CORRIGÉ : Résultant de 2 polynômes (extrait de CCP MP 2009)

1. a) u est bien à valeurs dans F (considérer les degrés).

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

$$\begin{aligned} u\big(\lambda(A,B)+\mu(C,D)\big) &= u\big((\lambda A+\mu C, \lambda B+\mu D)\big) \\ &= (\lambda A+\mu C)P+(\lambda B+\mu D)Q \\ &= \lambda(AP+BQ)+\mu(CP+DQ) \\ &= \lambda u(A,B)+\mu u(C,D) \end{aligned}$$

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

b) Si u est surjective, le polynôme constant égal à 1 possède un antécédent pour u donc il existe $(A,B)\in E\subset \mathbb{C}[X]\times\mathbb{C}[X]$ tel que $1=AP+BQ$.

Si P et Q avaient une racine commune α, on aurait alors $1=A(\alpha)P(\alpha)+B(\alpha)Q(\alpha)=0$...

Donc $\boxed{P \text{ et } Q \text{ n'ont pas de racine commune.}}$

c) Supposons que P et Q n'ont pas de racine commune et soit (A,B) appartenant à $\operatorname{Ker} u$. Alors $AP=-BQ$ donc P divise BQ.

Si α est une racine de P d'ordre de multiplicité k, alors $(X-\alpha)^k$ divise P donc BQ, donc divise B puisque α n'est pas racine de Q. Cela est vrai pour toutes les racines de P donc, P étant scindé, P divise B. Or $\deg B\leqslant p-1$ donc $\deg B<\deg P$ d'où 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, donc l'application linéaire $\boxed{u \text{ est injective.}}$

d) On a de plus $\dim E=\dim F=p+q$. Il y a donc équivalence entre u surjective et u injective.

Donc $\boxed{P \text{ et } Q \text{ n'ont pas de racine commune} \iff u \text{ bijective .}}$

2. a) Soit $(A,B)\in E$. $A\in\mathbb{C}_{q-1}[X]$ donc il existe des complexes $a_0,\dots,a_{q-1}$ tels que $A=\sum_{k=0}^{q-1}a_kX^k$. On aura donc $(A,0)=\sum_{k=0}^{q-1}a_k(X^k,0)$.

De même, $B\in\mathbb{C}_{p-1}[X]$ donc il existe des complexes $b_0,\dots,b_{p-1}$ tels que $B=\sum_{k'=0}^{p-1}b_{k'}X^{k'}$. On aura donc $(0,B)=\sum_{k'=0}^{p-1}b_{k'}(0,X^{k'})$.

Finalement, $(A,B)=(A,0)+(0,B)=\sum_{k=0}^{q-1}a_k(X^k,0)+\sum_{k'=0}^{p-1}b_{k'}(0,X^{k'})$, donc $\mathscr{B}$ est génératrice de E.

Il est facile de montrer, par des calculs similaires, que cette famille est libre.

$\boxed{\mathscr{B} \text{ est une base de } E.}$

(*Rem : cela est en fait un résultat du cours sur les espaces vectoriels produit...On pouvait aussi utiliser le fait que* $\dim E=\dim\mathbb{C}_{p-1}[X]+\dim\mathbb{C}_{q-1}[X]=p+q=\operatorname{card}\mathscr{B}$ *; cela était bien sûr plus rapide, mais j'ai ici refait la démonstration complète, qui permet justement de démontrer ce résultat sur les dimensions.*)

b) Notons M la matrice de u par rapport aux bases $\mathscr{B}$ et $\mathscr{B}'$ 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 $u(X^{j-1},0)=X^{j-1}P=\sum\limits_{k=0}^{p}a_kX^{j-1+k}$: 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 $u(0,X^{j-1})=X^{j-1}Q=\sum\limits_{k=0}^{q}b_kX^{j-1+k}$: 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 $M_{P,Q}$.

c) D'après a), $\mathrm{Res}(P,Q)=\det M_{P,Q}$, donc $\mathrm{Res}(P,Q)\neq 0$ si et seulement si $M_{P,Q}$ est inversible, i.e si et seulement si u est bijective ce qui, d'après 1. équivaut au fait que P et Q n'ont pas de racine commune.

3. 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 ce qui équivaut d'après la question précédente à $\mathrm{Res}(P,P')=0$.

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

(*on se ramène au calcul du déterminant d'une matrice triangulaire par blocs 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 $\boxed{X^3+aX+b \text{ admet une racine multiple si et seulement si } 4a^3+27b^2=0.}$

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

b) Notons $u_{P,Q}$ l'application de $\mathbb{C}_2[X]\times\mathbb{C}_3[X]$ qui à (A,B) associe $AP+BQ$. $u_{P,Q}$ est bijective d'après ce qui précède, d'où l'existence et l'unicité de (A_0,B_0).

Posons $A_0=a_0+a_1X+a_2X^2$ et $B_0=b_0+b_1X+b_2X^2+b_3X^3$. Alors,

$$A_0P+B_0Q=1 \iff u_{P,Q}(A_0,B_0)=1 \iff \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 1 & 0 & -1 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & -1 & 1 & 0\\ 1 & 0 & 0 & 1 & 0 & -1 & 1\\ 1 & 1 & 0 & 0 & 1 & 0 & -1\\ 0 & 1 & 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix} a_0\\ a_1\\ a_2\\ b_0\\ b_1\\ b_2\\ b_3\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

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, $AP+BQ=1$ équivaut à ou encore à $(A-A_0)P=(B_0-B)Q$. Donc, si (A,B) est solution, Q divise $(A-A_0)Q$ et vu que P et Q n'ont pas de racine commune, on en déduit comme dans la question 1.c., que Q divise $A-A_0$. Il existe donc $R\in\mathbb{C}[X]$ tel que $A=A_0+QR$; dans ces conditions $AP+BQ=A_0P+B_0Q$ équivaut à $PQR+QB=QB_0$ soit compte-tenu de l'intégrité de $\mathbb{C}[X]$ et du fait que $Q\neq 0$ à $B=B_0-PR$.

La réciproque est immédiate : si $A=A_0+QR$ et $B=B_0-PR$, on a $AP+BQ=1$.

Les solutions de $AP+BQ=1$ sont donc les couples de la forme $\boxed{(A_0+QR,B_0-PR) \text{ avec } R\in\mathbb{C}[X]}$