DM 1 pour le Vendredi 13 septembre 2024	**PC***

Pensez à laisser une marge sur les copies, au minimum 5 cm.*Dans tout le problème, $n \in \mathbb{N}^*$ est un entier fixé, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et on note respectivement $\mathscr{M}_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{K}$ et $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. La notation I_n désigne la matrice identité de taille n.*

Partie 1 Polynômes appliqués à une matrice

Si P est un élément de $\mathbb{K}[X]$ s'écrivant $P = \sum_{k=0}^{m} a_k X^k$ et $M \in \mathscr{M}_n(\mathbb{K})$, on définit la matrice $P(M)$ par :

$$P(M) = \sum_{k=0}^{m} a_k M^k \quad \textit{autrement dit} \quad P(M) = a_0 \mathrm{I}_n + a_1 M + a_2 M^2 + \cdots + a_m M^m$$

On remarque que $P(M) \in \mathscr{M}_n(\mathbb{K})$.

1. Pour $P = X^2 - X + 1$ et $M = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$, calculer $P(M)$.

2. Démontrer que pour P et Q appartenant à $\mathbb{K}[X]$ et $M \in \mathscr{M}_n(\mathbb{K})$, on a $(P+Q)(M) = P(M) + Q(M)$.

3. Démontrer que pour Q appartenant à $\mathbb{K}[X]$, k appartenant à $\mathbb{N}$ et $M \in \mathscr{M}_n(\mathbb{K})$, on a :

$$(X^k \times Q)(M) = M^k \times Q(M)$$

4. En déduire que pour $P, Q \in \mathbb{K}[X]$ et $M \in \mathscr{M}_n(\mathbb{K})$, on a $(P \times Q)(M) = P(M) \times Q(M)$.
Comme $P \times Q = Q \times P$, on en déduit en particulier que $P(M)$ et $Q(M)$ commutent puisque :

$$P(M)Q(M) = (P \times Q)(M) = (Q \times P)(M) = Q(M)P(M)$$

Partie 2 Polynôme annulateur, premières applications

Pour une matrice $M \in \mathscr{M}_n(\mathbb{K})$ et $P \in \mathbb{K}[X]$, on dit que P est un polynôme annulateur de M lorsque $P(M) = 0$ (matrice nulle de $\mathscr{M}_n(\mathbb{K})$. Le polynôme nul est toujours un polynôme annulateur de M, on s'intéresse donc en général aux polynômes non nuls qui sont annulateurs de M.

5. On considère la matrice $M = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$.
Calculer M^2 puis vérifier que $M^2 \in \mathrm{Vect}(M, \mathrm{I}_2)$ et en déduire un polynôme (non nul) annulateur de M.

6. On considère une matrice $M \in \mathscr{M}_n(\mathbb{K})$ et on note f l'endomorphisme canoniquement associé. On suppose que le polynôme $P = X^2 - X$ est annulateur de M.

(a) Que peut-on dire de f ?
(b) Que peut-on dire des sous-espaces $\mathrm{Im}(f)$ et $\mathrm{Ker}(f)$?
(c) On note $r = \mathrm{rg}(f)$, $(e_1, \dots, e_r)$ une base de $\mathrm{Im}(f)$ et $(e_{r+1}, \dots, e_n)$ une base de $\mathrm{Ker}(f)$. Que peut-on dire de la famille $\mathscr{B} = (e_1, \dots, e_n)$?
(d) Quelle est la matrice de f dans la base $\mathscr{B}$?

7. Sur le même principe. On considère une matrice $M \in \mathscr{M}_n(\mathbb{K})$ et on note f l'endomorphisme canoniquement associé. On suppose que le polynôme $P = X^2 - 1$ est annulateur de M. Que peut-on dire de f ?

Partie 3 Application à un calcul d'inverse de matrice

8. On considère la matrice $M = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & -3 \\ 1 & 1 & 2 \end{pmatrix}$ ainsi que le polynôme $P = X^3 - 2X^2 - X + 2$.

(a) Vérifier que le polynôme P est annulateur de M.

(b) En déduire le résultat du produit matriciel $M(M^2 - 2M - \mathrm{I}_3)$.

(c) En déduire une matrice M' telle que $MM' = \mathrm{I}_3$ (on exprimera M' comme une combinaison linéaire de I_3, M et M^2).

(d) En déduire que M est inversible et expliciter M^{-1}.

9. **Sur le même principe.** On suppose que M est une matrice de $\mathscr{M}_n(\mathbb{K})$ et $P = X^2 - X + 1$ est un polynôme annulateur de M. Démontrer que M est inversible et expliciter M^{-1} comme une combinaison linéaire de I_n et M.

Partie 4 Application à un calcul de puissance de matrice

10. On considère la matrice $M = \begin{pmatrix} 2 & 3 & 3 \\ -3 & -4 & -3 \\ 3 & 3 & 2 \end{pmatrix}$ ainsi que le polynôme $P = (X+1)(X-2)$.

(a) Vérifier que le polynôme P est annulateur de M.

(b) Soit $k \in \mathbb{N}$. Démontrer qu'il existe un polynôme $Q \in \mathbb{K}[X]$ ainsi que des scalaires $a_k, b_k \in \mathbb{K}$ tels que :

$$X^k = P(X)Q(X) + a_k X + b_k$$

(c) En substituant à X les racines de P, obtenir un système de 2 équations et 2 inconnues et le résoudre afin d'expliciter a_k et b_k.

(d) En substituant à X la matrice M, écrire M^k comme une combinaison linéaire de M et I_n.

11. **Sur le même principe.** On suppose que M est une matrice de $\mathscr{M}_n(\mathbb{K})$ et $P = (X-1)(X-3)$ est un polynôme annulateur de M. Pour $k \in \mathbb{N}$, expliciter M^k comme une combinaison linéaire de I_n et M.

Partie 5 Existence d'un polynôme annulateur et notion de polynôme minimal

Dans cette partie, M est un élément de $\mathscr{M}_n(\mathbb{K})$.

12. On considère une matrice $M \in \mathscr{M}_n(\mathbb{K})$. Démontrer que la famille $(\mathrm{I}_n, M, M^2, \dots, M^{n^2})$ est liée. En déduire qu'il existe un polynôme $P \in \mathbb{K}[X]$ qui est non nul et annulateur de M.

13. On considère l'ensemble :

$$A = \left\{\deg(P) \mid P \in \mathbb{K}[X],\ P \neq 0 \text{ et } P(M) = 0\right\}$$

Démontrer que l'ensemble A possède un minimum et que ce minimum est non nul.

On pose alors $m = \min(A)$, il existe donc un polynôme $P_0 \in \mathbb{K}[X]$ tel que $\deg P_0 = m$ et $P_0(M) = 0$. On dit que P_0 est un polynôme annulateur minimal de M. On note que, nécessairement, $P_0 \neq 0$.

14. Démontrer que si P est un polynôme annulateur de M et $\deg P < \deg P_0$, alors $P = 0$.

15. Démontrer que si $P \in \mathbb{K}[X]$ est un multiple de P_0, alors P est un polynôme annulateur de M.

16. On considère ici $P \in \mathbb{K}[X]$ un polynôme annulateur de M. Démontrer qu'il existe $Q, R \in \mathbb{K}[X]$ tels que :

$$P = P_0 Q + R \quad \text{et} \quad \deg R < \deg P_0$$

Établir que R est un polynôme annulateur de M. Que peut-on en déduire concernant P ?

La notion de polynôme annulateur existe également pour les endomorphismes. On considère un $\mathbb{K}$-espace vectoriel E. Pour un endomorphisme $f \in \mathscr{L}(E)$ et un entier $k \in \mathbb{N}$, on note :

$$f^k = \mathrm{id}_E \textit{ si } k = 0 \quad \textit{et} \quad f^k = \underbrace{f \circ f \circ \cdots \circ f}_{k \textit{ fois}} \textit{ sinon}$$

Pour un polynôme $P \in \mathbb{K}[X]$ noté $P = \sum_{k=0}^{m} a_k X^k$ on pose $P(f) = \sum_{k=0}^{m} a_k f^k = a_m f^m + \cdots + a_1 f + a_0 \,\mathrm{id}_E$. Lorsque $P(f) = 0$, on dit que P est un polynôme annulateur de f. Les applications sont les mêmes que pour les matrices déterminer l'inverse de f et ses puissances (à ce stade).

Correction DM 1

Partie 1 Polynômes appliqués à une matrice

1. On trouve $M^2 = \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}$ puis $P(M) = M^2 - M + \mathrm{I}_2 = \begin{pmatrix} 1 & 6 \\ 0 & 7 \end{pmatrix}$.

2. **Remarque : pour cette question, ainsi que la suivante, il faut se ramener à la définition donnée plus haut de polynôme appliqué à une matrice, c'est le seul moyen dont on dispose à ce moment pour appliquer un polynôme à une matrice.**
On note $P, Q \in \mathbb{K}[X]$ sous la forme :

$$P = \sum_{k=0}^{m} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{m} b_k X^k$$

avec $m \in \mathbb{N}$ et $a_0, \ldots, a_m, b_0, \ldots, b_m \in \mathbb{K}$ (ce qui est possible, m n'étant pas nécessairement le degré de P ou de Q). Posons $T = \lambda P + \mu Q$, on a alors par définition :

$$T = \lambda P + \mu Q = \sum_{k=0}^{m} (\lambda a_k + \mu b_k) X^k$$

puis : $(\lambda P + \mu Q)(M) = T(M) = \sum_{k=0}^{m} (\lambda a_k + \mu b_k) M^k = \lambda \sum_{k=0}^{m} a_k M^k + \mu \sum_{k=0}^{m} b_k M^k = \lambda P(M) + \mu Q(M)$.
Remarque : pour cette question et la suivante, il faut se ramener à une expression de la forme $T(M)$ avec des coefficients pour T pour pouvoir appliquer la définition.

3. On conserve la même notation pour le polynôme Q, on a donc $X^k Q = \sum_{j=0}^{m} b_j X^{j+k}$ et :

$$(X^k Q)(M) = \sum_{j=0}^{m} b_j M^{j+k} = M^k \sum_{j=0}^{m} b_j M^j = M^k Q(M)$$

4. **Remarque : il est intéressant de signaler, en répondant à cette question, que l'on utilise les deux questions précédentes.** On note toujours $P = \sum_{k=0}^{m} a_k X^k$. Avec les deux questions précédentes :

$$(P \times Q)(M) = \left(\sum_{k=0}^{m} a_k X^k Q \right)(M) = \sum_{k=0}^{m} a_k (X^k Q)(M) = \sum_{k=0}^{m} a_k M^k Q(M) = P(M)Q(M)$$

Partie 2 Polynôme annulateur, premières applications

5. **Remarque : la rédaction ne doit pas commencer par « si $M \in \mathrm{Vect}(M, \mathrm{I}_2)$ » car si on suppose une propriété, il n'est pas possible de la démontrer (à moins d'utiliser une rédaction compliquée).**
On trouve :

$$M^2 = \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix} \quad \text{et pour } \lambda, \mu \in \mathbb{K}, \quad \lambda M + \mu \mathrm{I}_2 = \begin{pmatrix} \lambda + \mu & 2\lambda \\ 0 & 3\lambda + \mu \end{pmatrix}$$

Il suffit donc de prendre $\lambda = 4$ et $\mu = -3$ pour avoir $M^2 = \lambda M + \mu \mathrm{I}_2$, on a donc $M^2 \in \mathrm{Vect}(M, \mathrm{I}_2)$. On vient de constater que $M^2 = 4M - 3\mathrm{I}_2$ autrement dit :

$$M^2 - 4M + 3\mathrm{I}_2 = 0$$

Le polynôme $P = X^2 - 4X + 3$ est donc annulateur de M (et non nul).

6. **Remarque : si f est un projecteur, c'est toujours le projecteur sur $\mathrm{Im}(f)$ parallèlement à (ou dans la direction de) $\mathrm{Ker}(f)$. Il se trouve que si f est un projecteur, on a aussi $\mathrm{Im}(f) = \mathrm{Ker}(f - \mathrm{id})$ donc f est également le projecteur sur $\mathrm{Ker}(f - \mathrm{id})$ parallèlement à $\mathrm{Ker}(f)$.**
   (a) Comme P est annulateur de M, on a $P(M) = M^2 - M = 0$ et on en déduit que $f^2 = f$. Comme f est un endomorphisme de $\mathbb{K}^n$, on en déduit que f est un projecteur de $\mathbb{K}^n$.
   (b) Comme f est un projecteur, c'est le projecteur sur $\mathrm{Im}(f)$ parallèlement à $\mathrm{Ker}(f)$ et les sous-espaces $\mathrm{Im}(f)$ et $\mathrm{Ker}(f)$ sont supplémentaires, ce que l'on note $\mathrm{Im}(f) \oplus \mathrm{Ker}(f) = \mathbb{K}^n$.
   (c) La famille $(e_1, \dots, e_r)$ est un base de $\mathrm{Im}(f)$, la famille $(e_{r+1}, \dots, e_r)$ est une base de $\mathrm{Ker}(f)$ et ces deux sous-espaces sont supplémentaires. D'après le théorème de concaténation des bases, la famille $\mathscr{B}$ obtenue en réunissant ces deux bases est une base de $\mathbb{K}^n$.
   (d) Considérons $x \in \mathbb{K}^n$. Pour déterminer $f(x)$, on doit décomposer x sous la forme $x = y + z$ avec $y \in \mathrm{Im}(f)$ et $z \in \mathrm{Ker}(f)$ et on a alors $f(x) = y$ (le projeté de $x = y + z$ sur $\mathrm{Im}(f)$ parallèlement à $\mathrm{Ker}(f)$ est y). En particulier, lorsque $x \in \mathrm{Im}(f)$, on a $x = y + z$ avec $y = x$ et $z = 0$ donc $f(x) = y = x$ (on retrouve ici le fait que $\mathrm{Im}(f) = \mathrm{Ker}(f - \mathrm{id})$). Si $x \in \mathrm{Ker}(f)$, on a bien entendu $f(z) = 0$. On a donc :

$$f(e_1) = e_1, \quad f(e_2) = e_2, \dots \quad f(e_r) = e_r \quad \text{et} \quad f(e_{r+1}) = \dots = f(e_n) = 0$$

   Ceci se traduit matriciellement par :

$$\mathrm{Mat}_{\mathscr{B}}(f) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

7. Sur le même principe, comme P est annulateur de M, on a $P(M) = M^2 - \mathrm{I}_n = 0$ donc $M^2 = \mathrm{I}_n$. Comme f est l'endomorphisme de $\mathbb{K}^n$ canoniquement associé à M, on a $f^2 = \mathrm{id}$ c'est à dire $f \circ f = \mathrm{id}$. Comme f est un endomorphisme, l'application f est une symétrie de $\mathbb{K}^n$.

Partie 3 Application à un calcul d'inverse de matrice

8. On trouve $M^2 = \begin{pmatrix} 4 & 3 & 3 \\ -3 & -2 & -3 \\ 3 & 3 & 4 \end{pmatrix}$, $M^3 = \begin{pmatrix} 6 & 7 & 9 \\ -5 & -6 & -9 \\ 7 & 7 & 8 \end{pmatrix}$ puis :

$$M^3 - 2M^2 - M + 2\mathrm{I}_3 = 0$$

donc $P = X^3 - 2X^2 - X + 2$ est annulateur de M. On a alors sans calcul supplémentaire :

$$M(M^2 - 2M - \mathrm{I}_3) = M^3 - 2M^2 - M = -2\mathrm{I}_3$$

Si on pose $M' = \frac{-1}{2}(M^2 - 2M - \mathrm{I}_3)$, on a avec ce qui précède $MM' = \mathrm{I}_3$. La matrice carrée M est ainsi inversible à droite, par conséquent M est inversible et on a :

$$M^{-1} = -\frac{1}{2}(M^2 - 2M - \mathrm{I}_3)$$

9. On a ici $P(M) = 0$ avec $P = X^2 - X + 1$ autrement dit $M^2 - M + \mathrm{I}_n = 0$ ou encore :

$$M(M - \mathrm{I}_n) = -\mathrm{I}_n$$

Posons $M' = \mathrm{I}_n - M$, avec ce qui précède on a $MM' = \mathrm{I}_n$. La matrice M est inversible à droite, par conséquent M est inversible et on a $M^{-1} = M' = \mathrm{I}_n - M$.

Partie 4 Application à un calcul de puissance de matrice

10. Comme $P = (X+1)(X-2)$, on a $P(M) = (M + \mathrm{I}_3)(M - 2\mathrm{I}_3)$ or :

$$M + \mathrm{I}_3 = \begin{pmatrix} 3 & 3 & 3 \\ -3 & -3 & -3 \\ 3 & 3 & 3 \end{pmatrix} \quad \text{et} \quad M - 2\mathrm{I}_3 = \begin{pmatrix} 0 & 3 & 3 \\ -3 & -6 & -3 \\ 3 & 3 & 0 \end{pmatrix}$$

puis en effectuant le produit de ces deux matrices on obtient $P(M) = 0$. Le polynôme $P = (X+1)(X-2)$ est donc annulateur de M. On considère $k \in \mathbb{N}$. Le polynôme P n'est pas le polynôme nul, donc on peut effectuer la division euclidienne de X^k par P. Il existe alors $Q, R \in \mathbb{K}[X]$ tels que :

$$X^k = PQ + R \quad \text{et} \quad \deg(R) < \deg(P)$$

Comme $\deg P = 2$, on a $\deg R \leqslant 1$ donc il existe $a_k, b_k \in \mathbb{K}$ tels que $R = a_k X + b_k$. On a ainsi :

$$X^k = P(X)Q(X) + a_k X + b_k$$

Les racines de P sont -1 et 2. Substituons à X ces valeurs, on obtient les relations :

$$\begin{aligned} (-1)^k &= P(-1)Q(-1) - a_k + b_k \\ 2^k &= P(2)Q(2) + 2a_k + b_k \end{aligned}$$

Comme $P(-1) = P(2) = 0$, on a :

$$\begin{aligned} (-1)^k &= -a_k + b_k \\ 2^k &= 2a_k + b_k \end{aligned}$$

En retranchant ces deux relations, on obtient $3a_k = 2^k - (-1)^k$. Avec la première relation on trouve alors :

$$b_k = (-1)^k + \frac{2^k - (-1)^k}{3} = \frac{2^k + 2(-1)^k}{3}$$

On a donc :

$$X^k = P(X)Q(X) + \frac{2^k - (-1)^k}{3} X + \frac{2^k + 2(-1)^k}{3}$$

Appliquons maintenant avec la matrice M, on obtient :

$$M^k = P(M)Q(M) + \frac{2^k - (-1)^k}{3} M + \frac{2^k + 2(-1)^k}{3} \mathrm{I}_3$$

et comme $P(M) = 0$:

$$M^k = \frac{2^k - (-1)^k}{3} M + \frac{2^k + 2(-1)^k}{3} \mathrm{I}_3$$

On a bien exprimé M^k comme combinaison linéaire de M et I_3.

11. Soit $k \in \mathbb{N}$. On réalise la division euclidienne de X^k par $P = (X-1)(X-3)$ (qui n'est pas le polynôme nul). Il existe ainsi $Q, R \in \mathbb{K}[X]$ tels que $X^k = PQ + R$ et $\deg R < \deg P$. On a ainsi $\deg R \leqslant 1$ donc il existe $a_k, b_k \in \mathbb{K}$ tels que $R = a_k X + b_k$. On a donc :

$$X^k = P(X)Q(X) + a_k X + b_k$$

On substitue les racines de P à X on obtient :

$$1^k = P(1)Q(1) + a_k + b_k \quad \text{et} \quad 3^k = P(3)Q(3) + 3a_k + b_k$$

et ainsi :

$$1 = a_k + b_k \quad \text{et} \quad 3^k = 3a_k + b_k$$

En retranchant ces relations, on obtient $2a_k = 3^k - 1$ puis :

$$b_k = 1 - a_k = 1 - \frac{3^k - 1}{2} = \frac{3 - 3^k}{2}$$

On en déduit alors :

$$M^k = P(M)Q(M) + \frac{3^k - 1}{2}M + \frac{3 - 3^k}{2}\mathrm{I}_n = \frac{3^k - 1}{2}M + \frac{3 - 3^k}{2}\mathrm{I}_n$$

C'est une combinaison linéaire de M et I_n.

Partie 5 Existence d'un polynôme annulateur et notion de polynôme minimal

12. La famille $(\mathrm{I}_n, M, \dots, M^{n^2})$ est de cardinal $n^2 + 1$. C'est une famille d'éléments de $\mathscr{M}_n(\mathbb{K})$ qui est de dimension n^2. Comme $n^2 < n^2 + 1$, cette famille ne peut pas être libre, elle est donc liée. Ceci signifie qu'il existe des scalaires $a_0, \dots, a_{n^2} \in \mathbb{K}$ non tous nuls tels que :

$$a_0\mathrm{I}_n + a_1 M + \cdots + a_{n^2} M^{n^2} = 0$$

Posons $P = a_0 + a_1 X + \cdots + a_{n^2} X^{n^2}$, on a alors $P(M) = 0$ donc P est annulateur de M et $P \neq 0$ (car ses coefficients ne sont pas tous nuls).

13. **Remarque : on va commencer par établir que A possède un minimum. On utilise pour cela le résultat suivant : un ensemble d'entiers non vide et minoré possède un minimum.**
Le degré d'un polynôme non nul est un entier naturel donc $A \subset \mathbb{N}$. D'après la question 6, la matrice M possède au moins un polynôme annulateur non nul, donc $A \neq \emptyset$. On sait que tout ensemble d'entiers naturels non vide admet un minimum, par conséquent A possède un minimum. Considérons un polynôme P constant, on le note $P = a$ avec $a \in \mathbb{K}$. On a alors $P(M) = a\mathrm{I}_n$ donc $P(M) = 0$ est équivalent à $a = 0$. On en déduit que A ne contient aucun polynôme constant. Par conséquent, pour tout $P \in A$, $\deg P \geqslant 1$. Posons $m = \min(A)$, par définition il existe $P \in A$ tel que $m = \deg P$ et d'après ce qu précède, $\deg P \geqslant 1$ donc $m \geqslant 1$ et donc $m \neq 0$.

14. Considérons $P \in \mathbb{K}[X]$ tel que $P(M) = 0$ et supposons $\deg P < \deg P_0$. On a donc $\deg P < m$ et ainsi $P \notin A$. Par définition de A, et sachant que $P(M) = 0$, on a nécessairement $P = 0$.

15. Considérons $P \in \mathbb{K}[X]$ multiple de P. Il existe alors $Q \in \mathbb{K}[X]$ tel que $P = P_0 Q$ et avec $P_0(M) = 0$ et les résultats admis :

$$P(M) = P_0(M)Q(M) = 0$$

donc P est annulateur de M.

16. Le polynôme P_0 n'est pas le polynôme nul donc on peut effectuer la division euclidienne de P par P_0 et on obtient qu'il existe $Q, R \in \mathbb{K}[X]$ tels que $P = P_0 Q + R$ et $\deg R < \deg P_0$. Appliquons ceci avec M, on obtient :

$$P(M) = P_0(M)Q(M) + R(M) = R(M)$$

On en déduit que R est annulateur de M. Comme $\deg R < \deg P_0 = m = \min A$, R est nécessairement le polynôme nul (question précédente). On a donc $P = P_0 Q$ et P est multiple de P_0. Avec la question précédente, on a démontré le résultat suivant : les polynômes annulateurs de M sont exactement les multiples de P_0.