L'Enseignement Mathématique (2) 58 (2012), 333–373

RÉSULTANT, DISCRIMINANT

par Michel DEMAZURE

A Jean-Pierre Serre, pour son 86-ième anniversaire.

INTRODUCTION

Dans le courant des années 1960, Bourbaki avait décidé de reprendre la première partie de son Traité pour en produire une édition définitive. L'idée avait été avancée d'en profiter pour adjoindre au chapitre IV (*Polynômes et Fractions Rationnelles*) du livre d'*Algèbre* ([Bou07b]) un appendice introduisant résultants et discriminants. C'est ainsi qu'à son « congrès » de juillet 1969, Bourbaki a discuté d'une proposition pour cet appendice (« rédaction n° 538 »). Il a été alors conclu à l'abandon du projet, en grande partie pour un problème de plan : les énoncés nécessaires sur les polynômes à plusieurs variables, comme le lemme de Gauss, bien qu'élémentaires, relèvent « naturellement » de la notion d'anneau factoriel, qui n'apparaît dans le traité qu'au chapitre VII de l'*Algèbre Commutative* ([Bou06b]).

Plusieurs articles et ouvrages sont parus depuis, qui développent cette théorie dans un cadre plus avancé, marqué notamment par l'utilisation de méthodes homologiques[1]). Il n'en demeure pas moins qu'une approche élémentaire reste utile, d'autant qu'elle permet d'obtenir à moindre coût le critère de lissité dont nous parlerons ci-dessous.

Cet article reprend la rédaction 538, avec quelques modifications et l'adjonction de deux appendices. J'ai conservé le style bourbachique, le

[1]) On pourra consulter le traité [GKZ08] de I. M. GELFAND, M. M. KAPRANOV et A. V. ZELEVINSKY et les articles [Jou80], [Jou91] et [Jou97] de J.-P. JOUANOLOU.

système de référence canonique du Traité et le « positionnement » de la rédaction 538 : le texte se place après les chapitres IV et V d'Algèbre ([Bou07b]) et n'utilise de la partie postérieure que les résultats de base sur les anneaux factoriels (rappelés dans l'appendice 1) et le théorème des zéros (démontré dans l'appendice 2).

Venons-en au *critère de lissité* pour les hypersurfaces de l'espace projectif.

Fixons deux entiers $n \geqslant 1$ et $d \geqslant 2$. Pour tout anneau k, notons $\mathcal{P}(k)$ le k-module formé des polynômes en n indéterminées (notées $X_1, \ldots, X_n$), à coefficients dans k, qui sont homogènes de degré d. On pose $\mathcal{P} = \mathcal{P}(\mathbf{Z})$ et on a naturellement un isomorphisme $k \otimes \mathcal{P} = \mathcal{P}(k)$.

Le $\mathbf{Z}$-module $\mathcal{P}$ est libre de base la famille des monômes $\mathbf{X}^{\boldsymbol{\alpha}}$, où $\boldsymbol{\alpha}$ parcourt l'ensemble des multi-indices $\boldsymbol{\alpha} = (\alpha_i) \in \mathbf{N}^n$ tels que $\alpha_1 + \cdots + \alpha_n = d$. On note $T_{\boldsymbol{\alpha}}$ les éléments de la base duale, chaque $T_{\boldsymbol{\alpha}}$ associant à $p \in \mathcal{P}$ le coefficient de $\mathbf{X}^{\boldsymbol{\alpha}}$ dans p. On note $U_{n,d}$ l'anneau des fonctions polynomiales sur $\mathcal{P}$, qui s'identifie à la $\mathbf{Z}$-algèbre des polynômes en les indéterminées $T_{\boldsymbol{\alpha}}$. Nous noterons $P_{n,d}$ le polynôme à coefficients dans $U_{n,d}$ donné par

$$P_{n,d}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\alpha}} T_{\boldsymbol{\alpha}} \mathbf{X}^{\boldsymbol{\alpha}}.$$

C'est le polynôme *universel*. À tout anneau A et tout polynôme $f \in \mathcal{P}(A)$, on associe l'homomorphisme $h_f : U_{n,d} \to A$ qui applique le coefficient $T_{\boldsymbol{\alpha}}$ de $P_{n,d}$ sur le coefficient de $X^{\boldsymbol{\alpha}}$ dans f. Pour tout $u \in U_{n,d}$, l'élément $h_f(u)$ de A n'est autre que l'image de f par l'application polynomiale $1_A \otimes u : \mathcal{P}(A) \to A$. On posera donc $h_f(u) = u(f)$. Par définition $u = u(P_{n,d})$.

Le *discriminant divisé universel* $\mathrm{disc} = \mathrm{disc}(P_{n,d})$ est un élément de $U_{n,d}$ jouissant notamment des trois propriétés suivantes.

a) Comme application polynomiale $\mathcal{P} \to \mathbf{Z}$, il est de degré $n(d-1)^{n-1}$ (n° 5, prop. 11, c)).

b) C'est un élément premier (appendice 1) de l'anneau $U_{n,d}$ (cor. 1 à la prop. 14 du n° 6) : il est irréductible comme polynôme de $\mathbf{Q} \otimes U_{n,d}$ (il l'est même comme polynôme de $\overline{\mathbf{Q}} \otimes U_{n,d}$) et n'est divisible par aucun entier > 1.

c) Pour tout corps algébriquement clos k et tout polynôme $f \in \mathcal{P}(k)$, les conditions suivantes sont équivalentes (n° 5, prop. 12) :

   (i) f et ses n dérivées partielles n'ont que l'origine comme zéro commun dans k^n ;

   (ii) $\mathrm{disc}(f)$ n'est pas nul.

De la propriété c) et du critère jacobien, on tire le *critère de lissité* suivant.

Soit S un schéma, notons $\mathcal{O}(S)$ l'anneau de ses fonctions globales, soit $f \in \mathcal{P}(\mathcal{O}(S))$ et soit $\mathrm{disc}(f) \in \mathcal{O}(S)$ *son discriminant. Considérons l'espace projectif $\mathbf{P}_S^{n-1}$ de dimension $n-1$ au-dessus de S, soit H le sous-schéma fermé d'équation $f = 0$ et soit s un point de S de corps résiduel $\kappa(s)$. Alors les conditions suivantes sont équivalentes :*

(i) *l'image f_s de f dans $\mathcal{P}(\kappa(s))$ est non nulle (ce qui signifie que la fibre H_s n'est pas l'espace entier) et H est lisse sur S en tous les points de H_s ;*

(ii) *L'élément* $\mathrm{disc}(f)(s)$ *du corps résiduel $\kappa(s)$ n'est pas nul.*

Notons que la version du critère jacobien utilisée ici est très simple. Par exemple, si x est un point de H et si $D_i f(x)$ est non nul dans le corps résiduel, alors la projection de H sur l'hyperplan de coordonnées $X_i = 0$ est étale en x, donc H est lisse sur S en x.

Cela étant, considérons la situation universelle, où l'on prend $S = \mathrm{Spec}(U_{n,d})$ et $f = P_{n,d}$. Notons Δ la partie de l'ensemble sous-jacent à S formée des $s \in S$ ne satisfaisant pas à la condition de lissité (i) ci-dessus. Le critère de lissité implique que Δ est décrite par l'équation $\mathrm{disc} = 0$. La conjonction des propriétés b) et c) signifie que Δ est le support d'un diviseur irréductible dont le discriminant divisé universel est une équation, ce qui le détermine au signe près, car 1 et -1 sont les seuls éléments inversibles de $U_{n,d}$.

Considérons maintenant l'anneau des fonctions de ce diviseur, c'est-à-dire le quotient de l'anneau $U_{n,d}$ par l'idéal principal engendré par l'élément disc. Il est intègre, notons k une clôture algébrique de son corps des fractions et soit $f \in \mathcal{P}(k)$ l'image canonique de $P_{n,d}$. Alors $\mathrm{disc}(f) = 0$, de sorte que les dérivées partielles $D_1 f, \ldots, D_n f$ ont d'après c) un zéro commun non trivial dans k^n. Mais cela implique que leur résultant $\mathrm{res}(D_1 f, \ldots, D_n f)$ est nul. Autrement dit, le résultant $\mathrm{disc}_r = \mathrm{res}(D_1 P_{n,d}, \ldots, D_n P_{n,d})$ est multiple de disc dans l'anneau $U_{n,d}$. Comme ces deux polynômes ont le même degré d'après a), le discriminant divisé universel *s'obtient en divisant le résultant* disc_r *par un contenu* (pgcd des coefficients, défini au signe près). Le lemme 11(n° 5) explicite ce contenu [2]).

La terminologie mérite un commentaire. La définition « classique » du discriminant (en caractéristique zéro) est le résultant disc_r des dérivées

[2]) qu'on trouve aussi dans [GKZ08], chap. 13, § 1.D.

partielles. L'approche par la théorie de l'élimination amène naturellement, comme on vient de le voir, au choix disc ci-dessus. La question du signe n'est pas tranchée. Le choix fait ici est de garder le signe de disc_r, c'est-à-dire de définir disc comme le quotient de disc_r par son contenu positif. Dans l'article [Sai] à paraître, T. SAITO introduit dans le cas où n est pair[3]), un « discriminant signé » $\epsilon(n,d)\,\mathrm{disc}$, avec $\epsilon(n,d) = (-1)^{(d-1)/2}$ si d est impair et $\epsilon(n,d) = (-1)^{d/2.n/2}$ si d est pair. Pour $d = 2$, on retrouve la valeur $(-1)^{n/2}\,\mathrm{disc} = (-1)^{n/2}\,\mathrm{disc}_r$ usuelle pour les formes quadratiques; pour $n = 2$, on retrouve le discriminant usuel des polynômes à une indéterminée (voir n° 5, exemple 5).

On démontre que le discriminant divisé universel est absolument irréductible en caractéristique 0, la démonstration restant valable en caractéristique p pour les « bons » p (n° 6, prop. 14). Le fait que cela reste vrai pour tout p, sauf lorsque $p = 2$ et que n est pair, n'est pas traité. Pour le faire par la méthode élémentaire suivie ici pour les « bons » p (cor. à la prop. 13 du n° 5), il faudrait exhiber des exemples adéquats. Pour une démonstration de ce fait et pour la situation exacte dans le cas exceptionnel, voir la proposition 2.5 and le théorème 4.1 de l'article [Sai] déjà cité.

Je terminerai cette introduction par un commentaire plus personnel.

Le cadre historique naturel de la Géométrie algébrique est celui des polynômes. Le développement de l'Algèbre moderne, commencé il y a près d'un siècle, a renvoyé les anneaux de polynômes au statut de cas particulier et les méthodes propres aux polynômes, comme la *Théorie de l'élimination*, au conservatoire. Mais « les objets sont têtus » et les méthodes explicites ne cessent de ressurgir. Un calcul est toujours plus général que le cadre théorique dans lequel on l'enferme à une période donnée. La résolution de l'équation du second degré, provenant des tablettes babyloniennes (et introduisant le premier discriminant de l'Histoire), reparaît dans la décomposition en carrés des formes quadratiques, dans la méthode des moindres carrés de Legendre-Gauss, dans l'orthonormalisation de Gram-Schmidt...

Au fameux « *Il faut éliminer la théorie de l'élimination* » de Dieudonné, Abhyankar avait répondu par un poème qui commençait par « *Eliminate, Eliminate, Eliminate / Eliminate the Eliminators of Elimination Theory* ». La décision de Bourbaki sur la rédaction 538 était « *Il est décidé que cette rédaction ira en appendice à AC XII, donc au frigidaire en attendant* ». L'en voilà sortie...

[3]) Dans cet article, le nombre de variables désigné par n dans notre texte est noté $n+2$, la lettre n y désignant la dimension de l'hypersurface H.

REMERCIEMENTS. Je remercie vivement N. Bourbaki qui m'a autorisé à utiliser ma rédaction originelle comme base de ce texte. C'est à l'insistance amicale de Jean-Pierre Serre qu'on doit cette exhumation et j'ai plaisir à lui dédier ce texte. Je remercie Pierre Cartier, Takeshi Saito, Jean-Pierre Serre et le referee pour leur relecture attentive et leurs suggestions d'améliorations.

1. THÉORÈME DE L'ÉLIMINATION

Dans la suite, tous les anneaux sont supposés commutatifs. Si k est un corps (commutatif), on appelle extension *de k une k-algèbre qui est un corps (commutatif).*

Nous utiliserons la notation suivante : si $h\colon A \to B$ est un homomorphisme d'anneaux, et si P est un élément de $A[X_1, \dots, X_n]$, nous noterons ${}^hP$ l'élément de $B[X_1, \dots, X_n]$ image de P par l'extension canonique de h aux anneaux de polynômes considérés.

LEMME 1. *Soient A un anneau, M un A-module de type fini, $\mathfrak{a} \subset A$ l'annulateur de M et $h\colon A \to k$ un homomorphisme de A dans un corps k. Pour que $M \otimes_A k \neq 0$, il faut et il suffit que $h(\mathfrak{a}) = 0$.*

Démonstration. Comme tout élément de $h(\mathfrak{a})$ annule le k-espace vectoriel $M \otimes_A k$, la condition est évidemment nécessaire. Inversement, supposons que $M \otimes_A k = 0$ et prouvons que $h(\mathfrak{a}) \neq 0$. Soient $(m_j)_{j=1,\dots,p}$ une famille génératrice finie de M, $f\colon A^p \to M$ l'homomorphisme de A-modules tel que $f((a_j)) = \sum a_j m_j$, N le noyau de f et $g\colon N \to A^p$ l'injection canonique. D'après [Bou07a], A, II, p. 58, prop. 5, on a une suite exacte de k-espaces vectoriels

$$N \otimes_A k \xrightarrow{g\otimes 1_k} k^p \xrightarrow{f\otimes 1_k} M \otimes_A k \to 0\,,$$

de sorte que $g \otimes 1_k$ est surjectif, ce qui signifie que les éléments $g(n) \otimes 1$, $n \in N$, engendrent le k-espace vectoriel k^p. D'après le théorème d'échange ([Bou07a], A, II, p. 95, th. 2), il existe donc $n_1, \dots, n_p \in N$ tels que la famille $(g(n_i) \otimes 1)_{i=1,\dots,p}$ soit une base de k^p. Si (e_j) est la base canonique de A^p et si $n_i = \sum_j a_{ij} e_j$, où $(a_{ij}) \in M_p(A)$, on a $g(n_i) \otimes 1 = \sum_j a_{ij} e_j \otimes 1 = \sum_j h(a_{ij}) e_j$, ce qui montre que la matrice $(h(a_{ij}))$ est inversible. Posons $d = \det(a_{ij}) \in A$; on a $h(d) = \det(h(a_{ij})) \neq 0$; d'autre part les formules de Cramer ([Bou07a], A, III, p. 102, formule (37)) entraînent que les vecteurs de_i sont des combinaisons linéaires des n_j, de sorte que $dA^p \subset N$, ou encore $d \in \mathfrak{a}$. On a donc bien $h(\mathfrak{a}) \neq 0$, ce qu'il fallait démontrer.

LEMME 2. *Soit E un anneau gradué de type $\mathbf{N}$. Pour $m \in \mathbf{N}$, notons E_m l'ensemble des éléments homogènes de degré m de E. Soient $a \in E_0$ et $\xi \in E_1$. Pour que a appartienne à $(1-\xi)E$, il faut et il suffit qu'il existe $m \in \mathbf{N}$ avec $a\xi^m = 0$.*

Démonstration. Soit $u = u_0 + \cdots + u_n$ un élément de E, avec $u_i \in E_i$ pour tout i. La relation $a = (1-\xi)u$ se décompose en relations homogènes $u_0 = a,\ u_1 = u_0\xi,\ \ldots,\ u_n = u_{n-1}\xi,\ u_n\xi = 0$. Cela s'écrit aussi $u_i = a\xi^i$ pour $i = 0, \ldots, n$ et $a\xi^{n+1} = 0$.

PROPOSITION 1. *Soit E un anneau gradué de type $\mathbf{N}$. Pour $m \in \mathbf{N}$, notons E_m l'ensemble des éléments homogènes de degré m de E et $\mathfrak{a}_m \subset E_0$ l'annulateur du E_0-module E_m. Supposons que le E_0-module E_1 soit de type fini et que l'anneau E soit engendré par $E_0 \cup E_1$. Notons $\mathfrak{a}$ la réunion des $\mathfrak{a}_m$. Alors $\mathfrak{a}$ est un idéal de E_0. Soit h un homomorphisme de E_0 dans un corps k. Les conditions suivantes sont équivalentes :*

(i) *On a $h(\mathfrak{a}) = 0$.*

(ii) *Il existe un corps K et des homomorphismes $f: E \to K$ et $i: k \to K$ tels que $i \circ h = f|E_0$ et $f(E_1) \neq 0$.*

Démonstration. L'homomorphisme canonique de E_0-algèbres de l'algèbre symétrique $S_{E_0}(E_1)$ dans E est surjectif. Si le E_0-module E_1 est engendré par $x_1, \ldots, x_q$ et si $n \in \mathbf{N}$, alors E_n est engendré par les $x_1^{n_1} \cdots x_q^{n_q}$ avec $\sum n_i = n$. On en déduit aussitôt les trois assertions suivantes :

1) L'homomorphisme $E_1 \otimes_{E_0} E_m \to E_{m+1}$ déduit de la multiplication de E est surjectif.
2) Pour tout $m \in \mathbf{N}$, le E_0-module E_m est de type fini.
3) Si $m \in \mathbf{N}$ est tel que $x_i^m = 0$ pour $i = 1, \ldots, q$, alors $E_n = 0$ pour $n > q(m-1)$.

D'après 1) ci-dessus, on a $\mathfrak{a}_m \subset \mathfrak{a}_{m+1}$ pour $m \in \mathbf{N}$, de sorte que $\mathfrak{a}$ est bien un idéal de E_0. Démontrons l'équivalence des conditions (i) et (ii) de l'énoncé.

(ii) $\Rightarrow$ (i) : avec les notations de (ii), soit $\xi \in E_1$ tels que $f(\xi) \neq 0$. Pour $n \in \mathbf{N}$ et $a \in \mathfrak{a}_n$, on a $a\xi^n = 0$, donc $i(h(a))f(\xi)^n = 0$, donc $h(a) = 0$ puisque K est un corps et que i est injectif.

(i) $\Rightarrow$ (ii) : supposons que $h(\mathfrak{a}_m) = 0$ pour tout m. D'après 2) ci-dessus et le lemme 1, on a $E_m \otimes_{E_0} k \neq 0$ pour tout m. Appliquant 3) ci-dessus à l'anneau gradué $F = E \otimes_{E_0} k$, on en conclut qu'il existe $\xi \in F_1$ tel que $\xi^m \neq 0$ pour tout m. Il résulte alors du lemme 2, appliqué avec $a = 1$, que $1_F - \xi$ n'est pas inversible dans F. L'idéal $(1_F - \xi)F$ est donc distinct

de F. Appliquant [Bou07a], A, I, p. 99, th. 1, on en déduit qu'il existe un idéal maximal $\mathfrak{m}$ de F contenant $1_F - \xi$. Soient K le corps $F/\mathfrak{m}$ et $p\colon F \to K$ la projection canonique; on a $p(\xi) = 1_K$. Notons $f\colon E \to K$ et $i\colon k \to K$ les homomorphismes définis par $f(x) = p(x \otimes 1_k)$ et $i(y) = p(1_E \otimes y)$. Alors $i(h(x)) = p(1_E \otimes h(x)) = p(x \otimes 1_k) = f(x)$, de sorte qu'on a bien $i \circ h = f|E_0$. Par ailleurs, écrivant $\xi = \sum x_j \otimes y_j$, avec $x_j \in E_1$ et $y_j \in k$, on a $1_K = p(\xi) = \sum f(x_j)i(y_j)$, ce qui implique $f(E_1) \neq 0$ et achève la démonstration.

REMARQUE. L'extension K de k construite dans la démonstration précédente est une k-algèbre de type fini, donc est de degré fini sur k (appendice 2). La condition (ii) est donc équivalente à celle qu'on obtient en y ajoutant que K est de degré fini sur k.

Soient A un anneau et I un idéal de l'anneau de polynômes $A[X_1, \ldots, X_n]$. Si $h\colon A \to B$ est un homomorphisme de A dans un anneau B, on appelle *zéro de I dans B^n* un élément (b_i) de B^n tel que ${}^hP(b_1, \ldots, b_n) = 0$ pour tout $P \in I$. Si I est engendré par les polynômes P_j, $j \in J$, on dit aussi que (b_i) est un *zéro commun aux P_j dans B^n*. Par exemple, si I est gradué et si $h(I \cap A) = 0$, il est clair que l'élément $(0) \in B^n$ est un zéro de I; on l'appelle le *zéro trivial*.

DÉFINITION 1. Soient A un anneau et I un idéal gradué de l'anneau des polynômes $A[X_1, \ldots, X_n]$. On appelle *idéal éliminant* de I et on note $\mathfrak{e}(I)$ l'idéal de A formé des a tels qu'il existe $m \in \mathbf{N}$ avec $aX_i^m \in I$ pour $i = 1, \ldots, n$.

Soit $h\colon A \to B$ un homomorphisme d'anneaux et soit J l'idéal de $B[X_1, \ldots, X_n]$ engendré par les polynômes ${}^hP$, où P parcourt I. Alors h applique $\mathfrak{e}(I)$ dans $\mathfrak{e}(J)$.

PROPOSITION 2 (THÉORÈME DE L'ÉLIMINATION). *Soient A un anneau, I un idéal gradué de l'anneau des polynômes $A[X_1, \ldots, X_n]$ et $\rho\colon A \to k$ un homomorphisme de A dans un corps k. Les conditions suivantes sont équivalentes :*

(i) *On a $\rho(\mathfrak{e}(I)) = 0$.*

(ii) *Il existe une extension K de k et un zéro non trivial de I dans K^n.*

(ii bis) *Il existe une extension K de k, de degré fini, et un zéro non trivial de I dans K^n.*

(iii) *Une extension algébriquement close L de k étant donnée, il existe un zéro non trivial de I dans L^n.*

Démonstration.

(ii bis) $\Rightarrow$ (iii) $\Rightarrow$ (ii) : c'est clair.

(ii) $\Rightarrow$ (i) : soit $(\xi_i) \in K^n$ un zéro non trivial de I et soit $a \in \mathfrak{e}(I)$. On a, pour tout i et pour $m \in \mathbf{N}$ assez grand, $aX_i^m \in I$, donc $\rho(a)\xi_i^m = 0$, d'où enfin $\rho(a) = 0$.

(i) $\Rightarrow$ (ii bis) : supposons que $\rho(\mathfrak{e}(I)) = 0$ et considérons l'anneau gradué $E = A[X_1, \ldots, X_n]/I$. On a $I \cap A \subset \mathfrak{e}(I)$, donc $\rho(I \cap A) = 0$. Comme $E_0 = A/(I \cap A)$, ρ se factorise par un homomorphisme $h: E_0 \to k$. D'autre part, l'annulateur $\mathfrak{a}_m$ du E_0-module E_m est l'image dans E_0 de l'ensemble des $a \in A$ tels que aP appartienne à I pour tout polynôme homogène P de degré m ; comme ce dernier ensemble est contenu dans $\mathfrak{e}(I)$, on a $h(\mathfrak{a}_m) \subset \rho(\mathfrak{e}(I)) = 0$. On peut donc appliquer à l'anneau E et à l'homomorphisme $h: E_0 \to k$ la proposition 1 et la remarque qui la suit, et il existe une extension K de k, de degré fini, et un homomorphisme $f: E \to K$ prolongeant h tel que $f(E_1) \neq 0$. L'homomorphisme composé $A[X_1, \ldots, X_n] \to E \to K$ est de la forme $P \mapsto P((\xi_i))$ où $(\xi_i) \in K^n$ est un zéro de I et où les ξ_i ne sont pas tous nuls, ce qui démontre (ii bis).

2. Polynômes homogènes universels

Soient $n \geqslant 1$ et $d \geqslant 0$ deux entiers. On note $U_{n,d}$ la $\mathbf{Z}$-algèbre de polynômes en les indéterminées $T_{\boldsymbol{\alpha}}$, où $\boldsymbol{\alpha}$ parcourt l'ensemble des multi-indices $\boldsymbol{\alpha} \in \mathbf{N}^n$ tels que $\alpha_1 + \cdots + \alpha_n = d$, et on pose

$$P_{n,d}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\alpha}} T_{\boldsymbol{\alpha}} \mathbf{X}^{\boldsymbol{\alpha}}.$$

Alors $P_{n,d}$ est un polynôme homogène de degré d en les indéterminées $X_1, \ldots, X_n$ à coefficients dans $U_{n,d}$.

Exemple 1. Pour $d = 0$, on a $U_{n,0} = \mathbf{Z}[T]$ et $P_{n,0}(X_1, \ldots, X_n) = T$.

Exemple 2. Pour $d = 1$, on a $U_{n,1} = \mathbf{Z}[T_1, \ldots, T_n]$ et $P_{n,1}(X_1, \ldots, X_n) = T_1X_1 + \cdots + T_nX_n$.

Exemple 3. Pour $d = 2$, on a $U_{n,2} = \mathbf{Z}[(T_S)]$, où S parcourt l'ensemble des parties de $[1, n]$ à 1 ou 2 éléments et

$$P_{n,2}(X_1, \ldots, X_n) = \sum_i T_{\{i\}} X_i^2 + \sum_{\{i,j\}} T_{\{i,j\}} X_i X_j,$$

où la seconde somme est étendue aux *sous-ensembles* de $[1, n]$ à deux éléments.

Soit A un anneau et soit f un polynôme homogène de degré d en les indéterminées $X_1, \dots, X_n$ et à coefficients dans A. Il existe un homomorphisme d'anneaux $h\colon U_{n,d} \to A$ et un seul tel que $f = {}^hP_{n,d}$. On le note h_f. Par construction, pour tout élément $u = u((T_{\boldsymbol{\alpha}})) \in U_{n,d}$, l'élément $h_f(u)$ de A s'obtient en substituant à chaque variable $T_{\boldsymbol{\alpha}}$ de u le coefficient de $\mathbf{X}^{\boldsymbol{\alpha}}$ dans le polynôme f. On dira aussi que $h_f(u)$ s'obtient *en substituant à* $P_{n,d} \in U_{n,d}[X_1, \dots, X_n]$ *le polynôme* $f \in A[X_1, \dots, X_n]$. On notera $\tilde{u}(f)$ l'élément $h_f(u)$ de A. On a ainsi par exemple $\tilde{u}(P_{n,d}) = u$.

En vertu de ce qui précède, on dira que $P_{n,d}$ est *le polynôme homogène universel* (relativement aux indéterminées $X_1, \dots, X_n$ et au degré d fixés).

Considérons maintenant un entier $r > 0$ et une suite $\mathbf{d} = (d_1, \dots, d_r) \in \mathbf{N}^r$. On notera $U_{n;\mathbf{d}}$ le produit tensoriel des $\mathbf{Z}$-algèbres U_{n,d_j}, qui s'identifie à la $\mathbf{Z}$-algèbre de polynômes en les indéterminées $T_{\boldsymbol{\alpha},j}$, où j parcourt l'intervalle $[1, r]$ et où, pour chaque j, $\boldsymbol{\alpha}$ parcourt l'ensemble des multi-indices $\boldsymbol{\alpha} \in \mathbf{N}^n$ tels que $\alpha_1 + \cdots + \alpha_n = d_j$.

Pour $j = 1, \dots, r$, notons $P_j \in U_{n;\mathbf{d}}[X_1, \dots, X_n]$ le polynôme ${}^{h_j}P_{n,d_j}$, où h_j est l'injection canonique du j-ème facteur U_{n,d_j} dans $U_{n;\mathbf{d}}$. C'est un polynôme homogène de degré d_j :

$$P_j(X_1, \dots, X_n) = \sum_{\boldsymbol{\alpha}} T_{\boldsymbol{\alpha},j}\mathbf{X}^{\boldsymbol{\alpha}}, \qquad j \in [1, r]\,.$$

Soit A un anneau et soit $\mathbf{f} = (f_1, \dots, f_r)$ une famille de polynômes homogènes de degrés respectifs $d_1, \dots, d_r$ en les indéterminées $X_1, \dots, X_n$ et à coefficients dans A. Il existe un homomorphisme d'anneaux $h\colon U_{n;\mathbf{d}} \to A$ et un seul tel que $f_j = {}^hP_j$ pour $j = 1, \dots r$. On le note $h_{\mathbf{f}}$. Comme dans le cas précédent d'une famille $\mathbf{d}$ réduite à un élément, pour tout élément $u = u((T_{\boldsymbol{\alpha},j})) \in U_{n;\mathbf{d}}$, l'élément $h_{\mathbf{f}}(u)$ de A s'obtient en substituant à chaque variable $T_{\boldsymbol{\alpha},j}$ de u le coefficient de $\mathbf{X}^{\boldsymbol{\alpha}}$ dans le polynôme f_j. On dira aussi que $h_{\mathbf{f}}(u)$ s'obtient *en substituant à chaque polynôme* P_j *de* $U_{n;\mathbf{d}}[X_1, \dots, X_n]$ *le polynôme* f_j *de* $A[X_1, \dots, X_n]$. On notera $\tilde{u}(f_1, \dots, f_r)$ l'élément $h_{\mathbf{f}}(u)$ de A. On a ainsi par exemple $\tilde{u}(P_1, \dots, P_r) = u$.

On dira que (P_j) est *la famille universelle de polynômes homogènes* et que $U_{n;\mathbf{d}}$ est *l'anneau universel de coefficients*, ou simplement l'anneau universel (relativement aux indéterminées $X_1, \dots, X_n$ et à la suite de degrés $d_1, \dots, d_r$ fixés).

EXEMPLE 4. Prenons tous les d_j égaux à 1. Alors $U_{n;\mathbf{d}}$ est l'algèbre de polynômes $\mathbf{Z}[T_{ij}]_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant r}$, avec $P_j = \sum_i T_{ij}X_i$. Le produit $P_1 \cdots P_r$ est homogène de degré r, d'où l'on déduit un homomorphisme d'anneaux $h\colon U_{n,r} \to U_{n;\mathbf{d}}$ tel que ${}^hP_{n,r} = P_1 \cdots P_r$. Le groupe symétrique $\mathfrak{S}_r$ opère dans

le produit tensoriel $U_{n;\mathbf{d}}$ par permutation des facteurs (on a donc $\sigma(T_{ij}) = T_{i\sigma(j)}$ pour $\sigma \in \mathfrak{S}_r$) et il est clair que l'image de h est formée de tenseurs symétriques.

3. Idéal résultant de r polynômes homogènes à n indéterminées

Dans ce numéro, nous fixons des entiers $n > 0$ et $r > 0$ et un élément $\mathbf{d} = (d_1, \ldots, d_r)$ de $\mathbf{N}^r$ tel que $d_j > 0$ pour $j = 1, \ldots, r$.

Considérons l'anneau universel de coefficients $U_{n;\mathbf{d}}$ et la famille universelle de polynômes $(P_1, \ldots, P_r)$ introduits au numéro précédent. Chaque P_j est un polynôme homogène de degré d_j en les indéterminées $X_1, \ldots, X_n$ à coefficients dans $U_{n;\mathbf{d}}$. On notera $I_{n;\mathbf{d}}$ l'idéal (gradué) de $U_{n;\mathbf{d}}[X_1, \ldots, X_n]$ engendré par les P_j et $\mathfrak{e}_{n;\mathbf{d}} = \mathfrak{e}(I_{n;\mathbf{d}}) \subset U_{n;\mathbf{d}}$ son idéal éliminant (n° 1, déf. 1).

Soit A un anneau et soit $\mathbf{f} = (f_1, \ldots, f_r)$ une famille de polynômes homogènes de degrés respectifs $d_1, \ldots, d_r$ en les indéterminées $X_1, \ldots, X_n$ et à coefficients dans A. Considérons l'homomorphisme $u \mapsto \tilde{u}(f_1, \ldots, f_r)$ de $U_{n;\mathbf{d}}$ dans A.

Définition 2. On appelle *idéal résultant* de la famille $(f_1, \ldots, f_r)$ et on note $R(f_1, \ldots, f_r)$ l'idéal de A engendré par les $\tilde{u}(f_1, \ldots, f_r)$, où u parcourt l'idéal $\mathfrak{e}_{n;\mathbf{d}}$ de $U_{n;\mathbf{d}}$.

Par exemple, $\mathfrak{e}_{n;\mathbf{d}}$ est l'idéal résultant $R(P_1, \ldots, P_r)$ de la famille universelle. On l'appellera *l'idéal résultant universel.*

Soient B un anneau et $g : A \to B$ un homomorphisme d'anneaux. Posons ${}^g\mathbf{f} = ({}^gf_1, \ldots, {}^gf_r)$. On a aussitôt $h_{{}^g\mathbf{f}} = g \circ h_{\mathbf{f}}$, donc

$$g(\tilde{u}(f_1, \ldots, f_r)) = \tilde{u}({}^gf_1, \ldots, {}^gf_r), \quad u \in U_{n;\mathbf{d}}.$$

En particulier, $R({}^gf_1, \ldots, {}^gf_r)$ est l'idéal de B engendré par $g(R(f_1, \ldots, f_r))$.

D'après la proposition 2 du n° 1, on a :

Scholie. *Soit A un anneau et, pour $j = 1, \ldots, r$, soit $f_j \in A[X_1, \ldots, X_n]$ un polynôme homogène de degré d_j. Notons I l'idéal de $A[X_1, \ldots, X_n]$ engendré par les f_j, soit $\mathfrak{e}(I) \subset A$ l'idéal éliminant de I, et soit $\rho : A \to k$ un homomorphisme de A dans un corps k. Les conditions suivantes sont équivalentes :*

(i) *On a $\rho(R(f_1, \ldots, f_r)) = 0$.*

(ii) *On a $\rho(\mathfrak{e}(I)) = 0$.*

(iii) *Il existe une extension K de k telle que les f_j aient un zéro commun non trivial dans K^n.*

(iii bis) *Il existe une extension K de k, de degré fini, telle que les f_j aient un zéro commun non trivial dans K^n.*

(iii ter) *Une extension algébriquement close L de k étant donnée, il existe un zéro commun non trivial des f_j dans L^n.*

REMARQUE 1. Notons $\mathfrak{r}$ l'idéal résultant $R(f_1,\dots,f_r)$. On a $\mathfrak{r} \subset \mathfrak{e}(I)$ et, en vertu de l'équivalence de (i) et (ii), tout idéal premier de A contenant $\mathfrak{r}$ contient $\mathfrak{e}(I)$. Ainsi, on a $\mathfrak{e}(I) = \mathfrak{r}$ lorsque $\mathfrak{r}$ est premier. * Plus généralement, $\mathfrak{e}(I)$ est compris entre $\mathfrak{r}$ et sa racine ([Bou06a], AC, II, § 2, n° 6, cor. 1 de la prop. 13). $_\star$

Il résulte notamment du scholie qu'on a $\mathfrak{e}_{n;\mathbf{d}} \neq 0$ pour $r \geqslant n$. En effet, les r polynômes $X_1^{d_1},\dots,X_n^{d_n},0,\dots,0$ n'ont pas de zéro commun non trivial dans un corps.

LEMME 3. *Soient A un anneau, f un élément de A, A_f l'anneau-quotient $A[T]/(fT-1)$ et $h\colon A \to A_f$ l'homomorphisme canonique.*

a) *Le noyau de h est formé des $a \in A$ tels qu'il existe $m \in \mathbf{N}$ avec $af^m = 0$.*

b) *Si A est intègre et si f est non nul, h est injectif et l'anneau A_f est intègre.*

Démonstration. La partie a) résulte immédiatement du lemme 2 appliqué à $E = A[T]$.

Démontrons b). Supposons A intègre et $f \neq 0$, et soit K le corps des fractions de A. Puisque f est inversible dans K, l'homomorphisme canonique de K dans $K[T]/(fT-1)$ est bijectif, et il suffit de prouver que l'homomorphisme canonique $A_f \to K[T]/(fT-1)$ est injectif, ou encore que $A[T]\cap(fT-1)K[T] = (fT-1)A[T]$. Soit donc $x = a_0+\cdots+a_nT^n \in A[T]$. Si on a $x \in (fT-1)K[T]$, il existe des éléments $d, b_0,\dots,b_{n-1}$ de A avec $d \neq 0$ et $d(a_0+\cdots+a_nT^n) = (1-fT)(b_0+\cdots+b_{n-1}T^{n-1})$. Cela s'écrit

$$da_0 = b_0\,,\quad da_1 = b_1 - fb_0\,,\quad \dots\,,\quad da_{n-1} = b_{n-1} - fb_{n-2}\,,\quad da_n = -fb_{n-1}\,,$$

ce qui implique aussitôt par récurrence sur i que chaque b_i est divisible par d. On a alors $x = (1-fT)(b_0/d+\cdots+(b_{n-1}/d)T^{n-1})$ donc $x \in (1-fT)A[T]$.

LEMME 4. *Soient V un anneau intègre, $Y_1, \dots, Y_r$ et X des indéterminées. Considérons l'anneau de polynômes*

$$V[\mathbf{Y}, X] = V[Y_1, \dots, Y_r, X]\,.$$

Pour chaque $j = 1, \dots r$, soit $Q_j \in V[Y_1, \dots, Y_{j-1}, X]$ un polynôme et soit F_j l'élément de $V[\mathbf{Y}, X]$ défini par:

$$F_j(Y_1, \dots, Y_r, X) = Q_j(Y_1, \dots, Y_{j-1}, X) + Y_j X^{d_j}\,.$$

Soit $\mathfrak{a}$ l'ensemble des $x \in V[\mathbf{Y}, X]$ tels que xX^m appartienne, pour m assez grand, à l'idéal engendré par les F_j. Alors $\mathfrak{a}$ est un idéal premier de $V[\mathbf{Y}, X]$ et on a $\mathfrak{a} \cap V[X] = 0$.

Démonstration. Introduisons l'anneau $V[X]_X = V[X, T]/(XT - 1)$ et l'homomorphisme canonique $u\colon V[X] \to V[X]_X$. Considérons de même l'homomorphisme canonique $v\colon V[\mathbf{Y}, X] \to V[\mathbf{Y}, X]_X$, avec $V[\mathbf{Y}, X]_X = V[\mathbf{Y}, X, T]/(XT - 1)$. Notons I l'idéal de $V[\mathbf{Y}, X]$ engendré par les F_j et soit J l'idéal de $V[\mathbf{Y}, X]_X$ engendré par $v(I)$, donc aussi engendré par les ${}^uF_j$. On déduit de v, par passage aux quotients, un homomorphisme $w\colon V[\mathbf{Y}, X]/I \to V[\mathbf{Y}, X]_X/J$. On a un diagramme commutatif d'applications canoniques

$$\begin{array}{ccc} V[X] & \xrightarrow{u} & V[X]_X \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ V[\mathbf{Y}, X]/I & \xrightarrow{w} & V[\mathbf{Y}, X]_X/J\,. \end{array}$$

D'après le lemme 3, b) appliqué à l'anneau intègre $V[X]$, l'homomorphisme u est injectif et l'anneau $V[X]_X$ est intègre. D'après le lemme 3, a) appliqué à $V[\mathbf{Y}, X]/I$, $\mathfrak{a}$ est le noyau de l'homomorphisme composé de w et de l'application canonique de $V[\mathbf{Y}, X]$ dans $V[\mathbf{Y}, X]/I$. Il nous suffit alors de prouver que β est bijectif. Cela impliquera en effet que $V[\mathbf{Y}, X]_X/J$ est intègre, donc que $\mathfrak{a}$ est premier, et que $w \circ \alpha$ est injectif, donc que $\mathfrak{a} \cap V[X] = 0$.

Posons pour simplifier $A = V[X]_X$ et $B = V[\mathbf{Y}, X]_X/J$. Par construction, B s'identifie au quotient de $A[Y_1, \dots, Y_r]$ par l'idéal J' engendré par les polynômes ${}^uF_j$. Mais, notant T' l'image de T dans A, on a $T'X = 1$, donc ${}^uF_j = X^{d_j}(Y_j + T'^{d_j}Q_j)$. Posons $G_j = -T'^{d_j}Q_j \in A[Y_1, \dots, Y_{j-1}]$. Comme X est inversible dans A, l'idéal J' est engendré par les r polynômes $Y_j - G_j(Y_1, \dots, Y_{j-1})$. Soient $y_1, \dots, y_r$ les éléments de A définis récursivement par

$$y_1 = G_1\,, \quad y_2 = G_2(y_1)\,, \quad \dots\,, \quad y_j = G_j(y_1, \dots, y_{j-1})\,, \quad \dots$$

et soit $\gamma\colon A[Y_1,\dots,Y_r]\to A$ l'homomorphisme qui applique tout polynôme $L(Y_1,\dots,Y_r)$ sur $L(y_1,\dots,y_r)\in A$. Alors γ induit par passage au quotient un homomorphisme $B\to A$ inverse de β. Cela montre que β est bijectif, comme annoncé, et achève la démonstration.

Rappelons qu'on a noté $I_{n;\mathbf{d}}$ l'idéal (gradué) de $U_{n;\mathbf{d}}[X_1,\dots,X_n]$ engendré par les polynômes universels $P_j(X_1,\dots,X_n)$ et que l'idéal résultant universel $\mathfrak{e}_{n;\mathbf{d}}\subset U_{n;\mathbf{d}}$ est formé des $u\in U_{n;\mathbf{d}}$ tels que, pour chaque $i=1,\dots,n$, il existe $m\in\mathbf{N}$ avec $uX_i^m\in I_{n;\mathbf{d}}$.

Dans la démonstration des propositions 3 et 4 qui suivent, nous utiliserons les notations suivantes. Pour $j=1,\dots r$, notons Y_j le coefficient de $X_n^{d_j}$ dans P_j, c'est l'une des indéterminées de l'anneau universel $U_{n;\mathbf{d}}$. Notons U_0 l'anneau de polynômes sur $\mathbf{Z}$ en toutes les indéterminées de $U_{n;\mathbf{d}}$ autres que les Y_j, de sorte que $U_{n;\mathbf{d}}$ s'identifie à l'anneau de polynômes $U_0[Y_1,\dots,Y_r]$ et que chaque P_j s'écrit

$$P_j=Y_jX_n^{d_j}+Q_j(X_1,\dots,X_n)\quad\text{avec}\quad Q_j\in U_0[X_1,\dots,X_n]\,.$$

L'idéal résultant universel $\mathfrak{e}_{n;\mathbf{d}}=R(P_1,\dots,P_r)\subset U_{n;\mathbf{d}}$ *est premier.* Plus généralement :

PROPOSITION 3. *Soit K un anneau intègre. Considérons l'anneau $U=K\otimes_{\mathbf{Z}}U_{n;\mathbf{d}}$ et soit $h\colon U_{n;\mathbf{d}}\to U$ l'homomorphisme canonique. Soit I l'idéal de $U[X_1,\dots,X_n]$ engendré par les polynômes ${}^hP_1,\dots,{}^hP_r$. Alors l'idéal éliminant $\mathfrak{e}(I)$ de U est premier.*

Démonstration. Notons $\mathfrak{a}$ l'ensemble des $u\in U[X_1,\dots,X_n]$ tels qu'il existe $m\in\mathbf{N}$ avec $uX_n^m\in I$. Soit V l'anneau $K\otimes U_0[X_1,\dots,X_{n-1}]$, de sorte que $U[X_1,\dots,X_n]$ s'identifie à $V[Y_1,\dots,Y_r,X_n]$. Les ${}^hQ_j$ appartiennent tous à $V[X_n]$. On peut donc appliquer le lemme 4 et on voit que $\mathfrak{a}$ est premier et ne contient aucun élément non nul de $V[X_n]$ et en particulier aucun des X_i.

Pour chaque $i=1,\dots,n$, notons $\mathfrak{a}_i$ l'ensemble des $u\in U[X_1,\dots,X_n]$ tel qu'il existe $m\in\mathbf{N}$ avec $uX_i^m\in I$. On a donc $\mathfrak{a}_n=\mathfrak{a}$ et par définition

$$\mathfrak{e}(I)=U\cap\bigcap_i\mathfrak{a}_i\,. \tag{1}$$

Soit $u\in\mathfrak{a}_i$. Il existe $m\in\mathbf{N}$ avec $uX_i^m\in I\subset\mathfrak{a}$. Comme $\mathfrak{a}$ est premier et ne contient pas X_i, on a $u\in\mathfrak{a}$. On donc prouvé l'inclusion $\mathfrak{a}_i\subset\mathfrak{a}_n$. Comme évidemment l'ordre des indéterminées X_i ne joue aucun rôle, on a $\mathfrak{a}_i\subset\mathfrak{a}_j$ pour tout couple (i,j). Il en résulte que les idéaux $\mathfrak{a}_i$ sont donc tous égaux. La relation (1) s'écrit donc $\mathfrak{e}(I)=U\cap\mathfrak{a}$, ce qui implique que $\mathfrak{e}(I)$ est premier.

COROLLAIRE. *Pour qu'un élément u de $U_{n;\mathbf{d}}$ appartienne à l'idéal résultant universel $\mathfrak{e}_{n;\mathbf{d}}$, il faut et il suffit que, pour tout corps k et toute famille $(f_1,\dots,f_r)$ de polynômes homogènes de $k[X_1,\dots,X_n]$ de degrés respectifs $d_1,\dots,d_r$ ayant un zéro non trivial dans k^n, on ait $\tilde{u}(f_1,\dots,f_r)=0$.*

Démonstration. La condition est nécessaire d'après le scholie. Inversement, supposons-la vérifiée. Puisque $\mathfrak{e}_{n;\mathbf{d}}$ est premier, l'anneau-quotient $U_{n;\mathbf{d}}/\mathfrak{e}_{n;\mathbf{d}}$ est intègre. Soit k son corps des fractions et soit $h\colon U_{n;\mathbf{d}}\to k$ l'homomorphisme canonique. Posons $f_j={}^hP_j$ pour $j=1,\dots,r$. D'après le scholie, il existe une extension K de k telle que les f_j aient un zéro commun non trivial dans K^n. Il résulte alors de l'hypothèse que $\tilde{u}(f_1,\dots,f_r).1_K=0$. Mais, puisque $\tilde{u}(f_1,\dots,f_r)=h(u)$, cela implique $u\in\ker h=\mathfrak{e}_{n;\mathbf{d}}$.

Soit A un anneau et soient $f_1,\dots,f_s$ des éléments de $A[X_1,\dots,X_n]$. On dit que la famille (f_j) est *algébriquement liée* s'il existe un polynôme $R\in A[T_1,\dots,T_s]$, non nul, tel que $R(f_1,\dots,f_s)=0$. On dit que (f_j) est *algébriquement libre* dans le cas contraire. Par exemple, la famille (X_j) est algébriquement libre.

LEMME 5. *Soient A un anneau, B une A-algèbre de polynômes en un nombre fini d'indéterminées, $f_1,\dots,f_s$ des éléments de $B[X_1,\dots,X_n]$ et $h\colon B\to A$ un homomorphisme. Si les f_j sont algébriquement liés, il en est de même des ${}^hf_j$.*

Démonstration. Si $B=A[U_1,\dots,U_m]$ et si $a_i=h(U_i)$, alors h est l'unique homomorphisme de A-algèbres tel que $h(U_i)=a_i$. Il se factorise en $h'\circ h''$, où $h''\colon A[U_1,\dots,U_m]\to A[U_1,\dots,U_{m-1}]$ est l'homomorphisme de $A[U_1,\dots,U_{m-1}]$-algèbres tel que $h''(U_m)=a_m$, et $h'\colon A[U_1,\dots,U_{m-1}]\to A$ est l'homomorphisme de A-algèbres tel que $h'(U_i)=a_i$ pour $i=1,\dots,m-1$. Raisonnant par récurrence sur m, on est donc ramené au cas où $m=1$, c'est-à-dire $B=A[U]$. Posons $a=h(U)$. Soit $R\in B[T_1,\dots,T_s]=A[U,T_1,\dots,T_s]$, non nul, tel que $R(U,f_1,\dots,f_s)=0$ et dont le degré en U est minimum parmi les éléments de $B[T_1,\dots,T_s]$ ayant ces propriétés. On a ${}^hR({}^hf_1,\dots,{}^hf_s)=0$ et il suffit de voir que ${}^hR$ est non nul. Mais ${}^hR(T_1,\dots,T_n)$ n'est autre que $R(a,T_1,\dots,T_n)$. S'il était nul, R s'écrirait $(U-a)R'$ avec $R'\in B[T_1,\dots,T_s]$ et on aurait $R'\neq 0$ et $R'(U,f_1,\dots,f_s)=0$ puisque $(U-a)$ ne divise pas zéro, ce qui contredirait le caractère minimal de R.

PROPOSITION 4. a) *L'idéal résultant universel $\mathfrak{e}_{n;\mathbf{d}}$ est nul si $r<n$, non nul si $r\geqslant n$.*

b) *Si $r=n$, l'idéal résultant universel $\mathfrak{e}_{n;\mathbf{d}}$ est principal.*

Démonstration. Démontrons d'abord un résultat auxiliaire. Soit $u \in \mathfrak{e}_{n;\mathbf{d}}$, identifié à un polynôme de $U_0[Y_1, \ldots, Y_r]$. Posons $s = \inf(n-1, r)$ et supposons que u ne fasse pas intervenir les indéterminées Y_j pour $j > s$, autrement dit que l'on ait $u = u(Y_1, \ldots, Y_s) \in U_0[Y_1, \ldots, Y_s]$. *Nous allons prouver que* $u = 0$, *c'est-à-dire que* $\mathfrak{e}_{n;\mathbf{d}} \cap U_0[Y_1, \ldots, Y_s] = 0$.

Rappelons qu'on a posé

$$P_j = Y_j X_n^{d_j} + Q_j(X_1, \ldots, X_n) \quad \text{avec} \quad Q_j \in U_0[X_1, \ldots, X_n].$$

Il existe par définition un entier $m \in \mathbf{N}$ et des polynômes $u_j(Y_1, \ldots, Y_r) \in U_0[Y_1, \ldots, Y_r]$ avec

$$u(Y_1, \ldots, Y_s) X_n^m = \sum_j u_j(Y_1, \ldots, Y_r)(Y_j X_n^{d_j} + Q_j(X_1, \ldots, X_n)).$$

Posons $Q'_j(X_1, \ldots, X_{n-1}) = -Q_j(X_1, \ldots, X_{n-1}, 1) \in U_0[X_1, \ldots, X_{n-1}]$. Substituant 1 à X_n et Q'_j à Y_j pour chaque j, on obtient, dans l'anneau $U_0[X_1, \ldots, X_{n-1}]$ la relation $u(Q'_1, \ldots, Q'_s) = 0$. Si u est non nul, la famille $(Q'_j)_{1 \leqslant j \leqslant s}$ est donc algébriquement liée.

Par définition de l'anneau universel, il existe un homomorphisme d'anneaux $h\colon U_{n;\mathbf{d}} \to \mathbf{Z}$ avec ${}^hP_j = -X_j X_n^{d_j - 1}$ pour $j \leqslant s$ et ${}^hP_j = 0$ pour $j > s$. Puisque h annule les Y_j, on en déduit un homomorphisme d'anneaux $k\colon U_0 \to \mathbf{Z}$ tel que pour $j = 1, \ldots, s$, on ait ${}^kQ_j = -X_j X_n^{d_j - 1}$ et donc ${}^kQ'_j = X_j$. D'après le lemme 5, la famille $(X_j)_{j=1,\ldots,s}$ de $\mathbf{Z}[X_1, \ldots, X_s]$ est liée si u est non nul. Par conséquent, u est nul et on a $\mathfrak{e}_{n;\mathbf{d}} \cap U_0[Y_1, \ldots, Y_s] = 0$ comme annoncé.

Cela étant, si on a $r < n$, donc $s = r$, on a $U_0[Y_1, \ldots, Y_s] = U_{n;\mathbf{d}}$ et par conséquent $\mathfrak{e}_{n;\mathbf{d}} = 0$. Cela prouve l'assertion a), puisque l'on sait déjà que $\mathfrak{e}_{n;\mathbf{d}} \neq 0$ lorsque r est $\geqslant n$. Si l'on a $r = n$, alors $s = n-1$ et par conséquent $\mathfrak{e}_{n;\mathbf{d}} \cap U_0[Y_1, \ldots, Y_{r-1}] = 0$. Pour prouver que l'idéal $\mathfrak{e}_{n;\mathbf{d}}$ est principal, il suffit alors d'appliquer le lemme suivant :

LEMME 6. *Soit A une $\mathbf{Z}$-algèbre de polynômes en un nombre fini d'indéterminées et soit $\mathfrak{p}$ un idéal premier de $A[X]$. Si $\mathfrak{p} \cap A = 0$, l'idéal $\mathfrak{p}$ est principal.*

Démonstration. Soit K le corps des fractions de A. D'après [Bou07b], A, IV, p. 11, prop. 11, l'idéal $\mathfrak{p}K$ de $K[X]$ est principal. Il existe donc $u(X) \in \mathfrak{p}$ et $a \in A$, avec $a \neq 0$, tels que $\mathfrak{p}K = (u(X)/a)K[X] = u(X)K[X]$. Soit $c \in A$ un contenu (appendice 1) de $u(X)$, de sorte que $u(X)/c$ appartient à $A[X]$ et est de contenu 1. On a $c(u(X)/c) \in \mathfrak{p}$ et $c \notin \mathfrak{p}$ puisque $\mathfrak{p} \cap A = 0$, donc $u(X)/c \in \mathfrak{p}$. Remplaçant $u(X)$ par $u(X)/c$, on peut donc supposer que $u(X)$

est de contenu 1. Soit $v(X)$ un élément non nul de $\mathfrak{p}$. Montrons que $v(X)$ est un multiple de $u(X)$ dans $A[X]$, donc que $u(X)$ engendre l'idéal $\mathfrak{p}$. Il existe $b \in A$ et $w(X) \in A[X]$, non nuls, avec $bv(X) = u(X)w(X)$. Alors b divise un contenu de $u(X)w(X)$, donc divise un contenu de $w(X)$ d'après le lemme de Gauss (appendice 1), et on a bien $v(X) = u(X)(w(X)/b)$, avec $w(X)/b \in A[X]$.

REMARQUE 2. La démonstration du lemme 6 n'utilise que le fait que A est factoriel.

COROLLAIRE. *Soient k un corps et I un idéal gradué de $k[X_1, \ldots, X_n]$ tel que $I_0 = 0$. Si I est engendré par des polynômes en nombre strictement inférieur à n, il existe une extension K de k, de degré fini, telle que I possède un zéro non trivial dans K^n.*

Démonstration. Cela résulte de la partie a) de la proposition 4 et du scholie.

4. RÉSULTANT DE n POLYNÔMES HOMOGÈNES À n INDÉTERMINÉES

Dans ce numéro, on fixe l'entier $n > 0$ et on se place dans le cas où $r = n$.

Pour chaque famille $\mathbf{d} = (d_1, \ldots, d_n)$ de $\mathbf{N}^n$ tel que $d_j > 0$ pour $j = 1, \ldots, n$, on note respectivement $U_{\mathbf{d}}$ et $\mathfrak{e}_{\mathbf{d}}$ l'anneau universel $U_{n;\mathbf{d}}$ et l'idéal éliminant universel $\mathfrak{e}_{n;\mathbf{d}}$ introduits au numéro précédent.

D'après la proposition 4, b) du n° 3, l'idéal $\mathfrak{e}_{\mathbf{d}}$ est principal. Soit $a \in U_{\mathbf{d}}$ un générateur de cet idéal. Considérons les polynômes $X_j^{d_j}$ de $\mathbf{Z}[X_1, \ldots, X_n]$ et l'entier $m = \tilde{a}(X_1^{d_1}, \ldots, X_n^{d_n})$. D'après le scholie du n° 3, on a $h(m) \neq 0$ pour tout homomorphisme h de $\mathbf{Z}$ dans un corps k. En particulier, m n'est divisible par aucun entier premier, donc est égal à 1 ou à -1. Comme les seuls éléments inversibles de l'anneau $U_{\mathbf{d}}$ sont 1 et -1, on voit que $u = a/m$ est l'unique générateur de l'idéal $\mathfrak{e}_{\mathbf{d}}$ tel que $\tilde{u}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$.

DÉFINITION 3. On note $R_{\mathbf{d}}$ l'unique élément u de $U_{\mathbf{d}}$ tel que $\mathfrak{e}_{\mathbf{d}} = uU_{\mathbf{d}}$ et $\tilde{u}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$. Pour chaque anneau A et chaque famille $(f_1, \ldots, f_n)$ de polynômes homogènes de $A[X_1, \ldots, X_n]$ de degrés respectifs $d_1, \ldots, d_n$, l'élément $\widetilde{R}_{\mathbf{d}}(f_1, \ldots, f_n)$ de A est noté $\mathrm{res}(f_1, \ldots, f_n)$ et appelé *résultant* de la famille $(f_1, \ldots, f_n)$.

REMARQUE 1. Dans l'anneau $U_{\mathbf{d}}$, on a

$$\operatorname{res}(P_1, \ldots, P_{j-1}, 0, P_{j+1}, \ldots, P_n) = 0$$

comme il résulte des cor. aux prop. 3 et 4 du n° 3 appliqués au corps des fractions de $U_{\mathbf{d}}$. Il s'ensuit que $\operatorname{res}(f_1, \ldots, f_n) = 0$ dès que l'un des polynômes f_j est nul; comme d'autre part un polynôme homogène non nul possède un degré uniquement déterminé, on voit que l'élément $\operatorname{res}(f_1, \ldots, f_n)$ ne dépend pas du choix de la famille $\mathbf{d}$ tel que f_j soit de degré d_j pour tout j. Cela justifie l'absence de la mention des d_j dans la notation du résultant.

On a par définition $R_{\mathbf{d}} = \operatorname{res}(P_1, \ldots, P_n)$. Aussi dirons-nous que $R_{\mathbf{d}}$ est le *résultant universel* (relativement aux degrés d_i). Puisque l'idéal $\mathfrak{c}_{\mathbf{d}}$ est premier (prop. 3 du n° 3), le polynôme $R_{\mathbf{d}}$ est premier (appendice 1).

SCHOLIE. *A chaque famille $(f_1, \ldots, f_n)$ de polynômes homogènes de degrés > 0 en $X_1, \ldots, X_n$ à coefficients dans un anneau A, nous avons associé un élément* $\operatorname{res}(f_1, \ldots, f_n)$ *de A. De plus:*

a) *si $h\colon A \to B$ est un homomorphisme d'anneaux, on a*

$$\operatorname{res}({}^h f_1, \ldots, {}^h f_n) = h(\operatorname{res}(f_1, \ldots, f_n))\,;$$

b) *si A est un corps, on a* $\operatorname{res}(f_1, \ldots, f_n) = 0$ *si et seulement s'il existe une extension K (de degré fini) de A telle que les f_j aient un zéro commun non trivial dans K^n;*

c) *on a* $\operatorname{res}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$, *pour toute famille (d_j) d'entiers strictement positifs;*

d) *pour toute famille (d_j) d'entiers strictement positifs, le résultant* $\operatorname{res}(P_1, \ldots, P_n)$ *des polynômes universels correspondants engendre un idéal premier de l'anneau universel de coefficients $U_{\mathbf{d}}$.*

EXEMPLE 1. Soient A un anneau, (a_{ij}) une matrice carrée d'ordre n à coefficients dans A. On a

$$\operatorname{res}\Big(\sum_i a_{1i}X_i, \ldots, \sum_i a_{ni}X_i\Big) = \det(a_{ij})\,.$$

Il suffit de faire la démonstration lorsque $A = U_{(1,\ldots,1)} = \mathbf{Z}[(T_{ij})_{1 \leqslant i,\, j \leqslant n}]$ et $a_{ij} = T_{ij}$, auquel cas la relation proposée s'écrit $R_{(1,\ldots,1)} = \det(T_{ij})$. D'après le corollaire à la proposition 3 du n° 3 et [Bou07a], A, III, p. 102, prop. 14, il existe $f = f((T_{ij})) \in A$ avec $\det(T_{ij}) = f((T_{ij}))\, R_{(1,\ldots,1)}$. Puisque $\det(T_{ij})$ est homogène de degré n, le polynôme f est homogène

de degré $s \leqslant n$. Attribuons alors la valeur 0 à chaque variable T_{ij} avec $i \neq j$. On obtient alors dans l'anneau $\mathbf{Z}[T_{11}, \ldots, T_{nn}]$ une relation $T_{11} \ldots T_{nn} = g(T_{11}, \ldots, T_{nn})\ \mathrm{res}(T_{11}X_1, \ldots, T_{nn}X_n)$, où g est un polynôme homogène de degré s. Mais, puisque le polynôme $\mathrm{res}(T_{11}X_1, \ldots, T_{nn}X_n)$ s'annule lorsque l'un des T_{ii} s'annule, il est divisible par le produit $T_{11} \cdots T_{nn}$. Cela implique que $s = 0$, donc que f est constant. Prenant pour (a_{ij}) la matrice unité, on voit que $f = 1$.

REMARQUE 2. a) On peut exprimer la relation précédente comme suit : le résultant d'une suite de n formes linéaires est le déterminant de cette suite relativement à la base canonique $(X_1, \ldots, X_n)$.

b) Il résulte de ce qui précède que le polynôme $\det(T_{ij})$ est premier.

REMARQUE 3. Les propriétés a) à d) du scholie caractérisent le résultant. En effet, supposons donné, pour chaque famille $(f_1, \ldots, f_n)$ de polynômes homogènes de degrés > 0 en $X_1, \ldots, X_n$ à coefficients dans un anneau A, un élément $\rho(f_1, \ldots, f_n)$ de A, de façon que les propriétés analogues soient satisfaites. Posons $a = \rho(P_1, \ldots, P_n) \in U_{\mathbf{d}}$. D'après a), on a $\rho(f_1, \ldots, f_n) = \tilde{a}(f_1, \ldots, f_n)$. Appliquant alors b) au corps des fractions de l'anneau intègre $U_{\mathbf{d}}/\mathfrak{e}_{\mathbf{d}}$ et à la famille image de la famille universelle, on voit qu'on a $a \in \mathfrak{e}_{\mathbf{d}}$, donc que a s'écrit $a = bR_{\mathbf{d}}$, avec $b \in U_{\mathbf{d}}$. Comme a et $R_{\mathbf{d}}$ sont premiers d'après la condition d), b est inversible, donc égal à ± 1. La condition c) implique alors $b = 1$.

Nous utiliserons à plusieurs reprises le résultat technique suivant :

LEMME 7. *Soit V une $U_{\mathbf{d}}$-algèbre de polynômes en un nombre fini d'indéterminées et soit $(q_1, \ldots, q_n)$ une famille de polynômes homogènes de degrés > 0 de $V[X_1, \ldots, X_n]$. Supposons que, pour tout homomorphisme h de V dans un corps k tel que la famille (P_j) ait un zéro commun non trivial dans k^n, il en soit de même de la famille (q_j). Alors* $\mathrm{res}(q_1, \ldots, q_n)$ *est divisible dans V par le résultant universel* $\mathrm{res}(P_1, \ldots, P_n)$.

Démonstration. L'anneau $V/VR_{\mathbf{d}}$ est une algèbre de polynômes sur l'anneau intègre $U_{\mathbf{d}}/U_{\mathbf{d}}R_{\mathbf{d}}$, donc est intègre. Notons k son corps des fractions. Il existe une extension K de k telle que les P_j aient un zéro commun non trivial dans K^n (propriétés a) et b) du scholie). Alors les q_j ont aussi un zéro commun non trivial dans K^n et (toujours d'après a) et b)) l'image de $\mathrm{res}(g_1, \ldots, g_n)$ dans k est nulle, donc $\mathrm{res}(g_1, \ldots, g_n)$ appartient à $VR_{\mathbf{d}}$.

Fixons une permutation $\sigma \in \mathfrak{S}_n$. Nous allons définir un élément D_σ de $\mathfrak{e}_{\mathbf{d}}$, appelé *déterminant de Sylvester d'indice* σ (pour les degrés fixés $d_1, \dots, d_n$). Posons

$$r = \sum_{i=1}^{n} (d_i - 1) + 1 = \sum_{i=1}^{n} d_i - n + 1$$

et soit M l'ensemble des monômes $\mathbf{X}^{\boldsymbol{\alpha}}$ pour $|\boldsymbol{\alpha}| = r$. Par définition de r, tout monôme de M est divisible par au moins un des $X_i^{d_i}$.

Pour $i = 1, \dots, n$, soit M_i la partie de M formée de ceux de ces monômes qui sont divisibles par $X_{\sigma(i)}^{d_{\sigma(i)}}$ et ne sont divisibles par aucun des $X_{\sigma(j)}^{d_{\sigma(j)}}$ pour $j < i$. Il est clair que les M_i forment une partition de M.

Pour chaque monôme $m \in M$, soit $i(m)$ l'unique entier tel que m appartienne à $M_{i(m)}$, soit $u(m)$ le monôme tel que

$$m = u(m) X_{\sigma(i(m))}^{d_{\sigma(i(m))}}$$

et posons

$$Q(m) = u(m) P_{\sigma(i(m))}\,.$$

La famille $(m)_{m \in M}$ est une base du $U_{\mathbf{d}}$-module libre des polynômes homogènes en les X_i de degré total r. Les Q_m appartiennent à ce module et on note D_σ le déterminant de la famille $(Q_m)_{m \in M}$ relativement à la base $(m)_{m \in M}$.

LEMME 8. *Le déterminant D_σ est un élément non nul de $\mathfrak{e}_{\mathbf{d}}$. Il n'est divisible par aucun entier > 1. Il est homogène et de degré $(d_1 \cdots d_n)/d_{\sigma(n)}$ en les coefficients du polynôme universel $P_{\sigma(n)}$.*

Démonstration. Par construction, l'élément $\widetilde{D}_\sigma(X_1^{d_1}, \dots, X_n^{d_n})$ est le déterminant de la matrice unité, donc est égal à 1, ce qui implique que D_σ n'est pas nul et n'est divisible par aucun entier > 1. Pour chaque $i = 1, \dots, n$, le monôme X_i^r appartient à M ; les formules de Cramer ([Bou07a], A, III, p. 102, formule (37)) entraînent que $D_\sigma X_i^r$ est une combinaison linéaire des $Q(m)$, donc appartient à l'idéal engendré par les P_j ; ainsi, D_σ appartient à $\mathfrak{e}_{\mathbf{d}}$ par définition de ce dernier. Enfin, D_σ est homogène de degré $\mathrm{Card}(M_i)$ en les coefficients de $P_{\sigma(i)}$ pour chaque i et notamment pour $i = n$. Mais M_n est l'ensemble des $\mathbf{X}^{\boldsymbol{\alpha}} \in M$ avec $\alpha_j < d_j$ pour $j \neq \sigma(n)$, de sorte qu'on a $\mathrm{Card}(M_n) = \prod_{j \neq \sigma(n)} d_j = (d_1 \cdots d_n)/d_{\sigma(n)}$.

PROPOSITION 5. *Soit A un anneau et, pour $i = 1, \dots, n$, soit f_i un polynôme homogène de degré $d_i > 0$ de $A[X_1, \dots, X_n]$.*

a) *Soient $\lambda_1, \dots, \lambda_n$ des éléments de A. On a*

$$\operatorname{res}(\lambda_1 f_1, \dots, \lambda_n f_n) = \lambda_1^{r_1} \cdots \lambda_n^{r_n} \operatorname{res}(f_1, \dots, f_n),$$

où $r_i = (d_1 \cdots d_n)/d_i = d_1 \cdots d_{i-1} d_{i+1} \cdots d_n$ pour $i = 1, \dots, n$.

b) *Soit $i \in [1, n]$ et soit f_i' un polynôme homogène de degré > 0 de $A[X_1, \dots, X_n]$. On a*

$$\operatorname{res}(f_1, \dots, f_{i-1}, f_i f_i', f_{i+1}, \dots, f_n) = \operatorname{res}(f_1, \dots, f_{i-1}, f_i, f_{i+1}, \dots, f_n) \cdot \operatorname{res}(f_1, \dots, f_{i-1}, f_i', f_{i+1}, \dots, f_n).$$

Démonstration. La démonstration s'effectue en plusieurs étapes.

1) Posons $r_i = (d_1 \cdots d_n)/d_i$. D'après le lemme 8, l'idéal $\mathfrak{c}_{\mathbf{d}}$ formé des multiples de $R_{\mathbf{d}}$ contient pour chaque i un élément non nul qui est homogène de degré r_i relativement aux coefficients de P_i. Il s'ensuit que $R_{\mathbf{d}}$ est homogène de degré s_i relativement aux coefficients de P_i avec $s_i \leqslant r_i$ ([Bou07b], A, IV, p. 9, remarque). *Pour démontrer* a)*, il suffit donc de démontrer que $s_i = r_i$ pour chaque i.*

2) Plaçons-nous dans les hypothèses de b) et notons d_{n+1} le degré de f_i'. Considérons l'anneau universel $U_{n;\mathbf{d}'}$, où $\mathbf{d}' = (d_1, \dots, d_n, d_{n+1})$ et les polynômes universels $P_1, \dots, P_{n+1} \in U'_{\mathbf{d}}[X_1, \dots, X_n]$, et posons

$$\begin{aligned} R &= \operatorname{res}(P_1, \dots, P_{i-1}, P_i, P_{i+1}, \dots, P_n), \\ R' &= \operatorname{res}(P_1, \dots, P_{i-1}, P_{n+1}, P_{i+1}, \dots, P_n), \\ S &= \operatorname{res}(P_1, \dots, P_{i-1}, P_i P_{n+1}, P_{i+1}, \dots, P_n). \end{aligned}$$

Pour démontrer b)*, il suffit de prouver que $S = RR'$.* En effet, il existe un homomorphisme d'anneaux $h\colon U_{n;\mathbf{d}'} \to A$ tel que ${}^hP_1 = f_1, \dots, {}^hP_n = f_n, {}^hP_{n+1} = f_i'$ et l'égalité cherchée n'est autre que $h(S) = h(R)h(R')$.

3) *Montrons que RR' divise S.* Appliquant le lemme 7 à l'anneau $V = U_{n,\mathbf{d}'}$ et à la famille $(P_1, \dots, P_{i-1}, P_i P_{n+1}, P_{i+1}, \dots, P_n)$, on voit que R divise S. On voit de même que R' divise S. Mais R est premier et il suffit maintenant de noter qu'il ne divise pas R', puisque R' est de degré 0 par rapport aux coefficients de P_i tandis que R ne l'est pas (cela résulte par exemple de la remarque 1).

4) *Dans l'anneau $\mathbf{Z}[T_1, \dots, T_n]$, l'élément* $\operatorname{res}(T_1 X_1^{d_1}, \dots, T_n X_n^{d_n})$ *est divisible par $T_1^{r_1} \cdots T_n^{r_n}$.* Raisonnons par récurrence sur $d_1 + \cdots + d_n \geqslant n$. Lorsque

$d_1+\cdots+d_n=n$, chaque d_i est égal à 1 et l'assertion résulte de l'exemple 1. Si $d_1+\cdots+d_n>n$, on a par exemple $d_1>1$. D'après l'hypothèse de récurrence, $\mathrm{res}(T_1X_1^{d_1-1},T_2X_2^{d_2},\ldots,T_nX_n^{d_n})$ est divisible par $T_1^{a/(d_1-1)}\cdots T_n^{a/d_n}$, où $a=(d_1-1)d_2\cdots d_n$, tandis que $\mathrm{res}(X_1,T_2X_2^{d_2},\ldots,T_nX_n^{d_n})$ est divisible par $T_2^{b/d_2}\cdots T_n^{b/d_n}$ avec $b=d_2\cdots d_n$. Appliquant 3), on en conclut que $\mathrm{res}(T_1X_1^{d_1},\ldots,T_nX_n^{d_n})$ est divisible par le produit des deux expressions précédentes, produit qui est bien $T_1^{r_1}\cdots T_n^{r_n}$.

5) *Fin de la démonstration*. D'après 1), on a

$$\mathrm{res}(T_1X_1^{d_1},\ldots,T_nX_n^{d_n})=T_1^{s_1}\cdots T_n^{s_n}\ \mathrm{res}(X_1^{d_1},\ldots,X_n^{d_n})=T_1^{s_1}\cdots T_n^{s_n}$$

avec $s_i\leqslant r_i$ pour tout i. Comparant à 4), on voit qu'on a $s_i=r_i$, ce qui achève de démontrer a). Enfin, avec les notations de 2), on a vu dans 3) que RR' divise S. Mais, d'après a), RR' et S ont le même multi-degré. Il existe donc un entier $a\in\mathbf{Z}$ avec $S=aRR'$. Comme on a $\widetilde{S}(X_1^{d_1},\ldots,X_i^{d_i+d_{n+1}},\ldots,X_n^{d_n})=1$, $\widetilde{R}(X_1^{d_1},\ldots,X_i^{d_i},\ldots,X_n^{d_n})=1$ et $\widetilde{R}'(X_1^{d_1},\ldots,X_i^{d_{n+1}},\ldots,X_n^{d_n})=1$, il s'ensuit que $a=1$, ce qui achève la démonstration.

COROLLAIRE 1. *Soit* $\mathbf{d}=(d_1,\ldots,d_n)$ *une suite d'entiers* >0. *Le résultant universel* $R_{\mathbf{d}}$ *est l'unique élément* $R\in U_{\mathbf{d}}$ *satisfaisant aux trois conditions suivantes :*

a) *Pour* $i=1,\ldots,n$, R *est homogène de degré* $(d_1\cdots d_n)/d_i$ *en les coefficients de* P_i.

b) *Si* k *est un corps, si, pour chaque* $i=1,\ldots,n$, f_i *est un polynôme homogène de degré* d_i *de* $k[X_1,\ldots,X_n]$ *et si les* f_i *ont un zéro commun non trivial dans* k^n, *alors* $\widetilde{R}(f_1,\ldots,f_n)=0$.

c) *On a* $\widetilde{R}(X_1^{d_1},\ldots,X_n^{d_n})=1$.

Démonstration. On sait déjà que $R_{\mathbf{d}}$ satisfait à ces conditions : a) résulte de la partie a) de la proposition 5 ; b) et c) résultent des conditions b) et c) du scholie. Inversement, soit $R\in U_{\mathbf{d}}$ satisfaisant à ces conditions. D'après le corollaire de la prop. 3 du n° 3, la condition b) implique qu'il existe $u\in U_{\mathbf{d}}$ avec $R=uR_{\mathbf{d}}$. La condition a) implique alors $u\in\mathbf{Z}$. On déduit enfin de la condition c) que $u=1$.

EXEMPLE 2. Pour $n=1$, on obtient

$$\mathrm{res}(\lambda X_1^{d_1})=\lambda\,.$$

EXEMPLE 3. Supposons $n=2$. A chaque polynôme homogène en deux indéterminées $Q(X_1,X_2)$, associons le polynôme en une indéterminée

$Q^\flat(X) = Q(X,1)$. Soient A un anneau, f et g deux polynômes homogènes de degrés respectifs $p > 0$ et $q > 0$ de $A[X_1, X_2]$, $f^\flat$ et $g^\flat$ les polynômes associés dans $A[X]$. Considérons le résultant $\mathrm{res}_{p,q}(f^\flat, g^\flat) \in A$ défini en [Bou07b], A, IV, p. 71, déf. 1. On a alors $\mathrm{res}(f,g) = \mathrm{res}_{p,q}(f^\flat, g^\flat)$. En effet, l'élément $R = \mathrm{res}_{p,q}(P_1^\flat, P_2^\flat) \in U_{(p,q)}$ jouit des propriétés a), b) et c) du corollaire 1, en vertu respectivement de [Bou07b], A, IV, p. 72, formule (28), p. 73, cor. 2 et p. 75, cor. 1, (i).

COROLLAIRE 2. *Soit* $\mathbf{d} = (d_1, \ldots, d_n)$ *une suite d'entiers* > 0 *et, pour chaque* i, *soit* $\sigma_i \in \mathfrak{S}_n$ *une permutation telle que* $\sigma_i(n) = i$. *Alors l'élément* $R_{\mathbf{d}}$ *de* $U_{\mathbf{d}}$ *est un plus grand commun diviseur des déterminants de Sylvester* D_{σ_i}.

Démonstration. Cela résulte du fait que $R_{\mathbf{d}}$ divise chacun des D_{σ_i}, que $R_{\mathbf{d}}$ et les D_{σ_i} ne sont divisibles par aucun entier > 1 (lemme 8) et que, pour chaque i, $R_{\mathbf{d}}$ et D_{σ_i} sont homogènes du même degré en les coefficients de P_i.

COROLLAIRE 3. *Avec les notations de la proposition* 5, *soit* $\sigma \in \mathfrak{S}_n$ *une permutation et soit* ϵ_σ *sa signature. On a*

$$\mathrm{res}(f_{\sigma(1)}, \ldots, f_{\sigma(n)}) = \epsilon_\sigma^{d_1 \cdots d_n} \mathrm{res}(f_1, \ldots, f_n)\,.$$

Démonstration. D'après le corollaire 1, il suffit de prouver la relation proposée lorsque $f_i = X_i^{d_i}$. Mais la partie b) de la proposition implique

$$\mathrm{res}(X_{\sigma(1)}^{d_{\sigma(1)}}, \ldots, X_{\sigma(n)}^{d_{\sigma(n)}}) = \mathrm{res}(X_{\sigma(1)}, \ldots, X_{\sigma(n)})^{d_1 \cdots d_n}.$$

et on conclut en appliquant l'exemple 1.

EXEMPLE 4. Soit A un anneau. Pour $j = 1, \ldots, n$, soit $(u_{ij})_{i \in E_j}$ une famille de d_j formes linéaires en $X_1, \ldots, X_n$ à coefficients dans A, de sorte que $\prod_{i \in E_j} u_{ij}$ est un polynôme homogène de degré d_j. On a alors

$$\mathrm{res}\Big(\prod_{i \in E_1} u_{i1}, \ldots, \prod_{i \in E_n} u_{in}\Big) = \prod_{(i_1, \ldots, i_n) \in E_1 \times \cdots \times E_n} \det(u_{i_1 1}, \ldots, u_{i_n n})\,.$$

Cela résulte en effet de la proposition 5, b) et de l'exemple 1.

Comme on l'a vu, le résultant universel $R_{\mathbf{d}}$ est irréductible en tant que polynôme à coefficients rationnels. Plus généralement :

PROPOSITION 6. *Pour tout anneau factoriel* K, *le polynôme* $1_K \otimes R_{\mathbf{d}}$ *est premier dans l'anneau de polynômes* $K \otimes_{\mathbf{Z}} U_{\mathbf{d}}$.

Démonstration. Posons $d = d_1 + \cdots + d_n$ et soit δ la suite formée de d fois l'entier 1. Considérons l'anneau universel de coefficients $U_{n,\delta}$ et la famille universelle de formes linéaires $(L_1, \ldots, L_d)$. Posons $V = K \otimes U_{n,\delta}$. C'est une algèbre de polynômes sur K, donc un anneau factoriel (appendice 1). Décomposons l'intervalle $[1, d]$ en n intervalles consécutifs $I_1, \ldots, I_n$, de longueurs respectives $d_1, \ldots, d_n$. Pour $j = 1, \ldots, n$, soit $\overline{P}_j \in V[X_1, \ldots, X_n]$ le produit des d_j formes linéaires $L_i.1_K$ pour $i \in I_j$, et soit $h\colon K \otimes U_{\mathbf{d}} \to V$ l'homomorphisme tel que ${}^h(P_j.1_K) = \overline{P}_j$ pour $j = 1, \ldots, n$. On a $h(R_{\mathbf{d}}.1_K) = \mathrm{res}(\overline{P}_1, \ldots, \overline{P}_n)$. Tous les éléments de l'image de h sont invariants sous l'action du groupe de permutations $G = \prod_j \mathfrak{S}_{I_j} \subset \mathfrak{S}_d$ (n° 2, exemple 4). Si $R_{\mathbf{d}}.1_K$ pouvait s'écrire comme produit de deux polynômes non constants de $K \otimes U_{\mathbf{d}}$, alors le résultant $\mathrm{res}(\overline{P}_1, \ldots, \overline{P}_n)$ pourrait s'écrire comme produit de deux polynômes de V, non constants et invariants sous l'action de G. Mais, d'après l'exemple 4 ci-dessus, cet élément est le produit d'une famille de polynômes premiers distincts, cette famille étant une orbite du groupe G. Une telle décomposition est donc impossible, ce qui achève la démonstration.

PROPOSITION 7. *Supposons $n \geqslant 2$. Soient A un anneau, $f_1, \ldots, f_n$ des polynômes homogènes de degrés > 0 de $A[X_1, \ldots, X_n]$ et soit $i \in [1, n]$ tel que $f_i = X_i^d$. Pour $j \neq i$, notons $\bar{f}_j$ le polynôme de $A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ obtenu en substituant 0 à X_i dans f_j. On a alors*

$$\mathrm{res}(f_1, \ldots, f_{i-1}, X_i^d, f_{i+1}, \ldots, f_n) = \mathrm{res}(\bar{f}_1, \ldots, \bar{f}_{i-1}, \bar{f}_{i+1}, \ldots, \bar{f}_n)^d.$$

Démonstration. Pour simplifier les notations, nous ferons la démonstration dans le cas $i = n$. D'après la proposition 5, b), il suffit de traiter le cas $d = 1$. Notons d_j le degré de f_j et posons $\mathbf{d} = (d_1, \ldots, d_{n-1})$ et $\mathbf{d}^\sharp = (d_1, \ldots, d_{n-1}, 1)$. Il suffit de faire la démonstration dans le cas où $A = U_{\mathbf{d}^\sharp}$ et $f_i = P_i$ pour $i = 1, \ldots, n-1$. Mais A est une algèbre de polynômes sur $U_{\mathbf{d}}$ et $\mathrm{res}(\overline{P}_1, \ldots, \overline{P}_{n-1})$ est le résultant universel $R_{\mathbf{d}} \in U_{\mathbf{d}}$. Appliquant le lemme 7, on voit que $\mathrm{res}(P_1, \ldots, P_{n-1}, X_n)$ est divisible dans A par $\mathrm{res}(\overline{P}_1, \ldots, \overline{P}_{n-1})$. Mais ces polynômes sont homogènes et de même degré ; leur rapport est donc un entier. La relation proposée étant vraie lorsque $f_i = X_i^{d_i}$ pour $i = 1, \ldots, n-1$, cet entier est égal à 1, ce qui achève la démonstration.

PROPOSITION 8. *Soient A un anneau, $f_1, \ldots, f_n$ des polynômes homogènes de degrés respectifs $d_i > 0$ de $A[X_1, \ldots, X_n]$, et $g_1, \ldots, g_n$ des polynômes homogènes de degrés respectifs $d_n - d_i$ (on convient que $g_i = 0$ lorsque $d_n - d_i$ est < 0). On a alors*

$$\mathrm{res}(f_1, \ldots, f_{n-1}, g_1 f_1 + \cdots + g_n f_n) = (g_n)^{d_1 \cdots d_{n-1}} \mathrm{res}(f_1, \ldots, f_n).$$

Démonstration. Nous allons classer les indices $i = 1, \ldots, n$ suivant le signe de $d_n - d_i$. D'après le cor. 3 à la prop. 5, les deux membres se modifient de la même manière lorsqu'on permute les polynômes $f_1, \ldots, f_{n-1}$. On peut donc supposer qu'il existe $s \in [1, n]$, tel qu'on ait $d_n - d_i < 0$ pour $i < s$, et $d_n - d_i \geqslant 0$ pour $s \leqslant i \leqslant n$. Ainsi, $g_i = 0$ est nul pour $i < s$ et est de degré $d_n - d_i$ pour $s \leqslant i \leqslant n$. Posons $\mathbf{d} = (d_1, \ldots, d_n)$ et $\mathbf{d}' = (d_1, \ldots, d_n, d_n - d_s, \ldots, d_n - d_n)$. Introduisons l'anneau universel $U_{n;\mathbf{d}'}$ et notons $P_1, \ldots, P_n, Q_s, \ldots, Q_n$ la suite universelle correspondante de polynômes. Notons au passage que Q_n, comme g_n, est de degré 0 par hypothèse. Il existe un homomorphisme d'anneaux $h\colon U_{n;\mathbf{d}'} \to A$ tel que ${}^hP_i = f_i$ pour $i = 1, \ldots, n$ et ${}^hQ_i = g_i$ pour $s \leqslant i \leqslant n$. Le premier membre de la relation à démontrer est donc l'image par h de l'élément $S = \operatorname{res}(P_1, \ldots, P_{n-1}, Q)$, avec $Q = Q_sP_s + \cdots + Q_nP_n$. Tout zéro commun à $P_1, \ldots, P_n$ étant un zéro de Q, on déduit directement du lemme 7 qu'il existe $u \in U_{n;\mathbf{d}'}$ tels que $u R_{\mathbf{d}} = S$. *Il s'agit donc de démontrer que l'on a* $u = Q_n^{d_1 \cdots d_{n-1}}$.

Mais S et $R_{\mathbf{d}}$ sont homogènes et de même degré $(d_1 \cdots d_n)/d_i$ relativement à l'ensemble des coefficients de chaque polynôme P_i. Il en résulte que u ne dépend pas de ces coefficients. Substituant alors les $X_i^{d_i}$ aux P_i, on obtient la relation $u = \operatorname{res}(X_1^{d_1}, \ldots, X_{n-1}^{d_{n-1}}, \overline{Q})$, avec $\overline{Q} = Q_sX_s^{d_s} + \cdots + Q_nX_n^{d_n}$. Par application itérée de la prop. 7, cela donne

$$u = \operatorname{res}(\overline{Q}(0, \ldots, 0, X_n))^{d_1 \cdots d_{n-1}} = \operatorname{res}(Q_nX_n^{d_n})^{d_1 \cdots d_{n-1}},$$

qui vaut bien $Q_n^{d_1 \cdots d_{n-1}}$ d'après l'exemple 2.

PROPOSITION 9. *Soient A un anneau, $f_1, \ldots, f_n$ des polynômes homogènes de degrés respectifs $d_i > 0$ de $A[X_1, \ldots, X_n]$, et (a_{ij}) une matrice carrée d'ordre n à coefficients dans A. Pour $i = 1, \ldots, n$, posons*

$$f_i'(X_1, \ldots, X_n) = f_i\Big(\sum_j a_{1j}X_j, \ldots, \sum_j a_{nj}X_j\Big).$$

On a

$$\operatorname{res}(f_1', \ldots, f_n') = \det(a_{ij})^{d_1 \cdots d_n} \operatorname{res}(f_1, \ldots, f_n).$$

Démonstration. Il suffit de faire la démonstration dans le cas où A est l'anneau $U_{\mathbf{d}}[(Z_{ij})]_{1 \leqslant i,j \leqslant n}$, $f_i = P_i$ pour tout i et $(a_{ij}) = (Z_{ij})$. Soit $h\colon A \to k$ un homomorphisme de A dans un corps k, posons $z_{ij} = h(Z_{ij})$. Si la matrice $z = (z_{ij})$ est inversible, le produit par z d'un zéro commun non trivial des P_i dans k^n est un zéro commun non trivial des P_i' ; si z n'est pas inversible, tout vecteur non nul du noyau de z est un zéro commun non trivial des P_i'.

Appliquant le lemme 7, on voit qu'il existe $u \in A$ avec $\mathrm{res}(P'_1, \ldots, P'_n) = u R_{\mathbf{d}}$. Mais u est alors homogène de degré 0 par rapport aux coefficients des P_i, donc appartient à $\mathbf{Z}[(Z_{ij})]$. Posant $X'_i = \sum_j Z_{ij} X_j$ pour tout i et substituant les $X_i^{d_i}$ aux P_i dans la relation précédente, on obtient

$$u = \mathrm{res}({X'_1}^{d_1}, \ldots, {X'_n}^{d_n}) = \mathrm{res}(X'_1, \ldots, X'_n)^{d_1 \cdots d_n} = \det(Z_{ij})^{d_1 \cdots d_n},$$

d'après la prop. 5, b) et l'exemple 1.

REMARQUE 4. La proposition précédente s'applique notamment lorsque $A = U_{\mathbf{d}}[Z_1, \ldots, Z_n]$ et $f_i = P_i$ pour $i = 1, \ldots, n$ et qu'on prend pour matrice (a_{ij}) la matrice diagonale $(Z_i \delta_{ij})$. On en conclut que si l'on munit $U_{\mathbf{d}}$ de la multigraduation de type $\mathbf{N}^n$ pour laquelle le coefficient de $\mathbf{X}^{\boldsymbol{\alpha}}$ dans chacun des P_i est de multidegré $\boldsymbol{\alpha}$, le résultant universel $\mathrm{res}(P_1, \ldots, P_n)$ est multihomogène de degré $(d_1 \cdots d_n, \ldots, d_1 \cdots d_n)$.

5. DISCRIMINANT D'UN POLYNÔME HOMOGÈNE À n INDÉTERMINÉES

Soient n et d deux entiers, avec $n > 0$ et $d \geqslant 2$. Si A est un anneau et $f \in A[X_1, \ldots, X_n]$ un polynôme homogène de degré d, nous noterons $J(f)$ l'idéal de $A[X_1, \ldots, X_n]$ engendré par f et ses n dérivées partielles $D_i f$ ([Bou07b], A, IV, p. 6).

Nous appellerons *zéros critiques* de f les zéros de l'idéal $J(f)$, c'est-à-dire les zéros communs à f et à ses dérivées partielles. Rappelons *l'identité d'Euler* ([Bou07b], A, IV, p. 8, prop. 6) :

$$\sum_{i=1,\ldots,n} X_i D_i f = d f .$$

Il en résulte que si l'entier d ne divise pas zéro dans A, tout zéro commun aux $D_i f$ est aussi un zéro de f, donc un zéro critique de f.

Il existe un unique homomorphisme d'anneaux $h\colon U_{n,d} \to A$ tel que $f = {}^h P_{n,d}$ et on peut traduire dans cette situation le scholie du n° 3 :

SCHOLIE. *Soient k un corps, $f \in k[X_1, \ldots, X_n]$ un polynôme homogène de degré d et $h\colon U_{n,d} \to k$ l'homomorphisme d'anneaux tel que $f = {}^h P_{n,d}$. Les trois propriétés suivantes sont équivalentes :*

(i) *On a* $h(\mathfrak{e}(J(P_{n,d}))) = 0$.

(ii) *On a* $\mathfrak{e}(J(f)) = 0$.

(iii) *Il existe une extension K de k telle que f possède un zéro critique non trivial dans K^n.*

(iii bis) *Il existe une extension K de k, de degré fini, telle que f possède un zéro critique non trivial dans K^n.*

(iii ter) *Une extension algébriquement close L de k étant donnée, il existe un zéro critique non trivial de f dans L^n.*

REMARQUE 1. On a $\mathbf{Z} \cap \mathfrak{e}(J(P_{n,d})) = 0$. En effet, distinguons deux cas. Pour $n = 1$, on a $U_{1,d} = \mathbf{Z}[T]$ et $P_{1,d}(X) = TX^d$, donc $J(P_{1,d})$ est engendré par TX^d et dTX^{d-1} et par conséquent $\mathfrak{e}(J(P_{1,d})) = T\mathbf{Z}[T]$. Pour $n \geqslant 2$, appliquons le scholie avec $k = \mathbf{Q}$ et $f = X_n^d$; puisque f possède le zéro critique $(1, 0, \ldots, 0) \in \mathbf{Q}^n$, $\mathfrak{e}(J(P_{n,d}))$ est contenu dans le noyau de h, mais la restriction de h à $\mathbf{Z}$ est injective.

L'idéal éliminant $\mathfrak{e}(J(P_{n,d})) \subset U_{n,d}$ est premier. Plus généralement:

PROPOSITION 10. *Soit K un anneau intègre. Considérons l'anneau $U = K \otimes_{\mathbf{Z}} U_{n,d}$ et soit $h\colon U_{n,d} \to U$ l'homomorphisme canonique. Alors l'idéal éliminant $\mathfrak{e}(J({}^hP_{n,d})) \subset U$ est premier.*

Démonstration. Notons pour simplifier $P = {}^hP_{n,d}$ et $J = J(P)$. Lorsque $n = 1$, on voit comme dans la remarque précédente que $\mathfrak{e}(J(P))$ est l'idéal $TK[T]$ de $K[T]$, donc est premier. On peut donc supposer $n \geqslant 2$. La démonstration est calquée sur celle de la proposition 3 du n° 3.

Soit $\mathfrak{a}$ l'idéal de $U[X_1, \ldots, X_n]$ formé des a tels que aX_n^m appartienne à J pour m assez grand. Exactement comme dans la proposition 3, il suffit de prouver que $\mathfrak{a}$ *est premier et ne contient aucun des X_i.*

Notons J' l'idéal de $U[X_1, \ldots, X_n]$ engendré par P et les D_iP pour $i < n$. Il résulte immédiatement de l'identité d'Euler que l'on a $X_n D_nP \in J'$, donc $X_nJ \subset J' \subset J$. Ainsi $\mathfrak{a}$ peut aussi être défini comme l'ensemble des $a \in U[X_1, \ldots, X_n]$ tels que aX_n^m appartienne à J' pour m assez grand. Mettons en évidence dans P les termes divisibles par X_n^{d-1} et leurs coefficients (les Y_i de la formule ci-dessous, qui sont certaines des indéterminées de U):

$$P = F(X_1, \ldots, X_n) + Y_1X_1X_n^{d-1} + \cdots + Y_{n-1}X_{n-1}X_n^{d-1} + Y_nX_n^d,$$

où F est de degré $d-2$ en X_n. On a, pour $j = 1, \ldots, n-1$,

$$D_jP = D_jF + Y_jX_n^{d-1}.$$

Mais $U[X_1, \ldots, X_n]$ est de la forme $V[Y_1, \ldots, Y_{n-1}, X_n]$ où V est l'anneau des polynômes à coefficients dans K dont les indéterminées sont tous les

coefficients de P autres que les Y_i, ainsi que les indéterminées X_j pour $j < n$. Les polynômes F et D_jF appartiennent à $V[X_n]$. Les propriétés annoncées de $\mathfrak{a}$ découlent alors directement du lemme 4 du n° 3, appliqué à la suite de polynômes $D_1P, \ldots, D_{n-1}P, P$.

Dans ce qui suit, pour tout anneau A et tout polynôme homogène $f \in A[X_1, \ldots, X_n]$ de degré $\geqslant 2$, nous notons $\Delta_{n,d}(f)$ et $\delta_{n,d}(f)$ les éléments de A définis par

$$\Delta_{n,d}(f) = \operatorname{res}(D_1 f, \ldots, D_{n-1} f, f),$$
$$\delta_{n,d}(f) = \operatorname{res}(D_1 f, \ldots, D_{n-1} f, D_n f).$$

Ils appartiennent par construction à l'idéal éliminant de $J(f)$.

En particulier, $\Delta_{n,d}(P_{n,d})$ et $\delta_{n,d}(P_{n,d})$ sont des éléments de $\mathfrak{e}(J(P_{n,d}))$. Si $h\colon U_{n,d} \to A$ est l'homomorphisme tel que ${}^hP_{n,d} = f$, alors $h(\Delta_{n,d}(P_{n,d})) = \Delta_{n,d}(f)$ et de même $h(\delta_{n,d}(P_{n,d})) = \delta_{n,d}(f)$.

EXEMPLE 1. On a $\Delta_{1,d}(TX^d) = \operatorname{res}(TX^d) = T$ et $\delta_{1,d}(TX^d) = \operatorname{res}(dTX^{d-1}) = dT$. Prenons plus généralement $A = \mathbf{Z}[T_1, \ldots, T_n]$ et $f(X_1, \ldots, X_n) = T_1X_1^d + \cdots + T_nX_n^d$, avec $d \geqslant 2$. On a alors

$$\delta_{n,d}(f) = d^{n(d-1)^{n-1}}(T_1 \cdots T_n)^{(d-1)^{n-1}}.$$

En effet, on a $D_i f = dT_iX_i^{d-1}$ donc, d'après la prop. 5, a) du n° 4, $\delta_{n,d}(f) = \prod_i (dT_i)^{(d-1)^{n-1}}$. Il en résulte notamment que $\delta_{n,d}(P_{n,d})$ n'est pas nul.

EXEMPLE 2. Prenons $A = \mathbf{Z}[T]$ et $f = X_1^d + TX_1X_2^{d-1}$, avec $d \geqslant 2$. On a alors

$$\delta_{2,d}(f) = (1-d)^{d-1}d^{d-2}T^d.$$

En effet, on a d'abord $\delta_{2,d}(f) = \operatorname{res}(dX_1^{d-1} + TX_2^{d-1}, (d-1)TX_1X_2^{d-2})$. Par multiplicativité et homogénéité du résultant relativement au second terme (prop. 5, b) du n° 4), $\delta_{2,d}(f)$ est le produit de $r_0 = (d-1)^{d-1}T^{d-1}$, de $r_1 = \operatorname{res}(dX_1^{d-1} + TX_2^{d-1}, X_1)$ et de $r_2 = \operatorname{res}(dX_1^{d-1} + TX_2^{d-1}, X_2^{d-2})$. Appliquant la prop. 7 du n° 4, on obtient $r_2 = \operatorname{res}(dX_1^{d-1})^{d-2} = d^{d-2}$. Appliquant cette même proposition ainsi que le cor. 3 à la prop. 5 du n° 4, on obtient $r_1 = (-1)^{d-1}\operatorname{res}(X_1, dX_1^{d-1} + TX_2^{d-1}) = (-1)^{d-1}\operatorname{res}(TX_2^{d-1}) = (-1)^{d-1}T$. Reportant les valeurs de r_0, r_1 et r_2 dans la relation $\delta_{2,d}(f) = r_0\, r_1\, r_2$, on obtient le résultat indiqué.

LEMME 9. *Si f est un polynôme homogène de degré $d \geqslant 2$ de $A[X_1, \ldots, X_n]$, $n \geqslant 2$, et si $\bar{f} \in A[X_1, \ldots, X_{n-1}]$ est obtenu en substituant 0 à X_n dans f, on a*

$$d^{(d-1)^{n-1}} \Delta_{n,d}(f) = \delta_{n,d}(f)\, \delta_{n-1,d}(\bar{f})\,.$$

Démonstration. On a successivement

$$\begin{aligned}
d^{(d-1)^{n-1}} \Delta_{n,d}(f) = & \\
&= \operatorname{res}(D_1 f, \ldots, D_{n-1} f, df) && (\text{n}^\text{o}\ 4,\ \text{prop. } 5,\ \text{a}))\\
&= \operatorname{res}(D_1 f, \ldots, D_{n-1} f, X_1 D_1 f + \ldots + X_n D_n f) && (\text{identité d'Euler})\\
&= \operatorname{res}(D_1 f, \ldots, D_{n-1} f, X_n D_n f) && (\text{n}^\text{o}\ 4,\ \text{prop. } 8)\\
&= \operatorname{res}(D_1 f, \ldots, D_{n-1} f, X_n)\, \operatorname{res}(D_1 f, \ldots, D_n f) && (\text{n}^\text{o}\ 4,\ \text{prop. } 5,\ \text{b}))\\
&= \delta_{n-1,d}(\bar{f})\, \delta_{n,d}(f) && (\text{n}^\text{o}\ 4,\ \text{prop. } 7)\,.
\end{aligned}$$

Dans la suite de ce numéro, étant donnés deux entiers $n \geqslant 0$ et $d \geqslant 2$, nous poserons :

$$a(n,d) = \frac{(d-1)^n - (-1)^n}{d}\,,$$
$$s(n,d) = \frac{n(d-1)^{n-1} - a(n,d)}{d}\,.$$

On a $a(0,d) = s(0,d) = 0$, $a(1,d) = 1$, $s(1,d) = 0$ et, pour $n \geqslant 2$,

$$a(n,d) = (d-2).\, a(n-1,d) + (d-1).\, a(n-2,d)\,, \tag{2}$$
$$s(n,d) = (d-1)^{n-2} + (d-2).\, s(n-1,d) + (d-1).\, s(n-2,d)\,, \tag{3}$$

ce qui montre que $a(n,d)$ et $s(n,d)$ sont des entiers $\geqslant 0$. On a par ailleurs,

$$a(n,d) + a(n-1,d) = (d-1)^{n-1}, \quad n \geqslant 1\,. \tag{4}$$

LEMME 10. *Si $f_{n,d} \in \mathbf{Z}[X_1, \ldots, X_n]$ est défini par*

$$f_{n,d}(X_1, \ldots, X_n) = X_1^d + X_1 X_2^{d-1} + X_2 X_3^{d-1} + \ldots + X_{n-1} X_n^{d-1}\,,$$

on a

$$\delta_{n,d}(f_{n,d}) = (1-d)^{(d-1)s(n,d)} d^{\,a(n,d)}.$$

Démonstration. Fixons d. Posons pour simplifier $f_n = f_{n,d}$ et $\delta_n = \delta_{n,d}(f_{n,d})$. On a $f_1 = X_1^d$, donc $\delta_1 = d = d^{a(1,d)}$, et d'après l'exemple 2, $\delta_2 = (1-d)^{d-1} d^{d-2} = (1-d)^{d-1} d^{a(2,d)}$. *Supposons $n > 2$ et raisonnons par*

récurrence. On a $D_n f = (d-1)X_n^{d-2}X_{n-1}$. Par homogénéité et multiplicativité du résultant (prop. 5 du n° 4) , δ_n est le produit de trois termes, à savoir

$$r_0 = (d-1)^{(d-1)^{n-1}},$$
$$r_1 = \mathrm{res}(D_1 f_n, \ldots, D_{n-1} f_n, X_n)^{d-2},$$
$$r_2 = \mathrm{res}(D_1 f_n, \ldots, D_{n-1} f_n, X_{n-1}).$$

Les deux résultants ci-dessus sont justiciables de la proposition 7 du n° 4. Lorsqu'on substitue 0 à X_n dans les $n-1$ premières dérivées de f_n, on trouve les dérivées de f_{n-1}, ce qui donne $r_1 = (\delta_{n-1})^{d-2}$. Pour calculer r_2, commençons par permuter les deux derniers polynômes, ce qui donne (cor. 3 à la prop. 5 du n° 4) $r_2 = \alpha r_2'$ avec $\alpha = (-1)^{(d-1)^n} = (-1)^{d-1}$ et $r_2' = \mathrm{res}(D_1 f_n, \ldots, D_{n-2} f_n, X_{n-1}, D_{n-1} f_n)$. Lorsqu'on substitue 0 à X_{n-1} dans les $n-2$ premières dérivées de f_n, on trouve les dérivées de f_{n-2}. Lorsqu'on substitue 0 à X_{n-1} dans $D_{n-1} f_n$, on obtient X_n^{d-1}, ce qui, par une nouvelle application de la prop. 7, donne $r_2' = (\delta_{n-2})^{d-1}$. On obtient ainsi la formule de récurrence

$$\delta_n = (1-d)^{(d-1)^{n-1}} . (\delta_{n-1})^{d-2} . (\delta_{n-2})^{d-1}.$$

Compte tenu des relations (2) et (3) et de l'hypothèse de récurrence, cela donne bien $\delta_n = (1-d)^{(d-1)s(n,d)} d^{a(n,d)}$.

Rappelons (appendice 1) que l'on appelle *contenu* d'un élément non nul P de la $\mathbf{Z}$-algèbre de polynômes $U_{n,d}$, le plus grand entier (positif) qui divise P.

LEMME 11. *Dans l'anneau $U_{n,d}$, $\Delta_{n,d}(P_{n,d})$ est de contenu* 1 *et $\delta_{n,d}(P_{n,d})$ est de contenu $d^{a(n,d)}$.*

Démonstration. Fixons $d \geqslant 2$. Notons $c(n)$ le contenu de $\delta_{n,d}(P_{n,d})$ et $C(n)$ le contenu de $\Delta_{n,d}(P_{n,d})$. Posons $q_n = \delta_{n,d}(P_{n,d})/c(n) \in U_{n,d}$. Pour tout anneau A et tout polynôme homogène $f \in A[X_1, \ldots, X_n]$ de degré d, on aura

$$\delta_{n,d}(f) = c(n)\tilde{q}_n(f), \tag{5}$$

de sorte que $c(n)$ divise $\delta_{n,d}(f)$. Il résulte alors du lemme 10 qu'il existe des entiers u_n et $s_n \geqslant 0$ avec

$$u_n c(n) = (d-1)^{s_n} d^{a(n,d)}. \tag{6}$$

Appliquant le lemme 9 et le lemme de Gauss (appendice 1), on obtient

$$d^{(d-1)^{n-1}} C(n) = c(n)c(n-1), \tag{7}$$

et donc d'après la relation (6)

$$d^{(d-1)^{n-1}} u_n u_{n-1} C(n) = (d-1)^{s_n+s_{n-1}} d^{\,a(n,d)+a(n-1,d)}.$$

D'après la formule (4), il en résulte qu'on a $u_n u_{n-1} C(n) = (d-1)^{s_n+s_{n-1}}$, ce qui implique que u_n est premier à d. Revenant à (6), on voit alors que $c(n)$ s'écrit $v d^{\,a(n,d)}$, avec v premier à d. Mais l'exemple 1 impose que $c(n)$ divise une puissance de d, donc que $v = 1$. Cela donne la valeur annoncée pour $c(n)$. Reportant dans (7) et appliquant à nouveau (4), on obtient $C(n) = 1$.

DÉFINITION 4. Soient A un anneau, $n \geqslant 1$ un entier et f un polynôme homogène de degré $d \geqslant 2$ de $A[X_1, \ldots, X_n]$. On appelle *discriminant divisé* de f, ou simplement *discriminant* de f, et on note $\mathrm{disc}(f)$ l'élément $\tilde{u}(f)$ de A, où u est l'élément de $U_{n,d}$ défini par

$$d^{\,a(n,d)} u = \mathrm{res}(D_1 P_{n,d}, \ldots, D_n P_{n,d}).$$

En particulier, l'élément $u = \mathrm{disc}(P_{n,d})$ de $U_{n,d}$ est appelé le *discriminant (divisé) universel*. C'est par construction un polynôme à coefficients entiers de contenu 1. Il est homogène de degré $n(d-1)^{n-1}$.

REMARQUE 2. Puisque l'idéal $\mathfrak{e}(J(P_{n,d}))$ est premier (prop. 10) et ne contient pas l'entier $d^{\,a(n,d)}$ (remarque 1), il contient $\mathrm{disc}(P_{n,d})$. Nous verrons ci-dessous (n° 6, cor. 1 à la prop. 14) qu'en fait le polynôme $\mathrm{disc}(P_{n,d})$ engendre l'idéal $\mathfrak{e}(J(P_{n,d}))$.

REMARQUE 3. Compte tenu de l'identité (4), la relation du lemme 9 peut aussi s'écrire $\Delta_{n,d}(f) = \mathrm{disc}(f)\,\mathrm{disc}(\bar{f})$.

EXEMPLE 3. On a $\mathrm{disc}(\lambda X^d) = \lambda$. Plus généralement, on a d'après l'exemple 1, et la relation $n(d-1)^{n-1} - a(n,d) = ds(n,d)$:

$$\mathrm{disc}(\lambda_1 X_1^d + \cdots + \lambda_n X_n^d) = d^{\,ds(n,d)} (\lambda_1 \cdots \lambda_n)^{(d-1)^{n-1}}.$$

EXEMPLE 4. Avec les notations du lemme 10, on a

$$\mathrm{disc}(f_{n,d}) = (1-d)^{(d-1)s(n,d)}.$$

EXEMPLE 5. Prenons $n = 2$. Comme dans l'exemple 3 du n° 4, associons à $f(X_1, X_2)$ le polynôme en une variable $f^{\flat}(X) = f(X, 1)$. Considérons le discriminant $\mathrm{dis_d}(f^{\flat})$ introduit en [Bou07b], A, IV, p. 79, formule (52). Compte

tenu de ce qui a été établi dans l'exemple cité, de la remarque 3 et de la formule (54) de *loc. cit.*, on voit qu'on a

$$\mathrm{disc}(f) = (-1)^{d(d-1)/2}\mathrm{dis_d}(f^b)\,.$$

EXEMPLE 6. Prenons $d = 2$, donc (n° 2, exemple 3)

$$P_{n,2}(X_1, \ldots, X_n) = \sum_i T_{\{i\}} X_i^2 + \sum_{\{i,j\}} T_{\{i,j\}} X_i X_j\,.$$

Soit M la matrice carrée d'ordre n telle que $M_{ii} = 2T_{\{i\}}$ et $M_{ij} = T_{\{i,j\}}$ pour $i \neq j$. On a $D_i P_{n,2} = \sum_j M_{ij} X_j$, donc $\mathrm{res}(D_1 P_{n,2}, \ldots, D_n P_{n,2}) = \det(M)$ d'après l'exemple 1 du n° 4. On a ainsi $\mathrm{disc}(P_{n,2}) = \det(M_{ij})$ lorsque n est pair et $\mathrm{disc}(P_{n,2}) = \frac{1}{2}\det(M_{ij})$ lorsque n est impair.

PROPOSITION 11. *Soient A un anneau, $n \geqslant 1$ un entier et f un polynôme homogène de degré $d \geqslant 2$ de $A[X_1, \ldots, X_n]$.*

a) *Pour tout homomorphisme d'anneaux $h\colon A \to B$, on a*

$$\mathrm{disc}({}^h f) = h(\mathrm{disc}(f))\,.$$

b) *On a*

$$\mathrm{res}(D_1 f, \ldots, D_n f) = d^{\,a(n,d)}\,\mathrm{disc}(f)\,.$$

c) *Pour tout $\lambda \in A$, on a*

$$\mathrm{disc}(\lambda f) = \lambda^{n(d-1)^{n-1}}\,\mathrm{disc}(f)\,.$$

d) *Si $n \geqslant 2$ et si $\bar{f} \in A[X_1, \ldots, X_{n-1}]$ est obtenu en substituant 0 à X_n dans f, on a*

$$\mathrm{res}(D_1 f, \ldots, D_{n-1} f, f) = \mathrm{disc}(f)\,\mathrm{disc}(\bar{f})\,.$$

e) *Soit (a_{ij}) une matrice carrée d'ordre n à coefficients dans A. Posons*

$$f'(X_1, \ldots, X_n) = f\Big(\sum_j a_{1j} X_j, \ldots, \sum_j a_{nj} X_j\Big)\,.$$

On a

$$\mathrm{disc}(f') = \det(a_{ij})^{d(d-1)^{n-1}}\,\mathrm{disc}(f)\,.$$

Démonstration. Les propriétés a) et b) résultent de la définition. La propriété d) a déjà été énoncée (remarque 3). Compte tenu de a), il suffit de prouver c) lorsque $A = U_{n,d}$ et $f = P_{n,d}$; mais, puisque d ne divise pas 0 dans A, c) résulte de b) et de la proposition 5, a) du n° 4.

De même, pour démontrer e), il suffit de le faire dans le cas où A est l'algèbre de polynômes $U_{n,d}[(Z_{ij})]$, où les Z_{ij} sont n^2 nouvelles indéterminées, avec $f = P_{n,d}$ et $a_{ij} = Z_{ij}$. On peut alors se placer dans le corps de fractions de A, ce qui nous ramène au cas où A est un corps de caractéristique 0 et il suffit de prouver dans ce cas qu'on a

$$\operatorname{res}(D_1 f', \dots, D_n f') = \det(a_{ij})^{d(d-1)^{n-1}} \operatorname{res}(D_1 f, \dots, D_n f)\,.$$

Mais, si cette relation est vraie pour deux matrices, elle est vraie pour leur produit. Il résulte alors de la prop. 14 de [Bou07a], A, II, p. 161 qu'il suffit de considérer les deux cas suivants :

1) il existe des entiers i et j, avec $i \neq j$, et un scalaire $\lambda \in A$ tels que $f'(X_1, \dots, X_n) = f(X_1, \dots, X_{i-1}, X_i + \lambda X_j, X_{i+1}, \dots, X_n)$, et il faut démontrer que l'on a $\operatorname{res}(D_1 f', \dots, D_n f') = \operatorname{res}(D_1 f, \dots, D_n f)$;

2) il existe des scalaires $\lambda_i \in A$, $i = 1, \dots, n$ tels que $f'(X_1, \dots, X_n) = f(\lambda_1 X_1, \dots, \lambda_n X_n)$, et il faut démontrer que l'on a $\operatorname{res}(D_1 f', \dots, D_n f') = (\lambda_1 \cdots \lambda_n)^{d(d-1)^{n-1}} \operatorname{res}(D_1 f, \dots, D_n f)$.

Dans le premier cas, on applique les prop. 8 et 9 du n° 4. Traitons le second. On a $D_j f'((X_i)) = \lambda_j D_i f((\lambda_i X_i))$. De la prop. 5 du n° 4, on tire alors

$$\operatorname{res}(D_1 f', \dots, D_n f') = (\lambda_1 \cdots \lambda_n)^{(d-1)^{n-1}} \operatorname{res}\big(D_1 f((\lambda_i X_i)), \dots, D_n f((\lambda_i X_i))\big),$$

tandis que la prop. 9 du n° 4 implique

$$\operatorname{res}\big(D_1 f((\lambda_i X_i)), \dots, D_n f((\lambda_i X_i))\big) = (\lambda_1 \cdots \lambda_n)^{(d-1)^n} \operatorname{res}(D_1 f, \dots, D_n f)\,.$$

On conclut en notant que $(d-1)^{n-1} + (d-1)^n = d(d-1)^{n-1}$.

REMARQUE 4. Puisque $d(d-1)^{n-1}$ est pair lorsque $n \geqslant 2$, il résulte de e) que le discriminant d'un polynôme ne dépend pas de l'ordre choisi sur les indéterminées.

REMARQUE 5. Appliquant e) comme dans la remarque 4 du n° 4, on voit que le discriminant universel $\operatorname{disc}(P_{n,d})$ est multihomogène de degré $(d(d-1)^{n-1}, \dots, d(d-1)^{n-1})$ pour la multigraduation dans laquelle le coefficient de $\mathbf{X}^{\boldsymbol{\alpha}}$ dans $P_{n,d}$ est de degré $\boldsymbol{\alpha}$.

REMARQUE 6. Le degré d étant fixé, notons pour simplifier $R_n \in U_{n,d}$ l'élément $\Delta_{n,d}(P_{n,d}) = \operatorname{res}(D_1 P_{n,d}, \dots, D_{n-1} P_{n,d}, P_{n,d})$. D'après la partie d) de la proposition, on a pour tout $n > 1$, $\operatorname{disc}(P_{n,d}) \operatorname{disc}(P_{n-1,d}) = R_n$, et on a vu que $\operatorname{disc}(P_{1,d}) = R_1$. Il s'ensuit que le discriminant universel peut s'exprimer

comme le produit alterné

$$\operatorname{disc}(P_{n,d}) = \frac{R_n R_{n-2} \cdots}{R_{n-1} \cdots} = \prod_{i=0,\ldots,n-1} (R_{n-i})^{(-1)^i}.$$

Fixons deux entiers $n \geqslant 1$ et $d \geqslant 2$. Nous allons démontrer simultanément les deux propositions suivantes :

PROPOSITION 12. *Soient k un corps et f un polynôme homogène de degré d de $k[X_1, \ldots, X_n]$. Pour qu'il existe une extension L de k telle que f possède un zéro critique non trivial dans L^n, il faut et il suffit que* $\operatorname{disc}(f) = 0$ *et, s'il en est ainsi, on peut prendre L de degré fini sur k.*

PROPOSITION 13. *Soit K un corps. Considérons la K-algèbre de polynômes $U = K \otimes_{\mathbf{Z}} U_{n,d}$. Il existe un polynôme irréductible $q \in U$, un scalaire $\alpha \in K^\star$ et un entier $m > 0$ tels que* $\operatorname{disc}(P_{n,d}.1_K) = \alpha q^m$ *et* $\mathfrak{e}(J(P_{n,d}.1_K)) = qU$.

Considérons d'abord l'anneau $U_{n,d}$, l'idéal $\mathfrak{a} = \mathfrak{e}(J(P_{n,d}))$ et l'élément $\operatorname{disc}(P_{n,d})$. On sait déjà que $\mathfrak{a}$ est premier (prop. 10) et contient $\operatorname{disc}(P_{n,d})$ (remarque 2).

LEMME 12. *Il existe un polynôme premier $q \in U_{n,d}$ et un entier $m > 0$ tels que $\mathfrak{a} = qU_{n,d}$ et* $\operatorname{disc}(P_{n,d}) = \pm q^m$.

Démonstration. Soit $q \in U_{n,d}$ un diviseur premier (c'est-à-dire irréductible et de contenu 1) de $\operatorname{disc}(P_{n,d})$. Notons F le corps des fractions de l'anneau intègre $U_{n,d}/qU_{n,d}$ et $h\colon U_{n,d} \to F$ l'homomorphisme canonique, et soit $f = {}^hP_{n,d} \in k[X_1, \ldots, X_n]$. On a $\operatorname{disc}(f) = h(\operatorname{disc}(P_{n,d})) = 0$, donc $\operatorname{res}(D_1 f, \ldots, D_n f) = 0$. Il existe donc une extension L de F telle que les $D_i f$ aient un zéro commun non trivial $\xi \in L^n$. Mais, d'après le lemme de Gauss (appendice 1), le contenu de q doit diviser celui de $\operatorname{disc}(P_{n,d})$, qui est égal à 1 ; l'homomorphisme canonique de $\mathbf{Z}$ dans $U_{n,d}/qU_{n,d}$ est donc injectif, de sorte qu'on a $d.1_F \neq 0$. L'identité d'Euler implique alors que ξ est un zéro critique (non trivial) de f. Il s'ensuit par le scholie de ce numéro que l'on a $h(\mathfrak{a}) = 0$, c'est-à-dire $\mathfrak{a} \subset qU_{n,d}$.

Écrivons alors $\operatorname{disc}(P_{n,d})$ comme un produit $q_1 \cdots q_m$ de facteurs premiers. L'idéal premier $\mathfrak{a}$ contient le produit $q_1 \cdots q_m$ et, d'après ce qu'on vient de voir, est contenu dans chacun des $q_i U_{n,d}$; il s'ensuit que les q_i sont tous associés, c'est-à-dire égaux au signe près. Si q est l'un d'entre eux, on a donc $\operatorname{disc}(P_{n,d}) = \pm q^m$ et $\mathfrak{a} = qU_{n,d}$.

Ce lemme étant acquis, démontrons maintenant les propositions 12 et 13.

Démonstration. Avec les notations de la proposition 12, considérons l'homomorphisme $h\colon U_{n,d} \to k$ tel que $f = {}^hP_{n,d}$. On a $\operatorname{disc}(f) = \pm\tilde{q}(f)^m$. Il est donc équivalent de dire que $\operatorname{disc}(f) = 0$, ou que $\tilde{q}(f) = 0$, ou encore que l'homomorphisme canonique $h\colon U_{n,d} \to F$ annule q, donc annule $\mathfrak{a}$. La proposition résulte alors directement du même scholie que précédemment.

Passons à la proposition 13. Posons $P = {}^hP_{n,d}$ et $\mathfrak{a} = \mathfrak{e}(J(P)) \subset U$. On a $\operatorname{disc}(P) \in \mathfrak{a}$, puisque $\operatorname{disc}(P) = h(\operatorname{disc}(P_{n,d}))$ et que $h(\mathfrak{e}(J(P_{n,d})))$ est contenu dans $\mathfrak{e}(J(P))$, et on sait déjà que $\mathfrak{a}$ est premier (prop. 10). Soit $q \in U$ un facteur irréductible de $\operatorname{disc}(P)$. Soit k le corps des fractions de l'anneau intègre U/qU et soit $h'\colon U \to k$ l'homomorphisme canonique. Comme $h'(\operatorname{disc}(P)) = 0$, il existe d'après la proposition 12 une extension L de k telle que le polynôme P ait un zéro critique non trivial dans L^n, ce qui implique, toujours d'après le même scholie, que l'on a $h'(\mathfrak{a}) = 0$, c'est-à-dire $\mathfrak{a} \subset qU$. Raisonnant alors exactement comme dans le lemme précédent, on en conclut qu'il existe un polynôme irréductible $q \in U$, un entier $m > 0$ et un élément inversible α de K tels que $\mathfrak{a} = qU$ et $\operatorname{disc}(P) = \alpha q^m$. Cela achève la démonstration des propositions 12 et 13.

COROLLAIRE. *Soit K un corps. Supposons qu'il existe une K-algèbre A et un polynôme homogène $f \in A[X_1, \ldots, X_n]$ de degré d tel que l'élément* $\operatorname{disc}(f) \in A$ *ne puisse s'écrire sous la forme αa^m, avec $\alpha \in K^\star$, $a \in A$ et $m > 1$. Alors le polynôme* $\operatorname{disc}(P_{n,d}).1_K \in K \otimes_{\mathbf{Z}} U_{n,d}$ *est irréductible et engendre l'idéal éliminant $\mathfrak{e}(J(P_{n,d}.1_K))$.*

Démonstration. Appliquons la proposition 13. Il existe un homomorphisme $h\colon K \otimes U_{n,d} \to A$ tel que ${}^h(P_{n,d}.1_K) = f$, donc $\operatorname{disc}(f) = \alpha h(q)^m$. On a alors nécessairement $m = 1$, donc $\operatorname{disc}(P_{n,d}).1_K = \alpha q$.

6. IRRÉDUCTIBILITÉ DU DISCRIMINANT

Soit K un corps. Considérons la K-algèbre de polynômes $A = K[Z_1, \ldots, Z_n]$ et le polynôme

$$P(X_1, \ldots, X_n) = \sum_i X_i^d - (Z_1X_1 + \cdots + Z_nX_n)^d \in A[X_1, \ldots, X_n]\,.$$

Nous démontrerons ci-dessous le lemme suivant :

LEMME 13. *Si la caractéristique de K ne divise ni d, ni $d-1$, l'élément* $\mathrm{disc}(P)$ *de* $K[Z_1,\dots,Z_n]$ *est irréductible.*

Appliquant le corollaire à la proposition 13, on en déduit :

PROPOSITION 14. *Soit K un corps dont la caractéristique ne divise ni d ni $d-1$. Alors le polynôme* $\mathrm{disc}(P_{n,d}).1_K \in K \otimes U_{n,d}$ *est irréductible et engendre l'idéal éliminant* $\mathfrak{e}(J(P_{n,d}.1_K))$.

COROLLAIRE 1. *Le discriminant universel* $\mathrm{disc}(P_{n,d})$ *est premier et engendre l'idéal éliminant* $\mathfrak{e}(J(P_{n,d}))$.

Démonstration. Appliquons la proposition 14 avec $K = \mathbf{Q}$. Puisque $\mathrm{disc}(P_{n,d})$ est irréductible comme polynôme à coefficients rationnels et de contenu 1, il est premier. Il engendre donc $\mathfrak{e}(J(P_{n,d}))$ d'après le lemme 12.

COROLLAIRE 2. *Soit $u \in U_{n,d}$. Les conditions suivantes sont équivalentes :*

(i) *L'élément u est divisible par* $\mathrm{disc}(P_{n,d})$.

(ii) *Pour tout corps K et tout polynôme homogène f de degré d de $K[X_1,\dots,X_n]$ possédant un zéro critique non trivial dans K^n, on a $\tilde{u}(f)=0$.*

Démonstration. (i) $\Rightarrow$ (ii) : cela résulte de la prop. 12.

(ii) $\Rightarrow$ (i) : l'anneau quotient $U_{n,d}/\mathrm{disc}(P_{n,d})U_{n,d}$ est intègre, soient k son corps des fractions, $h\colon U_{n,d} \to k$ l'homomorphisme canonique et $f = {}^hP_{n,d}$. On a $\mathrm{disc}(f)=0$. Appliquant à f la proposition 12, on voit qu'il existe une extension K de k telle que f possède un zéro critique non trivial dans K^n. La condition (ii) implique alors $\tilde{u}(f).1_K = 0$, donc $\tilde{u}(f)=0$. Mais on a $\tilde{u}(f) = h(u)$, donc $u \in \ker(h) = \mathrm{disc}(P_{n,d})U$.

Démonstration du lemme 13. On a $D_iP = dQ_i$, avec

$$Q_i = X_i^{d-1} - Z_i(Z_1X_1 + \cdots + Z_nX_n)^{d-1},$$

donc $d^{\,a(n,d)}\,\mathrm{disc}(P) = \mathrm{res}((D_iP)) = d^{n(d-1)^{n-1}}\,\mathrm{res}((Q_i))$ d'après la proposition 5, a) du n° 4. Si l'on note $\Delta(Z_1,\dots,Z_n) \in \mathbf{Z}[Z_1,\dots,Z_n]$ le résultant des Q_i, on a donc

$$\mathrm{disc}(P) = d^s\Delta(Z_1,\dots,Z_n) \quad \text{avec} \quad s = n(d-1)^{n-1} - a(n,d).$$

Notons au passage que le terme constant de Δ s'obtient en annulant les Z_i, donc est égal à 1 en vertu de l'exemple 3 du n° 5. Puisque d est inversible

dans K, il s'agit de prouver que Δ est irréductible, ce qui nous ramène au lemme suivant :

LEMME 14. *Si la caractéristique de K ne divise ni d, ni $d-1$, le polynôme Δ est irréductible dans $K[Z_1, \ldots, Z_n]$.*

Démonstration. Quitte à remplacer K par une extension convenable, on peut supposer qu'il possède une racine primitive $d-1$-ième de l'unité ([Bou07b], A, V, p. 77, prop. 4). Soit ζ une telle racine, de sorte qu'on a dans $K[X]$

$$X^{d-1} - 1 = \prod_{j=0,\ldots,d-2} (X - \zeta^j) .$$

Rappelons qu'on a noté A l'anneau $K[Z_1, \ldots, Z_n]$. Introduisons une deuxième série d'indéterminées $(T_1, \ldots, T_n)$, posons $B = K[T_1, \ldots, T_n]$ et soit $h\colon A \to B$ l'homomorphisme qui applique Z_i sur T_i^{d-1} pour chaque i. Posons

$$L(X_1, \ldots, X_n) = {}^h(\sum_i Z_i X_i) = \sum_i T_i^{d-1} X_i ,$$

de sorte que

$$\Delta(T_1^{d-1}, \ldots, T_n^{d-1}) = \mathrm{res}(X_1^{d-1} - (T_1 L)^{d-1}, \ldots, X_n^{d-1} - (T_n L)^{d-1}) .$$

Mais on a des décompositions en produit de formes linéaires

$$X_i^{d-1} - (T_i L)^{d-1} = \prod_{j_i=0,\ldots,d-2} (X_i - \zeta^{j_i} T_i L) .$$

En vertu de la proposition 5, b) du n° 4 (multiplicativité du résultant) et de l'exemple 1 du n° 4, le résultant de ces polynômes s'exprime donc comme produits de $(d-1)^n$ déterminants de formes linéaires. D'après le lemme 15 ci-dessous, on obtient dans $K[T_1, \ldots, T_n]$ la relation :

$$\Delta(T_1^{d-1}, \ldots, T_n^{d-1}) = \prod_{i=1,\ldots,n} \prod_{j_i=1,\ldots,d-1} (1 - \sum_i \zeta^{j_i} T_i^d) . \tag{8}$$

Mais les divers facteurs $(1 - \sum_i \zeta^{j_i} T_i^d)$ du produit précédent sont distincts deux à deux. Puisque $n > 1$, ils sont irréductibles dans $B = K[T_1, \ldots, T_n]$, d'après le lemme 16 ci-dessous, de sorte que la relation (8) fournit la décomposition du premier membre en polynômes irréductibles.

Soit $Q = Q(Z_1, \ldots, Z_n)$ un diviseur non constant de Δ dans $K[Z_1, \ldots, Z_n]$, qu'on peut supposer être de terme constant égal à 1. Alors $Q(T_1^{d-1}, \ldots, T_n^{d-1})$ divise le produit précédent, donc est le produit d'une partie non-vide de la décomposition précédente. Mais le polynôme $Q(T_1^{d-1}, \ldots, T_n^{d-1})$ reste

inchangé si l'on y substitue à chaque T_i un produit $\zeta^{k_i} T_i$. Une telle substitution remplace le facteur $(1 - \sum_i \zeta^{j_i} T_i^d)$ par $(1 - \sum_i \zeta^{j_i + k_i} T_i^d)$. Ces substitutions opérant transitivement dans l'ensemble des facteurs, il en résulte que la partie considérée est totale, donc que $Q = \Delta$, ce qui achève la démonstration.

On a utilisé ci-dessus les deux résultats suivants :

LEMME 15. *Soient (a_i) et (l_i) deux familles de n éléments d'un anneau et soit L la forme linéaire $\sum l_i X_i$. Le déterminant des n formes linéaires $L_i = X_i - a_i L$ dans la base (X_i) est égal à $1 - \sum_i a_i l_i$.*

Démonstration. Dans l'algèbre extérieure, on a $L \wedge L = 0$, donc

$$L_1 \wedge \ldots \wedge L_n = X_1 \wedge \ldots \wedge X_n - \sum_i a_i X_1 \wedge \ldots \wedge L \wedge \ldots \wedge X_n$$
$$= (1 - \sum_i a_i l_i) X_1 \wedge \ldots \wedge X_n .$$

LEMME 16. *Soient K un corps, $d > 0$ un entier tel que $d.1_K \neq 0$, et $a_1, \ldots, a_n$ des éléments de K dont au moins deux sont non nuls. Alors le polynôme $P = 1 + \sum_i a_i X_i^d$ est irréductible dans $K[X_1, \ldots, X_n]$.*

Démonstration. On peut supposer que a_1 et a_2 sont non nuls et, en l'étendant si nécessaire, que le corps K contient d racines d-ièmes de l'unité. Notons L le corps des fractions rationnelles à coefficients dans K en les indéterminées $X_2, \ldots, X_n$. Alors P s'écrit $a_1(X_1^d + b)$, avec $b = 1/a_1 + \sum_{i>1} a_i/a_1 X_i^d \in L$. Si P n'était pas irréductible dans $K[X_1, \ldots, X_n]$, alors $X_1^d + b$ ne serait pas irréductible dans $L[X_1]$ et il existerait, d'après le lemme 17 ci-dessous, un diviseur $m > 1$ de d et un élément $c \in L$ avec $b = c^m$. Or b étant un polynôme, c en est aussi un, puisque l'anneau $K[X_2, \ldots, X_n]$ est factoriel. Substituant 0 aux X_i pour $i > 2$ dans la relation précédente, on obtient une relation $1 + a_2 X_2^d = a_1 Q(X_2)^m$, avec $Q \in K[X_2]$. Par hypothèse, a_1, a_2, $d.1_K$ et $m.1_K$ sont non nuls. Dérivant, on voit que $Q(X_2)$ divise à la fois $1 + a_2 X_2^d$ et X_2^{d-1}, ce qui est impossible.

LEMME 17. *Soit L un corps et soit $d > 0$ un entier tel que $d.1_L \neq 0$ et que L contienne d racines d-ièmes de l'unité. Soit a un élément de L tel que le polynôme $P = X^d + a$ ne soit pas irréductible dans $L[X]$. Il existe un diviseur $m > 1$ de d et un élément b de L tels que $a = b^m$.*

Démonstration. Soit $Q = c_0X^n + \cdots + c_n$ un diviseur irréductible de P, avec $0 < n < d$. Pour toute racine d-ième ζ de l'unité, posons $Q_\zeta(X) = Q(\zeta X)$. C'est un diviseur irréductible de P. Il s'écrit

$$Q_\zeta(X) = c_0\zeta^n X^n + \cdots + c_n\,.$$

Les Q_ζ distincts sont en nombre au moins égal à celui des ζ^n et ont tous le même terme constant non nul, donc ne sont pas associés. Ainsi leur produit divise P, et leur nombre est au plus égal à d/n. Mais, si on note δ le pgcd de n et d, les ζ^n décrivent les racines de l'unité d'ordre d/δ. On obtient l'inégalité $d/\delta \leqslant d/n$, soit $n \leqslant \delta$ et en définitive $n = \delta$. Ainsi n divise d. Posons $m = d/n$ et, pour chaque racine m-ième de l'unité θ, choisissons l'un des polynômes Q_ζ avec $\zeta^n = \theta$. On obtient ainsi m polynômes de degré n dont le produit divise P, ce qui donne une décomposition de P, indexée par les racines m-ièmes de l'unité

$$X^n + a = c\prod_\theta (c_0\theta X^n + \cdots + c_n)\,.$$

Les termes extrêmes donnent alors $cc_0^m = 1$ et $cc_n^m = a$, donc $a = (c_n/c_0)^m$. Nous avons ainsi achevé la démonstration du lemme et par conséquent celle de la proposition 14.

EXEMPLE. Prenons $n = 2$ et $d = 3$, soit $P(X, Y) = X^3 + Y^3 - (aX + bY)^3$. On obtient $\mathrm{disc}(P) = 3^5\Delta(a, b)$, avec $\Delta = \prod(1 \pm a^{3/2} \pm b^{3/2})$, où le produit est étendu aux quatre choix de signes. Un calcul immédiat donne $\Delta = (a^3 + b^3 - 1)^2 - 4a^3b^3$.

APPENDICE 1 : ANNEAUX FACTORIELS

On rassemble dans cet appendice les énoncés de divisibilité utilisés dans le texte.

Soit A un anneau intègre. On dit que deux éléments non nuls a et b de A sont *associés* si les idéaux Aa et Ab sont égaux, c'est-à-dire si l'un est le produit de l'autre et d'un élément inversible, ou encore si chacun divise l'autre.

Un élément p de A est dit *premier* s'il est non nul et si l'idéal principal pA est premier, ce qui signifie que p n'est pas inversible et que, chaque fois qu'il divise un produit, il divise l'un des facteurs. En particulier, si un élément premier p divise un élément premier q, alors p et q sont associés. En effet, écrivons $q = ap$; comme q divise ap et ne divise pas a, il divise p ; de même p divise q.

On dit que A est *factoriel* si tout élément non nul et non inversible peut s'écrire comme produit d'une famille finie d'éléments premiers. Par exemple, un corps est factoriel et ne possède aucun élément premier, l'anneau $\mathbf{Z}$ est factoriel et ses éléments premiers sont les entiers naturels premiers et leurs opposés.

Supposons A factoriel et soient $x = p_1 \cdots p_r$ et $x = q_1 \cdots q_s$ deux décompositions d'un même élément non nul et non inversible x de A en produit d'éléments premiers. Alors $r = s$ et il existe une permutation σ telle que p_i soit associé à $q_{\sigma(i)}$ pour tout i. En effet, p_1 divise le produit des q_j, donc l'un des q_j, donc lui est associé. Écrivant $p_1 = uq_j$, on conclut par récurrence, en considérant les deux décompositions de x/p_1 et $x/(uq_j)$. Plus généralement, et par la même démonstration, si $p_1 \cdots p_r$ divise $q_1 \cdots q_s$, il existe une injection $\sigma\colon [1, r] \to [1, s]$ telle que p_i soit associé à $q_{\sigma(i)}$ pour tout i.

Ce résultat d'unicité (à des éléments inversibles près) montre que la définition donnée ci-dessus des anneaux factoriels équivaut à celle de [Bou06b], AC, VII, § 3 (voir notamment la prop. 2 de *loc. cit.* n° 3) et permet de faire fonctionner le mécanisme usuel de *plus grand commun diviseur* et *plus petit commun multiple* (cf. [Bou07b], A, VI, § 1, n° 8).

Si A est factoriel, l'anneau de polynômes $A[X_1, \ldots, X_n]$ est factoriel (voir par exemple [Bou06b], AC, VII, § 3, n° 5, cor. au th. 2). En particulier, les anneaux de polynômes $\mathbf{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$, où K est un corps, sont factoriels. Les éléments premiers de $K[X_1, \ldots, X_n]$ sont appelés polynômes *irréductibles*.

Soit A un anneau factoriel et soit $P \in A[X_1, \ldots, X_n]$ un polynôme non nul. On appelle *contenu* de P un pgcd c de ses coefficients. Alors P est le produit de $c \in A$ et du polynôme P/c de contenu 1. Les éléments premiers non constants de $A[X_1, \ldots, X_n]$ sont les polynômes P qui sont de contenu 1 et qui sont irréductibles dans $K[X_1, \ldots, X_n]$, où K est le corps des fractions de A. Le *lemme de Gauss* affirme que le contenu d'un produit est le produit des contenus. De manière équivalente, si les polynômes P et Q sont de contenu 1, alors leur produit est de contenu 1. En effet, si un élément premier m de A divisait le contenu de PQ, on obtiendrait par passage au quotient deux éléments non nuls et de produit nul de l'anneau intègre $(A/mA)[X_1, \ldots, X_n]$.

APPENDICE 2 : THÉORÈME DES ZÉROS

THÉORÈME. — *Soient k un corps et K une extension de k qui est une k-algèbre de type fini. Alors K est une extension algébrique de degré fini.*

Démonstration. Soit S une partie finie de K l'engendrant comme k-algèbre. Raisonnons par récurrence sur le cardinal de S. Soit x un élément de S, notons $k(x)$ la sous-extension engendrée par x. D'après l'hypothèse de récurrence, K est une extension de degré fini de $k(x)$. Il suffit de prouver que x est algébrique sur k, puisqu'alors $k(x)$ est une extension de degré fini de k.

Supposons donc x transcendant, de sorte que $k(x)$ est le corps des fractions de l'algèbre de polynômes $A = k[x]$. Soit $(e_i)_{1\leq i\leq n}$ une base (finie) du $k(x)$-espace vectoriel K telle que $e_1 = 1$. Tout élément de K s'exprime comme une combinaison linéaire des e_i dont les coefficients sont des quotients de deux éléments de A. Soit $p(x) \in A$ un dénominateur commun à toutes les coordonnées de tous les éléments $s.t$ pour s et t dans $S \cup \{1\}$. Considérons le sous-anneau B de $k(x)$ formé des fractions dont le dénominateur est une puissance de $p(x)$. L'ensemble des combinaisons linéaires des e_i à coefficients dans B est un sous-anneau contenant k et S, donc est égal à K. En particulier $k(x) = k(x)e_1$ est contenu dans $Be_1 = B$ et on en déduit $k(x) = B$.

Mais cela est absurde. Soit en effet $q(x)$ un polynôme non constant de $k[x] = A$. L'élément $1/q(x)$ de $k(x)$ peut s'écrire sous la forme d'une fraction $a(x)/p(x)^n$, ce qui signifie que $q(x)$ divise une puissance de $p(x)$, ce qui est évidemment exclus pour $q(x) = xp(x) + 1$.

COROLLAIRE (THÉORÈME DES ZÉROS). — *Soient k un corps, L une extension algébriquement close de k, A une k-algèbre de type fini et I un idéal de A distinct de A. Il existe un homomorphisme de k-algèbres $h\colon A \to L$ tel que $h(I) = 0$.*

Démonstration. Soit $\mathfrak{m}$ un idéal maximal de A contenant I ([Bou07a], A, I, p. 99, th. 1) et soit K le corps $A/\mathfrak{m}$. Alors K est de degré fini sur k d'après le théorème et il existe un homomorphisme de k-algèbres, nécessairement injectif, de K dans L ([Bou07b], A, V, p. 20, th. 1). L'homomorphisme composé $A \to A/m \to L$ annule $\mathfrak{m}$, donc I.

BIBLIOGRAPHIE

[Bou06a] BOURBAKI, N. *Algèbre Commutative, chapitres 1 à 4*. Springer-Verlag, Berlin-Heidelberg, 2006. Réimpression inchangée de l'édition originale (Hermann, Paris, 1961).

[Bou06b] —— *Algèbre Commutative, chapitres 5 à 7*. Springer-Verlag, Berlin-Heidelberg, 2006. Réimpression inchangée de l'édition originale (Hermann, Paris, 1975).

[Bou07a] —— *Algèbre, chapitres 1 à 3*. Springer-Verlag, Berlin-Heidelberg, 2007. Réimpression inchangée de la 2ème édition (Hermann, Paris, 1970).

[Bou07b] —— *Algèbre, chapitres 4 à 7*. Springer-Verlag, Berlin-Heidelberg, 2007. Réimpression inchangée de la 2ème édition (Masson, Paris, 1981).

[GKZ08] GELFAND, I. M., M. M. KAPRANOV and A. V. ZELEVINSKY. *Discriminants, Resultants and Multidimensional Determinants*. Reprint of the 1994 edition. Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, 2008.

[Jou80] JOUANOLOU, J.-P. Idéaux résultants. *Adv. Math. 37* (1980), 212–238.

[Jou91] —— Le formalisme du résultant. *Adv. Math. 90* (1991), 117–263.

[Jou97] —— Formes d'inertie et résultant : un formulaire. *Adv. Math. 126* (1997), 119–250.

[Sai] SAITO, T. The discriminant and the determinant of a hypersurface of even dimension. Preprint arXiv : 1110.1717 (2011–12).

(Reçu le 24 octobre 2011)

Michel Demazure

e-mail : michel@demazure.com