Devoir à la maison n° 18 : corrigé

Problème 1 — Puissances de matrices

Partie I –

1. Posons $E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $E_2 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $E_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$. On a clairement $\mathcal{A} = \text{vect}(E_1, E_2, E_3)$ donc $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R})$. De plus, la famille (E_1, E_2, E_3) est libre donc c'est une base de $\mathcal{A}$. Ainsi $\dim \mathcal{A} = 3$.

2. Comme $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R})$, c'est a fortiori un sous-groupe de $\mathcal{M}_3(\mathbb{R})$. De plus, $I_3 \in \mathcal{A}$ (choisir $a = b = 1$ et $c = 0$). Enfin, pour $a, b, c, a', b', c' \in \mathbb{R}$

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}\begin{pmatrix} a' & 0 & 0 \\ 0 & b' & c' \\ 0 & -c' & b' \end{pmatrix} = \begin{pmatrix} aa' & 0 & 0 \\ 0 & bb'-cc' & bc'+cb' \\ 0 & -bc'-cb' & bb'-cc' \end{pmatrix} = \begin{pmatrix} a' & 0 & 0 \\ 0 & b' & c' \\ 0 & -c' & b' \end{pmatrix}\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}$$

Ceci montre que $\mathcal{A}$ est stable par produit et commutatif.

3. On calcule $M^2 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -2 & 0 \end{pmatrix}$. Tout d'abord, on a bien $I_3, M, M^2 \in \mathcal{A}$. Soit $\lambda, \mu, \nu \in \mathbb{R}$ tels que $\lambda I_3 + \mu M + \nu M^2 = 0$. Ceci équivaut à $\begin{cases} \lambda - 2\mu + 4\nu = 0 \\ \lambda + \mu = 0 \\ -\mu - 2\nu = 0 \end{cases}$. On voit facilement que l'unique solution de ce système est le triplet nul. La famille (I_3, M, M^2) est donc libre. Puisque $\dim \mathcal{A} = 3$, cette famille est une base de $\mathcal{A}$.

4. On obtient $M^3 = 2M - 4I_3$.

Partie II –

1. Comme $\mathcal{A}$ est un anneau, il est stable par produit. On peut donc montrer par récurrence que pour tout $k \in \mathbb{N}$, $M^k \in \mathcal{A}$, d'où l'existence des réels a_k, b_k et c_k.

2. En écrivant $M^{k+1} = MM^k$, on trouve $\begin{cases} a_{k+1} = -2a_k \\ b_{k+1} = b_k - c_k \\ c_{k+1} = b_k + c_k \end{cases}$.

3. On a $z_{k+1} = b_{k+1} + ic_{k+1} = (b_k - c_k) + i(b_k + c_k) = (1+i)z_k$ pour tout $k \in \mathbb{N}$. La suite (z_k) est donc géométrique de raison $1+i$ et de premier terme $z_0 = b_0 + ic_0 = 1$: on a alors $z_k = (1+i)^k$ pour tout $k \in \mathbb{N}$. Enfin $b_k = \text{Re}(z_k) = \text{Re}\left((1+i)^k\right)$ pour tout $k \in \mathbb{N}$.

4. En utilisant la question **??**, on montre que $b_{k+2} = b_{k+1} - c_{k+1} = b_{k+1} - b_k - c_k = 2b_{k+1} - 2b_k$. La suite (b_k) est donc une suite récurrente linéaire d'ordre 2 dont le polynôme caractéristique est $X^2 - 2X + 2$. Les racines de ce polynômes sont donc $1 \pm i$. Il existe donc $\lambda, \mu \in \mathbb{C}$ tels que $b_k = \lambda(1+i)^k + \mu(1-i)^k$ pour tout $k \in \mathbb{N}$. Or $b_0 = b_1 = 1$ donc $\lambda = \mu = \frac{1}{2}$. Ainsi pour tout $k \in \mathbb{N}$, $b_k = \frac{(1+i)^k + \overline{(1+i)^k}}{2} = \text{Re}\left((1+i)^k\right)$.

5. Comme u_0, u_1 et u_2 sont entiers et que u_{n+3} s'exprime comme une combinaison linéaire à coefficients entiers de u_n et u_{n+1}, on prouve par récurrence triple ou par récurrence forte que la suite (u_n) est à valeurs entières.

6. Pour tout $n \in \mathbb{N}$, $\operatorname{tr}(M^{n+3}) = \operatorname{tr}(M^n M^3) = \operatorname{tr}(M^n(2M - 4I_3)) = 2\operatorname{tr}(M^{n+1}) - 4\operatorname{tr}(M^n)$ en utilisant la question **??** et la linéarité de la trace. De plus, $\operatorname{tr}(M^0) = \operatorname{tr}(I_3) = 3$, $\operatorname{tr}(M^1) = 0$ et $\operatorname{tr}(M^2) = 4$: les suites (u_n) et $(\operatorname{tr}(M^n))$ ont les mêmes trois premiers termes et vérifient la même relation de récurrence d'ordre 3, elles sont donc égales.

7. 2 divise bien $u_2 = 2$: on peut donc supposer p impair. Posons $n = \frac{p-1}{2}$.
Puisque (a_k) est géométrique de raison -2 et de premier terme $a_0 = 1$, on a $a_k = (-2)^k$ pour tout $k \in \mathbb{N}$. Ainsi

$$u_p = a_p + 2b_p = (-2)^p + 2\operatorname{Re}((1+i)^p) = -2^p + 2\sum_{k=0}^{p} \binom{p}{k} \operatorname{Re}(i^k)$$

Or pour k impair, $\operatorname{Re}(i^k) = 0$ donc

$$u_p = -2^p + \sum_{k=0}^{n} \binom{p}{2k} (-1)^k = -(2^p - 2) + 2\sum_{k=1}^{n} \binom{p}{2k} (-1)^k$$

D'après le petit théorème de Fermat, p divise $2^p - 2$ et puisque pour $1 \leqslant k \leqslant n$, on a $2 \leqslant 2k \leqslant p-1$, p divise également $\binom{p}{2k}$ d'après le rappel de l'énoncé. Ainsi p divise u_p.