
Mathématiques A : éléments de correction

Problème d'algèbre linéaire

Partie I

1. On obtient $A^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, d'où l'on tire $A^2 + I = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Le noyau de la matrice $A^2 + I$ n'est donc pas $\{0_{K^3}\}$, puisqu'il contient par exemple le premier vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ de la base canonique.

Cela montre que $A^2 + I$ n'est pas inversible.

2. On a

$$\begin{aligned} \chi_A &= \det(XI - A) \\ &= \begin{vmatrix} X & 0 & -1 \\ 0 & X & 0 \\ 1 & 0 & X \end{vmatrix} \\ &= X \begin{vmatrix} X & -1 \\ 1 & X \end{vmatrix} && \text{(dév. p.r. à la deuxième ligne)} \\ &= X(X^2 + 1) \\ &= X(X - i)(X + i). \end{aligned}$$

Le polynôme χ_A a donc trois racines complexes : 0, i et $-i$, ce qui montre que ces trois nombres complexes sont les trois valeurs propres complexes de A .

3. Sur \mathbb{C} , la matrice A , d'ordre 3, a trois valeurs propres distinctes, donc elle est diagonalisable. On a d'ailleurs déterminé les valeurs propres explicitement, ce qui montre que A est semblable à $\text{diag}(0, i, -i)$. Le polynôme caractéristique de A n'étant pas scindé sur \mathbb{R} , la matrice A n'est pas trigonalisable sur \mathbb{R} et donc *a fortiori* pas diagonalisable sur \mathbb{R} .

4. D'après le cours sur les opérations élémentaires sur les lignes, la matrice d'échange $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

est inversible, et égale à sa propre inverse. Autrement dit, $P \in GL_3(\mathbb{R}) \subseteq GL_3(\mathbb{C})$.

Comme

$$\begin{aligned} PAP^{-1} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} && \text{(échange des lignes)} \end{aligned}$$

1. <mailto:maxime.bourrigan@gmail.com>

$$= \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (\text{échange des colonnes})$$

$$= B,$$

on a donc bien que A et B sont semblables, qu'on les considère comme matrices réelles ou complexes.

Partie II

1. Soit $n \in \mathbb{N}^*$. L'application de transposition

$$T : \begin{cases} M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R}) \\ M \mapsto {}^t M \end{cases}$$

est un élément de $\mathcal{L}(M_n(\mathbb{R}))$. Par stabilité par combinaison linéaire, il en va de même de $T + \text{id}_{M_n(\mathbb{R})}$. On en déduit que

$$A_n(\mathbb{R}) = \ker(T + \text{id}_{M_n(\mathbb{R})})$$

est un sous-espace vectoriel de $M_n(\mathbb{R})$.

2. Soit $A \in A_3(\mathbb{R})$. On a alors

$$\forall i \in \llbracket 1, 3 \rrbracket, A_{i,i} = -A_{i,i} \quad \text{donc} \quad \forall i \in \llbracket 1, 3 \rrbracket, A_{i,i} = 0$$

En outre, si l'on note $\alpha = A_{3,2}$, $\beta = A_{1,3}$ et $\gamma = A_{2,1}$, on a $A_{2,3} = -\alpha$, $A_{3,1} = -\beta$ et $A_{1,2} = -\gamma$, d'où l'on tire

$$A = \begin{pmatrix} 0 & -\gamma & \beta \\ \gamma & 0 & -\alpha \\ -\beta & \alpha & 0 \end{pmatrix}.$$

3. On note, pour tous $i, j \in \llbracket 1, 3 \rrbracket$, $E_{i,j}$ la matrice dont le coefficient (i, j) vaut 1 et tous les autres valent 0. On pose par ailleurs $U = E_{3,2} - E_{2,3}$, $V = E_{1,3} - E_{3,1}$ et $W = E_{2,1} - E_{1,2}$. Remarquons que ces trois matrices sont bien éléments de $A_3(\mathbb{R})$. La question précédente se traduit en l'assertion

$$\forall A \in A_3(\mathbb{R}), \exists \alpha, \beta, \gamma \in \mathbb{R} : A = \alpha U + \beta V + \gamma W,$$

ce qui montre que (U, V, W) est une famille génératrice de $A_3(\mathbb{R})$.

Montrons maintenant la liberté de cette famille.

Soit $\alpha, \beta, \gamma \in \mathbb{R}$ tels que $\alpha U + \beta V + \gamma W = \mathbf{0}_{M_3(\mathbb{R})}$. Cela signifie

$$\begin{pmatrix} 0 & -\gamma & \beta \\ \gamma & 0 & -\alpha \\ -\beta & \alpha & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

et l'on obtient $\alpha = \beta = \gamma = 0$ en considérant les coefficients $(3, 2)$, $(1, 3)$ et $(2, 1)$ de part et d'autre de cette égalité.

Ainsi, (U, V, W) est une famille libre et génératrice de $A_3(\mathbb{R})$, ce qui montre qu'elle est une base de ce sous-espace vectoriel.

Puisqu'il admet une base à trois éléments, la dimension de ce sous-espace vectoriel est 3.

4. Soit $A \in A_3(\mathbb{R})$. On a

$$\begin{aligned}
\det A &= \det({}^t A) && \text{(prop. générale de dét)} \\
&= \det(-A) && \text{(car } A \in A_3(\mathbb{R})) \\
&= (-1)^3 \det A && \text{(trilinéarité de dét)} \\
&= -\det A,
\end{aligned}$$

ce qui démontre $\det A = 0$.

5. Notons $\mathcal{C} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ la base canonique de \mathbb{R}^3 et, pour tout $w \in \mathbb{R}^3$,

$$\varphi_w : \begin{cases} \mathbb{R}^3 \rightarrow \mathbb{R}^3 \\ v \mapsto w \wedge v. \end{cases}$$

La bilinéarité du produit vectoriel montre que φ_w est un endomorphisme de \mathbb{R}^3 .

Soit maintenant $\alpha, \beta, \gamma \in \mathbb{R}$ et $w = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \in \mathbb{R}^3$. On a

$$\begin{aligned}
\varphi_w(\mathbf{c}_1) &= w \wedge \mathbf{c}_1 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \wedge \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \gamma \\ -\beta \end{pmatrix} \\
\varphi_w(\mathbf{c}_2) &= w \wedge \mathbf{c}_2 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \wedge \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\gamma \\ 0 \\ \alpha \end{pmatrix} \\
\varphi_w(\mathbf{c}_3) &= w \wedge \mathbf{c}_3 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \wedge \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \beta \\ -\alpha \\ 0 \end{pmatrix},
\end{aligned}$$

donc

$$\text{Mat}_{\mathcal{C}}(\varphi_w) = \begin{pmatrix} 0 & -\gamma & \beta \\ \gamma & 0 & -\alpha \\ -\beta & \alpha & 0 \end{pmatrix} = \alpha U + \beta V + \gamma W.$$

Ainsi, étant donné $A \in A_3(\mathbb{R})$, on a l'équivalence

$$\exists! w \in \mathbb{R}^3 : \text{Mat}_{\mathcal{C}}(\varphi_w) = A \Leftrightarrow \exists! (\alpha, \beta, \gamma) \in \mathbb{R}^3 : A = \alpha U + \beta V + \gamma W,$$

et la deuxième assertion est vraie, précisément car (U, V, W) est une base de $A_3(\mathbb{R})$, comme on l'a montré à la question précédente. La première l'est donc aussi, ce qui conclut.

6(a). La matrice d'une rotation vectorielle de \mathbb{R}^3 est un élément de $\text{SO}_3(\mathbb{R})$. On a donc

$$\begin{aligned}
{}^t(R - R^{-1}) &= {}^t(R - {}^t R) && \text{(car } R \text{ orthogonale)} \\
&= {}^t R - R && \text{(car la transposition est linéaire et involutive)} \\
&= -(R - {}^t R) \\
&= -(R - R^{-1}),
\end{aligned}$$

ce qui montre que $R - R^{-1} \in A_3(\mathbb{R})$.

6(b). Supposons par l'absurde que l'unique vecteur w de \mathbb{R}^3 tel que $R - R^{-1}$ soit la matrice de l'application $u : v \mapsto w \wedge v$ soit le vecteur nul. Autrement dit, on suppose que

$$R - {}^t R = R - R^{-1} = \text{Mat}_{\mathcal{C}}(\varphi_{0_{\mathbb{R}^3}}) = \text{Mat}_{\mathcal{C}}(0_{\mathcal{L}(\mathbb{R}^3)}) = 0_{M_3(\mathbb{R})},$$

c'est-à-dire que R est symétrique.

La matrice R est donc à la fois orthogonale et symétrique, ce qui entraîne que

$${}^tR = R^{-1} = R,$$

ou encore que $R^2 = I$.

(L'énoncé oublie manifestement d'exclure le cas $r = \text{id}_{\mathbb{R}^3}$, rotation d'angle nul. Je rétablis cette hypothèse.)

Comme $R^2 = \text{Mat}_{\mathcal{C}}(r^2)$, on en déduit $r^2 = \text{id}_{\mathbb{R}^3}$. Or, r étant une rotation d'un certain angle $\omega \not\equiv 0 \pmod{\pi}$, r^2 est une rotation d'angle $2\omega \not\equiv 0 \pmod{2\pi}$. En particulier, on ne peut pas avoir $r^2 = \text{id}_{\mathbb{R}^3}$, ce qui nous fournit la contradiction souhaitée.

6(c). On a $\text{Mat}_{\mathcal{C}}(u) = R - R^{-1} = \text{Mat}_{\mathcal{C}}(r - r^{-1})$, par linéarité de $\text{Mat}_{\mathcal{C}} : \mathcal{L}(\mathbb{R}^3) \rightarrow M_3(\mathbb{R})$ et le fait que cette application linéaire préserve les inverses.

Puisqu'il s'agit en outre d'un isomorphisme, on a $u = r - r^{-1}$.

L'égalité $r(v) = v$ permet d'obtenir, en appliquant r^{-1} , $v = r^{-1}(v)$. On a donc

$$\begin{aligned} u(v) &= (r - r^{-1})(v) \\ &= r(v) - r^{-1}(v) \\ &= 0, \end{aligned}$$

ce qui était demandé.

L'axe de r étant par définition $\ker(r - \text{id}_{\mathbb{R}^3})$, ce qui précède s'applique notamment à un vecteur directeur v de l'axe de r . On a donc $u(v) = 0$, c'est-à-dire $w \wedge v = 0_{\mathbb{R}^3}$.

Cela montre que w et v sont colinéaires. Comme ils sont tous les deux non nuls (v , par définition d'un vecteur directeur et w , par la question précédente), on en déduit qu'il existe un réel $\lambda \neq 0$ tel que $w = \lambda v$. En particulier, w est également un vecteur directeur de l'axe de r , ce qui conclut.

6(d)i. Notons $\mathcal{B} = (e_1, e_2, e_3)$. On a alors

$$\text{Mat}_{\mathcal{B}}(r) = \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Comme r^{-1} est la rotation d'axe $\text{Vect}(w)$ et d'angle $-\theta$, on a d'après les propriétés de parité du sinus et du cosinus

$$\text{Mat}_{\mathcal{B}}(r^{-1}) = \begin{pmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

6(d)ii. On a

$$\begin{aligned} \text{Mat}_{\mathcal{B}}(u) &= \text{Mat}_{\mathcal{B}}(r) - \text{Mat}_{\mathcal{B}}(r^{-1}) \\ &= \begin{pmatrix} 0 & -2\sin \theta & 0 \\ 2\sin \theta & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

6(d)iii. Par ailleurs, on a, car la base \mathcal{B} est orthonormée directe

$$\begin{aligned} (2\sin \theta e_3) \wedge e_1 &= 2\sin \theta e_2 \\ (2\sin \theta e_3) \wedge e_2 &= -2\sin \theta e_1 \\ (2\sin \theta e_3) \wedge e_3 &= 0_{\mathbb{R}^3}. \end{aligned}$$

c'est-à-dire que $\text{Mat}_{\mathfrak{B}}(u) = \text{Mat}_{\mathfrak{B}}(\varphi_{2\sin\theta e_3})$, et donc que $\varphi_w = u = \varphi_{2\sin\theta e_3}$. D'après la question 5 (et plus précisément le résultat d'unicité), on en déduit que $w = 2\sin\theta e_3$, c'est-à-dire que $w = \frac{2\sin\theta}{\|w\|}w$.

Comme w est non nul, la famille (w) est libre et on peut tirer de cette égalité l'égalité $\frac{2\sin\theta}{\|w\|} = 1$, et

$$\text{donc } \sin\theta = \frac{1}{2}\|w\| > 0.$$

On a montré à la question 6(b) que la matrice de u dans la base canonique ne pouvait pas être nulle. Puisque la matrice d'un endomorphisme dans une base donnée n'est nulle que si l'endomorphisme est lui-même nul, cela entraîne que $\text{Mat}_{\mathfrak{B}}(u) \neq 0_{M_3(\mathbb{R})}$. Vu ce qui précède, on en déduit directement $\sin\theta \neq 0$.

Par ailleurs, la trace de deux matrices semblables (et donc de deux matrices d'un même endomorphisme dans des bases différentes) étant égales, on a

$$\text{tr}(R) = \text{tr}(\text{Mat}_{\mathcal{C}}(r)) = \text{tr}(\text{Mat}_{\mathfrak{B}}(r)) = 1 + 2\cos\theta,$$

$$\text{donc } \cos\theta = \frac{\text{tr}R - 1}{2}.$$

Comme $\theta \in [0, 2\pi[$ et $\sin\theta > 0$, on a $\theta \in]0, \pi[$, et on a ainsi

$$\begin{aligned} \theta &= \arccos \cos\theta \\ &= \arccos \frac{\text{tr}R - 1}{2}. \end{aligned}$$

6(e) On a

$$\begin{pmatrix} 1 & 1-\sqrt{3} & 1+\sqrt{3} \\ 1+\sqrt{3} & 1 & 1-\sqrt{3} \\ 1-\sqrt{3} & 1+\sqrt{3} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1+\sqrt{3} & 1-\sqrt{3} \\ 1-\sqrt{3} & 1 & 1+\sqrt{3} \\ 1+\sqrt{3} & 1-\sqrt{3} & 1 \end{pmatrix} = 9I,$$

d'où l'on tire $R^t R = I$, c'est-à-dire que $R \in O_3(\mathbb{R})$.

Par ailleurs, on obtient d'après la règle de Sarrus

$$\begin{aligned} \det(3R) &= 1 + (1 + \sqrt{3})^3 + (1 - \sqrt{3})^3 - 3(1 + \sqrt{3})(1 - \sqrt{3}) \\ &= 1 + 2\left((1 + \sqrt{3})^2 - (1 + \sqrt{3})(1 - \sqrt{3}) + (1 - \sqrt{3})^2\right) + 3 \times 2 \\ &= 1 + 2(8 + 2) + 6 \\ &= 27, \\ \text{donc } \det R &= \frac{27}{3^3} = 1, \end{aligned}$$

donc $R \in SO_3(\mathbb{R})$, ce qui entraîne que R est la matrice d'une rotation.

On calcule aisément

$$\begin{aligned} R - R^{-1} &= R - {}^t R \\ &= \frac{1}{3} \begin{pmatrix} 0 & -2\sqrt{3} & 2\sqrt{3} \\ 2\sqrt{3} & 0 & -2\sqrt{3} \\ -2\sqrt{3} & 2\sqrt{3} & 0 \end{pmatrix} \\ &= \frac{2\sqrt{3}}{3} \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}, \end{aligned}$$

qui est la matrice de φ_w dans la base canonique, où $w = \frac{2\sqrt{3}}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. Comme par ailleurs $\text{tr} R = 1$, l'endomorphisme associé à R dans la base canonique est la rotation d'axe la droite orientée dirigée par w (ou son multiple positif $(1, 1, 1)$) et d'angle $\frac{\pi}{2}$.

Partie III

1. Soit $X \in M_{n,1}(\mathbb{R})$. On a ${}^t X B X \in M_1(\mathbb{R})$, donc cette matrice est nécessairement symétrique. Autrement dit, on a

$${}^t X B X = {}^t ({}^t X B X) = {}^t X {}^t B {}^t ({}^t X) = {}^t X {}^t B X.$$

Appliqué à une matrice antisymétrique, cela donne

$${}^t X A X = {}^t X {}^t A X = {}^t X (-A) {}^t X = -{}^t X A X,$$

d'où l'on tire ${}^t X A X = 0$.

2. On a d'une part ${}^t X (A + I) X = {}^t X ((A + I) X) = {}^t X 0_{n,1} = 0$ et de l'autre

$${}^t X (A + I) X = {}^t X A X + {}^t X I X = {}^t X X,$$

grâce à la question précédente et à la bilinéarité du produit matriciel.

On a donc ${}^t X X = 0$, c'est-à-dire $\|X\|^2 = \sum_{k=1}^n X_{k,1}^2 = 0$, où l'on a noté $\|\cdot\|$ la norme euclidienne sur \mathbb{R}^n , identifié à $M_{n,1}(\mathbb{R})$. On en déduit $X = 0_{n,1}$.

3. La question précédente montre exactement que $\ker(A + I) = \{0_{n,1}\}$.
On en déduit $A + I \in GL_n(\mathbb{R})$.
4. On a (en notant notamment que la transposition est linéaire, et que la transposée d'une matrice M inversible est elle-même inversible, avec $({}^t M)^{-1} = {}^t (M^{-1})$, que l'on notera simplement ${}^t M^{-1}$).

$$\begin{aligned} {}^t B B &= {}^t ((I - A)(I + A)^{-1}) ((I - A)(I + A)^{-1}) \\ &= ({}^t I + {}^t A)^{-1} ({}^t I - {}^t A) (I - A) (I + A)^{-1} \\ &= (I - A)^{-1} (I + A) (I - A) (I + A)^{-1} \\ &= (I - A)^{-1} (I - A) (I + A) (I + A)^{-1} && \text{(car } I + A \text{ et } I - A \text{ commutent)} \\ &= I, \end{aligned}$$

ce qui montre que B est orthogonale.

5. On a

$$\begin{aligned} (I + B)(I + A) &= I + A + B(I + A) \\ &= I + A + (I - A)(I + A)^{-1}(I + A) \\ &= I + A + I - A \\ &= 2I, \end{aligned}$$

ce qui montre que $I + B$ est inversible, d'inverse $\frac{1}{2}(I + A)$.

6. On a

$$\begin{aligned} (I + B)C &= I - B && \text{donc } {}^t C {}^t (I + B) = {}^t (I - B) \\ &&& \text{donc } {}^t C (I + B^{-1}) = I - B^{-1} && \text{(car } B \text{ orthogonale)} \end{aligned}$$

$$\begin{aligned} \text{donc } {}^tC + {}^tCB^{-1} &= I - B^{-1} \\ \text{donc } {}^tC &= I - B^{-1} - {}^tCB^{-1}. \end{aligned}$$

On a

$$\begin{aligned} {}^tC &= {}^t(I-B) {}^t((I+B)^{-1}) \\ &= (I-B^{-1})(I+B^{-1})^{-1} && \text{(car B orthogonale)} \\ &= (B-I)B^{-1}((B+I)B^{-1})^{-1} \\ &= (B-I)B^{-1}B(B+I)^{-1} \\ &= -(I-B)(I+B)^{-1} \\ &= -(I+B)^{-1}(I-B) \\ &= -C, \end{aligned}$$

la relation de commutation utilisée à l'avant-dernière ligne provenant du fait que, puisqu'une matrice inversible commute toujours avec son inverse, les matrices $(I+B)^{-1}$ et $I+B$ commutent. Comme $I-B = 2I - (I+B)$ est une combinaison linéaire de I et de $I+B$, elle commute également avec $(I+B)^{-1}$.

Partie IV

1. L'hypothèse $AY = 0$ se traduit en $A^2X = 0$. On a alors

$$\begin{aligned} {}^tYY &= {}^t(AX)AX \\ &= {}^tX(-A)AX \\ &= -{}^tXA^2X \\ &= 0. \end{aligned}$$

2. Montrons d'abord que $\ker f$ et $\text{im } f$ sont en somme directe. Soit $y \in \ker f \cap \text{im } f$. Comme $y \in \text{im } f$, on peut trouver $x \in \mathbb{R}^n$ tel que $y = f(x)$ et $f(y) = 0$. On a donc (en notant encore \mathfrak{C} la base canonique de \mathbb{R}^n)

$$\begin{aligned} \text{Mat}_{\mathfrak{C}}(y) &= \text{Mat}_{\mathfrak{C}}(f(x)) = \text{Mat}_{\mathfrak{C}}(f) \text{Mat}_{\mathfrak{C}}(x) = A \text{Mat}_{\mathfrak{C}}(x) \\ \text{et } 0 &= \text{Mat}_{\mathfrak{C}}(0) = \text{Mat}_{\mathfrak{C}}(f(y)) = \text{Mat}_{\mathfrak{C}}(f) \text{Mat}_{\mathfrak{C}}(x) = A \text{Mat}_{\mathfrak{C}}(x). \end{aligned}$$

On peut donc appliquer la question précédente à $X = \text{Mat}_{\mathfrak{C}}(f)$ et donc à $Y = AX = \text{Mat}_{\mathfrak{C}}(y)$ et l'on obtient ${}^tYY = 0$. Comme à la question III.2, on en déduit $Y = 0$, ce qui entraîne $y = 0$. On a ainsi montré que $\ker f \cap \text{im } f = \{0\}$, c'est-à-dire que ces deux sous-espaces vectoriels sont en somme directe.

Par ailleurs, le théorème du rang appliqué à l'endomorphisme f entraîne que

$$\dim \text{im } f + \dim \ker f = \text{rg } f + \dim \ker f = n,$$

donc les deux espaces sont supplémentaires.

3. Soit $r = \dim \text{im } f$ et $\mathfrak{D} = (\mathfrak{d}_1, \dots, \mathfrak{d}_n)$ une base de \mathbb{R}^n adaptée à la décomposition en somme directe $\mathbb{R}^n = \text{im } f \oplus \ker f$. On a alors une matrice $C \in M_r(\mathbb{R})$ telle que l'on ait la décomposition par blocs

$$\text{Mat}_{\mathfrak{D}}(f) = \begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix}.$$

Comme $\text{im } f$ est un supplémentaire de $\ker f$, le théorème du rang entraîne que f induit un isomorphisme $\varphi : \text{im } f \rightarrow \text{im } f$, c'est-à-dire un automorphisme de $\text{im } f$.

Or, par construction, $(\mathfrak{d}_1, \dots, \mathfrak{d}_r)$ est une base de $\text{im } f$, et on a

$$\text{Mat}_{(\mathfrak{d}_1, \dots, \mathfrak{d}_r)}(\varphi) = C.$$

Ainsi, C est la matrice d'un automorphisme, ce qui montre $C \in \text{GL}_r(\mathbb{R})$.

Les matrices A et $\text{Mat}_{\mathfrak{D}}(f)$ étant deux matrices d'un même endomorphisme dans deux bases, elles sont semblables, ce qui conclut la preuve.

4. Puisque A est à coefficients réels, on a, pour tout $i \in \llbracket 1, n \rrbracket$,

$$\begin{aligned} \overline{(AX)_i} &= \overline{\sum_{k=1}^n A_{i,k} x_k} \\ &= \sum_{k=1}^n \overline{A_{i,k} x_k} && \text{(propriétés de la conjugaison)} \\ &= \sum_{k=1}^n A_{i,k} \overline{x_k}. && \text{(car } A \in M_n(\mathbb{R})) \end{aligned}$$

Avec les notations de l'énoncé, cela montre $\overline{AX} = A\overline{X}$.

On a alors

— d'une part,

$$\begin{aligned} {}^t \overline{X} A X &= {}^t \overline{X} \lambda X \\ &= \lambda {}^t \overline{X} X \\ &= \lambda \sum_{k=1}^n |x_k|^2; \end{aligned}$$

— de l'autre,

$$\begin{aligned} AX &= \lambda X \\ \text{donc } A\overline{X} &= \overline{\lambda X} = \overline{\lambda} \overline{X} && \text{(d'après la discussion précédente)} \\ \text{donc } {}^t \overline{X} A &= {}^t (A\overline{X}) \\ &= -{}^t (A\overline{X}) \\ &= -{}^t (\overline{\lambda} \overline{X}) \\ &= -\overline{\lambda} {}^t \overline{X} \\ \text{donc } {}^t \overline{X} A X &= -\overline{\lambda} ({}^t \overline{X} X) \\ &= -\overline{\lambda} \sum_{k=1}^n |x_k|^2. \end{aligned}$$

Comme X est un vecteur propre, il est non nul. Une somme de réels positifs n'étant nulle que si tous les réels sont nuls, on en déduit $\sum_{k=1}^n |x_k|^2 \neq 0$, donc le calcul précédent entraîne $\lambda = -\overline{\lambda}$, c'est-à-dire

que λ est imaginaire pur.

5. On a, pour tout $\lambda \in \mathbb{C}$,

$$\chi_A(\lambda) = \begin{vmatrix} \lambda I_r - C & 0 \\ 0 & \lambda I_{n-r} \end{vmatrix}.$$

En développant successivement par rapport aux $n - r$ dernières lignes, on obtient

$$\chi_A(\lambda) = \lambda^{n-r} \det(\lambda I_r - C),$$

c'est-à-dire (en passant de la fonction polynomiale au polynôme)

$$\chi_A = X^{n-r} \chi_C.$$

Ainsi, si $\lambda \in \mathbb{C} \setminus \{0\}$, on a la chaîne d'équivalences

$$\begin{aligned} \lambda \in \text{Spec}_{\mathbb{C}}(A) &\Leftrightarrow \chi_A(\lambda) = 0 \\ &\Leftrightarrow \lambda^{n-r} \chi_C(\lambda) = 0 \\ &\Leftrightarrow \chi_C(\lambda) = 0 && (\text{car } \lambda \neq 0) \\ &\Leftrightarrow \lambda \in \text{Spec}_{\mathbb{C}}(C). \end{aligned}$$

6. Toutes les valeurs propres de C sont non nulles, puisque C est inversible. D'après la question 5, les valeurs propres de C sont donc exactement les valeurs propres non nulles de A , ce qui entraîne (d'après la question 4) qu'il s'agit d'imaginaires purs non nuls. En particulier, C n'a pas de valeur propre réelle. Cela entraîne que le polynôme caractéristique χ_C (qui est élément de $\mathbb{R}[X]$, puisque C est une matrice réelle) n'a pas de racine réelle. Comme tout polynôme réel de degré impair a une racine (si P est de degré impair et de coefficient dominant a , on a $P(x) \xrightarrow{x \rightarrow \pm\infty} \pm\infty$ si $a > 0$ et $P(x) \xrightarrow{x \rightarrow \pm\infty} \mp\infty$ si $a < 0$, donc le théorème des valeurs intermédiaires généralisé – que l'on peut appliquer ici car la fonction polynomiale associée à P est continue – entraîne dans les deux cas que la fonction polynomiale associée à P s'annule sur \mathbb{R}), cela entraîne que $\deg \chi_C$ est pair. Comme le degré du polynôme caractéristique d'une matrice carrée est égale à son ordre, cela conclut.

Exercice de probabilités

1. Les variables aléatoires X et Y étant à valeurs dans \mathbb{N} , on doit avoir

$$\begin{aligned} \sum_{(k,\ell) \in \mathbb{N}^2} P(X = k, Y = \ell) = 1 &\quad \text{donc} \quad \sum_{k=0}^{+\infty} \sum_{\ell=0}^{+\infty} \frac{\alpha}{2^{k+\ell}} = 1 \\ &\quad \text{donc} \quad \alpha \sum_{k=0}^{+\infty} 2^{-k} \sum_{\ell=0}^{+\infty} 2^{-\ell} = 1 \\ &\quad \text{donc} \quad 2\alpha \sum_{k=0}^{+\infty} 2^{-k} = 1 \\ &\quad \text{donc} \quad 4\alpha = 1. \end{aligned}$$

Cela montre $\alpha = \frac{1}{4}$.

2. Commençons par déterminer la loi de X . Soit $k \in \mathbb{N}$. La famille $\left((Y = \ell) \right)_{\ell \in \mathbb{N}}$ étant un système complet d'événements, on a, d'après la formule des probabilités totales,

$$\begin{aligned} P(X = k) &= \sum_{\ell=0}^{+\infty} P\left((X = k) \cap (Y = \ell) \right) \\ &= \sum_{\ell=0}^{+\infty} P(X = k, Y = \ell) \end{aligned}$$

$$\begin{aligned}
&= \sum_{\ell=0}^{+\infty} \frac{2^{-k} 2^{-\ell}}{4} \\
&= 2^{-(k+2)} \sum_{\ell=0}^{+\infty} 2^{-\ell} \\
&= 2^{-(k+1)}.
\end{aligned}$$

Autrement dit, $X + 1$ suit la loi géométrique de paramètre $\frac{1}{2}$.

La formule donnant la loi conjointe de X et de Y étant symétrique, il en va de même de Y .
Pour $k, \ell \in \mathbb{N}$, on a

$$\begin{aligned}
P(X = k)P(Y = \ell) &= 2^{-(k+1)}2^{-(\ell+1)} \\
&= 2^{-(k+\ell+2)} \\
&= \frac{\alpha}{2^{k+\ell}} \\
&= P(X = k, Y = \ell),
\end{aligned}$$

ce qui montre que les variables aléatoires X et Y sont indépendantes.

3. On sait que la série entière $\sum_{k \geq 0} x^k$ est de rayon de convergence 1, et de somme $x \mapsto \frac{1}{1-x}$.

D'après, le théorème de dérivation des séries entières, on en déduit que les séries entières $\sum_{k \geq 1} k x^{k-1}$

et $\sum_{k \geq 2} k(k-1)x^{k-2}$ sont de rayon de convergence ≥ 1 , de sommes respectives

$$\begin{aligned}
\left(x \mapsto \frac{1}{1-x}\right)' &= \left(x \mapsto \frac{1}{(1-x)^2}\right) \\
\text{et } \left(x \mapsto \frac{1}{1-x}\right)'' &= \left(x \mapsto \frac{2}{(1-x)^3}\right).
\end{aligned}$$

4. Plutôt que d'utiliser les formules précédentes, on va utiliser le cours. On a vu à la question 2. que la variable aléatoire $X + 1$ suit la loi géométrique de paramètre $\frac{1}{2}$. On en déduit que $\mathbb{E}(X + 1) = 2$ et

$$\text{var}(X + 1) = \frac{1 - \frac{1}{2}}{\left(\frac{1}{2}\right)^2} = 2.$$

Ainsi,

$$\mathbb{E}X = \mathbb{E}(X + 1) - \mathbb{E}1 \quad (\text{linéarité de l'espérance})$$

$$= 1$$

$$\text{et } \text{var}(X) = \text{var}(X + 1) \quad (\text{variance et reparamétrage affine})$$

$$= 2.$$

Par ailleurs, toujours grâce à la question 2., on sait que X et Y sont indépendantes, donc

$$\text{cov}(X, Y) = 0.$$

5. Soit $n \in \mathbb{N}$. On a $(X \geq n) = \bigsqcup_{k=n}^{+\infty} (X = k)$ donc, par additivité,

$$\begin{aligned}
P(X \geq n) &= \sum_{k=n}^{+\infty} P(X = k) \\
&= \sum_{k=n}^{+\infty} 2^{-(k+1)} \\
&= 2^{-n}.
\end{aligned}$$

Naturellement, par symétrie, la même chose est vraie pour Y.

6. Minimum de deux variables aléatoires à valeurs dans \mathbb{N} , la variable aléatoire Z est à valeurs dans \mathbb{N} . Soit $n \in \mathbb{N}$. On a l'égalité d'événements

$$(Z \geq n) = (\min(X, Y) \geq n) = (X \geq n \text{ et } Y \geq n) = (X \geq n) \cap (Y \geq n),$$

donc

$$\begin{aligned}
P(Z \geq n) &= P((X \geq n) \cap (Y \geq n)) \\
&= P(X \geq n)P(Y \geq n) && \text{(par indépendance de X et Y)} \\
&= 2^{-n} 2^{-n} \\
&= 4^{-n}.
\end{aligned}$$

Par ailleurs, on a l'égalité d'événements

$$(Z \geq n) = (Z = n) \sqcup (Z \geq n + 1)$$

donc, par additivité,

$$\begin{aligned}
P(Z \geq n) = P(Z = n) + P(Z \geq n + 1) \quad \text{donc} \quad P(Z = n) &= P(Z \geq n) - P(Z \geq n + 1) \\
&= 4^{-n} - 4^{-(n+1)} \\
&= \frac{3}{4} \left(\frac{1}{4}\right)^n \\
&= 3 \times 2^{-(2n+2)}.
\end{aligned}$$

Ainsi, $Z + 1$ suit la loi géométrique de paramètre $\frac{3}{4}$.

7. Effectuons les trois calculs successivement.

— On a l'égalité d'événements $(X = Y) = \bigsqcup_{k=0}^{+\infty} (X = k, Y = k)$, donc, par additivité

$$\begin{aligned}
P(X = Y) &= \sum_{k=0}^{+\infty} P(X = k, Y = k) \\
&= \sum_{k=0}^{+\infty} 2^{-(2k+2)} \\
&= \sum_{k=0}^{+\infty} 4^{-(k+1)} \\
&= \frac{1}{3}.
\end{aligned}$$

— On a l'égalité d'événements $(X < Y) = \bigsqcup_{k=0}^{+\infty} (X = k, Y > k) = \bigsqcup_{k=0}^{+\infty} (X = k, Y \geq k + 1)$, donc, par additivité

$$\begin{aligned} P(X < Y) &= \sum_{k=0}^{+\infty} P(X = k, Y \geq k + 1) \\ &= \sum_{k=0}^{+\infty} P(X = k)P(Y \geq k + 1) && \text{(X et Y indépendantes)} \\ &= \sum_{k=0}^{+\infty} 2^{-(k+1)} 2^{-(k+1)} && \text{(questions 2. et 5.)} \\ &= \sum_{k=0}^{+\infty} 4^{-(k+1)} \\ &= \frac{1}{3}. \end{aligned}$$

— Distinguons deux cas :

- Si $r = 0$, on a l'égalité d'événements $(X = rY) = (X = 0)$, donc

$$\begin{aligned} P(X = rY) &= P(X = 0) \\ &= \frac{1}{2}. \end{aligned}$$

- Si $r > 0$, on peut trouver $a, b > 0$ premiers entre eux tels que $r = \frac{a}{b}$. On a alors l'égalité

$$\left\{ (n, d) \in \mathbb{N}^* \times \mathbb{N}^* \mid \frac{n}{d} = \frac{a}{b} \right\} = \{(ka, kb) \mid k \in \mathbb{N}^*\}.$$

En effet, l'inclusion réciproque est triviale.

Montrons l'inclusion directe. Soit $(n, d) \in \mathbb{N}^* \times \mathbb{N}^*$ tels que $\frac{n}{d} = \frac{a}{b}$. On peut réécrire cette égalité sous la forme $bn = ad$. Si l'on note $m = bn = ad$, ce nombre est à la fois multiple de a et de b , donc 2 de ab . On peut trouver $k \in \mathbb{N}$ tel que $m = kab$. Comme $m \neq 0, k \neq 0$, et l'on a

$$(n, d) = \left(\frac{m}{b}, \frac{m}{a} \right) = (ka, kb),$$

2. D'une manière ou d'une autre, il va falloir utiliser un résultat plus ou moins équivalent au lemme de Gauss, ce qui soulève le problème de la pertinence de cette question dans la filière PT. J'ai choisi d'utiliser le résultat suivant : si a et b sont premiers entre eux, tout multiple m commun à a et b est un multiple de ab . Quoique ce ne soit pas mathématiquement très pertinent, on peut montrer ce résultat à **partir** de l'existence et l'unicité de la décomposition en facteurs premiers, admise en PT. Voici par exemple une démonstration.

Soit m un multiple commun de a et b .

Écrivons les décompositions en facteurs premiers de a et b : on peut trouver des nombres premiers p_1, \dots, p_r et q_1, \dots, q_s , et des exposants $\mu_1, \dots, \mu_r, \nu_1, \dots, \nu_s > 0$ tels que $a = \prod_{i=1}^r p_i^{\mu_i}$ et $b = \prod_{j=1}^s q_j^{\nu_j}$. Comme a et b sont premiers entre eux,

aucun nombre premier ne divise simultanément a et b , donc $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset$.

Comme m est un multiple de a , on peut donc trouver $m' \in \mathbb{N}^*$ tel que $m = am'$.

On peut décomposer m' en facteurs premiers, en distinguant les premiers intervenant dans les décompositions précédentes et les « nouveaux » : on peut trouver ℓ_1, \dots, ℓ_t premiers et des exposants $\tilde{\alpha}_1, \dots, \tilde{\alpha}_r, \beta_1, \dots, \beta_s \geq 0$ et $\gamma_1, \dots, \gamma_t > 0$

tels que $m' = \prod_{i=1}^r p_i^{\tilde{\alpha}_i} \times \prod_{j=1}^s q_j^{\beta_j} \times \prod_{k=1}^t \ell_k^{\gamma_k}$. On en déduit $m = \prod_{i=1}^r p_i^{\alpha_i} \times \prod_{j=1}^s q_j^{\beta_j} \times \prod_{k=1}^t \ell_k^{\gamma_k}$, où l'on a posé, pour tout

$i \in \llbracket 1, r \rrbracket, \alpha_i = \tilde{\alpha}_i + \mu_i$.

Autrement dit, dans la décomposition en facteurs premiers de m , l'exposant α_i du nombre premier p_i est $\geq \mu_i$. Par

On a alors l'égalité d'événements $(X = rY) = \bigsqcup_{t=0}^{+\infty} (X = ka, Y = kb)$, donc, par additivité,

$$\begin{aligned} P(X = rY) &= \sum_{t=0}^{+\infty} P(X = ka, Y = kb) \\ &= \sum_{t=0}^{+\infty} 2^{-(ka+kb+2)} \\ &= \frac{1}{4} \sum_{t=0}^{+\infty} (2^{-(a+b)})^t \\ &= \frac{1}{4} \frac{1}{1 - 2^{-(a+b)}}. \end{aligned}$$

8. X et Y prenant leurs valeurs dans \mathbb{N} , la différence T prend ses valeurs dans \mathbb{Z} .

Le couple (Z, T) prend donc ses valeurs dans $\mathbb{N} \times \mathbb{Z}$.

Soit $(n, d) \in \mathbb{N} \times \mathbb{Z}$.

Notons Ω le domaine des variables aléatoires de l'exercice. On a, pour tout $\omega \in \Omega$, la chaîne d'équivalences

$$T(\omega) \geq 0 \Leftrightarrow X(\omega) \geq Y(\omega) \Leftrightarrow Z(\omega) = Y(\omega).$$

Ainsi, si $d \geq 0$,

$$\begin{aligned} (T(\omega) = d \text{ et } Z(\omega) = n) &\Leftrightarrow (X(\omega) - Y(\omega) = d \text{ et } Y(\omega) = n) \\ &\Leftrightarrow (X(\omega) = d + n \text{ et } Y(\omega) = n), \end{aligned}$$

et on peut faire le même genre de raisonnements dans le cas $d \leq 0$.

On va donc distinguer deux cas :

- Si $d \geq 0$, on a l'égalité d'événements

$$\begin{aligned} ((Z, T) = (n, d)) &= (Z = n, T = d) \\ &= (X = d + n, Y = n), \end{aligned}$$

donc

$$\begin{aligned} P((Z, T) = (n, d)) &= P(X = d + n, Y = n) \\ &= 2^{-(2n+d+2)}. \end{aligned}$$

- Si $d \leq 0$, par le même genre de raisonnement,

$$\begin{aligned} P((Z, T) = (n, d)) &= P(X = n, Y = n - d) \\ &= 2^{-(2n-d+2)} \end{aligned}$$

symétrie, on montre de la même façon que l'exposant β_j du nombre premier q_j est $\geq \nu_j$.

Ainsi, $m = \prod_{i=1}^r p_i^{\alpha_i} \times \prod_{j=1}^s q_j^{\beta_j} \times \prod_{k=1}^t \ell_k^{\gamma_k} = \underbrace{\prod_{i=1}^r p_i^{\mu_i}}_{=a} \times \underbrace{\prod_{j=1}^s q_j^{\nu_j}}_{=b} \times \underbrace{\prod_{i=1}^r p_i^{\alpha_i - \mu_i} \times \prod_{j=1}^s q_j^{\beta_j - \nu_j} \times \prod_{k=1}^t \ell_k^{\gamma_k}}_{\in \mathbb{N}^*}$, ce qui montre que m est

multiple de ab .

(Notons que dans le cas $d = 0$, les deux raisonnements sont valides et donnent le même résultat).
On a donc

$$\forall (n, d) \in \mathbb{N} \times \mathbb{Z}, P((Z, T) = (n, d)) = 2^{-(2n+|d|+2)}.$$

Avant de déterminer si Z et T sont indépendantes, on va déterminer la loi de T .

Soit $d \in \mathbb{Z}$. On a l'égalité d'événements $(T = d) = \bigsqcup_{n \in \mathbb{N}} (Z = n, T = d)$ donc, par additivité,

$$\begin{aligned} P(T = d) &= \sum_{n=0}^{+\infty} P(Z = n, T = d) \\ &= \sum_{n=0}^{+\infty} 2^{-(2n+|d|+2)} \\ &= 2^{-|d|} \sum_{n=0}^{+\infty} 2^{-(2n+2)} \\ &= \frac{2^{-|d|}}{3}. \end{aligned}$$

On a donc bien, pour tous $n \in \mathbb{N}$ et $d \in \mathbb{Z}$, $P(Z = n, T = d) = P(Z = n)P(T = d)$, ce qui montre que Z et T sont indépendantes.

9. Soit $k, \ell \in \mathbb{N}$. Remarquons que $P(X = k) = 2^{-(k+1)} > 0$. On a l'égalité d'événements

$$(Z = \ell, X = k) = \begin{cases} (X = k, Y = \ell) & \text{si } \ell < k \\ (X = k, Y \geq k) & \text{si } \ell = k \\ \emptyset & \text{si } \ell > k \end{cases}$$

$$\text{donc } P(Z = \ell, X = k) = \begin{cases} P(X = k)P(Y = \ell) & \text{si } \ell < k \\ P(X = k)P(Y \geq k) & \text{si } \ell = k \\ 0 & \text{si } \ell > k \end{cases} \quad (\text{car } X \text{ et } Y \text{ indépendantes})$$

$$\begin{aligned} \text{donc } P(Z = \ell | X = k) &= \frac{P(Z = \ell, X = k)}{P(X = k)} \\ &= \begin{cases} P(Y = \ell) & \text{si } \ell < k \\ P(Y \geq k) & \text{si } \ell = k \\ 0 & \text{si } \ell > k \end{cases} \\ &= \begin{cases} 2^{-(\ell+1)} & \text{si } \ell < k \\ 2^{-k} & \text{si } \ell = k \\ 0 & \text{si } \ell > k \end{cases} \end{aligned}$$

d'après les questions 2. et 5.