Devoir maison 11

▸ Problème : autour des matrices symétriques

Dans tout le problème, n désigne un entier naturel supérieur ou égal à 2 fixé.
On rappelle que $\mathcal{S}_n(\mathbf{R})$ désigne l'ensemble des matrices symétriques de $\mathcal{M}_n(\mathbf{R})$. Pour $p \in \mathbf{N}^*$, on note $\mathcal{E}_p$ l'ensemble des matrices symétriques de $\mathcal{M}_n(\mathbf{R})$ dont la puissance p est égale à l'identité, c'est-à-dire

$$\mathcal{E}_p = \{M \in \mathcal{S}_n(\mathbf{R}) \mid M^p = I_n\}.$$

On note également $\mathcal{E} = \bigcup_{p \in \mathbf{N}^*} \mathcal{E}_p = \{M \in \mathcal{S}_n(\mathbf{R}) \mid \exists p \in \mathbf{N}^*,\ M^p = I_n\}$.

Préliminaires

1. Prouver que si $M \in \mathcal{M}_n(\mathbf{R})$ est une matrice symétrique, alors pour tout $k \in \mathbf{N}$, M^k est également une matrice symétrique.
2. Montrer que pour tout $M \in \mathcal{M}_n(\mathbf{R})$, $MM^\top$ est une matrice symétrique.
3. Montrer que pour tout $M \in \mathcal{S}_n(\mathbf{R})$, $\operatorname{tr}(M^2) \geqslant 0$. Quand cette inégalité est-elle une égalité ?

Partie I. Étude d'un cas particulier

Dans cette partie, on note J_n la matrice de $\mathcal{M}_n(\mathbf{R})$ dont tous les coefficients valent 1, et on pose, pour $a, b \in \mathbf{R}$, $M(a,b) = aI_n + bJ_n$.
On note également $\mathcal{M} = \{M(a,b),\ (a,b) \in \mathbf{R}^2\}$.

4. Prouver que l'application $(a,b) \mapsto M(a,b)$ est injective sur $\mathbf{R}^2$.
5. Calculer J_n^2, et en déduire, pour tout $k \in \mathbf{N}$, la valeur de J_n^k.
6. Sans récurrence, prouver que pour tout $(a,b) \in \mathbf{R}^2$ et pour tout $p \in \mathbf{N}^*$, $M(a,b)^p = M\left(a^p, \dfrac{(a+nb)^p - a^p}{n}\right)$.
7. Prouver que pour tout $M \in \mathcal{M} \cap \mathcal{E}$, $M^2 = I_n$.

Partie II. Cas général

Le but de cette partie est de généraliser le résultat de la question 5, et de prouver que pour tout $M \in \mathcal{E}$, $M^2 = I_n$.

8. **Trichons un peu :** un résultat important du programme de seconde année, appelé le théorème spectral permet de prouver facilement le résultat demandé.
   Ce théorème affirme que si $M \in \mathcal{M}_n(\mathbf{R})$ est une matrice symétrique, alors il existe des réels $\lambda_1, \dots, \lambda_n$ et une matrice $P \in GL_n(\mathbf{R})$ tels que $M = P^{-1}\operatorname{Diag}(\lambda_1, \dots, \lambda_n)P$.
   En admettant ce théorème, prouver que pour tout $M \in \mathcal{E}$, $M^2 = I_n$.
   Vous prouverez l'an prochain ce résultat, et expliquerez comment trouver les réels λ_i et la matrice P. Dans la suite du sujet, et même jusqu'à la fin de l'année, toute utilisation de ce théorème est interdite !
9. Soit $M \in \mathcal{E}_4$. Simplifier $\left(M^2 - I_n\right)^2$ et $\left(M^3 - M\right)^2$, puis montrer que $M^2 = I_n$.
10. Soit $p \in \mathbf{N}^*$ impair, et soit $M \in \mathcal{E}_p$. On pose alors $S = \sum_{k=0}^{p-1} M^k$.
    a. Simplifier MS, puis prouver que $S^2 = pS$.
    b. Pour tout $k \in [\![0, p-1]\!]$, on note r_k le reste de la division euclidienne de $2k$ par p. Montrer que l'application $k \mapsto r_k$ réalise une bijection de $[\![0, p-1]\!]$ sur lui-même.
    c. En déduire que $\sum_{0 \leqslant i,j \leqslant p-1} \left(M^j - M^i\right)^2 = 0_n$.

d. À l'aide de la question 3, prouver que $M = I_n$.

11. Prouver enfin que pour toute matrice $M \in \mathscr{E}$, $M^2 = I_n$.

12. **Une application :** déterminer toutes les matrices $M \in \mathscr{M}_n(\mathbf{R})$ telles que $MM^\top M = I_n$.
On pourra se souvenir que $MM^\top$ est toujours une matrice symétrique.

CORRECTION DU DEVOIR MAISON 11

▸ Problème : autour des matrices symétriques

Préliminaires

1. Soit $M \in \mathcal{M}_n(\mathbf{R})$ symétrique. Alors pour tout $k \in \mathbf{N}$, $\left(M^k\right)^\top = (M^\top)^k = M^k$, et donc M^k est symétrique.
2. Soit $M \in \mathcal{M}_n(\mathbf{R})$. Alors $(MM^\top)^\top = (M^\top)^\top M^\top = MM^\top$, donc $MM^\top$ est symétrique.
3. Soit $M = (m_{i,j})_{1\leqslant i,j\leqslant n} \in \mathcal{M}_n(\mathbf{R})$. Alors

$$\operatorname{tr}(M^2) = \sum_{i=1}^{n} [M^2]_{i,i} = \sum_{i=1}^{n}\sum_{j=1}^{n} m_{i,j}m_{j,i}.$$

Mais puisque M, est symétrique, pour tout $(i,j) \in [\![1,n]\!]^2$, $m_{j,i} = m_{i,j}$.

Et donc $\operatorname{tr}\left(M^2\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} m_{i,j}^2 \geqslant 0$.

Et puisqu'une somme de carrés est nulle si et seulement si chacun de ses termes est nul, on a donc l'égalité $\operatorname{tr}(M^2) = 0$ si et seulement si pour tout $(i,j) \in [\![1,n]\!]^2$, $m_{i,j} = 0$, donc si et seulement si $M = 0_n$.

Partie I. Étude d'un cas particulier.

4. Soient $(a,b),(a',b') \in \mathbf{R}^2$ tels que $M(a,b) = M(a',b')$.
Alors par identification des coefficients situés sur la première ligne et deuxième colonne[1], $b = b'$.
Et par identification de n'importe lequel des coefficients diagonaux, on obtient $a+b = a'+b'$, si bien que $a = a'$, et donc $(a,b) = (a',b')$.
Ainsi, l'application $(a,b) \mapsto M(a,b)$ est bien injective.

[1] En fait n'importe quel coefficient hors diagonale aurait fait l'affaire.

5. Il est classique que $J_n^2 = nJ_n$. En effet, pour tout $(i,j) \in [\![1,n]\!]$, on a

$$[J_n^2]_{i,j} = \sum_{k=1}^{n} [J_n]_{i,k}[J_n]_{k,j} = \sum_{k=1}^{n} 1 = n.$$

Et alors $J_n^3 = J_n^2 J_n = nJ_nJ_n = nJ_n^2 = n^2 J_n$, etc, une récurrence facile prouve alors que pour tout $k \in \mathbf{N}$, $J_n^k = n^{k-1}J_n$.

À la main

Il est tout aussi convaincant d'écrire

$$\begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix}\begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix} = \begin{pmatrix} n & \dots & n \\ \vdots & & \vdots \\ n & \dots & n \end{pmatrix}.$$

6. Soit $(a,b) \in \mathbf{R}^2$. Puisque l'identité commute à toute matrice, aI_n et bJ_n commutent. Et donc par la formule du binôme, pour tout $p \in \mathbf{N}^*$,

$$\begin{aligned} M(a,b)^p &= \sum_{k=0}^{p}\binom{p}{k}(bJ_n)^k(aI_n)^{p-k} \\ &= \sum_{k=0}^{p}\binom{p}{k}b^k J_n^k a^{p-k} \\ &= a^p I_n + \sum_{k=1}^{p}\binom{p}{k}b^k a^{p-k}n^{k-1}J_n \\ &= a^p I_n + \frac{1}{n}\left(\sum_{k=1}^{n}(nb)^k a^{p-k}\right)J_n \\ &= a^p I_n + \frac{1}{n}\left((a+nb)^p - a^p\right)J_n = M\left(a^p, \frac{(a+nb)^p - a^p}{n}\right). \end{aligned}$$

Remarque

Le terme correspondant à $k = 0$ doit être mis à part, car la formule $J_n^k = n^{k-1}J_n$ n'est pas valable pour $k = 0$.

7. Soit $M \in \mathcal{M} \cap \mathcal{E}$, et soit $p \in \mathbf{N}^*$ tel que $M^p = I_n$.
Notons a, b les[2] réels tels que $M = M(a,b)$.
On a donc $M\left(a^p, \frac{(a+nb)^p - 1}{n}\right) = I_n = M(1,0)$. Donc par la question 4, $\begin{cases} a^p = 1 \\ (a+nb)^p - a^p = 0 \end{cases}$.

[2] Ils sont unique par la question 4.

Donc en particulier, $a = \pm 1$, si bien que $a^2 = 1$, et $(a+nb)^p = a^p$, si bien que $a + nb = \pm 1$.
Et donc on $M^2 = M(a,b)^2 = M\left(a^2, \dfrac{(a+nb)^2 - a^2}{n}\right) = M\left(1, \dfrac{1-1}{n}\right) = I_n$.

Partie II. Cas général.

8. Soient donc $M \in \mathscr{E}$, $p \in \mathbf{N}^*$ tel que $M \in \mathscr{E}_p$, et soient P inversible et $\lambda_1, \dots, \lambda_n$ des scalaires tels que $M = P^{-1}\text{Diag}(\lambda_1, \dots, \lambda_n)P$.
Notons $D = \text{Diag}(\lambda_1, \dots, \lambda_n)$, de sorte que

$$M^p = (P^{-1}DP)^p = P^{-1}DPP^{-1}DPP^{-1}DP \cdot P^{-1}DP = P^{-1}D^2PP^{-1}DP \cdots P^{-1}DP = P^{-1}D^pP.$$

Et donc $M^p = I_n \Leftrightarrow P^{-1}D^pP = I_n \Leftrightarrow D^p = PP^{-1} = I_n$.
Mais $D^p = \text{Diag}\left(\lambda_1^p, \dots, \lambda_n^p\right)$, si bien que $\lambda_1^p = \cdots = \lambda_n^p = 1$.
Et donc tous les λ_i valent 1 ou -1, si bien que tous les λ_i^2 sont égaux à 1. Et donc $D^2 = I_n$, de sorte que $M^2 = P^{-1}D^2P = P^{-1}P = I_n$.

9. On a $\left(M^2 - I_n\right)^2 = M^4 - 2M^2 + I_n = 2I_n - 2M^2$.
Par ailleurs, $\left(M^3 - M\right)^2 = M^6 - 2M_4 + M^2 = 2M^2 - 2I_n$.

Les matrices $M^2 - I_n$ et $M^3 - M$ sont symétriques, et donc par la question 3, $\text{tr}\left(\left(M^2 - I_n\right)^2\right) \geqslant 0$ et $\text{tr}\left(\left(M^3 - M\right)^2\right) \geqslant 0$.
Mais le calcul précédent prouve que ces traces sont opposées, donc elles sont nécessairement toutes deux égales à 0.
Mais si $\text{tr}\left((M^2 - I_n)^2\right) = 0$, par la question 3, $M^2 - I_n = 0_n \Leftrightarrow M^2 = I_n$.

10.a. On a $MS = M\sum_{k=0}^{p-1} M^k = \sum_{k=1}^{p} M^k$.
Mais $M^p = I_n = M^0$ par hypothèses, donc $MS = \sum_{k=0}^{p-1} M^k = S$.
On en déduit aisément que pour tout $k \in \mathbf{N}$, $M^kS = S$, et donc

$$S^2 = \left(\sum_{k=0}^{p-1} M^k\right) S = \sum_{k=0}^{p-1} M^kS = \sum_{k=0}^{p-1} S = pS.$$

10.b. Commençons par noter que l'application $k \mapsto r_k$ est nécessairement injective sur $[\![0, p-1]\!]$.
Soient donc $k, k' \in [\![0, p-1]\!]$ tels que $r_k = r_{k'}$.
Notons que puisque $2k \in [\![0, 2p-2]\!]$, cela signifie que $2k = r_k$ ou que $2k = p + r_k$, et de même pour k'.
Puisque p est impair, si $2k = p + r_k$, alors on ne peut pas avoir $2k' = r_k$. Et donc $2k' = p + r_k$, si bien que $k = k'$.
Et pour les mêmes raisons, si $2k = r_k$, alors $2k' = r_k$, et donc $k = k'$.
Donc déjà l'application $k \mapsto r_k$ est injective.

Reste à prouver qu'elle est surjective. Soit donc $j \in [\![1, p]\!]$.
► Si j est pair. Alors il existe $j' \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right]$ tel que $j = 2j'$.
Et alors puisque $j = 2j' < p$, $r_{j'} = 2j' = j$, si bien que j' est un antécédent de j.
► Si j est impair, soit $j' \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right]$ tel que $j = 2j'+1$. Alors $p + j = p + 2j' + 1 = 2\left(j' + \dfrac{p+1}{2}\right)$, avec $j' + \dfrac{p+1}{2} \in [\![0, p-1]\!]$, si bien que $j' + \dfrac{p+1}{2}$ est un antécédent de j.

Ainsi, l'application $k \mapsto r_k$ est surjective, et donc réalise une bijection de $[\![0, p-1]\!]$ sur lui-même.

10.c. On a donc

$$\sum_{0 \leqslant i,j \leqslant p-1} \left(M^j - M^i\right)^2 = \sum_{0 \leqslant i,j \leqslant p-1} \left(M^{2j} - 2M^{i+j} + M^{2i}\right) = 2\sum_{0 \leqslant i,j \leqslant p-1} M^{2j} - 2\sum_{0 \leqslant i,j \leqslant p-1} M^{i+j}.$$

Remarque

En fait, on pourrait s'arrêter ici.
En effet, on considère une application qui va d'un ensemble fini dans lui-même, donc dans un ensemble de même cardinal (ici p).
Si elle est injective, alors elle ne prend pas deux fois la même valeur, et doit donc prendre au moins une fois chaque valeur. Autrement dit, si elle est injective, elle est surjective.
Ceci sera prouvé rigoureusement plus tard, mais le raisonnement était suffisamment intuitif pour être acceptable dès maintenant.

Mais $\sum_{0\leqslant i,j\leqslant p-1} M^{i+j} = \left(\sum_{i=0}^{p-1} M^i\right)\left(\sum_{j=0}^{p-1} M^j\right) = S^2 = pS$.

Et par ailleurs, puisqu'avec les notations de la question précédente[3], $M^{2j} = M^{r_j}$, on a

$$\sum_{0\leqslant i,j\leqslant p-1} M^{2j} = \sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-1} M^{r_j}\right) = p\sum_{j=0}^{p-1} M^{r_j}.$$

Puisque $j \mapsto r_j$ réalise une bijection de $[\![0, p-1]\!]$ sur lui-même, $\sum_{j=0}^{p-1} M^{r_j} = \sum_{j=0}^{p-1} M^j = S$.

Et donc $\sum_{0\leqslant i,j\leqslant p-1} \left(M^j - M^i\right)^2 = pS - pS = 0_n$.

[3] Et car $M^p = I_n$.

Détails

Ces deux sommes ont les mêmes termes (pas forcément dans le même ordre), à savoir toutes les M^k, pour $k \in [\![0, p-1]\!]$, chacune apparaissant une seule fois.

10.d. Puisque M est symétrique, les $M^j - M^i$ le sont aussi. Or, par linéarité de la trace,

$$\sum_{0\leqslant i,j\leqslant p-1} \operatorname{tr}\left((M^j - M^i)^2\right) = \operatorname{tr}\left(\sum_{0\leqslant i,j\leqslant n} (M^j - M^i)^2\right) = \operatorname{tr}(0_n) = 0.$$

Et puisqu'il s'agit d'une somme de nombres positifs[4], elle est nulle si et seulement si chacun de ses termes est nul. Autrement dit si et seulement si pour tout $(i, j) \in [\![0, p-1]\!]$, $\operatorname{tr}\left((M^j - M^i)^2\right) = 0 \Leftrightarrow M^i = M^j$.
En particulier, on doit donc avoir[5], $M = I_n$.

[4] C'est la question 3.

[5] Pour $(i, j) = (1, 0)$.

11. Prouvons par récurrence forte sur $p \geqslant 2$ que pour tout $M \in \mathcal{E}_p$, $M^2 = I_n$.
Pour $p = 2$, il n'y a rien à prouver.
Soit $p \geqslant 3$, et supposons que pour tout $k \in [\![2, p-1]\!]$, $M \in \mathcal{E}_k \Rightarrow M^2 = I_n$.
Soit alors $M \in \mathcal{E}_p$. Si p est premier, alors nécessairement p impair, et donc par la question 10, $M = I_n$, donc $M^2 = I_n$.
Soit p possède un facteur premier impair k, et alors si $p = dk$, il vient $I_n = M^p = (M^d)^k$, si bien que $M^d = I_n$, et puisque $d < p$, par hypothèse de récurrence, $M^2 = I_n$.
Soit 2 est le seul facteur premier de p, et alors puisque $p \geqslant 3$, 4 divise p, si bien qu'il existe d tel que $p = 4d$, et donc $I_n = (M^d)^4$.
Par la question 9, $M^{2d} = I_n$, et puisque $2d < p$, on en déduit que $M^2 = I_n$.
Donc la propriété est bien héréditaire, et donc par le principe de récurrence est vraie à tout rang, si bien que pour tout $M \in \mathcal{E} = \bigcup_{p\in\mathbf{N}^*} \mathcal{E}_p$, $M^2 = I_n$.

12. **Une application** : soit donc M une matrice telle que $MM^\top M = I_n$.
En transposant, il vient $M^\top MM^\top = I_n$, et en multipliant ces deux relations, $(MM^\top)^3 = I_n$, avec $MM^\top$ symétrique.
Et alors par la question 10, $MM^\top = I_n$, si bien que dans la relation de départ, il ne reste que $M = I_n$.
Inversement, $M = I_n$ est bien solution au problème posé, et donc l'unique matrice $M \in \mathcal{M}_n(\mathbf{R})$ telle que $MM^\top M = I_n$ est l'identité.