

Préliminaires

0-1 $A[X]$ est non vide; si P et Q sont deux éléments de $A[X]$ on voit que $P - Q$ appartient à $A[X]$. On en déduit que $(A[X], +)$ est un sous-groupe de $(K[X], +)$. On vérifie enfin que 1 appartient à $A[X]$ et que $A[X]$ est stable pour la multiplication. On peut alors conclure que $A[X]$ est un sous-anneau de $K[X]$.

0-2 Le déterminant d'une matrice est un polynôme à coefficients entiers en les coefficients de la matrice. On en déduit que si P et Q sont deux éléments de $A[X]$ alors $Res(P, Q)$ est un élément de A .

0-3 Ici $K = \mathbb{C}(X)$ et $A = \mathbb{C}[X]$. Soit P un élément de $\mathbb{C}[X][Y]$, il existe $A_j \in \mathbb{C}[X]$, pour $0 \leq j \leq n$, tels que $P(X, Y) = \sum_{j=1}^n A_j(X)Y^j$, puis en explicitant les polynômes A_j , $P(X, Y) = \sum_{j=1}^n \sum_{i=0}^{r_j} a_{i,j} X^i Y^j$. On a alors la forme souhaitée.

On suppose que $P(X, Y) = \sum_{i,j \geq 0} a_{i,j} X^i Y^j = \sum_{i,j \geq 0} b_{i,j} X^i Y^j$. On a alors la relation $\sum_{j \geq 0} (\sum_{i \geq 0} (a_{i,j} - b_{i,j}) X^i) Y^j = 0$, ce qui entraîne, par unicité de l'écriture des éléments de $K[Y]$ dans la base $(Y^j)_{j \in \mathbb{N}}$: pour tout $j \in \mathbb{N}$, $\sum_{i \geq 0} (a_{i,j} - b_{i,j}) X^i = 0$. On en déduit (en utilisant le même argument dans $\mathbb{C}[X]$) que, pour tous $i, j \geq 0$, $a_{i,j} = b_{i,j}$. On en conclut que P s'écrit de façon unique sous la forme proposée.

Enfin, si $P \neq 0$, $\{i + j \mid a_{i,j} \neq 0\}$ est un sous-ensemble fini, non vide, de \mathbb{N} , il admet donc un plus grand élément $d(P)$.

I La propriété fondamentale du résultant

I-1 On suppose P et Q non premiers entre eux. En appelant Δ le PGCD de P et Q , on a $P = \Delta P_1$ et $Q = \Delta Q_1$. On voit alors que le couple (Q_1, P_1) vérifie les relations demandées.

Réciproquement on suppose qu'il existe A et B non nuls vérifiant $\begin{cases} \deg A < \deg Q \text{ et } \deg B < \deg P \\ AP = BQ \end{cases}$. Le polynôme P divise AP et donc également BQ . Or, si P est premier avec Q , le théorème de Gauss permet d'affirmer que P divise B . Cela n'est pas possible car B est non nul et de degré strictement inférieur au degré de P . On en déduit que P et Q ne sont pas premiers entre eux.

I-2-a $(1, X, \dots, X^d)$ est clairement une base de $K[X]_d$; l'espace est donc de dimension $d + 1$.

I-2-b On a clairement $f((A, B) + \lambda(C, D)) = f(A + \lambda C, B + \lambda D) = f(A, B) + \lambda f(C, D)$ en utilisant les règles de calcul dans $K[X]$. On considère la famille $\mathcal{B} = ((1, 0), (X, 0), \dots, (X^{m-1}, 0), (0, 1), (0, X), \dots, (0, X^{n-1}))$, il est facile de montrer que c'est une base de $K[X]_{m-1} \times K[X]_{n-1}$ (par exemple en remarquant qu'elle est libre et de cardinal $m + n$). On considère ensuite \mathcal{B}' la base canonique de $K[X]_{m+n-1}$. On vérifie enfin que la matrice de f dans les bases \mathcal{B} et \mathcal{B}' est la transposée de la matrice résultante de l'énoncé.

I-3 On suppose que P et Q sont premiers entre eux. Soit $(A, B) \in \text{Ker } f$. On a alors $AP = -BQ$ avec $\deg A < m$ et $\deg B < n$. La question 1 permet d'affirmer que $A = 0$ ou $B = 0$. Mais si $A = 0$, alors $BQ = 0$ puis $B = 0$ (car $Q \neq 0$ et $K[X]$ est intègre). On fait de même si $B = 0$. Finalement on obtient $\text{ker } f = \{(0, 0)\}$, c'est-à-dire f est injective. On en déduit que f est un isomorphisme entre les deux espaces vectoriels de dimension $m + n$, $K[X]_{m-1} \times K[X]_{n-1}$ et $K[X]_{m+n-1}$, puis que le déterminant de la matrice de f dans les bases \mathcal{B} et \mathcal{B}' est non nul. On a donc montré que $Res_K(P, Q) \neq 0$.

Réciproquement on suppose que $Res_K(P, Q) \neq 0$. On en déduit que f est injective. La question 1 prouve alors que P et Q sont premiers entre eux.

I-4 Pour $\lambda \neq 0$, on a $\lambda^n P(\frac{X}{\lambda}) = \sum_{i=0}^n \lambda^{n-i} a_i X^i$ et $\lambda^m Q(\frac{X}{\lambda}) = \sum_{j=0}^m \lambda^{m-j} b_j X^j$.

Dans le calcul du résultant $Res_{\mathbb{C}}(\lambda^n P(\frac{X}{\lambda}), \lambda^m Q(\frac{X}{\lambda}))$ il faut donc remplacer, pour tous i, j , a_i par $\lambda^{n-i} a_i$ et b_j par $\lambda^{m-j} b_j$.

La matrice résultante de $\lambda^n P(\frac{X}{\lambda}), \lambda^m Q(\frac{X}{\lambda})$ se déduit donc de celle de P, Q par les opérations élémentaires suivantes :

- pour $1 \leq i \leq m$, multiplication de la ligne i par λ^{n+i-1} ;
- pour $1 \leq i \leq m$, multiplication de la ligne $m+i$ par λ^{m+i-1} ;
- pour $1 \leq j \leq m+n$, division de la colonne j par λ^{j-1} .

Le résultant est donc multiplié par $\lambda^{n+(n+1)+\dots+(n+m-1)} \times \lambda^{m+(m+1)+\dots+(m+n-1)}$ et divisé par $\lambda^{0+1+\dots+(m+n-1)}$ soit au total multiplié par λ^{mn} .

II Une courbe unicursale

Soit (x, y) un point de l'arc paramétré. Alors il existe $t \in \mathbb{R}$ tel que $\begin{cases} x = t^2 + t \\ y = t^3 + 2t^2 \end{cases}$. On considère les polynômes de $\mathbb{R}[X]$: $P(T) = T^2 + T - x$ et $Q(T) = T^3 + 2T^2 - y$. Ces deux polynômes admettent t comme racine commune, on en déduit qu'ils ne sont pas premiers entre eux et que $\text{Res}_{\mathbb{R}}(P, Q) = 0$.

$$\text{On a } \text{Res}_{\mathbb{R}}(P, Q) = \begin{vmatrix} -x & 1 & 1 & 0 & 0 \\ 0 & -x & 1 & 1 & 0 \\ 0 & 0 & -x & 1 & 1 \\ -y & 0 & 2 & 1 & 0 \\ 0 & -y & 0 & 2 & 1 \end{vmatrix} = -x^3 + y^2 - xy + 2x^2 - y$$

On en déduit que $-x^3 + y^2 - xy + 2x^2 - y = 0$ est une équation cartésienne de la courbe.

Réciproquement, soit (x, y) un point vérifiant $-x^3 + y^2 - xy + 2x^2 - y = 0$. Les polynômes $P(T)$ et $Q(T)$ précédents ne sont pas premiers entre eux donc admettent un diviseur commun $\Delta(T)$ non constant. $\Delta(T)$ est aussi un diviseur de $(T+1)P(T) - Q(T) = (1-x)T + y - x$ donc si $x \neq 1$ alors $\deg(\Delta) = 1$, Δ admet une racine $t \in \mathbb{R}$ et l'on a $P(t) = Q(t) = 0$ donc le point (x, y) est sur la courbe. Si $x = 1$, on constate que $y = 1$ et que $t = (-1 \pm \sqrt{5})/2$ est racine commune à $P(T)$ et $Q(T)$ donc le point $(1, 1)$ est aussi sur la courbe.

III Entiers algébriques

III-1 On déduit du préliminaire 0-2 que $\text{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y))$ est un élément de $\mathbb{Z}[X]$.

Si M est la matrice résultante les éléments de ses n_2 premières lignes sont dans $\mathbb{Z}[X]$ et ceux des n_1 dernières lignes sont dans \mathbb{Z} . Les seuls éléments de degré n_1 sont situés sur la diagonale de M . De l'expression $\det M = \sum_{\sigma \in \mathcal{S}_{m+n}} \epsilon(\sigma) m_{1,\sigma(1)} \dots m_{m+n,\sigma(m+n)}$, on déduit que $\text{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y))$ est de degré au plus $n_1 n_2$. De plus pour avoir un terme de degré $n_1 n_2$, il faut nécessairement prendre les n_2 premiers termes sur la diagonale, c'est-à-dire imposer $\sigma(i) = i$ pour tout $1 \leq i \leq n_2$. On voit qu'ensuite, pour n'avoir aucun terme nul dans le produit, il faut, pour tout $n_2 + 1 \leq i \leq n_2 + n_1$, $\sigma(i) \leq i$. Seul $\sigma = id$ vérifie les conditions imposées, et on vérifie facilement que $\prod_{i=1}^{n_1+n_2} m_{i,i}$ est unitaire de degré $n_1 n_2$.

De plus $\text{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y))(z_1 + z_2) = \text{Res}_{\mathbb{Q}}(P_1(z_1 + z_2 - Y), P_2(Y))$. Ce dernier résultant est nul car les deux polynômes $P_1(z_1 + z_2 - Y)$ et $P_2(Y)$ admettent z_2 comme racine commune et ils ne sont donc pas premiers entre eux.

On déduit des deux résultats précédents que $z_1 + z_2$ est un entier algébrique.

III-2 Il est clair que 1 est élément de \mathcal{O} car il est annulé par le polynôme $X - 1$. De plus si P_1 annule z_1 , alors $Q(X) = (-1)^{n_1} P_1(-X)$ est unitaire et annule $-z_1$. On déduit de ces deux propriétés et de la question précédente que \mathcal{O} est un sous-groupe de \mathbb{C} . Pour montrer que c'est un sous-anneau il suffit de prouver que \mathcal{O} est stable pour la multiplication.

Soit z_1 et z_2 éléments de \mathcal{O} non nuls (le cas où une des racines est nulle est trivial). On suppose donc qu'il existe P_1 et P_2 éléments unitaires de $\mathbb{Z}[X]$ tels que $P_1(z_1) = P_2(z_2) = 0$. En notant $P_2(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$, on a donc :

$$z_2^n + a_{n-1}z_2^{n-1} + \dots + a_0 = 0$$

et donc en divisant par z_2^n :

$$1 + a_{n-1}z^{-1} + \dots + a_0z^{-n} = 0$$

Donc le polynôme $Q(X) = a_0X^n + \dots + 1$ annule $1/z_2$. On pose alors $P(X) = \text{Res}_{\mathbb{C}(X)}(P_1(XY), Q(Y))$. Comme dans la question précédente, on montre que ce polynôme est unitaire de degré $nd(P_1)$. D'autre part $P_1(z_1z_2Y)$ et $Q(X)$ admettent comme racines commune $1/z_2$ et donc $P(z_1z_2) = \text{Res}_{\mathbb{C}}(P(z_1z_2Y), Q(Y)) = 0$. On conclut que z_1z_2 est algébrique.

IV Équations algébriques : le théorème de Bézout faible.

IV-1 On applique l'algorithme d'Euclide à P_1 et Q_1 . On obtient successivement $P_1 = (XY + 1)Q_1 + (-X^2Y - X)$, puis $Q_1 = (-X^2Y - X)(\frac{-1}{X}Y + \frac{1}{X^2}) + (X + \frac{1}{X})$. On en déduit P_1 et Q_1 sont premiers entre eux dans $\mathbb{C}(X)[Y]$. X est un facteur commun non constant aux polynômes X et X^2 . On déduit de ces résultats que P_1 et Q_1 vérifient (C_1) mais pas (C_2) .

Il est clair que P_2 et Q_2 vérifient (C_2) . En appliquant l'algorithme d'Euclide on montre qu'ils vérifient également (C_1) .

P_3 divise Q_3 donc les polynômes ne vérifient pas (C_1) . En revanche on voit qu'ils vérifient (C_2) .

IV-2-a On suppose que P et Q vérifient (C_1) . Donc, d'après le théorème de Bézout, il existe F_0, \dots, F_p et G_0, \dots, G_q éléments de $\mathbb{C}(X)$ tels que : $(\sum_{i=0}^p F_i(X)Y^i)P(X, Y) + (\sum_{j=0}^q G_j(X)Y^j)Q(X, Y) = 1$. En multipliant cette égalité par M le PPCM des dénominateurs des fractions $F_0, \dots, F_p, G_0, \dots, G_q$ on obtient une relation de la forme $AP + BQ = C$ avec $A, B \in \mathbb{C}[X][Y]$ et $C \in \mathbb{C}[X]$.

IV-2-b On suppose que P et Q vérifient (C_1) et (C_2) . Soit (z_1, z_2) solution du système. On a alors $C(z_1) = 0$. Or le polynôme C est non nul, il n'y a donc qu'un nombre fini de valeurs de z_1 possibles. Fixons un tel z_1 . On a $P(z_1, Y) = \sum_{i=0}^n P_i(z_1)Y^i$ et $Q(z_1, Y) = \sum_{j=0}^m Q_j(z_1)Y^j$. L'un au moins de ces deux éléments de $\mathbb{C}[Y]$ n'est pas nul car sinon $X - z_1$ diviserait les $n + m + 2$ polynômes $P_0, \dots, P_n, Q_0, \dots, Q_m$, ce qui contredirait (C_2) . Finalement pour cette valeur de z_1 Il n'y a qu'un nombre fini de z_2 tel que $P(z_1, z_2) = Q(z_1, z_2) = 0$. On en déduit que le système n'a qu'un nombre fini de solutions.

On suppose que P et Q ne vérifient pas (C_1) . Il existe $R(X, Y) = \sum_{k=0}^p R_k(X)Y^k$ non constant dans $\mathbb{C}(X)[Y]$ diviseur commun à P et Q . Soit $z_1 \in \mathbb{C}$ non racine de l'un des R_i , $1 \leq i \leq p$. $R(z_1, Y)$ est un élément non constant de $\mathbb{C}[Y]$. Il existe au moins un élément z_2 tel que $R(z_1, z_2) = 0$. On en déduit qu'il existe une infinité de couples (z_1, z_2) solutions du système (il existe une infinité de choix possibles pour z_1).

On suppose que P et Q ne vérifient pas (C_2) . Il existe $\alpha \in \mathbb{C}$ tel que $X - \alpha$ divise les $n + m + 2$ polynômes $P_0, \dots, P_n, Q_0, \dots, Q_m$. On voit alors que, pour tout $z \in \mathbb{C}$, $P(\alpha, z) = Q(\alpha, z) = 0$ et donc que le système admet une infinité de solutions.

IV-3 Soit $\sum_{k=0}^n a_k X^k Y^{n-k}$ la somme des termes de degré n dans $P(X, Y)$ et $\sum_{k=0}^m b_k X^k Y^{m-k}$ la somme des termes de degré m dans $Q(X, Y)$. On pose $Z = X + \lambda Y$ où $\lambda \in \mathbb{C}$ est à déterminer. Soient P_1, Q_1 les polynômes définis par $P_1(Z, Y) = P(X + \lambda Y, Y)$ et $Q_1(Z, Y) = Q(X + \lambda Y, Y)$. On a de manière évidente $d(P_1) \leq n$, $d(Q_1) \leq m$. De plus, le terme en Y^n dans P_1 est égal à $\sum_{k=0}^n a_k \lambda^k Y^n = P_2(\lambda)Y^n$ et celui en Y^m dans Q_1 est égal à $\sum_{k=0}^m b_k \lambda^k Y^m = Q_2(\lambda)Y^m$. Il suffit donc de choisir λ non racine de P_2 ni Q_2 ce qui est possible car ces polynômes sont non nuls.

IV-4 On a $R(z) = \text{Res}_{\mathbb{C}}(P(z, Y), Q(z, Y))$. D'après **I-4** on a $\frac{R(z)}{z^{mn}} = \text{Res}_{\mathbb{C}}(\frac{1}{z^n}P(z, zY), \frac{1}{z^m}Q(z, zY))$.

Or $\frac{1}{z^n}P(z, zY) = \sum_{i=0}^n \frac{1}{z^{n-i}}P_i(z)Y^i$. Chaque P_i étant de degré inférieur ou égal à $n - i$, et donc, pour tout $0 \leq i \leq n$, $\frac{1}{z^{n-i}}P_i(z)$ admet une limite (égale au coefficient de degré $n - i$ de P_i) quand $|z|$ tend vers $+\infty$. On procède de même pour $\frac{1}{z^m}Q(z, zY)$ et on en déduit que tous les éléments de la matrice résultante ont une limite quand $|z|$ tend vers $+\infty$. On en conclut, par continuité du déterminant, que $\text{Res}_{\mathbb{C}}(\frac{1}{z^n}P(z, zY), \frac{1}{z^m}Q(z, zY))$ admet une limite finie quand $|z|$ tend vers $+\infty$.

IV-5 P et Q vérifiant (C_1) et (C_2) , le système en $(x, y) : P(x, y) = Q(x, y) = 0$ a un nombre fini de solutions. Si l'on transforme P et Q en P_1 et Q_1 comme au **IV-3** le système transformé a aussi un nombre fini de solutions donc P_1 et Q_1 vérifient aussi (C_1) . En particulier, le polynôme $R_1(Z) = \text{Res}_{\mathbb{C}(Z)}(P_1(Z, Y), Q_1(Z, Y))$ est non nul et de degré au plus mn d'après la question précédente. Considérons $u \in \mathbb{C}$ tel que le système en $v : P_1(u, v) = Q_1(u, v) = 0$ admette k solutions v_1, \dots, v_k . On démontre que u est racine d'ordre k de $R_1(Z)$ ce qui suffit à prouver que le système en $(z, y) : P_1(z, y) = Q_1(z, y) = 0$ a au plus mn solutions.

On considère l'application :

$$f_1(Z) : \begin{cases} \mathbb{C}(Z)[Y]_{m-1} \times \mathbb{C}(Z)[Y]_{n-1} & \longrightarrow \mathbb{C}(Z)[Y]_{m+n-1} \\ (A, B) & \longmapsto AP_1 + BQ_1 \end{cases}$$

dont la matrice dans les bases canoniques de $\mathbb{C}(Z)[Y]_{m-1} \times \mathbb{C}(Z)[Y]_{n-1}$ et $\mathbb{C}(Z)[Y]_{m+n-1}$ est la transposée de la matrice résultante de $P_1(Z, Y), Q_1(Z, Y)$ considérés comme des polynômes en Y à coefficients dans $\mathbb{C}(Z)$.

Soit $S(Y) = (Y - v_1) \dots (Y - v_k)$, on prend comme nouvelle base de $\mathbb{C}(Z)[Y]_{m+n-1}$ la famille :

$$\mathcal{B} = (1, Y, \dots, Y^{k-1}, S, YS, \dots, Y^{m+n-k-1}S).$$

La matrice de f_1 dans la base canonique de $\mathbb{C}(Z)[Y]_{m-1} \times \mathbb{C}(Z)[Y]_{n-1}$ et la base \mathcal{B} est la matrice dans \mathcal{B} de la famille de polynômes en Y à coefficients dans $\mathbb{C}(Z)$:

$$\mathcal{F}(Z) = (P_1, YP_1, \dots, Y^{m-1}P_1, Q_1, YQ_1, \dots, Y^{n-1}Q_1).$$

On a donc $R_1(Z) = \alpha \det_{\mathcal{B}}(\mathcal{F}(Z))$ où $\alpha \in \mathbb{C}^*$ est le déterminant de la base canonique de $\mathbb{C}(Z)[Y]_{m+n-1}$ dans \mathcal{B} . Par hypothèse $P_1(u, Y)$ et $Q_1(u, Y)$ sont divisibles par $S(Y)$ donc les k premières coordonnées dans \mathcal{B} des polynômes constituant $\mathcal{F}(Z)$ sont des polynômes en Z nuls en u et donc divisibles par $Z - u$. Les k premières colonnes de $\text{mat}_{\mathcal{B}}(\mathcal{F}(Z))$ étant divisibles par $Z - u$, le déterminant est divisible par $(Z - u)^k$ comme annoncé.

IV-6 On prend les polynômes $P(X, Y) = XY^2 + X + 1$ et $Q(X, Y) = X^2Y^3 + XY^2$. Les solutions du système $P(z_1, z_2) = Q(z_1, z_2) = 0$ sont les couples $(-1, 0), (j, -\bar{j})$ et $(\bar{j}, -j)$. Les polynômes P et Q satisfont (C_1) et (C_2) et pourtant le système n'a pas $d(P)d(Q) (= 6)$ solutions.

V Topologie

On note D° l'intérieur de D . On va montrer que $D^\circ = \Gamma$ où Γ désigne l'ensemble des matrices diagonalisables dont les valeurs propres sont toutes distinctes.

Si P_M désigne le polynôme caractéristique de M alors $M \in \Gamma \Leftrightarrow P'_M = P_M$ sont premiers entre eux. On pose alors

$$\begin{aligned} \psi : M_n(\mathbb{C}) &\longmapsto \mathbb{C} \\ M &\longmapsto \text{Res}_{\mathbb{C}}(P_M, P'_M) \end{aligned}$$

La fonction ψ est continue et $\Gamma = \psi^{-1}(\mathbb{C}^*)$ donc Γ est un ouvert contenu dans D et donc $\Gamma \subset D^\circ$.

Réciproquement, on raisonne par l'absurde en supposant l'existence de M telle que : $M \in D^\circ$ et $M \notin \Gamma$. Il existe donc une matrice inversible P telle que :

$$P^{-1}MP = \begin{bmatrix} \lambda & 0 & \cdots & \cdots & 0 \\ 0 & \lambda & & & \vdots \\ \vdots & & \lambda_3 & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \lambda_n \end{bmatrix}$$

Pour tout p entier positif, on pose :

$$M_p = \begin{bmatrix} \lambda & 1/p & 0 & \cdots & 0 \\ 0 & \lambda & & & \vdots \\ \vdots & & \lambda_3 & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \lambda_n \end{bmatrix}$$

Cette matrice n'est pas diagonalisable car sinon la matrice $A = \begin{bmatrix} \lambda & 1/p \\ 0 & \lambda \end{bmatrix}$ serait diagonalisable donc semblable à λI_2 mais comme cette dernière matrice commute avec toutes les matrices de $M_2(\mathbb{C})$ on en déduit que A n'est pas diagonalisable.

De plus $M = \lim_{p \rightarrow +\infty} P M_p P^{-1}$ donc M appartient au complémentaire de D° dans $M_n(\mathbb{C})$ (limite d'une suite dans un fermé). Ce qui est absurde.