 0, \lambda_{ir} = -\lambda_{ri}(1 \leq i \leq r-1)$, then the matrix $S = [\lambda_{ij}](1 \leq i, j \leq r)$ is skew-symmetric and it satisfies (after (2), (3))

$$\begin{bmatrix} g_1 \\ \vdots \\ g_r \end{bmatrix} = S \begin{bmatrix} f_1 \\ \vdots \\ f_r \end{bmatrix}.$$

Again the remark in 1. shows that $(g_1, \ldots, g_r) \in Im(\theta_2)$, and we are done $\big(\ker(\theta_1) = Im(\theta_2)\big)$.

Proof of (ii). Assuming $b(n-1)$ true, let us prove $a(n)$. So we have $r < n$. It is sufficient to see

$$X_n^s f \in (f_1, \ldots, f_r) \Longrightarrow f \in (f_1, \ldots, f_r),$$

for all $s \geq 0$ (cf. II., 6.). We can take $s = 1$. Start with an equality in C as

$$X_n f = h_1 f_1 + \ldots + h_r f_r. \tag{4}$$

For a polynomial $P = P(X_1, \ldots, X_n)$, we note $P^\circ = P(X_1, \ldots, X_{n-1}, 0)$. It follows that

$$h_1^\circ f_1^\circ + \ldots + h_r^\circ f_r^\circ = 0 \text{ in } C^\circ := A[X_1, \ldots, X_{n-1}].$$

But $f_1^\circ, \ldots, f_r^\circ$ are *generic* polynomials in $n-1$ variables $X_1, \ldots, X_{n-1}$. Therefore, by $b(n-1)$, there exists a skew-symmetric matrix $[\lambda_{ij}](1 \leq i, j \leq r)$, with $\lambda_{ij} \in C^\circ$, such that

$$\begin{bmatrix} h_1^\circ \\ \vdots \\ h_r^\circ \end{bmatrix} = [\lambda_{ij}] \begin{bmatrix} f_1^\circ \\ \vdots \\ f_r^\circ \end{bmatrix}. \tag{5}$$

Put $g_i = \sum_{j=1}^r \lambda_{ij} f_j$. Then $\sum_{i=1}^r g_i f_i = 0$, by skew-symmetricity of the matrix $[\lambda_{ij}]$. Since $g_i^\circ = h_i^\circ (1 \leq i \leq r)$ by (5) (λ_{ij} does not contain X_n!), one has

$$h_i - g_i = X_n l_i \quad \text{in} \quad C.$$

Consequently one obtains from (4)

$$X_n \Phi = \underbrace{\sum_{i=1}^r g_i f_i}_{0} + X_n \sum_{i=1}^r l_i f_i.$$

That is $\Phi = \sum l_i f_i : \Phi$ is a trivial T.F.

The theorem is established.

The following corollary is important for the study of Trägheitsformen belonging to A in the case $r = n$ (cf. Proof of Theorem (2., V.)).

3. COROLLARY. *Assume $r = n$ and let Φ be a non-trivial Trägheitsform with respect to the polynomials $f_1, \ldots, f_r$. Let U be any coefficient $U_{i,\alpha}$ of the f_j's. Then, as polynomial in U, Φ has degree $\deg_U(\Phi) \geq 1$.*

Proof. Let Φ be a T.F. such that $\deg_U(\Phi) = 0$ for some $U = U_{i,\alpha}$. Write f_i as $f_i = U_{i\alpha} X^\alpha + g_i$. Consider a relation of the form

$$X^\beta \Phi = h_1 f_1 + \ldots + h_n f_n \text{ in } C,$$

and take its image by the map $\varphi : C = A[X_1, \ldots, X_n] \to C_{X_1 \ldots X_n}$ defined as k-algebra homomorphism by

$$\begin{aligned} &\varphi : C = k[U_{j,\gamma} \mid 1 \leq j \leq n, |\gamma| = d_j][X_1, \ldots, X_n] \to C_{X_1 \ldots X_n} \\ &\varphi(U_{i,\alpha}) = -g_i / X^\alpha, \\ &\varphi(U_{j,\gamma}) = U_{j,\gamma} \quad \text{if } (j, \gamma) \neq (i, \alpha), \\ &\varphi(X_t) = X_t \text{ for all } t. \end{aligned}$$

Since in $C_{X_1\ldots X_n}$ one has $\varphi(f_0) = f_0, \varphi(f_j) = f_j (j \neq i)$ and $\varphi(f_i) = 0$, it follows

$$X^{\beta} f_0 = H_1 f_1 + \ldots + H_{i-1} f_{i-1} + H_{i+1} f_{i+1} + \ldots + H_n f_n \text{ in } C_{X_1\ldots X_n}.$$

But $X_1 \ldots X_n$ is not a zero-divisor in C; whence

$$X^{\rho} X^{\beta} f_0 = l_1 f_1 + \ldots + l_{i-1} f_{i-1} + l_{i+1} f_{i+1} + \ldots + l_n f_n \text{ in } C$$

for some $\rho \in \mathbb{N}^n$. By II.6. this implies that f_0 is a T.F. with respect to the polynomials $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n$ (take as ground ring $k' = k[U_{i,\gamma} \mid |\gamma| = d_i]$). The assertion (a) in the theorem 2. above says that in this case ($n-1$ polynomials in n variables) f_0 is a trivial T.F. : $f_0 \in (f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$. In particular f_0 is a trivial T.F. with respect to $f_1, \ldots, f_n$.

In fact the preceding proof gives a more precise result than the corollary :

If $r = n$ and if f_0 is a T.F. where some inderminate $U_{i,\alpha}$ does not appear, then $f_0 \in (f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$.

4. HURWITZ THEOREM (2^{nd} part).

We have

c. $\mathcal{T}_s = (f_1, \ldots, f_r)_s$ for $s > d_1 + \ldots + d_r - r$.
d. $\left[H_1(K_\bullet(f_1, \ldots, f_r; C))\right]_s = 0$ for $s > d_1 + \ldots + d_r - r + 1$.

(Recall that $(\ )_s$ denotes the homogeneous part of degree s; cf. 1.).

Proof— We look for integral functions

$$\varphi = \varphi(d_1, \ldots, d_r, n) \ , \ \psi = \psi(d_1, \ldots, d_r, n)$$

such that

c. $\mathcal{T}_s = (f_1, \ldots, f_r)_s$ for $s > \varphi$;
d. $\left[H_1(K_\bullet)\right]_s = 0 \quad$ for $s > \psi(K_\bullet = K_\bullet(f_1, \ldots, f_r; C))$.

To construct candidates for φ and ψ, one proceeds as in the proof of the 1^{st} part by showing

$$d(n-1) \Longrightarrow c(n) \Longrightarrow d(n).$$

(The integer n in $c(n)$ indicates that the number of the *variables* is $n, \ldots$).

1°) Let us begin by the implication $c(n) \Longrightarrow d(n)$: We have

$$H_1(K_\bullet)_s = Z_1(K_\bullet)_s / B_1(K_\bullet)_s.$$

Let $(g_1, \ldots, g_r) \in Z_1(K_\bullet)_s$ such that its image under the differential θ_1 be zero :

$$f_1 g_1 + \ldots + f_r g_r = 0.$$

In the graded KOSZUL complex $K_\bullet$ (see 1.), $(g_1, \ldots, g_r) = g_1 e_1 + \ldots + g_r e_r$ is homogeneous of degree s. So g_i is homogeneous of degree $s - d_i$.

One wants to prove $(g_1, \ldots, g_r) \in B_1(K_\bullet)_s$ if $s > \psi$. We know from the proof of the 1^{st} part in 2. that g_r is a T.F. with respect to $f_1, \ldots, f_{r-1}$ (homogeneous of degree $s - d_r$).

If $s - d_r > \varphi(d_1, \ldots, d_{r-1}, n)$ then, applying $c(n)$, one has

$$g_r = \lambda_{r1} f_1 + \ldots + \lambda_{r,r-1} f_{r-1}, \quad \text{where } \lambda_{ri} \in C_{s-d_r-d_i}.$$

Substituting in $\sum_{i=1}^{n} f_i g_i = 0$, we obtain

$$\underbrace{(\lambda_{r1} f_r + g_1)}_{\deg s-d_1} f_1 + \ldots + \underbrace{(\lambda_{r,r-1} f_r + g_{r-1})}_{\deg s-d_{r-1}} f_{r-1} = 0.$$

Hence, if $s > \psi(d_1, \ldots, d_{r-1}, n)$ we can obtain the result by induction on $r =$ the number of polynomials (in a similar way as in 2.).

Conclusion : For the implication $c(n) \Longrightarrow d(n)$ to be true, it is enough that the functions φ and ψ satisfy

$$(*) \qquad \begin{aligned} &\psi(d_1, \ldots, d_r, n) \geq \min\{\max(\varphi_i + d_i, \psi_i) \mid 1 \leq i \leq r\} \\ \text{with } &\varphi_i = \varphi(d_1, \ldots, \hat{d}_i, \ldots, d_r, n) \\ &\psi_i = \psi(d_1, \ldots, \hat{d}_i, \ldots, d_r, n). \end{aligned}$$

2°) Consider now the implication $d(n-1) \Longrightarrow c(n)$:

Let $H \in \mathcal{T}_s$. We want to show $H \in (f_1, \ldots, f_r)_s$ if $s > \varphi$. We can suppose $X_n H \in (f_1, \ldots, f_r)$ (since $X_n^t H \in (f_1, \ldots, f_r)$ for some $t \geq 0$). So

$$X_n H = g_1 f_1 + \ldots + g_r f_r \quad \text{for some } g_i \in C_{s+1-d_i} (1 \leq i \leq n).$$

Putting $Q^\circ = Q(X_1, \ldots, X_{n-1}, 0)$ for $Q = Q(X_1, \ldots, X_n)$ as in 2., we have

$$g_1^\circ f_1^\circ + \ldots + g_r^\circ f_r^\circ = 0 \text{ in } C_{s+1}.$$

To apply $d(n-1)$ in this situation (where the number of variables is $n-1$), it suffices that

$$(**) \qquad \varphi(d_1, \ldots, d_r, n) \geq \psi(d_1, \ldots, d_r, n-1) - 1.$$

The argument can then be achieved similarly to the corresponding proof in 2.

The following functions satisfy (*) and (**) :

$$\varphi(d_1, \ldots, d_r, n) = d_1 + \ldots + d_r - r$$
$$\psi(d_1, \ldots, d_r, n) = d_1 + \ldots + d_r - r + 1.$$

They have been given by HURWITZ. Note that they are independent of n.

To finish the proof, let us say that the case $r = 1$ has to be checked since the implication $c(n) \Longrightarrow d(n)$ uses induction on r. Because of the 1st part of the theorem (2.), one can assume $r \geq n$. So $r = 1$ implies $n = 1$ and then c. and d. are immediate.

5. Level of a homogeneous Trägheitsform.

HURWITZ theorem allows to determine the "level" of a homogeneous Trägheitsform.

DEFINITION.. — *Let $\mathfrak{f}$ be a homogeneous T.F. in $C = A[X_1, \ldots, X_n]$ with respect to $f_1, \ldots, f_r$. The level of $\mathfrak{f}$ is the smallest integer $s \geq 0$ such that*

$$X^\alpha \mathfrak{f} \in (f_1, \ldots, f_r) \quad \textit{for all } \alpha \quad \textit{with } |\alpha| = s.$$

So a trivial homogeneous Trägheitsform has a level equal to zero. We saw in II.2. that when $r = n$ the Jacobian of $f_1, \ldots, f_r$ is a T.F. of level 1.

Let $\mathfrak{f} \in \mathcal{T}_t$ (= Trägheitsformen of degree t). Take $\alpha \in \mathbb{N}^n$ with $|\alpha| = \delta + 1 - t (\delta = d_1 + \ldots + d_r - r)$. Hence $X^\alpha \mathfrak{f} \in \mathcal{T}_{\delta+1}$.

By HURWITZ theorem (2nd part) one has $\mathcal{T}_{\delta+1} = (f_1, \ldots, f_r)_{\delta+1}$. Whence

$$\text{level}(\mathfrak{f}) \leq \delta + 1 - \deg(\mathfrak{f}) \ (\text{lev} = \text{level})$$

PROPOSITION. *If $r = n$ and if $\mathfrak{f}$ is a non-trivial homogeneous Trägheitsform, then*

$$\boxed{\text{lev}\,(\mathfrak{f}) = \delta + 1 - \deg(\mathfrak{f})}.$$

Proof. Let $\mathfrak{f} \in \mathcal{T}_t$ be a non-trivial T.F. Hence $t \leq \delta$ (4.).

i) It is sufficient to show the implication

$$\text{(1)} \qquad \text{lev}(\mathfrak{f}) = 1 \Longrightarrow \deg(\mathfrak{f}) = \delta.$$

Indeed put $s = \text{lev}\,(\mathfrak{f})$. So $s \geq 1$ and there exists $\beta \in \mathbb{N}^n$ such that $|\beta| = s - 1$ and $X^\beta \mathfrak{f} \notin (f_1, \ldots, f_n)$. It follows that $X^\beta \mathfrak{f}$ is a non-trivial T.F. with $\text{lev}(X^\beta \mathfrak{f}) = 1$. Hence $\deg(X^\beta \mathfrak{f}) = \delta$ by (1), that is, $\deg(\mathfrak{f}) = \delta + 1 - s$ as desired.

ii) We have to prove (1). Assume $\operatorname{lev}(f) = 1$.

Case $n = 1$: One has $X_1 f = h f_1$ in $C = A[X_1]$, with h homogeneous and $f_1 = U X_1^{d_1}$. So

$$\deg(f) = \deg(h) + d_1 - 1 = \deg(h) + \delta \geq \delta.$$

But we know $\deg(f) \leq \delta$. Thus $\deg(f) = \delta$.

Case $n \geq 2$: Suppose $\deg(f) < \delta$ (We know $\deg \leq \delta$).

We are going to show that f is a trivial T.F., which will contradict the hypothesis. The argument is similar to the proof of the 1^{st} part of HURWITZ theorem. Fix $p \in \{1, \ldots, n-1\}$.

Since $\operatorname{lev}(f) = 1$ we have

$$X_p f = g_1 f_1 + \ldots + g_n f_n \qquad (2)$$

$$X_n f = h_1 f_1 + \ldots + h_n f_n \qquad (3)$$

with g_j, h_j homogeneous in C.

Whence

$$l_1 f_1 + \ldots + l_n f_n = 0, \text{ with } l_j = X_n g_j - X_p h_j.$$

But $H_1(K_\bullet(f_1, \ldots, f_n; C)) = 0$ (2.b.). So there exists a skew- symmetric matrix $[\gamma_{ij}]_{1 \leq i,j \leq n}$ over $C = A[X_1, \ldots, X_n]$ such that

$$\begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix} = [\gamma_{ij}] \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix}.$$

In particular one has

$$X_n g_n - X_p h_n = \gamma_{n1} f_1 + \ldots + \gamma_{n,n-1} f_{n-1} \; (\gamma_{nn} = 0).$$

Substituting 0 for X_n, we obtain

$$X_p h_n^\circ = -\gamma_{n1}^\circ f_1^\circ - \ldots - \gamma_{n,n-1}^\circ f_{n-1}^\circ.$$

So h_n° is a T.F. with respect to $f_1^\circ, \ldots, f_{n-1}^\circ$. These polynomials are generic and homogeneous in $X_1, \ldots, X_{n-1}$. On the other hand (3) above gives

$$\deg(h_n^\circ) = \deg(f) + 1 - d_n < \delta + 1 - d_n = d_1 + \ldots + d_{n-1} - (n-1).$$

Since $X_p h_n^\circ \in (f_1^\circ, \ldots, f_{n-1}^\circ)$ in $A[X_1, \ldots, X_{n-1}]$ for all $p = 1, \ldots, n-1$, we deduce that the T.F. h_n° with respect to $f_1^\circ, \ldots, f_{n-1}^\circ$ is trivial, by induction on n $\big($since $\operatorname{lev}(h_n^\circ) \leq 1$ and $\deg(h_n^\circ) < d_1 + \ldots + d_{n-1} - (n-1)\big)$ [The case $n = 1$ is immediate : if P is a homogeneous T.F. of level 1 and $\deg(P) < \delta = d_1 - 1$, then P is a trivial T.F.]. Therefore one has a relation

$$(4) \qquad h_n^\circ = \lambda_{n1} f_1^\circ + \ldots + \lambda_{n,n-1} f_{n-1}^\circ \text{ in } A[X_1, \ldots, X_{n-1}].$$

Now the equality (3) gives

$$(5) \qquad h_1^\circ f_1^\circ + \ldots + h_n^\circ f_n^\circ = 0.$$

Using the 1^{st} part of HURWITZ theorem and the relations (3), (4) and (5), one proves that $\wp$ is a trivial T.F. First (4) and (5) imply

$$u_1 f_1^\circ + \ldots + u_{n-1} f_{n-1}^\circ = 0 \text{ in } A[X_1, \ldots, X_{n-1}]$$

where $u_i = \lambda_{ni} f_n^\circ + h_i^\circ$. But $H_1\big(K_\bullet(f_1^\circ, \ldots, f_{n-1}^\circ; A[X_1, \ldots, X_{n-1}]\big)$ is equal to 0; thus

$$\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = [\lambda_{ij}] \begin{bmatrix} f_1^\circ \\ \vdots \\ f_{n-1}^\circ \end{bmatrix}$$

for some skew-symmetric matrix $[\lambda_{ij}]_{1 \leq i,j \leq n-1}$ over $A[X_1, \ldots, X_{n-1}]$. Putting $\lambda_{nn} = 0$ and $\lambda_{in} = -\lambda_{ni} (1 \leq i \leq n-1)$ we obtain

$$h_j^\circ = \sum_{i=1}^{n} \lambda_{ji} f_i^\circ \; (1 \leq j \leq n).$$

Now let $h'_j = \sum_{i=1}^n \lambda_{ji} f_i$. Hence $(h'_j)^\circ = h_j^\circ$ (λ_{ji} does not contain X_n), and so

$$h_j = h'_j + X_n \rho_j \text{ for some } \rho_j \text{ in } C = A[X_1, \ldots, X_n].$$

From (3) one has

$$X_n \wp = \sum_{j=1}^{n} h'_j f_j + X_n \sum_{j=1}^{n} \rho_j f_j.$$

By skew-symmetricity of $[\lambda_{ij}]_{1 \leq i,j \leq n}$, the sum $\sum h'_j f_j$ is equal to 0. It comes $\wp = \sum \rho_j f_j$. Hence $\wp$ is a trivial T.F., and that is the end of the proof of the proposition.

V. DEFINITION OF THE RESULTANT.

Let us recall that notation and data are those fixed in paragraph I.

1. We saw in II.5. that $\mathcal{B} = H^{\circ}_{\mathcal{M}}(B)$ is the ideal of Trägheitsformen in B. It is homogeneous, as is also the ideal $\mathcal{T}$ of Trägheitsformen in C. We denote as usual by $\mathcal{B}_s$, $\mathcal{T}_s$ the homogeneous part of degree s. (The grading here is defined by the *variables* $X_1, \ldots, X_n : \deg(X_i) = 1$).

We denoted $\mathcal{A}$ the ideal $\mathcal{T}_0$ of T.F. of degree 0. Since the canonical map $A \to B = C/(f_1, \ldots, f_r)$ is injective, we have

$$\mathcal{A} = \mathcal{T}_0 = \mathcal{B}_0 \subset A.$$

The ideal $\mathcal{A}$ is called the *resultant ideal* (see II.8.).

For any $i \in [n]$, $B_{(X_i)}$ stands for the degree 0 homogeneous part of the $\mathbb{Z}$- graded ring $B_{(X_i)}$. By II.5-6-7, we have

$$A/\mathcal{A} \underset{\text{inj.}}{\hookrightarrow} C/\mathcal{T} \xrightarrow{\sim} B/\mathcal{B}$$
$$B/\mathcal{B} \underset{\text{inj.}}{\hookrightarrow} B_{X_i} \xleftarrow{\sim} A_1[X_1, \ldots, X_n, X_i^{-1}]$$

(all maps are canonical). In particular, there is an exact sequence

$$0 \to \mathcal{A} \to A \to B_{(X_i)}$$
$$\text{with } B_{(X_i)} \xleftarrow{\sim} A_1\left[\frac{X_1}{X_i}, \ldots, \frac{X_n}{X_i}\right].$$

Recall $A_1 = k$ [certain coefficients of $f_1, \ldots, f_r$]. Therefore, we have the following assertion :

PROPOSITION.. — *If the ground ring k is an integral domain, then the three ideals $\mathcal{T}, \mathcal{B}$ and $\mathcal{A}$ are prime.*

2. From now on, unless stated otherwise, we assume that we are in the case where $r = n$, i.e.

the number of polynomials =the number of variables.

We want to show the following, for an *arbitrary* ground ring k.

THEOREM.. — *The resultant ideal $\mathcal{A}$ is principal, and has a generator $R = R(f_1, \ldots, f_n)$ such that $R(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$.*

Let us explain the notation : $\mathcal{A}$ is an ideal of the ring

$$A = k[U_{i,\alpha} \mid (i, \alpha) \in [n] \times \mathbb{N}^n : |\alpha| = d_i].$$

So $R = R(f_1, \dots, f_n)$ is a polynomial over k in the indeterminates $U_{i,\alpha}$ (= coefficients of the $f_i's$). Hence $R(X_1^{d_1}, \dots, X_n^{d_n})$ is the specialization of $R(f_1, \dots, f_n)$ induced by the specializations $f_1 \mapsto X_1^{d_1}, \dots, f_n \mapsto X_n^{d_n}$ (see I.).

We will see later that the element $R(f_1, \dots, f_n)$ as defined above is not necessarily unique, but there is one determined in a *canonical* way.

Several steps are needed to prove the theorem. They will occupy the whole remain of this section.

3. Assume k is a *unique factorization domain* (U.F.D). Fix any indeterminate $U_{i,\alpha}$ in A and call it U. Then the polynomial ring $A = A'[U]$ is a U.F.D., since $A' = k[U_{j,\beta} \mid U_{j,\beta} \neq U]$. We are going to work in A under *this form.*

We know that the MACAULAY determinants are non-trivial Trägheitsformen (III.). So $\mathcal{A} \neq (0)$. On the other hand, by (IV.3.), every $a \in \mathcal{A}, a \neq 0$, has $\deg_U(a) \geq 1$. Therefore we have an integer

$$s = \inf[\deg_U(a)] \geq 1 (a \in \mathcal{A}, a \neq 0).$$

ASSERTION. *There exists a prime element R in $\mathcal{A}$ such that* $\deg_U(R) = s$. *Any such an element generates the ideal $\mathcal{A}$.*

Proof.— Take $a \in \mathcal{A}, a \neq 0$, such that $\deg_U(a) = s$. There is a decomposition in a product of prime factors $a = q_1 \dots q_t$ in $A = A'[U]$. But $\mathcal{A}$ is a prime ideal by the Proposition in 1. Hence some $q_{i_0} \in \mathcal{A}$. Now $\deg_U(q_{i_0}) \geq 1$ by IV.3. and $\deg_U(q_{i_0}) \leq \deg_U(a) = s$. Thus, by definition of s, $\deg_U(q_{i_0}) = s$.

Putting $R = q_{i_0}$, let us show that R generates the ideal $\mathcal{A} \subset A = A'[U]$. Let $b \in \mathcal{A}$. Since A' has no zero-divisor, we can apply euclidean division and obtain

$$\lambda b = Rw + v, \text{ with } \lambda \in A', v = 0 \text{ or } \deg_U(v) < s.$$

Thus $v = \lambda b - Rw \in \mathcal{A}$ and, if $v \neq 0$, $\deg_U(v) \geq 1$ (loc.cit.). Here again the definition of s implies $v = 0$. One deduces that the prime element R divides λ or b. But $\lambda \in A'$ does not contain U while R does; so R divides b. Consequently, R is a generator of $\mathcal{A}$, as required (*) .

4. The ring k is still assumed to be a U.F.D. So, by 3., $\mathcal{A}$ is principal, generated by a prime element called a *resultant* of $(f_1, \dots, f_n)$

$$R = R(f_1, \dots, f_n).$$

This is unique only up to multiplication by a unit in A' hence in k (Recall that we have $A = A'[U], A' = k[U_{j,\beta} \mid U_{j,\beta} \neq U]$).

(*) We see in this proof of the assertion above how the hypothesis $r = n$ is fundamental and how useful is the corollary IV.3.

Since $\mathcal{A} = \mathrm{Ker}(A \longrightarrow B_{(X_n)})$ (see 1.), we have an exact sequence

$$A \xrightarrow[\cdot R]{} A \longrightarrow B_{(X_n)} \; (\cdot R = \text{ multiplication by } R).$$

In fact, if $a \in A$ then

$$(\star) \qquad A \xrightarrow[\cdot a]{} A \longrightarrow B_{(X_n)} \text{ exact} \Longleftrightarrow \mathcal{A} = (a)\cdot$$

This shows that, after any polynomial extension of the ring k, the resultant ideal is still generated by R (A and $B_{(X_n)}$ are polynomial rings over k; cf 1.).

More precisely, write

$$A = A_k, \mathcal{A} = \mathcal{A}_k, R = R_k, \ldots.$$

to indicate that the ground ring we are working over is k.

Then one has

$$\mathcal{A}_K = (R_k) \text{ in } A_K$$

for all K of the form $k[V]$. In other words

$$R_K(f_1, \ldots, f_n) = R_k(f_1, \ldots, f_n) \text{ in } A_K,$$

up to a unit in k. Of course the polynomials $f_1, \ldots, f_n$ remain generic by polynomial extension of k.

5. Since A is a polynomial ring over k, with the coefficients of $f_1, \ldots, f_n$ as indeterminates, R is a polynomial in these coefficients. We denote by $\deg_{f_j}(R)$ its degree (*) with respect to the coefficients $U_{j,\beta}$ of f_j.

(*) R divides $D(\delta + 1)$ after III.1.; hence R is *homogeneous* in the $U_{j,\beta}$'s, with j fixed.

LEMMA 5.1. *We have* $\deg_{f_j}(R) = d_1 \dots d_n/d_j$ *for all* $j \in [n]$.

Proof.— Let $j \in [n]$ and let σ be a permutation in S_n such that $\sigma(n) = j$. We know by III.3. that $D^\sigma(\delta+1) \in \mathcal{A}$ and that $\deg_{f_j} D^\sigma(\delta+1) = d_1 \dots d_n/d_j$. Thus R divides $D^\sigma(\delta+1)$ and hence $\deg_{f_j}(R) \leq d_1 \dots d_n/d_j$. To see the inequality $\deg_{f_j}(R) \geq d_1 \dots d_n/d_j$, we will use a partial multiplicative property of $R(f_1, \dots, f_n)$ which is going to be proved in the following subparagraph. Recall that $\deg_{f_j}(R) \geq 1$ for all j (IV.3.).

6. Here we take the ring k in the form

$$k = k'[U'_{1,\alpha}, U''_{1,\beta} \mid |\alpha| = d'_1, |\beta| = d''_1]$$

where k' is a commutative ring with 1, d'_1 and d''_1 are integers ≥ 1 such that $d'_1 + d''_1 = d_1$. Consider the *generic* polynomials over k'

$$f'_1 = \sum U'_{1,\alpha} X^\alpha (|\alpha| = d'_1)$$
$$f''_1 = \sum U''_{1,\alpha} X^\alpha (|\alpha| = d''_1).$$

LEMMA 6.1. *Suppose* k' *is a U.F.D. Then the following divisibility*

$$R(f'_1, f_2, \dots, f_n) R(f''_1; f_2, \dots, f_n) \mid R(f'_1 f''_2, f_2, \dots, f_n)$$

holds in the ring

$$k'[U'_{1,\alpha}, U''_{1,\beta}, U_{j,\gamma}](|\alpha| = d'_1, |\beta| = d''_1; j \neq 1, |\gamma| = d_j)$$

(We will see later that in fact we have an equality, up to a unit in k'.) Let us make precise the definition of the resultants above. To simplify notation, put

$$R' = R(f'_1, f_2, \dots, f_n), R'' = R(f''_1, f_2, \dots, f_n)$$
$$R_0 = R(f'_1 f''_1, f_2, \dots, f_n).$$

Then R_0 is obtained from $R(f_1, f_2, \dots, f_n)$ by the specialization $f_1 \longmapsto f'_1 f''_1$;

R' is defined as $R(f_1, \dots, f_n)$ in 4. with the ground ring $k'[U''_{1,\beta} \mid |\beta| = d''_1]$; similarly for R'' but with $k'[U'_{1,\alpha} \mid |\alpha| = d'_1]$.

Of course, R_0, R', R'' are all determined up to a unit in k'.

Proof of the Lemma.

By specialization, R_0 is a Trägheitsform w.r.t. $(f'_1 f''_1, f_2, \dots, f_n)$ (*) since $R(f_1, \dots, f_n)$ is w.r.t. $(f_1, \dots, f_n)$. But $(f'_1 f''_1, f_2, \dots, f_n) \subset (f'_1, f_2, \dots, f_n)$ and so R_0 is a T.F. with respect to $(f'_1, f_2, \dots, f_n)$. On the other hand, by 3. R' generates the ideal

$$\mathcal{A}' = \mathcal{A}(f'_1, f_2, \dots, f_n) \subset k'[U''_{1,\beta}][U'_{1,\alpha}, U_{j,\gamma} \mid j \neq 1],$$

(*) Definition of T.F. here is similar to the generic case.

analogous to $\mathcal{A} = \mathcal{A}(f_1, f_2, \ldots, f_n)$. Hence R' divides R_0. In the same way, R'' divides R_0. Now, by 4., we have (up to a unit in k')

$$R' = R_{k'}(f_1', f_2, \ldots, f_n)\,,\ R'' = R_{k'}(f_1'', f_2, \ldots, f_n).$$

Thus R', R'' are distinct prime elements because $\deg_{f_1'}(R') \geq 1$ and $\deg_{f_1'}(R'') = 0$. So $R'R'' \mid R_0$.

7. Continuation of the proof of Lemma 5.1.

i) In the case of $d_1 = \ldots = d_n = 1$, we know (II.1.) that $D = \det(f_1, \ldots, f_n)$ is a T.F. Thus $R \mid D$, and since $\deg_{f_i}(D) = 1$, we have $\deg_{f_i}(R) = 1$ (we know that $\deg_{f_i}(R) \geq 1$). So the lemma is true in this case.

ii) In a similar way as Lemma 6.1. we have

$$(7.1) \qquad R(f_1, \ldots, f_j', \ldots, f_n) R(f_1, \ldots, f_j'', \ldots, f_n) \mid R(f_1, \ldots, f_j' f_j'', \ldots, f_n)$$

for all j. Let us specialize each f_j to the product of d_j *generic* linear forms $l_{j1}, l_{j2}, \ldots, l_{jd_j}$. This supposes that the ring k contains the coefficients of all the l_{jq}*'s* (see 6. for an analogous situation). Put

$$g_j = \prod l_{jq}\, (1 \leq q \leq d_j).$$

Therefore the product

$$\prod R(l_{1q_1}, \ldots, l_{nq_n})\ (1 \leq q_1 \leq d_1, \ldots, 1 \leq q_n \leq d_n)$$

divides $R(g_1, \ldots, g_n)$ (7.1.) *Fix* $j \in [n]$; the case i) shows that $\deg_{l_{jq_j}} R(l_{1q_1}, \ldots, l_{nq_n}) = 1$ and hence the degree w.r.t. all the coefficients of $l_{j1}, \ldots, l_{jdj}$ of $R(g_1, \ldots, g_n)$ is $\geq d_1 d_2 \ldots d_n$.

Let $v_{j,\alpha}(|\alpha| = d_j)$ be the coefficients of the polynomial g_j (in the variables $X_1, \ldots, X_n$). As polynomial in the $v_{j,\alpha}$*'s* $R(g_1, \ldots, g_n)$ has degree equal to $\deg_{f_j} R(f_1, \ldots, f_n)$.

But each $v_{j\alpha}$ is a homogeneous polynomial of degree d_j in the coefficients of $l_{j1}, l_{j2}, \ldots, l_{jd_j}$. It follows that $\deg_{f_j} R(f_1, \ldots, f_n) \geq d_1 \ldots d_n / d_j$ as desired. Lemma 5.1. is proven.

8. Case $k = \mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}, p$ prime.

i) Let us take $k = \mathbb{Z}$. We know from 3. that $\mathcal{A} = \mathcal{A}_{\mathbb{Z}}$ is generated by one element R, and that such an element is necessarily prime. Hence two such elements are equal up to a unit in $\mathbb{Z}$, that is up to a sign. Now, choose a generator $R = R(f_1, \ldots, f_n)$ of $\mathcal{A}$ and do the specialization $f_i \longmapsto X_i^{d_i}$ $(1 \leq i \leq n)$. This implies $R(f_1, \ldots, f_n) \longmapsto R(X_1^{d_1}, \ldots, X_n^{d_n}), D(\delta{+}1) \longmapsto 1$ (See Proof in III.1.). Since $R(f_1, \ldots, f_n)$

divides $D(\delta+1)$ (loc.cit.), we obtain $R(X_1^{d_1},\dots,X_n^{d_n})=\pm 1$. Consequently, *there exists a unique generator* $R_{\mathbb{Z}}=Ret_{\mathbb{Z}}(f_1,\dots,f_n)$ *of* $\mathcal{A}=\mathcal{A}_{\mathbb{Z}}$ *such that* $Ret_{\mathbb{Z}}(X_1^{d_1},\dots,X_n^{d_n})=1$ (*)

ii) Let p be a prime number and $k=\mathbb{Z}/p\mathbb{Z}$. The same arguments as in i) show that the ideal $\mathcal{A}=\mathcal{A}_k$ is generated by one element $R=R_k(f_1,\dots,f_n)$, unique up to a unit in k, and that $R_k(X_1^{d_1},\dots,X_n^{d_n})$ is a unit in k. Therefore *there exists a unique element* $R_k=\mathrm{Ret}_k(f_1,\dots,f_n)$ *which generates* $\mathcal{A}=\mathcal{A}_k$ *and such that* $\mathrm{Ret}_k(X_1^{d_1},\dots,X_n^{d_n})=1$.

Let $\overline{R_{\mathbb{Z}}}$ be the class mod p in A_k of the resultant $R_{\mathbb{Z}}$ defined in i). By definition of a Trägheitsform, we have $\overline{R_{\mathbb{Z}}}\in\mathcal{A}_k$. Moreover $\overline{R_{\mathbb{Z}}}\neq 0$ since $\overline{\mathrm{Ret}_{\mathbb{Z}}(X_1^{d_1},\dots,X_n^{d_n})}=\bar{1}$. Hence $\overline{R_{\mathbb{Z}}}=a\,R_k, a\in A_k$, and by Lemma 5.1. we have $\deg_{f_i}(\overline{R_{\mathbb{Z}}})=\deg_{f_i}(R_k)$ for all i. Thus $a\in k$. Using the specialization $f_j\mapsto X_j^{d_j}\,(1\le j\le n)$, one obtains $a=1$. So

$$\mathrm{Ret}_k(f_1,\dots,f_n)=\overline{\mathrm{Ret}_{\mathbb{Z}}(f_1,\dots,f_n)}.$$

9. General case.

From 4.($\star$) and 8.i)-ii) above, we see that the sequence

$$\text{(S)}\qquad 0\longrightarrow A_{\mathbb{Z}}\xrightarrow[\cdot R_{\mathbb{Z}}]{}A_{\mathbb{Z}}\longrightarrow(B_{\mathbb{Z}})_{(X_n)}\ \text{(with ground ring }=\mathbb{Z})$$

is exact and, mod all p, it remains exact since it has then the form

$$0\longrightarrow A_K\xrightarrow[\cdot R_K]{}A_K\longrightarrow(B_K)_{(X_n)}\ \text{(with ground ring }=K=\mathbb{Z}/p\mathbb{Z}).$$

Taking an arbitrary ring k, we deduce that the sequence $(S)\otimes_{\mathbb{Z}}k$

$$0\longrightarrow A_k\xrightarrow[\cdot R]{}A_k\longrightarrow(B_k)_{(X_n)}$$

is exact, with $R=$ the image of $R_{\mathbb{Z}}$ in A_k by the map induced by the canonical one $\mathbb{Z}\to k$. Indeed, since $A_{\mathbb{Z}}$ and $(B_{\mathbb{Z}})_{(X_n)}$ are free $\mathbb{Z}-$modules (see 1.), the cokernel of the map $A_{\mathbb{Z}}\to(B_{\mathbb{Z}})_{(X_n)}$ is a torsion free $\mathbb{Z}-$module (hence flat) (**).

Therefore, R generates the ideal $\mathcal{A}_k$ in A_k by 4.($\star$) (and, moreover, R is a *non-zero divisor*). Now $R=R(f_1,\dots,f_n)$ satisfies $R(X_1^{d_1},\dots,X_n^{d_n})=1$ in k because R is, by definition, the image of $R_{\mathbb{Z}}$ in A_k (8.i).

(*) Because of the standard notation res for the residue, we prefer the symbol Ret for the resultant (like Det for determinant).

(**) The statement used (and easy to check) is the following. Let $M\xrightarrow{u}N\xrightarrow{v}P$ be an exact sequence of $\mathbb{Z}-$modules, with N and P torsion free. If, modulo every prime, the sequence is still exact, then Coker (v) is torsion free.

That is the end of the proof of the theorem stated in section 2.

10. In this section we discuss uniqueness of the element defined in Theorem 2. and define the resultant.

ASSERTION. *If the ground ring k is arbitrary, then the element $R(f_1, \ldots, f_n)$ as defined in Theorem 2. is not necessarily unique. If k is reduced, then it is unique.*

Proof.— In 9. we saw that $\mathcal{A}_k$ is generated by an element R, which is a non-zerodivisor and equal to the image of $R_{\mathbb{Z}}$ (8.i). Let $R' = R'(f_1, \ldots, f_n)$ be any other generator of $\mathcal{A}_k$ such that : $R'(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$. There exist $S, T \in A_k$ satisfying

$$R' = S\, R,\ R = TR'.$$

Since R does not divide zero in A_k, one has $TS = 1$. In particular, S is a unit in $A_k = k[U_{i\alpha}]$.

ii) If k is reduced, then $S \in k$, and by specialization $f_i \mapsto X_i^{d_i} (1 \leq i \leq n)$ one obtains $S = 1$ from the equality $R' = R$.

i)) Now assume that k is not reduced. Let a be a nilpotent element in k, $a \neq 0$. Denote by U some coefficient $U_{j\beta}$ of the $f_i's$ which specializes to zero when the polynomials $f_1, \ldots, f_n$ are specialized to $X_1^{d_1}, \ldots, X_n^{d_n}$ (respectively). (We suppose $n \geq 2$). Take

$$R_1 = (1 + aU)R \in A_k.$$

As $1 + aU$ is a unit in A_k, R_1 generates the ideal $\mathcal{A}_k$. Moreover

$$R_1(X_1^{d_1}, \ldots, X_n^{d_n}) = (1 + a.0)R(X_1^{d_1}, \ldots, X_n^{d_n}) = 1.$$

Since $R_1 \neq R$, we are done.

DEFINITIONS.

a) *The unique element* $\mathrm{Ret}_{\mathbb{Z}}(f_1, \ldots, f_n)$ *defined in* (8.i) *is called* **the resultant** *of the generic polynomials* $f_1, \ldots, f_n$ over $\mathbb{Z}$.

b) *For an arbitrary ground ring k, we put*

$$\mathrm{Ret}_k(f_1, \ldots, f_n) = \overline{\mathrm{Ret}_{\mathbb{Z}}(f_1, \ldots, f_n)}$$

where the latter is the image of $\mathrm{Ret}_{\mathbb{Z}}(f_1, \ldots, f_n)$ *under the canonical map* $A_{\mathbb{Z}} \to A_k$ *(induced by the natural map* $\mathbb{Z} \to k$*). We know that* $\mathrm{Ret}_k(f_1, \ldots, f_n)$ *generates the resultant ideal* $\mathcal{A}_k$ *and has the property* $\mathrm{Ret}_k(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$. *It is called* **the resultant** *of the generic polynomials $f_1, \ldots, f_n$ over k.*

c) If $g_1, \ldots, g_n \in k[X_1, \ldots, X_n]$ are homogeneous of degrees $d_1, \ldots, d_n$, then $\mathrm{Ret}_k(g_1, \ldots, g_n)$ will stand for the specialization of $\mathrm{Ret}_k(f_1, \ldots, f_n)$ induced by the specializations $f_i \mapsto g_i$ (see I.). Sometimes we will consider a mixed case

$$\mathrm{Ret}_k(f_1, \ldots, f_s, g_{s+1}, \ldots, g_n).$$

defined in a similar way, and called *the resultant* of $f_1, \ldots, f_s, g_{s+1}, \ldots, g_n$.

While proving Theorem 2., some properties of the resultant have been established. We state them and give examples in the next paragraph.

VI. FIRST PROPERTIES AND EXAMPLES OF THE RESULTANT.

1. First properties of the resultant.

The resultant $\mathrm{Ret}_k(f_1, \dots, f_n)$ has been defined in V.10. All of the following properties are immediate from its construction in V.

a) $\mathrm{Ret}_k(f_1, \dots, f_n)$ *generates the resultant ideal* $\mathcal{A}_k$ *and* $\mathrm{Ret}_k(X_1^{d_1}, \dots, X_n^{d_n}) = 1$.

b) *If* $k = \mathbb{Z}$ then $\mathrm{Ret}_k(f_1, \dots, f_n)$ *is the unique element in* $A_k = k[U_{i,\alpha} \mid 1 \le i \le n, |\alpha| = d_i]$ *which has property* a).

c) *One has*

$$\mathrm{Ret}_k(f_1, \dots, f_n) = \overline{\mathrm{Ret}_{\mathbb{Z}}(f_1, \dots, f_n)},$$

where $\bar{a}$ *is the image of* $a \in A_{\mathbb{Z}}$ *by the canonical map* $A_{\mathbb{Z}} \to A_k$. *In particular if* $k = k'[V]$, *then* $\mathrm{Ret}_k(f_1, \dots, f_n) = \mathrm{Ret}_{k'}(f_1, \dots, f_n)$.

d) $\mathrm{Ret}_k(f_1, \dots, f_n)$ *is not a zero-divisor in* A_k.

e) *If* k *is an integral domain, then* $\mathrm{Ret}_k(f_1, \dots, f_n)$ *is irreducible in the polynomial ring* A_k. *In particular if* $k = \mathbb{Z}$, *then* $\mathrm{Ret}_k(f_1, \dots, f_n)$ *is geometrically irreducible* (by c)).

f) *For each* $i (1 \le i \le n), \mathrm{Ret}_k(f_1, \dots, f_n)$ *is a homogeneous polynomial in the coefficients* $U_{i,\alpha}$ *of* f_i *the degree of which is equal to* $d_1 \dots d_n / d_i$.

g) Multiplicativity property. *Let* $i \in [n]$ *and let* f_i', f_i'' *be generic polynomials over* k. *Then we have*

$$\begin{aligned}&\mathrm{Ret}_k(f_1, \dots, f_{i-1}, f_i' f_i'', f_{i+1}, \dots, f_n)\\ =&\mathrm{Ret}_k(f_1, \dots, f_{i-1}, f_i', f_{i+1}, \dots, f_n)\, \mathrm{Ret}_k(f_1, \dots, f_{i-1}, f_i'', f_{i+1}, \dots, f_n).\end{aligned}$$

This equality takes place in the polynomial ring $k[E]$ where E is the set of the coefficients of the generic polynomials $f_1, \dots, f_{i-1}, f_i', f_i'', f_{i+1}, \dots, f_n$.

Proof.— a) and c) are stated in V.10., b) in V.8., d) in V.9. Property e) is a consequence of Proposition in V.1. Property f) is shown for k a unique factorization domain (Lemma 5.1. in V), hence it is true for $k = \mathbb{Z}$. So by c), f) is true for k arbitrary (Recall that $\mathcal{A}_k$ contains MACAULAY determinants and that these are not zero, III.). To see g) it is enough, by c), to do it for $k = \mathbb{Z}$. Using the divisibility relation V. (7.1.) and property f), one shows that the equality to establish is true up to a multiplicative element $\lambda \in \mathbb{Z}$. Now the specializations

$$f_j \mapsto X_j^{d_j} (j \ne i), f_i' \mapsto X_i^{d_i'}, f_i^{d_i''} \mapsto X_i^{d_i''} \, (d_i' = \deg(f_i'), d_i'' = \deg(f_i''))$$

imply $\lambda = 1$, and we are done.

EXAMPLES.

2.a) Let $n = 1$. So $f_1 = U X_1^{d_1}$, and, since $\mathrm{Ret}_k(f_1)$ is homogeneous in U of degree $d_1/d_1 = 1$, we have $\mathrm{Ret}_k(f_1) = \lambda U (\lambda \in k)$. But $\mathrm{Ret}_k(X_1^1) = 1$. Hence $\lambda = 1$, and

$$\mathrm{Ret}_k(f_1) = U.$$

b) *Assume* $d_1 = \ldots = d_n = 1$ (i.e. $f_1, \ldots, f_n$ are linear forms). *Then*

$$\mathrm{Ret}_k(f_1, \ldots, f_n) = \mathrm{Det}(f_1, \ldots, f_n).$$

(Det = determinant).

Proof.— Let us write $f_i = \sum_{j=1}^n U_{ij} X_j$. Thus

$$D = \mathrm{Det}(f_1, \ldots, f_n) = |U_{ij}| (1 \leq i, j \leq n).$$

After 1.c) it is enough to work with $k = \mathbb{Z}$. We know that D is a Trägheitsform w.r.t. $f_1, \ldots, f_n$ (II.1.). Then there exists $a \in A = \mathbb{Z}[U_{ij}]$ such that (1.a)

$$D = a \mathrm{Ret}_{\mathbb{Z}}(f_1, \ldots, f_n).$$

But $\deg_{f_i}(D) = 1$ for all i. Therefore $a \in \mathbb{Z}$ since $\deg_{f_i}$ of $\mathrm{Ret}_{\mathbb{Z}}(f_1, \ldots, f_n)$ is equal to 1 for all i (1.f.). We have $\mathrm{Det}(X_1, \ldots, X_n) = 1$ and $\mathrm{Ret}_{\mathbb{Z}}(X_1, \ldots, X_n) = 1$, so $a = 1$.

c) *If* $n = 2$, *then* (III.2.)

$$\mathrm{Ret}_k(f_1, f_2) = D(d_1 + d_2 - 1) \text{ (= SYLVESTER det.)}$$

Proof.— To specify the ground ring k we denote a MACAULAY determinant (III.) by $D(t) = D_k(t)$. From the definition it is clear that $\overline{D_{\mathbb{Z}}(t)} = D_k(t)$ where $\bar{a}$ is the image of $a \in A_{\mathbb{Z}}$ defined by the natural map $\mathbb{Z} \to k$.

To check the desired relation it is then sufficient to do it the case $k = \mathbb{Z}$. By III.1. one has

$$D_{\mathbb{Z}}(d_1 + d_2 - 1) = \lambda \, \mathrm{Ret}_{\mathbb{Z}}(f_1, f_2)$$

with $\lambda \in A_{\mathbb{Z}} = \mathbb{Z}[U_{1\alpha}, U_{2\beta} \mid |\alpha| = d_1, |\beta| = d_2]$ (1.a.). But $D_{\mathbb{Z}}(d_1 + d_2 - 1)$ is the SYLVESTER determinant of the polynomials f_1, f_2 (III.2.). Thus its degree as polynomial in the $U_{1\alpha}$ is d_2 and its degree as polynomial in the $U_{2\beta}$ is d_1. Since $\mathrm{Ret}_{\mathbb{Z}}(f_1, f_2)$ has the same property (1.f.), λ belongs to $\mathbb{Z}$. Now $D_{\mathbb{Z}}(d_1 + d_2 - 1)$ and $\mathrm{Ret}_{\mathbb{Z}}(f_1, f_2)$ specialize to 1 when f_1 and f_2 are specialized to $X_1^{d_1}, X_2^{d_2}$. Hence $\lambda = 1$.

The next example is the first less familiar one.

3. We suppose that $f_1, \cdots, f_{n-1}$ are linear forms (i.e. $d_1 = \ldots = d_{n-1} = 1$) and denote by U_{ij} their coefficients

$$f_i = \sum_{j=1}^{n} U_{ij} X_j \ (1 \leq i \leq n-1).$$

Let $\Delta_1, \ldots, \Delta_n \in A = k[U_{ij} \mid 1 \leq i \leq n-1, 1 \leq j \leq n]$ be defined by the formula

$$\mathrm{Det}(f_1, \ldots, f_{n-1}, \sum_1^n V_j X_j) = \Delta_1 V_1 + \ldots + \Delta_n V_n,$$

where $V_1, \cdots, V_n$ are new indeterminates. So $\Delta_1, \ldots, \Delta_n$ are *signed* minors of the matrix

$$\begin{bmatrix} U_{ij} \\ \hline V_1 \cdots \cdot V_n \end{bmatrix}$$

The resultant of the generic polynomials $f_i = f_i(X_1, \ldots, X_n)(1 \leq i \leq n)$ *is equal to* $f_n(\Delta_1, \ldots, \Delta_n)$.

Proof.— Assume that one knows that $f_n(\Delta_1, \ldots, \Delta_n)$ is a T.F. with respect to $f_1, \ldots, f_n$. Then one proceeds as in the preceding examples :
- The case $k = \mathbb{Z}$ is sufficient (1.c.);
- $f_n(\Delta_1, \ldots, \Delta_n) = \lambda \mathrm{Ret}(f_1, \ldots, f_n)$, with $\lambda \in A$ (1.a.);
- looking at the degrees, one has

$$\deg_{f_n}[f_n(\Delta_1, \ldots, \Delta_n)] = 1$$
$$\deg_{f_i}[f_n(\Delta_1, \ldots, \Delta_n)] = d_n \text{ for all } i \neq n,$$

  since $\deg_{f_i}(\Delta_j) = 1$ (all $i \neq n$, all j);
- but the resultant here has the same corresponding degrees (1.f.), therefore $\lambda \in \mathbb{Z}$;
- specialize : $f_i \longmapsto X_i (i \neq n), f_n \longmapsto X_n^{d_n}$; then Δ_j specializes to 0 if $j \neq n$ and to 1 if $j = n$. Since $f_n(0, \ldots, 0, 1) = 1$, one obtains $\lambda = 1$ (1.a.), and we are done.

The proof will be achieved from the next subparagraph.

4. We keep the assumption $d_1 = \ldots = d_{n-1} = 1$ and the notation made in number 3.

ASSERTION. *For all* i, j, *we have*

$$\Delta_i X_j - \Delta_j X_i \in (f_1, \ldots, f_{n-1})$$

in the ring $k[U_{pq}, X_t] (1 \leq p \leq n-1, 1 \leq q \leq n, 1 \leq t \leq n)$.

Proof.— ([J1] 5.4.) Assume $i < j$ and take the following matrix

$$M = \begin{array}{c} \left[\begin{array}{ccccccc} U_{11} & \dots & X_iU_{1i} & \dots & U_{1j} & \dots & U_{1n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ U_{n-1,1} & \dots & X_iU_{n-1,i} & \dots & U_{n-1,j} & \dots & U_{n-1,n} \\ 0 & \dots & -X_j & \dots & 1 & \dots & 0 \end{array}\right] \\ \begin{array}{cc} \uparrow \qquad\qquad & \uparrow \\ \text{col.}i \qquad\qquad & \text{col.}j \end{array} \end{array}.$$

We are going to compute Det$M$ in two different ways. Let us expand with respect to the last row :

$$\operatorname{Det} M = -X_j\Delta_i + X_i\Delta_j \text{ (by definition of} \Delta_1, \dots, \Delta_n).$$

Now in the matrix M multiply each s^{th} column by $X_s (s \neq i)$ and then add it to the i^{th} column; the result is

$$M' = \begin{array}{c} \left[\begin{array}{ccccccc} & & f_1 & & & & \\ & & & & U_{lm} & & \\ & U_{pq} & \vdots & & & & \\ & & f_{n-1} & & & & \\ \hline 0 & \dots & 0 & \dots & 1 & \dots & 0 \end{array}\right] \\ \begin{array}{cc} \uparrow \qquad\qquad & \uparrow \\ \text{col.}i \qquad\qquad & \text{col.}j \end{array} \end{array}.$$

Expanding w.r.t. the last row, we see that Det(M') belongs to the ideal $(f_1, \dots, f_{n-1})$. This proves our assertion since Det$M$ = DetM'.

COROLLARY. *Let* $g = g(X_1, \dots, X_n) \in k[U_{pq}, X_t]$ *be a homogeneous polynomial of degree* d (w.r.t. $X_1, \dots, X_n$). *Then*

$$X_1^d g(\Delta_1, \dots, \Delta_n) - \Delta_1^d g(X_1, \dots, X_n) \in (f_1, \dots, f_{n-1}).$$

Applying this result to f_n, we see that $X_1^{d_n} f_n(\Delta_1, \dots, \Delta_n)$ belongs to $(f_1, \dots, f_{n-1}, f_n)$ in the ring C; thus $f_n(\Delta_1, \dots, \Delta_n)$ is a Trägheitsform (II.6.) w.r.t. $f_1, \dots, f_n$ (This completes the proof of the statement in 3.).

The corollary above is a particular case of the following simple fact :

LEMMA. *Let* R *be a commutative ring with* 1, *and let* $P_1, Q_1, \dots, P_n, Q_n \in R[X_1, \dots, X_n]$. *Assume* I *is an ideal of* $R[X_1, \dots, X_n]$ *such that*

$$P_1Q_j - Q_1P_j \in I \quad \text{for all} \quad j.$$

Then, for every homogeneous polynomial $g = g(X_1, \ldots, X_n)$ of degree $d \geq 1$, we have

$$P_1^d g(Q_1, \ldots, Q_n) - Q_1^d g(P_1, \ldots, P_n) \in I.$$

Proof of the lemma. It is enough to show the result when g is a monomial $X_1^{\alpha_1} \ldots X_n^{\alpha_n} (\alpha_1 + \ldots + \alpha_n = d)$. Now *use the following property of an ideal* :

$(a - b \in I$ and $a' - b' \in I) \Longrightarrow aa' - bb' \in I$

$(aa' - bb' = (a-b)a' + (a'-b')b\,!\,)$. One obtains

$\prod_j (P_1 Q_j)^{\alpha_j} - \prod_j (Q_1 P_j)^{\alpha_j} \in I$;

that is $P_1^d g(Q_1, \ldots, Q_n) - Q_1^d g(P_1, \ldots, P_n) \in I$.

Our purpose now is to compute the resultant when $n = 3$ and $d_1 = d_2 = d_3 = 2$ (three quadratic forms in three variables). We need before some general construction of Trägheitsformen.

5. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. *Assume* that the polynomials f_i can be written in the following form

$$(*) \qquad f_i = \sum_{j=1}^{n} X_j^{\alpha_j + 1} f_{ij} \quad (1 \leq i \leq n).$$

Then denote by J_α the determinant

$$J_\alpha = \text{ Det}\,[f_{ij}]_{1 \leq i,j \leq n} \in C = A[X_1, \ldots, X_n]$$

(For example if $\alpha = 0$ then the good Jacobian $\tilde{J}$ defined in II.3. is of the form J_α.)

The polynomial J_α is homogeneous in $X_1, \ldots, X_n$ of degree $\delta - |\alpha|$ (Recall $\delta = d_1 + \ldots + d_n - n$). *Moreover it is a Trägheitsform with respect to $f_1, \ldots, f_n$*. Indeed :

- multiply the 1^{st} column in J_α by $X_1^{\alpha_1+1}$;
- add to the new 1^{st} column each j^{th} column multiplied by $X_j^{\alpha_j+1}$, with $j \neq 1$;
- the new determinant has now the form

$$X_1^{\alpha_1+1} J_\alpha = \begin{vmatrix} f_1 & f_{12} & \cdots\cdots & f_{1n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ f_n & f_{n2} & \cdots\cdots & f_{nn} \end{vmatrix}$$

(by definition $(*)$ of the f_{ij}). Hence $X_1^{\alpha_1+1} J_\alpha \in (f_1, \ldots, f_n)$, and thus J_α is a T.F. (II.6.).

EXAMPLE : $n = 3, d_1 = d_2 = d_3 = 2$.

In this case we denote by $U_\gamma, V_\gamma, W_\gamma$ the coefficients of f_1, f_2, f_3 respectively. For example f_1 is written in the following form :

$$f_1 = U_{200}X_1^2 + U_{110}X_1X_2 + U_{101}X_1X_3 + U_{020}X_2^2 + U_{011}X_2X_3 + U_{002}X_3^2.$$

Here $\delta = 3$; so if a decomposition $(*)$ as above exists, $\alpha \in \mathbb{N}^3$ must satisfy $|\alpha| \leq 3$: more precisely one has $\alpha_1 \leq 1, \alpha_2 \leq 1, \alpha_3 \leq 1$. It is easy to see that

$$(*)\text{ exists} \iff \alpha \in \{(0,0,0,),(1,0,0),(0,1,0),(0,0,1)\}$$

Taking for example $\alpha = (1,0,0)$, we have

$$\begin{aligned} f_1 &= X_1^2U_{200} + X_2(U_{110}X_1 + U_{020}X_2) + X_3(U_{101}X_1 + U_{011}X_2 + U_{002}X_3) \\ f_2 &= X_1^2V_{200} + X_2(V_{110}X_1 + V_{020}X_2) + X_3(V_{101}X_1 + V_{011}X_2 + V_{002}X_3) \\ f_3 &= X_1^2W_{200} + X_2(W_{110}X_1 + W_{020}X_2) + X_3(W_{101}X_1 + W_{011}X_2 + W_{002}X_3). \end{aligned}$$

The associated determinant is

$$J_{100} = \begin{vmatrix} U_{200} & U_{110}X_1 + U_{020}X_2 & U_{101}X_1 + U_{011}X_2 + U_{002}X_3 \\ V_{200} & V_{110}X_1 + V_{020}X_2 & V_{101}X_1 + V_{011}X_2 + V_{002}X_3 \\ W_{200} & W_{110}X_1 + W_{020}X_2 & W_{101}X_1 + W_{011}X_2 + W_{002}X_3 \end{vmatrix}.$$

Similarly one explicits J_{010}, J_{001}. They are homogeneous of degree 2.

6. Computation of $\mathrm{Ret}(f_1, f_2, f_3)(n = 3, d_1 = d_2 = d_3 = 2)$.

Consider the ordered set

$$E = \{(2,0,0),(1,1,0),(1,0,1),(0,2,0),(0,1,1,),(0,0,2)\} \subset \mathbb{N}^3.$$

Let $|a_{\alpha\beta}|_{\alpha,\beta\in E} \in A = k[U_\alpha, V_\beta, W_\gamma | \alpha, \beta, \gamma \in E]$ be the following determinant :

$$\begin{array}{c} \alpha\backslash\beta \\ 200 \\ 110 \\ 101 \\ 020 \\ 011 \\ 002 \end{array} \begin{array}{c} \begin{array}{cccccc} 200 & 110 & 101 & 020 & 011 & 002 \end{array} \\ \begin{vmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} \end{array} \begin{array}{l} \\ \leftarrow f_1 \\ \leftarrow J_{001} \\ \leftarrow J_{010} \\ \leftarrow f_2 \\ \leftarrow J_{100} \\ \leftarrow f_3 \end{array}$$

The coefficients $a_{\alpha\beta}$ in each row are those of the corresponding polynomial written right. Let us show that this determinant $|a_{\alpha\beta}|$ is a Trägheitsform w.r.t. f_1, f_2, f_3.

The same operations as in II.1. (multiply the 1^{st} column by X_1^2, add to it each other column $n°\beta$ multiplied by X^β) show that

$$X_1^2 \cdot |a_{\alpha\beta}| \in (f_1, J_{001}, J_{010}, f_2, J_{100}, f_3)$$

in $C = A[X_1, X_2, X_3]$. Since $J_{001}, J_{010}, J_{100}$ are T.F. (5.), there exists $t \geq 0$ such that

$$X_1^t\ J_\gamma \in (f_1, f_2, f_3) \text{ for all } \gamma \in \{(0,0,1), (0,1,0), (1,0,0)\}.$$

Thus $X_1^{t+2} \cdot |a_{\alpha\beta}| \in (f_1, f_2, f_3)$, and hence $|a_{\alpha\beta}|$ is a T.F. (II.6.).

ASSERTION. *The resultant $Ret_k(f_1, f_2, f_3)$ is equal to the determinant $|a_{\alpha\beta}|$ defined above.*

Proof.– One can suppose $k = \mathbb{Z}$ (VI.1.c.). We just proved that $a = |a_{\alpha\beta}|$ is a T.F. Hence $a = \lambda R$ for some $\lambda \in A$, with $R = Ret(f_1, f_2, f_3)$ (VI.1.a). Now for each $i = 1, 2, 3$, J_γ is homogeneous of degree 1 w.r.t. the coefficients of $f_i (\gamma = (0,0,1), (0,1,0), (1,0,0))$ (see explicitation of J_{100} in 5.). Therefore the coefficients of f_i appear in exactly four rows of the determinant $|a_{\alpha\beta}|$. One deduces that $\deg_{fi}(a) = 4$. But $\deg_{fi}(R) = 4$ by VI.1.f); whence $\lambda \in \mathbb{Z}$. If each f_j is specialized to X_j^2, then we have the specializations

$$J_{001} \longmapsto X_1X_2,\ J_{010} \longmapsto X_1X_3,\ J_{100} \longmapsto X_2X_3 \text{ (cf 5.)}$$

This shows that the matrix $[a_{\alpha\beta}]$ specializes to the identity matrix. Because $Ret(X_1^2, X_2^2, X_3^2) = 1$, one obtains $\lambda = 1$, as desired.

REMARK. The construction of the determinant $|a_{\alpha\beta}|$ in 6. is a particular case of a more general process. Let d be an integer such that

$$0 \leq d \leq \delta = d_1 + \ldots + d_n - n.$$

Consider $E_d = \{\alpha \in \mathbb{N}^n \mid |\alpha| = d\}$ (ordered lexicographically). Assume that the following property holds :

$$(P) \left[\begin{array}{l} \text{if } \alpha \in E_d \text{ and } \alpha_i < d_i \text{ for all } i \in \{1, \ldots, n\}, \\ \text{then } f_1, \ldots, f_n \text{ can be decomposed in the form} \\ f_i = \sum_{j=1}^n X_j^{\beta_j+1} f_{ij} (1 \leq i \leq n), \text{ with } \beta = (d_1 - \alpha_1 - 1, \ldots, d_n - \alpha_n - 1). \end{array} \right.$$

In this case put $J_\beta = Det[f_{ij}]_{1 \leq i,j \leq n}$ as in 5. Let us construct a determinant $|a_{\alpha\beta}|_{\alpha,\beta \in E_d}$ which is a T.F. Fix $\alpha \in E_d$.

i) If there exists i such that $\alpha_i \geq d_i$, then denote by $i(\alpha)$ the minimal integer ≥ 1 having this property, and put

$a_{\alpha\beta} =$ the coefficient of X^β in $\frac{X^\alpha}{X_{i(\alpha)}^{d_{i(\alpha)}}} \cdot f_{i(\alpha)}$, for all $\beta \in E_d$.

ii) If not, put

$a_{\alpha\beta} =$ the coefficient of X^β in J_γ with $\gamma = (d_1 - \alpha_1 - 1, \ldots, d_n - \alpha_n - 1)$.

Then one obtains a determinant $|a_{\alpha\beta}|_{\alpha,\beta \in E_d}$ which is a T.F. belonging to A, in the same way as in 6.

In the case $n = 3, d_1 = d_2 = d_3 = 2$ (5.6.), the integer $d = 2 (\leq \delta = 3)$ is the smallest one such that the property (P) holds. If $d = 3$, (P) is again true and one finds a determinant $|a_{\alpha\beta}|(\alpha, \beta \in E_3)$ which has 10 rows defined by the polynomials

$$X_1 f_1, X_2 f_1, X_3 f_1, X_1 f_2, X_2 f_2, X_3 f_2, X_1 f_3, X_2 f_3, X_3 f_3, J_{000}.$$

This determinant is still equal to $Ret(f_1, f_2, f_3)$, the proof being the same as in 6.

Finally let us note that modulo $(f_1, \ldots, f_n)$ the decomposition of f_i stated in (P) is unique. Hence the determinant $|a_{\alpha\beta}|(\alpha, \beta \in E_d)$ is uniquely defined since it belongs to A.

VII. FURTHER PROPERTIES OF THE RESULTANT.

In the preceding chapter we saw some properties of the resultant coming directly from its construction. Now we are going to study other properties of the resultant which generalize those of the determinant.

Recall that $Ret_k(f_1,\dots,f_n)$ is the resultant of the generic polynomials $f_1,\dots,f_n$ over k (homogeneous of degrees $d_1,\dots,d_n$ respectively). It lives in the ring

$$A = A_k = k[U_{i,\alpha} \mid 1 \le i \le n, |\alpha| = d_i],$$

where the $U_{i,\alpha}$ ($|\alpha| = d_i$) are the coefficients of f_i. If $g_1,\dots,g_n$ are homogeneous polynomials in $k[X_1,\dots,X_n]$, then *the resultant* $Ret_k(g_1,\dots,g_n)$ (V.10.) *will satisfy the same formulas as* $Ret_k(f_1,\dots,f_n)$, *by specialization.*

1. *Let* ρ *be a permutation of* $1,2,\dots,n$. *Then*

$$Ret_k\left(f_{\rho(1)},\dots,f_{\rho(n)}\right) = \epsilon(\rho)^s Ret_k(f_1,\dots,f_n)$$

where $\epsilon(\rho)$ *is the signature of* ρ *and* $s = d_1\dots d_n$.

Proof.– It suffices to take $k = \mathbb{Z}$ (VI.1.c). The resultant ideals $\mathcal{A} = \mathcal{A}(f_1,\dots,f_n)$ and $\mathcal{A}' = \mathcal{A}\left(f_{\rho(1)},\dots,f_{\rho(n)}\right)$ are equal in the ring $A_{\mathbb{Z}}$ since $(f_1,\dots,f_n) = \left(f_{\rho(1)},\dots,f_{\rho(n)}\right)$ in $C = A_{\mathbb{Z}}[X_1,\dots,X_n]$ (by definition of Trägheitsformen, II.4.). Hence VI.1.a)-e) show that

$$Ret\left(f_{\rho(1)},\dots,f_{\rho(n)}\right) = \epsilon Ret(f_1,\dots,f_n),\ \epsilon = \pm 1.$$

Specializing f_i to $X_i^{d_i}$ we have

$$\begin{aligned}\epsilon &= Ret\left(X_{\rho(1)}^{d_{\rho(1)}},\dots,X_{\rho(n)}^{d_{\rho(n)}}\right) \quad \text{(VI.1.a)}\\ &= \mathrm{Ret}\left(X_{\rho(1)},\dots,X_{\rho(n)}\right)^s \quad \text{(VI.1.g. : multiplicativity).}\end{aligned}$$

But $l_i = l_i(X_1,\dots,X_n) = X_{\rho(i)} (1 \le i \le n)$ are linear polynomials, and we know (by specialization) from VI.2.b) that $Ret(l_1,\dots,l_n) = Det(l_1,\dots,l_n)$. So $Ret(l_1,\dots,l_n) = \epsilon(\rho)$ (determinant of the permutation ρ), as desired.

2. *Assume* $k = k'[V]$ *(k' commutative ring with* 1*,* V *indeterminate). Then for each* i *we have*

$$Ret_k(f_1,\dots,Vf_i,\dots,f_n) = V^s Ret_k(f_1,\dots,f_n)$$

with $s = d_1\dots d_n/d_i$.

This follows from the property (1.f) in VI.

Note here that $Ret_k(f_1, \dots, f_n) = Ret_{k'}(f_1, \dots, f_n)$ (by VI.c).

3. *Let us fix some $i \in [n]$. For every $j \neq i$ such that $d_j = d_i$, we suppose given an indeterminate V_j and that*

$$k = k'[V_j \mid j \neq i : d_j = d_i].$$

We have

$$\mathrm{Ret}_k(f_1, \dots, f_i', \dots, f_n) = \mathrm{Ret}_k(f_1, \dots, f_i, \dots, f_n)$$

where $f_i' = f_i + \sum_{\substack{j \neq i \\ d_j = d_i}} V_j f_j$.

Proof.— To simplify the notation, we take $i = n$. Since $(f_1, \dots, f_{n-1}, f_n') = (f_1, \dots, f_n)$ as ideals in $A_k[X_1, \dots, X_n]$, and since $R' = Ret_k(f_1, \dots, f_{n-1}, f_n')$ is a T.F. with respect to $f_1, \dots, f_{n-1}, f_n\prime$, we have (VI.1.a)

$$R' = \lambda R \text{ for some } \lambda \in A_k,$$

with $R = Ret_k(f_1, \dots, f_n)$. Denote by $W_\gamma(|\gamma| = d_n)$ the coefficients of f_n' as polynomial in $X_1, \dots, X_n$. So

$$W_\gamma = U_{n\gamma} + \sum_{j \neq n} V_j U_{j,\gamma},$$

and hence the coefficients of $f_1, \dots, f_{n-1}, f_n'$ are algebraically independants over k. This means that $f_1, \dots, f_{n-1}, f_n'$ are generic over k; thus (loc.cit.)

$$R = \mu R' \text{ for some } \mu \in A_k.$$

As usual, by (VI.1.c) we can assume $k' = \mathbb{Z}$. Therefore $\lambda\mu = 1$; in particular $\lambda \in \mathbb{Z}$. Now the specialization $V_j \longmapsto 0$ implies $\lambda = 1$, and we are done.

4. Divisibility property (MERTENS [ME])(*)

Let K be a commutative ring with 1, and let $g_1, \dots, g_n, h_1, \dots, h_n$ be homogeneous polynomials of deg ≥ 1 *in $K[X_1, \dots, X_n]$ such that $(h_1, \dots, h_n) \subset (g_1, \dots, g_n)$. Then $Ret_K(g_1, \dots, g_n)$* divides *$Ret_K(h_1, \dots, h_n)$ in K.*

Proof.— By hypothesis, there exist $h_{ij} \in K[X_1, \dots, X_n]$ such that

$$(1) \qquad h_i = \sum_{j=1}^{n} h_{ij} g_j \quad (1 \leq i \leq n),$$

(*) This is a particular case of a theorem by MERTENS.

with h_{ij} homogeneous. Assume that $g_1, \dots, g_n$ are *generic* over K with coefficients $V_{i,\alpha}$ for g_i, and that the coefficients of all the h_{ij}, let us say $W_{ij,\beta}$, are *indeterminates* over K distinct from the $V_{i\alpha}$. So (1) takes place now in the ring

$$\begin{aligned} L &= K[W_{ij,\beta}, V_{s,\alpha} \mid 1 \leq i, j, s \leq n, \beta, \alpha] \\ &= M[V_{s,\alpha} \mid 1 \leq s \leq n, |\alpha| = \deg(g_s)] \end{aligned}$$

Hence by *specialization*, it is enough to see that

$$Ret_M(g_1, \dots, g_n) \mid Ret_M(h_1, \dots, h_n) \text{ in L} \tag{2}$$

(see Definitions in V.10 and the property VI.1.c). Now there exists $t \geq 0$ such that $X_1^t Ret_M(h_1, \dots, h_n) \in (h_1, \dots, h_n)$ (by specialization from the generic case). Thus $X_1^t Ret_M(h_1, \dots, h_n) \in (g_1, \dots, g_n)$, and hence $Ret_M(h_1, \dots, h_n)$ is a T.F. with respect to $g_1, \dots, g_n$, which are generic over M.

It follows that (2) is true (VI.1.a).

5.a) Invariant property.

We suppose the ground ring k of the following form

$$k = k'[V_{ij} \mid 1 \leq i, j \leq n].$$

Recall $A_k = k[U_{i\alpha} \mid 1 \leq i \leq n, |\alpha| = d_i]$, and consider in $C_k = A_k[X_1, \dots, X_n]$ the linear polynomials

$$l = (l_1, \dots, l_n), l_i = V_{i1}X_1 + \dots + V_{in}X_n.$$

For a polynomial $g = g(X_1, \dots, X_n)$, put

$$g \circ l = g(l_1, \dots, l_n).$$

Then we have the formula

$$Ret_k(f_1 \circ l, \dots, f_n \circ l) = Det(l_1, \dots, l_n)^s Ret_k(f_1, \dots, f_n)$$

with $s = d_1 \dots d_n$.

Proof.— As usual the case $k' = \mathbb{Z}$ is sufficient. On the other hand we know that (VI.1.c)

$$R := Ret_k(f_1, \dots, f_n) = Ret_{k'}(f_1, \dots, f_n) \in A_{k'}.$$

Since R is a T.F. with respect to $f_1, \dots, f_n$, there exists $t \geq 1$ such that

$$X_i^t R \in (f_1, \dots, f_n) \text{ in the ring } A_{k'}[X_1, \dots, X_n]$$

for all i. Apply the following $A_{k'}$- algebra homomorphism

$$C_{k'} = A_{k'}[X_1, \ldots, X_n] \longrightarrow C_k = A_k[X_1, \ldots, X_n]$$
$$X_i \longmapsto l_i$$

and obtain the relations

$$h_i := l_i^t R \in (f_1 \circ l, \ldots, f_n \circ l) \text{ in } C_k (1 \leq i \leq n).$$

The divisibility property (4.) shows then that

$$Ret_k(f_1 \circ l, \ldots, f_n \circ l) \text{ divides } Ret_k(h_1, \ldots, h_n).$$

One has (2., VI.1.g)

$Ret_k(h_1, \ldots, h_n) = R^p Ret_k(l_1, \ldots, l_n)^q$ for some p, q,

$Ret_k(l_1, \ldots, l_n) = Det(l_1, \ldots, l_n) = D$. Since $k' = \mathbb{Z}$, the elements R and D are prime in A_k (not associated : D contains V_{ij} while R does not). We deduce

$$Ret_k(f_1 \circ l, \ldots, f_n \circ l) = \varepsilon\, D^u R^v$$

with $\varepsilon = \pm 1, u, v \in \mathbb{N}$. To determine ε, u, v, we specialize as follows :

$$f_i \mapsto U_i X_i^{d_i}\ ,\ l_i \mapsto V_{ii} X_i$$

($U_i = U_{i\alpha}$ = coefficient of $X_i^{d_i}$ in f_i). It comes then

$$\begin{aligned} &Ret(U_1 V_{11}^{d_1} X_1^{d_1}, \ldots, U_n V_{nn}^{d_n} X_n^{d_n}) = \\ &\varepsilon \big(V_{11} \ldots V_{nn}\big)^u Ret(U_1 X_1^{d_1}, \ldots, U_n X_n^{d_n})^v \end{aligned}$$

Using homogeneity and multiplicativity as above, one obtains

$$\prod_{i=1}^{n} (U_i V_{ii}^{d_i})^{d_1 \ldots d_n / d_i} = \varepsilon (V_{11} \ldots V_{nn})^u \big(\prod_{i=1}^{n} U_i^{d_1 \ldots d_n / d_i}\big)^v.$$

So $\varepsilon = 1, u = d_1 \ldots d_n, v = 1$.

b) Composition formula (FAA DE BRUNO, MERTENS) [F], [ME].
In fact the formula established in a) is a particular case of the following. Consider an integer $d \geq 1$ and polynomials

$$g_i = \sum_{|\alpha|=d} W_{i\alpha} X^\alpha \quad (1 \leq i \leq n),$$

and assume $k = k'[W_{i\alpha} \mid 1 \leq i \leq n, |\alpha| = d]$ (so that $g_1, \ldots, g_n$ are generic over k'). Put $g = (g_1, \ldots, g_n)$ and

$$f_i \circ g = f_i(g_1, \ldots, g_n).$$

Then one has

$$\mathrm{Ret}_k(f_1 \circ g, \ldots, f_n \circ g) = \mathrm{Ret}(g_1, \ldots, g_n)^s \, \mathrm{Ret}_k(f_1, \ldots, f_n)^t$$

with $s = d_1 \ldots d_n$ *and* $t = d^{n-1}$.

Proof : quite similar to that of a). One has only to consider $\mathrm{Ret}(g_1, \ldots, g_n)$ instead of $\mathrm{Ret}(l_1, \ldots, l_n) = \mathrm{Det}(l_1, \ldots, l_n)$ and, at the end, to specialize g_i in the following form : $g_i \longmapsto W_i X_i^d$, where $W_i =$ coefficient of X_i^d in g_i.

6. Weight property. Let m be a fixed integer in $\{1, \ldots, n\}$. To each coefficient $U_{i\alpha}$ of f_i we attach a weight

$$wg(U_{i\alpha}) = \alpha_m \big(\alpha = (\alpha_1, \ldots, \alpha_n), |\alpha| = d_i\big).$$

Then the resultant $Ret_k(f_1, \ldots, f_n) \in A_k = k[U_{i\alpha} \mid 1 \leq i \leq n, |\alpha| = d_i]$ *is isobaric with respect to* wg *and has a weight equal to* $d_1 \ldots d_n$.

Proof.— We can assume that $k = k'[V]$. For simplification, we take $m = n$.

The endomorphism $A_k = k[U_{i\alpha}] \longrightarrow A_k$:

$$U_{i\alpha} \longmapsto V^{\alpha_n} U_{i\alpha}$$

induces another one $\varphi : C_k \longrightarrow C_k$ (where C_k is considered as a $k[X_1, \ldots, X_n]$-algebra). We have to prove that

$$Ret_k\big(\varphi(f_1), \ldots, \varphi(f_n)\big) = V^s Ret_k(f_1, \ldots, f_n)$$

with $s = d_1 \ldots d_n$. But

$$\begin{aligned} \varphi(f_i) = f_i(l_1, \ldots, l_n) \text{ with } l_i &= l_i(X_1, \ldots, X_n) = X_i (i \neq n) \\ l_n &= l_n(X_1, \ldots, X_n) = V X_n. \end{aligned}$$

So the result follows from the invariant property, by specialization, since $Det(l_1, \ldots, l_n) = V$.

7. Covariant property.

Let us assume $d_1 = \ldots = d_n = d$ *and* $k = k'[V_{ij} \mid 1 \leq i, j \leq n]$. *Then the following formula holds :*

$$Ret_k\Big(\sum_1^n V_{1j} f_j, \ldots, \sum_1^n V_{nj} f_j\Big) = \big(Det[V_{ij}]\big)^s Ret_k(f_1, \ldots, f_n),$$

where $s = d^{n-1}$.

Proof.— It suffices to prove the formula for $k' = \mathbb{Z}$. Let $D = Det[V_{ij}]_{1 \leq i,j \leq n}$, and $g_i = \sum_1^n V_{ij} f_j$. In the ring $A_k[D^{-1}]$ we have an equality of ideals

$$(g_1, \ldots, g_n) = (f_1, \ldots, f_n).$$

Applying the divisibility property (4.), we see that there exists a unit λ in $A_k[D^{-1}]$ such that

$$Ret(g_1, \ldots, g_n) = \lambda \, Ret(f_1, \ldots, f_n) \text{ in} A_k \left[D^{-1}\right]$$

(we are over $\mathbb{Z}$, $Ret(f_1, \ldots, f_n)$ is irreducible ... cf. VI.1). Now D is irreducible since D is the resultant of linear generic forms over $\mathbb{Z}$ (Example 2.b) in VI). Hence $\lambda = \pm D^t$, for some $t \geq 0$. Specialize : $f_i \mapsto X_i^{d_i}, V_{ij} \mapsto 0 (i \neq j)$. This implies (2.)

$$\left(V_{11} \ldots V_{nn}\right)^{d^{n-1}} = \pm \left(V_{11} \ldots V_{nn}\right)^t,$$

and we are done.

8. LAPLACE formula.

Assume $n \geq 2$ and take $m \in \{1, \ldots, n-2\}$. Put

$$g_i = f_i(X_1, \ldots, X_m, 0, \ldots, 0) \text{ for } 1 \leq i \leq m,$$
$$g_i = f_i(0, \ldots, 0, X_{m+1}, \ldots, X_n) \text{ for } m+1 \leq i \leq n.$$

Then the following formula holds :

$$Ret(f_1, \ldots, f_m, g_{m+1}, \ldots, g_n) = Ret_k(g_1, \ldots, g_m)^s Ret_k(g_{m+1}, \ldots, g_n)^t$$

with $s = d_{m+1} \ldots d_n, t = d_1 \ldots d_m$.

(In the 1^{st} member $g_{m+1}, \ldots, g_n$ are considered as polynomials in $X_1, \ldots, X_n$, while in the $2^{nd} g_1, \ldots, g_m$ are considered as polynomials in $X_1, \ldots, X_m$ and $g_{m+1}, \ldots, g_n$ in $X_{m+1}, \ldots, X_n$).

This formula generalizes the LAPLACE formula for the determinants.

Proof.— The case $k = \mathbb{Z}$ is enough. Let us put

$$R_1 = Ret(g_1, \ldots, g_m), R_2 = Ret(g_{m+1}, \ldots, g_n).$$

By definition $g_1, \ldots, g_m$ are generic in the variables $X_1, \ldots, X_m$, and $g_{m+1}, \ldots, g_n$ are genric in $X_{m+1}, \ldots, X_n$. There exists an integer $q \geq 1$ such that

$$h_i := X_i^q R_2 \in (g_{m+1}, \ldots, g_n) \text{ for all } i = m+1, \ldots, n$$

(by definition of a T.F., II.4.). Thus we have an inclusion of ideals in $A_{\mathbb{Z}} = \mathbb{Z}[\text{ coeff. of } f_1, \ldots, f_n]$

$$(f_1, \ldots, f_m, h_{m+1}, \ldots, h_n) \subset (f_1, \ldots, f_m, g_{m+1}, \ldots, g_n).$$

The divisibility property (4.) says to us that

$$\begin{aligned} &Ret(f_1, \ldots, f_m, g_{m+1}, \ldots, g_n) \text{ divides} \\ &Ret(f_1, \ldots, f_m, h_{m+1}, \ldots, h_n). \end{aligned}$$

But one has (homogeneity and multiplicativity)

$$Ret(f_1, \ldots, f_m, h_{m+1}, \ldots, h_n) = R_2^u Ret(f_1, \ldots, f_m, X_{m+1}, \ldots, X_n)^v$$

for some integers u, v. Assume for a while that we have shown

$$Ret(f_1, \ldots, f_m, X_{m+1}, \ldots, X_n) = R_1.$$

In $A_{\mathbb{Z}}$ (factorial ring) R_1 and R_2 are non-associated prime elements (since they don't contain the same indeterminates). So we have

$$Ret(f_1, \ldots, f_m, g_{m+1}, \ldots, g_n) = \varepsilon\, R_1^a R_2^b, \varepsilon = \pm 1, a, b \in \mathbb{N}.$$

Taking the degree of both sides w.r.t. the coefficients of f_i, we obtain (VI.1.f)

$$\begin{aligned} d_2 \ldots d_n &= a\, d_2 \ldots d_m \quad \text{if } i = 1, \\ d_1 \ldots d_{n-1} &= b\, d_{m+1} \ldots d_{n-1} \text{ if } i = n. \end{aligned}$$

Thus $a = d_{m+1} \dots d_n$ and $b = d_1 \dots d_m$. Now the usual specialization $f_i \mapsto X_i^{d_i} (1 \leq i \leq n)$ implies $\varepsilon = 1$.

It remains to check the equality assumed true above. By induction, it suffices to prove the following lemma :

9. LEMMA. *Putting $g^\circ = g(X_1, \dots, X_{n-1}, 0)$ for a polynomial $g = g(X_1, \dots, X_n)$, we have*

$$Ret_k(f_1, \dots, f_{n-1}, X_n) = Ret_k(f_1^\circ, \dots, f_{n-1}^\circ)$$

in the ring $L = k[U_{i\alpha} \mid 1 \leq i \leq n-1, |\alpha| = d_i] (n \geq 2)$.

Proof.— It suffices to see it with $k = \mathbb{Z}$ (VI.1.c). Let us put

$$R = Ret_k(f_1, \dots, f_{n-1}, X_n)$$
$$R^\circ = Ret_k(f_1^\circ, \dots, f_{n-1}^\circ).$$

There exists $t \geq 0$ such that

$$X_1^t R \in (f_1, \dots, f_{n-1}, X_n) \subset L[X_1, \dots, X_n],$$

since R is a T.F. with respect to $f_1, \dots, f_{n-1}, X_n$ (by specialization $f_n \longmapsto X_n$ in the case $d_n = 1$). Substitute 0 for X_n and obtain

$$X_1^t R \in (f_1^\circ, \dots, f_{n-1}^\circ) \text{ in } L[X_1, \dots, X_{n-1}]$$

(n is assumed ≥ 2). But $f_1^\circ, \dots, f_{n-1}^\circ$ are *generic* homogeneous polynomials in $X_1, \dots, X_{n-1}$ over k. It follows then that

$$R = \lambda R^\circ, \text{for some } \lambda \in L$$

by II.6 and VI.1.a). Using VI.1.f), we see that, for each $i \in \{1, \dots, n-1\}$, R and R° have the same degree w.r.t. the coefficients of f_i. Hence $\lambda \in k$, and the specialization $f_j \longmapsto X_j^{d_j} (1 \leq j \leq n-1)$ shows that $\lambda = 1$. This completes the proof of the lemma, and hence the LAPLACE formula is established.

We say that $Ret(f_1^\circ, \dots, f_{n-1}^\circ)$ is the "*resultant of $f_1, \dots, f_{n-1}$ at infinity*" $(n \geq 2)$. This definition is justified by the following. Assume that k is an algebraically closed field and that $g_1, \dots, g_{n-1} \in k[X_1, \dots, X_n]$ are specializations of $f_1, \dots, f_{n-1}$. The preceding lemma shows that

$$Ret(g_1, \dots, g_{n-1}, X_n) = Ret(g_1^\circ, \dots, g_{n-1}^\circ).$$

A common zero $x = (x_1, \dots, x_n) \in P_k^{n-1}$ of the equations $g_1 = 0, \dots, g_n = 0$ (with $g_n = X_n$) is necessarily at infinity in P_k^{n-1}. Therefore the polynomials $g_1, \dots, g_{n-1}$ have a common zero at infinity in P_k^{n-1} if and only if $Ret(g_1^\circ, \dots, g_{n-1}^\circ) = 0$ (see II.8.).

REFERENCES

[B] **BOURBAKI, N.** Algèbre, Chapitre 10. (Masson, 1980).

[F] **FAA DE BRUNO.** L'élimination (1859).

[G] **GRÖBNER, W.** Moderne algebraische Geometrie (Springer, Wien 1949).

[H] **HURWITZ, A.** Über die Trägheitsformen eines algebraischen Moduls, Annali di Math. pura ed applicata (3) 20, (1913) 113-151.

[J1] **JOUANOLOU, J.-P.** Le formalisme du résultant, Adv. in Math. Vol. 90, N°2 (1991) 117-263.

[J2] **JOUANOLOU, J.-P.** Idéaux résultants, Adv. in Math. Vol. 37, N°3 (1980) 212-238.

[MA] **MACAULAY, F.-S.** Some formulas in elimination, Proc. London Math. Soc. (1) 35 (1903) 3-27.

[ME] **MERTENS, F.** Über die bestimmenden Eigenschaften der Resultante von n-Formen mit n Veränderlichen, Sitzungsberichte der Wiener Akademie 93 (1886) 527-566.

[EGA] **GROTHENDIECK, A. - DIEUDONNÉ, J.** Éléments de géométrie algébrique, Publ. Math. I.H.E.S. 4 (1960), 8 (1961)...

[EGAI] **GROTHENDIECK, A. - DIEUDONNÉ, J.** Éléments de géométrie algébrique I (Springer- Verlag, 1971).

[RB] **MUMFORD, D.** The *red book* of varieties and schemes, Lect. Notes in Math. 1358 (Springer-Verlag, 1988).

[YB] **HARTSHORNE, R.** Algebraic geometry (Springer-Verlag, 1977).

[W] **VAN DER WAERDEN, B.L.** Modern algebra (Unger Publishing, 1949).

NOTA BENE

Pour des raisons de santé (de l'auteur), et des problèmes de frappe (du manuscrit), le texte présent n'a pu voir le jour plus tôt. Cependant, la version manuscrite a connu une diffusion certaine, dès l'automne 1992. Je voudrais remercier vivement Madame Pilar MEYER qui vient d'en assurer l'excellent traitement (de texte !).

Strasbourg, le 3 juin 1997

Abd'allah AL AMRANI.