Appendice III

APPENDICE III

(1) Résultants et discriminants

Désignons par A un anneau intègre (commutatif avec élément unité) et par K son corps des fractions.

LEMME 1. *Soit M un A-module libre de type fini et soit u un endomorphisme de M. Si u est surjectif, c'est un isomorphisme.*

L'application $u \otimes 1$ est un endomorphisme surjectif de $M \otimes_A K$, donc un isomorphisme puisque $M \otimes_A K$ est un espace vectoriel de dimension finie. On conclut en remarquant que l'application canonique de M dans $M \otimes_A K$ est injective.

Pour tout entier naturel m, on désigne par A_m l'ensemble des polynômes de $A[T]$ de degré strictement inférieur à m. C'est un A-module libre de rang m.

Soient p et q deux polynômes de $A[T]$ de degré m et n respectivement. On désigne par $\phi(p, q)$ l'application A-linéaire de $A_n \times A_m$ dans A_{m+n} définie par

$$\phi(p, q)(u, v) = up + vq .$$

Les polynômes

$$(1, 0), \ldots, (T^{n-1}, 0), (0, 1), \ldots, (0, T^{m-1}) \quad (\text{resp. } 1, \ldots, T^{m+n-1})$$

forment une base de $A_n \times A_m$ (resp. A_{m+n}). On appelle *résultant de p et q* et l'on désigne par Rés (p, q) le déterminant de l'application $\phi(p, q)$ exprimé dans ces bases. Si l'on pose

$$p = p_m + p_{m-1} T + \ldots + p_0 T^m \quad \text{et} \quad q = q_n + q_{n-1} T + \ldots + q_0 T^n$$

le résultant de p et q est donné par la formule

$$\text{Rés}(p,q) = \begin{vmatrix} p_m & 0 & . & . & 0 & q_n & . & 0 & 0 \\ . & p_m & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & q_n & . \\ . & . & . & . & 0 & . & . & . & q_n \\ p_0 & . & . & . & p_m & . & . & . & . \\ 0 & p_0 & . & . & . & q_0 & . & . & . \\ . & 0 & . & . & . & 0 & . & . & . \\ . & . & . & . & . & . & . & q_0 & . \\ 0 & 0 & . & . & p_0 & 0 & . & 0 & q_0 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\\d\\e\end{matrix}}\right\} m+1 \\ \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} n-1 \end{matrix}$$

$$\underbrace{\qquad\qquad}_{n} \qquad \underbrace{\qquad\qquad}_{m}$$

Il résulte de cette définition que Rés (p, q) est un polynôme homogène de degré n en $p_0, ..., p_m$, homogène de degré m en $q_0, ..., q_n$. Son terme de plus haut degré en p_m et q_0 est $p_m^n q_0^m$.

Pour tout homomorphisme ρ de A dans un anneau intègre B, on a

$$\text{Rés}\left(\rho(p), \rho(q)\right) = \rho\left(\text{Rés}(p,q)\right).$$

On dit que p et q sont *étrangers* (ou aussi *premiers entre eux*) s'ils engendrent l'anneau $A[T]$.

LEMME 2. *On suppose que l'un au moins des coefficients p_0 ou q_0 est inversible. Les conditions suivantes sont équivalentes :*

(1) Les polynômes p et q sont étrangers.

(2) L'application $\phi(p,q)$ est un isomorphisme.

(3) Le résultant de p et q est inversible dans A.

Il suffit de montrer que les conditions (1) et (2) sont équivalentes.

Supposons par exemple q_0 inversible et (1) vérifiée. En particulier, pour tout polynôme r de A_{m+n}, on a

$$r = up + vq$$

avec u et v dans $A[T]$. La division euclidienne des polynômes montre que l'on a

$$u = u'q + u'' \qquad \text{avec} \qquad \deg(u'') < n.$$

On a alors

$$r = u''p + (u' + v)q \qquad \text{avec} \qquad \deg(u' + v) < m.$$

Ceci montre que l'application $\phi(p, q)$ est surjective. Le lemme 1 montre que c'est un isomorphisme.

Réciproquement, supposons (2) vérifiée. On peut écrire

$$1 = up + vq$$

pour certains polynômes u et v de A_n et A_m respectivement. Ceci montre que p et q sont étrangers.

LEMME 3. *Supposons A factoriel. Si les polynômes p et q sont moniques, irréductibles et distincts, ils sont étrangers.*

Raisonnons par l'absurde. Il existe alors des polynômes u et v non nuls de degré strictement inférieur à n et m respectivement tels que

$$up + vq = 0$$

(lemme 2). Le polynôme q étant irréductible, il n'appartient pas à l'idéal (p). Le polynôme v non plus pour des raisons de degré. Puisque $A[T]$ est factoriel et le polynôme p irréductible, l'idéal (p) est premier, ce qui est absurde.

Soit L une clôture algébrique de K. On peut écrire

$$p = p_0 \prod_{1 \leq j \leq m} (T - \alpha_j) \quad \text{et} \quad q = q_0 \prod_{1 \leq k \leq n} (T - \beta_k)$$

pour certains éléments $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ de L. La fonction

$$S = p_0^n q_0^m \prod_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} (\beta_k - \alpha_j)$$

est symétrique par rapport à $\alpha_1, \ldots, \alpha_m$ (resp. $\beta_1, \ldots, \beta_n$). C'est donc une fonction polynomiale de $p_0, \ldots, p_m$ et $q_0, \ldots, q_n$. Remarquons que l'on a

$$S = (-1)^{mn} p_0^n \prod_{1 \leq j \leq m} q(\alpha_j) = q_0^m \prod_{1 \leq k \leq n} p(\beta_k).$$

En particulier, le polynôme S est homogène de degré n en $p_0, \ldots, p_m$ et homogène de degré m en $q_0, \ldots, q_n$. Son terme de plus haut degré en p_m et q_0 est $p_m^n q_0^m$.

Les coefficients des polynômes p et q sont liés aux racines par les formules

$$p_j = (-1)^j \sigma_j(\alpha_1, \ldots, \alpha_m) \quad \text{et} \quad q_j = (-1)^j \sigma_j(\beta_1, \ldots, \beta_n)$$

où σ_j désigne la j^e fonction symétrique élémentaire à m ou n indéterminées. Ceci montre que Rés (p, q) est une fonction polynomiale en $p_0, \alpha_1, \ldots, \alpha_m, q_0, \beta_1, \ldots, \beta_n$. Cette fonction polynomiale est divisible par $\beta_k - \alpha_j$. En effet, si α_j est égal à β_k, les polynômes p et q ne sont pas étrangers (lemme 2).

Il résulte de toutes ces remarques que l'on a la formule

$$\boxed{\text{Rés}(p, q) = p_0^n q_0^m \prod_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} (\beta_k - \alpha_j)}$$

En particulier, le résultant de p et q s'annule si et seulement si l'une des conditions suivantes est vérifiée:

(1) L'un des coefficients p_0 ou q_0 est nul.

(2) Les polynômes p et q ont une racine commune dans L.

Soit p un polynôme de $A[T]$ et soit p' le polynôme dérivé $\dfrac{\partial p}{\partial T}$. On appelle *discriminant de* p et l'on désigne par $\text{Dis}(p)$ le résultant de p et p'.

Avec les notations précédentes, on a

$$p' = p_0 \sum_{1 \leq j \leq p} (T - \alpha_1) \ldots \widehat{(T - \alpha_j)} \ldots (T - \alpha_m)$$

et par conséquent,

$$p'(\alpha_k) = p_0 \prod_{\substack{1 \leq j \leq m \\ j \neq k}} (\alpha_k - \alpha_j) .$$

La formule précédente montre que l'on a

$$\boxed{\text{Dis}(p) = p_0^{2m-1} \prod_{\substack{1 \leq j,\ k \leq m \\ j \neq k}} (\alpha_j - \alpha_k)}$$

En particulier, le discriminant de p s'annule si et seulement si l'une des conditions suivantes est vérifiée:

(1) Le coefficient dominant de p est nul.

(2) Le polynôme p a une racine double dans L.

LEMME 4. *Supposons A factoriel. Si le polynôme p est monique irréductible, le discriminant* $\text{Dis}(p)$ *est non nul.*

Raisonnons par l'absurde en supposant que $\text{Dis}(p)$ est nul, donc non inversible dans K. Le lemme 2 montre qu'il existe deux polynômes u et v de degré strictement inférieur à $m-1$ et m respectivement dans $K[T]$ tels que

$$up + vp' = 0 .$$

Quitte à multiplier cette égalité par un élément convenable de A, on peut supposer que u et v appartiennent à $A[T]$. On procède alors comme dans le lemme 3.

(2) Théorème de normalisation

Tous les anneaux (et tous les corps) considérés sont commutatifs, avec élément unité.

THÉORÈME 1 (Elément primitif). *Soit K un corps de caractéristique zéro et soit L une extension finie de K. Il existe alors un élément α de L tel que L soit engendré par α sur K.*

De manière plus précise, pour toute partie infinie S de K et tout système de générateurs $\alpha_1, \ldots, \alpha_n$ de L sur K, il existe des éléments $\lambda_1, \ldots, \lambda_n$ de S tels que l'élément

$$\alpha = \lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n$$

engendre L sur K.

Par récurrence sur n, on se ramène immédiatement au cas où L est engendré par deux éléments α_1 et β_1. Désignons par p et q les polynômes minimaux de α_1 et β_1 respectivement dans $K[T]$. Dans une extension convenable de K, on peut écrire

$$p = \prod_{1 \leq j \leq m} (T - \alpha_j) \quad \text{et} \quad q = \prod_{1 \leq j \leq n} (T - \beta_j).$$

Les racines $\alpha_1, \ldots, \alpha_m$ (resp. $\beta_1, \ldots, \beta_n$) étant deux à deux distinctes, il existe un élément λ de S tel que

$$\alpha_j + \lambda\beta_k \neq \alpha_1 + \lambda\beta_1 \text{ pour } 1 \leqslant j \leqslant m \qquad 2 \leqslant k \leqslant n.$$

Posons

$$\alpha = \alpha_1 + \lambda\beta_1$$

et montrons que L est engendré par α. Il suffit évidemment de montrer que β_1 appartient à $K(\alpha)$. Par construction, le plus grand commun diviseur des polynômes $q(T)$ et $p(\alpha - \lambda T)$ de $K(\alpha)[T]$ est le polynôme $T - \beta_1$. Ceci montre que le polynôme minimal de β_1 dans $K(\alpha)[T]$ est $T - \beta_1$, d'où l'assertion.

LEMME 5. *Soit B un anneau et soit A un sous-anneau de B. Pour tout élément x de B, les conditions suivantes sont équivalentes :*

(1) Il existe un entier naturel n et des éléments $a_1, \ldots, a_n$ de A tels que

$$x^n + a_1x^{n-1} + \ldots + a_n = 0.$$

(2) Il existe un sous-A-module M non nul de type fini dans B tel que M contienne xM.

Supposons (1) vérifiée et désignons par M le sous-module de B engendré par $1, x, \ldots, x^{n-1}$. Il est clair que xM est contenu dans M.

Réciproquement, supposons (2) vérifiée et désignons par $m_1, \ldots, m_n$ des générateurs de M. Il existe une famille $(a_{jk})_{1 \leqq j,k \leqq n}$ d'éléments de A telle que

$$xm_j = \sum_{1 \leqq k \leqq n} a_{jk} m_k \quad \text{pour} \quad 1 \leqslant j \leqslant n .$$

Ceci peut s'écrire

$$\begin{bmatrix} x - a_{11} & . & . & . & a_{1n} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{n1} & . & . & . & x - a_{nn} \end{bmatrix} \begin{bmatrix} m_1 \\ . \\ . \\ . \\ m_n \end{bmatrix} = 0$$

et puisque les éléments $m_1, \ldots, m_n$ ne sont pas tous nuls, le déterminant de la matrice de gauche fournit la relation cherchée.

On dit que x est *entier sur* A s'il vérifie les conditions du lemme 5. On dit que B est *entier sur* A si tous ses éléments sont entiers sur A.

On appelle *fermeture intégrale de* A *dans* B l'ensemble des éléments de B entiers sur A.

LEMME 6. *Soient* C *un anneau,* B *un sous-anneau de* C *et* A *un sous-anneau de* B.

(1) Supposons que B *soit une* A*-algèbre de type fini. Pour que* B *soit entier sur* A*, il faut et il suffit que ce soit un* A*-module de type fini.*

(2) Si C *est entier sur* B *et* B *entier sur* A*, alors* C *est entier sur* A.

(3) La fermeture intégrale A' *de* A *dans* B *est un sous-anneau de* B*. Tout élément de* B *entier sur* A' *appartient à* A'.

La première assertion résulte immédiatement des définitions. Démontrons la seconde. Soit x un élément de C et soit $b_1, \ldots, b_n$ des éléments de B tels que

$$x^n + b_1 x^{n-1} + \ldots + b_n = 0 .$$

La sous-algèbre B_1 de B engendrée par $b_1, \ldots, b_n$ est un A-module de type fini d'après (1). On en déduit que $B_1[x]$ est un A-module de type fini. Comme la multiplication par x envoie $B_1[x]$ dans lui-même, ceci démontre l'assertion.

Démontrons (3). Soient x et y des éléments de A' et soient M et N deux A-modules de type fini dans B tels que M contienne xM et N contienne yN. Il suffit de remarquer que la multiplication par $x + y$, $x - y$ et xy envoie le A-module de type fini MN dans lui-même. La deuxième assertion résulte de (2): tout élément de B entier sur A' est entier sur A.

LEMME 7. *Soit A un anneau factoriel et soit L une extension finie de son corps des fractions K.*

(1) La fermeture intégrale de A dans K est égale à A.

(2) Le polynôme minimal de tout élément x de L entier sur A appartient à $A[T]$.

Désignons par $\frac{x}{y}$ un élément de K et par $a_1, \ldots, a_n$ des éléments de A tels que

$$\left(\frac{x}{y}\right)^n + a_1\left(\frac{x}{y}\right)^{n-1} + \ldots + a_n = 0 .$$

On peut écrire cette relation sous la forme

$$x^n + a_1 y x^{n-1} + \ldots + a_n y^n = 0 .$$

On en déduit aisément que tout élément irréductible de A divisant y divise aussi x, ce qui démontre la première assertion.

Désignons par p le polynôme minimal de x dans $K[T]$ et par r un polynôme monique de $A[T]$ tel que $r(x)$ soit nul. Il existe un polynôme q de $K[T]$ tel que

$$r = pq .$$

Dans une extension convenable $\tilde{K}$ de K, on peut écrire

$$p = \prod_{1 \leq j \leq m} (T - \alpha_j) \qquad q = \prod_{1 \leq k \leq n} (T - \beta_k).$$

Par définition, les éléments $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ appartiennent à la fermeture intégrale A' de A dans $\tilde{K}$. Ceci montre que les coefficients de p (et de q) sont entiers sur A (lemme 6). L'assertion résulte alors de (1).

THÉORÈME 2 (Noether). *Soit κ un corps infini et soit B une κ-algèbre intègre. On suppose que B est engendrée par des éléments $y_1, \ldots, y_m$ et que le degré de transcendance sur κ du corps des fractions L de B est égal à n.*

Il existe alors une famille $(a_{jk})_{1 \leq j \leq n,\, 1 \leq k \leq m}$ *d'éléments de* κ *telle que* B *soit entier sur* $\kappa[x_1, \ldots, x_n]$, *où l'on a posé*

$$x_j = \sum_{1 \leq k \leq m} a_{jk} y_k \quad \text{pour} \quad 1 \leqslant j \leqslant n .$$

La démonstration va se faire par récurrence sur $m - n$, l'assertion étant triviale si n est égal à m.

Supposons donc $m - n$ strictement positif. Il existe un polynôme p non nul de $\kappa[T_1, \ldots, T_m]$ tel que

$$p(y_1, \ldots, y_m) = 0 .$$

Ce polynôme s'écrit d'une manière et d'une seule

$$p = p_0 + \ldots + p_r$$

où p_j est homogène de degré j et p_r non nul. Désignons par $a_1, \ldots, a_{m-1}$ des éléments de κ tels que $p_r(a_1, \ldots, a_{m-1}, 1)$ soit non nul et posons

$$t_1 = y_1 - a_1 y_m, \ldots, \; t_{m-1} = y_{m-1} - a_{m-1} y_m, \; t_m = y_m .$$

Par substitution, on voit que l'on a

$$t_m^r \, p_r(a_1, \ldots, a_{m-1}, 1) + q(t_1, \ldots, t_m) = 0$$

où q est un polynôme de degré strictement inférieur à r en t_m. Ceci montre que t_m est entier sur l'anneau $\kappa[t_1, \ldots, t_{m-1}]$. Le lemme 6 et l'hypothèse de récurrence fournissent alors le résultat.

Conservons les notations du théorème 2. On désigne par A l'anneau $\kappa[x_1, \ldots, x_n]$ et par K son corps des fractions. Il existe des éléments $x_{n+1}, \ldots, x_m$ de B qui engendrent le A-module B et le théorème de l'élément primitif implique qu'il existe une combinaison linéaire α de $x_{n+1}, \ldots, x_m$ telle que

$$L = K(\alpha) .$$

Désignons par p le polynôme minimal de α. C'est un polynôme monique irréductible appartenant à $A[T]$ (lemme 7). Son discriminant Δ est non nul (lemme 4).

LEMME 8. *La multiplication par* Δ *envoie* B *dans* $A[\alpha]$.

Dans une extension convenable $\tilde{K}$ de K, on peut écrire

$$p = \prod_{1 \leq j \leq r} (T - \alpha_j) \quad \text{avec} \quad \alpha = \alpha_1 .$$

Tout élément x de L s'écrit d'une manière et d'une seule

$$x = \sum_{0 \leq k \leq r-1} \xi_k \alpha^k$$

avec $\xi_0, \ldots, \xi_{r-1}$ dans K. On pose alors

$$x^{(j)} = \sum_{0 \leq k \leq r-1} \xi_k \alpha_j^k$$

pour tout entier j compris entre 1 et r. Le déterminant de ce système d'équations linéaires est donné par la formule

$$D = \begin{vmatrix} 1 & \alpha_1 & . & . & . & \alpha_1^{r-1} \\ 1 & \alpha_2 & . & . & . & \alpha_2^{r-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & \alpha_r & . & . & . & \alpha_r^{r-1} \end{vmatrix} = \prod_{1 \leq j < k \leq r} (\alpha_k - \alpha_j)$$

Le carré de ce déterminant n'est autre que le discriminant Δ. Ceci montre que le système d'équations ci-dessus admet une solution et une seule

$$\xi_k = \frac{1}{D} \sum_{1 \leq j \leq r} a_{k,j} x^{(j)} .$$

Notons que D et les éléments $a_{k,j}$ appartiennent à la fermeture intégrale A' de A dans $\tilde{K}$. D'autre part, si x est entier sur A, il en est ainsi des éléments $x^{(2)}, \ldots, x^{(r)}$ et par conséquent de

$$\Delta \xi_k = D \sum_{1 \leq j \leq r} a_{k,j} x^{(j)} .$$

Comme ce dernier élément appartient à K, il est dans A (lemme 7). Le lemme en découle aussitôt.