Exercice : Théorème de Mason (1984) et Théorème de Fermat pour les polynômes

1. Soit z une racine de ABC de multiplicité n.
1er cas : supposons que z soit racine de A de multiplicité n. Alors z est racine de A' de multiplicité $n-1$ donc $(X-z)^{n-1}$ divise AB' et $A'B$ donc divise $D = AB' - A'B$, ce qui prouve que z est racine de D de multiplicité $\geqslant n-1$.
Par symétrie, si z est racine de B, le raisonnement est le même.
2ème cas : supposons que z soit racine de C de multiplicité n, alors $A' = C' - B'$ donc $D = (C'-B')B - (C-B)B' = C'B - CB'$ et le même raisonnement peut être tenu.

2. (a) $\mathbb{C}$ étant un corps algébriquement clos, ABC est donc scindé et on peut l'écrire :
$ABC = \lambda \prod_{i=1}^{\mu} (X-z_i)^{\alpha_i}$.
On remarque que $\deg(ABC) = \deg A + \deg B + \deg C = \sum_{i=1}^{\mu} \alpha_i$.
D'après la question précédente, $\prod_{i=1}^{\mu}(X-z_i)^{\alpha_i - 1}$ divise D donc $\deg D \geqslant \sum_{i=1}^{\mu}(\alpha_i - 1) = \deg A + \deg B + \deg C - \mu$.
Par conséquent : $\mu \geqslant \deg(A) + \deg(B) + \deg(C) - \deg(D)$.
(b) Montrons que $\mu > \max\{\deg(A), \deg(B), \deg(C)\}$ par l'absurde.
pfli, supposons que $\deg A = \max\{\deg A, \deg B, \deg C\}$ et $\mu \leqslant \deg A$ alors avec l'inégalité précédente, $\deg D \geqslant \deg B + \deg C$.
Or $D = C'B - B'C$ et $\deg(C'B) = \deg(CB') = \deg C + \deg B - 1$ ce qui implique $\deg D \leqslant \deg C + \deg B - 1$, d'où la contradiction.
Les autres cas se traitent de la même façon.

3. Supposons que l'équation $A^n + B^n = C^n$ ait une solution dans $\mathbb{C}[X]$ avec $n \geqslant 3$.
On remarque que si A et B ont une racine commune z, elle se retrouve chez C, de même si B et C ont une racine commune, comme $A^n = C^n - B^n$, elle se retrouve chez A.
Quitte alors à diviser par $(X-z)$, on peut supposer que A, B et C n'ont aucune racine commune.
Ce qui fait que, derechef A^n, B^n et C^n non plus.
Supposons qu'après ces divisions, l'un des trois polynômes soit de degré strictement positif.
On pourrait donc appliquer le théorème de Mason (question 2.(b)) en notant que, μ, le nombre de racines distinctes de $A^nB^nC^n$ est le même que celui de ABC .
$\mu > \max\{\deg(A^n), \deg(B^n), \deg(C^n)\} = n\max\{\deg(A), \deg(B), \deg(C)\} \geqslant 3\max\{\deg(A), \deg(B), \deg(C)\}$.
Or $\mu \leqslant \deg(ABC) = \deg A + \deg B + \deg C \leqslant 3\max\{\deg(A), \deg(B), \deg(C)\}$, d'où la contradiction.

Par conséquent, lors de la simplification par des termes de la forme $(X-z)$ où z était une racine commune de A, B et C, nous avons abouti à $\tilde{A}^n + \tilde{B}^n = \tilde{C}^n$ avec $\tilde{A}, \tilde{B}, \tilde{C}$ trois polynômes constants.
Par conséquent, cela revient à dire qu'il existe un polynôme P et trois complexes α, β, γ tels que $A = \alpha P, B = \beta P$ et $C = \gamma P$ avec $\alpha^n + \beta^n = \gamma^n$.

Problème

I **1)** Soit g l'endomorphisme de F *induit* par f. Appliquons le théorème du rang à g.
$\dim F = \dim \operatorname{Im} g + \dim \operatorname{Ker} g$.
Or $\operatorname{Im} g = f(F)$ et $\operatorname{Ker} g = F \cap \operatorname{Ker} f$. Par conséquent, $\operatorname{Ker} g \subset \operatorname{Ker} f$ et comme $\operatorname{Ker} f$ est de dimension 1, alors $\operatorname{Ker} g$ est soit égal à $\operatorname{Ker} f$, soit égal à $\{0_E\}$.
Si $\operatorname{Ker} g$ était égal à $\{0_E\}$, alors g serait inversible, mais comme f est nilpotente, g l'est aussi.
On aboutit donc à une contradiction.
Il s'ensuit que $\operatorname{Ker} g = \operatorname{Ker} f$ et est donc de dimension 1.
En conclusion : $\dim f(F) = \dim F - 1$.

2) En appliquant le résultat précédent et en itérant, sachant que $\operatorname{Im} f^k$ est stable par f, on obtient $\dim \operatorname{Im} f^k = n-k$ puis, par théorème du rang, $\dim \operatorname{Ker} f^k = k$

3) On va montrer que les sev stables sont les $\operatorname{Ker} f^k = k$, avec $0 \leqslant k \leqslant n$.
Soit donc F un sev stable de dimension p, et notons comme précédemment, g l'endomorphisme de F *induit* par f.
On a vu dans la question précédente que le noyau de g est de dimension 1 et que g est nilpotente. On sait d'autre

part que l'indice de nilpotence est inférieur ou égal à la dimension de l'espace.
Par conséquent, $g^p = 0$. On a donc, pour tout $x \in F$, $g^p(x) = 0 \Longrightarrow f^p(x) = 0 \Longrightarrow x \in \operatorname{Ker} f^p$.
On a donc $F \subset \operatorname{Ker} f^p$ et égalité des dimensions, par conséquent $F = \operatorname{Ker} f^p$.

II **1)** Immédiat car $\mathcal{L}(E, \mathbb{K})$ est de dimension n.

2) φ est clairement linéaire.
Par égalité des dimensions des espaces de départ et d'arrivée, il suffit de montrer que φ est surjective.
Si ce n'était pas le cas, $\dim \operatorname{Im} \varphi < n$, donc $\operatorname{Im} \varphi$ serait inclus dans un hyperplan H.
Soit $\alpha_1 x_1 + ... + \alpha_n x_n = 0$, l'équation cartésienne de H.
On a donc $\alpha_1 f_1(x) + ... + \alpha_n f_n(x) = 0$ pour tout $x \in E$, ce qui revient à $\alpha_1 f_1 + ... + \alpha_n f_n = 0$, ce qui donnerait une relation de dépendance linéaire non triviale, ce qui contredirait la liberté de la famille $f_1, ..., f_n$.
Conclusion : φ est surjective.

3) On en déduit que φ est injective, i.e. $\operatorname{Ker} f_1 \cap ... \cap \operatorname{Ker} f_n = \{0_E\}$.

4) Soit F un sev de E et H un hyperplan de E.
Par la formule de Grassmann : $\dim(F+H) = \dim F + \dim H - \dim(F \cap H)$. Or $F + H \subset E$, donc $\dim(F+H) \leqslant n$.
On obtient donc $\dim F + n - 1 - \dim(F \cap H) \leqslant n$ d'où $\dim(F \cap H) \geqslant \dim F - 1$.

5) Les noyaux des g_i sont des hyperplans. Par application de l'inégalité précédente et par itération, on obtient que $\dim\Big(\operatorname{Ker} g_1 \cap ... \cap \operatorname{Ker} g_k\Big) \geqslant n - k$.
Par ailleurs, si on complète $(g_1, ..., g_k)$ en une base $(g_1, ..., g_n)$, alors $\dim\Big(\operatorname{Ker} g_1 \cap ... \cap \operatorname{Ker} g_n\Big) = 0$ d'après la question 3.
Pour arriver à 0, et par itération de l'inégalité de la question 4, il faut que toutes les inégalités de la question 4 soient des égalités.
En conclusion, $\dim\Big(\operatorname{Ker} g_1 \cap ... \cap \operatorname{Ker} g_k\Big) = n - k$.

III Matrices magiques :

On notera $\mathcal{MG}$ l'ensemble des matrices magiques.

1) Ces questions étant relativement faciles, on se bornera donc à donner les réponses sans les calculs qui y ont mené.

a) $Vect \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$

b) $Vect \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$

c) Soit A une matrice symétrique magique, alors, si on note $J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, $A - \dfrac{\operatorname{tr}(A)}{3} J$ est une matrice magique symétrique de trace nulle, donc appartient à la droite vectorielle donnée à la question précédente.
On en déduit que l'ensemble des matrices magique symétrique est $Vect \left\{ \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right\}$

d) Montrons que l'espace vectoriel des matrices magiques est la somme directe des matrices magiques symétriques et des matrices magiques antisymétriques.
Si A est une matrice magique, alors il en va de même de A^T. Comme l'ensemble des matrices magiques est un sev, on en déduit que $\dfrac{A + A^T}{2}$ et $\dfrac{A - A^T}{2}$ sont respectivement magique symétrique et magique antisymétrique.
D'où le résultat car il est clair que l'intersection de ces deux sev est la matrice nulle.
Par conséquent, la dimension de l'e.v. des matrices magiques pour $n = 3$ est 3.

2) **Cas général :**

a) $f_1 + ... + f_n = g_1 + ... + g_n = \sum\limits_{1 \leqslant i,j \leqslant n} a_{ij}$.
D'où une RDLNT, et la ligature de la famille de ces $2n$ formes linéaires.

b) Soient $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_{n-1}$ des réels tels que $\lambda_1 f_1 + ... + \lambda_n f_n + \mu_1 g_1 + ... \mu_{n-1} g_{n-1} = 0$. Alors si on évalue cette relation en $E_{i,n}$, on obtient $\lambda_i = 0$, pour tout $i \in [\![1, n]\!]$.
Puis, en évaluant en $E_{1,i}$ pour tout $1 \leqslant i \leqslant n - 1$, on obtient $\mu_i = 0$. D'où la liberté de cette famille.

c) D'après II.5., on trouve $n^2 - (2n - 1) = (n - 1)^2$.

d) Soit A une matrice semi-magique et soit $\alpha = f_1(A) = ... = g_n(A)$. Notons J la matrice dont tout les coefficients valent 1.

Alors $B = A - \alpha J$ est semi-magique et vérifie $f_1(B) = ... = g_n(B) = 0$.
On en déduit que si on note SMG_n l'e.v. des matrices semi-magiques et SMG'_n l'e.v. des matrices semi-magiques dont la somme des coefficients sur chaque ligne et chaque colonne est nulle, alors $SMG_n = SMG'_n \oplus Vect(J)$. Par conséquent la dimension de l'e.v. des matrices semi-magiques vaut $n^2 - 2n + 2$.

3) Reprenons le raisonnement de la question précédente.

Notons MG_0 l'ensemble des matrices magiques dont la somme des coefficients des lignes, des colonnes et des diagonales vaut 0.
Supposons $n \geqslant 4$ et montrons que $(f_1, \dots, f_n, g_1, \dots, g_{n-1}, Tr, Atr)$ est une famille libre.
Soient donc $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_{n-1}, \alpha, \beta$ des réels tels que $\lambda_1 f_1 + ... + \lambda_n f_n + \mu_1 g_1 + ... \mu_{n-1} g_{n-1} + \alpha Tr + \beta Atr = 0$.
On évalue cette relation en $E_{i,n}$, on obtient $\lambda_i = 0$, pour tout $2 \leqslant i \leqslant n-1$, ainsi que $\lambda_1 + \beta = 0$ et $\lambda_n + \alpha = 0$.
On évalue ensuite en $E_{2,i}$: on obtient : $\mu_1 = \mu_3 = ... = \mu_{n-2} = \mu_n = 0$ ainsi que $\mu_2 + \alpha = 0$ et $\mu_{n-1} + \beta = 0$.
On évalue ensuite en $E_{3,i}$: on obtient : $\mu_1 = \mu_2 = \mu_4 = ... = \mu_{n-3} = \mu_{n-1} = \mu_n = 0$ ainsi que $\mu_3 + \alpha = 0$ et $\mu_{n-2} + \beta = 0$.
Ces deux dernières lignes entraînent que $\alpha = \beta = 0$ et donc la nullité des derniers coefficients.
Par conséquent : cette famille est bien libre.

On peut conclure comme dans la question précédente : on obtient $\dim MG_0 = n^2 - (2n+1)$, puis $\dim MG = n^2 - 2n$. On remarque que cette formule est vérifiée pour $n = 3$.