

Equation matricielle

\mathbb{R} désigne l'ensemble des nombres réels.

On considère p un entier naturel supérieur ou égal à 2.

On notera :

$M_2(\mathbb{R})$ l'ensemble des matrices carrées d'ordre 2 à coefficients réels,

$GL_2(\mathbb{R})$ l'ensemble des matrices inversibles de $M_2(\mathbb{R})$,

$D_2(\mathbb{R})$ l'ensemble des matrices diagonales de $M_2(\mathbb{R})$ et

I la matrice identité de $M_2(\mathbb{R})$.

Le but de ce problème est l'étude des ensembles $\mathcal{R}(p) = \{A \in M_2(\mathbb{R}) / A^p = I\}$.

Dans les parties II et III, E désigne un \mathbb{R} -espace vectoriel de dimension 2 muni d'une base $\mathcal{B} = (e_1, e_2)$, et Id_E désigne l'identité de E .

Partie I : Etude générale

1. $\mathcal{R}(p)$ est-il un sous-espace vectoriel de $M_2(\mathbb{R})$?
2. Soit $A \in \mathcal{R}(p)$. Montrer que $A \in GL_2(\mathbb{R})$ et que $A^{-1} \in \mathcal{R}(p)$.
3. Soit $A \in \mathcal{R}(p)$ et $P \in GL_2(\mathbb{R})$. Montrer que $P^{-1}AP \in \mathcal{R}(p)$.
4. Montrer que $\mathcal{R}(p) \cap D_2(\mathbb{R})$ est un ensemble fini dont on déterminera le cardinal.
5. On considère q un entier naturel supérieur ou égal à 2, et on appelle d le plus grand diviseur commun à p et q . Montrer que $\mathcal{R}(p) \cap \mathcal{R}(q) = \mathcal{R}(d)$.

Partie II : Cas $p=2$

1. Soit $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice de $M_2(\mathbb{R})$ et $Q = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
 - 1.a Exprimer la matrice PQ .
 - 1.b En déduire que P est inversible ssi $ad - bc \neq 0$ et exprimer son inverse P^{-1} lorsque tel est le cas.
2. Soit A un élément de $\mathcal{R}(2)$ tel que $A \neq I$ et $A \neq -I$ et soit u l'endomorphisme de E dont la matrice dans la base \mathcal{B} est A .
 - 2.a Démontrer que $\ker(u - \text{Id}_E) \oplus \ker(u + \text{Id}_E) = E$.
 - 2.b En déduire qu'il existe une base de E dans laquelle la matrice de u est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
 - 2.c Montrer qu'il existe quatre réels a, b, c et d tels que $ad - bc \neq 0$ et $A = \frac{1}{ad - bc} \begin{pmatrix} ad + bc & -2ab \\ 2cd & -ad - bc \end{pmatrix}$.

Partie III : Cas $p=3$

Dans toute la suite du problème, M désigne un élément de $\mathcal{R}_2(3)$, et v l'endomorphisme de E dont la matrice dans \mathcal{B} est M . On considère les ensembles $F = \ker(v - \text{Id}_E)$ et $G = \ker(v^2 + v + \text{Id}_E)$ où $v^2 = v \circ v$.

- 1.a Montrer que $F \cap G = \{0\}$.
- 1.b Soit $x \in E$. Montrer que $\frac{1}{3}(x + v(x) + v^2(x)) \in F$ et que $\frac{1}{3}(2x - v(x) - v^2(x)) \in G$.
En déduire que $E = F \oplus G$.
2. Que peut-on dire de M si F est de dimension 2 ?

Années d'utilisation :

3. Le but de cette question est de montrer à l'aide d'un raisonnement par l'absurde que F n'est pas de dimension 1. On suppose donc que F est de dimension 1.
- 3.a Montrer qu'il existe une base $\mathcal{G} = (g_1, g_2)$ de E telle que F soit la droite vectorielle engendrée par g_1 et G soit la droite vectorielle engendrée par g_2 .
- 3.b En considérant le vecteur $v^2(g_2) + v(g_2) + g_2$, obtenir une contradiction.
4. On suppose dans cette question que F est de dimension 0.
- 4.a Montrer que $(e_1, v(e_1))$ est une base de E .
- 4.b En déduire qu'il existe un réel a et un réel non nul b tels que $M = \frac{1}{b} \begin{pmatrix} ab & -1-a-a^2 \\ b^2 & -ab-b \end{pmatrix}$.

Correction

d'après Mines de Sup 1998

Partie I

1. $\mathcal{R}(p)$ n'est pas un sous-espace vectoriel car $O \notin \mathcal{R}(p)$.
2. Si $A \in \mathcal{R}(p)$ alors $A \times A^{p-1} = I$. Par le théorème d'inversibilité, A est inversible et $A^{-1} = A^{p-1}$.
De plus, en multipliant p fois la relation $A^p = I$ par A^{-1} on obtient $I = (A^{-1})^p$ donc $A^{-1} \in \mathcal{R}(p)$.
3. $(P^{-1}AP)^p = (P^{-1}AP) \times (P^{-1}AP) \times \dots \times (P^{-1}AP) = P^{-1}A^pP = P^{-1}P = I$ donc $P^{-1}AP \in \mathcal{R}(p)$.
4. Soit $A \in D_2(\mathbb{R})$, $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ donc $A^p = \begin{pmatrix} a^p & 0 \\ 0 & b^p \end{pmatrix}$.
Par suite $A^p = I \Leftrightarrow a^p = b^p = 1$.
Si p est impair alors $A^p = I \Leftrightarrow a = b = 1$ et par suite $\mathcal{R}(p) \cap D_2(\mathbb{R}) = \{I\}$ de cardinal 1.
Si p est pair alors $A^p = I \Leftrightarrow a = \pm 1, b = \pm 1$ et par suite
 $\mathcal{R}(p) \cap D_2(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ de cardinal 4.
5. Si $A \in \mathcal{R}(d)$ alors $A^d = I$ donc $\forall k \in \mathbb{N}, A^{dk} = I$. Par suite $\mathcal{R}(d) \subset \mathcal{R}(p) \cap \mathcal{R}(q)$.
Si $A \in \mathcal{R}(p) \cap \mathcal{R}(q)$ alors $A^p = A^q = I$. Par l'égalité de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $pu + qv = d$.
On a alors $A^d = (A^p)^u \times (A^q)^v = I$ donc $A \in \mathcal{R}(d)$. Ainsi $\mathcal{R}(p) \cap \mathcal{R}(q) \subset \mathcal{R}(d)$ puis l'égalité.
Notons qu'il est possible d'écrire $A^d = (A^p)^u \times (A^q)^v$ avec $u, v \in \mathbb{Z}$ car A est inversible.

Partie II

- 1.a $PQ = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$.
- 1.b Si $ad-bc = 0$ alors $PQ = O$ donc P ne peut pas être inversible.
Si $ad-bc \neq 0$ alors $P \times \left(\frac{1}{ad-bc} Q \right) = I$ et par le théorème d'inversibilité P est inversible et
$$P^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$
- 2.a Notons que $u^2 = \text{Id}_E$ car $A^2 = I$.
Soit $x \in \ker(u - \text{Id}_E) \cap \ker(u + \text{Id}_E)$. On a $u(x) = x$ et $u(x) = -x$ donc $x = 0$.
Ainsi $\ker(u - \text{Id}_E)$ et $\ker(u + \text{Id}_E)$ sont en somme directe.
Soit $x \in E$. Posons $y = \frac{x + u(x)}{2}$ et $z = \frac{x - u(x)}{2}$.

Années d'utilisation :

On a $x = y + z$, $y \in \ker(u - \text{Id}_E)$ et $z \in \ker(u + \text{Id}_E)$ car $u(u(x)) = u^2(x) = x$.

Par suite $\ker(u - \text{Id}_E)$ et $\ker(u + \text{Id}_E)$ sont supplémentaires dans E .

- 2.b Puisque $A \neq \pm I$, $u \neq \pm I$ et par suite les espaces $\ker(u - \text{Id}_E)$ et $\ker(u + \text{Id}_E)$ ne sont ni l'un ni l'autre égaux à E . Ce sont donc des droites vectorielles. Soit (e'_1) et (e'_2) des bases de celles-ci, $\mathcal{B}' = (e'_1, e'_2)$ est une base E (car $\ker(u - \text{Id}_E) \oplus \ker(u + \text{Id}_E) = E$) dans laquelle la matrice de u est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

- 2.c Notons P la matrice de passage de \mathcal{B} à \mathcal{B}' .

Puisque P est inversible $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc \neq 0$ et $P^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Par changement de base : $A = P \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} P^{-1}$ ce qui donne $A = \frac{1}{ad - bc} \begin{pmatrix} ad + bc & -2ab \\ 2cd & -ad - bc \end{pmatrix}$.

Partie III

- 1.a Soit $x \in F \cap G$. On a $v(x) = x$ et $v^2(x) + v(x) + x = 0$ donc $3x = 0$ puis $x = 0$.

Par suite $F \cap G = \{0\}$.

- 1.b Notons que $v^3 = \text{Id}_E$ car $M^3 = I$.

Notons $y = \frac{1}{3}(x + v(x) + v^2(x))$ et $z = \frac{1}{3}(2x - v(x) - v^2(x))$

$v(y) = \frac{1}{3}(v(x) + v^2(x) + x) = y$ donc $y \in F$.

$v^2(z) + v(z) + z = \frac{1}{3}(2v^2(x) + 2v(x) + 2x - (x + v^2(x) + v(x)) - (v(x) + x + v^2(x))) = 0$ donc $z \in G$.

Puisque de surcroît, $x = y + z$, on a $E = F + G$ et comme $F \cap G = \{0\}$ on conclut $E = F \oplus G$.

2. Si $\dim F = 2$ alors $F = E$ donc $v = \text{Id}_E$ puis $M = I$.

- 3.a Supposons $\dim F = 1$. On a alors $\dim G = 1$. Soit (g_1) base de F et (g_2) base de G . La famille $\mathcal{G} = (g_1, g_2)$ est une base de $E = F \oplus G$ de la forme voulue.

- 3.b $g_2 \in G$ donc $v^2(g_2) + v(g_2) + g_2 = 0$ puis $v^3(g_2) + v^2(g_2) + v(g_2) = v(0) = 0$ donc $v(g_2) \in G$.

Or $\dim G = 1$ donc $\exists \lambda \in \mathbb{R}$ tel que $v(g_2) = \lambda g_2$. Mais alors $v^2(g_2) + v(g_2) + g_2 = 0$ donne

$(\lambda^2 + \lambda + 1)g_2 = 0$ puis $\lambda^2 + \lambda + 1 = 0$. Or cette équation n'a pas de solutions réelles. Absurde.

4. On suppose $\dim F = 0$ donc $G = E$ ce qui signifie $v^2 + v + \text{Id}_E = 0$.

- 4.a Si $(e_1, v(e_1))$ est liée alors on peut écrire $v(e_1) = \lambda e_1$ (car $e_1 \neq 0$).

Mais alors $0 = v^2(e_1) + v(e_1) + e_1 = (\lambda^2 + \lambda + 1)e_1$ d'où $\lambda^2 + \lambda + 1 = 0$. Impossible.

Par suite $(e_1, v(e_1))$ est libre et puisque cette famille est formée de $2 = \dim E$ vecteurs de E , c'est une base de E .

- 4.b Notons a, b les coordonnées de $v(e_1)$ dans la base (e_1, e_2) .

La matrice de passage de (e_1, e_2) à $(e_1, v(e_1))$ est $P = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ avec $b \neq 0$ et $P^{-1} = \frac{1}{b} \begin{pmatrix} b & -a \\ 0 & 1 \end{pmatrix}$.

La matrice de v dans $(e_1, v(e_1))$ est $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ car $v^2(e_1) = -e_1 - v(e_1)$.

La relation de changement de base donne : $M = P \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} P^{-1} = \frac{1}{b} \begin{pmatrix} ab & -1 - a - a^2 \\ b^2 & -ab - b \end{pmatrix}$.