DM13
Pour le mercredi 12/03

(avec corrigé)

Problème 1. Polynôme annulateur d'une matrice

Soit $M \in \mathscr{M}_n(\mathbb{C})$ une matrice à coefficients complexes. Si $P(X) = \sum_{k=0}^{d} a_k X^k$, on définit l'évaluation de P en M par

$$P(M) = \sum_{k=0}^{d} a_k M^k, \text{ avec la convention } M^0 = \mathrm{I}_n.$$

Ainsi, si $P(X) = 2X^2 + 3X - 4$, et $A \in \mathscr{M}_n(\mathbb{C})$, $P(A) = 2A^2 + 3A - 4\mathrm{I}_n$.
Un polynôme P est appelé polynôme annulateur de M si $P(M) = 0$ (matrice nulle).
On peut remarquer que si $M \in \mathscr{M}_n(\mathbb{C})$, si P et Q sont deux polynômes, alors

$$(P+Q)(M) = P(M) + Q(M) \texttt{ et } (PQ)(M) = P(M) \times Q(M).$$

On rappelle donc que si P est un polynôme et M est une matrice, $P(M)$ est **une matrice**.

Partie I. Propriétés générales

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

1. Montrer que si P est un polynôme annulateur de M, alors pour tout polynÔme Q, $Q \times P$ est un polynôme annulateur de M.

On suppose que P est un polynôme annulateur de M. Soit alors Q dans $\mathbb{C}[X]$. Alors $(QP)(M) = Q(M) \times P(M)$. Mais $P(M) = 0$, donc $(QP)(M) = Q(M) \times 0 = 0$.

---

2. Démontrer que si M admet un polynôme annulateur P vérifiant $P(0) \neq 0$, alors M est inversible.

C'est que si le terme constant de P étant non nul, on peut écrire I_n comme le produit de M par une matrice qui commute à M.

---

3. Démontrer que si M admet un polynôme annulateur de la forme X^k, où $k \in \mathbb{N}$, alors M n'est pas inversible.

L'ensemble des matrices inversibles est stable par multiplication. Donc si M est inversible alors M^k est inversible pour tout $k \in \mathbb{N}$, donc non nul. L'implication contraposée fait conclure.

Partie II. Un exemple

On pose ici $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$.

4. Montrer que $P(X) = X^2 + X - 2$ est un polynôme annulateur de A.

Calculons $P(A)$:

$$\begin{aligned} P(A) &= A^2 + A - \mathrm{I}_3 \\ &= \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = 0_3, \end{aligned}$$

donc P est bien un polynôme annulateur de A.

5. En déduire que A est inversible et donner l'expression des coefficients de son inverse.

On sait que $A^2 + A - 2\mathrm{I}_3 = 0$, donc $A(A + \mathrm{I}_3) = 2\mathrm{I}_3$, donc $AB = \mathrm{I}_3$ où $B = \frac{1}{2}(A + \mathrm{I}_3)$, donc A est inversible d'inverse $B = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

6. Déterminer, pour n dans $\mathbb{N}$, le reste de la division euclidienne de X^n par P (on ne demande pas le quotient).

Soit n dans $\mathbb{N}$. On sait que le reste de la division de X^n par P est de degré 1, il est donc de la forme $aX + b$. On a donc

$$X^n = Q(X)(X^2 + X - 2) + aX + b.$$

Or, $X^2 + X - 2 = (X - 1)(X + 2)$. En évaluant l'égalité précédente en 1, on obtient $1 = a + b$. En l'évaluant en -2, on obtient $(-2)^n = -2a + b$. D'où $a = \frac{1}{3}(1 - (-2)^n)$ et $b = \frac{1}{3}(2 + (-2)^n)$. Donc le reste de la division euclidienne de X^n par $X^2 + X - 2$ est $\frac{1}{3}(1 - (-2)^n)X + \frac{1}{3}(2 + (-2)^n)$.

7. En déduire une expression de A^n pour tout entier naturel n.

Soit n dans $\mathbb{N}$. On sait que

$$X^n = Q(X)P(X) + \frac{1}{3}\left(1-(-2)^n\right)X + \frac{1}{3}\left(2+(-2)^n\right),$$

donc

$$A^n = Q(A)P(A) + \frac{1}{3}\left(1-(-2)^n\right)A + \frac{1}{3}\left(2+(-2)^n\right)\mathrm{I}_3,$$

donc, comme $P(A) = 0$,

$$\begin{aligned}
&A^n \\
&= \frac{1}{3}\left(1-(-2)^n\right)A + \frac{1}{3}\left(2+(-2)^n\right)\mathrm{I}_3 \\
&= \frac{1}{3}\begin{pmatrix} (-2)^n-1 & 1-(-2)^n & 1-(-2)^n \\ 1-(-2)^n & (-2)^n-1 & 1-(-2)^n \\ 1-(-2)^n & 1-(-2)^n & (-2)^n-1 \end{pmatrix} - \frac{1}{3}\begin{pmatrix} 2+(-2)^n & 0 & 0 \\ 0 & 2+(-2)^n & 0 \\ 0 & 0 & 2+(-2)^n \end{pmatrix} \\
&= \frac{1}{3}\begin{pmatrix} 1-(-2)^{n+1} & 1-(-2)^n & 1-(-2)^n \\ 1-(-2)^n & 1-(-2)^{n+1} & 1-(-2)^n \\ 1-(-2)^n & 1-(-2)^n & 1-(-2)^{n+1} \end{pmatrix}
\end{aligned}$$

Partie III. Matrice compagnon associée à un polynôme – théorème de Cayley-Hamilton

Si $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$ est un polynôme **unitaire** (avec $(a_0, \dots, a_{n-1})$ des complexes), on définit la matrice compagnon associée à P par

$$C_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

8. Si P est un polynôme unitaire de degré n $\mathbb{C}[X]$, si $\alpha_1, \dots, \alpha_r$ sont les racines de P et $m_1, \dots, m_r$ leurs multiplicités, exprimer $\mathrm{Tr}(C_P)$ en fonction de $\alpha_1, \dots, \alpha_r$ et $m_1, \dots, m_r$.

D'après la définition, $\mathrm{Tr}(C_P) = -a_{d-1}$. Or, d'après les relations coefficients racines, $-a_{d-1}$ est la somme des racines de P, donc $\mathrm{Tr}(C_P) = m_1\alpha_1 + \cdots + m_r\alpha_r$.

---

9. Dans cette question seulement, $P(X) = X^3 - X^2 + X - 2$.

(i) Donner l'expression de $A = C_P$.

La matrice compagnon de P est $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$.

(ii) Calculer A^2, A^3 et vérifier que $P(A) = 0$.

On calcule alors

$$A^2 = \begin{pmatrix} 0 & 2 & 2 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 2 & 2 & 0 \\ -1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix},$$

d'où

$$A^3 - A^2 + A - 2 = \begin{pmatrix} 2 & 2 & 0 \\ -1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 2 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 0$$

Le but de la suite de la partie est de généraliser ce résultat, qui est un cas particulier du **théorème de Cayley-Hamilton** : pour tout polynôme P unitaire, $P(C_P) = 0$.

Soit P un polynôme unitaire, $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$. On pose $A = C_P$.

On définit pour k dans $[\![1, n]\!]$ le vecteur colonne à n lignes e_k comme $e_k = (\delta_{ik})_{1 \leqslant i \leqslant n}$. Ainsi,

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Dans cette partie, on ne demande pas nécessairement un passage par l'écriture formelle des coefficients d'un produit : un calcul matriciel direct, s'il est mené explicitement et clairement, peut être bien plus parlant.

10. Donner la valeur de Ae_1, puis de $A^k e_1$ pour tout k dans $[\![0, n]\!]$.

On fait le calcul directement avec les matrices $n \times n$

$$Ae_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_2.$$

On remarque que de même, $A^2 e_1 = Ae_2 = e_3$ et que pour tout k dans $[\![0, n-1]\!]$, $A^k e_1 = e_{k+1}$.

Ensuite,

$$A^n e_1 = Ae_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -a_0 \\ -a_1 \\ -a_2 \\ \vdots \\ -a_{n-1} \end{pmatrix}$$

---

11. Démontrer que $P(A)e_1 = 0$ (vecteur nul), i.e. que $\left(A^n + \sum_{k=0}^{n-1} a_k A^k\right) e_1 = 0$.

On calcule

$$\begin{aligned}
\left(A^n + \sum_{k=0}^{n-1} a_k A^k\right) e_1 &= A^n e_1 + \sum_{k=0}^{n-1} a_k A^k e_1 \\
&= \begin{pmatrix} -a_0 \\ -a_1 \\ -a_2 \\ \vdots \\ -a_{n-1} \end{pmatrix} + a_0 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_{n-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} -a_0 \\ -a_1 \\ -a_2 \\ \vdots \\ -a_{n-1} \end{pmatrix} + \begin{pmatrix} a_0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}
\end{aligned}$$

---

12. En déduire que pour tout j dans $[\![1, n]\!]$, $P(A)e_j = 0$.

Si $j \in [\![1, n]\!]$, $e_j = A^j \times e_1$. Donc

$$\begin{aligned}
P(A)e_j &= \left(A^n + \sum_{k=0}^{n-1} a_k A^k\right) e_j \\
&= \left(A^n + \sum_{k=0}^{n-1} a_k A^k\right) A^j e_1 \\
&= \left(A^{n+j} + \sum_{k=0}^{n-1} a_k A^{k+j}\right) e_1 \\
&= A^j \left(A^n + \sum_{k=0}^{n-1} a_k A^k\right) e_1 = A^j P(A) e_1 = 0.
\end{aligned}$$

D'où le résultat ! (c'était infiniment plus simple que de refaire tous les calculs !)

---

13. Conclure que $P(A) \times \mathrm{I}_n = 0$ puis que $P(A) = 0$.

On remarque que la matrice I_n est la matrice $(e_1\ e_2\ \cdots\ e_n)$ (avec les vecteurs e_k accollés), donc $P(A)\mathrm{I}_n = (P(A)e_1\ P(A)e_2\ \cdots\ P(A)e_n) = (0\ 0\ \cdots\ 0)$. Donc $A\mathrm{I}_n = 0$, donc, comme I_n est inversible, $A = 0$.

Partie IV. Idéal annulateur d'une matrice

Soit A dans $\mathscr{M}_n(\mathbb{C})$, on note $\mathrm{Ann}(A)$ l'ensemble des polynômes annulateurs de A :

$$\mathrm{Ann}(A) = \{P \in \mathbb{C}[X],\ P(A) = 0\}.$$

On donne ensuite la définition d'un **idéal** de $\mathbb{C}[X]$. Une partie $\mathscr{I}$ de $\mathbb{C}[X]$ est un idéal de $\mathbb{C}[X]$ si :

- $\mathscr{I}$ est un sous-groupe de $(\mathbb{C}[X], +)$.
- pour tout P dans $\mathscr{I}$ et Q dans $\mathbb{C}[X]$, $Q \times P \in \mathscr{I}$.

14. Montrer que $\mathrm{Ann}(A)$ est un idéal de $\mathbb{C}[X]$.

Déjà, si $A \in \mathscr{M}_n(\mathbb{C})$, $\mathrm{Ann}(A) \neq \emptyset$ car $0 \in \mathrm{Ann}(A)$. Ensuite, si $(P, Q) \in \mathrm{Ann}(A)^2$, $P(A) = Q(A) = 0$ donc $(P - Q)(A) = 0$, donc $\mathrm{Ann}(A)$ est un sous-groupe de $\mathbb{C}[X]$. Enfin, si $P \in \mathrm{Ann}(A)$ et $Q \in \mathbb{C}[X]$, $PQ \in \mathrm{Ann}(A)$ par la question 1. Donc $\mathrm{Ann}(A)$ est un idéal de $\mathbb{C}[X]$.

Afin de mieux comprendre la stucture des polynômes annulateurs d'une matrice, on va pour terminer ce problème déterminer la structure des idéaux de $\mathbb{C}[X]$. On va montrer le résultat suivant :

Les idéaux de $\mathbb{C}[X]$ sont les $P.\mathbb{C}[X] = \{Q \in \mathbb{C}[X],\ P|Q\}$, où $P \in \mathbb{C}[X]$.

15. Montrer que si $P \in \mathbb{C}[X]$, $P.\mathbb{C}[X]$ est un idéal de $\mathbb{C}[X]$.

Soit $P \in \mathbb{C}[X]$. Alors $P.\mathbb{C}[X] \neq \emptyset$ car $0 = P \times 0 \in P.\mathbb{C}[X]$. Ensuite, si A et B sont dans $P.\mathbb{C}[X]$, on dispose de U et V dans $\mathbb{C}[X]$ tels que $A = PU$ et $B = PV$, donc $A - B = P(U - V) \in P.\mathbb{C}[X]$. Donc $P.\mathbb{C}[X]$ est un sous-groupe de $(\mathbb{C}[X], +)$. Enfin, si $A \in P.\mathbb{C}[X]$ et $B \in \mathbb{C}[X]$, on dispose de $U \in \mathbb{C}[X]$ tel que $A = PU$ donc $AB = PUB \in P.\mathbb{C}[X]$. Donc $P\mathbb{C}[X]$ est bien un idéal de $\mathbb{C}[X]$.

Soit maintenant $\mathscr{I}$ un idéal de $\mathbb{C}[X]$, que l'on va supposer non réduit à 0 (s'il est réduit à 0, $\mathscr{I} = 0.\mathbb{C}[X]$).

16. Montrer que $\mathscr{I}$ admet un polynôme non nul de degré minimal, P_0, et que $\mathscr{I} = P_0.\mathbb{C}[X]$.

Soit $D = \{\deg(P),\ P \in \mathscr{I}\} \cap \mathbb{N}$. Comme $\mathscr{I}$ n'est pas réduit à 0, il contient un polynôme de degré $\geqslant 0$, donc D est une partie non vide de $\mathbb{N}$. D contient donc un plus petit élément d_0. Il existe alors un polynôme P_0 de $\mathscr{I}$ de degré d_0.
Écrivons la division euclidienne de Q par P_0 : $Q = P_0S + R$, avec $\deg(R) < \deg(P_0)$. Comme $\mathscr{I}$ est un idéal et que $P_0 \in \mathscr{I}$, $P_0S \in \mathscr{I}$. Donc, comme $Q \in \mathscr{I}$, $Q - P_0S \in \mathscr{I}$, donc $R \in \mathscr{I}$. Si $R \neq 0$, on aurait $0 \leqslant \deg(R) < \deg(P_0)$, ce qui contredirait la minimalité du degré de P_0. Donc $R = 0$ et P_0 divise Q.

On conclut alors que $\mathscr{I} \subset P_0.\mathbb{C}[X]$. Mais si $P_0 \in \mathscr{I}$, alors pour tout U dans $\mathbb{C}[X]$, $P_0.U \in \mathscr{I}$. Donc $P_0.\mathbb{C}[X] \subset \mathscr{I}$. Par double inclusion, on en déduit que $\mathscr{I} = P_0.\mathbb{C}[X]$.

---

17. Montrer alors que pour toute matrice A, il existe un unique polynôme **unitaire** π_A tel que $\mathrm{Ann}(A) = \pi_A.\mathbb{C}[X]$.

Si A est une matrice, on a vu que $\mathrm{Ann}(A)$ était un idéal de $\mathbb{C}[X]$. Par la question précédente, $\mathrm{Ann}(A)$ est donc de la forme $\pi_A.\mathbb{C}[X]$, avec π_A un polynôme de $\mathbb{C}[X]$.

On appelle ce polynôme le polynôme minimal de A.

18. Si A est une matrice compagnon, montrer que π_A n'est pas le polynôme nul.

Si A est la matrice compagnon d'un polynôme unitaire non nul P, alors $P(A) = 0$ par la partie précédente. Donc $\mathrm{Ann}(A)$ n'est pas réduit à 0, donc π_A ne peut pas être nul ! (sinon $\mathrm{Ann}(A) = 0.\mathbb{C}[X] = \{0\}$.

---

19. Si A est une matrice niplotente, montrer qu'il existe k dans $\mathbb{N}$ tel que $\pi_A(X) = X^k$.

Si A est nilpotente, on dispose de k dans $\mathbb{N}$ tel que $A^k = 0$. Donc X^k est un polynôme annulateur de A. Il doit nécessairement être divisible par π_A, donc π_A divise X^k donc π_A est de la forme X^ℓ avec $\ell < k$.
