Résultants

Préparation à l'agrégation, 29 mars 2016

Antoine Chambert-Loir

Résumé. — Définition et propriétés élémentaires du résultant de deux polynômes en une indéterminée, discriminant. Applications à la loi de réciprocité quadratique et au théorème des zéros de Hilbert.

1. Définition et propriété principale

Définition 1.1. — *Soit A un anneau (commutatif et unitaire). Soit $P, Q \in A[T]$ des polynômes en une indéterminée T à coefficients dans A ; soit m, n des entiers $\geqslant 0$ tels que $\deg(P) \leqslant m$ et $\deg(Q) \leqslant n$. On appelle* résultant *(en degrés (m,n)) de P et Q le déterminant de l'application linéaire*

$$\Phi_{P,Q} \colon A[T]_{<n} \times A[T]_{<m} \to A[T]_{<m+n}, \qquad (U,V) \mapsto UP + VQ$$

dans les bases $(1, T, \dots, T^{n-1}; 1, T, \dots, T^{m-1})$ de $A[T]_{<n} \times A[T]_{<m}$ et $(1, T, \dots, T^{m+n-1})$ de $A[T]_{<m+n}$. On le note $\operatorname{Res}_{m,n}(P,Q)$.

Remarque 1.2. — Supposons que $P = a_0 + a_1 T + \dots + a_m T^m$ et $Q = b_0 + b_1 T + \dots + b_n T^n$. En écrivant la matrice de l'application linéaire $\Phi_{P,Q}$ dans les bases indiquées, on peut donc calculer le résultant de P et Q comme le déterminant d'une matrice de taille $m+n$, appelée *matrice de Sylvester* :

$$\operatorname{Res}_{m,n}(P,Q) = \begin{vmatrix} a_0 & & & & b_0 & & \\ a_1 & a_0 & & & b_1 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & b_0 \\ a_m & & \ddots & a_0 & \vdots & & b_1 \\ & \ddots & & a_1 & b_n & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_m & & & b_n \end{vmatrix}.$$

Explicitement, le vecteur-colonne $(a_0, \dots, a_m)$ est recopié n fois, à chaque fois décalé d'une ligne vers le bas, puis le vecteur-colonne $(b_0, \dots, b_n)$ est recopié m fois, à chaque fois décalé d'une ligne vers le bas.

Remarque 1.3. — Le résultant de P et Q est un élément de A.

Soit $f \colon A \to B$ un homomorphisme d'anneaux ; notons $P \mapsto P^f$ l'homomorphisme de $A[T]$ dans $B[T]$ qui applique un polynôme $P = \sum c_j T^j$ sur $P^f = \sum f(c_j) T^j$. Alors, $\operatorname{Res}_{m,n}(P^f, Q^f) = f(\operatorname{Res}_{m,n}(P,Q))$. En effet, la matrice de l'application linéaire Φ_{P^f,Q^f} est obtenue en appliquant f aux coefficients de la matrice de l'application linéaire $\Phi_{P,Q}$.

Remarque 1.4. — La formule fondée sur le déterminant de Sylvester montre que le résultant $\mathrm{Res}_{m,n}(P,Q)$ s'exprime comme un polynôme en les coefficients $a_0,\dots,a_m,b_0,\dots,b_n$ de P et Q.

Précisément, considérons l'anneau $A=\mathbf{Z}[a_0,\dots,a_m,b_0,\dots,b_n]$ des polynômes à coefficients entiers en $(m+1)+(n+1)$ indéterminées $a_0,\dots,a_m,b_0,\dots,b_n$, et les polynômes $P=a_0+a_1+\dots+a_mT^m$ et $Q=b_0+\dots+b_nT^n$ à coefficients dans cet anneau. Notons $R_{m,n}$ le résultant $\mathrm{Res}_{m,n}(P,Q)$; c'est un élément de cet anneau de polynômes. On peut démontrer qu'il est irréductible.

Le polynôme $R_{m,n}$ est de degré $m+n$, et qu'il est homogène de degré n en les indéterminées $(a_0,\dots,a_m)$ et est homogène de degré m en les indéterminées $(b_0,\dots,b_n)$.

Démontrons aussi que $R_{m,n}$ est quasi-homogène de degré mn si l'on attribue le poids i aux indéterminées a_i et b_i. Pour cela, développons le déterminant de Sylvester suivant les permutations σ de $\{1,\dots,m+n\}$. Le terme correspondant à une telle permutation est égal à $\prod_{i=1}^n a_{\sigma(i)-i}\prod_{i=n+1}^{m+n} b_{\sigma(i)-i+n}$ si $0\leqslant\sigma(i)-i\leqslant m$ pour $1\leqslant i\leqslant n$ et $0\leqslant\sigma(i)-i+n\leqslant n$ pour $n+1\leqslant i\leqslant m$; il est nul sinon. Lorsqu'il n'est pas nul, le poids de ce monôme est donc égal à

$$\sum_{i=1}^n(\sigma(i)-i)+\sum_{i=n+1}^{m+n}(\sigma(i)-i+n)=\sum_{i=1}^{m+n}\sigma(i)-\sum_{i=1}^{m+n}i+nm=nm$$

puisque σ est une permutation. Nous avons ainsi démontré que $R_{m,n}$ est somme de monômes de poids mn, ce qui signifie exactement que $R_{m,n}$ est quasi-homogène de poids mn.

Pour tout anneau B et tout couple (p,q) de polynômes à coefficients dans B, de degrés $\leqslant m$ et $\leqslant n$ respectivement, il existe un unique homomorphisme d'anneaux $f\colon A\to B$ tel que $p=P^f$ et $q=Q^f$: pour tous i,j, cet homomorphisme applique a_i sur le coefficient de T^i de p et b_j sur le coefficients de T^j de q. Alors, $\mathrm{Res}_{m,n}(p,q)=R_{m,n}^f=R_{m,n}(p,q)$ est obtenu en évaluant le polynôme $R_{m,n}$ en les coefficients de p et q.

Cette remarque nous permettra, pour démontrer certaines formules générales, de supposer que l'anneau A est intègre, voire même, en considérant son corps des fractions, que c'est un corps, voire même, en en considérant une clôture algébrique, qu'il est algébriquement clos.

Remarque 1.5. — Supposons que $A=\mathbf{R}$. Pour tout entier n, soit $\mathscr{P}_n$ l'espace affine réel des polynômes unitaires de degré n et soit $\pi\colon\mathscr{P}_m\times\mathscr{P}_n\to\mathscr{P}_{m+n}$ l'application produit. Elle est polynomiale ; calculons sa différentielle en un couple (P,Q). Comme $\mathscr{P}_n$ est un espace affine dirigé par l'espace vectoriel $\mathbf{R}[T]_{<n}$, on doit calculer $\pi(P+U,Q+V)$ pour $U\in\mathbf{R}[T]_{<m}$ et $V\in\mathbf{R}[T]_{<n}$. On a ainsi

$$\begin{aligned}\pi(P+U,Q+V)&=(P+U)(Q+V)=PQ+(VP+UQ)+UV\\&=\pi(P,Q)+\Phi_{P,Q}(V,U)+\mathrm{O}((\|U\|+\|V\|)^2),\end{aligned}$$

où $\|\cdot\|$ est une norme arbitraire sur $\mathbf{R}[T]_{<m}$ (resp. sur $\mathbf{R}[T]_{<n}$). Ainsi, à l'échange près des facteurs, l'application $\Phi_{P,Q}$ est la différentielle de l'application π.

Le théorème d'inversion locale entraîne donc le cas particulier suivant. *Supposons $\mathrm{Res}_{m,n}(P,Q)\neq0$. Il existe alors des voisinages $\mathscr{U}$ de P dans $\mathscr{P}_m$, $\mathscr{V}$ de Q dans $\mathscr{P}_n$, $\mathscr{W}$ de PQ dans $\mathscr{P}_{m+n}$ telle que l'application π induise, par restriction, un $\mathscr{C}^\infty$-difféomorphisme de $\mathscr{U}\times\mathscr{V}$ sur $\mathscr{W}$.*

Proposition 1.6. — *Soit K un corps, soit $P,Q\in K[T]$ des polynômes en une indéterminée T à coefficients dans K et soit m,n des entiers >0 tels que $\deg(P)\leqslant m$ et*

$\deg(Q) \leqslant n$. Pour que $\mathrm{Res}_{m,n}(P,Q) = 0$, il faut et il suffit que l'une au moins des deux propriétés suivantes soit vérifiée :

(1) *On a $\deg(P) < m$ et $\deg(Q) < n$;*

(2) *Les polynômes P et Q ne sont pas premiers entre eux dans $K[T]$.*

Remarque 1.7. — Si l'on peut prendre $m = 0$, alors $P = p_0$ est constant et l'on a $\mathrm{Res}_{m,n}(P,Q) = p_0^n$; ainsi $\mathrm{Res}_{0,n}(P,Q) = 0$ si et seulement si $P = 0$ et $n > 0$. De même, si l'on peut prendre $n = 0$, alors $\mathrm{Res}_{m,0}(P,Q) = 0$ si et seulement si $Q = 0$ et $m > 0$.

Démonstration. — Notons $\Phi = \Phi_{P,Q}$. Par définition, $\mathrm{Res}_{m,n}(P,Q) = 0$ si et seulement si l'application linéaire Φ de $K[T]_{<n} \times K[T]_{<m}$ dans $K[T]_{<m+n}$ n'est pas injective, c'est-à-dire s'il existe des polynômes U et V dans $K[T]$ tels que $UP + VQ = 0$ et $\deg(U) < n$ et $\deg(V) < m$.

Supposons $P = 0$. On a alors $\mathrm{Res}_{m,n}(P,Q) = 0$, car $n > 0$. De plus, soit $\deg(Q) = 0 < n$, soit Q est un facteur commun de P et Q de degré > 0. Cela prouve l'assertion dans ce cas et la preuve lorsque $Q = 0$ est similaire.

On suppose dans la suite de la démonstration que P et Q sont non nuls.

Supposons que $\deg(P) < m$ et $\deg(Q) < n$; alors, $\Phi(-Q, P) = 0$, donc $\mathrm{Res}_{m,n}(P,Q) = 0$.

Supposons que P et Q aient un facteur commun D de degré > 0 ; soit P_1 et Q_1 des polynômes tels que $P = DP_1$ et $Q = DQ_1$. Puisque $\deg(D) > 0$, on a $\deg(P_1) < m$ et $\deg(Q_1) < n$; alors, $\Phi(-Q_1, -P_1) = -PQ_1 + QP_1 = -DP_1Q_1 + DP_1Q_1 = 0$. Ainsi, Φ n'est pas injective et $\mathrm{Res}_{m,n}(P,Q) = 0$.

Supposons maintenant que $\mathrm{Res}_{m,n}(P,Q) = 0$ et soit $U, V \in K[T]$ des polynômes non nuls tels que $UP+VQ = 0$, $\deg(U) < n$ et $\deg(V) < m$. Supposons que P et Q soient premiers entre eux. Alors, P divise $-UP = VQ$, donc P divise V, d'après le lemme de Gauss ; on a donc $m > \deg(V) \geqslant \deg(P)$. Toujours d'après le lemme de Gauss, Q divise $-VQ = UP$, donc P divise U, d'où $n > \deg(U) \geqslant \deg(Q)$. □

Exemple 1.8. — Soit k un corps et soit K une extension de K. Soit $\alpha, \beta \in K$, soit $P, Q \in k[T]$ des polynômes non nuls tels que $P(\alpha) = Q(\beta) = 0$; posons $m = \deg(P)$ et $n = \deg(Q)$.

(1) Soit $R = \mathrm{Res}(P(X-T), Q) \in k[X]$ le résultant des polynômes $P(X-T)$ et $Q(T)$ considérés comme éléments de $k[X][T]$. On a $R(\alpha+\beta) = 0$. En effet, $R(\alpha + \beta) = \mathrm{Res}_{m,n}(P(\alpha+\beta-T), Q(T)) = 0$ car β est une racine commune des polynômes $P(\alpha+\beta-T)$ et $Q(T)$. Soit de plus $x \in K$ (voire une extension K' de K). On a $R(x) = \mathrm{Res}_{m,n}(P(x-T), Q(T))$ et $\deg_T(P(x-T)) = m$, $\deg(Q) = n$; si $R(x) = 0$, alors il existe une racine t de Q telle que $x - t$ soit racine de P ; l'ensemble des éléments de K' qui sont somme d'une racine de P et d'une racine de Q est fini. En prenant x distinct de ces éléments, on a donc $R(x) \neq 0$ ce qui prouve que le polynôme R n'est pas nul.

Cela donne par exemple une démonstration constructive de ce que la somme de deux éléments de K algébriques sur k est algébrique sur k.

(2) Posons $\tilde{P}(X,T) = P(X/T)T^m$; c'est un élément de $k[X,T]$. On démontre de façon similaire que le polynôme $\mathrm{Res}_{m,n}(\tilde{P}(X,T), Q(T)) \in k[X]$ n'est pas nul et annule $\alpha\beta$.

(3) Soit $f \in k[T]$; posons $\gamma = f(\alpha)$ et $n = \deg(f)$. Alors, le polynôme $R = \mathrm{Res}_{m,n}(P(T), X - f(T)) \in k[T]$ n'est pas nul et vérifie $R(\gamma) = 0$.

(4) Soit $F \in k[X,Y]$ un polynôme tel que $F(\alpha,\beta) = 0$. Alors, le polynôme $R = \mathrm{Res}_{m,n}(P(T), F(X,T)) \in k[T]$ n'est pas nul et vérifie $R(\beta) = 0$.

Corollaire 1.9. — *Soit A un anneau factoriel, soit $P, Q \in A[T]$ des polynômes en une indéterminée T à coefficients dans A et soit m, n des entiers $\geqslant 0$ tels que $\deg(P) \leqslant m$ et $\deg(Q) \leqslant n$. Soit p un élément irréductible de A ; soit k le corps des fractions de l'anneau intègre $A/(p)$. Pour que p divise $\operatorname{Res}_{m,n}(P, Q)$, il faut et il suffit que l'une des deux propriétés suivantes soit vérifiée :*

(1) *Les coefficients dominants a_m de P et b_n de Q sont multiples de p ;*

(2) *Les images $\bar{P}$ et $\bar{Q}$ de P et Q par l'homomorphisme de réduction modulo p de $A[T]$ dans $k[T]$ ont un facteur commun dans $k[T]$.*

Corollaire 1.10. — *Soit k un corps algébriquement clos, soit $P, Q \in k[T_1, \dots, T_d]$ des polynômes en n indéterminées $T_1, \dots, T_d$ et à coefficients dans k, soit m, n des entiers $\geqslant 0$ tels que $m \geqslant \deg_{T_d}(P)$ et $n \geqslant \deg_{T_d}(Q)$. Soit donc $R \in k[T_1, \dots, T_{d-1}]$ le résultant « en T_d » de P et Q, considérés comme des éléments de $k[T_1, \dots, T_{d-1}][T_d]$.*

Pour $a \in k^{d-1}$, on a $R(a) = 0$ si et seulement si l'une des deux conditions suivantes est vérifiée :

(1) *On a $\deg(P(a, T)) < m$ et $\deg(Q(a, T)) < n$;*

(2) *Les polynômes $P(a, T)$ et $Q(a, T)$ ont une racine commune dans k.*

En particulier, lorsque $d = 2$, le résultant en Y fournit l'équation des abscisses des points d'intersection des deux courbes planes définies par des polynômes P, $Q \in k[X, Y]$.

Remarque 1.11. — Le résultant $\operatorname{Res}_{m,n}(P, Q)$ appartient à l'idéal de $A[T]$ engendré par P et Q.

Soit Ψ l'application linéaire de $A[T]_{<m+n}$ dans $A[T]_{<m} \times A[T]_{<n}$ dont la matrice dans les bases indiquées est la transposée de la matrice des cofacteurs de la matrice de $\Phi_{P,Q}$. On a donc $\Phi_{P,Q} \circ \Psi = \deg(\Phi_{P,Q}) \operatorname{Id}$. Appliquons cette égalité au polynôme 1 et posons $(U, V) = \Psi(1)$. On a donc $UP + VQ = \operatorname{Res}_{m,n}(P, Q)$, donc $\operatorname{Res}_{m,n}(P, Q) \in (P, Q)$.

2. Formules

On va maintenant donner quelques formules explicites pour le résultant.

Lemme 2.1. — *On a $\operatorname{Res}_{m,n}(P, Q) = (-1)^{mn} \operatorname{Res}_{n,m}(Q, P)$.*

Démonstration. — Soit c la permutation circulaire $(1, \dots, m+n) \to (2, \dots, m+n, 1)$; sa signature est $(-1)^{m+n-1}$. La matrice de $\Phi_{Q,P}$ est obtenue en appliquant la permutation circulaire des colonnes $(1, \dots, m+n) \to (n+1, \dots, n+m, 1, \dots, n)$, égale à c^n ; sa signature est donc égale à $(-1)^{(m+n-1)n} = (-1)^{mn}(-1)^{n^2-n} = (-1)^{mn}$ puisque $n^2 - n$ est pair. □

Lemme 2.2. — *On a $\operatorname{Res}_{0,n}(1, Q) = 1$ et $\operatorname{Res}_{m,0}(P, 1) = 1$.*

Démonstration. — En effet, dans ces cas, l'application $\Phi_{P,Q}$ est l'identité. □

Lemme 2.3. — *Pour tous $a, b \in A$, on a $\operatorname{Res}_{m,n}(aP, bQ) = a^n b^m \operatorname{Res}_{m,n}(P, Q)$.*

Démonstration. — Cela découle de l'homogénéité du déterminant de Sylvester : pour le couple (aP, bQ), il se déduit de celui du couple (P, Q) en multipliant par a les n premières colonnes, et par b les m dernières. □

Proposition 2.4. — *On suppose que Q est unitaire de degré n, de sorte que la A-algèbre $\Lambda_Q = A[T]/(Q)$ est un A-module libre de rang n. Le résultant $\operatorname{Res}_{m,n}(P, Q)$ est le déterminant de la multiplication par (la classe de) P dans Λ_Q.*

Démonstration. — Soit $\theta\colon A[T]_{<n} \times A[T]_{<m} \to A[T]_{m+n}$ l'application linéaire donnée par $(U,V) \mapsto U + VQ$. Comme Q est unitaire, le théorème de division euclidienne assure qu'elle est bijective ; notons (α,β) son inverse : on a donc $\alpha(U) + \beta(U)Q = U$ pour tout $U \in A[T]_{<m+n}$.

Pour $U \in A[T]_{<n}$ et $V \in A[T]_{<m}$, on a

$$\Phi_{P,Q}(U,V) = UP + VQ = \alpha(UP) + \beta(UP)Q + VQ = \theta(\alpha(UP), V + \beta(UP)),$$

donc $\mathrm{Res}_{m,n}(P,Q)$ est le produit du déterminant de θ et du déterminant de l'application $(U,V) \mapsto (\alpha(UP), V + \beta(UP))$.

La matrice de θ est triangulaire supérieure, et comme Q est unitaire, sa diagonale est formée de 1 ; on a donc $\det(\theta) = 1$.

La matrice de $(U,V) \mapsto (\alpha(UP), V+\beta(UP))$ est triangulaire supérieure par blocs, donc son déterminant est le produit des déterminants de deux blocs diagonaux. Le bloc en haut à gauche est la matrice de la multiplication par P dans Λ_Q. Le bloc en bas à droite est l'identité.

Cela démontre la proposition. □

Corollaire 2.5. — *Pour tout $a \in A$, on a $\mathrm{Res}_{m,1}(P, T-a) = P(a)$ et $\mathrm{Res}_{1,n}(T-a, Q) = (-1)^n Q(a)$.*

Démonstration. — L'algèbre $\Lambda_{T-a} = A[T]/(T-a)$ est égale à A, et la classe de P dans cette algèbre est égale à $P(a)$. La proposition entraîne donc la première égalité $\mathrm{Res}_{m,1}(P, T-a) = P(a)$. On a $\mathrm{Res}_{1,n}(T-a, Q) = (-1)^n \mathrm{Res}_{n,1}(Q, T-a)$, d'où la seconde égalité. □

Corollaire 2.6. — *Soit P_1, P_2, Q des polynômes de $A[T]$, soit m_1, m_2, n des entiers $\geqslant 0$ tels que $\deg(P_1) \leqslant m_1$, $\deg(P_2) \leqslant m_2$ et $\deg(Q) \leqslant n$. On a*

$$\mathrm{Res}_{m_1+m_2,n}(P_1P_2, Q) = \mathrm{Res}_{m_1,n}(P_1, Q)\,\mathrm{Res}_{m_2,n}(P_2, Q).$$

Démonstration. — Il suffit de démontrer cette formule lorsque P_1, P_2, Q sont des polynômes à coefficients indéterminés a_i (pour $0 \leqslant i \leqslant m_1$), b_j (pour $0 \leqslant j \leqslant m_2$) et c_k (pour $0 \leqslant k \leqslant n$) et l'anneau A est l'anneau des polynômes $\mathbf{Z}[(a_i),(b_j),(c_k)]$. On peut même prouver l'égalité dans le corps des fractions K de A. Observons que l'on a alors $\deg(P_1) = m_1$, $\deg(P_2) = m_2$ et $\deg(Q) = n$. Posons $m = m_1 + m_2$ et $P = P_1P_2$. Les deux membres sont homogènes de degrés $m_1 + m_2$ en les coefficients de Q ; on peut donc supposer que Q est unitaire.

Soit Λ_Q l'algèbre $K[T]/(Q)$. Notons μ_P la multiplication par un polynôme P dans cette algèbre. D'après la proposition, on a $\mathrm{Res}_{m_1,n}(P_1, Q) = \det(\mu_{P_1})$, et de même pour P_2 et $P = P_1P_2$. Comme $\mu_{P_1P_2} = \mu_{P_1} \circ \mu_{P_2}$, on a la formule voulue. □

Corollaire 2.7. — *On suppose $P = a\prod_{i=1}^m (T-\alpha_i)$ et $Q = b\prod_{j=1}^n (T-\beta_j)$. Alors,*

$$\mathrm{Res}_{m,n}(P,Q) = b^m \prod_{j=1}^n P(\beta_j) = (-1)^{mn} a^n \prod_{i=1}^m Q(\alpha_i) = a^n b^m \prod_{i=1}^m \prod_{j=1}^n (\beta_j - \alpha_i).$$

Remarque 2.8. — En raisonnant par récurrence sur n, on peut aussi démontrer le corollaire précédent directement grâce à des combinaisons linéaires judicieuses de colonnes. En effet, si $Q =$

$b\prod_{j=1}^n (T-\beta_j) = b_0 + b_1 T + \dots + b_n T^n$, on a $(T-\beta)Q = -\beta Q + TQ$, de sorte que

$$\operatorname{Res}_{m,n+1}(P,(T-\beta)Q) = \begin{vmatrix}
a_0 & & & & -\beta b_0 & & \\
a_1 & a_0 & & & b_0-\beta b_1 & \ddots & \\
\vdots & \ddots & \ddots & & b_1-\beta b_2 & \ddots & -\beta b_0 \\
a_m & & \ddots & a_0 & \vdots & & b_0-\beta b_1 \\
 & \ddots & & a_1 & b_n & & \vdots \\
 & & \ddots & \vdots & & \ddots & b_{n-1}-\beta b_n \\
 & & & a_m & & & b_n
\end{vmatrix}.$$

En partant du bas, ajoutons à chaque ligne β fois la suivante. On obtient ainsi

$$\operatorname{Res}_{m,n+1}(P,(T-\beta)Q) = \begin{vmatrix}
P(\beta) & \beta P(\beta) & \cdots & \beta^{n-1}P(\beta) & 0 & & \\
a_1+a_2\beta+\dots & P(\beta) & & \beta^{n-2}P(\beta) & b_0 & \ddots & \\
\vdots & \ddots & \ddots & \vdots & b_1 & \ddots & 0 \\
a_m & & \ddots & P(\beta) & \vdots & & b_0 \\
 & \ddots & & a_1+\beta a_2+\dots & b_n & & \vdots \\
 & & \ddots & \vdots & & \ddots & b_{n-1} \\
 & & & a_m & & & b_n
\end{vmatrix}.$$

La première ligne est multiple de $P(\beta)$, on a donc

$$\operatorname{Res}_{m,n+1}(P,(T-\beta)Q) = P(\beta)\begin{vmatrix}
1 & \beta & \cdots & \beta^{n-1} & 0 & & \\
a_1+a_2\beta+\dots & P(\beta) & & \beta^{n-2}P(\beta) & b_0 & \ddots & \\
\vdots & \ddots & \ddots & \vdots & b_1 & \ddots & 0 \\
a_m & & \ddots & P(\beta) & \vdots & & b_0 \\
 & \ddots & & a_1+\beta a_2+\dots & b_n & & \vdots \\
 & & \ddots & \vdots & & \ddots & b_{n-1} \\
 & & & a_m & & & b_n
\end{vmatrix}.$$

En partant de la droite, soustrayons à chacune des n premières lignes β fois la précédente. On obtient

$$\operatorname{Res}_{m,n+1}(P,(T-\beta)Q) = P(\beta)\begin{vmatrix}
1 & 0 & \cdots & 0 & 0 & & \\
a_1+a_2\beta+\dots & a_0 & & 0 & b_0 & \ddots & \\
\vdots & \ddots & \ddots & \vdots & b_1 & \ddots & 0 \\
a_m & & \ddots & a_0 & \vdots & & b_0 \\
 & \ddots & & a_1 & b_n & & \vdots \\
 & & \ddots & \vdots & & \ddots & b_{n-1} \\
 & & & a_m & & & b_n
\end{vmatrix}.$$

En développant ce déterminant suivant la première ligne, on trouve ainsi

$$\operatorname{Res}_{m,n+1}(P,(T-\beta)Q) = P(\beta)\operatorname{Res}_{m,n}(P,Q).$$

Le reste de la formule s'en déduit par récurrence.

3. Résultant et algorithme d'Euclide

Les formules explicites du paragraphe précédent permettent de fournit un algorithme assez efficace pour calculer le résultant.

On pose $P_0 = P$ et $P_1 = Q$ puis, pour tout entier k tel que $P_k \neq 0$, soit P_{k+1} le reste de la division euclidienne de P_{k-1} par P_k. D'après l'algorithme d'Euclide, il existe un plus petit entier d tel que $P_{d+1} = 0$, et P_d est le pgcd de P et Q.

On sait que $\operatorname{Res}_{m,n}(P,Q) = 0$ si P et Q ne sont pas premiers entre eux, c'est-à-dire si $\deg(P_d) \neq 0$.

On suppose dans la suite que P et Q sont premiers entre eux. Pour $k \leqslant d$, notons n_k le degré de P_k et a_k son coefficient dominant. Par homogénéité du résultant en le second polynôme, on a

$$\operatorname{Res}_{n_{k-1},n_k}(P_{k-1},P_k) = a_k^{n_{k-1}} \operatorname{Res}_{n_{k-1},n_k}(P_{k-1},P_k/a_k).$$

De plus, $\operatorname{Res}_{n_{k-1},n_k}(P_{k-1},P_k/a_k)$ est le déterminant de la multiplication par P_{k-1} dans l'algèbre $K[T]/(P_k)$. Comme $P_{k+1} \equiv P_{k-1} \pmod{P_k}$, c'est aussi le déterminant de la multiplication par P_{k+1} dans cette algèbre, de sorte que

$$\operatorname{Res}_{n_{k-1},n_k}(P_{k-1},P_k) = a_k^{n_{k-1}} \operatorname{Res}_{n_{k+1},n_k}(P_{k+1},P_k) = a_k^{n_{k-1}} (-1)^{n_k n_{k+1}} \operatorname{Res}_{n_k,n_{k+1}}(P_k,P_{k+1}).$$

Enfin, on a

$$\operatorname{Res}_{n_{d-1},n_d}(P_{d-1},P_d) = \operatorname{Res}_{n_{d-1},0}(P_{d-1},a_d) = a_d^{n_{d-1}} \operatorname{Res}_{n_{d-1},0}(P_{d-1},1) = a_d^{n_{d-1}}.$$

On a donc

$$\operatorname{Res}_{m,n}(P,Q) = \prod_{k=1}^{d} a_k^{n_{k-1}} \prod_{k=1}^{d-1} (-1)^{n_k n_{k+1}}.$$

4. Discriminant

Définition 4.1. — *Soit $P \in A[T]$ un polynôme de degré m dont le coefficient dominant a_m est inversible ; on appelle discriminant de P l'expression*

$$\operatorname{Disc}(P) = (-1)^{m(m-1)/2} a_m^{-1} \operatorname{Res}_{m,m-1}(P,P').$$

Remarque 4.2. — Prenons pour anneau A un anneau de polynômes $\mathbf{Z}[a_0,\dots,a_m]$ et pour polynôme P le polynôme $P = a_0 + a_1T + \dots + a_mT^m$ dont les coefficients sont les indéterminées. Soit $R = \operatorname{Res}_{m,m-1}(P,P')$. Dès qu'on évalue le polynôme R en un polynôme p dont le coefficient de T^m est nul, on a $\deg(p) < m$ et $\deg(p') < m-1$, donc $R(p) = \operatorname{Res}_{m,m-1}(p,p') = 0$. Par suite, R est multiple de a_m et il existe un unique polynôme $D_m \in \mathbf{Z}[a_0,\dots,a_m]$ tel que $a_mD_m = (-1)^{m(m-1)} = R$. En particulier, $\operatorname{Disc}(p) = D_m(p)$ pour tout polynôme p de degré m dont le coefficient dominant est inversible.

Le polynôme D_m est homogène de degré $2m-2$. Si a_i est de poids i, il est quasi-homogène de poids $m(m-1)$.

Proposition 4.3. — *Soit K un corps et soit $P \in K[T]$ un polynôme de degré n. Les conditions suivantes sont équivalentes : (i) $\operatorname{Disc}(P) = 0$; (ii) P et P' ont un facteur commun ; (iii) P et P' ont une racine commune dans une clôture algébrique.*

Proposition 4.4. — *Si $P = a\prod_{i=1}^m (T-\alpha_i)$, on a*

$$\operatorname{Disc}(P) = a^{2m-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Démonstration. — Faisons d'abord le calcul dans l'anneau des polynômes $\mathbf{Z}[a, \alpha_1, \dots, \alpha_m]$, c'est-à-dire lorsque P est le « polynôme générique scindé ». Par définition, on a

$$(-1)^{m(m-1)/2} a \operatorname{Disc}(P) = \operatorname{Res}_{m,m-1}(P, P') = (-1)^{m(m-1)} a^{m-1} \prod_{i=1}^{m} P'(\alpha_i).$$

D'autre part, pour tout $i \in \{1, \dots, m\}$, on a

$$P'(\alpha_i) = a \prod_{j \neq i} (\alpha_j - \alpha_i),$$

de sorte que

$$\begin{aligned} a \operatorname{Disc}(P) &= (-1)^{m(m-1)/2} a^{2m-1} \prod_{j \neq i} (\alpha_j - \alpha_i) \\ &= a^{2m-1} \prod_{j<i} (\alpha_j - \alpha_i)^2. \end{aligned}$$

En simplifiant par a, on a le résultat voulu.

Le calcul précédent reste valable si a est inversible, voire si a est simplifiable dans A. Dans le cas général, $\operatorname{Disc}(P)$ s'obtient par évaluation du discriminant du polynôme générique scindé, d'où le résultat. □

Exemple 4.5. — (1) Pour $P = aT^2 + bT + c$, on a $\operatorname{Disc}(P) = b^2 - 4ac$.

(2) Pour $P = T^3 + pT + q$, on a $\operatorname{Disc}(P) = -4p^3 - 27q^2$.

(3) Plus généralement, si $P = T^n + pT + q$, alors $\operatorname{Disc}(P) = (-1)^{n(n-1)/2}(q^{n-1}n^n + p^n(1-n)^{n-1})$.

Il suffit de traiter le dernier exemple dans le cas où $q \neq 0$ et P et P' sont scindés, c'est-à-dire $P = \prod_{i=1}^n (T - \alpha_i)$ et $P' = nT^{n-1} + p = n(T^{n-1} + p/n) = n \prod_{j=1}^{n-1} (T - \beta_j)$. Alors,

$$\operatorname{Disc}(P) = (-1)^{n(n-1)/2} \operatorname{Res}_{n,n-1}(P, P') = (-1)^{n(n-1)} n^n \prod_{j=1}^{n-1} P(\beta_j).$$

Pour tout j, on a $\beta_j^{n-1} = -p/n$, donc

$$P(\beta_j) = \beta_j^n + p\beta_j + q = p(1 - 1/n)\beta_j + q,$$

de sorte que

$$\begin{aligned} \operatorname{Disc}(P) &= (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} \big(p(1-1/n)\beta_j + q\big) \\ &= (-1)^{n(n-1)/2} p^{n-1} (1-n)^{n-1} n \prod_{j=1}^{n-1} \left(\frac{qn}{p(1-n)} - \beta_j \right) \\ &= (-1)^{n(n-1)/2} p^{n-1} (1-n)^{n-1} P'(qn/p(1-n)) \\ &= (-1)^{n(n-1)/2} p^{n-1} (1-n)^{n-1} \big(n(qn/p(1-n))^{n-1} + p\big) \\ &= (-1)^{n(n-1)/2} \left(q^{n-1} n^n + (1-n)^{n-1} p^n\right). \end{aligned}$$

Remarque 4.6. — Supposons $A = \mathbf{R}$ et identifions à $\mathbf{R}^n$ l'espace affine des polynômes unitaires de degré n, par l'application $(a_1, \dots, a_n) \mapsto T^n + a_1 T^{n-1} + \dots + a_n$. Soit $f \colon \mathbf{R}^n \to \mathbf{R}^n$ l'application qui applique $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{R}^n$ sur le polynôme $P_\alpha = \prod_{i=1}^n (T - \alpha_i)$.

Elle est polynomiale, donnée aux signes près par les polynômes symétriques élémentaires : $F\colon \alpha \mapsto (-s_1(\alpha), \ldots, (-1)^n s_n(\alpha))$.

Comme $s_i(T_1, \ldots, T_n) = s_i(T_1, \ldots, T_{n-1}) + T_n s_{i-1}(T_1, \ldots, T_{n-1})$, on a

$$\partial_n s_i = s_{i-1}(T_1, \ldots, T_{n-1}) = s_{i-1} - T_n s_{i-2}(T_1, \ldots, T_{n-1}) = s_{i-1} - T_n \partial_n s_{i-1}.$$

Par symétrie, on a plus généralement :

$$\partial_j s_i = s_{i-1}(T_1, \ldots, \widehat{T_i}, \ldots, T_n) = s_{i-1} - T_i \partial_j s_{i-1},$$

soit encore

$$(-1)^m \partial_i s_m = (-1)^m s_{m-1} + (-1)^{m-1} T_i \partial_i s_{m-1}.$$

Pour $i = 1$, on a $\partial_j s_i = 1$; ces formules sont donc valables à condition de poser $s_0 = 1$.

Voici une astuce pour calculer le jacobien de l'application f. Définissons deux vecteurs-ligne $\mathbf{1} = (1, \ldots, 1)$ et $\mathbf{T} = (T_1, \ldots, T_n)$; notons $*$ le produit composante par composante des vecteurs-ligne. Posons $L_0 = \mathbf{1}$; si $1 \leqslant m \leqslant n$, notons L_m l'opposé de la ligne d'indice m de J_f ; on a donc $L_m = (-1)^{m-1} s_{m-1} \mathbf{1} + N_1 * L_{m-1}$, de sorte que le déterminant J_f vérifie

$$\begin{aligned} J_f &= (-1)^n \det(L_1, \ldots, L_n) \\ &= (-1)^n \det(\mathbf{1}, -s_1 + \mathbf{1} + \mathbf{T} * L_1, \ldots, (-1)^{n-1} s_{n-1} \mathbf{1} + \mathbf{T} * L_{n-1}) \\ &= (-1)^n \det(\mathbf{1}, \mathbf{T} * L_1, \ldots, \mathbf{T} * L_{n-1}) \\ &= \cdots \\ &= (-1)^n \det(\mathbf{1}, \mathbf{T}, \ldots, \mathbf{T}^{n-1}), \end{aligned}$$

où on retrouve le déterminant de Vandermonde. Ainsi,

$$J_f = (-1)^n \prod_{j>i} (T_j - T_i).$$

Par conséquent, $|\mathrm{Disc}(P_\alpha)| = J_f(\alpha)^2$.

Le théorème d'inversion locale fournit alors le résultat : *Soit $\alpha \in \mathbf{R}^n$ un vecteur à coordonnées deux à deux distinctes ; il existe un voisinage ouvert U de α dans $\mathbf{R}^n$ et un voisinage ouvert V de P_α dans l'espace des polynômes unitaires de degré n tel que l'application f induise un $\mathscr{C}^\infty$-difféomorphisme de U sur V.*

Autrement dit, sur V, on peut exprimer les racines d'un polynôme de façon $\mathscr{C}^\infty$ en ses coefficients.

5. Résultant et réciprocité quadratique

***Définition 5.1* (Symbole de Legendre).** — *Soit p un nombre premier $\geqslant 3$ et soit a un élément de $\mathbf{F}_p^\times$. On pose $\left(\dfrac{a}{p}\right) = 1$ si a est un carré, et $\left(\dfrac{a}{p}\right) = -1$ sinon.*

Proposition 5.2. — *Pour tout $a \in \mathbf{F}_p^\times$, on a $\left(\dfrac{a}{p}\right) = a^{(p-1)/2}$.*

Démonstration. — Comme le groupe multiplicatif de $\mathbf{F}_p$ est de cardinal $p-1$, on a $a^{p-1} = 1$ pour tout $a \in \mathbf{F}_p^\times$, de sorte que $(a^{(p-1)/2})^2 = 1$. Par suite, $a^{(p-1)/2} = \pm 1$. Si a est un carré, disons $a = b^2$, alors $a^{(p-1)/2} = b^{p-1} = 1$. Les carrés de $\mathbf{F}_p^\times$ sont l'image du morphisme de groupes $a \mapsto a^2$, dont le noyau est $\{\pm 1\}$; il y a donc $(p-1)/2$ carrés. Ces carrés sont solutions de l'équation polynomiale $T^{(p-1)/2} = 1$, qui a au plus $(p-1)/2$ solutions ; ce sont donc exactement les solutions de cette équation. Ainsi, si a n'est pas un carré, on a $a^{(p-1)/2} = -1$. □

5.3. — Soit p un nombre impair. Considérons le polynôme cyclotomique d'indice p, $\Phi_p = X^{p-1} + \cdots + 1$. Comme il est réciproque, il existe un unique polynôme $T_p \in \mathbf{Z}[X]$ de degré $(p-1)/2$ tel que $\Phi_p = T_p(X + 1/X)X^{(p-1)/2}$.

Soit K un corps algébriquement clos et soit $a \in K$ une racine de Φ_p. Il existe deux éléments $x \in K$ tels que $x + \frac{1}{x} = a$, ce sont les solutions de l'équation $x^2 - ax + 1 = 0$; elles sont inverses l'une de l'autre. (Ces deux racines sont confondues, égales à 1 si $a = 2$, et à -1 si $a = 0$; sinon, elles sont distinctes.) On a donc $\Phi_p(x) = T_p(a)x^{(p-1)/2} = 0$. Comme $(X-1)\Phi_p(X) = X^p - 1$, on a $x^p = 1$.

Si $x = 1$, alors $p = 0$ dans K et K est de caractéristique p. Alors, $a = 2$. Dans ce cas, on a $\Phi_p = (X-1)^{p-1}$ et $a = 2$ est l'unique racine de T_p. (Autrement dit, $T_p = (X-2)^{(p-1)/2}$.)

Supposons que $x \neq 1$. Alors, x est une racine primitive p-ième de l'unité, et la caractéristique de K est distincte de p.

***Théorème 5.4* (Réciprocité quadratique).** — *Soit $p \neq q$ des nombres premiers impairs. On a* $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Démonstration. — Soit $R = \operatorname{Res}_{(p-1)/2,(q-1)/2}(T_p, T_q)$ le résultant des polynômes T_p et T_q. C'est un entier ; nous allons démontrer que $R = \left(\dfrac{q}{p}\right)$.

Démontrons d'abord que $R = \pm 1$. Sinon, soit ℓ un nombre premier qui divise R. Comme T_p et T_q sont unitaires, ils ont un facteur commun dans $\mathbf{F}_\ell[X]$. Soit K une clôture algébrique du corps fini $\mathbf{F}_\ell$ et soit $a \in K$ une racine commune à T_p et T_q. Soit $x \in K$ tel que $a = x + 1/x$. Alors $x^p = x^q = 1$. Comme p et q sont premiers et distincts, ils sont premiers entre eux, on a donc $x = 1$ et $a = 2$. D'après la discussion précédente, la caractéristique de K, ℓ, est égale à p et à q, ce qui est impossible puisque $p \neq q$.

Calculons maintenant l'image de R modulo p. Soit K une clôture algébrique du corps fini $\mathbf{F}_p$. L'image $R \cdot 1_K$ de R dans K est le résultant des polynômes T_p et T_q, considérés comme éléments de $K[X]$. Dans K, 2 est la seule racine de T_p, avec multiplicité $(p-1)/2$. On a ainsi

$$R \cdot 1_K = \prod_{T_p(\alpha)=0} Q(\alpha) = T_q(2)^{(p-1)/2} = \Phi_q(1)^{(p-1)/2} = q^{(p-1)/2} = \left(\frac{q}{p}\right).$$

Cela démontre la congruence $R \equiv \left(\dfrac{q}{p}\right) \pmod{p}$.

Comme l'entier $\left(\dfrac{q}{p}\right)$ est le seul élément de $\{\pm 1\}$ qui satisfasse cette congruence, on a prouvé que $R = \left(\dfrac{q}{p}\right)$.

Par symétrie, on a $\operatorname{Res}(T_q, T_p) = \left(\dfrac{p}{q}\right)$.

Puisque $\operatorname{Res}(T_p, T_q) = (-1)^{(p-1)(q-1)/4} \operatorname{Res}(T_q, T_p)$, on en déduit alors la loi de réciprocité quadratique :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

□

6. Résultant et théorème des zéros de Hilbert

Définition 6.1. — *Soit K un corps et soit I un idéal de $K[T_1, \dots, T_n]$. On définit $V(I)$ comme l'ensemble des $a \in K^n$ tels que $P(a) = 0$ pour tout $P \in I$.*

Si $1 \in I$, alors $V(I) = \emptyset$, de façon évidente. La réciproque est fausse en général. Par exemple, si $K = \mathbf{R}$ et $n = 1$, on a $V((T^2 + 1)) = 0$, le polynôme $T^2 + 1$ n'ayant pas de racine dans $\mathbf{R}$.

La théorème des zéros de Hilbert affirme que la réciproque est vraie lorsque le corps K est algébriquement clos. Sa preuve utilise quelques résultats auxiliaires que nous démontrons tout de suite.

Lemme 6.2. — *Soit K un corps infini, soit n un entier $\geqslant 1$ et soit $P \in K[T_1, \dots, T_n]$ un polynôme non nul. Il existe $a \in K^n$ tel que $P(a) \neq 0$.*

Démonstration. — On raisonne par récurrence sur n ; l'assertion est classique si $n = 1$, un polynôme non nul ayant moins de racines que son degré. Soit alors d le degré de P par rapport à l'indéterminée T_n et écrivons $P = P_d T_n^d + \dots + P_0$, où $P_0, \dots, P_d \in K[T_1, \dots, T_{n-1}]$; par hypothèse, $P_d \neq 0$. Par récurrence, il existe $a' \in K^{n-1}$ tel que $P_d(a') \neq 0$. Le polynôme $P(a', T) \in K[T]$ n'est pas nul ; d'après le cas $n = 1$, il existe $b \in K$ tel que $P(a', b) \neq 0$ et la famille $a = (a', b)$ convient. □

Proposition 6.3. — *Soit K un corps infini, soit n un entier $\geqslant 1$ et soit $P \in K[T_1, \dots, T_n]$ un polynôme non constant, soit d son degré. Il existe alors $(a_1, \dots, a_{n-1}) \in K^{n-1}$ tel que le coefficient de T_n^d du polynôme $P(T_1 + a_1T_n, \dots, T_{n-1} + a_{n-1}T_n, T_n)$ soit non nul.*

Démonstration. — Soit P_k la composante homogène de degré k de P, de sorte que $P = P_0 + \dots + P_d$. Par hypothèse, $P_d \neq 0$. Le coefficient de T_n^d du polynôme $P(T_1 + a_1T_n, \dots, T_{n-1} + a_{n-1}T_n, T_n)$ est égal à $P_d(a_1, \dots, a_{n-1}, 1)$. Comme P_d est homogène, le polynôme $P_d(T_1, \dots, T_{n-1}, 1)$ n'est pas nul. D'après le lemme précédent, il existe $a \in K^{n-1}$ tel que $P_d(a, 1) \neq 0$, de sorte que a convient. □

Théorème 6.4 **(Théorème des zéros de Hilbert, forme faible)**
Soit K un corps algébriquement clos. Soit I un idéal de $K[T_1, \dots, T_n]$, distinct de $K[T_1, \dots, T_n]$. Alors $V(I) \neq \emptyset$.

Démonstration. — Si $n = 0$, on a $K[T_1, \dots, T_n] = K$; ainsi, on a $I = 0$ et $V(I) = K^0$ (un singleton).

On démontre alors le résultat par récurrence sur n en le supposant vérifié dans le cas d'un anneau de polynômes en $< n$ indéterminées. Comme $V((0)) = K^n$, on peut supposer que $I \neq 0$. Soit P un polynôme non nul appartenant à I ; alors P n'est pas constant. Soit $d = \deg(P)$ et supposons que le coefficient de T_n^d de P ne soit pas nul.

L'idéal $K[T_1, \dots, T_{n-1}] \cap I$ est un idéal strict de $K[T_1, \dots, T_{n-1}]$. Par récurrence, il existe donc $a' = (a_1, \dots, a_{n-1}) \in K^{n-1}$ tel que $Q(a') = 0$ pour tout $Q \in K[T_1, \dots, T_{n-1} \cap I$. Soit alors $J \subset K[T]$ l'ensemble des polynômes de la forme $Q(a', T)$, pour $Q \in I$. C'est l'image de I par l'homomorphisme (surjectif) d'anneaux de $K[T_1, \dots, T_n]$ dans $K[T]$ qui applique T_j sur a_j pour $j \leqslant n - 1$ et T_n sur T ; c'est donc un idéal de $K[T]$.

L'anneau $K[T]$ est principal ; soit $Q \in I$ un polynôme tel que $Q(a', T)$ soit un générateur de J. Soit $R \in K[T_1, \dots, T_{n-1}]$ le résultant de P et Q, considérés comme polynômes de

$K[T_1,\dots,T_{n-1}][T_n]$. C'est un élément de l'idéal engendré par P et Q, donc est un élément de $I\cap K[T_1,\dots,T_{n-1}]$. Par le choix de a', on a donc $R(a')=0$. Comme P est unitaire en T_n, cela signifie que les polynômes $P(a',T)$ et $Q(a',T)$ ont un facteur commun. Puisque $P(a',T)\neq 0$, cela entraîne que $Q(a',T)$ n'est pas inversible. Il existe donc $a_n\in K$ tel que $Q(a',a_n)=0$; posons $a=(a',a_n)$.

Pour tout polynôme $Q_1\in I$, $Q_1(a',T)$ est multiple de $Q(a',T)$, donc s'annule en a_n ; par conséquent, $Q_1(a)=0$. Cela démontre que $a\in V(I)$ et conclut la démonstration du théorème sous l'hypothèse particulière faite sur sur le polynôme P.

Traitons maintenant le cas général. D'après la proposition, il existe $b\in K^{n-1}$ tel que le coefficient de T_n^d du polynôme $P(T_1+b_1T_n,\dots,T_{n-1}+b_{n-1}T_n,T_n)$ ne soit pas nul. Considérons l'unique homomorphisme f de K-algèbres de $K[T_1,\dots,T_n]$ dans elle-même tel que $f(T_j)=T_j+b_jT_n$ pour $1\leqslant j\leqslant n-1$ et $f(T_n)=T_n$. C'est un automorphisme, son inverse est l'unique homomorphisme de K-algèbres qui applique T_n sur lui-même et T_j sur $T_j-b_jT_n$. L'image $f(I)$ de I est donc un idéal strict de $K[T_1,\dots,T_n]$. Il existe ainsi $a\in K^n$ tel que $f(P)(a)=0$ pour tout $P\in I$. Comme $f(P)(a)=P(a_1+b_1a_n,\dots,a_{n-1}+b_{n-1}a_n,a_n)$, cela démontre que $a'=(a_1+b_1a_n,\dots,a_{n-1}+b_{n-1}a_n,a_n)$ appartient à $V(I)$. □

Corollaire 6.5. — *Soit K un corps algébriquement clos.*

(1) *Pour tout $a\in K^n$, l'idéal $M_a=(T_1-a_1,\dots,T_n-a_n)$ de $K[T_1,\dots,T_n]$ est un idéal maximal.*

(2) *Pour tout idéal maximal M de l'anneau $K[T_1,\dots,T_n]$, il existe un unique $a\in K^n$ tel que $M=M_a$.*

Démonstration. — Par des divisions euclidiennes successives, on démontre que M_a est le noyau de l'homomorphisme de $K[T_1,\dots,T_n]$ dans K donné par $P\mapsto P(a)$. Comme cet homomorphisme est surjectif et son image est un corps, cela entraîne que M_a est maximal.

Soit $a,b\in K^n$ tels que $M_a=M_b$. Pour tout j, $T_j-a_j\in M_a$ s'évalue sur b_j-a_j en b, donc $b_j=a_j$. Cela prouve que $a=b$.

Soit M un idéal maximal de $K[T_1,\dots,T_n]$. D'après la forme faible du théorème des zéros de Hilbert, il existe $a\in K^n$ tel que $P(a)=0$ pour tout $P\in M$. Ainsi, $M\subset M_a$. Puisque M est un idéal maximal, on a $M=M_a$. □