# 1 Exercices

**Exercice 1.1** Soit $E$ un espace vectoriel réel de dimension finie $3n$. Soit $f \in \mathcal{L}(E)$ vérifiant $\text{rg}(f) = 2n$ et $f^3 + f = 0$.
Etablir l'existence d'une base où la matrice de $f$ est $\begin{pmatrix} 0_n & 0_n & 0_n \\ 0_n & 0_n & I_n \\ 0_n & -I_n & 0_n \end{pmatrix}$.

**Exercice 1.2** Soit $G \subset \mathcal{L}(\mathbb{R}^n)$ un groupe pour la composition des applications.

1. Montrer que tous les éléments de $G$ ont même rang $p$.
2. Montrer qu'il existe une base $B$ dans laquelle tout élément de $G$ est représenté par une matrice de la forme $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ avec $A \in GL_p(\mathbb{R})$.
3. Montrer l'équivalence des trois propositions qui suivent :
   (a) $A$ appartient à un groupe $G$ du type précédent.
   (b) $A$ et $A^2$ ont même rang.
   (c) $\mathbb{R}^n$ est somme directe de $\text{Im}\, A$ et $\ker A$.

**Exercice 1.3** Soit $a$ un endomorphisme de $\mathbb{R}^n$ tel que $a^q - I_n = 0$ (avec $q \in \mathbb{N}^\times$).
Montrer que $\dim(\ker(a - I_n)) = \dfrac{1}{q} \sum_{i=1}^{q} \text{tr}(a^i)$.

**Exercice 1.4** Soit $A \in \mathfrak{M}_3(\mathbb{R})$ telle que $A^3 + A^2 + A = 0$. Montrer que $A$ est semblable à $\begin{pmatrix} 0 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$

# 2 Indications

**Indication pour l'exercice 1.1 :** Utiliser le théorème du noyau. Ensuite, à partir d'un vecteur non nul $e_1$ de $\ker(f^2+I)$, vérifier que $(e_1, f(e_1))$ est stable par $f$ et qu'il s'agit d'une famille libre. Ensuite considérer $e_3 \notin \text{Vect}(e_1, f(e_1))$ et montrer que $(e_3, f(e_3))$ est stable par $f$ et libre. Procéder par itération

**Indication pour l'exercice 1.2 :**

1. Utiliser les propriétés naturels de l'élément neutre $E$ pour la loi et utiliser que $\text{rg}(u \circ v) \leqslant \max(\text{rg}(u), \text{rg}(v))$ pour voir que tous les éléments ont le rang de $E$.

2. Montrer que $E$ est un projecteur qui commute avec tous les éléments de $G$ (dont les espaces stables de $E$ sont stables par $g$)

3. $a) \Rightarrow b)$ se fait par calcul matriciel par bloc
   $b) \Rightarrow c)$ comparer $\text{Im}\, A$ et $\text{Im}\, A^2$ ainsi que $\ker A$ et $\ker A^2$ puis utiliser le théorème du rang
   $c) \Rightarrow a)$ écrire la matrice de l'endomorphisme $u$ attaché à $A$ dans une base adaptée à $\text{Im}\, A$ et $\ker A$

**Indication pour l'exercice 1.3 :** Introduire la matrice $A$ de $a$ dans une base fixée et diagonaliser $A$ sur $\mathbb{C}$ *(pour ceux qui n'ont pas commencer la réduction des endomorphismes, introduire $u$ un endomorphisme de $\mathbb{C}^n$ dont la matrice dans la base canonique est $A$ puis utiliser le théorème des noyaux, choisir une base de chaque espace* $\ker(A-\zeta I)$*, regrouper les bases, écrire la matrice de $v$ dans cette dernière base et utiliser le fait que la trace ne dépend pas de la base).*
En déduire la valeur de $\text{tr}(A^i)$, utiliser ensuite Fubini et se rappeler que $\sum_{k=0}^{n} q^k = \cdots$ (attention à ne pas diviser par 0)

**Indication pour l'exercice 1.4 :** Justifier que $A$ a nécessairement des valeurs propres réelles puis les rechercher. Ensuite, à l'aide du théorème des noyaux, montrer que si $A \neq 0$ alors $\text{rg}\, A \geqslant 2$ (montrer que $x$ et $Ax$ sont libres pour un $x$ bien choisi). Choisir $e_1$ dans $\ker A$ puis, à partir de $x$ et $Ax$, construire les vecteurs $e_2, e_3$ tels que l'endomorphisme associé à $A$ ait la matrice recherchée dans la base $(e_1, e_2, e_3)$ (on vérifiera que la connaissance de $e_2$ entraine la connaissance de $e_3$)

# 3 Corrections

**Correction de l'exercice 1.1 :** L'endomorphisme $f$ admet $P(X) = X^3 + X = X(X^2+1)$ comme polynôme annulateur. Les polynômes $X$ et $X^2+1$ étant premier entre eux dans $\mathbb{R}[X]$, le théorème des noyaux montre que

$$\mathbb{R}^{3n} = \ker(f) \oplus \ker(f^2 + \mathrm{Id})$$

Puisque l'on sait que $\mathrm{rg}(f) = 2n$, le théorème du rang montre que $\dim\ker(f) = 3n - 2n = n$. Ensuite, en passant à la dimension dans la somme directe précédente, on obtient que $\dim\ker(f^2+\mathrm{Id}) = 2n$.

Analyse : Soit $\mathcal{B} = (e_1, ..., e_n, g_1, .., g_n, h_1, ..., h_n)$ une base de $\mathbb{R}^{3n}$. Alors on a :

$$\begin{aligned} mat(f,\mathcal{B}) &= \begin{pmatrix} 0_n & 0_n & 0_n \\ 0_n & 0_n & I_n \\ 0_n & -I_n & 0_n \end{pmatrix} \Leftrightarrow \forall i \in [\![1,n]\!], \quad \begin{cases} f(e_i) = 0 \\ f(g_i) = -h_i \\ f(h_i) = g_i \end{cases} \Leftrightarrow \begin{cases} e_i \in \ker f \\ h_i = -f(g_i) \\ f(-f(g_i)) = g_i \end{cases} \Leftrightarrow \begin{cases} e_i \in \ker f \\ h_i = -f(g_i) \\ -f^2(g_i)) = g_i \end{cases} \\ &\Leftrightarrow \begin{cases} e_i \in \ker f \\ h_i = -f(g_i) \\ g_i + f^2(g_i) = 0 \end{cases} \Leftrightarrow \begin{cases} e_i \in \ker f \\ h_i = -f(g_i) \\ g_i \in \ker(f^2+\mathrm{Id}) \end{cases} \end{aligned}$$

Par conséquent, pour construire la base $\mathcal{B}$, il faut et il suffit de choisir $n$ vecteurs libres $(e_i)_{i\in[\![1,n]\!]}$ dans $\ker f$, $n$ vecteurs libres $(g_i)_{i\in[\![1,n]\!]}$ dans $\ker(f^2+\mathrm{Id})$ puis de s'assurer que la famille $(e_1, .., e_n, g_1, .., g_n, -f(g_1), .., -f(g_n))$ soit libre.
L'espace $\ker(f)$ étant de dimension $n$, il admet une base $(e_1, ..e_n)$
Ensuite, si $g_i \in \ker(f^2+\mathrm{Id})$ alors $-f(g_i) \in \ker(f^2+\mathrm{Id})$ *(Cela résulte soit du cours d'algèbre linéaire qui affirme que* $\ker P(f)$ *est stable par* $f$*, soit d'un calcul direct*

$$h_i + f^2(h_i) = -f(g_i) + f^2(-f(g_i)) = -(f(g_i) + f^3(g_i)) = -f(g_i + f^2(g_i)) = -f(0) = 0$$

On en déduit que si l'on construit les $n$ vecteurs $(g_i)_{i\in[\![1,n]\!]}$, la famille $(g_1, .., g_n, -f(g_1), .., -f(g_n))$ appartient à $\ker(f^2+\mathrm{Id})$.
En outre, puisque l'on dispose de la somme directe

$$\mathbb{R}^{3n} = \ker(f) \oplus \ker(f^2 + \mathrm{Id})$$

et que la famille $(e_1, ..., e_n)$ est une base de $\ker(f)$, le fait que la famille $(e_1, .., e_n, g_1, .., g_n, -f(g_1), .., -f(g_n))$ soit une base de $\mathbb{R}^{3n}$ est équivalent au fait que la famille $(g_1, .., g_n, -f(g_1), .., -f(g_n))$ soit une base de $\ker(f^2+\mathrm{Id})$.
Pour finir, la famille $(g_1, .., g_n, -f(g_1), .., -f(g_n))$ étant de cardinal $2n$ et l'espace $\ker(f^2+\mathrm{Id})$ étant aussi de dimension $2n$, montrer que la famille $(g_1, .., g_n, -f(g_1), .., -f(g_n))$ est une base de $\ker(f^2+\mathrm{Id})$ est équivalent à montrer que cette famille est libre

Synthèse : Puisque $\ker(f)$ est de dimension $n$, $\ker(f)$ possède une base $(e_1, .., e_n)$ formée de $n$ vecteurs.
Ensuite, soit $g_1$ un vecteur non nul de $\ker(f^2+\mathrm{Id})$, on sait que le vecteur $-f(g_1)$ appartient à $\ker(f^2+\mathrm{Id})$. Montrons que la famille $(g_1, -f(g_1))$ est libre, ce qui équivaut au fait que la famille $(g_1, f(g_1)$ soit libre. Supposons qu'elle soit liée, puisque $g_1$ est un vecteur non nul, cela implique que $f(g_1)$ est colinéaire à $g_1$. Il existe alors un réel $\lambda$ tel que $f(g_1) = \lambda g_1$. En composant pas $f$ et se rappelant que $g_1 \in \ker(f^2+\mathrm{Id})$ on obtient que

$$f^2(g_1) = \lambda f(g_1) \Leftrightarrow -g_1 = \lambda\lambda g_1 \Leftrightarrow \underbrace{g_1}_{\neq 0}(\lambda^2+1) = 0 \Leftrightarrow \lambda^2 + 1 = 0$$

Or $\lambda$ est un nombre réel donc $\lambda^2 + 1 \neq 0$, ce qui nous fournit une contradiction et ce qui prouve que la famille $(g_1, f(g_1))$ est une famille libre.
Si $n = 1$ alors $\dim\ker(f^2+\mathrm{Id}) = 2$ et la famille $(g_1, -f(g_1))$ est une base de $\ker(f^2+\mathrm{Id})$ et c'est fini.
Sinon, il existe un vecteur $g_2 \in \ker(f^2+\mathrm{Id})$ et n'appartenant pas à $\mathrm{Vect}(g_1, -f(g_1))$. Par conséquent, la famille $(g_1, -f(g_1), g_2)$ appartient à $\ker(f^2+\mathrm{Id})$ et elle est libre. Montrons que la famille $(g_1, -f(g_1), g_2, -f(g_2))$ est libre, ou ce qui revient au même, que la famille $(g_1, f(g_1), g_2, f(g_2))$ est libre. Puisque la famille $(g_1, f(g_1), g_2)$ est libre, cela revient à montrer que $f(g_2) \notin \mathrm{Vect}(g_1, f(g_1), g_2)$. Supposons que $f(g_2) \in \mathrm{Vect}(g_1, f(g_1), g_2)$ alors il existe trois constantes réelles $a, b, c$ telles que

$$f(g_2) = ag_1 + bf(g_1) + cg_2 \underset{f\circ}{\Rightarrow} f^2(g_2) = af(g_1) + bf^2(g_1) + cf(g_2) \Leftrightarrow -g_2 = af(g_1) - bg_1 + cf(g_2)$$

On en déduit les deux égalités suivantes

$$\begin{cases} f(g_2) = ag_1 + bf(g_1) + cg_2 \\ -g_2 = af(g_1) - bg_1 + cf(g_2) \end{cases} \Leftrightarrow \begin{cases} -cg_2 + f(g_2) = ag_1 + bf(g_1) \\ -g_2 - cf(g_2) = -bg_1 + af(g_1) \end{cases} \underset{cL_1+L_2}{\Rightarrow} (1+c^2)g_2 = \underbrace{(ac-b)g_1 + (bc+a)f(g_1)}_{\in \mathrm{Vect}(g_1, f(g_1))}$$

Puisque $c \in \mathbb{R}$, le réel $1+c^2$ est non nul, donc on peut effectuer la division et l'on obtient que $g_2 \in \mathrm{Vect}(g_1, f(g_1))$ ce qui est contraire au choix que l'on a fait pour $g_2$. Par conséquent, $f(g_2) \notin \mathrm{Vect}(g_1, f(g_1), g_2)$ et la famille $(g_1, -f(g_1), g_2, -f(g_2)$ est

libre. Si $n=4$ alors $(g_1,-f(g_1),g_2,-f(g_2)$ est une base de $\ker(f^2+\mathrm{Id})$ et c'est fini.
On procède ainsi par récurrence. Supposons avoir construit la famille libre $(g_1,-f(g_1),...,g_k,-f(g_k))$ avec $k\leqslant n$.
Si $k=n\Leftrightarrow 2k=2n$, c'est fini, sinon $k<n\Leftrightarrow 2k<2n$.
Dans ce cas, il existe un vecteur $g_{k+1}$ appartenant à $\ker(f^2+\mathrm{Id})$ (qui est de dimension $2n>2k$) tel que

$$g_{k+1}\notin \mathrm{Vect}(\underbrace{g_1,-f(g_1),...,g_k,-f(g_k)}_{2k \text{ vecteurs}})$$

donc la famille $(g_1,-f(g_1),...,g_k,-f(g_k),g_{k+1})$ est libre. Le vecteur $f(g_{k+1})$ appartient à $\ker(f^2+\mathrm{Id})$ et montrons que la famille $(g_1,-f(g_1),...,g_{k+1},-f(g_{k+1}))$ est libre, ce qui revient à montrer que

$$f(g_{k+1})\notin \mathrm{Vect}(g_1,f(g_1),..,g_k,f(g_k),g_{k+1}).$$

Supposons que $f(g_{k+1})\in \mathrm{Vect}(g_1,f(g_1),..,g_k,f(g_k),g_{k+1})$ alors il existe $2k+1$ réelles $(a_q)_{q\in[\![1,k]\!]},(b_q)_{q\in[\![1,k]\!]}$ et $c$ telles que

$$\begin{aligned} f(g_{k+1}) &= \left(\sum_{q=1}^{k} a_q g_q+b_q f(g_q)\right)+cg_{k+1} \underset{f\circ}{\Rightarrow} f^2(g_{k+1})=\left(\sum_{q=1}^{k} a_q f(g_q)+b_q f^2(g_q)\right)+cf(g_{k+1}) \\ &\Leftrightarrow -g_{k+1}=\left(\sum_{q=1}^{k} a_q f(g_q)-b_q g_q\right)+cf(g_{k+1}) \end{aligned}$$

On en déduit les deux égalités suivantes

$$\left\{\begin{array}{l} f(g_{k+1})=\left(\sum\limits_{q=1}^{k} a_q g_q+b_q f(g_q)\right)+cg_{k+1} \\ -g_{k+1}=\left(\sum\limits_{q=1}^{k} a_q f(g_q)-b_q g_q\right)+cf(g_{k+1}) \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} -cg_{k+1}+f(g_{k+1})=\left(\sum\limits_{q=1}^{k} a_q g_q+b_q f(g_q)\right) \\ -g_{k+1}-cf(g_{k+1})=\left(\sum\limits_{q=1}^{k} a_q f(g_q)-b_q g_q\right) \end{array}\right.$$

$$\underset{cL_1+L_2}{\Rightarrow} (1+c^2)g_{k+1} = \underbrace{\left(\sum_{q=1}^{k}(ca_q-b_q)g_q+(cb_q+a)f(g_q)\right)}_{\in \mathrm{Vect}\,\mathrm{Vect}(g_1,f(g_1),..,g_k,f(g_k))}$$

Puisque $c\in\mathbb{R}$, le réel $1+c^2$ est non nul, donc on peut effectuer la division et l'on obtient que $g_{k+1}\in\mathrm{Vect}(g_1,f(g_1),..,g_k,f(g_k))$ ce qui est contraire au choix que l'on a fait pour $g_{k+1}$. Par conséquent, $f(g_{k+1})\notin\mathrm{Vect}(g_1,f(g_1),..,g_k,f(g_k),g_{k+1})$ et la famille $(g_1,-f(g_1),...,g_{k+1},-f(g_{k+1}))$ est libre.
La récurrence est donc prouver et en choisissant $k=n$, on obtient l'existence d'une famille libre $(g_1,-f(g_1),...,g_n,-f(g_n))$ contenue dans $\ker(f^2+\mathrm{Id})$. Par conséquent, d'après les raisonnements menés dans l'analyse, on en déduit que

$$(e_1,..,e_n,g_1,..,g_n,-f(g_1),..,-f(g_n))$$

est une base de $\mathbb{R}^{3n}$ et la matrice de $f$ dans cette base est $\begin{pmatrix} 0_n & 0_n & 0_n \\ 0_n & 0_n & I_n \\ 0_n & -I_n & 0_n \end{pmatrix}$

**Correction de l'exercice 1.2 :**

1. *Rappelons que si $u$ et $v$ sont deux endomorphismes d'un même espace vectoriel de dimension finie $E$ alors*

$$\mathrm{rg}(u\circ v)\leqslant \min(\mathrm{rg}(u),\mathrm{rg}(v))$$

*Cela résulte simplement des inclusions ensembles suivantes :* $\mathrm{Im}(u\circ v)\subset\mathrm{Im}(u)$ *et* $\ker v\subset\ker(u\circ v)$.
Soit $e$ l'élément neutre de $G$ pour la multiplication (et $e\neq\mathrm{Id}$ à priori car $G$ est inclu dans $\mathcal{L}(E)$ et non dans $GL(E)$, penser à $G=\{\begin{pmatrix} a & 0 \\ 0 & 0\end{pmatrix},\quad a\in\mathbb{R}^{\times}\}$ qui est clairement un groupe pour la multiplication des matrices et dont l'élément neutre est $e=\begin{pmatrix} 1 & 0 \\ 0 & 0\end{pmatrix}\neq I_2$)
Soit $g$ un élément de $G$ (donc $g$ est un endomorphisme de $\mathbb{R}^n$) alors, par définition de l'élément neutre, on a

$$\forall g\in G,\quad g\circ e=g$$

ce qui implique que

$$\mathrm{rg}(g)=\mathrm{rg}(g\circ e)\leqslant\min(\mathrm{rg}(g),\mathrm{rg}(e))\leqslant\mathrm{rg}(e)\Rightarrow(1):\forall g\in G,\quad \mathrm{rg}(g)\leqslant\mathrm{rg}(e)$$

donc tout élément $g$ de $G$ a un rang moindre que le rang de l'élément neutre $e$. D'autre part, $G$ étant un groupe, tout élément $g$ de $G$ admet un inverse $g^{-1}$ qui appartient à $G$ et qui vérifie $e = g \circ g^{-1}$ donc

$$\mathrm{rg}(e) \leqslant \min(\mathrm{rg}(g), \mathrm{rg}(g^{-1})) \leqslant \mathrm{rg}(g) \Rightarrow (2) : \forall g \in G, \quad \mathrm{rg}(e) \leqslant \mathrm{rg}(g)$$

c'est-à-dire que le rang de tout élément $g$ de $G$ est supérieur ou égal au rang de $e$. Les inégalités (1) et (2) nous donne l'égalité (3)

$$(3) : \forall g \in G, \quad \mathrm{rg}(g) = \mathrm{rg}(e),$$

donc tous les éléments de $g$ ont le même rang : celui de l'élément neutre $e$.

2. Nous allons de nouveau utiliser l'élément neutre $e$ de $G$ (qui est clairement un élément central de notre histoire). Puisque $e$ est un élément neutre de $G$, il vérifie l'égalité remarquable $e^2 = e$. Mais comme $e$ est également un endomorphisme de $\mathbb{R}^n$, l'égalité précédente montre que $e$ est un projecteur de $\mathbb{R}^n$. La caractérisation des projecteur montre que $\mathbb{R}^n$ est la somme directe de $\ker(e)$ et $\mathrm{Im}(e)$ et que $\mathrm{Im}(e) = \ker(e - \mathrm{Id})$, nous en déduisons l'égalité remarquable :

$$\mathbb{R}^n = \ker(e) \oplus \mathrm{Im}(e) = \ker(e) \oplus \ker(e - \mathrm{Id})$$

Ensuite, puisque tout élément $g$ de $G$ commute avec $e$ et puisque $g$ et $e$ sont des endomorphismes, nous obtenons que les espaces propres de $e$ sont stables par tout élément de $g$, c'est-à-dire que

$$g(\ker(e)) \subset \ker(e) \quad \text{et} \quad g(\ker(e - \mathrm{Id})) \subset \ker(e - \mathrm{Id}).$$

Si l'on choisit une base $\mathcal{B}_0$ de $\ker(e)$ et une base $\mathcal{B}_1$ de $\ker(e - \mathrm{Id})$, le fait que $\mathbb{R}^n = \ker(e) \oplus \ker(e - \mathrm{Id})$ implique que $\mathcal{B} = (\mathcal{B}_0, \mathcal{B}_1)$ est une base de $\mathbb{R}^n$ et la matrice de tout élément $g$ dans la base $\mathcal{B}$ est de la forme

$$mat_{\mathcal{B}}(g) = \begin{array}{c} \begin{matrix} \ker(e-\mathrm{Id}) & \ker(e) \end{matrix} \\ \begin{pmatrix} A_g & 0 \\ 0 & 0 \end{pmatrix} \begin{matrix} \ker(e - \mathrm{Id}) \\ \ker(e) \end{matrix} \end{array},$$

où $A_g$ est une matrice carrée. En particulier, si $g$ est l'élément neutre $e$ de $G$, le fait que $e_{|\ker(e-\mathrm{Id})} = \mathrm{Id}_{\ker(e-\mathrm{Id})}$ et $e_{|\ker(e)} = 0_{\ker(e)}$ permet d'expliciter la matrice de $e$ dans la base $\mathcal{B}$ :

$$mat_{\mathcal{B}}(e) = \begin{pmatrix} \mathrm{Id}_p & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{où } p = \dim(\ker(e - \mathrm{Id})) = \mathrm{rg}(e)$$

Montrons pour finir que $A_g$ est une matrice inversible dans $\mathfrak{M}_p(\mathbb{R})$.
Soit $g$ un élément de $G$. Puisque $G$ est un groupe, $g$ admet un inverse $h$ dans $G$, c'est-à-dire que

$$g \circ h = h \circ g = e.$$

En passant à leurs matrices respectives dans la base $\mathcal{B}$, on obtient

$$\begin{gathered} mat_{\mathcal{B}}(g) \times mat_{\mathcal{B}}(h) = mat_{\mathcal{B}}(h) \times mat_{\mathcal{B}}(g) = mat_{\mathcal{B}}(e) \\ \Leftrightarrow \begin{pmatrix} A_g & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} A_h & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A_h & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} A_g & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix} \\ \Leftrightarrow A_g A_h = A_h A_g = I_p \end{gathered}$$

ce qui démontre que $A_g \in GL_p(\mathbb{R})$

3. Montrons les équivalences en montrant successivement que $a) \Rightarrow b), \quad b) \Rightarrow c), \quad c) \Rightarrow a)$

   $a) \Rightarrow b)$ Puisque $u$ appartient à un groupe multiplicatif $G$ inclu dans $\mathcal{L}(E)$, les éléments $u$ et $u^2$ sont dans $G$. La question 1) montre qu'ils ont même rang.

   $b) \Rightarrow c)$ Nous avons pour commencer les inclusions ensemblistes

   $$(1) : \ker(u) \subset \ker(u^2) \text{ et } \mathrm{Im}(u^2) \subset \mathrm{Im}(u).$$

   En passant au rang et en utilisant le théorème du rang, on obtient que

   $$\begin{aligned} &[n - \mathrm{rg}(u) \leqslant n - \mathrm{rg}(u^2) \text{ et } \mathrm{rg}(u^2) \leqslant \mathrm{rg}(u)] \Leftrightarrow [\mathrm{rg}(u^2) \leqslant \mathrm{rg}(u) \text{ et } \mathrm{rg}(u^2) \leqslant \mathrm{rg}(u)] \Leftrightarrow \mathrm{rg}(u^2) = \mathrm{rg}(u) \\ (2) : \quad &\Leftrightarrow \dim(\mathrm{Im}\, u^2) = \dim(u) \Leftrightarrow n - \dim(\mathrm{Im}(u^2)) = n - \dim(\mathrm{Im}(u)) \Leftrightarrow \dim\ker(u^2) = \dim\ker(u) \end{aligned}$$

   Puisque $\ker(u) \subset \ker(u^2)$ et $\dim\ker(u) = \dim\ker(u^2)$, on en déduit que

   $$\ker(u) = \ker(u^2)$$

et par le même procédé, on obtient que

$$\mathrm{Im}(u) = \mathrm{Im}(u^2).$$

Montrons que $\ker(u)$ et $\mathrm{Im}(u)$ sont en somme directe. Soit $y$ un élément de $\ker(u) \cap \mathrm{Im}(u)$. Alors $u(y) = 0$ et il existe un élément $x$ de $E$ tel que $y = u(x)$, ce qui nous permet d'écrire

$$u(u(x)) = 0 \Leftrightarrow u^2(x) = 0$$

donc $x \in \ker(u^2) = \ker(u)$. On en déduit que $y = u(x) = 0$ donc $\ker(u) \cap \mathrm{Im}(u) = \{0\}$ et $\ker(u)$ et $\mathrm{Im}(u)$ sont bien en somme directe. D'autre part, nous disposons de l'inclusion

$$\ker(u) \oplus \mathrm{Im}(u) \subset \mathbb{R}^n$$

et la dimension de $\ker(u) \oplus \mathrm{Im}(u)$ est égale à

$$\dim \ker(u) + \dim \mathrm{Im}(u) = n = \dim \mathbb{R}^n$$

(d'après le théorème du rang), ce qui nous permet d'affirmer que

$$\ker(u) \oplus \mathrm{Im}(u) = \mathbb{R}^n$$

$c) \Rightarrow a)$ Fixons une base $\mathcal{B}_0$ de $\ker(u)$ et une base $\mathcal{B}_1$ de $\mathrm{Im}(u)$. Le fait que $\ker(u)$ et $\mathrm{Im}(u)$ sont en somme directe implique que $\mathcal{B} = (\mathcal{B}_0, \mathcal{B}_1)$ est une base de $\mathbb{R}^n$ et la matrice de $u$ dans cette base est de la forme

$$mat_{\mathcal{B}}(u) = \begin{array}{c} \begin{matrix} \mathrm{Im}(u) & \ker(u) \end{matrix} \\ \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{l} \mathrm{Im}(u) \\ \ker(u) \end{array}$$

Or nous avons les égalités

$$\left(\mathrm{rg}(mat_{\mathcal{B}}(u)) = \mathrm{rg}(u) \quad \text{et} \quad \mathrm{rg}\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} = \mathrm{rg}(A)\right) \Rightarrow \mathrm{rg}(A) = \mathrm{rg}(u).$$

Si l'on note $p = \mathrm{rg}(u)$, la matrice $A$ est de taille $\dim \mathrm{Im}(u) = \mathrm{rg}(u) = p$ et son rang est $p$ donc $A \in GL_p(\mathbb{R})$. Si l'on note $G'$ l'ensemble suivant

$$G' = \{\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}, \quad B \in GL_p(\mathbb{R})\}.$$

Montrons que $G'$ est un groupe pour la multiplication de matrices.

- $G'$ est non vide : $\begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix} \in G'$.
- $G'$ est stable par produit : Si $X_1$ et $X_2$ sont deux éléments de $G'$ alors il existe deux matrices $B_1$ et $B_2$ de $GL_p(\mathbb{R})$ telles que pour

  $$i = 1, 2, \quad X_i = \begin{pmatrix} B_i & 0 \\ 0 & 0 \end{pmatrix}$$

  Le calcul matriciel par bloc montre que $X_1X_2 = \begin{pmatrix} B_1B_2 & 0 \\ 0 & 0 \end{pmatrix}$ et comme $B_1B_2 \in GL_p(\mathbb{R})$, on en déduit que $X_1X_2 \in G'$
- Le produit est associatif : cela résulte que le produit des matrices est associatif
- Le produit admet un élément neutre : Si l'on considère la matrice $E = \begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix}$, on a $\forall \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \in G'$,

  $$\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} BI_p & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix},$$
  $$\begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_pB & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}$$

  ce qui montre que $E$ est l'élément neutre de $G'$
- Tout élément de $G'$ admet un inverse : Soit $\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \in G'$. Par définition $B \in GL_p(\mathbb{R})$,donc $B^{-1} \in GL_p(\mathbb{R})$ et la matrice $\begin{pmatrix} B^{-1} & 0 \\ 0 & 0 \end{pmatrix}$ appartient à $G'$. Pour finir, les égalités

  $$\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} B^{-1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} BB^{-1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix} = E$$
  $$\begin{pmatrix} B^{-1} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} B^{-1}B & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & 0 \end{pmatrix} = E$$

montre que $\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}$ admet un inverse dans $G'$ qui est la matrice $\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}$, ce qui achève la preuve que $G'$ est un groupe pour la multiplication des matrices.

Si l'on note $G$ l'ensemble

$$G = \{g \in \mathcal{L}(\mathbb{R}^n) \text{ tel que } mat_{\mathcal{B}}(g) \in G'\},$$

où rappelons-le $\mathcal{B} = (\mathcal{B}_0, \mathcal{B}_1)$ est la base définitie au début de la question, alors $G$ est un groupe pour la composition des endomorphismes de $\mathbb{R}^n$ (la preuve est laissée au soin du lecteur, elle utilise essentiellement le fait que $mat_{\mathcal{B}}(g \circ h) = mat_{\mathcal{B}}(g) \times mat_{\mathcal{B}}(h)$) et par construction $mat_{\mathcal{B}}(u) \in G'$ donc $u \in G$.

**Correction de l'exercice 1.3 :** On peut traiter cet exercice selon deux méthodes

- Première méthode :
L'endomorphisme $a$ de $\mathbb{R}^n$ possède le polynôme $X^q - 1$ comme polynôme annulateur. Malheureusement ce polynôme n'est pas scindé sur $\mathbb{R}$ mais il est scindé sur $\mathbb{C}$. Nous allons en fait nous ramener à $\mathbb{C}$ par l'astuce suivante (c'est un peu plus qu'une astuce, c'est une méthode pour passer du champs des réels au champs des complexes).
Considérons la base canonique $\mathcal{B}_{\mathbb{R}}$ de $\mathbb{R}^n$ et notons $A$ la matrice de $a$ dans la base $\mathcal{B}$, c'est-à-dire $A = mat(a, \mathcal{B}_{\mathbb{R}})$. La matrice $A$ est à coefficients réels donc elle peut être vue comme une matrice à coefficients complexes. Considérons alors la base canonique $\mathcal{B}_{\mathbb{C}}$ de $\mathbb{C}^n$ et notons $b$ l'unique endomorphisme de $\mathbb{C}^n$ tel que $A = mat(b, \mathcal{B}_{\mathbb{C}})$. L'endomorphisme $b$ admet $X^q - 1$ comme polynôme annulateur puisque

$$mat(b^q, \mathcal{B}_{\mathbb{C}}) = (mat(b, \mathcal{B}_{\mathbb{C}}))^q = A^q = (mat(a, \mathcal{B}_{\mathbb{R}}))^q = mat(a^q, \mathcal{B}_{\mathbb{R}}) = mat(\mathrm{Id}, \mathcal{B}_{\mathbb{R}}) = I_n \Rightarrow b^q = \mathrm{Id}$$

(et on est sauvé car la matrice identité de $\mathfrak{M}_n(\mathbb{R})$ est la même que celle de $\mathfrak{M}_n(\mathbb{C})$.
**Si l'on a fait le cours sur la diagonalisation** : Le polynôme $X^q - 1$ est scindé à racines simples sur $\mathbb{C}$ (donc $b$ est diagonalisable sur $\mathbb{C}$) et ses racines sont des racines $q^{ième}$ de l'unité.
**Si l'on n'a pas fait le cours sur la diagonalisation mais si l'on connait le théorème des noyaux** :
Le polynôme $X^q - 1$ est scindé à racines simples sur $\mathbb{C}$ et sa décomposition est donnée par

$$X^q - 1 = \prod_{k=0}^{q-1} (X - \exp(\frac{2i\pi k}{q})$$

Le théorème des noyau montre que l'on a

$$\mathbb{C}^n = \bigoplus_{k=0}^{q-1} \ker(b - \exp(\frac{2i\pi k}{q}) \mathrm{Id})$$

Considérons pour chaque $k \in [\![0, q-1]\!]$, une base $\mathcal{B}_k$de $\ker(b - \exp(\frac{2i\pi k}{q}) \mathrm{Id})$ lorsque $\ker(b - \exp(\frac{2i\pi k}{q}) \mathrm{Id}) \neq \{0\}$. Alors, la somme précédente étant directe, la réunion des $\mathcal{B}_k$ forment une base $\mathcal{B}'_{\mathbb{C}}$ de $\mathbb{C}^n$.
**La suite est pour tout le monde** :
Pour tout entier $k \in [\![0, q-1]\!]$, notons $\zeta_k = \exp(\frac{2i\pi k}{q})$. Il est de notoriété publique que l'ensemble des racines $q^{ième}$ de l'unité est l'ensemble $\{\zeta_k, \quad k \in [\![0, q-1]\!]\}$. Notons $r_k$ la multiplicité de $\zeta_k$ dans $b$, autrement dit

$$r_k = \dim_{\mathbb{C}} \ker(b - \zeta_k) = \dim_{\mathbb{C}} E_{\zeta_k}(b),$$

l'entier $r_k$ pouvant bien entendu être nul, ce qui arrive lorsque $\zeta_k$ n'est pas valeur propre de $A$.
Le fait que $b$ soit diagonalisable et que ses valeurs soient des racines $q^{ième}$ de l'unité montre l'existence d'une base $\mathcal{B}'_{\mathbb{C}}$ (réunion des $\mathcal{B}_k$ pour ceux qui n'on pas fait la diagonalisation) de $\mathbb{C}^n$ telle que

$$mat(b, \mathcal{B}'_{\mathbb{C}}) = \begin{pmatrix} \zeta_0 I_{r_0} & & (0) \\ & \ddots & \\ (0) & & \zeta_{q-1} I_{r_{q-1}} \end{pmatrix},$$

ce qui nous assure que

$$mat(b^i, \mathcal{B}'_{\mathbb{C}}) = \begin{pmatrix} (\zeta_0)^i I_{r_0} & & (0) \\ & \ddots & \\ (0) & & (\zeta_{q-1})^i I_{r_{q-1}} \end{pmatrix}$$

La trace d'un endomorphisme ne dépendant pas de la base choisie et étant la trace de sa matrice dans une base quelconque, on en déduit que

$$\mathrm{tr}(A^i) = \mathrm{tr}(b^i) = (\zeta_0)^i \,\mathrm{tr}(I_{r_0}) + \cdots + (\zeta_{q-1})^i \,\mathrm{tr}(I_{r_{q-1}}) = (\zeta_0)^i r_0 + \cdots + (\zeta_{q-1})^i r_{q-1} = \sum_{p=0}^{q-1} (\zeta_p)^i r_p$$

Nous pouvons alors écrire

$$\sum_{i=1}^{q} \mathrm{tr}(A^i) = \sum_{i=1}^{q}\sum_{p=0}^{q-1} (\zeta_p)^i r_p \underset{\text{Fubini}}{=} \sum_{p=0}^{q-1}\sum_{i=1}^{q} (\zeta_p)^i r_p = \sum_{p=0}^{q-1} r_p \sum_{i=1}^{q} (\zeta_p)^i$$

Il nous reste à évaluer les sommes $\sum_{i=1}^{q} (\zeta_p)^i$, où rappelons-le $\zeta_p$ est une racine $q^{ième}$ de l'unité.

Si $p = 0$ alors $\zeta_0 = 1$ et $\sum_{i=1}^{q} (\zeta_0)^i = \sum_{i=1}^{q} 1 = q$.

Si $p \in [\![1, q-1]\!]$ alors $\zeta_p \neq 1$ et l'on a :

$$\begin{aligned}\sum_{i=1}^{q} (\zeta_p)^i &= (\zeta_p)^1 + (\zeta_p)^2 + \cdots + (\zeta_p)^{q-1} + (\zeta_p)^q = (\zeta_p)^1 + (\zeta_p)^2 + \cdots + (\zeta_p)^{q-1} + 1 \\ &= 1 + (\zeta_p)^1 + (\zeta_p)^2 + \cdots + (\zeta_p)^{q-1} = \frac{1-(\zeta_p)^q}{1-\zeta_p} = \frac{1-1}{1-\zeta_p} = 0\end{aligned}$$

Nous en déduisons naturellement que

$$\sum_{i=1}^{q} \mathrm{tr}(A^i) = r_0 \sum_{i=1}^{q} (\zeta_0)^i = r_0 q \Leftrightarrow \frac{1}{q}\sum_{i=1}^{q} \mathrm{tr}(A^i) = r_0 = \dim_{\mathbb{C}} \ker(b - \mathrm{Id})$$

Nous avons presque l'égalité demandée. Il suffit de se rappeler le lien entre matrice et endomorphisme.
On rappelle que la matrice de $b$ dans la base canonique $\mathcal{B}_{\mathbb{C}^n}$ de $\mathbb{C}^n$ est la matrice $A$. Soit $x = (x_1, .., x_n)$ un vecteur de $\mathbb{C}^n$, $X$ sa matrice des coordonnées dans la base canonique. Par définition, on a $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et le vecteur formé des coordonnées de $b(x)$ est simplement la matrice colonne $AX$. Par conséquent, les égalités $b(x) = x$ et $AX = X$ sont équivalentes, en fait on a même un isomorphisme de $\ker(b - \mathrm{Id})$ sur $\ker(A - \mathrm{Id})$ donné par $x \to X$, ce qui implique que

$$\dim_{\mathbb{C}} \ker(b - \mathrm{Id}) = \dim_{\mathbb{C}} \ker(A - I_n)$$

Ensuite, $n - \dim_{\mathbb{C}} \ker(A - I_n)$ représente le rang dans $\mathbb{C}^n$ des vecteurs colonnes de $A - I_n$, $n - \dim_{\mathbb{R}}(\ker(A - I_n)$ représente le rang dans $\mathbb{R}^n$ des vecteurs colonnes de $A - I_n$. Puisque $A - I_n$ est à coefficients réels, ses vecteurs colonnes sont à coordonnées réelles et le rang d'une famille de vecteurs à coordonnées réels est le même dans $\mathbb{R}^n$ (vu comme $\mathbb{R}$-espace vectoriel) ou dans $\mathbb{C}^n$ (vu comme $\mathbb{C}$-espace vectoriel) (la preuve se trouve dans la remarque ci-dessous)
Par conséquent, on a

$$n - \dim_{\mathbb{C}} \ker(A - I_n) = n - \dim_{\mathbb{R}}(\ker(A - I_n) \Leftrightarrow \dim_{\mathbb{C}} \ker(A - I_n) = \dim_{\mathbb{R}}(\ker(A - I_n)$$

et puisque $A$ est la matrice de $a$ dans la base canonique $\mathcal{B}_{\mathbb{R}}$ de $\mathbb{R}^n$, nous obtenons la formule tant attendue

$$\dim_{\mathbb{R}}(\ker(A - I_n)) = \frac{1}{q}\sum_{i=1}^{q} \mathrm{tr}(A^i) \Leftrightarrow \dim_{\mathbb{R}}(\ker(a - I_n)) = \frac{1}{q}\sum_{i=1}^{q} \mathrm{tr}(a^i).$$

*Remarque : Le rang d'une famille étant le plus grand nombre de vecteurs libres d'une famille, il suffit de montrer que toute famille de vecteurs $(f_1, .., f_p)$* ***à coordonnées réelles*** *est libre sur $\mathbb{C}$ ssi elle est libre sur $\mathbb{R}$.*

*Si $(f_1, .., f_p)$ est libre sur $\mathbb{C}$, et soient $\lambda_1, .., \lambda_p$ des réels tels que $\sum_{i=1}^{p} \lambda_i f_i = 0$. Les $\lambda_i$ étant réels, on peut les considérer comme des complexes et l'égalité précédente fournit une relation de dépendance linéaires de $f_i$ sur $\mathbb{C}$. Ces derniers étant libres sur $\mathbb{C}$, cela implique que tous les $\lambda_i$ sont nuls donc la famille $(f_1, .., f_p)$ est libre sur $\mathbb{R}$.*

*Si $(f_1, .., f_p)$ est libre sur $\mathbb{R}$, et soient $\lambda_1, .., \lambda_p$ des complexes tels que $\sum_{i=1}^{p} \lambda_i f_i = 0$. En passant aux coordonnées, en tenant compte que les coordonnées de $f_i$ sont réelles et en séparant les parties réelles et imaginaires des $\lambda_i$, on aboutit à deux systèmes équivalents à $\sum_{i=1}^{p} \underbrace{\mathrm{Re}(\lambda_i)}_{\in\mathbb{R}} f_i = 0$ et $\sum_{i=1}^{p} \underbrace{\mathrm{Im}(\lambda_i)}_{\in\mathbb{R}} f_i = 0$. Ces deux égalités sont des relations de dépendance linéaire sur $R$ des $f_i$. Ces derniers étant libres sur $\mathbb{R}$, cela implique que tous les $\mathrm{Re}(\lambda_i)$ et $\mathrm{Im}(\lambda_i)$ sont nuls. On en déduit immédiatement que tout les $\lambda_i$ sont nuls, ce qui démontre que la famille $(f_1, .., f_p)$ est libre sur $\mathbb{C}$.*

- Deuxième méthode (pour ceux qui aiment les groupes) :
On introduit l'endomorphisme $p$ de $\mathbb{R}^n$ défini par

$$p = \frac{1}{q}(\mathrm{Id} + a + \cdots + a^{q-1})$$

Montrons que $p$ est un projecteur. Pour commencer, puisque $a^q = \mathrm{Id}$, on a

$$a \circ p = \frac{1}{q}(a + a^2 + \cdots + a^{q-1} + a^q) = \frac{1}{q}(a + a^2 + \cdots + a^{q-1} + \mathrm{Id}) = \frac{1}{q}(\mathrm{Id} + a + \cdots + a^{q-1}) = p$$

Par une récurrence évidente, on obtient que $\forall k \in [\![0, q-1]\!], \quad a^k \circ p = p$ et en sommant ces égalités sur $k$ variant de 0 à $q-1$, on obtient

$$\sum_{k=0}^{q-1} a^k \circ p = \sum_{k=0}^{q-1} p \Leftrightarrow \left( \underbrace{\sum_{k=0}^{q-1} a^k}_{=q\times p} \right) \circ p = q \times p \Leftrightarrow q \times p \circ p = q \times p \Leftrightarrow p \circ p = p$$

donc $p$ est bien un projecteur de $\mathbb{R}^n$. On sait que la trace d'un projecteur est égal à son rang donc

$$\mathrm{tr}(p) = \mathrm{rg}(p) \Leftrightarrow \mathrm{tr}(\frac{1}{q}\sum_{k=0}^{q-1} a^k) = \mathrm{rg}(p) \Leftrightarrow \frac{1}{q}\sum_{k=0}^{q-1} \mathrm{tr}(a^k) = \mathrm{rg}(p) \qquad (1)$$

Pour obtenir la formule souhaitée, il suffit de montrer que

$$\mathrm{rg}(p) = \dim \ker(a - \mathrm{Id}) \Leftrightarrow \dim \mathrm{Im}\, p = \dim \ker(a - \mathrm{Id})$$

Soit $x \in \ker(a - \mathrm{Id})$ alors $a(x) = x$ ce qui implique que pour tous les entiers $k \in [\![0, k-1]\!]$, $a^k(x) = x$ donc

$$\forall x \in \ker(a - \mathrm{Id}), \quad p(x) = \frac{1}{q}\sum_{k=0}^{q-1} a^k(x) = \frac{1}{q}\sum_{k=0}^{q-1} x = \frac{1}{q} \times q \times x = x.$$

Nous venons donc de montrer que

$$(2) \qquad \ker(a - \mathrm{Id}) \subset \ker(p - \mathrm{Id}) = \mathrm{Im}\, p$$

(caractérisation des projecteurs).
Réciproquement, si $x \in \mathrm{Im}(p) = \ker(p - \mathrm{Id})$, l'égalité $p = a \circ p$, que nous avons montré précédemment, nous fournit les égalités suivantesmontre que

$$\forall x \in \mathrm{Im}\, p, \quad p(x) = x \underset{a\circ}{\Rightarrow} a(p(x)) = a(x) \underset{a\circ p = p}{\Leftrightarrow} p(x) = a(x) \underset{\text{puisque } p(x)=x}{\Rightarrow} x = a(x) \Rightarrow x \in \ker(a - \mathrm{Id})$$

Nous venons de montrer que

$$(3) \qquad \mathrm{Im}\, p \subset \ker(a - \mathrm{Id}).$$

Les égalités (2) et (3) montrent que $\mathrm{Im}(p) = \ker(a - \mathrm{Id})$ donc, en passant au dimension, on obtient $\mathrm{rg}(p) = \dim \ker(a - \mathrm{Id})$ et la formule (1) nous fournit alors l'égalité recherchée

$$\frac{1}{q}\sum_{k=0}^{q-1} \mathrm{tr}(a^k) = \dim \ker(a - \mathrm{Id})$$

*Remarque : en général, si $G$ est un groupe commutatif fini de $GL_n(k)$, où $k$ est corps de caractéristique distinct de* $\mathrm{card}\, G$, *alors* $p = \dfrac{1}{\mathrm{card}\, G}\sum_{g\in G} g$ *(qui est la moyenne des éléments du groupe) est un projecteur sur* $\bigcap_{g\in G} \ker(g - \mathrm{Id})$.
*Dans notre cas puisque $A$ est un élément d'ordre finie de $GL_n(\mathbb{R})$, le groupe* $< A >= \{A^k, \quad k \in [\![0, q-1]\!]\}$ *engendré par $A$ est fini et le projecteur s'écrit simplement* $p = \dfrac{1}{q}\sum_{k=0}^{q-1} A^k$.
*Exercice subsidiaire : Montrer que $S$ est une partie finie de* $\mathfrak{M}_n(\mathbb{R})$ *(ses éléments n'étant pas nécessairement inversibles) stable par produit alors* $\mathrm{card}\, S$ *divise* $\sum_{s\in S} \mathrm{tr}(s)$

**Correction de l'exercice 1.4 :** La matrice $A=0$ est solution évidente de l'équation. Supposons maintenant que $A\neq 0$. La matrice admet le polynôme $X^3+X^2+X$ comme polynôme annulateur. Ce dernier se décompose en produit d'irréductibles sur $\mathbb{R}[X]$ de la façon suivante :

$$X^3+X^2+X=X(X^2+X+1)$$

Le théorème des noyaux montre alors que

$$\mathbb{R}^3=\ker(A)\oplus\ker(A^2+A+I_3)$$

Montrons que $\ker(A)\neq\{0\}$ : Le polynôme caractéristique de $A$ est à coefficients réels et de degré 3 (puisque $A\in\mathfrak{M}_3(\mathbb{R})$). Or tout polynôme à coefficients réels de degré impair admet au moins une racine réelle donc $A$ admet au moins une valeur propre réelle. Soit $\lambda$ une valeur propre réelle de $A$ et $x$ un vecteur propre de $A$ associé à cette valeur propre $A$. Par définition, on a $Ax=\lambda x$ avec $x\neq 0$, ce qui implique que

$$\begin{aligned}A^2x &= A(Ax)=A(\lambda x)=\lambda Ax=\lambda\lambda x=\lambda^2x\\ A^3x &= A(A^2x)=A(\lambda^2x)=\lambda^2Ax=\lambda^2\lambda x=\lambda^3x\end{aligned}$$

Puisque $A^3+A^2+A=0$, on en déduit que

$$(A^3+A^2+A)x=0\Leftrightarrow A^3x+A^2x+Ax=0\Leftrightarrow\lambda^3x+\lambda^2x+\lambda x=0\Leftrightarrow\lambda(\lambda^2+\lambda+1)x=0$$

Or le vecteur $x$ étant non et le polynôme $X^2+X+1$ n'admettant aucune racine réelle, l'égalité précédente implique que $\lambda=0$. Par conséquent, $A$ admet une unique valeur propre réelle qui est 0 donc, $A$ étant non nulle, on a :

$$\ker(A)\neq\{0\}\text{ et }\neq\mathbb{R}^3\Rightarrow 2\geqslant\underbrace{\dim\ker A}_{=3-\mathrm{rg}(A)}\geqslant 1\Leftrightarrow 2\geqslant 3-\mathrm{rg}(A)\geqslant 1\Leftrightarrow 1\leqslant\mathrm{rg}(A)\leqslant 2$$

Montrons que $\mathrm{rg}(A)=2$ et $\dim\ker(A)=1$ : Puisque $\mathbb{R}^3=\ker(A)\oplus\ker(A^2+A+I_3)$ et que $\ker(A)\neq\mathbb{R}^3$, on est certain que $\ker(A^2+A+I_3)\neq\{0\}$.
Soit $x\in\ker(A^2+A+I_3)\backslash\{0\}$. Montrons que la famille $(x,Ax)$ est libre dans $\mathbb{R}^3$. Pour cela, procédons par l'absurde. Si la famille $(x,Ax)$ est liée alors, puisque $x\neq 0$, cela signifie que $Ax$ est colinéaire à $x$. Il existe alors un réel $\lambda$ tel que $Ax=\lambda x$ donc

$$A^2x=A(Ax)=A(\lambda x)=\lambda Ax=\lambda\lambda x=\lambda^2x$$

Puisque $x\in\ker(A^2+A+I_3)$, on a

$$(A^2+A+I_3)x=0\Leftrightarrow A^2x+Ax+x=0\Leftrightarrow\lambda^2x+\lambda x+x=0\Leftrightarrow(\lambda^2+\lambda+1)\underbrace{x}_{\neq 0}=0\Rightarrow\lambda^2+\lambda+1=0$$

Or $\lambda$ est un réel et l'équation $X^2+X+1$ n'admet aucune solution dans $\mathbb{R}$, ce qui implique que $(x,Ax)$ n'est pas une famille liée donc $(x,Ax)$ est libre. Ensuite, il est évident que $Ax\in\mathrm{Im}(A)$ et, puisque $x\in\ker(A^2+A+I_3)$, on a

$$A^2x+Ax+x=0\Leftrightarrow x=-Ax-A^2x=A(-x-Ax)$$

donc $x\in\mathrm{Im}(A)$, ce qui implique que $\dim\mathrm{Im}(A)=\mathrm{rg}(A)\geqslant 2$. Or nous avons vu précédemment que $\mathrm{rg}(A)\leqslant 2$ donc $\mathrm{rg}(A)=2$ et le théorème du rang implique $\dim\ker A=1$.
En utilisant la somme directe $\mathbb{R}^3=\ker(A)\oplus\ker(A^2+A+I_3)$, on peut même affirmer que $\dim\ker(A^2+A+\mathrm{Id})=2$
Montrons que $A$ est semblable à la matrice recherchée : Puisque $\dim\ker(A)=1$, il existe un vecteur $e_1\in\mathbb{R}^3$ tel que $\ker A=\mathrm{Vect}(e_1)$. Ensuite, pour montrer que $A$ est semblable à la matrice $B=\begin{pmatrix}0&0&0\\0&\frac{1}{2}&\frac{\sqrt{3}}{2}\\0&-\frac{\sqrt{3}}{2}&\frac{1}{2}\end{pmatrix}$, il faut et il suffit de trouver deux vecteurs $e_2$ et $e_3$ tel que

$$\left\{\begin{array}{c}Ae_2=-\frac{1}{2}e_2-\frac{\sqrt{3}}{2}e_3\\ Ae_3=\frac{\sqrt{3}}{2}e_2-\frac{1}{2}e_3\end{array}\right.\Leftrightarrow\left\{\begin{array}{c}(A+\frac{1}{2}I)e_2=-\frac{\sqrt{3}}{2}e_3\\ (A+\frac{1}{2}I)e_3=\frac{\sqrt{3}}{2}e_2\end{array}\right.\Leftrightarrow\left\{\begin{array}{l}e_3=-\frac{2}{\sqrt{3}}(A+\frac{1}{2}I)e_2\\ e_2=\frac{2}{\sqrt{3}}(A+\frac{1}{2}I)e_3=-\frac{4}{3}(A+\frac{1}{2}I)^2e_2\end{array}\right.$$

$$\Leftrightarrow\left\{\begin{array}{l}e_3=-\frac{2}{\sqrt{3}}(A+\frac{1}{2}I)e_2\\ ((A+\frac{1}{2}I)^2+\frac{3}{4})e_2=0\end{array}\right.\Leftrightarrow\left\{\begin{array}{c}e_3=-\frac{2}{\sqrt{3}}(A+\frac{1}{2}I)e_2\\ (A^2+A+I)e_2=0\end{array}\right.$$

Ainsi, il faut et il suffit que vecteur $e_2$ appartienne à $\ker(A^2+A+I)$, qui est de dimension 2.
Considérons un vecteur $e_2$ non nul appartenant à $\ker(A^2+A+I_3)$ et soit $e_3$ le vecteur défini par

$$e_3 = -\frac{2}{\sqrt{3}}(A+\frac{1}{2}I)e_2$$

Montrons que la famille $(e_2, e_3)$ est libre. Puisque l'on a :

$$\text{Vect}(e_2,e_3) = \text{Vect}(e_2, -\frac{2}{\sqrt{3}}Ae_2 - \frac{1}{\sqrt{3}}e_2) = \text{Vect}(e_2, Ae_2)$$

et que nous avons vu dans la partie "Montrons que $\text{rg}(A)=2$ et $\dim\ker(A)=1$" que la condition $e_2 \in \ker(A^2+A+I_3)\backslash\{0\}$ implique que la famille $(e_2, Ae_2)$ est libre, nous pouvons affirmer que $\dim \text{Vect}(e_2,e_3) = \dim \text{Vect}(e_2, Ae_2) = 2$, ce qui entraine que les vecteurs $e_2$ et $e_3$ sont libres.
Ensuite, puisque $A$ laisse stable $\ker(A^2+A+I_3)$ (toute matrice $B$ laisse stable $\ker P(B)$ pour tout polynôme $B$) et puisque $e_2 \in \ker(A^2+A+I_3)$, on est assuré que $Ae_2 \in \ker(A^2+A+I_3)$ donc $\underbrace{\text{Vect}(e_2,e_3)}_{\dim=2} = \text{Vect}(e_2,Ae_2) \subset \underbrace{\ker(A^2+A+I_3)}_{\dim=2}$ et par égalité des dimensions, on a $\text{Vect}(e_2,e_3) = \ker(A^2+A+I_3)$, c'est-à-dire que $(e_2,e_3)$ est une base de $\ker(A^2+A+I_3)$. Or le fait que le vecteur $e_1$ forme une base de $\ker(A)$ combiné à la somme directe

$$\mathbb{R}^3 = \ker(A) \oplus \ker(A^2+A+I_3)$$

montre que $(e_1,e_2,e_3)$ est une base de $\mathbb{R}^3$. Les égalités

$$Ae_1 = 0, \quad Ae_2 = -\frac{1}{2}e_2 - \frac{\sqrt{3}}{2}e_3, \quad Ae_3 = \frac{\sqrt{3}}{2}e_2 - \frac{1}{2}e_3$$

montrent que, si $P$ désigne la matrice de changement de base de la base canonique dans la base $(e_1,e_2,e_3)$, on a

$$A = P\begin{pmatrix} 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} P^{-1}.$$