

Séance à distance – Corrigé

Réduction (1) : exemples d'introduction et polynômes d'endomorphismes

Rappels utilisés tout au long du corrigé

Trois outils

Changement de base. Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de E , P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ (colonnes : coordonnées des vecteurs de $\mathcal{B}'$ dans $\mathcal{B}$), $A = \text{Mat}_{\mathcal{B}}(u)$ et $D = \text{Mat}_{\mathcal{B}'}(u)$, alors $D = P^{-1}AP$, c'est-à-dire $A = PDP^{-1}$.

Même endomorphisme, deux bases. Si $A = \text{Mat}_{\mathcal{B}}(u)$ et $D = \text{Mat}_{\mathcal{B}'}(u)$, alors A^k et D^k sont les matrices de u^k dans $\mathcal{B}$ et $\mathcal{B}'$, et plus généralement $Q(A)$ et $Q(D)$ sont les matrices de $Q(u)$ (proposition 7.11). En particulier $A^k = PD^kP^{-1}$ (récurrence : exercice 1, question 6(a)) et $Q(A) = 0 \iff Q(u) = 0 \iff Q(D) = 0$.

Reste de X^k modulo un annulateur. Ce n'est pas un théorème du cours mais une *méthode* : elle est rédigée à chaque utilisation (exercices 10, 11, 12, 15), en trois temps : division euclidienne de X^k par $P \neq 0$, évaluation aux racines (dérivation si racine double), puis $A^k = Q_k(A)P(A) + R_k(A) = R_k(A)$.

1 Deux exemples pour comprendre ce qu'est la réduction

Exercice 1 – guidé, pour tous : une matrice de taille 2.

1. Par définition de la matrice d'un endomorphisme dans la base canonique, les coordonnées de $f(x, y)$ sont données par

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}, \quad \text{donc} \quad \boxed{f(x, y) = (y, x)}.$$

f échange les deux coordonnées.

2. La famille (e_1, e_2) compte deux vecteurs dans $\mathbb{R}^2$, qui est de dimension 2 : il suffit de montrer qu'elle est libre. Le déterminant de la famille dans la base canonique vaut

$$\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = 1 \cdot (-1) - 1 \cdot 1 = -2 \neq 0,$$

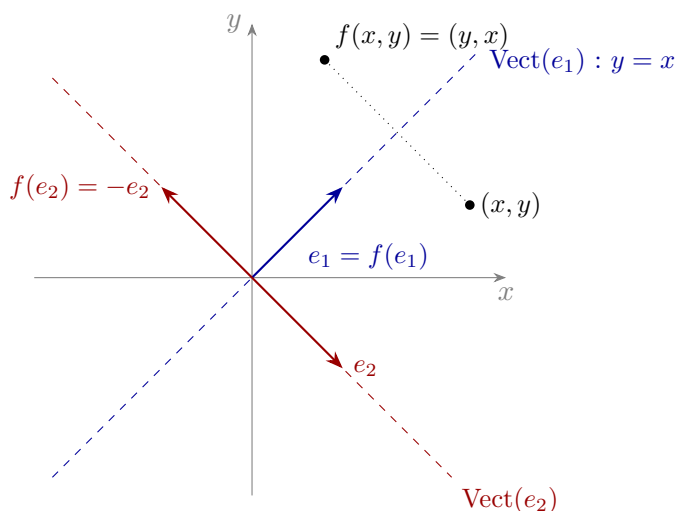
donc (e_1, e_2) est libre, et $\mathcal{B}' = (e_1, e_2)$ **est une base de $\mathbb{R}^2$** . (On peut aussi dire : e_1 et e_2 ne sont pas colinéaires.)

3. D'après la question 1 : $f(e_1) = f(1, 1) = (1, 1) = e_1$ et $f(e_2) = f(1, -1) = (-1, 1) = -e_2$. Ainsi

$$f(e_1) = 1 \cdot e_1 + 0 \cdot e_2, \quad f(e_2) = 0 \cdot e_1 + (-1) \cdot e_2, \quad \text{d'où} \quad \boxed{D = \text{Mat}_{\mathcal{B}'}(f) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}.$$

Les colonnes de D sont les coordonnées de $f(e_1)$ et $f(e_2)$ dans la base $\mathcal{B}'$.

4. Tout vecteur de $\text{Vect}(e_1)$ s'écrit te_1 et $f(te_1) = tf(e_1) = te_1 : f$ **fixe chaque vecteur de la droite** $\text{Vect}(e_1)$ (c'est la première bissectrice $y = x$). Tout vecteur de $\text{Vect}(e_2)$ s'écrit te_2 et $f(te_2) = -te_2 : f$ **change en son opposé chaque vecteur de** $\text{Vect}(e_2)$ (la droite $y = -x$). Comme $\mathbb{R}^2 = \text{Vect}(e_1) \oplus \text{Vect}(e_2)$ (c'est une base), f est la **symétrie par rapport à la droite** $\text{Vect}(e_1)$, **parallèlement à** $\text{Vect}(e_2)$. Comme $e_1 \perp e_2$, c'est même la symétrie orthogonale (réflexion) d'axe la première bissectrice : géométriquement, échanger x et y revient bien à réfléchir le plan par rapport à la droite $y = x$.



5. La matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ a pour colonnes les coordonnées de e_1, e_2 dans $\mathcal{B}$:

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Par la formule de l'inverse d'une matrice de taille 2 (avec $\det P = -2$) :

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

(Vérification : $P^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2I_2$, donc $P \cdot \frac{1}{2}P = I_2$.)

Calculons PDP^{-1} :

$$PD = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad PDP^{-1} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = A.$$

On a bien $\boxed{A = PDP^{-1}}$, conformément à la formule de changement de base $D = P^{-1}AP$.

6. (a) Montrons par récurrence sur $k \in \mathbb{N}$ la propriété $\mathcal{H}_k$: « $A^k = PD^kP^{-1}$ ».

Initialisation. $A^0 = I_2$ et $PD^0P^{-1} = PP^{-1} = I_2$: $\mathcal{H}_0$ est vraie.

Hérédité. Supposons $\mathcal{H}_k$ vraie. Alors

$$A^{k+1} = A \cdot A^k = (PDP^{-1})(PD^kP^{-1}) = PD \underbrace{(P^{-1}P)}_{=I_2} D^k P^{-1} = PD^{k+1}P^{-1},$$

ce qui est $\mathcal{H}_{k+1}$. **Conclusion :** $A^k = PD^kP^{-1}$ pour tout $k \in \mathbb{N}$.

Les simplifications viennent du produit $P^{-1}P = I_2$ qui apparaît *entre* deux facteurs consécutifs : dans $A^k = (PDP^{-1})(PDP^{-1}) \dots (PDP^{-1})$, tous les $P^{-1}P$ intérieurs disparaissent et il ne reste que le P de gauche, les k facteurs D et le P^{-1} de droite.

- (b) Une matrice diagonale s'élève à la puissance k coefficient par coefficient : $D^k = \begin{pmatrix} 1 & 0 \\ 0 & (-1)^k \end{pmatrix}$.

Donc

$$\begin{aligned} A^k &= PD^kP^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-1)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & (-1)^k \\ 1 & -(-1)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 + (-1)^k & 1 - (-1)^k \\ 1 - (-1)^k & 1 + (-1)^k \end{pmatrix}. \end{aligned}$$

Ainsi : si k est pair, $A^k = I_2$; si k est impair, $A^k = A$.

- (c) Directement : $A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. Donc $A^{2m} = (A^2)^m = I_2$ et $A^{2m+1} = A^{2m}A = A$: on retrouve le résultat.

C'était prévisible : f est une symétrie, et une symétrie est une involution ($f \circ f = \text{Id}$), donc $A^2 = I_2$. Appliquer deux fois une réflexion ramène chaque point à sa place.

Exercice 2 – ★ même méthode, en autonomie.

1. $g(x, y) = (x + 2y, 2x + y)$, donc

$$g(e_1) = g(1, 1) = (3, 3) = 3e_1, \quad g(e_2) = g(1, -1) = (-1, 1) = -e_2.$$

Dans la base $\mathcal{B}' = (e_1, e_2)$, la matrice de g est donc diagonale :

$$D = \text{Mat}_{\mathcal{B}'}(g) = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}.$$

Par la formule de changement de base, $D = P^{-1}AP$ avec la même matrice de passage P qu'à l'exercice 1, donc $A = PDP^{-1}$ avec $D = \text{diag}(3, -1)$.

2. Le raisonnement par récurrence de l'exercice 1 ne dépend pas de D : $A^k = PD^kP^{-1}$ pour tout $k \in \mathbb{N}$, avec $D^k = \text{diag}(3^k, (-1)^k)$. Donc

$$\begin{aligned} A^k &= \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3^k & 0 \\ 0 & (-1)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 3^k & (-1)^k \\ 3^k & -(-1)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 3^k + (-1)^k & 3^k - (-1)^k \\ 3^k - (-1)^k & 3^k + (-1)^k \end{pmatrix}. \end{aligned}$$

Vérification. $k = 0$: $\frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I_2$; $k = 1$: $\frac{1}{2} \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} = A$.

Exercice 3 – guidé, pour tous : une matrice de taille 3.

1. Les colonnes de Q sont les coordonnées de e_1, e_2, e_3 dans la base canonique :

$$Q = \begin{pmatrix} 1 & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \\ 1 & 0 & \frac{\sqrt{2}}{2} \end{pmatrix}.$$

En développant selon la deuxième ligne (un seul coefficient non nul, en position (2, 2), de signe +) :

$$\det Q = 1 \cdot \begin{vmatrix} 1 & -\frac{\sqrt{2}}{2} \\ 1 & \frac{\sqrt{2}}{2} \end{vmatrix} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} = \sqrt{2} \neq 0.$$

La famille (e_1, e_2, e_3) est donc libre ; comme elle a 3 vecteurs dans $\mathbb{R}^3$, $\mathcal{B}' = (e_1, e_2, e_3)$ est une base de $\mathbb{R}^3$.

2. On calcule les produits $B e_i$ (vecteurs écrits en colonnes) :

$$\begin{aligned} B \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &= \frac{1}{2} \begin{pmatrix} 1+1 \\ \sqrt{2}-\sqrt{2} \\ 1+1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = e_1, \\ B \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} &= \frac{1}{2} \begin{pmatrix} -\sqrt{2} \\ 0 \\ \sqrt{2} \end{pmatrix} = \begin{pmatrix} -\frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix} = e_3, \\ B \begin{pmatrix} -\frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix} &= \frac{1}{2} \begin{pmatrix} -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}\cdot\sqrt{2}}{2} - \frac{\sqrt{2}\cdot\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ -2 \\ 0 \end{pmatrix} = -e_2. \end{aligned}$$

Donc $g(e_1) = e_1$, $g(e_2) = e_3$, $g(e_3) = -e_2$, et, en mettant en colonnes les coordonnées dans $\mathcal{B}'$:

$$R = \text{Mat}_{\mathcal{B}'}(g) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

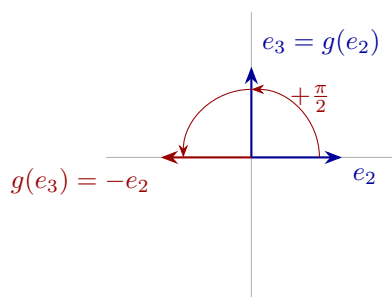
Q est la matrice de passage de la base canonique à $\mathcal{B}'$, donc la formule de changement de base donne $R = Q^{-1}BQ$, soit $B = QRQ^{-1}$.

3. Sur $\text{Vect}(e_1)$. $g(te_1) = te_1$: g **fixe chaque vecteur de la droite** $\text{Vect}(e_1)$.

Sur Π . Soit $y = \alpha e_2 + \beta e_3 \in \Pi$. Par linéarité, $g(y) = \alpha g(e_2) + \beta g(e_3) = \alpha e_3 - \beta e_2 \in \Pi$: **le plan Π est stable par g** . Dans la base (e_2, e_3) de Π , l'endomorphisme induit a pour matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

qui est la matrice de la rotation d'angle $\frac{\pi}{2}$: g **agit sur Π comme un quart de tour** ($e_2 \mapsto e_3 \mapsto -e_2 \mapsto -e_3 \mapsto e_2$).



Le plan $\Pi = \text{Vect}(e_2, e_3)$ vu de dessus (depuis e_1).

Interprétation complète. On remarque que $e_1 \perp e_2$, $e_1 \perp e_3$, $e_2 \perp e_3$ et $\|e_2\| = \|e_3\| = 1$: g est la **rotation d'axe** $\text{Vect}(e_1)$ **et d'angle** $\frac{\pi}{2}$. On comprend maintenant la lettre R et le titre de l'exercice.

4. Par blocs, $R = \begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}$ avec $\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, et $\rho^2 = -I_2$, $\rho^4 = I_2$. Donc

$$R^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad R^4 = (R^2)^2 = I_3.$$

B^4 et R^4 sont les matrices du même endomorphisme $g^4 = g \circ g \circ g \circ g$, dans la base canonique et dans B' respectivement (la matrice d'une composée est le produit des matrices). Or $R^4 = I_3$ signifie $g^4 = \text{Id}$, dont la matrice dans la base canonique est I_3 :

$$\boxed{B^4 = I_3}.$$

(On peut aussi écrire $B^4 = QR^4Q^{-1} = QQ^{-1} = I_3$ par la récurrence de l'exercice 1, question 6(a).)

L'égalité $B \cdot B^3 = I_3$ (avec $B^3 \in \mathcal{M}_3(\mathbb{R})$) montre que B est **inversible** et $B^{-1} = B^3$. (Géométriquement : l'inverse d'un quart de tour est trois quarts de tour.)

5. Soit $k \in \mathbb{N}$ et $k = 4q + r$ sa division euclidienne par 4 ($q \in \mathbb{N}$, $r \in \{0, 1, 2, 3\}$). Alors

$$B^k = B^{4q}B^r = (B^4)^qB^r = I_3^qB^r = B^r : \quad \boxed{B^k = B^r \text{ où } r \text{ est le reste de } k \text{ modulo } 4}.$$

Comme $2026 = 4 \times 506 + 2$, $B^{2026} = B^2$. Calculons $B^2 = \frac{1}{4}M^2$ avec $M = \begin{pmatrix} 1 & -\sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & \sqrt{2} & 1 \end{pmatrix}$:

$$M^2 = \begin{pmatrix} 1-2+1 & -\sqrt{2}+0+\sqrt{2} & 1+2+1 \\ \sqrt{2}+0-\sqrt{2} & -2+0-2 & \sqrt{2}+0-\sqrt{2} \\ 1+2+1 & -\sqrt{2}+0+\sqrt{2} & 1-2+1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 4 \\ 0 & -4 & 0 \\ 4 & 0 & 0 \end{pmatrix},$$

donc

$$\boxed{B^{2026} = B^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}.$$

Contrôle : $B^2e_1 = (1, 0, 1) = e_1$ et $B^2e_2 = -e_2$, conformément à R^2 (un demi-tour autour de $\text{Vect}(e_1)$).

6. (a) Soit $y = \alpha e_2 + \beta e_3 \in \Pi$. On a vu que $g(y) = -\beta e_2 + \alpha e_3$, donc

$$g(g(y)) = -\beta g(e_2) + \alpha g(e_3) = -\beta e_3 - \alpha e_2 = -y.$$

(C'est le bloc $\rho^2 = -I_2$: deux quarts de tour font un demi-tour.)

(b) Soient $y \in \Pi$ et $\lambda \in \mathbb{R}$ tels que $g(y) = \lambda y$. En appliquant g (linéaire) : $g(g(y)) = \lambda g(y) = \lambda^2 y$. D'après (a), $g(g(y)) = -y$, d'où $\lambda^2 y = -y$, soit $(\lambda^2 + 1)y = 0$. Or $\lambda^2 + 1 \geq 1 > 0$ car λ est réel ; donc $y = 0$.

Autrement dit : aucun vecteur non nul de Π n'est envoyé sur un multiple de lui-même, ce qui est bien l'intuition d'un quart de tour.

(c) Supposons qu'il existe une base (v_1, v_2, v_3) de $\mathbb{R}^3$ dans laquelle la matrice de g est diagonale, $\text{diag}(\lambda_1, \lambda_2, \lambda_3)$. Cela signifie $g(v_i) = \lambda_i v_i$ pour $i = 1, 2, 3$: chaque droite $\text{Vect}(v_i)$ est stable par g . D'après le bonus, la seule droite stable est $\text{Vect}(e_1)$, donc $v_1, v_2, v_3 \in \text{Vect}(e_1)$, et trois vecteurs d'une même droite ne peuvent pas former une famille libre de $\mathbb{R}^3$: contradiction. **La matrice de g n'est diagonale dans aucune base de $\mathbb{R}^3$.**

Moralité : on ne peut pas toujours « diagonaliser » ; la forme R (un 1 et un bloc de rotation) est ici la forme la plus simple possible sur $\mathbb{R}$.

Bonus **. Comme (e_1, e_2, e_3) est une base, $\mathbb{R}^3 = \text{Vect}(e_1) \oplus \Pi$: tout $x \in \mathbb{R}^3$ s'écrit de façon unique $x = ae_1 + y$ avec $a \in \mathbb{R}$ et $y \in \Pi$.

Soit $x \neq 0$ tel que la droite $\text{Vect}(x)$ soit stable par g . Alors $g(x) \in \text{Vect}(x)$: il existe $\lambda \in \mathbb{R}$ tel que $g(x) = \lambda x$. Écrivons $x = ae_1 + y$; puisque $g(e_1) = e_1$ et $g(y) \in \Pi$,

$$g(x) = ae_1 + g(y) \quad \text{et} \quad \lambda x = \lambda ae_1 + \lambda y.$$

Par unicité de la décomposition dans $\text{Vect}(e_1) \oplus \Pi$, l'égalité $g(x) = \lambda x$ équivaut à

$$a = \lambda a \quad \text{et} \quad g(y) = \lambda y.$$

La seconde égalité donne $y = 0$ par la question 6(b). Donc $x = ae_1$ avec $a \neq 0$ (car $x \neq 0$), et $\text{Vect}(x) = \text{Vect}(e_1)$ (la première égalité donne d'ailleurs $\lambda = 1$). Réciproquement, $\text{Vect}(e_1)$ est bien stable ($g(e_1) = e_1$). **La seule droite stable par g est $\text{Vect}(e_1)$, l'axe de la rotation.**

Remarque

Sur $\mathbb{C}$, l'équation $\lambda^2 + 1 = 0$ a des solutions $(\pm i)$ et le raisonnement de 6(b) tombe : la matrice B , vue dans $\mathcal{M}_3(\mathbb{C})$, est diagonalisable, avec les « valeurs propres » $1, i, -i$. Le corps de base compte dans les questions de réduction.

2 Polynômes d'endomorphismes et de matrices

2.1 Définition

Exercice 4 – ★ calculs de base.

1. Pour $P = 2X + 3$: $P(A) = 2A + 3I_2 = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix} + \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 6 & 11 \end{pmatrix}$. (Le 3 devient $3I_2$: il ne s'ajoute qu'à la diagonale.)

Pour $P = X^2 - 5X - 2$: $A^2 = \begin{pmatrix} 1+6 & 2+8 \\ 3+12 & 6+16 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$, puis

$$P(A) = A^2 - 5A - 2I_2 = \begin{pmatrix} 7-5-2 & 10-10 \\ 15-15 & 22-20-2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

On remarque que $P(A) = 0_2$: $X^2 - 5X - 2$ est un polynôme annulateur de A . Ce n'est pas un hasard : $5 = \text{tr } A$ et $-2 = \det A$ (exercice 9).

2. Pour une matrice diagonale, $D^k = \text{diag}(\lambda_1^k, \lambda_2^k, \lambda_3^k)$ pour tout $k \in \mathbb{N}$ (récurrence immédiate : le produit de deux matrices diagonales se fait coefficient par coefficient ; pour $k = 0$ on obtient I_3). Si $P = \sum_{k=0}^d a_k X^k$, alors, par linéarité,

$$\begin{aligned} P(D) &= \sum_{k=0}^d a_k D^k = \sum_{k=0}^d a_k \text{diag}(\lambda_1^k, \lambda_2^k, \lambda_3^k) = \text{diag}\left(\sum_k a_k \lambda_1^k, \sum_k a_k \lambda_2^k, \sum_k a_k \lambda_3^k\right) \\ &= \text{diag}(P(\lambda_1), P(\lambda_2), P(\lambda_3)). \end{aligned}$$

Pour $D = \text{diag}(1, 2, 1)$ et $P = X^2 - 3X + 2 = (X - 1)(X - 2)$: $P(1) = 0$ et $P(2) = 0$, donc $P(D) = 0_3$ sans aucun calcul matriciel.

3. $u^2(x, y) = u(u(x, y)) = u(2x - y, x) = (2(2x - y) - x, 2x - y) = (3x - 2y, 2x - y)$.
Pour $P = X^2 - 1$, $P(u) = u^2 - \text{Id}$, donc

$$P(u)(x, y) = u^2(x, y) - (x, y) = (3x - 2y - x, 2x - y - y) = \boxed{(2x - 2y, 2x - 2y)}.$$

4. $P(d) = d^2 - d$, donc pour $Q \in \mathbb{R}_3[X]$: $P(d)(Q) = d^2(Q) - d(Q) = \boxed{Q'' - Q'}$.

Pour $Q = X^3$: $Q' = 3X^2$, $Q'' = 6X$, donc $P(d)(X^3) = 6X - 3X^2$.

Enfin $d^4(Q) = Q''''$; comme $\deg Q \leq 3$, chaque dérivation baisse le degré d'au moins 1 (ou annule) et $Q'''' = 0$. Donc $d^4 = 0_{\mathcal{L}(E)}$: X^4 est un polynôme annulateur de d . (Et $d^3 \neq 0$ car $d^3(X^3) = 6$.)

Exercice 5 – ★ vrai ou faux.

1. **Vrai.** Écrivons $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$ (sommes finies, en complétant par des 0). Alors $P + \lambda Q = \sum_k (a_k + \lambda b_k) X^k$ et

$$(P + \lambda Q)(u) = \sum_k (a_k + \lambda b_k) u^k = \sum_k a_k u^k + \lambda \sum_k b_k u^k = P(u) + \lambda Q(u).$$

L'application $P \mapsto P(u)$ est **linéaire** de $\mathbb{K}[X]$ dans $\mathcal{L}(E)$.

2. **Faux.** Avec $P = X^2$: $P(u + v) = (u + v) \circ (u + v) = u^2 + u \circ v + v \circ u + v^2$, qui n'a aucune raison d'être $u^2 + v^2$. Contre-exemple concret : $E \neq \{0\}$, $u = v = \text{Id}$: $P(u + v) = (2\text{Id})^2 = 4\text{Id}$ alors que $P(u) + P(v) = 2\text{Id}$.

C'est une erreur classique : $P \mapsto P(u)$ est linéaire *en* P , mais $u \mapsto P(u)$ n'est pas linéaire *en* u (sauf si $\deg P \leq 1$ et $P(0) = 0$).

3. En développant avec soin (la composition est distributive sur l'addition, mais *pas commutative*) :

$$(u + v)^2 = (u + v) \circ (u + v) = u \circ u + u \circ v + v \circ u + v \circ v = u^2 + u \circ v + v \circ u + v^2.$$

L'égalité $(u + v)^2 = u^2 + 2u \circ v + v^2$ équivaut donc à $v \circ u = u \circ v$: **vrai si et seulement si u et v commutent**, faux en général.

Contre-exemple. Dans $\mathbb{R}^2$, u et v de matrices $U = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $V = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Alors $U^2 = V^2 = 0$,

$$UV = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad VU = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{et}$$

$$(U + V)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I_2 \quad \text{alors que} \quad U^2 + 2UV + V^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Cas où c'est automatiquement vrai : si v est un polynôme en u (par exemple $v = \lambda \text{Id}$), car deux polynômes en u commutent. C'est ce qui permet d'écrire $(u - \lambda \text{Id})^2 = u^2 - 2\lambda u + \lambda^2 \text{Id}$ sans hypothèse.

4. **Faux.** Un projecteur p vérifie $p^2 = p$, donc $P = X^2 - X$ (polynôme non nul) annule p . Il suffit de prendre $p \neq 0$: par exemple $p(x, y) = (x, 0)$ dans $\mathbb{R}^2$. On a $P(p) = 0$ avec $p \neq 0$ et $P \neq 0$. Autrement dit, $\mathcal{L}(E)$ **n'est pas intègre** : un produit (une composée) peut être nul sans qu'aucun facteur ne le soit. C'est précisément ce qui rend les polynômes annulateurs intéressants.

2.2 Produit de polynômes, lien avec les matrices

Exercice 6 – ★ vérifier sur des exemples.

1. $P(A) = A - I_2 = \begin{pmatrix} 0 & 2 \\ 3 & 3 \end{pmatrix}$ et $Q(A) = A + 2I_2 = \begin{pmatrix} 3 & 2 \\ 3 & 6 \end{pmatrix}$.

$$P(A)Q(A) = \begin{pmatrix} 0 \cdot 3 + 2 \cdot 3 & 0 \cdot 2 + 2 \cdot 6 \\ 3 \cdot 3 + 3 \cdot 3 & 3 \cdot 2 + 3 \cdot 6 \end{pmatrix} = \begin{pmatrix} 6 & 12 \\ 18 & 24 \end{pmatrix},$$

$$Q(A)P(A) = \begin{pmatrix} 3 \cdot 0 + 2 \cdot 3 & 3 \cdot 2 + 2 \cdot 3 \\ 6 \cdot 3 & 3 \cdot 2 + 6 \cdot 3 \end{pmatrix} = \begin{pmatrix} 6 & 12 \\ 18 & 24 \end{pmatrix}.$$

Enfin $PQ = (X - 1)(X + 2) = X^2 + X - 2$ et, avec $A^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$ (exercice 4),

$$(PQ)(A) = A^2 + A - 2I_2 = \begin{pmatrix} 7 + 1 - 2 & 10 + 2 \\ 15 + 3 & 22 + 4 - 2 \end{pmatrix} = \begin{pmatrix} 6 & 12 \\ 18 & 24 \end{pmatrix}.$$

Les trois matrices coïncident, comme l'affirme la proposition : $(PQ)(A) = P(A)Q(A) = Q(A)P(A)$.

2. $u(x, y) = (2x - y, x)$, donc $u(1, 0) = (2, 1)$ et $u(0, 1) = (-1, 0) : A = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$. Puis

$$A^2 = \begin{pmatrix} 4-1 & -2+0 \\ 2+0 & -1+0 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}, \quad A^2 - I_2 = \begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix}.$$

Or à l'exercice 4, $(u^2 - \text{Id})(x, y) = (2x - 2y, 2x - 2y)$, dont la matrice dans la base canonique est bien $\begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix}$. On a vérifié $\text{Mat}_{\mathcal{B}}(P(u)) = P(A)$.

3. D'après l'exercice 3, $B^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, donc

$$B^2 + I_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Un vecteur (x, y, z) est dans $\text{Ker}(B^2 + I_3)$ si et seulement si $x + z = 0$ (les trois lignes donnent $x + z = 0, 0 = 0, x + z = 0$). Donc

$$\text{Ker}(B^2 + I_3) = \{(x, y, -x) : x, y \in \mathbb{R}\} = \text{Vect}((1, 0, -1), (0, 1, 0)) = \text{Vect}(e_3, e_2) = \Pi,$$

puisque $e_3 = -\frac{\sqrt{2}}{2}(1, 0, -1)$. $\text{Ker}(B^2 + I_3)$ **est le plan Π de la rotation**. On savait à l'avance qu'il serait stable par B : c'est le noyau d'un polynôme en B (proposition 7.10).

De même, $B - I_3 = \frac{1}{2} \begin{pmatrix} -1 & -\sqrt{2} & 1 \\ \sqrt{2} & -2 & -\sqrt{2} \\ 1 & \sqrt{2} & -1 \end{pmatrix}$. Le système $(B - I_3)X = 0$ s'écrit (après multiplication par 2, et en divisant la deuxième ligne par $\sqrt{2}$)

$$\begin{cases} -x - \sqrt{2}y + z = 0 \\ x - \sqrt{2}y - z = 0 \\ x + \sqrt{2}y - z = 0 \end{cases}$$

La troisième ligne est l'opposée de la première. En ajoutant les deux premières : $-2\sqrt{2}y = 0$, donc $y = 0$, puis $z = x$. Ainsi $\text{Ker}(B - I_3) = \text{Vect}((1, 0, 1)) = \text{Vect}(e_1)$, **l'axe de la rotation**, lui aussi stable par B comme noyau d'un polynôme en B .

Bilan : les deux sous-espaces géométriquement naturels de la rotation (axe et plan) sont des noyaux de polynômes en B , et $\mathbb{R}^3 = \text{Ker}(B - I_3) \oplus \text{Ker}(B^2 + I_3)$, en lien avec l'annulateur $(X - 1)(X^2 + 1)$ de l'exercice 8.

Exercice 7 – ★★ polynômes en A et commutant.

1. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On calcule

$$AM = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad MA = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}.$$

$AM = MA$ équivaut au système $a + c = a, b + d = a + b, c = c, d = c + d$, c'est-à-dire $c = 0$ et $d = a$. Donc

$$\mathcal{C}(A) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{K} \right\}.$$

Une telle matrice s'écrit $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = aI_2 + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = aI_2 + b(A - I_2) = (a - b)I_2 + bA$: c'est $\alpha I_2 + \beta A$ avec $\alpha = a - b$, $\beta = b$.

Conclusion. Toute matrice du commutant est un polynôme en A (de degré ≤ 1) : $\mathcal{C}(A) \subset \mathbb{K}[A]$. L'inclusion réciproque est toujours vraie (un polynôme en A commute avec A). Donc $\mathcal{C}(A) = \mathbb{K}[A] = \text{Vect}(I_2, A)$, de dimension 2.

2. Pour tout k , $I_2^k = I_2$, donc $P(I_2) = (\sum_k a_k)I_2 = P(1)I_2$: $\mathbb{K}[I_2] = \text{Vect}(I_2)$, l'ensemble des matrices scalaires, de dimension 1.

Toute matrice commute avec I_2 : $\mathcal{C}(I_2) = \mathcal{M}_2(\mathbb{K})$, de dimension 4.

L'inclusion $\mathbb{K}[A] \subset \mathcal{C}(A)$ **n'est donc pas toujours une égalité**. (On verra à l'exercice 19 dans quels cas elle l'est pour une matrice diagonale.)

2.3 Polynômes annulateurs

Exercice 8 – ★ trouver un polynôme annulateur.

1. (a) $P = (X - 2)(X - 3) = X^2 - 5X + 6$. Avec $A^2 = \begin{pmatrix} 4 & 2+3 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 0 & 9 \end{pmatrix}$:

$$P(A) = A^2 - 5A + 6I_2 = \begin{pmatrix} 4 - 10 + 6 & 5 - 5 \\ 0 & 9 - 15 + 6 \end{pmatrix} = 0_2.$$

(b) $A - 2I_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, $A - 3I_2 = \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix}$, et

$$(A - 2I_2)(A - 3I_2) = \begin{pmatrix} 0 \cdot (-1) + 1 \cdot 0 & 0 \cdot 1 + 1 \cdot 0 \\ 0 & 0 \end{pmatrix} = 0_2.$$

C'est la proposition $(PQ)(A) = P(A)Q(A)$, avec $P = X - 2$ et $Q = X - 3$, qui garantit que ce produit vaut $((X - 2)(X - 3))(A) = P(A)$. On peut donc tester un annulateur factorisé *sans le développer*.

- (c) Dans les deux calculs, $P(A) = 0_2$: $P = (X - 2)(X - 3)$ **est un polynôme annulateur de A** .
2. (a) Un projecteur est un endomorphisme p vérifiant $p \circ p = p$. Donc $p^2 - p = 0$: $X^2 - X = X(X - 1)$ **annule** p . C'est de degré minimal dès que $p \neq 0$ et $p \neq \text{Id}$: un annulateur de degré 1, $aX + b$ avec $a \neq 0$, donnerait $p = -\frac{b}{a}\text{Id}$, et un projecteur scalaire λId vérifie $\lambda^2 = \lambda$, donc est 0 ou Id.
- (b) Une symétrie vérifie $s \circ s = \text{Id}$. Donc $X^2 - 1 = (X - 1)(X + 1)$ **annule** s , de degré minimal dès que $s \neq \pm\text{Id}$ (même argument).
3. $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est la matrice de la rotation d'angle $\frac{\pi}{2}$: deux quarts de tour font un demi-tour, $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$. Donc $X^2 + 1$ **annule** A . Un annulateur de degré 1 forcerait A à être scalaire, ce qu'elle n'est pas : le degré 2 est minimal.
- La matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ de l'exercice 1 est celle d'une symétrie, et $A^2 = I_2$: $X^2 - 1$ **annule** A , de degré minimal (A n'est pas scalaire).
4. On calcule les puissances de N :

$$N^2 = \begin{pmatrix} 0 & 0 & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad N^3 = N^2N = 0_3.$$

Donc X^3 **annule** N . Est-ce le plus petit degré ? Cherchons $\alpha N^2 + \beta N + \gamma I_3 = 0_3$:

$$\alpha N^2 + \beta N + \gamma I_3 = \begin{pmatrix} \gamma & \beta a & \alpha ac + \beta b \\ 0 & \gamma & \beta c \\ 0 & 0 & \gamma \end{pmatrix}.$$

Nécessairement $\gamma = 0$. Si $ac \neq 0$, alors $\beta a = 0$ donne $\beta = 0$, puis $\alpha ac = 0$ donne $\alpha = 0$: il n'y a pas d'annulateur non nul de degré ≤ 2 , et X^3 **est de degré minimal lorsque** $ac \neq 0$. Si $ac = 0$ mais $N \neq 0$, alors $N^2 = 0$ et X^2 convient (de degré minimal car N n'est pas scalaire). Si $N = 0$, X convient.

5. Tous les coefficients de J^2 valent $\sum_{k=1}^n 1 \cdot 1 = n$: $J^2 = nJ$. Donc $X^2 - nX = X(X - n)$ **annule** J . Pour $n \geq 2$, J n'est pas scalaire, donc le degré 2 est minimal. (Pour $n = 1$, $J = I_1$ et $X - 1$ convient.)

6. Degré 4. On a vu $B^4 = I_3$: $X^4 - 1$ **annule** B .

Degré 3. Posons $P = (X - 1)(X^2 + 1)$. On calcule $P(R) = (R - I_3)(R^2 + I_3)$ grâce à la proposition sur les produits :

$$R - I_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & -1 \end{pmatrix}, \quad R^2 + I_3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad (R - I_3)(R^2 + I_3) = 0_3$$

(la seule colonne non nulle de $R^2 + I_3$ est la première, et la première colonne de $R - I_3$ est nulle). Donc $P(R) = 0_3$.

Pourquoi cela suffit. D'après la proposition 7.11, $P(g)$ a pour matrice $P(B)$ dans la base canonique et $P(R)$ dans la base $\mathcal{B}'$. L'égalité $P(R) = 0_3$ signifie donc $P(g) = 0_{\mathcal{L}(\mathbb{R}^3)}$, et la matrice de l'endomorphisme nul dans la base canonique est 0_3 : $P(B) = 0_3$. $(X - 1)(X^2 + 1)$ **annule** B .

En termes matriciels : si $B = QRQ^{-1}$, alors $B^k = QR^kQ^{-1}$ pour tout k (récurrence de l'exercice 1) et, par linéarité, $P(B) = QP(R)Q^{-1}$. Deux matrices semblables ont les mêmes polynômes annulateurs.

Minimalité. Un annulateur $\alpha R^2 + \beta R + \gamma I_3 = \begin{pmatrix} \alpha + \beta + \gamma & 0 & 0 \\ 0 & -\alpha + \gamma & -\beta \\ 0 & \beta & -\alpha + \gamma \end{pmatrix}$ nul impose

$\beta = 0$, $\gamma = \alpha$, puis $2\alpha = 0$: seul le polynôme nul convient. Le degré 3 est donc minimal.

Lecture géométrique. Le facteur $X - 1$ correspond à l'axe (où $g = \text{Id}$) et le facteur $X^2 + 1$ au plan (où $g^2 = -\text{Id}$) : P est le produit des annulateurs des deux morceaux.

Exercice 9 – ★ le cas de la taille 2 : à connaître.

On calcule

$$A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix}, \quad (a + d)A = \begin{pmatrix} a^2 + ad & ab + bd \\ ac + cd & ad + d^2 \end{pmatrix},$$

donc

$$A^2 - (a + d)A = \begin{pmatrix} bc - ad & 0 \\ 0 & bc - ad \end{pmatrix} = -(ad - bc)I_2, \quad \text{soit} \quad \boxed{A^2 - (a + d)A + (ad - bc)I_2 = 0_2}.$$

Ainsi $X^2 - \text{tr}(A)X + \det(A)$ **annule toute matrice de** $\mathcal{M}_2(\mathbb{K})$ (c'est le théorème de Cayley-Hamilton en taille 2). Pour $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$: $\text{tr} A = 5$ et $\det A = 4 - 6 = -2$, d'où l'annulateur $X^2 - 5X - 2$ trouvé « par hasard » à l'exercice 4.

Remarque

Ce polynôme est de degré minimal dès que A n'est pas scalaire (un annulateur de degré 1 forcerait $A = \lambda I_2$). Pour une matrice de taille 2 non scalaire, on connaît donc toujours *le* bon polynôme annulateur, sans calcul.

2.4 Application 1 : calculer les puissances

Exercice 10 – guidé, pour tous.

1. $\text{tr } A = 2$ et $\det A = 1 - 4 = -3$, donc $P = X^2 - 2X - 3$ annule A . Ses racines sont 3 et -1 (somme 2, produit -3) : $P = (X - 3)(X + 1)$.
2. P est non nul, de degré 2 : la division euclidienne de X^k par P dans $\mathbb{R}[X]$ fournit un quotient Q_k et un reste R_k de degré ≤ 1 , que l'on écrit $R_k = a_k X + b_k$ avec $a_k, b_k \in \mathbb{R}$:

$$X^k = Q_k P + a_k X + b_k.$$

3. On évalue cette égalité de polynômes en 3 puis en -1 , racines de P (le terme $Q_k P$ s'annule) :

$$\begin{cases} 3a_k + b_k = 3^k \\ -a_k + b_k = (-1)^k \end{cases}$$

En soustrayant : $4a_k = 3^k - (-1)^k$, puis $b_k = (-1)^k + a_k$. Donc

$$\boxed{a_k = \frac{3^k - (-1)^k}{4}, \quad b_k = \frac{3^k + 3(-1)^k}{4}}.$$

4. En appliquant l'égalité polynomiale à A : $A^k = Q_k(A) P(A) + a_k A + b_k I_2 = a_k A + b_k I_2$, soit

$$A^k = \begin{pmatrix} a_k + b_k & 2a_k \\ 2a_k & a_k + b_k \end{pmatrix}$$

avec $a_k + b_k = \frac{2 \cdot 3^k + 2(-1)^k}{4} = \frac{3^k + (-1)^k}{2}$ et $2a_k = \frac{3^k - (-1)^k}{2}$. On retrouve exactement la formule de l'exercice 2 :

$$A^k = \frac{1}{2} \begin{pmatrix} 3^k + (-1)^k & 3^k - (-1)^k \\ 3^k - (-1)^k & 3^k + (-1)^k \end{pmatrix}.$$

Quelle méthode préférer ? La méthode du polynôme annulateur ne demande ni de deviner une base adaptée, ni d'inverser P ; elle ne nécessite que $\text{tr } A$ et $\det A$ en taille 2. La diagonalisation, elle, explique *pourquoi* 3^k et $(-1)^k$ apparaissent (ce sont les valeurs sur les droites stables) et se généralise mieux aux grandes tailles quand on connaît les droites stables. Les deux sont à connaître ; en taille 2, l'annulateur est souvent le plus rapide.

Exercice 11 – ★ en autonomie.

1. $\text{tr } A = 3$, $\det A = 0 - (-2) = 2$: $P = X^2 - 3X + 2 = (X - 1)(X - 2)$ annule A (exercice 9). Soit $k \in \mathbb{N}$. Comme $P \neq 0$, la division euclidienne de X^k par P fournit $Q_k \in \mathbb{R}[X]$ et un reste de degré ≤ 1 : il existe $a_k, b_k \in \mathbb{R}$ tels que $X^k = Q_k P + a_k X + b_k$. En évaluant en les racines 1 et 2 de P :

$$\begin{cases} a_k + b_k = 1 \\ 2a_k + b_k = 2^k \end{cases} \quad \implies \quad a_k = 2^k - 1, \quad b_k = 2 - 2^k.$$

En appliquant l'égalité polynomiale à A , et comme $P(A) = 0_2$:

$$A^k = Q_k(A)P(A) + a_k A + b_k I_2 = a_k A + b_k I_2 = \begin{pmatrix} 3a_k + b_k & -a_k \\ 2a_k & b_k \end{pmatrix} = \boxed{\begin{pmatrix} 2^{k+1} - 1 & 1 - 2^k \\ 2^{k+1} - 2 & 2 - 2^k \end{pmatrix}},$$

puisque $3a_k + b_k = 3 \cdot 2^k - 3 + 2 - 2^k = 2 \cdot 2^k - 1 = 2^{k+1} - 1$. Pour $k = 1$: $\begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix} = A$;
pour $k = 0$: I_2 .

2. $\star \star \operatorname{tr} A = 4$, $\det A = 3 - (-1) = 4$: $P = X^2 - 4X + 4 = (X - 2)^2$, **racine double 2**. On écrit

$$X^k = Q_k(X - 2)^2 + a_k X + b_k. \quad (*)$$

Évaluer en 2 donne une seule équation : $2a_k + b_k = 2^k$. Il en manque une : on **dérive** (*) (dérivation formelle des polynômes) :

$$kX^{k-1} = Q'_k(X - 2)^2 + 2Q_k(X - 2) + a_k,$$

et on évalue en 2 (les deux termes contenant $(X - 2)$ s'annulent) : $a_k = k 2^{k-1}$ (pour $k \geq 1$; pour $k = 0$ on lit directement $a_0 = 0$, $b_0 = 1$, ce qui est aussi ce que donne la formule avec la convention $0 \cdot 2^{-1} = 0$). Puis $b_k = 2^k - 2a_k = 2^k - k2^k = (1 - k)2^k$.

Comme en 1, on applique (*) à A : $A^k = Q_k(A)P(A) + a_k A + b_k I_2 = a_k A + b_k I_2 = \begin{pmatrix} 3a_k + b_k & a_k \\ -a_k & a_k + b_k \end{pmatrix}$ avec

$$3a_k + b_k = 3k2^{k-1} + 2^k - k2^k = 2^{k-1}(3k + 2 - 2k) = 2^{k-1}(k + 2),$$

$$a_k + b_k = k2^{k-1} + 2^k - k2^k = 2^{k-1}(k + 2 - 2k) = 2^{k-1}(2 - k),$$

d'où

$$\boxed{A^k = 2^{k-1} \begin{pmatrix} k+2 & k \\ -k & 2-k \end{pmatrix}} \quad (k \in \mathbb{N}).$$

Vérifications. $k = 0$: $\frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I_2$. $k = 1$: $\begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix} = A$. $k = 2$: la formule donne $2 \begin{pmatrix} 4 & 2 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ -4 & 0 \end{pmatrix}$, et le calcul direct $A^2 = \begin{pmatrix} 9-1 & 3+1 \\ -3-1 & -1+1 \end{pmatrix}$ confirme.

Remarque

Dans le cas d'une racine double λ , le reste s'écrit toujours $R_k = \lambda^k + k\lambda^{k-1}(X - \lambda)$: c'est le développement de Taylor de X^k en λ tronqué à l'ordre 1. Les puissances font alors apparaître des termes en $k 2^k$ et plus seulement des exponentielles : la matrice n'est pas diagonalisable (on le verra), et cela se lit dans ses puissances.

2.5 Application 2 : inverser

Exercice 12 – $\star$ application directe.

1. D'après l'exercice 10, $A^2 - 2A - 3I_2 = 0_2$, et le coefficient constant -3 est non nul. On isole : $A^2 - 2A = 3I_2$, soit $A(A - 2I_2) = 3I_2$, soit

$$A \cdot \frac{1}{3}(A - 2I_2) = I_2.$$

Comme A est carrée, un seul produit suffit : A **est inversible et**

$$A^{-1} = \frac{1}{3}(A - 2I_2) = \frac{1}{3} \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}.$$

Vérification : $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} -1+4 & 2-2 \\ -2+2 & 4-1 \end{pmatrix} = 3I_2.$

2. (a) Comme I_3 et J commutent, on peut développer : $A^2 = (J - I_3)^2 = J^2 - 2J + I_3 = 3J - 2J + I_3 = J + I_3$. Donc

$$A^2 - A - 2I_3 = (J + I_3) - (J - I_3) - 2I_3 = 0_3.$$

$X^2 - X - 2 = (X - 2)(X + 1)$ **annule** A .

- (b) Le coefficient constant est $-2 \neq 0$. On isole : $A^2 - A = 2I_3$, soit $A(A - I_3) = 2I_3$, donc A **est inversible et**

$$A^{-1} = \frac{1}{2}(A - I_3) = \frac{1}{2}(J - 2I_3) = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

Vérification : la première ligne de $A(J - 2I_3)$ est $(0, 1, 1) \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = (2, 0, 0)$, et

de même pour les autres lignes par symétrie : $A(J - 2I_3) = 2I_3$.

- (c) Soit $k \in \mathbb{N}$. Le polynôme $P = (X - 2)(X + 1)$ est non nul, de degré 2 : la division euclidienne de X^k par P s'écrit $X^k = Q_k P + a_k X + b_k$ avec $Q_k \in \mathbb{R}[X]$ et $a_k, b_k \in \mathbb{R}$. En évaluant en les racines 2 et -1 :

$$\begin{cases} 2a_k + b_k = 2^k \\ -a_k + b_k = (-1)^k \end{cases} \implies a_k = \frac{2^k - (-1)^k}{3}, \quad b_k = \frac{2^k + 2(-1)^k}{3}.$$

En appliquant à A , et puisque $P(A) = 0_3$ par (a) : $A^k = Q_k(A)P(A) + a_k A + b_k I_3 = a_k A + b_k I_3$: tous les coefficients diagonaux valent b_k et tous les autres valent a_k :

$$A^k = \frac{1}{3} \begin{pmatrix} 2^k + 2(-1)^k & 2^k - (-1)^k & 2^k - (-1)^k \\ 2^k - (-1)^k & 2^k + 2(-1)^k & 2^k - (-1)^k \\ 2^k - (-1)^k & 2^k - (-1)^k & 2^k + 2(-1)^k \end{pmatrix}.$$

Vérification : $k = 1$ donne diagonale $\frac{2-2}{3} = 0$ et hors diagonale $\frac{2+1}{3} = 1$, c'est A . Et $k = -1$ (formellement) donne diagonale $\frac{1/2-2}{3} = -\frac{1}{2}$, hors diagonale $\frac{1/2+1}{3} = \frac{1}{2}$: c'est bien A^{-1} .

3. L'annulateur $X^2 - nX = X(X - n)$ a un coefficient constant **nul** : l'égalité $J^2 - nJ = 0_n$ se factorise en $J(J - nI_n) = 0_n$, et il n'y a aucun terme en I_n à isoler. La méthode ne s'applique pas.

Et de fait, J **n'est pas inversible** (pour $n \geq 2$) : si elle l'était, en multipliant $J(J - nI_n) = 0_n$ par J^{-1} on obtiendrait $J - nI_n = 0_n$, ce qui est faux (les coefficients hors diagonale de J valent 1, pas 0). On peut aussi dire que toutes les colonnes de J sont égales, donc $\text{rg } J = 1 < n$.

Remarque

On devine la règle générale (exercice 18) : A est inversible si et seulement si elle possède un annulateur P avec $P(0) \neq 0$. Le fait que 0 soit racine de *tous* les annulateurs de J est le signe que J n'est pas inversible : 0 est ce qu'on appellera une « valeur propre » de J .

2.6 Une conséquence : tout polynôme en u est de petit degré

Exercice 13 – ★ illustration.

1. Comme $s^2 = \text{Id}$, on a $s^{2m} = (s^2)^m = \text{Id}$ et $s^{2m+1} = s$ pour tout $m \in \mathbb{N}$: toute puissance de s est Id ou s . Si $P = \sum_k a_k X^k$, alors

$$P(s) = \sum_{k \text{ pair}} a_k \text{Id} + \sum_{k \text{ impair}} a_k s = \alpha \text{Id} + \beta s \quad \text{avec} \quad \alpha = \sum_{k \text{ pair}} a_k, \quad \beta = \sum_{k \text{ impair}} a_k.$$

On peut aussi écrire $\alpha = \frac{P(1)+P(-1)}{2}$ et $\beta = \frac{P(1)-P(-1)}{2}$ (évaluer $P(s) = \alpha \text{Id} + \beta s$ en remplaçant formellement s par 1 puis -1 ; ou faire la division euclidienne de P par $X^2 - 1$ et évaluer le reste en ± 1). (C'est la proposition 7.23 avec l'annulateur $X^2 - 1$ de degré 2 : $\mathbb{K}[s] = \text{Vect}(\text{Id}, s)$.)

Pour $s^5 - 3s^2 + s$: $s^5 = s$, $s^2 = \text{Id}$, donc $s^5 - 3s^2 + s = s - 3\text{Id} + s = \boxed{2s - 3\text{Id}}$. Contrôle par les formules : $P(1) = 1 - 3 + 1 = -1$, $P(-1) = -1 - 3 - 1 = -5$, $\alpha = \frac{-1-5}{2} = -3$, $\beta = \frac{-1+5}{2} = 2$.

2. Soit $P = (X - 1)(X^2 + 1) = X^3 - X^2 + X - 1$. On effectue la division euclidienne de X^4 par P : on cherche $X^4 = (X + c)P + R$ avec $\deg R \leq 2$. Or

$$(X + 1)(X^3 - X^2 + X - 1) = X^4 - X^3 + X^2 - X + X^3 - X^2 + X - 1 = X^4 - 1,$$

donc $X^4 = (X + 1)P + 1$, c'est-à-dire $Q_4 = X + 1$ et $R_4 = 1$. En appliquant à B :

$$B^4 = (B + I_3) \underbrace{P(B)}_{=0_3} + 1 \cdot I_3 = \boxed{0 \cdot B^2 + 0 \cdot B + 1 \cdot I_3 = I_3}.$$

C'est parfaitement cohérent avec $B^4 = I_3$ trouvé à l'exercice 3 : on vient même de le redémontrer, puisque $X^4 - 1 = (X + 1)(X - 1)(X^2 + 1)$ est un multiple de l'annulateur P .

3 Exercices d'application

Exercice 14 – ★ suites récurrentes couplées.

Les relations $u_{k+1} = u_k + 2v_k$ et $v_{k+1} = 2u_k + v_k$ s'écrivent

$$\begin{pmatrix} u_{k+1} \\ v_{k+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} u_k \\ v_k \end{pmatrix}, \quad \text{soit} \quad X_{k+1} = AX_k \quad \text{avec} \quad A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Par récurrence immédiate, $X_k = A^k X_0$ pour tout $k \in \mathbb{N}$ (vrai pour $k = 0$; si $X_k = A^k X_0$ alors $X_{k+1} = AX_k = A^{k+1} X_0$). Avec la formule de A^k (exercices 2 et 10) et $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, X_k est la *première colonne* de A^k :

$$\boxed{u_k = \frac{3^k + (-1)^k}{2}, \quad v_k = \frac{3^k - (-1)^k}{2}}.$$

Vérification : $u_1 = 1$, $v_1 = 2$, ce qui est bien $u_1 = u_0 + 2v_0 = 1$ et $v_1 = 2u_0 + v_0 = 2$. Et u_k, v_k sont entiers (somme et différence de deux entiers de même parité, divisées par 2), comme il se doit.

Équivalent. $u_k = \frac{3^k}{2} \left(1 + \left(-\frac{1}{3}\right)^k\right)$ et $\left(-\frac{1}{3}\right)^k \rightarrow 0$, donc $\boxed{u_k \underset{k \rightarrow +\infty}{\sim} \frac{3^k}{2}}$ (et de même $v_k \sim \frac{3^k}{2}$). C'est

le terme en 3^k , associé à la droite stable $\text{Vect}(e_1)$, qui domine.

Exercice 15 – ★ la matrice $I_n + J$.

1. Par récurrence sur $k \geq 1$. Pour $k = 1$: $J^1 = n^0 J$. Si $J^k = n^{k-1} J$, alors $J^{k+1} = J^k J = n^{k-1} J^2 = n^{k-1} \cdot nJ = n^k J$ (avec $J^2 = nJ$, exercice 8). **Donc** $J^k = n^{k-1} J$ **pour tout** $k \geq 1$. (Attention, c'est faux pour $k = 0$: $J^0 = I_n \neq \frac{1}{n} J$.)

2. On remplace $J = A - I_n$ dans $J^2 = nJ$ (licite car A et I_n commutent) :

$$(A - I_n)^2 = n(A - I_n) \iff A^2 - 2A + I_n = nA - nI_n \iff A^2 - (n+2)A + (n+1)I_n = 0_n.$$

$P = X^2 - (n+2)X + (n+1) = (X-1)(X-(n+1))$ **annule** A , et $P(0) = n+1 \neq 0$. On isole : $A(A - (n+2)I_n) = -(n+1)I_n$, donc A est inversible et

$$A^{-1} = \frac{1}{n+1}((n+2)I_n - A) = \frac{1}{n+1}((n+1)I_n - J) = \boxed{I_n - \frac{1}{n+1}J}.$$

Vérification : $(I_n + J)(I_n - \frac{1}{n+1}J) = I_n + J - \frac{1}{n+1}J - \frac{1}{n+1}J^2 = I_n + J(1 - \frac{1}{n+1} - \frac{n}{n+1}) = I_n$.

3. *Par le binôme*. La formule du binôme $(M+N)^k = \sum_{i=0}^k \binom{k}{i} M^i N^{k-i}$ est valable dans $\mathcal{M}_n(\mathbb{K})$ **à condition que M et N commutent** (c'est le cas de I_n et J , puisque I_n commute avec tout). Donc, en isolant le terme $i=0$ et en utilisant la question 1 pour $i \geq 1$:

$$A^k = \sum_{i=0}^k \binom{k}{i} J^i = I_n + \sum_{i=1}^k \binom{k}{i} n^{i-1} J = I_n + \frac{1}{n} \left(\sum_{i=1}^k \binom{k}{i} n^i \right) J = I_n + \frac{(1+n)^k - 1}{n} J,$$

en reconnaissant $\sum_{i=0}^k \binom{k}{i} n^i = (1+n)^k$ (binôme dans $\mathbb{K}$), auquel on a retiré le terme $i=0$ égal à 1.

Par l'annulateur. Soit $k \in \mathbb{N}$. Comme $P \neq 0$ est de degré 2, la division euclidienne de X^k par P s'écrit $X^k = Q_k P + a_k X + b_k$ avec $Q_k \in \mathbb{K}[X]$ et $a_k, b_k \in \mathbb{K}$. On évalue en les racines 1 et $n+1$ de P :

$$\begin{cases} a_k + b_k = 1 \\ (n+1)a_k + b_k = (n+1)^k \end{cases} \implies a_k = \frac{(n+1)^k - 1}{n}, \quad b_k = 1 - a_k.$$

En appliquant à A , et comme $P(A) = 0_n$: $A^k = Q_k(A)P(A) + a_k A + b_k I_n = a_k(I_n + J) + (1 - a_k)I_n = I_n + a_k J$, soit

$$\boxed{A^k = I_n + \frac{(n+1)^k - 1}{n} J} \quad (k \in \mathbb{N}),$$

ce qui coïncide avec le calcul par le binôme. (Pour $k=0$: I_n ; pour $k=1$: $I_n + J$. Et pour $k=-1$, la formule donne $I_n + \frac{1}{n+1}J = I_n - \frac{1}{n+1}J = A^{-1}$: encore une fois cohérent.)

Exercice 16 – ★★ différences finies sur $\mathbb{R}_n[X]$.

1. *Linéarité*. Pour $Q, R \in E$ et $\lambda \in \mathbb{R}$: $(\lambda Q + R)(X+1) = \lambda Q(X+1) + R(X+1)$ (substitution de $X+1$ dans un polynôme), donc $\Delta(\lambda Q + R) = \lambda \Delta(Q) + \Delta(R)$.

À valeurs dans E . Si $\deg Q \leq n$, alors $Q(X+1)$ est encore de degré $\leq n$ (composer par $X+1$, de degré 1, ne change pas le degré), et la différence de deux polynômes de degré $\leq n$ est de degré $\leq n$. **Δ est un endomorphisme de E .**

Calculs. $\Delta(1) = 1 - 1 = 0$; $\Delta(X) = (X+1) - X = 1$; $\Delta(X^2) = (X+1)^2 - X^2 = 2X + 1$.

2. Soit $Q = \sum_{k=0}^d a_k X^k$ avec $d \geq 1$ et $a_d \neq 0$. Par le binôme, $(X+1)^k = X^k + kX^{k-1} + \dots$ (termes de degré $\leq k-2$) pour $k \geq 1$, et $(X+1)^0 - X^0 = 0$. Donc

$$\Delta(Q) = \sum_{k=1}^d a_k ((X+1)^k - X^k) = \sum_{k=1}^d a_k (kX^{k-1} + \dots) = d a_d X^{d-1} + (\text{termes de degré} \leq d-2).$$

Comme $d a_d \neq 0$, $\deg \Delta(Q) = \deg Q - 1$.

Par récurrence, pour tout $Q \in E$ et tout $j \in \mathbb{N}$, $\Delta^j(Q)$ est nul ou de degré $\leq n - j$: tant que le degré est ≥ 1 il baisse de 1, et Δ annule les constantes. Ainsi $\Delta^n(Q)$ est une constante

et $\Delta^{n+1}(Q) = 0$. **Donc** $\Delta^{n+1} = 0_{\mathcal{L}(E)} : X^{n+1}$ **est un polynôme annulateur de Δ** . Il est de degré minimal, car $\Delta^n(X^n) = n! \neq 0$ (le coefficient dominant est multiplié successivement par $n, n-1, \dots, 1$), donc X^n n'annule pas Δ , ni aucun X^j avec $j \leq n$; et un annulateur de Δ de degré $\leq n$ autre que ces monômes est exclu par la minimalité que l'on peut vérifier directement (si $\sum_{j=0}^n c_j \Delta^j = 0$, l'appliquer à $1, X, \dots, X^n$ successivement donne $c_0 = 0$, puis $c_1 = 0$, etc.).

3. On développe la composée (la composition est distributive, et toutes les puissances de Δ commutent) :

$$\begin{aligned} (\text{Id} + \Delta) \circ \sum_{k=0}^n (-1)^k \Delta^k &= \sum_{k=0}^n (-1)^k \Delta^k + \sum_{k=0}^n (-1)^k \Delta^{k+1} \\ &= \sum_{k=0}^n (-1)^k \Delta^k - \sum_{k=1}^{n+1} (-1)^k \Delta^k = \text{Id} - (-1)^{n+1} \Delta^{n+1}. \end{aligned}$$

(Somme télescopique : c'est l'identité $(1+x)(1-x+x^2-\dots+(-1)^n x^n) = 1 + (-1)^n x^{n+1}$.)
Comme $\Delta^{n+1} = 0$:

$$\boxed{(\text{Id} + \Delta) \circ \sum_{k=0}^n (-1)^k \Delta^k = \text{Id} .}$$

4. Posons $w = \sum_{k=0}^n (-1)^k \Delta^k$. On vient de voir $\tau \circ w = \text{Id}$. Comme $\tau = \text{Id} + \Delta$ et w sont deux polynômes en Δ , ils commutent : $w \circ \tau = \tau \circ w = \text{Id}$. **Donc τ est inversible et $\tau^{-1} = w = \sum_{k=0}^n (-1)^k \Delta^k$.**

Puisque $\tau(Q) = Q(X+1)$, son inverse est la substitution contraire : $\tau^{-1}(Q) = Q(X-1)$ (en effet $\tau(Q(X-1)) = Q(X)$). On obtient donc la formule

$$Q(X-1) = \sum_{k=0}^n (-1)^k \Delta^k(Q) \quad \text{pour tout } Q \in \mathbb{R}_n[X].$$

Vérification pour $n=2$, $Q = X^2$. $\Delta(X^2) = 2X+1$, $\Delta^2(X^2) = \Delta(2X+1) = 2\Delta(X) + \Delta(1) = 2$,
et

$$X^2 - (2X+1) + 2 = X^2 - 2X + 1 = (X-1)^2 = Q(X-1). \quad \checkmark$$

Remarque

Cet exercice est l'exemple type de la méthode d'inversion : $\text{Id} + \Delta$ est inversible dès que Δ est *nilpotent*, et l'inverse est la « série géométrique » $\sum (-1)^k \Delta^k$, qui est ici une somme finie. L'annulateur est X^{n+1} ; l'annulateur de τ est $(X-1)^{n+1}$, dont le coefficient constant $(-1)^{n+1}$ est non nul.

Exercice 17 – ★★ un annulateur scindé à racines simples.

1. De $u^2 - 3u + 2\text{Id} = 0$ on tire $u^2 - 3u = -2\text{Id}$, soit $u \circ (u - 3\text{Id}) = -2\text{Id}$, soit

$$u \circ \frac{1}{2}(3\text{Id} - u) = \text{Id}.$$

Posons $v = \frac{1}{2}(3\text{Id} - u)$. On a $u \circ v = \text{Id}$; comme v est un polynôme en u , $v \circ u = u \circ v = \text{Id}$ (ici E n'est pas supposé de dimension finie, cette vérification des deux côtés est donc indispensable). **Donc u est inversible et $u^{-1} = \frac{1}{2}(3\text{Id} - u)$.**

2. $F = \text{Ker}(u - \text{Id})$ et $G = \text{Ker}(u - 2\text{Id})$ sont les noyaux de polynômes en u : ils sont stables par u (proposition 7.10). Directement : si $x \in F$, $u(x) = x$, donc $u(u(x)) = u(x)$, c'est-à-dire $u(x) \in F$; de même, si $u(x) = 2x$ alors $u(u(x)) = 2u(x)$ et $u(x) \in G$.
3. Soit $x \in F \cap G$. Alors $u(x) = x$ et $u(x) = 2x$, donc $x = 2x$, donc $x = 0$. $F \cap G = \{0\}$.

4. Le polynôme annulateur se factorise : $X^2 - 3X + 2 = (X - 1)(X - 2)$, donc $(u - \text{Id}) \circ (u - 2\text{Id}) = (u - 2\text{Id}) \circ (u - \text{Id}) = 0$.

$y = 2x - u(x) = -(u - 2\text{Id})(x)$, donc $(u - \text{Id})(y) = -(u - \text{Id}) \circ (u - 2\text{Id})(x) = 0 : y \in F$.

$z = u(x) - x = (u - \text{Id})(x)$, donc $(u - 2\text{Id})(z) = (u - 2\text{Id}) \circ (u - \text{Id})(x) = 0 : z \in G$.

Enfin $y + z = 2x - u(x) + u(x) - x = x$.

5. D'après 4, tout $x \in E$ est somme d'un élément de F et d'un élément de G : $E = F + G$. Avec $F \cap G = \{0\}$ (question 3), $E = F \oplus G$.

Si E est de dimension finie, prenons une base $(f_1, \dots, f_p)$ de F et une base $(g_1, \dots, g_q)$ de G ; leur concaténation est une base de E (adaptée à la somme directe), et dans cette base $u(f_i) = f_i$, $u(g_j) = 2g_j$: **la matrice de u est diagonale**, $\text{diag}(1, \dots, 1, 2, \dots, 2)$ avec p fois 1 et q fois 2.

Lien avec la partie 1. C'est exactement ce qui s'est passé pour la symétrie de l'exercice 1 : annulateur $(X - 1)(X + 1)$, $\text{Ker}(f - \text{Id}) = \text{Vect}(e_1)$, $\text{Ker}(f + \text{Id}) = \text{Vect}(e_2)$, $\mathbb{R}^2 = \text{Vect}(e_1) \oplus \text{Vect}(e_2)$ et matrice $\text{diag}(1, -1)$ dans la base adaptée. Pour la matrice $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$: annulateur $(X - 3)(X + 1)$ et $\mathbb{R}^2 = \text{Ker}(g - 3\text{Id}) \oplus \text{Ker}(g + \text{Id})$. En revanche, pour la rotation de l'exercice 3, l'annulateur $(X - 1)(X^2 + 1)$ a un facteur $X^2 + 1$ sans racine réelle, et le noyau $\text{Ker}(B^2 + I_3) = \Pi$ n'est pas une « droite où g est une homothétie » : c'est pour cela que B n'est pas diagonalisable sur $\mathbb{R}$.

Principe général (à venir) : si u admet un annulateur scindé à racines simples $\prod (X - \lambda_i)$, alors $E = \bigoplus \text{Ker}(u - \lambda_i \text{Id})$ et u est diagonalisable.

Exercice 18 - *** l'inverse est toujours un polynôme.

- E est de dimension finie n , donc $\mathcal{L}(E)$ est de dimension finie n^2 . La famille $(\text{Id}, u, u^2, \dots, u^{n^2})$ compte $n^2 + 1$ vecteurs de $\mathcal{L}(E)$: elle est liée. Il existe donc des scalaires $a_0, \dots, a_{n^2}$ non tous nuls tels que $\sum_{k=0}^{n^2} a_k u^k = 0$, c'est-à-dire $P(u) = 0$ avec $P = \sum a_k X^k \neq 0$ (cours 7.18).
- Comme $P \neq 0$, il possède un coefficient non nul; soit m le plus petit indice tel que $a_m \neq 0$ (la *valuation* de P). Alors $P = \sum_{k \geq m} a_k X^k = X^m \sum_{k \geq m} a_k X^{k-m} = X^m S$ avec $S = \sum_{k \geq m} a_k X^{k-m}$, dont le coefficient constant est $S(0) = a_m \neq 0$. (Autrement dit : on factorise par la plus grande puissance de X possible, m étant la multiplicité de 0 comme racine de P .)
- $0 = P(u) = (X^m S)(u) = u^m \circ S(u)$. Comme u est inversible, u^m l'est aussi (d'inverse $(u^{-1})^m$). En composant à gauche par $(u^{-1})^m$:

$$S(u) = (u^{-1})^m \circ u^m \circ S(u) = (u^{-1})^m \circ 0 = 0.$$

S est un polynôme annulateur de u avec $S(0) \neq 0$.

4. Écrivons $S = a_d X^d + \dots + a_1 X + a_0$ avec $a_0 = S(0) \neq 0$. L'égalité $S(u) = 0$ s'écrit

$$u \circ (a_d u^{d-1} + \dots + a_1 \text{Id}) = -a_0 \text{Id}, \quad \text{soit} \quad u \circ \left(-\frac{1}{a_0} (a_d u^{d-1} + \dots + a_1 \text{Id}) \right) = \text{Id}.$$

(Si $d = 0$, $S = a_0$ et $S(u) = a_0 \text{Id} = 0$ force $E = \{0\}$, cas trivial où $u^{-1} = 0 \in \mathbb{K}[u]$; on suppose donc $d \geq 1$.) Posons $v = -\frac{1}{a_0} (a_d u^{d-1} + \dots + a_1 \text{Id})$. On a $u \circ v = \text{Id}$, et u est inversible, donc en composant par u^{-1} à gauche, $v = u^{-1}$. **Ainsi $u^{-1} = v \in \mathbb{K}[u]$: l'inverse de u est un polynôme en u .**

5. ($\Leftarrow$) Si P annule u avec $P(0) \neq 0$, la méthode 7.24 (celle de la question 4, avec $S = P$) fournit $v \in \mathbb{K}[u]$ tel que $u \circ v = \text{Id}$; comme v est un polynôme en u , $v \circ u = u \circ v = \text{Id}$, donc u est inversible. (Ici on n'a même pas besoin de la dimension finie.)

($\Rightarrow$) Si u est inversible, les questions 1 à 3 fournissent un annulateur S avec $S(0) \neq 0$.

Conclusion : u est inversible si et seulement si u admet un polynôme annulateur P tel que $P(0) \neq 0$. En termes qui viendront bientôt : u est inversible si et seulement si 0 n'est pas racine de son polynôme minimal.

Remarque

Pour les matrices, cela donne : $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si l'un de ses annulateurs a un coefficient constant non nul, et dans ce cas $A^{-1} \in \mathbb{K}[A]$. L'exemple de J (exercice 12) montre que, lorsque A n'est pas inversible, tous ses annulateurs s'annulent en 0.

Exercice 19 – *** commutant d'une matrice diagonale.

Notons $D = \text{diag}(d_1, d_2, d_3)$ avec $d_1 = 1, d_2 = 2, d_3 = 3$.

1. Multiplier à gauche par une matrice diagonale multiplie la ligne i par d_i ; multiplier à droite multiplie la colonne j par d_j . Précisément, pour tous i, j :

$$(DM)_{ij} = \sum_k D_{ik} m_{kj} = d_i m_{ij}, \quad (MD)_{ij} = \sum_k m_{ik} D_{kj} = m_{ij} d_j.$$

Donc $DM = MD$ si et seulement si, pour tous i, j : $(d_i - d_j) m_{ij} = 0$. Pour $i = j$ c'est automatique ; pour $i \neq j$, comme $d_i \neq d_j$ (les trois valeurs 1, 2, 3 sont distinctes), cela équivaut à $m_{ij} = 0$. **M commute avec D si et seulement si M est diagonale.** (Réciproquement, deux matrices diagonales commutent bien.)

2. On utilise les polynômes de Lagrange associés aux points 1, 2, 3 :

$$L_1 = \frac{(X-2)(X-3)}{(1-2)(1-3)} = \frac{(X-2)(X-3)}{2}, \quad L_2 = \frac{(X-1)(X-3)}{(2-1)(2-3)} = -(X-1)(X-3),$$

$$L_3 = \frac{(X-1)(X-2)}{(3-1)(3-2)} = \frac{(X-1)(X-2)}{2}.$$

Ils vérifient $L_i(j) = 1$ si $i = j$ et 0 sinon. Le polynôme $P = \alpha L_1 + \beta L_2 + \gamma L_3$ (de degré ≤ 2) vérifie donc $P(1) = \alpha, P(2) = \beta, P(3) = \gamma$.

3. Soit $M \in \mathcal{C}(D)$. D'après 1, $M = \text{diag}(\alpha, \beta, \gamma)$. D'après 2, il existe $P \in \mathbb{K}[X]$ tel que $P(1) = \alpha, P(2) = \beta, P(3) = \gamma$, et d'après l'exercice 4 (question 2), $P(D) = \text{diag}(P(1), P(2), P(3)) = M$. Donc $M \in \mathbb{K}[D] : \mathcal{C}(D) \subset \mathbb{K}[D]$. L'inclusion réciproque est toujours vraie. **Donc $\mathcal{C}(D) = \mathbb{K}[D]$, et c'est l'espace des matrices diagonales, de dimension 3.**

Cohérence : $(X-1)(X-2)(X-3)$ annule D (degré 3, et pas moins : un annulateur de degré ≤ 2 devrait avoir trois racines 1, 2, 3), donc par la proposition 7.23, $\mathbb{K}[D] = \text{Vect}(I_3, D, D^2)$, famille libre (on peut le vérifier avec un déterminant de Vandermonde) : dimension 3.

4. **Non.** Pour $D' = \text{diag}(1, 1, 2)$, la question 1 donne : M commute avec D' si et seulement si $m_{ij} = 0$ dès que $d_i \neq d_j$, c'est-à-dire $m_{13} = m_{31} = m_{23} = m_{32} = 0$. Donc

$$\mathcal{C}(D') = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e \end{pmatrix} \right\}, \quad \dim \mathcal{C}(D') = 5.$$

Alors que $P(D') = \text{diag}(P(1), P(1), P(2)) : \mathbb{K}[D'] = \text{Vect}(I_3, D')$ (annulateur $(X-1)(X-2)$ de degré 2), de dimension 2. On a $\mathbb{K}[D'] \subsetneq \mathcal{C}(D')$.

Où le raisonnement échoue. En question 1, la condition $(d_i - d_j)m_{ij} = 0$ ne force plus $m_{12} = m_{21} = 0$ puisque $d_1 = d_2$: le commutant contient des matrices non diagonales. Et en question 3, un polynôme en D' a toujours ses deux premiers coefficients diagonaux *égaux* ($P(1)$ et $P(1)$) : on ne peut atteindre $\text{diag}(\alpha, \beta, \gamma)$ que si $\alpha = \beta$. Le point clé était que les d_i soient **deux à deux distincts**.

Remarque

On démontre plus généralement : pour une matrice diagonale D à coefficients diagonaux deux à deux distincts, $\mathcal{C}(D) = \mathbb{K}[D]$ est de dimension n ; dès qu'une valeur se répète, le commutant est strictement plus gros que $\mathbb{K}[D]$. Comparer avec l'exercice 7 : pour $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (non diagonalisable, mais « une seule valeur »), l'égalité $\mathcal{C}(A) = \mathbb{K}[A]$ tient pourtant.