Calculatrices interdites. L'exercice et le problème sont indépendants.

Exercice

Soit $N \in \mathbb{N}$.
On considère une suite (X_n) de variables aléatoires indépendantes définies sur un espace probabilisé $(\Omega, \mathscr{A}, \mathbf{P})$ suivant toutes la loi uniforme sur $\{0, 1, \ldots, N\}$. On pose alors pour tout entier p non nul, $Y_p = X_1 + \cdots + X_p$.

1) Déterminer la loi de Y_2.

2) a) Soit $q \in \mathbb{N}$, montrer que pour tout $k \in \mathbb{N}$,

$$\sum_{i=0}^{k} \binom{i+q}{q} = \binom{k+q+1}{q+1}.$$

b) En déduire que pour tout $p \in \mathbb{N}^*$ et tout $k \leqslant N$,

$$\mathbf{P}(Y_p = k) = \frac{1}{(N+1)^p} \binom{k+p-1}{p-1}$$

On pourra procéder par récurrence.

On note T le numéro p du tirage tel que pour la première fois la somme Y_p soit strictement supérieure à N :

$$\begin{array}{rccc} T: & \Omega & \to & \mathbb{N}^* \cup \{+\infty\} \\ & \omega & \mapsto & \min\{p \in \mathbb{N}^* \ , \ Y_p(\omega) > N\} \end{array}$$

Si pour tout $p \in \mathbb{N}^*$, $Y_p(\omega) \leqslant N$ on pose $T(\omega) = +\infty$.

3) Justifier que T est une variable aléatoire discrète.
On exprimera en particulier $(T = +\infty)$ en fonctions des variables aléatoires $(Y_p)_{p \in \mathbb{N}^*}$.

4) Soit $k \in \mathbb{N}^*$.

a) Calculer $\mathbf{P}(T > k)$.

b) Déterminer un équivalent de $\mathbf{P}(T > k)$ quand $k \to +\infty$.

c) En déduire que l'événement $(T = +\infty)$ est négligeable.

Problème

Notations et définitions

Dans tout le problème, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$ et n un entier naturel non nul.

On note $\mathbb{K}_n[X]$ le sous-espace vectoriel de $\mathbb{K}[X]$ des polynômes de degré inférieur ou égal à n à coefficients dans $\mathbb{K}$ et $\mathscr{M}_n(\mathbb{K})$ la $\mathbb{K}$-algèbre des matrices carrées de taille n à coefficients dans $\mathbb{K}$. La matrice unité est notée I_n et on désigne par $GL_n(\mathbb{K})$ le groupe des matrices inversibles de $\mathscr{M}_n(\mathbb{K})$.

Pour toute matrice A de $\mathscr{M}_n(\mathbb{K})$, on note $A^\top$ la transposée de la matrice A, $\mathrm{rg}(A)$ son rang, $\mathrm{tr}(A)$ sa trace, $\chi_A = \det(XI_n - A)$ son polynôme caractéristique, π_A son polynôme minimal et $\mathrm{sp}(A)$ l'ensemble de ses valeurs propres dans $\mathbb{K}$.

Dans tout le problème, E désigne un espace vectoriel sur le corps $\mathbb{K}$ de dimension finie n, et $\mathscr{L}(E)$ est l'algèbre des endomorphismes de E. On note f un endomorphisme de E.

On note $f^0 = \mathrm{Id}_E$ et $\forall k \in \mathbb{N},\ f^{k+1} = f^k \circ f = f \circ f^k$.

Si $Q \in \mathbb{K}[X]$ avec $Q = a_0 + a_1 X + \cdots + a_m X^m$, $Q(f)$ désigne l'endomorphisme $a_0 \mathrm{Id}_E + a_1 f + \cdots + a_m f^m$. On note $\mathbb{K}[f]$ la sous-algèbre commutative de $\mathscr{L}(E)$ constituée des endomorphismes $Q(f)$ quand Q décrit $\mathbb{K}[X]$.

De même, on utilise les notations suivantes, similaires à celles des matrices, pour un endomorphisme f de E : $\mathrm{rg}(f),\ \mathrm{tr}(f),\ \chi_f,\ \pi_f$ et $\mathrm{sp}(f)$.

Enfin, on dit que f est *cyclique* si et seulement s'il existe un vecteur x_0 dans E tel que $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$ soit une base de E.

Partie I - Matrices compagnes et endomorphismes cycliques

I.A. Généralités

Soit $M \in \mathscr{M}_n(\mathbb{K})$.

1) Montrer que M et $M^\top$ ont même spectre.
2) Montrer que $M^\top$ est diagonalisable si et seulement si M est diagonalisable.

I.B. Matrices compagnes

3) Soit $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{K}^n$ et $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.
On considère la matrice dite compagne de Q

$$C_Q = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & & \vdots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & -a_{n-2} \\ 0 & \dots & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Déterminer en fonction de Q le polynôme caractéristique de C_Q.

4) Soit λ une valeur propre de ${C_Q}^\top$. Déterminer la dimension et une base du sous-espace propre associé.

I.C. Endomorphismes cycliques

5) Montrer que f est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E dans laquelle la matrice de f est de la forme C_Q, où Q est un polynôme unitaire de degré n.

6) Soit f un endomorphisme cyclique. Montrer que f est diagonalisable si et seulement si χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples.

7) Montrer que si f est cyclique, alors $(\mathrm{Id}, f, f^2, \ldots, f^{n-1})$ est une famille libre d'endomorphismes et le polynôme minimal de f est de degré n.

I.D. Application à une démonstration du théorème de Cayley-Hamilton

On ne suppose plus f cyclique.

8) Soit x un vecteur non nul de E. Montrer qu'il existe un entier p strictement positif tel que :

$$\left\{\begin{array}{l}\text{la famille } (x, f(x), f^2(x), \ldots, f^{p-1}(x)) \text{ est libre} \\ \ \text{et} \\ \exists(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \in \mathbb{K}^p \text{ tel que : } \alpha_0 x + \alpha_1 f(x) + \cdots + \alpha_{p-1} f^{p-1}(x) + f^p(x) = 0_E\end{array}\right.$$

9) Justifier que $\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$ est stable par f.

10) Montrer que $X^p + \alpha_{p-1}X^{p-1} + \cdots + \alpha_0$ divise le polynôme χ_f.

11) Retrouver que $\chi_f(f)$ est l'endomorphisme nul.

Partie II - Endomorphismes commutants, décomposition de Frobenius

On appelle commutant de f l'ensemble $\mathscr{C}(f) = \{g \in \mathscr{L}(E)/\ f \circ g = g \circ f\}$.

12) Montrer que $\mathscr{C}(f)$ est une sous-algèbre de $\mathscr{L}(E)$.

II.A. Commutant d'un endomorphisme cyclique

On suppose que f est cyclique et on choisit un vecteur x_0 dans E tel que $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$ est une base de E.
Soit $g \in \mathscr{C}(f)$, un endomorphisme qui commute avec f.

13) Justifier l'existence de $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ de $\mathbb{K}$ tels que

$$g(x_0) = \sum_{k=0}^{n-1} \lambda_k f^k(x_0)$$

14) Montrer alors que $g \in \mathbb{K}[f]$.

15) Établir que $g \in \mathscr{C}(f)$ si et seulement s'il existe un polynôme $R \in \mathbb{K}_{n-1}[X]$ tel que $g = R(f)$.

II.B. Décomposition de Frobenius

Soit $f \in \mathscr{L}(E)$.
On se propose de démontrer le théorème de décomposition de Frobenius : il existe une base $\mathscr{B}$ de E telle que la matrice de f dans la base $\mathscr{B}$ est une matrice diagonale par blocs dont les blocs diagonaux sont des matrices compagnes.
On note d le degré de π_f.

16) Soit $x \in E$. On note $I_{f,x} = \{P \in \mathbb{K}[X] / \ P(f)(x) = 0_E\}$.

   a) Montrer qu'il existe un unique polynôme unitaire noté $\pi_{f,x} \in \mathbb{K}[X]$ tel que $I_{f,x} = \pi_{f,x}\mathbb{K}[X]$ et que $\pi_{f,x}$ divide π_f.
   b) On note d_x le degré de $\pi_{f,x}$. Montrer que $(x, f(x), \ldots, f^{d_x-1}(x))$ est libre.

17) a) Montrer que si la réunion de deux sous-espaces vectoriels F et G de E est un sous-espace vectoriel, l'un contient l'autre.

   On admet que ce résultat se généralise ainsi : si $F_1, \ldots, F_r$ sont des sous-espaces vectoriels dont la réunion est un sous-espace vectoriel, alors l'un des sous-espaces F_i contient tous les autres.

   b) En déduire qu'il existe un vecteur x_1 de E tel que $d_{x_1} = d$.
   On pourra considérer les sous-espaces vectoriels $\mathrm{Ker}(\pi_{f,x}(f))$.

On considère x_1 un élément de E tel que $d_{x_1} = d$.
On pose $e_1 = x_1$, $e_2 = f(x_1)$, …, $e_d = f^{d-1}(x_1)$ et $E_1 = \mathrm{Vect}(e_1, e_2, \ldots, e_d)$.

18) Montrer que $E_1 = \{P(f)(x_1) / \ P \in \mathbb{K}[X]\}$ et que E_1 est stable par f.

On note ψ_1 l'endomorphisme induit par f sur le sous-espace vectoriel E_1.

19) Justifier que ψ_1 est cyclique. En déduire que si $d = n$ alors f est cyclique.

On complète, si nécessaire, $(e_1, e_2, \ldots, e_d)$ en une base $(e_1, e_2, \ldots, e_n)$ de E. Soit Φ la d-ième forme coordonnée qui à tout vecteur x de E associe sa coordonnée suivant e_d dans la base $(e_1, \ldots, e_n)$. On note $F = \{x \in E / \ \forall i \in \mathbb{N}, \ \Phi(f^i(x)) = 0\}$.

20) Montrer que F est stable par f et que E_1 et F sont en somme directe.

Soit Ψ l'application linéaire de E dans $\mathbb{K}^d$ définie, pour tout $x \in E$, par

$$\Psi(x) = (\Phi(f^i(x)))_{0 \leqslant i \leqslant d-1} = (\Phi(x), \Phi(f(x)), \ldots, \Phi(f^{d-1}(x)))$$

21) Montrer que Ψ induit un isomorphisme entre E_1 et $\mathbb{K}^d$.

22) Montrer que $E = E_1 \oplus F$.

23) En déduire qu'il existe r sous-espaces vectoriels de E, notés $E_1, \ldots, E_r$, tous stables par f, tels que :
   — $E = E_1 \oplus \cdots \oplus E_r$;
   — pour tout $1 \leqslant i \leqslant r$, l'endomorphisme ψ_i induit par f sur le sous-espace vectoriel E_i est cyclique ;
   — si on note P_i le polynôme minimal de ψ_i, alors P_{i+1} divise P_i pour tout entier i tel que $1 \leqslant i \leqslant r-1$.

II.C. Commutant d'un endomorphisme quelconque

24) Montrer que la dimension de $\mathscr{C}(f)$ est supérieure ou égale à n.

25) On suppose que f est un endomorphisme tel que l'algèbre $\mathscr{C}(f)$ est égale à $\mathbb{K}[f]$. Montrer que f est cyclique.

Partie III - Preuve du résultat admis à la question 17

26) Démontrer le résultat admis à la question 17.