152 Déterminant. Exemples et applications

I Formes n-linéaires alternées, déterminant

A anneau commutatif unitaire, E A-module libre de rang n

I.1. Formes n-linéaires alternées, déterminant dans une base

Def 1 Une application n-linéaire $E^n \to A$ est dite alternée si pour tous $x_1, \dots, x_n \in E$ tels qu'il existe $i \neq j$ avec $x_i = x_j$, alors $f(x_1, \dots, x_n) = 0$

Def/Prop 2 L'ensemble des formes n-linéaires alternées sur E est un module libre de rang 1. Pour toute base B de E, il existe une unique application n-linéaire alternée telle que $f(B) = 1$. On l'appelle déterminant dans la base B, noté $\det_B$. Si $x_i = \sum_{j=1}^{n} x_{i,j} e_j$ dans la base B ($B = (e_1, \dots, e_n)$). On a
$$\det_B(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1\sigma(1)} \times \dots \times x_{n\sigma(n)}$$

Prop 3 Soit f forme n-linéaire alternée, B une base. Alors $f = f(B) \times \det_B$.
En particulier, si B et B' sont deux bases, $\det_{B'} = \det_{B'}(B) \times \det_B$

Rq 4 Ajouter à x_i une combinaison linéaire de $x_1, \dots x_{i-1}, x_{i+1}, \dots, x_n$ ne change pas la valeur du déterminant (dans n'importe quelle base)

Ex 5 Si B est la base canonique de $\mathbb{R}^2$, $x_1 = (a_1\ b_1)$ $x_2 = (a_2\ b_2)$, alors $\det_B(x_1, x_2) = a_1 b_2 - a_2 b_1$

I.2 Déterminant d'un endomorphisme, d'une matrice

Def 6 Soit $f \in End(E)$. On note $\det(f) = \det_B(f(B))$ (ne dépend pas de la base B)

Ex 7 $\det(Id_E) = 1$

Def 8 Soit $M \in M_n(A)$. On note $\det(M)$ le déterminant de l'application induite par M sur A^n

Prop 9 Si M est la matrice de f dans une certaine base, $\det(f) = \det(M)$

Prop 10 • Soient $M, N \in M_n(A)$. $\det(MN) = \det(M)\det(N)$
• Soient $f, g \in End(E)$. $\det(fg) = \det(f)\det(g)$

Prop 11 Si $M \in GL_n(A)$, $\det(M) \in A^\times$

Prop 12 : $\det : GL_n(A) \to A^\times$ est un morphisme de groupes surjectif

Def 13 On appelle groupe spécial linéaire le groupe $SL_n(A) := \ker(\det)$

Appli 14 On a un isomorphisme de groupes $GL_n(A) \cong SL_n(A) \rtimes A^\times$

II Cofacteurs, comatrice, méthodes de calcul

On note $M_{i,j}$ le coefficient de M en position (i,j)

II.1. Mineurs, cofacteurs, comatrice

Def 15 Soit $M \in M_n(A)$. On appelle mineur de M tout déterminant d'une matrice extraite. Dans le cas où l'on a supprimé la i-ème ligne et j-ième colonne, on le note $\Delta_{i,j}$. On appelle cofacteur en (i,j) noté $cof_{i,j}$, l'élément $(-1)^{i+j}\Delta_{i,j}$

Prop 16 (développement selon une ligne/colonne)
• $\det M = \sum_{i=1}^{n} cof_{i,j} M_{i,j}$ pour tout j • $\det M = \sum_{j=1}^{n} cof_{i,j} M_{i,j}$ pour tout i

Ex 17 : $\det \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} = \det(M)$

Rq 18 : Ces formules fournissent un algorithme de calcul du déterminant en $O(n!)$

Prop 19 Si A est un corps, le rang de M est le plus grand entier r tel qu'il existe une matrice extraite de M de taille $r \times r$ de déterminant non nul

Appli 20 Dans le cas $A = \mathbb{R}$ ou $\mathbb{C}$, l'ensemble des matrices de rang inférieur ou égal à d est un fermé

Def 21 (Comatrice) Soit $M \in M_n(A)$. On appelle comatrice de M, notée $\hat{M}$, la matrice des cofacteurs de M

Ex. 22 Sur $\mathbb{Z}$ si $M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ $\hat{M} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ & ...

Prop 23 $M \times \hat{M}^t = \hat{M}^t \times M = \det(M) \times I_n$

Appli 24 Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $M \in GL_2(A)$, $M^{-1} = \det(M)^{-1} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Th 25 Soit $f \in End(A^n)$. Alors $\boxed{DV1}$
• f est surjectif si et seulement si f est bijectif si et seulement si $\det(f) \in A^\times$
• f est injectif si et seulement si $\det(f)$ n'est pas diviseur de zéro
On calcule le conoyau de f dans le cas $A = \mathbb{Z}$, $A = K[T_1, \dots, T_n]$

Coro 26 Soient $x_1, \dots, x_n \in E$. $x_1, \dots, x_n$ sont libres si et seulement si leur déterminant dans une base n'est pas un diviseur de zéro

• $x_1,\dots,x_n$ sont une base si et seulement si leur déterminant dans une base est inversible

II.2 Méthodes de calcul (On s'intéresse au calcul de déterminant de matrices)

Prop 27 $\det(M) = \det(M^t)$

Rq 28 Par le résultat précédent, toute opération effectuée sur les colonnes pour calculer le déterminant peut aussi être effectuée sur les lignes ; dans la suite, on énonce les résultats sur les colonnes

Prop 29 • Le déterminant dépend linéairement des colonnes : multiplier une colonne par $a \in A$ multiplie le déterminant par a

• ajouter à une colonne une combinaison linéaire des autres colonnes ne change pas le déterminant

• échanger les colonnes selon $\sigma \in \mathfrak{S}_n$ multiplie le déterminant par $\varepsilon(\sigma)$

Appli 30 • Vandermonde : $\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & & & \vdots \\ \vdots & & & & \\ 1 & x_n & \cdots & \cdots & x_n^{n-1}\end{pmatrix} = \prod_{1\le i<j\le n} (x_j - x_i)$

• circulant (sur un corps K) $\det\begin{pmatrix} c_1 & \cdots & c_n \\ c_n & c_1 \cdots & c_{n-1} \\ \vdots & & \\ c_2 & \cdots c_n & c_1\end{pmatrix} = \prod_{i=1}^{n} P(y_i)$ où $\begin{cases} P = \sum_{i=0}^{n-1} c_{i+1} X^i \\ \text{les } y_i \text{ sont les racines } n\text{-ièmes de l'unité dans une clôture algébrique}\end{cases}$

Prop 31 Si $M = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}$, $\det(M) = \prod_{i=1}^{n} \lambda_i$; $\det\left(\begin{array}{c|c} A & B \\ \hline 0 & C\end{array}\right) = \det(A) \times \det(C)$

Prop 32 L'algorithme de Gauss (exemple en annexe) permet le calcul du déterminant avec une complexité (en nombre d'opérations) en $O(n^3)$ (sur un corps uniquement)

III Applications à l'algèbre

III.1 Système de Cramer

Def 33 Un système de Cramer est un système d'équations linéaires $MX=B$ où $M \in GL_n(A)$, $X, B \in M_{n,1}(A)$ d'inconnue X

Prop 34 Soit $MX=B$ un système de Cramer. L'équation possède une unique solution $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n\end{pmatrix}$ avec $x_i = \det_{B_c}(M_1,\dots,M_{i-1},B,M_{i+1},\dots,M_n) \times \det(M)^{-1}$

où B_c est la base canonique de A^n, et M_i la i-ème colonne de M

Ex 35 Si $M = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$, $B = \begin{pmatrix} \lambda \\ \mu\end{pmatrix}$, $x_1 = (ad-bc)^{-1} \times (\lambda d - \mu b)$, $x_2 = (ad-bc)^{-1} \times (\mu a - \lambda c)$

III.2 Polynôme caractéristique

Def 36 Soit $M \in M_n(A)$. On appelle polynôme caractéristique de M noté χ_M, le polynôme $\det(X I_d - M)$. Pour $P \in GL_n(A)$, $\chi_{PMP^{-1}} = \chi_M$: on définit le polynôme caractéristique de $f \in \mathrm{End}(E)$ comme celui de sa matrice dans une base quelconque

Ex 37 Si $M = \begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix} \in M_2(\mathbb{R})$, $\chi_M = X^2+1$

Th 38 (Cayley Hamilton) $\chi_M(M) = 0$

Appli 39 Calcul du polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$

On se place désormais sur un corps K

Def 40 Une valeur propre de $f \in \mathrm{End}(E)$ est un élément $\lambda \in K$ tel qu'il existe $v \in E\setminus\{0\}$ tel que $f(v) = \lambda v$

Ex 41 Si f est la multiplication par $\begin{pmatrix} 1 & 1 \\ 0 & 2\end{pmatrix}$ dans $\mathbb{C}^2$, les valeurs propres de f sont 1, 2

Prop 42 Les valeurs propres de f sont exactement les racines de χ_f.

Appli 43 On a $\chi_M(X) = \sum_{i=0}^{n-1} c_i X^i + X^n$ où $c_i = (-1)^{n-i} \sum_{\lambda \in \Lambda} \Sigma_i(\lambda)$ avec Σ_i le i-ème polynôme symétrique élémentaire et Λ l'ensemble des (*)

III.3 Résultant, discriminant

On suppose A intègre factoriel

On fixe $P = a_0 + \dots + a_p X^p$, $Q = b_0 + \dots + b_q X^q$, $a_p \neq 0$, $b_q \neq 0$

On note $A_k[X]$ l'ensemble des polynômes de degré inférieur ou égal à k

Def 44 Soit $\varphi : A_{q-1}[X] \times A_{p-1}[X] \to A_{p+q-1}[X]$, $(U,V) \mapsto UP+VQ$

On appelle matrice de Sylvester de P et Q la matrice de φ dans les bases :

$((1,0),(X,0),\dots,(X^{q-1},0),(0,1),(0,X),\dots,(0,X^{p-1}))$

$(1, X, \dots, X^{p+q-1})$

(*) valeurs propres de M dans un corps de décomposition de χ_M (comptées avec multiplicité)

Ex 45 Si $P = X^2 + aX + b$ $Q = X + c$, leur matrice de Sylvester est
$\begin{pmatrix}1&1&0\\a&c&1\\b&0&c\end{pmatrix}$

Def 46 On appelle résultant de P et Q, noté $Res(P,Q)$, le déterminant de la matrice de Sylvester de P et Q

Ex 47 En reprenant l'exemple précédent, $Res(P,Q) = c^2 + b - ac$

Prop 48 P et Q ont un facteur commun non constant (dans $A[X]$) si et seulement si leur résultant est nul

Prop 49 Si A est un corps algébriquement clos, on peut remplacer "avoir un facteur commun non constant" par "avoir une racine commune"

Rq 50 Par $A[X_1,\dots,X_n] \cong A[X_1,\dots,X_{n-1}][X_n]$, la prop 48 est vraie pour des polynômes à plusieurs variables. On notera $Res_{X_n}(P,Q) \in A[X_1,\dots,X_{n-1}]$

Appli 51 Les courbes d'équation $X^2+Y^2=2$, $XY=1$ se coupent en $(1,1)$, $(-1,-1)$ dans $\mathbb{R}^2$, $\mathbb{C}^2$

Thm 52 Soient $P, Q \in \mathbb{C}[X,Y]$ sans facteurs communs. Soient d, d' le degré total de P et Q. Soit $V(P) = \{(x,y)\in\mathbb{C}^2 \mid P(x,y)=0\}$. Alors $|V(P)\cap V(Q)| \leq dd'$ $\boxed{\text{DEV 2}}$

On se place sur un corps K

Def 53 Soit $P\in K[X]$ de degré $p \geq 2$. On appelle discriminant de P l'élément $dis(P) = (-1)^{\frac{p(p-1)}{2}} a_p^{-1} res(P,P')$

Prop 54 Si P est scindé sur K, alors P est à racines simples ssi $dis(P)\neq 0$

IV Applications à la topologie, à l'analyse

IV 1 L'application déterminant sur $\mathbb{R}$, $\mathbb{C}$ — Ici $K=\mathbb{R}$ ou $\mathbb{C}$, $M_n(K)$ muni de sa topologie usuelle

Prop 55 $\det : M_n(K) \to K$ est continue

Appli 56 • $GL_n(\mathbb{C})$ est un ouvert dense connexe
• $GL_n(\mathbb{R})$ est un ouvert dense non connexe
• $SL_n(K)$ est fermé

Coro 57 L'ensemble des matrices avec n valeurs propres distinctes est un ouvert dense (dans $\mathbb{C}$)

Appli 58 $\chi_{AB} = \chi_{BA}$ sur $\mathbb{C}$, $\mathbb{R}$

Appli 59 Preuve de Cayley-Hamilton pour les matrices diagonalisables

Prop 60 det est une application C^∞ et $D(\det)_X(H) = Tr({}^t com(X) H)$

Appli 61 $SL_n(\mathbb{R})$ est une variété de dimension n^2-1, d'espace tangent en l'identité les matrices de trace nulle

IV 2. Volume et déterminant. On note λ la mesure de Lebesgue sur $\mathbb{R}^n$

Def 62 Soient $v_1,\dots,v_n \in \mathbb{R}^n$. La mesure de Lebesgue du parallélépipède délimité par $v_1,\dots,v_n$ est égal à la valeur absolue du déterminant de $v_1,\dots,v_n$ dans une base orthonormée (le déterminant d'une matrice orthogonale vaut ±1)

Appli 63 L'aire d'un triangle de sommets $(x_1,y_1),(x_2,y_2),(x_3,y_3)$ est $\frac{1}{2}[(x_2-x_1)(y_3-y_1)-(x_3-x_1)(y_2-y_1)]$

Appli 64 Inégalité de Hadamard : $|\det(M)| \leq \prod_{i=1}^{n} \|M_i\|$ (colonnes de M)

Prop 65 Pour X mesurable, A matrice, $\lambda(AX) = |\det A||X|$

Def 66 Soit $f\in C^1(\mathbb{R}^n,\mathbb{R}^n)$. Le jacobien de f en x, noté $\det(J_f(x))$ est le déterminant de l'application linéaire $(Df)_x$

Prop 67 Soit $f \in C^1(\mathbb{R}^n,\mathbb{R}^n)$ tel que $f(0)=0$, $(Df)_0$ soit inversible. Alors
$$\lim_{r\to 0} \frac{\lambda(f(B(0,r)))}{\lambda(B(0,r))} = |\det(J_f(x))|$$

Thm 68 Soit $\phi : U \to V$ un C^1-difféomorphisme, $f \in L^1(V)$. Alors $x \mapsto f(\phi(x))|\det J_\phi(x)| \in L^1(U)$ et $\int_V f(y)dy = \int_U f(\phi(x))|\det(J_\phi(x))|dx$

Appli 69 Si X, Y sont indépendantes de loi normale $N(0,\sigma^2)$ alors $R = X^2+Y^2$, $\Theta = \arctan\left(\frac{Y}{X}\right)$ (défini presque partout) vérifient $R \sim \mathcal{E}\left(\frac{1}{2\sigma^2}\right)$, $\Theta \sim \mathcal{U}[0,2\pi]$

Références

Partie I-II Gourdon + Lang (adapter les résultats de Gourdon au cas d'un anneau quelconque)

Cramer : Gourdon

Polynôme caractéristique : Gourdon

Résultant : Tauvel

Jacobien) changement de variable. Gourdon (Analyse) + Rouvière

DEV 1 Dans les documents du site de la prépa agreg de Rennes 1

DEV 2

Exemple d'utilisation du pivot de Gauss pour le calcul de déterminant

$$M = \begin{pmatrix} 3 & 7 & 9 \\ 2 & 0 & -1 \\ 0 & 5 & 8 \end{pmatrix}$$

$$M \sim \begin{pmatrix} 3 & 7 & 9 \\ 0 & -14/3 & -7 \\ 0 & 5 & 8 \end{pmatrix} \sim \begin{pmatrix} 3 & 7 & 9 \\ 0 & -14/3 & -7 \\ 0 & 0 & 1/2 \end{pmatrix}$$

$$\det(M) = 3 \times (-14/3) \times (1/2) = -7$$

* Pourquoi $\det(a, \dots, a, \dots, b, \dots, 0) = -\det(a, \dots, b, \dots, a, \dots, 0)$
* Pourquoi $\det(a_1, \dots, a_n) = \varepsilon(\sigma) \det(a_{\sigma(1)}, \dots, a_{\sigma(n)})$
* $\det \exp(A)$ avec $A \in \mathcal{M}_n(\mathbb{C})$.
* Démo de Vandermonde.
* toutes les formes n-linéaires alternées sont-ils des déterminant.
* si $AB = BA$, Montrer que $\mathrm{Com}(A)$ et $\mathrm{Com}(B)$ commutent.

* équadiff, wronskien
* forme quadratique : invariant (dans $\mathbb{Q}$, dans $\mathbb{F}_q$).
* géométrie : * points coplanaires...
  * points milieu d'un poly qui converge vers le barycentre des racines.

Autres DEV : * ellipsoïde de John...
* Wronskien.
* Déterminant de Cayley-Menger.
* $GL_n(\mathbb{R})$ a 2 composantes connexes ?

produit vectoriel.

Th de Müntz

Det de Gram.

Déterminant des matrices à coefficients dans un anneau

Cette note présente une relecture (complétée) d'un résultat que l'on trouve dans LEICHTNAM, SCHAUER, Exercices corrigés de Mathématiques posés aux oraux X-ENS, Algèbre 1, *Ellipses*. Il peut servir de développement pour la leçon :

- Déterminant. Exemples et applications.

Par ailleurs, comme les anneaux les plus importants au programme (mis à part les corps) sont les anneaux principaux, en insistant plus sur l'aspect ¡¡ matrices à coefficients dans un anneau principal ¿¿ on peut aussi imaginer une utilisation dans les leçons :

- Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- Anneaux principaux. Applications.

Soit donc A un anneau commutatif avec un élément unité noté 1.

Théorème : *Soit M une matrice de taille n à coefficients dans A, et $f : A^n \to A^n$ l'endomorphisme A-linéaire associé. Alors :*

(1) *f est surjectif ssi f est bijectif ssi* $\det(f)$ *est inversible dans A.*
(2) *f est injectif ssi* $\det(f)$ *est non diviseur de zéro dans A.*

De plus, dans le cas injectif,

(3) *Si $A = \mathbb{Z}$, le conoyau de f est fini de cardinal* $|\det(f)|$.
(4) *Si $A = k[X]$, le conoyau de f est un k-espace vectoriel de dimension finie égale à* $\deg(\det(f))$.

Rappelons que le *conoyau* est le quotient de l'ensemble but par l'image, i.e. $\operatorname{coker}(f) = A^n/f(A^n)$. Le conoyau est une mesure du défaut de surjectivité de la même façon que le noyau est une mesure du défaut d'injectivité. Ainsi, f est surjectif si et seulement si $\operatorname{coker}(f) = 0$.

Démonstration : On notera $e_1, \dots, e_n$ la base canonique de A^n.

(1) Si f est surjectif, pour tout i il existe un vecteur ϵ_i tel que $f(\epsilon_i) = e_i$. Si l'on pose $g(e_i) = \epsilon_i$ pour tout i, on définit un unique morphisme $g : A^n \to A^n$. De plus, on a $f \circ g = \mathrm{Id}$ car ceci est vrai pour tous les e_i, qui forment une partie génératrice. On en déduit que $\det(f)\det(g) = 1$ et donc $\det(f)$ est inversible. Alors, la formule de la comatrice :

$$M\,{}^t\tilde{M} = {}^t\tilde{M}M = \det(M)\,\mathrm{Id}$$

montre que f est bijectif. Comme enfin bijectif implique surjectif, on a tout démontré.

(2) Posons $d = \det(f)$. Si d est non diviseur de zéro, supposons que $f(x) = 0$. Matriciellement, on a $Mx = 0$ et en appliquant la transposée de la comatrice, on trouve $dx = 0$. En regardant les coordonnées de x, l'hypothèse sur d implique que $x = 0$ donc f est injectif.

Réciproquement, si d est diviseur de zéro, on va montrer que f n'est pas injectif. Soit $u \in A$ non nul tel que $ud = 0$.

Si pour tout mineur μ de M on a $u\mu = 0$, alors en particulier ceci est vrai pour les mineurs de taille 1, i.e. les coefficients de la matrice M. On a donc $f(ue_1) = 0$, or $ue_1 \neq 0$, donc f n'est pas injectif.

Sinon, il existe une matrice extraite N de M telle que $u\det(N) \neq 0$. Choisissons une telle matrice de taille r maximale ; on a $r < n$ puisque $ud = 0$. Quitte à réordonner les vecteurs de base à la source et au but, c'est-à-dire à multiplier M à gauche et à droite par des matrices de permutation, on peut supposer que N est la matrice de taille r située en haut à gauche. Maintenant, pour chaque $i \in \{1, \dots, n\}$, bordons les r premières lignes de M inférieurement avec la i-ème ligne, et appelons P_i la matrice de taille $r+1$ située à gauche :

$$P_i = \begin{pmatrix} m_{1,1} & \dots & m_{1,r+1} \\ \vdots & & \vdots \\ m_{r,1} & \dots & m_{r,r+1} \\ m_{i,1} & \dots & m_{i,r+1} \end{pmatrix} .$$

Pour $i \leq r$ la matrice P_i a deux lignes égales donc son déterminant est nul, et pour $i \geq r+1$ c'est une matrice extraite de M de taille $r+1$, donc son déterminant est annulé par u compte tenu de l'hypothèse sur r. Dans les deux cas $u\det(P_i) = 0$, et si on développe par rapport à la dernière ligne, on trouve $u\sum_{j=1}^{r+1}(-1)^j m_{i,j}\mu_j = 0$ où μ_j est le mineur du coefficient de position $(r+1, j)$. Pour i variant, ces égalités disent exactement que $M(ux) = 0$ où x est le vecteur de coordonnées $(-\mu_1, \dots, (-1)^{r+1}\mu_{r+1}, 0, \dots, 0)$. Comme $u\mu_{r+1} = u\det(N) \neq 0$, on a $ux \neq 0$, donc f n'est pas injectif.

(3) D'après les résultats sur les classes de congruence de matrices à coefficients dans un anneau principal, il existe des matrices R, S inversibles à coefficients dans $\mathbb{Z}$ telles que $D := RMS$ est diagonale d'éléments diagonaux égaux aux facteurs invariants $d_1, \dots, d_n$ tels que $d_i | d_{i+1}$ pour tout i. On en déduit que

$$\operatorname{coker}(f) \simeq \mathbb{Z}^n / D(\mathbb{Z}^n) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$$

de sorte que $|\operatorname{coker}(f)| = d_1 \dots d_n = |\det(f)|$.

(4) Le raisonnement est le même : il existe des matrices R, S inversibles à coefficients dans $k[X]$ telles que $D := RMS$ est diagonale d'éléments diagonaux égaux aux facteurs invariants $P_1, \dots, P_n$ tels que $P_i | P_{i+1}$ pour tout i. On en déduit que

$$\operatorname{coker}(f) \simeq \frac{k[X]}{(P_1)} \times \dots \times \frac{k[X]}{(P_n)}$$

puis $\dim_k(\operatorname{coker}(f)) = \deg(P_1) + \dots + \deg(P_n) = \deg(P_1 \dots P_n) = \deg(\det(f))$. $\square$

Théorème de Bézout faible

Leçons concernées :
144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
152 : Déterminant. Exemples et applications.

Références :
Szpirglas, Mathématiques L3 - Algèbre, p 592
Mérindol, Nombres et algèbre, p 386

Soit k un corps infini et A dans $k[X][Y]$. On note $Z(A)$ l'ensemble des zéros de A sur k^2.

Théorème : Soient P et Q dans $k[X][Y]$ premiers entre eux et de degrés n et m.
Alors $\#Z(P) \cap Z(Q) \leqslant mn$.

Démonstration :
• *Étape 1 :* Montrons que $Z(P) \cap Z(Q)$ est fini.

Notons $R_Y = Res_Y(P, Q)$ et $R_X = Res_X(P, Q)$ et considérons $(x, y) \in Z(P) \cap Z(Q)$. Comme $R_Y(x) = Res_Y(P(x, Y), Q(x, Y))$ et que $P(x, Y)$ et $Q(x, Y)$ ont un facteur commun (car ils ont y comme racine commune), $R_Y(x) = 0$. De même, $R_X(y) = 0$.

Donc $\#Z(P) \cap Z(Q) \leqslant \#Z(R_Y)\#Z(R_X)$
Or, $\#Z(R_Y)\#Z(R_X) \leqslant deg(R_Y)deg(R_X)$ car R_X et R_Y sont non nuls, car P et Q sont premiers entre eux.
Donc $Z(P) \cap Z(Q)$ est fini.

• *Étape 2 :* Majoration de $deg(R_Y)$.

Notons
$$P(X, Y) = \sum_{k=0}^{p} a_k(X)Y^k \quad Q(X, Y) = \sum_{k=0}^{p} b_k(X)Y^k$$
On a alors $deg(a_k) \leqslant m - k$ et $deg(a_k) \leqslant n - k$.

R_Y est le déterminant de la matrice de Sylvester de P et Q en Y. Notons $C = (c_{i,j})$ cette matrice.
On a alors :

$$\forall j \in [\![1, q]\!] \qquad c_{i,j} = \begin{cases} a_{p-(i-j)} & \text{si } 0 \leqslant i - j \leqslant p \\ 0 & \text{sinon} \end{cases}$$

$$\forall j \in [\![q+1, q+p]\!] \qquad c_{i,j} = \begin{cases} b_{q-(i-j+q)} & \text{si } 0 \leqslant i - j + q \leqslant q \\ 0 & \text{sinon} \end{cases}$$

Donc

$$\forall \sigma \in \mathfrak{S}_{p+q},\ deg\Big(\epsilon(\sigma)\prod_{j=1}^{p+q} c_{\sigma(j),j}\Big) = \sum_{j=1}^{p+q} deg(c_{\sigma(j),j}) \leqslant \sum_{j=1}^{q}(m - p + \sigma(j) - j) + \sum_{j=q+1}^{q+p}(n - j + \sigma(j))$$
$$= mq - pq + np = mn + (m-p)(q-n) \leqslant mn$$

Or

$$R_Y = \sum_{\sigma \in \mathfrak{S}_{p+q}} \epsilon(\sigma) \prod_{j=1}^{p+q} c_{\sigma(j),j}$$

Donc $deg(R_Y) \leqslant mn$.

• *Étape 3 :* Un changement de variable.
Nous avons vu que pour tout (x,y) dans $Z(P) \cap Z(Q)$, $R_Y(x) = 0$. Donc, si les éléments de $Z(P) \cap Z(Q)$ ont tous des abscisses différentes, on a le résultat souhaité.
Montrons que, comme k est supposé infini et que $Z(P) \cap Z(Q)$ est fini, il existe une transvection de k^2 rendant toutes les abscisses des éléments de $Z(P) \cap Z(Q)$ différentes.

Posons $u \notin \{\frac{x-x'}{y'-y} \mid y \neq y',\ (x,y),\ (x',y') \in Z(P) \cap Z(Q)\}$

Comme $Z(P) \cap Z(Q)$ est fini et que k est infini, un tel u existe.
On peut alors effectuer le changement de variable $X' = X + uY,\ Y' = Y$ et poser $\tilde{P}(X',Y') = P(X,Y)$ et $\tilde{Q}(X',Y') = Q(X,Y)$.

De plus, si $(x,y) \neq (x',y')$, alors $x + uy \neq x' + uy'$. Donc la fonction suivante est injective :

$$\begin{aligned} \varphi \ : \ Z(P) \cap Z(Q) &\longrightarrow Z(Res_{Y'}(\tilde{P},\tilde{Q})) \\ (x,y) &\longmapsto x + uy \end{aligned}$$

φ est bien définie : si $(x,y) \in Z(P) \cap Z(Q)$, $P(x,y) = Q(x,y) = 0$ donc $\tilde{P}(x+uy,y) = \tilde{Q}(x+uy,y) = 0$ donc $Res_{Y'}(\tilde{P},\tilde{Q})(x+uy) = 0$.

Donc

$$\#Z(P) \cap Z(Q) \leqslant \#Z(Res_{Y'}(\tilde{P},\tilde{Q})) \leqslant deg(Res_{Y'}(\tilde{P},\tilde{Q}))$$

Finalement, Comme $deg(P) = deg(\tilde{P})$ et $deg(Q) = deg(\tilde{Q})$

$$deg(Res_{Y'}(\tilde{P},\tilde{Q})) \leqslant mn$$

Ce qui conclut la preuve.

Remarques : La version forte du théorème de Bézout affirme que , sous certains hypothèses, il y a exactement mn solutions, comptées avec multiplicités.
De plus, on peut considérer que k de cardinal quelconque, voire que k est un anneau intègre factoriel. En passant à la clôture algébrique du corps des fractions de k, on se ramène au cas du théorème sans réduire le nombre de solutions.