PROBLÈME : RÉSULTANT DE DEUX POLYNÔMES

I. Définition et propriétés

1. Étude de la bijectivité de u

a) Soit (A, B), (C, D) deux éléments de E et λ, μ deux nombres complexes. Alors, vu que $\mathbb{C}[X]$ est une algèbre,

$$\begin{aligned} u\big(\lambda(A,B)+\mu(C,D)\big) &= u\big((\lambda A+\mu C, \lambda B+\mu D)\big) \\ &= P(\lambda A+\mu C)+Q(\lambda B+\mu D) \\ &= \lambda(PA+QB)+\mu(PC+QD) \\ &= \lambda u(A,B)+\mu u(C,D) \end{aligned}$$

donc $\boxed{u \text{ est linéaire.}}$

b) Si u est bijective, le polynôme constant égal à 1 possède un antécédent pour u *i.e.* il existe $(A, B) \in E \subset \mathbb{C}[X] \times \mathbb{C}[X]$ tel que $1 = PA + QB$.
D'après le théorème de Bézout, on en déduit que $\boxed{P \text{ et } Q \text{ sont premiers entre eux.}}$

c) Supposons P et Q premiers entre eux et soit (A, B) appartenant à $\operatorname{Ker} u$. Alors $AP = -BQ$ donc P divise BQ et comme P et Q sont premiers entre eux, P divise B d'après le théorème de Gauss ; or $\deg B \leqslant p-1 < \deg P$ donc nécessairement $B = 0$. De même, Q divise A et $\deg A < \deg Q$ donc $A = 0$. Le noyau de u est donc réduit au vecteur nul de E, et comme $\dim E = p + q = \dim F$, on en déduit que l'application linéaire $\boxed{u \text{ est bijective.}}$

2. Matrice de u

a) $\boxed{\text{Notons } M \text{ la matrice de } u \text{ par rapport aux bases } \mathcal{B} \text{ et } \mathcal{B}' \text{ et montrons que } M = M_{P,Q}}$ (définie par l'énoncé). Remarquons que ces deux matrices sont carrées d'ordre $p + q$.

Soit $j \in [\![1, q]\!]$, alors $u(X^{j-1}, 0) = X^{j-1}P = \sum\limits_{k=0}^{p} a_k X^{j-1+k}$: donc la colonne numéro j de M est ${}^t(0, \cdots, 0, a_0, a_1, \cdots, a_p, 0, \cdots, 0)$ (colonne commençant par $j-1$ zéros et se terminant par $q-j$ zéros) qui est également la colonne numéro j de $M_{P,Q}$.

De même, si $j \in [\![1, p]\!]$, alors $u(0, X^{j-1}) = X^{j-1}Q = \sum\limits_{k=0}^{q} b_k X^{j-1+k}$: donc la colonne numéro $j+q$ de M est ${}^t(0, \cdots, 0, b_0, b_1, \cdots, b_q, 0, \cdots, 0)$ (colonne commençant par $j-1$ zéros et se terminant par $p-j$ zéros) qui est également la colonne numéro $j+q$ de $M_{P,Q}$.

b) D'après a), $\operatorname{Res}(P, Q) = \det M_{P,Q} = \det u$, donc $\operatorname{Res}(P, Q) \neq 0$ si et seulement si u est bijective ce qui, d'après 1. équivaut au fait que P et Q soient premiers entre eux.

3. Racine multiple

a) Rappelons qu'un nombre complexe a est racine multiple de P si et seulement si $P(a) = P'(a) = 0$. On en déduit que P admet une racine multiple si et seulement si les polynômes P et P' admettent une racine complexe commune c'est-à-dire ne sont pas premiers entre eux ce qui équivaut d'après la question précédente à $\operatorname{Res}(P, P') = 0$.

b) Si $P = X^3 + aX + b$, $P'(X) = 3X^2 + a$ d'où $\text{Res}\,(P, P') = \begin{vmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 27b^2 + 4a^3$

(*on se ramène au calcul du déterminant d'une matrice triangulaire par blocs pour le partage 3-2 en effectuant les opérations élémentaires* $L_2 \leftarrow L_2 - \frac{a}{3}L_4$ *et* $L_3 \leftarrow L_3 - \frac{a}{3}L_5$)

Donc $\boxed{X^3 + aX + b \text{ admet une racine multiple si et seulement si } 4a^3 + 27b^2 = 0.}$

II. Applications

4. Équation de Bézout

a) Pour montrer que P et Q sont premiers entre eux, il suffit d'après 2.b) de vérifier que leur résultant n'est pas nul. Or $\text{Res}\,(P, Q) = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} = 1 \neq 0$

b) Notons u l'application de $\mathbb{C}_2[X] \times \mathbb{C}_3[X]$ qui à (A, B) associe $PA + QB$ et posons $A_0 = a_0 + a_1X + a_2X^2$ et $B_0 = b_0 + b_1X + b_2X^2 + b_3X^3$. Alors,

$$PA_0 + QB_0 = 1 \iff u(A_0, B_0) = 1 \iff \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

En effectuant les opérations élémentaires suivantes : $L_4 \leftarrow L_4 - L_1$, $L_5 \leftarrow L_5 - L_1 - L_2$, $L_6 \leftarrow L_6 - L_2 - L_3$, $L_7 \leftarrow L_7 - L_3$ on obtient le système équivalent suivant :

$$\left\{ \begin{array}{ccccccccccccc} a_0 & & & + & b_0 & & & & & & & = & 1 \\ & a_1 & & - & b_0 & + & b_1 & & & & & = & 0 \\ & & a_2 & & & - & b_1 & + & b_2 & & & = & 0 \\ & & & & & & & - & b_2 & + & b_3 & = & -1 \\ & & & & & & & & & - & b_3 & = & -1 \\ & & & & b_0 & & & & & & & = & 0 \\ & & & & & & b_1 & - & b_2 & + & b_3 & = & 0 \end{array} \right.$$

qui admet pour unique solution : $(a_0, a_1, a_2, b_0, b_1, b_2, b_3) = (1, -1, -1, 0, 1, 2, 1)$ ce qui fournit la solution $\boxed{(A_0, B_0) = (1 - X - X^2, X + 2X^2 + X^3)}$

c) Dans ces conditions, $PA + QB = 1$ équivaut à $PA + QB = PA_0 + QB_0$ ou encore à $P(A - A_0) = Q(B_0 - B)$. Donc, si (A, B) est solution, Q divise $P(A - A_0)$ et vu que P et Q sont premiers entre eux, Q divise $A - A_0$ d'après le théorème de Gauss. Il existe donc $R \in \mathbb{C}[X]$ tel que $A = A_0 + QR$; dans ces conditions $PA + QB = PA_0 + QB_0$ équivaut à $PQR + QB = QB_0$ soit compte-tenu de l'intégrité de $\mathbb{C}[X]$ et du fait que $Q \neq 0$ à $B = B_0 - PR$. Les solutions de $PA + QB = 1$ sont donc les couples de la forme $\boxed{(A_0 + QR, B_0 - PR) \text{ avec } R \in \mathbb{C}[X]}$

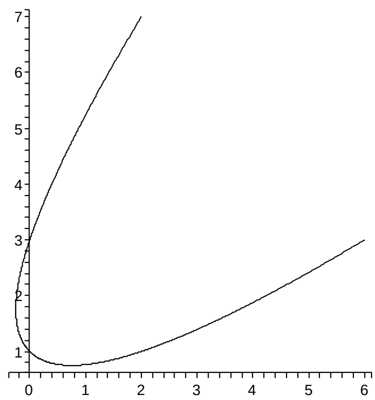
5. **Équation d'une courbe**

a) Si $\left\{\begin{array}{l} x(t)=t^2+t \\ y(t)=t^2-t+1 \end{array}\right.$, x et y sont dérivables et $\left\{\begin{array}{l} x'(t)=2t+1 \\ y'(t)=2t-1 \end{array}\right.$ d'où le tableau de variations :

t	$-\infty$		$-\frac{1}{2}$		$\frac{1}{2}$		$+\infty$
$x'(t)$		$-$	0	$+$	2	$+$	
$x(t)$	$+\infty$	$\searrow$	$-\frac{1}{4}$	$\nearrow$	$\frac{3}{4}$	$\nearrow$	$+\infty$
$y(t)$	$+\infty$	$\searrow$	$\frac{7}{4}$	$\searrow$	$\frac{3}{4}$	$\nearrow$	$+\infty$
$y'(t)$		$-$	-2	$-$	0	$+$	

Tangentes particulières : Γ présente une tangente verticale en $(-\frac{1}{4}, \frac{7}{4})$ et une tangente horizontale en $(\frac{3}{4}, \frac{3}{4})$.

Branches infinies : Lorsque t tend vers $+\infty$ ou vers $-\infty$, $x(t) \sim t^2$ et $y(t) \sim t^2$ donc $x(t)$ et $y(t)$ tendent vers $+\infty$ et $\frac{y(t)}{x(t)}$ tend vers 1. De plus $y(t)-x(t)=-2t-1$ tend vers $-\infty$ quand t tend vers $+\infty$ (resp. tend vers $+\infty$ quand t tend vers $-\infty$). Quand t tend vers $+\infty$ ou vers $-\infty$ l'arc présente donc une branche parabolique de direction asymptotique $y=x$.



b) Si M de coordonnées (x,y) appartient à la courbe de représentation paramétrique $\left\{\begin{array}{l} x(t)=P(t) \\ y(t)=Q(t) \end{array}\right.$, il existe $t \in \mathbb{R}$ tel que $x=P(t)$ et $y=Q(t)$, donc en notant $A(X)=P(X)-x$ et $B(X)=Q(X)-y$, les polynômes A et B ont une racine commune t donc un résultant nul d'après 2.b).

En particulier, si $P(t)=t^2+t$ et $Q(t)=t^2-t+1$,

$$\operatorname{Res}(A,B)=\begin{vmatrix} -x & 0 & 1-y & 0 \\ 1 & -x & -1 & 1-y \\ 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} -x+y-1 & 2y-2 & 1-y & 0 \\ 2 & -x+1+y & -1 & 1-y \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

soit $\operatorname{Res}(A,B)=(-x+y-1)(-x+y+1)-2(2y-2)=x^2+y^2-2xy-4y+3$ donc un point M de coordonnées (x,y) appartenant à Γ vérifie : $x^2+y^2-2xy-4y+3=0$.

c) Si $q(x,y)=x^2+y^2-2xy$, $q(x,y)=\begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}$ avec $A=\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$. Les valeurs propres de A sont $\lambda_1=0$ (car $\operatorname{rg}(A)=1<2$) et $\lambda_2=2$ (car $\operatorname{Tr}(A)=0+\lambda_2=2$) donc la courbe d'équation cartésienne $x^2+y^2-2xy-4y+3=0$ est une parabole ou une droite ou la réunion de deux droites parallèles. Or d'après l'étude faite en a) et b), elle n'est ni une droite, ni une réunion de deux droites parallèles, donc $\boxed{\text{il s'agit d'une parabole.}}$

6. Nombre algébrique

Si $P(X) = X^3 - 3$ et $Q_y(X) = (y - X)^2 - 7$,

$$\operatorname{Res}(P, Q_y) = \begin{vmatrix} -3 & 0 & y^2 - 7 & 0 \\ 0 & -3 & -2y & y^2 - 7 \\ 1 & 0 & 1 & -2y \\ 0 & 1 & 0 & 1 \end{vmatrix} = y^4 - 20y^2 + 16$$

Or P admet pour racines $\sqrt{3}$ et $-\sqrt{3}$ et Q_y admet pour racines $y + \sqrt{7}$ et $y - \sqrt{7}$, donc P et Q_y admettent une racine commune si et seulement si $[\sqrt{3} = y + \sqrt{7}$ ou $-\sqrt{3} = y + \sqrt{7}$ ou $\sqrt{3} = y - \sqrt{7}$ ou $-\sqrt{3} = y - \sqrt{7}]$ *i.e.* si et seulement si $y \in \{\sqrt{3} + \sqrt{7}, \sqrt{3} - \sqrt{7}, -\sqrt{3} + \sqrt{7}, -\sqrt{3} - \sqrt{7}\}$. Comme on sait que les polynômes P et Q_y admettent une racine commune si et seulement si leur résultant est nul, on en déduit que le polynôme $\boxed{R(X) = X^4 - 20X^2 + 16}$ admet pour racines $\sqrt{3} + \sqrt{7}, \sqrt{3} - \sqrt{7}, -\sqrt{3} + \sqrt{7}, -\sqrt{3} - \sqrt{7}$. Il est bien de degré 4 et à coefficients dans $\mathbb{Z}$.