Corrigé du problème : résultant de deux polynômes

I. Définition et propriétés

1. **Cas où u est bijective**
   E et F sont des espaces vectoriels et u est clairement linéaire.
   Supposons u bijective. Alors le polynôme constant 1 possède un antécédent (A, B), qui fournit une identité de Bezout $PA + QB = 1$. Cela montre que P et Q sont premiers entre eux.
   Supposons P et Q premiers entre eux, en particulier P et Q sont non nuls. Montrons que $\ker u = \{0\}$. Soit $(A, B) \in E$ tel que $PA + QB = 0$. Alors $PA = -QB$, donc P divise QB. Comme P et Q sont premiers entre eux, par le lemme de Gauss, cela montre que P divise B. Or $B \in \mathbb{C}_{p-1}[X]$ signifie $\deg(B) < \deg(P)$. Donc $B = 0$. Comme $PA = 0$, $P \neq 0$ et $\mathbb{C}[X]$ est intègre, $A = 0$. Cela montre l'injectivité de u. Comme $\dim E = \dim F = p + q$, cela montre que u est bijective.
2. **Matrice de u**
   (a) Il est immédiat par définition que la matrice de u par rapport aux bases $\mathcal{B}$ et $\mathcal{B}'$ est $M_{P,Q}$.
   (b) L'application u est bijective si et seulement si sa matrice $M_{P,Q}$ est inversible, donc si et seulement si le déterminant $\mathrm{Res}(P, Q)$ de cette matrice est non nul. La question 1 montre que cela équivaut à P et Q sont premiers entre eux. Le corps $\mathbb{C}$ étant algébriquement clos, P et Q sont premiers entre eux si et seulement si ils n'ont pas de racine complexe commune. Cela conclut.
3. **Racine multiple**
   (a) On sait qu'un polynôme P de $\mathbb{C}[X]$ admet une racine multiple dans $\mathbb{C}$ si et seulement si P et P' ont une racine commune. Donc un polynôme P de $\mathbb{C}[X]$ admet une racine multiple dans $\mathbb{C}$ si et seulement si $\mathrm{Res}(P, P') = 0$.

   Remarque : Res(P, P') s'appelle le discriminant de P.

   (b) i. Si $a = 0$, le polynôme $aX^2 + bX + c$ est de degré $\leqslant 1$ et ne peut donc pas avoir de racine multiple. Sinon le polynôme $aX^2 + bX + c$ est de degré 2 et d'après la question précédente, il admet une racine multiple si et seulement si $\begin{vmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{vmatrix} = a(b^2 - 4ac) = 0$ donc si et seulement si $b^2 - 4ac = 0$. La condition nécessaire et suffisante pour que $aX^2 + bX + c$ admette une racine double est donc (sans surprise) $a \neq 0$ et $b^2 - 4ac = 0$.

   ii. D'après la question précédente, le polynôme $X^3 + aX + b$ admet une racine multiple si et seulement si $\mathrm{Res}(X^3 + aX + b, 3X^2 + a) = 0$, donc si et seulement si : $\begin{vmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 4a^3 + 27b^2 = 0$

4. **Équation de Bézout**

(a) Le résultant de P et Q vaut : $\begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} = 1 \neq 0$. Cela montre que P et Q sont premiers entre eux.

(b) On cherche un élément (A_0, B_0) de E tel que $u(A_0, B_0) = 1$, ce qui donne matriciellement $M_{P,Q}\, Y = Z$ où Y désigne la matrice colonne 7×1 des coordonnées de (A_0, B_0) dans la base $\mathcal{B}$ et Z est la matrice des coordonnées du polynôme constant 1 dans la base $\mathcal{B}'$ de F. Le calcul donne $Y = {}^t(1, -1, -1, 0, 1, 2, 1)$, donc :

$$A_0 = 1 - X - X^2,\ B_0 = X + 2X^2 + X^3.$$

Remarque : pour calculer les coefficients de l'identité de Bezout, l'algorithme le plus souvent utilisé est l'algorithme d'Euclide étendu.

(c) Le sous-espace affine des éléments (A, B) de $\mathbb{C}[X] \times \mathbb{C}[X]$ vérifiant l'équation affine $AP+BQ = 1$ est de la forme $(A_0, B_0)+\ker U$ où U est l'application $(A, B) \mapsto AP+BQ$ de $\mathbb{C}[X]\times\mathbb{C}[X]$ dans $\mathbb{C}[X]$. En reprenant les arguments de la première question avec P et Q premiers entre eux, on trouve que $AP = -BQ$ si et seulement si il existe $R \in \mathbb{C}[X]$ tel que $B = PR$ et $A = -QR$. Ainsi les couples (A, B) vérifiant $AP + BQ = 1$ sont de la forme

$$A = A_0 - QR,\ B = B_0 + PR$$

pour $R \in \mathbb{C}[X]$ quelconque.

II. Applications

5. **Matrices à valeurs propres toutes distinctes**

(a) L'application de $\mathcal{M}_n(\mathbb{C})$ dans l'espace vectoriel normé $\mathbb{C}_{n+1}[X]$ qui associe à une matrice son polynôme caractéristique est continue. L'application de $\mathbb{C}_{n+1}[X]$ dans $\mathbb{C}$ qui associe à un polynôme son discriminant $\mathrm{Res}(P, P')$ est également continue. Une matrice a des valeurs propres deux à deux distinctes si et seulement si son image par la composée de ces deux applications est non nulle. Donc l'espace D_0 est l'image réciproque de l'ouvert $\mathbb{C} \setminus \{0\}$ par une application continue de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$, c'est un ouvert de $\mathcal{M}_n(\mathbb{C})$.

(b) Les matrices de D_0 sont toutes diagonalisables, donc $D_0 \subset D$ et comme D_0 est ouvert, $D_0 \subset \mathring{D}$. Pour montrer l'inclusion $\mathring{D} \subset D_0$, on va montrer que tout élément de $D \setminus D_0$ n'est pas dans $\mathring{D}$. Soit M un matrice diagonalisable ayant deux valeurs propres égales. Il existe donc une matrice inversible P telle que $P^{-1}MP$ est la matrice diagonale $\mathrm{diag}(\lambda, \lambda, \lambda_3, \ldots, \lambda_n)$. Considérons la matrice nilpotente N dont tous les coefficients sont nuls sauf le coefficient de la première ligne et deuxième colonne valant 1. Pour tout entier n, la matrice $P^{-1}MP + \frac{1}{n}N$ n'est pas diagonalisable (elle a les mêmes valeurs propres que M mais son espace propre pour la valeur propre λ est de dimension $d-1$ où d est la dimension de l'espace propre de M pour la valeur propre λ). Donc la suite de matrices $(M + \frac{1}{n}PNP^{-1})_{n\in\mathbb{N}}$ est contenue dans $\mathcal{M}_n(\mathbb{C}) \setminus D$ et converge vers M, ce qui prouve que $M \notin \mathring{D}$ et conclut.

6. **Nombre algébrique**

Les racines de $P(X) = X^2 - 3$ sont $\pm\sqrt{3}$ et pour tout $x \in \mathbb{C}$, celles de $Q_x(X) = (x-X)^2 - 7$ sont $x \pm \sqrt{7}$. Donc P et Q_x ont une racine commune si et seulement si $x \pm \sqrt{7} = \pm\sqrt{3}$ c'est-à-dire $x = \pm\sqrt{3} \pm \sqrt{7}$. Le résultant $\mathrm{Res}(P, Q_x)$ est une fonction polynomiale de x et il s'annule si et seulement si $x = \pm\sqrt{3} \pm \sqrt{7}$. En particulier il a $\sqrt{3} + \sqrt{7}$ pour racine. Ce polynôme vaut :

$$\begin{vmatrix} -3 & 0 & x^2-7 & 0 \\ 0 & -3 & -2x & x^2-7 \\ 1 & 0 & 1 & -2x \\ 0 & 1 & 0 & 1 \end{vmatrix} = x^4 - 20x + 16$$

et ses racines sont $\pm\sqrt{7} \pm \sqrt{3}$.

Remarque : on montre ainsi que la somme de deux nombres algébriques est un nombre algébrique et on peut donner expicitement un polynôme annulateur de la somme.

7. **Courbe algébrique paramétrée**

Soit $(x, y) \in \mathbb{R}^2$. Il exise $t \in \mathbb{R}$ tel que $x = t^2 + t$, $y = t^2 - t + 1$ si et seulement si les deux polynômes $T^2 + T - x$ et $T^2 - T + 1 - y$ ont une racine commune. Ceci montre que $(x, y) \in \mathcal{C}$ si et seulement si le résultant de ces deux polynômes est nul. Ce résultant est un polynôme [précisément une application polynomiale] en x, y. Le calcul donne $P(x, y) = x^2 + y^2 - 2xy - 4y + 3$. On reconnait l'équation d'une conique dont on peut vérifier que c'est bien une parabole (il est clair que $\mathcal{C}$ n'a qu'une composante connexe et part à l'infini).