

ÉPREUVES

Chapitre 1

ALGÈBRE LINÉAIRE ET RÉDUCTION DES ENDOMORPHISMES

ÉTANT donné un endomorphisme ou une matrice, on peut se demander s'il existe une base dans laquelle cet endomorphisme ou cette matrice admet une forme simple. Plus précisément, on cherche si, dans une classe de similitude, on peut trouver un élément d'expression simple, par exemple une matrice diagonale, diagonale par blocs ou triangulaire. Afin de répondre à cette question, on s'intéresse dans un premier temps aux sous-espaces stables et compagnons indispensables aux polynômes d'endomorphismes ou de matrices.

Soit \mathbb{K} un corps infini (par exemple $\mathbb{K} = \mathbb{R}, \mathbb{C}, \dots$). Dans l'ensemble de ce chapitre, E désigne un \mathbb{K} -espace vectoriel de dimension quelconque dans un premier temps, puis de dimension finie à partir de la section II.2.

I. SOUS-ESPACES STABLES

Commençons par approfondir les notions développées dans le chapitre 19 de *Mathématiques L1* (Pearson Education, 2006).

I.1. Sous-espaces stables

Définition 1.1.

◇ Soient f un endomorphisme de E et F un sous-espace vectoriel de E .

On dit que F est stable par f si $f(F) \subset F$.

◇ Si F est un sous-espace stable, l'endomorphisme $\tilde{f} : F \rightarrow F$ défini par $\tilde{f}(x) = f(x)$ pour tout $x \in F$ est appelé endomorphisme induit par f sur F .

On notera aussi $\tilde{f} = f|_F$ cette restriction de f à F .

Soit $x \in E$. Si deux sous-espaces F_1 et F_2 sont stables par f et contiennent x , alors leur intersection est un sous-espace non réduit à zéro (il contient x) et stable par f . Il existe donc un sous-espace E_x stable par f et tel que tout sous-espace F de E stable par f et contenant x contient E_x . On dira que E_x est le plus petit (pour l'inclusion) sous-espace stable par f contenant x .

Rappel

Puissances de composition

Les puissances de composition de f sont définies par $f^0 = \text{Id}_E$ et, pour tout $k \in \mathbb{N}$, $f^{k+1} = f \circ f^k$.

Proposition 1.2. Soient f un endomorphisme de E et $x \in E$. Le plus petit sous-espace stable par f contenant x est le sous-espace engendré par la famille $(f^k(x))_{k \in \mathbb{N}}$.

PREUVE. Notons E_x le plus petit sous-espace stable par f contenant x .

Comme $\text{Vect}(f^k(x))_{k \in \mathbb{N}}$ est un sous-espace de E contenant x et stable par f , alors $E_x \subset \text{Vect}(f^k(x))_{k \in \mathbb{N}}$.

Réciproquement, pour tout $k \in \mathbb{N}$, $f^k(x) \in E_x$ (par récurrence, car $x \in E_x$ et E_x est stable par f). D'où $E_x = \text{Vect}(f^k(x))_{k \in \mathbb{N}}$. ■

Proposition 1.3. Soient f et g deux endomorphismes de E tels que $f \circ g = g \circ f$. Alors, le noyau et l'image de g sont des sous-espaces stables par f .

PREUVE.

- si $x \in \ker(g)$, alors $g(f(x)) = f(g(x)) = f(0_E) = 0_E$, d'où $f(x) \in \ker(g)$;
- si $y \in \mathfrak{Im}(g)$, alors il existe $x \in E$ tel que $y = g(x)$. Par conséquent, $f(y) = f(g(x)) = g(f(x)) \in \mathfrak{Im}(g)$. ■

Déterminons les sous-espaces stables dans les quelques cas particuliers suivants :

1. Tous les sous-espaces sont stables par une homothétie.
2. Rappelons qu'un projecteur est un endomorphisme p satisfaisant $p^2 = p$ et qu'un projecteur réalise une projection sur $\mathfrak{Im}(p) = \ker(p - \text{Id})$ parallèlement à $\ker(p)$ (voir la section II.4. du chapitre 19 de *Mathématiques L1*, Pearson Education, 2006). Montrons qu'un sous-espace est stable par un projecteur p si et seulement s'il est la somme directe d'un sous-espace de $\mathfrak{Im}(p)$ et d'un sous-espace de $\ker(p)$.
Soit F un sous-espace stable par p . L'endomorphisme \tilde{p} induit par p sur F est un projecteur de F ; par conséquent, F est la somme directe du noyau de \tilde{p} et de l'image de \tilde{p} qui sont, respectivement, des sous-espaces de $\mathfrak{Im}(p)$ et de $\ker(p)$.
Réciproquement, la somme directe d'un sous-espace de $\mathfrak{Im}(p)$ et d'un sous-espace de $\ker(p)$ est bien un sous-espace stable, car p laisse invariant tous les éléments de $\mathfrak{Im}(p)$.
3. De même, les sous-espaces stables par une symétrie s sont obtenus comme somme directe d'un sous-espace de $\ker(s - \text{Id})$ et d'un sous-espace de $\ker(s + \text{Id})$.
4. Supposons ici que E est de dimension finie et considérons f un endomorphisme de E , nilpotent d'indice $n = \dim E$ (i.e. $f^n = 0$ et $f^{n-1} \neq 0$). Montrons que les sous-espaces stables sont les $\ker(f^k)$ pour $k \in \{1, \dots, n\}$. Il est immédiat que ces sous-espaces sont stables d'après la proposition précédente.
Soit F un sous-espace stable par f ; l'endomorphisme \tilde{f} induit par f sur F est nilpotent. Notons p son indice. On a alors $F = \ker(\tilde{f}^p) \subset \ker(f^p)$.

L'intérêt des sous-espaces stables est qu'ils permettent d'obtenir une première version plus simple d'un endomorphisme : si l'on dispose d'une décomposition de E en somme directe de sous-espaces stables par f , alors l'étude de f est équivalente à l'étude des endomorphismes induits par f sur chacun de ces sous-espaces.

I.2. Polynômes d'un endomorphisme ou d'une matrice

Rappelons avant de commencer cette section que l'ensemble $\mathbb{K}[X]$ muni de l'addition, de la multiplication entre polynômes et de la multiplication par un scalaire jouit de la structure d'algèbre.

Définition 1.4. Soit $f \in L(E)$.

Pour tout polynôme $P(X) = \sum_{k=0}^N \alpha_k X^k \in \mathbb{K}[X]$, on définit l'endomorphisme $P(f)$ par

$$P(f) = \sum_{k=0}^N \alpha_k f^k.$$

On vérifie rapidement que l'ensemble des polynômes en un endomorphisme $f \in L(E)$ est une sous-algèbre de $L(E)$ et que l'on a la proposition suivante.

Proposition 1.5. *Soit $f \in L(E)$. L'application qui, à un polynôme $P \in \mathbb{K}[X]$, associe l'endomorphisme $P(f) \in L(E)$ est un morphisme d'algèbres.*

PREUVE. Il suffit de vérifier avec la définition que, pour tout $(P, Q) \in \mathbb{K}[X]^2$ et tout $(\lambda, \mu) \in \mathbb{K}^2$, on a

$$\begin{aligned} 1(f) &= \text{Id}_E \\ (\lambda P + \mu Q)(f) &= \lambda P(f) + \mu Q(f) \\ (PQ)(f) &= P(f) \circ Q(f). \end{aligned}$$

Proposition 1.6. *Soient un endomorphisme $f \in L(E)$ et des polynômes P et Q . Les endomorphismes $P(f)$ et $Q(f)$ commutent. En particulier, $\ker P(f)$ est un sous-espace stable par f pour tout polynôme $P \in \mathbb{K}[X]$.*

PREUVE. Par linéarité, il suffit de vérifier que $f^m \circ f^n = f^n \circ f^m$. ■

Le résultat suivant est essentiel pour la suite de ce chapitre, car il permet de « décomposer » un espace vectoriel en une somme directe de sous-espaces vectoriels adaptés à la réduction des endomorphismes, comme nous le verrons à partir de la section II.3.

Théorème 1.7. *(théorème de décomposition des noyaux)*
Soient $(P_k)_{k \in \{1, \dots, N\}}$ une famille de polynômes deux à deux premiers entre eux et un endomorphisme $f \in L(E)$. Alors,

$$\ker \left(\prod_{k=1}^N P_k \right) (f) = \bigoplus_{k=1}^N \ker P_k(f).$$

De plus, le projecteur de $\ker \left(\prod_{k=1}^N P_k \right) (f)$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f .

PREUVE. Montrons ce résultat par récurrence sur le cardinal $N \geq 2$ de la famille de polynômes :
 ◊ si P_1 et P_2 sont deux polynômes premiers entre eux, le théorème de Bezout (voir la proposition 13.51 du chapitre 13 de *Mathématiques L1*, Pearson Education, 2006) nous assure de l'existence de polynômes U_1 et U_2 tels que $U_1 P_1 + U_2 P_2 = 1$, i.e. tels que $U_1(f) \circ P_1(f) + U_2(f) \circ P_2(f) = \text{Id}$. D'où, pour tout $x \in \ker(P_1 P_2)(f)$, $x = U_1(f) \circ P_1(f)(x) + U_2(f) \circ P_2(f)(x)$ avec $U_1(f) \circ P_1(f)(x) \in \ker P_2(f)$ et $U_2(f) \circ P_2(f)(x) \in \ker P_1(f)$ (en utilisant la commutation des polynômes en f). Par ailleurs, si $x \in \ker P_1(f) \cap \ker P_2(f)$, alors $x = U_1(f) \circ P_1(f)(x) + U_2(f) \circ P_2(f)(x) = 0$. On déduit de ces deux résultats que $\ker P_1(f)$ et $\ker P_2(f)$ sont supplémentaires dans $\ker(P_1 P_2)(f)$;
 ◊ Soit $N \geq 2$. Supposons que le théorème est établi pour toute famille de N polynômes deux à deux premiers entre eux. Soit $(P_k)_{k \in \{1, \dots, N+1\}}$ une famille de polynômes deux à deux premiers entre eux. Alors $\prod_{k=1}^N P_k$ et P_{N+1} sont premiers entre eux, et l'on peut appliquer le théorème à cette famille de deux polynômes ; d'où

$$\ker \left(\prod_{k=1}^{N+1} P_k \right) (f) = \ker \prod_{k=1}^N P_k(f) \oplus \ker P_{N+1}(f).$$

Il suffit désormais d'utiliser l'hypothèse de récurrence pour conclure à la décomposition. Revenons à une famille $(P_k)_{k \in \{1, \dots, N\}}$ de polynômes deux à deux premiers entre eux. Puisque P_j et $\prod_{k=1, k \neq j}^N P_k$ sont premiers entre eux, il existe des polynômes U_j et V_j tels que $U_j P_j + V_j \prod_{k=1, k \neq j}^N P_k = 1$. Posons $p_j = (V_j \prod_{k=1, k \neq j}^N P_k)(f)$ et vérifions que p_j est bien le projecteur de $\ker \left(\prod_{k=1}^N P_k \right)(f)$ sur $\ker P_j(f)$ parallèlement à $\bigoplus_{k=1, k \neq j}^N \ker P_k(f)$. En effet, tout élément x du noyau de $P_j(f)$ vérifie $x = (U_j P_j)(f)(x) + (V_j \prod_{k=1, k \neq j}^N P_k)(f)(x) = p_j(x)$, et tout élément $y = P_j(f)(x)$ de l'image de $P_j(f)$ satisfait

$$p_j(y) = p_j(P_j(f)(x)) = V_j(f) \circ \left(\prod_{k=1}^N P_k \right)(f)(x) = 0_E.$$

L'endomorphisme p_j coïncide avec le projecteur recherché sur deux sous-espaces supplémentaires, donc est égal à ce projecteur. ■

Test 1.1.

Soient deux polynômes P et Q de pgcd D et un endomorphisme $f \in L(E)$. Établir que $\ker P(f) \cap \ker Q(f) = \ker D(f)$.

Test 1.2.

Soient deux polynômes P et Q de ppcm M et un endomorphisme $f \in L(E)$. Établir que $\ker P(f) + \ker Q(f) = \ker M(f)$.

I.3. Idéal des polynômes annulateurs

Définition 1.8. Soient $f \in L(E)$ et $P \in \mathbb{K}[X]$ non nul.

On dit que P est un polynôme annulateur de f si l'endomorphisme $P(f)$ est l'endomorphisme identiquement nul.

Proposition 1.9. Tout endomorphisme d'un espace vectoriel de dimension finie admet un polynôme annulateur.

PREUVE. Soit f un endomorphisme de E , \mathbb{K} -espace vectoriel de dimension finie n . Alors, la famille $(f^k)_{k \in \{0, \dots, n^2\}}$ comporte $n^2 + 1$ vecteurs de $L(E)$, espace de dimension n^2 : elle est donc liée. Il existe donc $(\alpha_k)_{k \in \{0, \dots, n^2\}} \in \mathbb{K}^{n^2+1}$ non nul tel que

$$\sum_{k=0}^{n^2} \alpha_k f^k = 0_{L(E)}.$$

Remarque. Nous verrons plus loin (théorème 1.30 de Cayley-Hamilton) que l'on peut, dans ce cas, déterminer en fait un polynôme annulateur de degré n (le *polynôme caractéristique*). ■

Test 1.3.

Un endomorphisme peut-il admettre un polynôme annulateur de degré 0 ?

Test 1.4.

Quels endomorphismes admettent un polynôme annulateur de degré 1 ?

Proposition 1.10. *Soit $f \in L(E)$. L'ensemble des polynômes annulateurs de f ou nul jouit de la structure d'idéal de l'anneau $\mathbb{K}[X]$.*

PREUVE. C'est clairement un sous-groupe additif de $\mathbb{K}[X]$. Si P est un polynôme annulateur de f et $Q \in \mathbb{K}[X]$, alors QP est un polynôme annulateur de f ; en effet,

$$(QP)(f) = Q(f) \circ P(f) = Q(f) \circ 0_{L(E)} = 0_{L(E)}. \quad \blacksquare$$

Comme l'anneau $\mathbb{K}[X]$ est euclidien, il est en particulier principal, donc tous les idéaux de $\mathbb{K}[X]$ peuvent être engendrés par un unique polynôme (voir la section III.5. du chapitre 13 de *Mathématiques L1*, Pearson Education, 2006). On en déduit la définition suivante.

Définition 1.11. *Soit $f \in L(E)$ admettant un polynôme annulateur. Le polynôme minimal de f est le polynôme unitaire qui engendre l'idéal des polynômes annulateurs de f .*

Test 1.5.

Déterminer l'ensemble des polynômes annulateurs d'une homothétie, d'un projecteur, d'une symétrie.

Test 1.6.

Montrer que la dérivation usuelle $D : P \mapsto P'$ est un endomorphisme de $\mathbb{K}[X]$ qui n'admet pas de polynôme annulateur.

I.4. Utilisation pratique d'un polynôme annulateur

Proposition 1.12. *Soit $f \in L(E)$ admettant un polynôme annulateur P tel que $P(0) \neq 0$. Alors f est inversible (i.e. $f \in GL(E)$).*

PREUVE. Écrivons $P(X) = \sum_{k=0}^N \alpha_k X^k$ avec $N > 0$ et $\alpha_0 = P(0) \neq 0$. Comme $P(f) = 0_{L(E)}$, on obtient, en isolant le terme en Id_E ,

$$f \circ \left(-\frac{1}{\alpha_0} \sum_{k=1}^N \alpha_k f^{k-1} \right) = \text{Id}_E.$$

D'après la propriété de commutation des polynômes en f , on en déduit que f est inversible et que $f^{-1} = -\frac{1}{\alpha_0} \sum_{k=1}^N \alpha_k f^{k-1}$. ■

EXEMPLE 1.13. Soit f un endomorphisme de E qui vérifie $(f - 2\text{Id}) \circ (f - 3\text{Id}) = 0$ sans être une homothétie. Cherchons les réels λ tels que $h_\lambda = f - \lambda\text{Id}$ soit non inversible (nous verrons plus loin que ces réels sont les valeurs propres de f). Comme le polynôme $(X - 2)(X - 3)$ est annulateur de f , on en déduit que $(X + \lambda - 2)(X + \lambda - 3)$ est annulateur de h_λ . Donc, si $\lambda \notin \{2, 3\}$, l'endomorphisme h_λ est inversible car son polynôme annulateur n'admet pas 0 pour racine. En revanche, ni h_2 , ni h_3 ne sont inversibles car, sinon, l'autre est nul (et donc f est une homothétie) puisque $h_2 \circ h_3 = 0$.

La réciproque du résultat précédent est évidemment fautive avec un polynôme annulateur quelconque. En revanche, la situation est plus claire avec le polynôme minimal, comme le détaille la proposition suivante.

Proposition 1.14. *Soit $f \in L(E)$ admettant un polynôme annulateur. f est inversible si et seulement si 0 n'est pas racine de son polynôme minimal.*

PREUVE. Avec la proposition précédente, il suffit d'étudier le sens direct. Supposons que f soit inversible et que 0 soit racine du polynôme minimal P de f , i.e. $P = XQ$. On en déduit $f \circ Q(f) = 0_{L(E)}$, or f est inversible et, par conséquent, $Q(f) = 0_{L(E)}$, ce qui contredit la minimalité de P . Par conséquent, 0 n'est pas racine du polynôme minimal. ■

Proposition 1.15. *Soit un endomorphisme $f \in L(E)$ admettant un polynôme annulateur de degré N . Alors, pour tout entier $m \in \mathbb{N}$, $f^m \in \text{vect}(f^k)_{k \in \{0, \dots, N-1\}}$, c'est-à-dire l'endomorphisme f^m est une combinaison linéaire des $(f^k)_{k \in \{0, \dots, N-1\}}$.*

PREUVE. Soient $f \in L(E)$ de polynôme annulateur P de degré N et $m \in \mathbb{N}$. D'après la division euclidienne dans $\mathbb{K}[X]$, il existe $(Q_m, R_m) \in \mathbb{K}[X]^2$ tel que

$$X^m = Q_m(X).P(X) + R_m(X),$$

avec $\deg(R_m(X)) < \deg(P(X))$. En évaluant cette identité en f , on trouve que $f^m = R_m(f)$, d'où le résultat. ■

En fait, on peut aussi utiliser en pratique la démonstration de ce résultat pour obtenir l'expression explicite de f^m pour tout entier $m \in \mathbb{N}$. Il suffit pour cela de savoir obtenir le reste dans une division de polynôme. Détaillons les calculs dans un cas particulier.

EXEMPLE 1.16. Soient $(a, b) \in \mathbb{C}^2$ avec $a \neq b$ et f un endomorphisme dont un polynôme annulateur est $P(X) = (X - a)(X - b)$. Déterminons f^m pour tout entier $m \in \mathbb{N}$. Le reste de la division euclidienne de X^m par P est un polynôme de degré au plus 1, que nous noterons $\alpha_m X + \beta_m$. Reste à déterminer les valeurs des complexes α_m et β_m . Pour cela, précisons la relation de division euclidienne en a et en b :

$$\begin{cases} a^m = a.\alpha_m + \beta_m \\ b^m = b.\alpha_m + \beta_m. \end{cases}$$

En conclusion, $f^m = \frac{a^m - b^m}{a - b}f + \frac{b.a^m - a.b^m}{b - a}\text{Id}_E$.

Méthode

Calculer les puissances d'un endomorphisme

On procède en déterminant le reste dans la division euclidienne du polynôme X^m par un polynôme annulateur de f (de degré aussi petit que possible). Ensuite, il suffit d'appliquer le morphisme d'algèbre entre polynômes et polynômes en f pour retrouver l'expression de f^m .

Test 1.7.

Soit f un endomorphisme de polynôme annulateur $(X - a)^2$.
Déterminer les puissances de f .

Test 1.8.

Montrer que, si l'endomorphisme f d'un espace de dimension finie est inversible, alors f^{-1} est un polynôme en f .

II. RÉDUCTION DES ENDOMORPHISMES, DES MATRICES**II.1. Éléments propres**

Définition 1.17. Soit f un endomorphisme de E .

- Une valeur propre λ de f est un scalaire tel que $f - \lambda \text{Id}$ ne soit pas injective, i.e. tel qu'il existe $x \in E$ non nul qui satisfait $f(x) = \lambda x$.
- Un vecteur propre de f associé à la valeur propre λ est un vecteur x non nul tel que $f(x) = \lambda x$.
- Le sous-espace propre de f associé à la valeur propre λ est le sous-espace $\ker(f - \lambda \text{Id})$.

On remarquera que le sous-espace propre de f associé à la valeur propre λ contient exactement 0 et les vecteurs propres de f associés à λ .

Proposition 1.18. Des vecteurs propres associés à des valeurs propres deux à deux distinctes forment une famille libre.

EXEMPLE 1.19. Pour tout réel a , la fonction $x \mapsto e^{ax}$ est un vecteur propre de la dérivation (qui est un endomorphisme de $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$). Par conséquent, pour tout n -uplet de réels deux à deux distincts (a_1, \dots, a_n) , la famille $(x \mapsto e^{a_i x})_{i \in \{1, \dots, n\}}$ est libre.

PREUVE. Procédons par récurrence sur le cardinal N de la famille de vecteurs propres considérée :

- si $N = 1$, alors la famille ne contient qu'un vecteur qui est non nul (car vecteur propre), donc la famille est libre ;
- soit $N \in \mathbb{N}^*$; supposons que toute famille de N vecteurs propres associés à des valeurs propres deux à deux distinctes soit libre, et considérons (x_1, \dots, x_{N+1}) une famille de $N + 1$ vecteurs propres associés aux valeurs propres deux à deux distinctes $\lambda_1, \dots, \lambda_{N+1}$.

Soit $(\alpha_1, \dots, \alpha_{N+1}) \in \mathbb{K}^{N+1}$. Si $\sum_{i=1}^{N+1} \alpha_i x_i = 0_E$, alors $f\left(\sum_{i=1}^{N+1} \alpha_i x_i\right) = 0_E$, c'est-à-dire

$\sum_{i=1}^{N+1} \lambda_i \alpha_i x_i = 0_E$. En combinant ces deux relations, on trouve

$$\sum_{i=1}^N (\lambda_{N+1} - \lambda_i) \alpha_i x_i = 0_E.$$

D'après notre hypothèse de récurrence, pour tout $i \in \{1, \dots, N\}$, $\alpha_i = 0$ (car $\lambda_{N+1} \neq \lambda_i$ par hypothèse). On en déduit que α_{N+1} est également nul car x_{N+1} est non nul, d'où la liberté. ■

Corollaire 1.20. Soit E un espace vectoriel de dimension finie n . Tout endomorphisme de E admet au plus n valeurs propres distinctes.

PREUVE. Une famille constituée de vecteurs propres associés à chacune des valeurs propres est libre (d'après la proposition précédente), et de cardinal égal au nombre de valeurs propres distinctes. Or le cardinal d'une famille libre est inférieur ou égal à la dimension de l'espace, d'où le résultat. ■

Remarque. Le nombre de valeurs propres d'un endomorphisme d'un espace vectoriel de dimension infinie n'est pas borné, comme on peut le voir avec les exemples suivants :

- l'endomorphisme φ de $\mathbb{K}[X]$ défini par $\varphi(P) = XP'$ admet tous les entiers naturels comme valeur propre puisque, pour tout $n \in \mathbb{N}$, $\varphi(X^n) = nX^{n-1}$;
- l'endomorphisme dérivation de l'espace des fonctions réelles indéfiniment dérivables $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ admet tous les réels comme valeur propre ; en effet, pour tout $a \in \mathbb{R}$, $t \mapsto e^{at}$ est un vecteur propre associé à la valeur propre a .

Proposition 1.21. *Des sous-espaces propres associés à des valeurs propres deux à deux distinctes sont en somme directe.*

PREUVE. Soient $E_{\lambda_1}, \dots, E_{\lambda_N}$ des sous-espaces propres associés à des valeurs propres deux à deux distinctes $\lambda_1, \dots, \lambda_N$. Soit x un élément de la somme de ces sous-espaces propres ; supposons que x admette deux décompositions distinctes sur cette somme :

$$x = \sum_{k=1}^N x_k = \sum_{k=1}^N x'_k.$$

Alors $\sum_{k=1}^N (x_k - x'_k) = 0_E$; or chacun des termes de cette somme est soit nul, soit un vecteur propre.

D'après la dernière proposition, $x_k - x'_k = 0$ pour tout $i \in \{1, \dots, N\}$ (sinon on aurait trouvé une combinaison linéaire nulle non triviale de vecteurs propres associés à des valeurs propres deux à deux distinctes). On obtient l'unicité de la décomposition de x et, par conséquent, que les espaces $E_{\lambda_1}, \dots, E_{\lambda_N}$ sont en somme directe. ■

EXEMPLE 1.22. Dans $E = \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$, le sous-espace vectoriel \mathcal{P} des fonctions paires et le sous-espace vectoriel \mathcal{I} des fonctions impaires sont en somme directe. En effet, ce sont les sous-espaces propres associés aux valeurs propres 1 et -1 de l'endomorphisme de E défini par $f \mapsto \hat{f}$ où $\hat{f} : x \mapsto f(-x)$.

Remarque. Remarquons quelques liens entre sous-espaces propres et sous-espaces stables :

- ◊ un sous-espace propre est un sous-espace stable, et même, plus généralement, tout sous-espace vectoriel d'un sous-espace propre est un sous-espace stable ;
- ◊ la réciproque est évidemment fautive (il suffit de considérer tout l'espace, par exemple) ; en revanche, une droite vectorielle est stable si et seulement si elle est engendrée par un vecteur propre.

Proposition 1.23. *Soit f un endomorphisme admettant un polynôme annulateur. Les valeurs propres de f appartiennent à l'ensemble des racines d'un polynôme annulateur de f .*

PREUVE. Soient f un endomorphisme de polynôme annulateur P , λ une valeur propre de f et x un vecteur propre associé à λ . On a, pour tout $k \in \mathbb{N}$, $f^k(x) = \lambda^k x$ par une récurrence immédiate.

Par conséquent, $P(f)(x) = P(\lambda)x$. Comme P est annulateur de f , on trouve $P(\lambda)x = 0_E$ puis $P(\lambda) = 0$ car x est non nul (car vecteur propre). ■

Attention**La réciproque est bien évidemment fausse**

En effet, étant donné un polynôme annulateur, on peut trouver un polynôme annulateur admettant d'autres racines arbitrairement choisies. En revanche, on verra que, en dimension finie, il existe un polynôme privilégié (le polynôme caractéristique) dont toutes les racines sont valeurs propres de l'endomorphisme associé.

Cette dernière proposition nous donne une méthode efficace pour déterminer les valeurs propres d'un endomorphisme lorsqu'on connaît un polynôme annulateur. La section suivante sera consacrée à un polynôme annulateur particulier que l'on saura déterminer : le polynôme caractéristique.

Méthode**Détermination des éléments propres**

Pour éviter le calcul des valeurs propres *via* la résolution d'un système linéaire, on peut procéder en trois temps : recherche d'un polynôme annulateur simple, calcul des racines de ce polynôme, vérification que les racines trouvées sont effectivement valeurs propres.

Une fois les valeurs propres connues, il suffit de résoudre un système linéaire pour lequel on dispose de la méthode du pivot de Gauss (voir la section III du chapitre 16 de *Mathématiques L1*, Pearson Education, 2006)

Test 1.9.

Quelles sont les valeurs propres d'un projecteur ? d'une symétrie ?

Test 1.10.

Soit f un endomorphisme de \mathbb{R}^3 de polynôme

annulateur $X^3 - 5X^2 + 8X - 4$. Montrer que les valeurs propres de f sont strictement positives.

Test 1.11.

Montrer que les racines du polynôme minimal de l'endomorphisme f (s'il existe) sont les valeurs propres de f .

Remarque. La définition des éléments propres donnée dans cette section repose sur des idées algébriques. Toutefois, il serait trop restrictif de se limiter à ces considérations tant ces notions sont riches. En géométrie, les vecteurs propres représentent des directions privilégiées. Cela découle directement de la notion physique d'axes de rotation propre d'un solide en mécanique ou des quantifications en atomistique, mais aussi de l'analyse en composantes principales de données statistiques.

Dorénavant (jusqu'à la fin du chapitre), nous nous limiterons à l'étude de la réduction en dimension finie ; par conséquent, E est désormais de *dimension finie*.

Par ailleurs, nous donnons les définitions pour les matrices et les endomorphismes, mais adoptons une présentation en termes d'endomorphisme (et non de matrice) pour simplifier l'écriture des démonstrations. Les résultats équivalents pour les matrices seront résumés dans un encadré synthèse à la fin de chaque paragraphe.

II.2. Polynôme caractéristique

Définition 1.24. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . Le polynôme caractéristique de f est le polynôme χ_f défini par $\chi_f(X) = \det(f - X\text{Id})$. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Le polynôme caractéristique de A est le polynôme χ_A défini par $\chi_A(X) = \det(A - X\text{Id})$.

Remarque. D'après les propriétés du déterminant (voir la proposition 20.9. du chapitre 20 de Mathématiques L1, Pearson Education, 2006), $\chi_A = \chi_{P^{-1}AP}$ et, par conséquent, le polynôme caractéristique d'un endomorphisme f est le polynôme caractéristique de n'importe laquelle de ses matrices.

L'un des intérêts de ce polynôme est la recherche des valeurs propres comme l'indique la proposition suivante.

Proposition 1.25. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . Les racines de χ_f sont exactement les valeurs propres de f .

PREUVE. λ est une racine de χ_f si et seulement si $\det(f - \lambda\text{Id}) = 0$, c'est-à-dire si et seulement si $f - \lambda\text{Id}$ n'est pas inversible, ce qui est la définition de λ valeur propre. ■

Ce résultat implique en particulier que le polynôme minimal et le polynôme caractéristique ont les mêmes racines. Il est donc important de comprendre la multiplicité de celles-ci pour mettre en évidence la différence entre ces deux polynômes dans l'étude de la réduction.

Définition 1.26. La multiplicité d'une valeur propre λ d'un endomorphisme f d'un espace vectoriel de dimension finie est sa multiplicité en tant que racine du polynôme caractéristique χ_f .

Puisque les valeurs propres d'un endomorphisme coïncident exactement avec les racines de son polynôme caractéristique, on obtient l'expression suivante des coefficients du polynôme caractéristique.

Proposition 1.27. Soient f un endomorphisme d'un espace vectoriel de dimension finie n et $(\lambda_k)_{k \leq n}$ les valeurs propres de f comptées avec leur multiplicité. Notons $\chi_f = \sum_{k=0}^n a_k X^k$ le polynôme caractéristique de f que l'on suppose scindé. Alors les coefficients sont $a_n = (-1)^n$ et

$$\forall 0 < k \leq n, \quad a_{n-k} = (-1)^{n-k} \sum_{1 \leq j_1 < \dots < j_k \leq n} \prod_{i=1}^k \lambda_{j_i}.$$

PREUVE. La valeur de a_n se déduit du développement par la règle de Sarrus du déterminant définissant le polynôme caractéristique. Les autres coefficients s'obtiennent en utilisant les relations entre coefficients et racines d'un polynôme. ■

Remarque. Ces formules s'avèrent en général peu maniables. Toutefois, un cas particulier important de cette proposition est obtenu en considérant les endomorphismes f d'un espace vectoriel de dimension 2; en effet, le polynôme caractéristique de f est alors $\chi_f(X) = X^2 - \text{tr}(f)X + \det(f)$.

Définition 1.28. Soient f un endomorphisme d'un espace vectoriel de dimension finie et λ une valeur propre de f de multiplicité m_λ . Le sous-espace caractéristique de f associé à la valeur propre λ est $\ker(f - \lambda \text{Id})^{m_\lambda}$.

Proposition 1.29. Soient f un endomorphisme d'un espace vectoriel de dimension finie et λ une valeur propre de f . Le sous-espace caractéristique de f associé à la valeur propre λ est stable par f .

PREUVE. Ces sous-espaces sont stables par f , car ce sont les noyaux de polynômes en f qui commutent donc avec f (proposition 1.6). ■

Remarque. Puisque les noyaux itérés d'un endomorphisme forment une suite croissante d'espaces vectoriels, on remarque que le sous-espace propre associé à une valeur propre λ est inclus dans le sous-espace caractéristique associé à λ . On utilisera plus ou moins directement (dans la section consacrée à la trigonalisation) les autres noyaux itérés qui jouent un rôle intermédiaire entre sous-espace propre et sous-espace caractéristique.

Pour comprendre le rôle important des sous-espaces caractéristiques pour la réduction, expliquons que le polynôme caractéristique est annulateur :

Théorème 1.30. (Cayley-Hamilton)
Soit f un endomorphisme d'un espace vectoriel de dimension finie. Le polynôme caractéristique de f est annulateur de f .

PREUVE. Soient $x \in E$, F_x le plus petit sous-espace vectoriel stable par f et contenant x (c'est-à-dire le sous-espace engendré par la famille $(f^k(x))_{k \in \mathbb{N}}$, d'après la proposition 1.2) et \tilde{f} l'endomorphisme induit par f sur F_x . Nous allons d'abord montrer que $\chi_{\tilde{f}}(f)(x) = 0$, puis que $\chi_{\tilde{f}}$ divise χ_f , ce qui montrera que $\chi_f(f)(x) = 0$.

Soit $p = \dim F_x$. Par construction, $\mathcal{B} = (f^k(x))_{k \leq p-1}$ est une base de F_x et $f^p(x)$ admet une décomposition que l'on note $f^p(x) = \sum_{k=0}^{p-1} a_k f^k(x)$. Écrivons la matrice \tilde{A} de \tilde{f} dans la base \mathcal{B} .

Rappelons que les vecteurs colonnes de \tilde{A} sont les images par f des vecteurs de la base. Il en découle que

$$\tilde{A} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & a_0 \\ 1 & \ddots & & & \vdots & a_1 \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & a_{p-1} \end{pmatrix},$$

et son polynôme caractéristique est $\chi_{\tilde{f}}(X) = (-1)^p \left[X^p - \sum_{k=0}^{p-1} a_k X^k \right]$ (voir l'exemple 1.32). La décomposition de $f^p(x)$ sur la base \mathcal{B} entraîne que $\chi_{\tilde{f}}(f)(x) = 0$. D'après le théorème de la base incomplète (théorème 18.22 de *Mathématiques L1*, Pearson Education, 2006), on peut compléter la base \mathcal{B} en une base $(x, f(x), \dots, f^{p-1}(x), e_{p+1}, \dots, e_n)$ de E . Dans cette base, la matrice A de f sera de la forme

$$A = \begin{pmatrix} \tilde{A} & A_{12} \\ 0 & A_{22} \end{pmatrix},$$

où A_{22} est une matrice carrée de taille $n-p$ (A est triangulaire par blocs). Le déterminant d'une telle matrice est le produit des déterminants des blocs diagonaux (voir l'exercice 20.4 du chapitre 20 de *Mathématiques L1*, Pearson Education, 2006). Il en découle que $\chi_f(X) = \chi_{\tilde{f}}(X) \cdot \chi_{A_{22}}(X)$. Comme $\chi_{\tilde{f}}(f)(x) = 0$, on a $\chi_f(f)(x) = \chi_{A_{22}}(f) \circ \chi_{\tilde{f}}(f)(x) = 0$. Cette relation étant vraie pour tout $x \in E$, on a bien $\chi_f(f) = 0$. ■

Corollaire 1.31. *Soit f un endomorphisme d'un espace vectoriel de dimension finie E , de polynôme caractéristique scindé. Alors E est la somme directe des sous-espaces caractéristiques de f . En particulier, la dimension d'un sous-espace caractéristique est égale à la multiplicité de la valeur propre.*

PREUVE. Le premier point est une application du théorème des noyaux (théorème 1.7) au polynôme χ_f .

Notons F_λ le sous-espace caractéristique de f associé à la valeur propre λ . L'endomorphisme induit par $f - \lambda \text{Id}$ sur F_λ est nilpotent d'indice m_λ , donc la dimension n_λ de F_λ est inférieure ou égale à m_λ et le polynôme caractéristique de $f|_{F_\lambda}$ est $(X - \lambda)^{n_\lambda}$. On déduit de la décomposition en somme directe que le polynôme caractéristique de f est le produit des polynômes caractéristiques de $f|_{F_\lambda}$ pour λ valeur propre de f . En identifiant, on trouve que $n_\lambda = m_\lambda$. ■

Maintenant que l'on a commencé à expliquer l'utilité du polynôme caractéristique, il convient de s'arrêter un instant sur les méthodes à mettre en œuvre pour le calculer et, plus généralement, sur les propriétés de ces coefficients.

◇ En revenant à la définition du polynôme caractéristique, sa détermination peut se réduire à un calcul de déterminant ; malheureusement, avec la règle de Sarrhus, ce calcul s'avère d'une complexité exponentielle (pour une définition précise de ces notions, voir le chapitre 5.) en la dimension de l'espace (ou, de manière équivalente, en la taille de la matrice). Cette approche coûteuse sur le plan calculatoire permet toutefois d'exprimer les coefficients du polynôme caractéristique à l'aide des mineurs de la matrice considérée (et, donc, de vérifier leur régularité comme fonctions des coefficients). On peut parvenir à un meilleur résultat en utilisant le pivot de Gauss (dont la complexité est de l'ordre du cube de la dimension de la matrice).

◇ Une alternative à ce calcul est donnée par l'algorithme de Souriau-Faddeev (également attribué à Le Verrier), dont on vérifie aisément qu'il est de complexité polynomiale.

On définit par récurrence la suite finie de matrices par : $M_0 = M$ et, pour tout $k \leq n-1$,

$$M_{k+1} = M(M_k - \frac{1}{k+1} \text{tr}(M_k)I_n).$$

Une fois ces calculs effectués, on retrouve le polynôme caractéristique de M comme

$$\chi_M(X) = (-1)^n \left[X^n - \sum_{k=1}^n \frac{1}{k} \text{tr}(M_{k-1})X^{n-k} \right].$$

En effet, si l'on note $\chi_M(X) = \sum_{k=0}^n a_k X^k$, l'expression des coefficients a_k en terme de polynôme symétrique en les valeurs propres $(\lambda_i)_{i \leq n}$ peut être réécrite en utilisant les sommes de Newton définies par $\Sigma_k = \sum_{i=1}^n \lambda_i^k = \text{tr}(M^k)$ pour $k \leq n$:

$$\forall k \leq n, \quad \sum_{j=1}^k a_{k-j} \Sigma_j = 0.$$

Il suffit ensuite de montrer, par récurrence sur $k \leq n$, que $\text{tr}(M_{k-1}) = a_{n-k}$.

Remarque. Nous avons déjà vu que les coefficients du polynôme caractéristique s'exprimaient à l'aide des valeurs propres, et l'on peut penser que cela fournit une méthode pour déterminer le polynôme caractéristique. Toutefois, cette approche n'est en général pas utile pour déterminer χ_f , car on cherche souvent le polynôme caractéristique pour obtenir les valeurs propres, et non l'inverse.

EXEMPLE 1.32. Reprenons l'exemple de la preuve du théorème de Cayley-Hamilton.

On appelle « matrice compagnon » ou « matrice de Fröbenius » d'un polynôme $P(X) =$

$$(-1)^n \left[X^n - \sum_{k=0}^{n-1} a_k X^k \right] \text{ la matrice } \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & a_0 \\ 1 & \ddots & & & \vdots & a_1 \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}.$$

Le polynôme caractéristique $\Delta(a_0, \dots, a_{n-1})(X)$ d'une telle matrice peut se calculer facilement en développant par rapport à la première ligne ou la première colonne : on trouve alors

$$\begin{aligned} \Delta(a_0, \dots, a_{n-1})(X) &= (-1)^{n+1} a_0 - X \cdot \Delta(a_1, \dots, a_{n-1})(X) \\ &= (-1)^n (-a_0 + X \cdot \Delta(a_1, \dots, a_{n-1})(X)), \end{aligned}$$

d'où $\Delta(a_0, \dots, a_{n-1})(X) = P$. On a donc montré que le polynôme caractéristique de la matrice compagnon de P était P .

Un corollaire direct de ce calcul est que tout polynôme dont le monôme dominant est $(-1)^n X^n$ est le polynôme caractéristique d'un endomorphisme (d'une matrice).

Synthèse

Récapitulatif sommaire en termes de matrices

Le polynôme caractéristique d'une matrice A est défini par $\chi_A(X) = \det(A - XI)$. Ce polynôme est annulateur, et ses racines sont exactement les valeurs propres de A .

Pour toute racine λ du polynôme caractéristique χ_A de multiplicité m_λ , on définit le sous-espace caractéristique associé à λ par $\ker(A - \lambda I)^{m_\lambda}$. Le sous-espace caractéristique associé à λ est stable par f et de dimension m_λ .

De plus, si le polynôme caractéristique est scindé, \mathbb{K}^n est somme directe des sous-espaces caractéristiques et A est semblable à une matrice diagonale par blocs.

II.3. Critères de diagonalisation

Commençons par un bref rappel de calcul matriciel.

Rappel

Les vecteurs colonnes d'une matrice sont les images des vecteurs de la base.

En particulier, si la matrice M est diagonale, alors la base canonique est une base de vecteurs propres de M .

Définition 1.33.

- ◇ Une endomorphisme est diagonalisable s'il existe une base dans laquelle sa matrice est diagonale, i.e. s'il existe une base de vecteurs propres pour cet endomorphisme.
- ◇ Une matrice est diagonalisable si et seulement si elle est semblable à une matrice diagonale.

Remarque. Avec cette définition et celle de la relation de similitude, on vérifie immédiatement qu'une matrice est diagonalisable si et seulement si l'application linéaire qui lui est canoniquement associée est diagonalisable. Par conséquent, nous allons énoncer les critères de diagonalisabilité pour les endomorphismes.

L'objectif de ce paragraphe est d'obtenir des conditions nécessaires et/ou suffisantes pour la diagonalisabilité d'un endomorphisme. Commençons par un résultat simple.

Proposition 1.34. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . Si f admet n valeurs propres deux à deux distinctes, alors f est diagonalisable.

PREUVE. Si f admet n valeurs propres deux à deux distinctes, alors une famille de vecteurs propres associés à chacune de ces valeurs propres est libre (d'après la proposition 1.21) et de cardinal n , donc c'est une base. On a trouvé une base de vecteurs propres de f , donc f est diagonalisable. ■

Corollaire 1.35. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . Si son polynôme caractéristique χ_f est scindé à racines simples, alors f est diagonalisable.

PREUVE. Les racines de χ_f sont les valeurs propres de f . L'hypothèse implique que f admet n valeurs propres distinctes, donc est diagonalisable d'après la proposition précédente. ■

Passons désormais à des critères (i.e. des conditions nécessaires et suffisantes) de diagonalisabilité.

Théorème 1.36. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . Alors f est diagonalisable si et seulement si f admet un polynôme annulateur scindé à racines simples.

PREUVE.

(\Rightarrow) Si f est diagonalisable, il existe une base dans laquelle A , la matrice de f , est diagonale. Notons $(\alpha_k)_{k \leq m}$ les éléments diagonaux deux à deux distincts de cette matrice et montrons

que le polynôme $\prod_{k=1}^m (X - \alpha_k)$ est annulateur de f . Il suffit de montrer que ce polynôme est

annulateur de la matrice A . La matrice $\prod_{k=1}^m (A - \alpha_k I)$ est le produit de matrices diagonales,

donc est la matrice diagonale dont le terme en position i, i est obtenu en effectuant les produits des éléments en position i, i des matrices $(A - \alpha_k I)_{k \leq m}$. Or, pour tout $i \leq n$, il existe au moins une matrice $A - \alpha_k I$ dont le coefficient en position i, i est nul. Par

conséquent, la matrice $\prod_{k=1}^m (A - \alpha_k I)$ est nulle.

(\Leftrightarrow) Soit $P(X) = \prod_{k=1}^m (X - \lambda_k)$ (avec $\lambda_k \neq \lambda_j$ dès que $k \neq j$) un polynôme annulateur de f scindé à racines simples. Puisque les complexes $(\lambda_k)_{1 \leq k \leq m}$ sont deux à deux distincts, les polynômes $(X - \lambda_k)_{1 \leq k \leq m}$ sont deux à deux premiers entre eux. En appliquant le théorème des noyaux (théorème 1.7), on obtient la décomposition de E comme somme directe de sous-espaces propres de $f : E = \bigoplus_{k=1}^m \ker(f - \lambda_k \text{Id})$. Par conséquent, f est diagonalisable. ■

EXEMPLE 1.37. Les projecteurs et les symétries sont diagonalisables, car ils admettent des polynômes annulateurs scindés à racines simples (respectivement $X^2 - X$ et $X^2 - 1$).

Test 1.12.

Que dire d'un endomorphisme nilpotent et diagonalisable ?

Test 1.13.

À quelle condition un endomorphisme de rang 1 est-il diagonalisable ?

Test 1.14.

Un endomorphisme f tel que $f^2 = -\text{Id}$ est-il diagonalisable ?

Test 1.15.

À quelle condition un endomorphisme dont la matrice dans une base est triangulaire avec des coefficients diagonaux égaux à 1 est-il diagonalisable ?

Test 1.16.

Soient f un endomorphisme diagonalisable et F un sous-espace stable pour f . Montrer que \tilde{f} l'endomorphisme induit par f sur F est un endomorphisme de F diagonalisable.

Théorème 1.38. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . f est diagonalisable si et seulement si son polynôme caractéristique χ_f est scindé et si la dimension de chaque sous-espace propre est égale à la multiplicité de la valeur propre correspondante dans χ_f .

PREUVE. D'après le théorème de décomposition des noyaux (théorème 1.7) et le théorème de Cayley-Hamilton (théorème 1.30), E est la somme directe des sous-espaces caractéristiques. Or chaque sous-espace caractéristique contient le sous-espace propre associé à la même valeur propre. Par conséquent, E est la somme directe des sous-espaces propres *si et seulement si* les sous-espaces propres et caractéristiques associés à une même valeur propre sont égaux (*i.e.* s'ils ont même dimension). On trouve le résultat annoncé en rappelant que la dimension d'un sous-espace caractéristique est égale à la multiplicité de la valeur propre associée. ■

Corollaire 1.39. Soit $f \in L(E)$ un endomorphisme d'un espace vectoriel de dimension n . f est diagonalisable si et seulement si la somme des dimensions des sous-espaces propres est égale à n .

PREUVE. La somme des dimensions des sous-espaces propres est inférieure à la somme des dimensions des sous-espaces caractéristiques (qui vaut n). L'égalité n'est possible que si chaque espace propre a la même dimension que l'espace caractéristique associé. Le résultat provient de la proposition précédente. ■

Synthèse

Récapitulatif sommaire en termes de matrices

Soit $A \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique χ_A .

Chacune des conditions suivantes est nécessaire et suffisante pour que la matrice A soit diagonalisable :

- ◇ χ_A est scindé et la dimension de chaque sous-espace caractéristique est égale à la multiplicité de la valeur propre correspondante ;
- ◇ A admet un polynôme annulateur scindé à racines simples ;
- ◇ la somme des dimensions des sous-espaces propres est égale à n .

Chacune des conditions suivantes est suffisante pour que la matrice A soit diagonalisable :

- ◇ A admet n valeurs propres deux à deux distinctes ;
- ◇ χ_A est scindé à racines simples.

II.4. Critère de codiagonalisation

Définition 1.40. Une famille d'endomorphismes $(f_k)_{k \leq N}$ d'un espace de dimension finie E est dite codiagonalisable s'il existe une base de E dans laquelle chacun des endomorphismes f_k pour $k \leq N$ admet une matrice diagonale.

D'après les résultats sur les sous-espaces stables déjà montrés, on sait que les sous-espaces propres d'un endomorphisme sont stables pour tous les endomorphismes commutant avec lui. En fait, ce résultat s'inscrit dans un cadre plus général, et la commutativité entre endomorphismes diagonalisables est une condition nécessaire et suffisante pour la codiagonalisabilité.

Proposition 1.41. Une famille d'endomorphismes diagonalisables $(f_k)_{k \leq N}$ d'un espace de dimension finie E est codiagonalisable si et seulement si pour tout couple $(i, j) \in \llbracket 1, N \rrbracket^2$, f_i et f_j commutent.

PREUVE. S'il existe une base dans laquelle chacun des endomorphismes f_k pour $k \leq N$ admet une matrice diagonale, alors les endomorphismes commutent deux à deux (car deux matrices diagonales commutent).

Réciproquement, montrons par récurrence sur N que, si tous les endomorphismes (d'une famille de N endomorphismes diagonalisables) commutent deux à deux, la famille est alors codiagonalisable. Le résultat est évidemment vrai pour un endomorphisme diagonalisable.

Soit $N \in \mathbb{N}^*$: supposons que toute famille de N endomorphismes diagonalisables qui commutent deux à deux est codiagonalisable, et considérons une famille $(f_i)_{i \leq N+1}$ de $N+1$ endomorphismes qui satisfont ces conditions. Si tous les f_i sont des homothéties, alors le résultat est établi ; sinon, il existe au moins un endomorphisme (que nous supposons être f_{N+1} quitte à réordonner la famille) qui admette au moins deux sous-espaces propres, et donc $E = E_{N+1} \oplus F$ avec E_{N+1} un sous-espace propre de f_{N+1} et F la somme des autres sous-espaces propres de f_{N+1} . Chacun de ces deux sous-espaces est stable par $(f_k)_{k \leq N}$: les N endomorphismes induits sur E_{N+1} (respectivement sur F) sont diagonalisables et commutent deux à deux, donc sont codiagonalisables d'après l'hypothèse de récurrence. En concaténant les bases ainsi déterminées de E_{N+1} et de F , on obtient une base de E où chacun des endomorphismes $(f_i)_{i \leq N+1}$ admet une matrice diagonale. ■

Synthèse

Récapitulatif en termes de matrices

Une famille de matrices $(A_k)_{k \leq N}$ est dite codiagonalisable s'il existe une matrice inversible P telle que la famille $(P^{-1}A_k P)_{k \leq N}$ soit constituée de matrices diagonales.

Une famille de matrices diagonalisables est codiagonalisable *si et seulement si* les matrices commutent deux à deux.

II.5. Critères de trigonalisation

Définition 1.42.

- ◇ Une endomorphisme est trigonalisable s'il existe une base dans laquelle sa matrice est triangulaire.
- ◇ Une matrice est trigonalisable si et seulement si elle est semblable à une matrice triangulaire.

Commençons par étudier le cas simple des endomorphismes nilpotents, qui nous serviront ensuite de briques élémentaires pour obtenir la trigonalisation d'un endomorphisme quelconque.

Proposition 1.43. *Soit n un endomorphisme nilpotent d'indice p d'un espace vectoriel E de dimension finie. Il existe une base dans laquelle la matrice de n est triangulaire supérieure avec des zéros sur la diagonale.*

PREUVE. La suite des noyaux itérés $(\ker n^k)_{k < p}$ est strictement croissante pour l'inclusion et $\ker n^p = E$. Dans la base de E associée à cette suite (*i.e.* obtenue en prenant une base de $\ker n$ et en la complétant successivement en une base de $\ker n^2$, puis en complétant la base ainsi obtenue en une base de $\ker n^3 \dots$), la matrice de n est triangulaire supérieure stricte. ■

Théorème 1.44. *Un endomorphisme est trigonalisable si et seulement s'il admet un polynôme annulateur scindé.*

PREUVE. Si l'endomorphisme f est trigonalisable, il existe une base dans laquelle sa matrice est triangulaire. En calculant le polynôme caractéristique de f en se plaçant dans cette base, on trouve que celui-ci est scindé : il est égal au produit des termes $(\alpha_{i,i} - X)$ avec $(\alpha_{i,i})_{i \leq n}$ les termes diagonaux de la matrice de f dans cette base.

Réciproquement, supposons que f admette un polynôme annulateur scindé $\prod_{i=1}^m (X - \lambda_i)^{\alpha_i}$. D'après le théorème de décomposition des noyaux (théorème 1.7), l'espace E est la somme directe des $F_{\lambda_i} = \ker(f - \lambda_i \text{Id})^{\alpha_i}$, et il suffit donc de montrer que l'endomorphisme induit par f sur chacun de ses sous-espaces caractéristiques est trigonalisable. Or, chacun de ces endomorphismes induits est la somme d'une homothétie $\lambda_i \text{Id}$ et d'un endomorphisme nilpotent $f - \lambda_i \text{Id}$. D'après la proposition 1.43, Il existe donc une base de F_{λ_i} telle que $f - \lambda_i \text{Id}$ admette une matrice triangulaire supérieure et que $\lambda_i \text{Id}$ admette une matrice diagonale : l'endomorphisme induit par f sur F_{λ_i} est donc trigonalisable. En concaténant les bases obtenues pour chacun de ces sous-espaces, on obtient une base de E dans laquelle la matrice de f est triangulaire. ■

Corollaire 1.45. *Un endomorphisme sur un \mathbb{C} -espace vectoriel (respectivement une matrice carrée à coefficient dans \mathbb{C}) est trigonalisable.*

PREUVE. Cela est une application directe du résultat ci-dessus, en remarquant que \mathbb{C} est algébriquement clos (théorème de d'Alembert-Gauss, voir la proposition 13.68. du chapitre 13 de *Mathématiques L1*, Pearson Education, 2006), donc que tous les polynômes non constants de $\mathbb{C}[X]$ sont scindés. ■

Dans les démonstrations précédentes, on s'est appuyé sur la décomposition de l'endomorphisme induit par f sur un sous-espace caractéristique comme somme d'une homothétie et d'un endomorphisme nilpotent. Si l'on considère l'endomorphisme dans sa globalité, on obtient la décomposition suivante.

Proposition 1.46. (*décomposition de Jordan-Dunford*)

Soit f un endomorphisme d'un espace vectoriel E de dimension finie annulant un polynôme scindé. Alors, il existe un unique couple d'endomorphismes (d, n) tel que

- $f = n + d$;
- n et d commutent ;
- n est nilpotent ;
- d est diagonalisable.

PREUVE. Montrons dans un premier temps l'existence d'un tel couple.

Nous avons déjà montré dans la preuve précédente que, sous ces hypothèses, $E = \bigoplus_{k=1}^m \ker(f - \lambda_k \text{Id})^{\alpha_k}$ (par application du théorème des noyaux, théorème 1.7) et que l'endomorphisme induit par f sur ces sous-espaces était la somme d'une homothétie d_k et d'un endomorphisme nilpotent n_k . Notons, de plus (toujours d'après le théorème de décomposition des noyaux), que la projection p_i sur $\ker(f - \lambda_i \text{Id})^{\alpha_i}$ parallèlement à $\bigoplus_{k=1, k \neq i}^m \ker(f - \lambda_k \text{Id})^{\alpha_k}$ est un polynôme en f .

Posons enfin $d = \sum_{k=1}^m \lambda_k p_k$ et $n = f - d$, et vérifions les propriétés de la proposition :

- par construction, $f = d + n$;
- d est un polynôme en f , comme somme de polynômes en f donc commute avec f et par conséquent avec $n = f - d$;
- n est nilpotent, car l'endomorphisme induit par n sur chacun des sous-espaces $\ker(f - \lambda_i \text{Id})^{\alpha_i}$ est nilpotent ;
- d est diagonalisable, car sa matrice est diagonale dans une base adaptée à la décomposition $E = \bigoplus_{k=1}^m \ker(f - \lambda_k \text{Id})^{\alpha_k}$.

Montrons maintenant l'unicité de cette décomposition.

Soient (d, n) le couple construit précédemment et (\tilde{d}, \tilde{n}) un couple satisfaisant aux conditions de la proposition. Chacun de ces quatre endomorphismes commute avec f , donc laisse stable les sous-espaces $\ker(f - \lambda_k \text{Id})^{\alpha_k}$ pour $k \leq m$. Notons (d_k, n_k) et $(\tilde{d}_k, \tilde{n}_k)$ les endomorphismes induits par ces endomorphismes sur le sous-espace $\ker(f - \lambda_k \text{Id})^{\alpha_k}$. n_k et \tilde{n}_k commutent et sont tous deux nilpotents, donc leur différence est nilpotente d'indice inférieur ou égal à la somme de leurs indices. Or $n_k - \tilde{n}_k = \tilde{d}_k - \lambda_k \text{Id}$ est diagonalisable. Le seul endomorphisme diagonalisable et nilpotent est l'endomorphisme nul ; d'où $\tilde{d}_k = \lambda_k \text{Id}$ et $n_k = \tilde{n}_k$ et, par conséquent, $d = \tilde{d}$ et $n = \tilde{n}$. ■

Remarque. Dans la preuve de cette décomposition, on a en particulier retrouvé que, si un endomorphisme f est diagonalisable de valeurs propres $(\lambda_i)_{i \leq m}$, alors $f = \sum_{i=1}^m \lambda_i p_i$ avec p_i le projecteur sur le sous-espace propre associé à λ_i parallèlement à la somme des autres.

Remarque. Déduisons de la décomposition de Jordan-Dunford, de la proposition 1.46, une version multiplicative pour les endomorphismes inversibles. Soient f un endomorphisme inversible de E et (d, n) le couple de Jordan. On a alors d inversible et $f = d \circ (\text{Id}_E + d^{-1} \circ n)$ avec :

- ◊ d est diagonalisable ;
- ◊ $\text{Id}_E + d^{-1}n$ est unipotent (*i.e.* somme de l'identité et d'un endomorphisme nilpotent) ;
- ◊ d et $\text{Id}_E + d^{-1}n$ commutent.

On a toujours l'unicité de la décomposition.

EXEMPLE 1.47. La décomposition de Jordan-Dunford de la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est $I + N$ avec

$N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Plus généralement, on obtient la décomposition de Jordan-Dunford en utilisant la preuve, à savoir, en isolant sur chaque sous-espace caractéristique la partie homothétique associée à la valeur propre.

Test 1.17.

Déterminer la décomposition de Jordan-Dunford

de la matrice $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

Test 1.18.

Déterminer la décomposition de Jordan-Dunford

de la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$.

Synthèse

Récapitulatif sommaire en termes de matrices

Une matrice est trigonalisable *si et seulement si* elle annule un polynôme scindé, donc une matrice est toujours trigonalisable dans $\mathcal{M}_n(\mathbb{C})$.

Toute matrice trigonalisable peut se décomposer de manière unique comme la somme de deux matrices qui commutent, et telle que l'une est diagonalisable et l'autre nilpotente.

II.6. Endomorphismes semi-simples

Avertissement : ce paragraphe, de lecture plus ardue, peut être passé en première lecture.

Dans les paragraphes précédents, nous avons adopté une stratégie d'étude centrée sur les polynômes annulateurs, et une propriété fondamentale pour ces résultats est le caractère scindé des polynômes annulateurs. Si le corps de base est \mathbb{C} (ou n'importe quel corps algébriquement clos), tous les polynômes non constants (donc, en particulier, les polynômes annulateurs) sont scindés. En revanche, sur le corps \mathbb{R} , entre autres, la situation est un peu plus compliquée. L'objectif de cette courte partie est de traiter le cas de certains endomorphismes dont aucun polynôme annulateur n'est scindé.

Définition 1.48. *Un endomorphisme d'un espace vectoriel E de dimension finie est dit semi-simple si son polynôme minimal est le produit de polynômes irréductibles deux à deux distincts. On dit que f est simple si E n'admet pas d'autre sous-espace stable que $\{0\}$ et E .*

Test 1.19.

Quels sont les endomorphismes semi-simples d'un \mathbb{C} -espace vectoriel ?

Test 1.20.

Soit f un endomorphisme d'un espace vectoriel de dimension finie. Montrer que, si χ_f est le produit de polynômes irréductibles deux à deux distincts, alors f est semi-simple.

Commençons par un premier résultat sur des endomorphismes semi-simples particuliers, qui nous sera utile dans l'étude générale qui suit.

Proposition 1.49. *Soit f un endomorphisme semi-simple d'un espace vectoriel de dimension finie. Si le polynôme minimal de f est irréductible, alors tout sous-espace stable par f admet un supplémentaire stable par f .*

PREUVE. Soit F un sous-espace stable par f . Notons x_1 un élément du complémentaire de F et $G_1 = \text{Vect}(f^k(x_1))_{k \in \mathbb{N}}$. G_1 est clairement stable par f ; montrons que G_1 est en somme directe avec F . Considérons un élément non nul $y \in F \cap G_1$; il existe un polynôme P tel que $y = P(f)(x_1)$. Notons π_1 le polynôme unitaire qui engendre l'idéal $\{Q \in \mathbb{K}[X], Q(f)(x_1) = 0\}$; ce polynôme est non constant (car $x_1 \neq 0$) et divise le polynôme minimal. Les polynômes P et π_1 sont premiers entre eux, car π_1 est irréductible et ne divise pas P (puisque $y \neq 0$). Le théorème de Bezout nous assure de l'existence de polynômes U et V tels que $UP + V\pi_1 = 1$. Alors $x_1 = U(f)P(f)(x_1) = U(f)(y)$, d'où $x_1 \in F$ car F est stable par f . D'où la contradiction avec la définition de x_1 , et G_1 est en somme directe avec F . Si F et G_1 ne sont pas supplémentaires, on recommence le même procédé en remplaçant F par $F \oplus G_1$. ■

Proposition 1.50. *Un endomorphisme f d'un espace vectoriel de dimension finie est semi-simple si et seulement si tout sous-espace stable par f admet un supplémentaire stable par f .*

PREUVE.

(\Rightarrow) Le polynôme minimal de f se décompose sous forme de produit de polynômes irréductibles deux à deux distincts $(P_i)_{i \leq r}$. Les sous-espaces $F_i = \ker P_i(f)$ vérifient $E = \bigoplus_{i=1}^r F_i$.

Tout sous-espace F stable par f vérifie $F = \bigoplus_{i=1}^r (F \cap F_i)$. Pour chaque $i \leq r$, P_i est alors le polynôme minimal de l'endomorphisme induit par f sur F_i (car il est annulateur et irréductible). On déduit de la proposition précédente qu'il existe un sous-espace vectoriel G_i stable par f , supplémentaire de $F \cap F_i$ dans F_i .

Par conséquent, $G = \bigoplus_{i=1}^r G_i$ est un supplémentaire de F stable par f .

(\Leftarrow) Raisonnons par l'absurde : si le polynôme minimal de f admet un facteur irréductible d'exposant supérieur ou égal à 2, alors il s'écrit $P^2 \cdot Q$. Le sous-espace $F = \ker P(f)$ est un sous-espace stable, donc admet un supplémentaire G stable par f . Montrons que $(PQ)(f)$ est l'endomorphisme nul : $(PQ)(f)$ s'annule clairement sur $\ker P(f)$ et, pour tout $x \in G$, $(PQ)(f)(x) \in G$, car G est stable par f , et $(PQ)(f)(x) \in F$ car P^2Q est annulateur de f . Par conséquent, PQ est un polynôme annulateur de f de degré strictement inférieur au polynôme minimal. D'où la contradiction, et le polynôme annulateur n'admet pas de facteur carré. ■

Proposition 1.51. *Soit f un endomorphisme semi-simple d'un espace vectoriel E de dimension finie. Il existe une décomposition $E = \bigoplus_{k=1}^m E_k$ tel que l'endomorphisme induit par f sur chacun des espaces E_i n'admette que $\{0\}$ et E_i comme sous-espaces stables (i.e. tel que, pour tout $i \leq m$, $f|_{E_i}$ soit simple).*

PREUVE. Le polynôme caractéristique χ_f de f se décompose en produit de polynômes irréductibles deux à deux distincts $\chi_f(X) = \prod_{k=1}^m P_k(X)$. Il suffit désormais de montrer que, pour tout $i \leq m$, f_i , l'endomorphisme induit par f sur $\ker P_i(f)$ est simple. Si F est un sous-espace non trivial de $\ker P_i(f)$ stable par f_i , alors le polynôme minimal de l'endomorphisme induit par f_i sur F divise le polynôme minimal de $f_i : P_i$, ce qui contredit le caractère minimal de P_i . On a donc montré par l'absurde que f_i était simple. ■

Ce dernier résultat de décomposition est relativement important, car on connaît les endomorphismes simples d'un \mathbb{R} ou \mathbb{C} -espace vectoriel :

- il ne peut y avoir d'endomorphisme simple d'un \mathbb{C} -espace vectoriel que si la dimension est 1. On retrouve donc que tout endomorphisme semi-simple d'un \mathbb{C} -espace vectoriel est diagonalisable ;
- il ne peut y avoir d'endomorphisme simple d'un \mathbb{R} -espace vectoriel que si la dimension est 1 ou 2. La proposition montre que les endomorphismes semi-simples admettent, dans une base convenablement choisie, une matrice diagonale par blocs avec des blocs de taille au plus 2.

Remarque. Pour obtenir au paragraphe précédent la décomposition de Jordan-Dunford, on a supposé que l'endomorphisme f annulait un polynôme scindé. Si l'on veut se passer de cette hypothèse, il faut avoir recours aux endomorphismes semi-simples ; on peut alors établir de manière analogue le résultat suivant.

Tout endomorphisme f d'un espace vectoriel E de dimension finie admet une unique décomposition $f = n + d$, avec deux endomorphismes n et d qui commutent tels que n est nilpotent et d est semi-simple.

III. QUELQUES EXEMPLES DE RÉDUCTION POUR L'ANALYSE

Pour terminer ce chapitre, illustrons les méthodes de réduction à travers quelques exemples tirés du cours d'analyse.

III.1. Étude des suites récurrentes linéaires

Recherchons les suites $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ et $(w_n)_{n \in \mathbb{N}}$ définies par $(u_0, v_0, w_0) \in \mathbb{C}^3$ et par la relation de récurrence

$$\forall n \in \mathbb{N} \quad \begin{cases} u_{n+1} = 3u_n + v_n - w_n \\ v_{n+1} = 3v_n + 2w_n \\ w_{n+1} = 3w_n. \end{cases}$$

Pour cela, réécrivons la relation de récurrence sous la forme $X_{n+1} = AX_n$ avec $X_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$

pour tout entier $n \in \mathbb{N}$ et $A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 3 & 2 \\ 0 & 0 & 3 \end{pmatrix}$.

On obtient par une récurrence immédiate que $X_n = A^n X_0$; il reste donc à déterminer A^n . Comme A est triangulaire, le calcul de son polynôme caractéristique est immédiat et l'on trouve $\chi_A(X) = -(X-3)^3$. Posons la division euclidienne de X^n (pour n fixé) par χ_A : $X^n = Q_n(X)\chi_A(X) + a_n X^2 + b_n X + c_n$.

En évaluant X^n et ses dérivées en 3, on vérifie que (a_n, b_n, c_n) satisfait le système suivant :

$$\begin{cases} 9a_n + 3b_n + c_n = 3^n \\ 6a_n + b_n = n3^{n-1} \\ 2a_n = n(n-1)3^{n-2}. \end{cases}$$

D'où $a_n = \frac{n(n-1)}{2}3^{n-2}$, $b_n = (-n^2 + 2n)3^{n-1}$ et $c_n = \frac{1}{2}(n^2 - 3n + 2)3^n$. Par conséquent, le calcul de A^2 nous amène au résultat suivant :

$$\forall n \in \mathbb{N}, \quad A^n = 3^{n-2} \begin{pmatrix} 9 & 3n & n^2 - 4n \\ 0 & 9 & 6n \\ 0 & 0 & 9 \end{pmatrix}.$$

On conclut alors que $u_n = 3^{n-2}(9u_0 + 3nv_0 + (n^2 - 4n)w_0)$, $v_n = 3^{n-1}(3v_0 + 2nw_0)$ et $w_n = 3^n w_0$.

III.2. Un calcul d'exponentielle de matrices

Le paragraphe précédent montre comment la réduction d'une matrice permet de calculer les puissances d'une matrice et, par conséquent, d'en déduire l'expression des suites récurrentes linéaires associées à cette matrice. Une autre utilisation en analyse provient des équations différentielles linéaires, dont on peut exprimer les solutions à l'aide de l'exponentielle de la matrice associée à cette équation.

Rappel

Rappels concernant l'exponentielle de matrices

- ◇ L'exponentielle d'une matrice A est la matrice $\exp A$ définie par $\sum_{k=0}^{\infty} \frac{A^k}{k!}$.
- ◇ La solution du système différentiel $Y'(t) = AY(t)$ de condition initiale $Y(0) = Y_0$ est donnée par $Y(t) = \exp(tA).Y_0$.

Réolvons le système linéaire différentiel $\begin{cases} x'(t) = x(t) + 2y(t) - 2z(t) \\ y'(t) = 2x(t) + y(t) - 2z(t) \\ z'(t) = 2x(t) + 2y(t) - 3z(t) \end{cases}$. Pour cela, utilisons la

réduction de A pour déterminer l'exponentielle de la matrice $A = \begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & -2 \\ 2 & 2 & -3 \end{pmatrix}$.

Le polynôme caractéristique de A est $-(X-1)(X+1)^2$, donc les seules valeurs propres sont

1 et -1 . En calculant les vecteurs propres associés, on trouve $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ pour la valeur propre 1

et $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ pour la valeur propre -1 . Soit P la matrice obtenue en juxtaposant ces trois

vecteurs propres : alors $P^{-1}AP = \text{diag}(1, -1, -1)$ et, par suite, pour tout $n \in \mathbb{N}$, $P^{-1}A^nP = \text{diag}(1, (-1)^n, (-1)^n)$. En particulier,

$$P^{-1}(\exp(tA))P = \sum_{k=0}^{\infty} \frac{t^k}{k!} \text{diag}(1, (-1)^k, (-1)^k) = \text{diag}(e^t, e^{-t}, e^{-t}).$$

Par conséquent, $\exp(tA) = P \text{diag}(e^t, e^{-t}, e^{-t}) P^{-1}$. On en déduit donc les solutions du système linéaire :

$$\begin{cases} x(t) = x_0 e^t & + y_0(e^t - e^{-t}) + z_0(e^{-t} - e^t) \\ y(t) = x_0(e^t - e^{-t}) + y_0 e^t & + z_0(e^{-t} - e^t) \\ z(t) = x_0(e^t - e^{-t}) + y_0(e^t - e^{-t}) + z_0(2e^{-t} - e^t). \end{cases}$$

IV. EXERCICES

1.1. *

Déterminer si les matrices suivantes sont diagonalisables sur \mathbb{R} . Le cas échéant, donner une matrice de passage P correspondante et la matrice diagonale obtenue D .

$$M_1 = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 7 & 0 & 3 \\ -1 & 4 & -1 \\ 1 & 0 & 5 \end{pmatrix} \quad M_4 = \begin{pmatrix} 7 & 0 & 3 \\ -3 & 4 & 5 \\ 1 & 0 & 5 \end{pmatrix}$$

1.2. *

Déterminer une condition sur $(a, b, c) \in \mathbb{C}^3$ pour

que la matrice $A = \begin{pmatrix} 1 & a & b \\ 0 & 3 & c \\ 0 & 0 & 3 \end{pmatrix}$ soit diagonalisable.

1.3. *

Soit a un réel. Posons

$$M_a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ a^2 - a - a - 1 & a^2 + 1 & \end{pmatrix}.$$

Quelles sont les valeurs de a pour lesquelles M_a est diagonalisable ?

1.4. **

Soient E un \mathbb{R} -espace vectoriel de dimension 3 et B une base de E . Pour tout réel c , on considère f_c l'endomorphisme de E dont la matrice dans

la base B est

$$M_c = \begin{pmatrix} c & 0 & c^2 + c - 1 \\ 1 - c & 1 & -c^2 - c + 1 \\ 0 & 0 & 1 - c^2 \end{pmatrix}.$$

1. Calculer le polynôme caractéristique de f_c .
2. Donner les valeurs propres de f_c et leur multiplicité (discuter en fonction des valeurs de c).
3. Déterminer les valeurs de c pour lesquelles f_c est un projecteur. Déterminer, pour chacune de ces valeurs, les éléments caractéristiques de f_c .

1.5. *

Soit A la matrice définie par

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

1. Trouver l'ensemble des valeurs propres de A .
2. En déduire une matrice diagonale D et une matrice inversible P telle que $A = PDP^{-1}$.
3. Expliciter les suites u , v et w définies par les réels u_0, v_0, w_0 et, pour tout $n \in \mathbb{N}$, par les relations de récurrence

$$\begin{cases} u_{n+1} = & 2v_n - w_n \\ v_{n+1} = 3u_n - 2v_n & \\ w_{n+1} = -2u_n + 2v_n + w_n & \end{cases}.$$

1.6. **

Soit $A \in M_n(\mathbb{C})$ de coefficients $(a_{i,j})_{1 \leq i, j \leq n}$.

1. Montrer que, pour toute valeur propre λ de A , il existe $k \in \{1, \dots, n\}$ tel que

$$|\lambda - a_{k,k}| \leq \sum_{j=1, j \neq k}^n |a_{k,j}|.$$

2. Supposons de plus que A soit à diagonale strictement dominante, *i.e.*

$$\forall k \in \{1, \dots, n\}, |a_{k,k}| > \sum_{j=1, j \neq k}^n |a_{k,j}|.$$

Déduire de la question précédente que A est inversible.

1.7. **

Soit n un entier naturel supérieur ou égal à 2.

1. Soit tr l'application linéaire, qui à toute matrice de $\mathcal{M}_n(\mathbb{R})$, associe la somme de ses éléments diagonaux.

- (a) Montrer que $\text{Im tr} = \mathbb{R}$.
- (b) En déduire la dimension de $\ker \text{tr}$.
- (c) Établir que $\mathcal{M}_n(\mathbb{R}) = \ker \text{tr} \oplus \text{Vect}(I)$.

2. Soit f l'application qui, à toute matrice M de $\mathcal{M}_n(\mathbb{R})$, associe $f(M) = M + \text{tr}(M)I$.

- (a) Montrer que f est un endomorphisme de $\mathcal{M}_n(\mathbb{R})$.
- (b) Utiliser la première question pour déterminer les valeurs propres de f . En déduire que f est un automorphisme diagonalisable de $\mathcal{M}_n(\mathbb{R})$.

3. Soit g l'application qui, à toute matrice M de $\mathcal{M}_n(\mathbb{R})$, associe $g(M) = M + \text{tr}(M)J$, où J désigne une matrice non nulle de $\mathcal{M}_n(\mathbb{R})$ dont la trace est nulle.

- (a) Établir que le polynôme $X^2 - 2X + 1$ est un polynôme annulateur de g .
- (b) Montrer que 1 est la seule valeur propre possible de g .
- (c) g est-il diagonalisable ?

1.8. **

Soit $(a, b) \in [0, 1]^2$ tel que $(a, b) \neq (0, 0)$.

Définissons la matrice $A = \begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}$.

1. Déterminer le polynôme caractéristique de A puis les valeurs propres de A .
 A est-elle diagonalisable ?

2. Montrer que, pour tout entier $n \in \mathbb{N}$, la puissance n -ème de A est donnée par

$$\frac{1}{a+b} \begin{pmatrix} b & a \\ b & a \end{pmatrix} + \frac{(1-a-b)^n}{a+b} \begin{pmatrix} a & -a \\ -b & b \end{pmatrix}.$$

3. Montrer que $\frac{1}{a+b} \begin{pmatrix} b & a \\ b & a \end{pmatrix}$ est le produit de $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ par ${}^t X$ où X est un vecteur propre de ${}^t A$.

1.9. **

Considérons la matrice A de coefficients $(a_{i,j})_{i,j \leq n}$, tels que $a_{i,j} = 1$ si $i = n$ ou $j = n$ et $a_{i,j} = 0$ sinon. Déterminer les valeurs propres de A et en déduire que A est diagonalisable.

1.10. ***

Soient A et B deux matrices codiagonalisables. Montrer qu'il existe un polynôme Q tel que $A = Q(B)$.

1.11. ***

Soit $A \in \mathcal{M}_n(\mathbb{R})$ qui admet n valeurs propres deux à deux distinctes, positives ou nulles $(\lambda_i)_{i \leq n}$. On pose $A = PDP^{-1}$ avec $D = \text{diag}(\lambda_i)_{i \leq n}$.

1. Montrer qu'une matrice R vérifie $R^2 = A$ si et seulement si la matrice $S = P^{-1}RP$ vérifie $S^2 = D$.
2. Montrer que $DS = SD$, puis que la matrice S est diagonale.
3. Déterminer les matrices R telles que $R^2 = A$.

1.12. ***

Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que χ_A est scindé si et seulement si χ_{A^2} est scindé à racines positives.

COMPLÉMENT 1. DES GRAPHES ET DES PROBABILITÉS DANS *Google*

Comment *Google* décide de l'importance d'une page web

Après avoir abordé avec une grande généralité la réduction des endomorphismes en dimension finie (et donc des matrices), intéressons-nous à une application pratique spectaculaire de la réduction : l'algorithme de classement des pages du *moteur de recherche Google*, appelé *PageRank*. Cet algorithme, proposé en 1998 par les fondateurs Sergey Brin et Lawrence Page, est l'un des atouts majeurs de l'efficacité de *Google* (même si son importance est moins prépondérante aujourd'hui avec les dernières innovations du groupe).

Pour expliquer le principe de l'algorithme, nous devons modéliser le réseau Internet et étudier comment manipuler l'information structurelle qu'il contient. Ensuite, nous verrons comment réduire la démarche de *Google* à de simples calculs matriciels. Nous détaillerons alors un résultat proche du cours, le théorème de Perron-Frobenius, qui nous donne une estimation de l'asymptotique de la suite des puissances d'une matrice en fonction de ces valeurs propres.

◊ Cela nous permettra de justifier la convergence dans l'algorithme *PageRank*, pièce essentielle du fameux moteur de recherche *Google*.

◊ Ensuite, nous utiliserons une interprétation de marches aléatoires sur le réseau informatique pour étudier des problèmes similaires, comme l'étude asymptotique de processus aléatoires appelés chaînes de Markov.

1.1. Modéliser Internet

Afin de pouvoir développer les outils mathématiques nécessaires à un moteur de recherche aussi performant que *Google*, il convient de répondre à ces trois questions :

- ◊ comment modéliser le réseau Internet ?
- ◊ comment mesurer la pertinence d'une page en fonction d'une requête donnée ?
- ◊ comment renvoyer rapidement la liste des pages pertinentes pour une requête donnée ?

La réponse à la troisième question relève de l'informatique théorique et n'a pas sa place dans ce chapitre. En revanche, les réponses aux deux premières vont nous amener à étudier la clé de voûte du succès de *Google* : le système *PageRank* de classification des pages Internet.

Internet est un graphe

La première chose à faire pour étudier le réseau Internet consiste à en trouver une représentation mathématique. L'objet adapté est alors le graphe dont la définition formelle est la suivante.

Définition 1.52. *Un graphe orienté fini est un couple (E, V) où E est un ensemble fini et V est une partie de E^2 . Un élément de E est appelé sommet du graphe, un élément de V arête du graphe.*

Internet serait donc un graphe dont les sommets sont les pages Internet et une arête un lien d'une page vers une autre.

Changer une page dans l'ensemble du réseau ne change pas la structure du réseau (à condition de préserver les liens). Par conséquent, on peut se ramener à étudier l'ensemble de toutes les arêtes qui est décrit par une matrice à coefficients positifs appelée matrice d'adjacence.

Définition 1.53. *Notons $E = \{x_1, \dots, x_N\}$. La matrice d'adjacence d'un graphe orienté fini (E, V) est la matrice $M \in \mathcal{M}_N(\mathbb{R})$ telle que, pour tout $(i, j) \in \{1, \dots, N\}^2$, $m_{i,j} = 1$ si $(x_i, x_j) \in V$, $m_{i,j} = 0$ sinon.*

L'intérêt de cette matrice apparaît clairement lorsque l'on calcule ses puissances :

Proposition 1.54. Soient M la matrice d'adjacence d'un graphe orienté fini (E, V) et $k \in \mathbb{N}^*$. Le coefficient d'indice (i, j) de M^k est le nombre de suites $(a_u)_{u \leq k}$ telles que $a_1 = x_i$, $a_k = x_j$ et, pour tout $u < k$, $(a_u, a_{u+1}) \in V$. Autrement dit, les coefficients de la puissance k -ième de la matrice d'adjacence dénombrent les chemins de longueur k reliant deux sommets du graphe.

Ces notions sont essentielles en combinatoire mais nous ne les développerons pas davantage, pour nous concentrer sur le modèle du moteur de recherche *Google*.

Méthode

Idée générale

L'idée sous-jacente à l'étude et au stockage d'informations sur le réseau Internet est de considérer le réseau comme un gigantesque graphe où les sommets sont les différentes pages Web (environ 30 milliards de pages) et les arêtes les liens entre ces pages.

Naviguons au hasard sur Internet

Maintenant que nous disposons d'une modélisation du réseau, il faut définir l'importance d'une page. La première idée consiste à considérer qu'une page est importante si de nombreux liens pointent vers elle (ce qui pourrait s'écrire avec la matrice d'adjacence du graphe et de ses puissances). Toutefois, nous affrontons un biais important : un administrateur crapuleux pourrait créer des centaines de liens pointant vers sa page et, ainsi, augmenter l'importance de sa page (sans en augmenter la qualité). Il convient donc de remplacer la matrice d'adjacence par une autre matrice qui décrit le graphe et contient également l'information du nombre total de liens pointant vers chaque page. Aussi introduit-on la matrice L définie par $l_{i,j} = \frac{1}{d_i}$ si la page numérotée i pointe vers la page j , $l_{i,j} = 0$ sinon, où, pour tout $i \leq n$, nous notons d_i le nombre de liens issus de la page numérotée i . Cette matrice présente une propriété très intéressante, car la somme des termes de chacune de ses lignes vaut 1 ; on dit qu'elle est « stochastique ».

Définition 1.55. Soit $M \in \mathcal{M}_n(\mathbb{R})$.

La matrice M est dite stochastique si ses coefficients sont positifs et si, sur chaque ligne, la somme des coefficients est égale à 1.

Essayons d'interpréter cette nouvelle matrice. Pour cela, prenons un singe savant que l'on installe devant un ordinateur. Après s'être familiarisé avec la souris, notre singe commence à cliquer gaiement d'une page vers une autre. Comme il ne sait pas lire, il clique aléatoirement : si la page sur laquelle il se trouve comporte d liens, il choisira chacun des liens avec la même probabilité $\frac{1}{d}$. Plus précisément, notons (x_i) les pages du réseau et X_n la n -ième page visitée par le singe.

Anticipant sur le chapitre de probabilités, notons $P(X_n = x_i)$ la probabilité pour la n -ième page visitée, soit la page x_i .

Alors puisque notre singe navigue au hasard, on aura

$$P(X_{n+1} = x_i) = \sum_j l_{i,j} P(X_n = x_j). \quad (1.1)$$

En effet, s'il se trouve sur une page qui ne pointe pas vers x_j , il n'a aucune chance d'y atterrir en un clic ; s'il est sur une page qui comporte d_i liens (dont l'un vers la page x_j), il ira avec la probabilité $\frac{1}{d_i}$. Abandonnons-le un instant pour regarder de plus près la relation (1.1). En introduisant, pour tout $n \in \mathbb{N}$, le vecteur U_n de coordonnées $(P(X_n) = x_i)_i$, la relation (1.1) se traduit matriciellement par $U_{n+1} = LU_n$. Nous avons vu à la fin du chapitre 1 que cela

impliquait $U_n = L^n U_0$, et qu'il était important de connaître des informations sur les valeurs propres de L pour obtenir l'asymptotique de la suite (vectorielle) $(U_n)_n$.

Synthèse

Mesure de l'importance d'une page

On considère qu'une page est importante si de nombreux liens pointent vers elle. Pour éviter les fraudes, on modifie la matrice d'adjacence pour une nouvelle matrice L qui prend en compte le nombre de liens. Cette matrice L se trouve aussi être une modélisation d'une marche aléatoire entre les différentes pages du réseau.

Avant d'aller plus loin, expliquons pourquoi l'asymptotique de la suite (U_n) nous intéresse : étant donné que le singe avance au hasard, il va finir par arriver (avec une grande fréquence) sur des pages importantes (car de nombreux liens pointent vers elles). Aussi la position du singe sur la page x_i , après de nombreux clics, est-elle un bon indicateur de l'importance de cette page.

Le système *PageRank*

Toutefois, il se pose encore un problème : sur le réseau Internet (comme dans les réseaux routiers), il y a des culs-de-sac, *i.e.* des pages qui ne pointent vers aucune autre page. Outre la lassitude de notre singe, qui ne voit plus les images bouger, cela entraîne un défaut pour notre méthode car ces pages souvent futiles (elles n'ont aucune référence) nous bloquent et, donc, apparaissent arbitrairement importantes.

Pour éviter cet écueil, nous allons à chaque étape proposer à notre singe de poursuivre ses clics avec une certaine probabilité $c \in]0, 1[$ ou d'aller n'importe où sur la toile (même s'il n'y a pas de lien depuis la page sur laquelle on se trouve) avec la probabilité c .

Si nous essayons d'écrire une relation matricielle comme au paragraphe précédent, on trouve $U_{n+1} = GU_n$ où $G = cL + (1-c)J$ avec J la matrice dont tous les coefficients sont égaux à $\frac{1}{N}$ (N étant le nombre de pages du réseau).

G est encore une matrice stochastique comme combinaison convexe de deux matrices stochastiques, mais elle présente une autre propriété importante : elle est primitive car strictement positive (grâce à l'introduction de J).

Définition 1.56. Soit $M \in \mathcal{M}_n(\mathbb{R})$.

- ◊ M est dite positive (respectivement strictement positive) si tous ses coefficients sont positifs (respectivement strictement positifs).
- ◊ M est dite primitive s'il existe $k \in \mathbb{N}$ tel que M^k soit strictement positif.
- ◊ M est dite ergodique si elle est à la fois stochastique et primitive.

Prenons un petit exemple avant de revenir à notre matrice G .

EXEMPLE 1.57. La matrice $\begin{pmatrix} 0,5 & 0,5 \\ 0,25 & 0,75 \end{pmatrix}$ est ergodique, alors que $\begin{pmatrix} 0,5 & 0,5 \\ 0 & 1 \end{pmatrix}$ est stochastique mais non primitive.

La propriété d'ergodicité de G est peut-être difficile à saisir de prime abord, mais nous allons voir avec le théorème de Perron-Frobenius qu'elle s'avère essentielle pour assurer la convergence de la suite (U_n) .

Méthode

Algorithme pour déterminer le vecteur *PageRank* de *Google*

Pour obtenir le vecteur U qui, à chaque page, associe son importance sur le réseau, il suffit :

- ◇ de calculer la matrice G de *Google* ;
- ◇ de calculer récursivement U_n (on verra que cette suite converge vers U pour toute valeur initiale U_0) ;

Cet algorithme, qui s'appelle algorithme de *PageRank*, a assuré à *Google* sa pertinence et sa fiabilité.

1.2. Le théorème de Perron-Frobenius

Énoncé

Le théorème de Perron-Frobenius est un résultat assurant la convergence des suites vectorielles définies par une relation matricielle. La version que nous présentons est la plus courante et repose sur le caractère primitif de la matrice.

Théorème 1.58. *Pour toute matrice primitive A , il existe une valeur propre λ et un unique vecteur propre U associé à λ tels que :*

- ◇ pour toute valeur propre μ de A différente de λ , on ait $|\mu| < \lambda$;
- ◇ les composantes de U soient positives et de somme 1.

De plus, si $\lambda = 1$, on note $\phi_k(U_0)$ la somme des valeurs absolues des coefficients de $A^k U_0 - U$ avec U_0 un vecteur quelconque, alors $\phi_k(U_0) = O(\rho^k)$ avec ρ le plus grand module des valeurs propres de A différentes de λ .

Remarque. Si la matrice est ergodique, la valeur propre dominante (λ dans le théorème précédent) est égale à 1 et, donc, la suite $(\phi_n(U_0))$ converge vers 0, i.e. $(A^n U_0)$ converge vers U .

Il est essentiel de remarquer que ce résultat de convergence ne dépend pas du premier terme U_0 . Par conséquent, peu importe la position initiale du singe sur le réseau : il suffit qu'il se déplace sur le réseau à l'aide de la matrice G .

Convergence de l'algorithme *PageRank*

Nous pouvons donc appliquer le théorème de Perron-Frobenius à la matrice G qui est ergodique : il existe un vecteur propre U associé à la valeur propre 1 (qui est le vecteur du système *PageRank*). De plus, ce vecteur est la limite de la suite $(G^n U_0)_n$ qui converge exponentiellement vite, plus précisément de l'ordre de $(c^n)_n$. Cela a une conséquence pratique importante : en effet, pour faire fonctionner le moteur de recherche, il n'est pas nécessaire de chercher à calculer exactement U , mais il suffit d'en détenir une bonne approximation qui s'obtienne en seulement quelques itérations de la suite $(G^n U_0)_n$ pour un vecteur initial U_0 quelconque. Aussi, les ordinateurs de la compagnie *Google* ne calculent pas U mais simplement une valeur de la suite (U_n) pour un indice n assez grand. Cela est essentiel pour deux raisons :

- le moindre calcul avec G est très long ; n'oublions pas que la taille de la matrice G est le nombre de pages du réseau, et que chaque itération nécessite le carré de ce nombre en opérations arithmétiques ;

- la matrice G évolue avec le temps : le réseau n'est pas figé et la structure de graphe évolue en permanence (nouveau lien, pages retirées...); il convient donc de réactualiser G assez fréquemment.

REMARQUE – L'utilisation du théorème de Perron-Frobenius dans ce contexte permet de mettre en évidence le rôle essentiel des éléments propres. On peut en donner une autre écriture moins explicite en utilisant cette fois le théorème du point fixe à l'application $y \mapsto Gy$ qui est contractante de rapport c . Il convient de réaliser alors que cette inégalité de contraction n'est qu'une majoration des valeurs propres de G distinctes de 1.

1.3. Une généralisation à d'autres processus aléatoires

Nous avons vu que la marche aléatoire du singe sur le réseau s'interprétait avec une relation matricielle, et que l'étude asymptotique ne dépendait que de la matrice. Il est alors légitime de se demander si d'autres processus ne jouissent pas des mêmes propriétés. On découvre ainsi une large classe de processus aléatoires appelés chaînes de Markov.

Nous supposons dans cette partie que le lecteur a consulté le chapitre sur les probabilités.

Matrice de transition d'une chaîne

On cherche ici à étudier un phénomène aléatoire qui change d'état avec le temps. Pour simplifier, on considère que notre phénomène n'admet qu'un nombre **fini** d'états et que le temps est **discret** (*i.e.* les changements éventuels ont lieu au temps entier). Par exemple, regardons si une machine dans un atelier connaît ou non une panne le jour numéro n après sa mise en service- notre système admet deux états : en fonctionnement ou en panne.

Pour utiliser un peu de formalisme probabiliste, précisons les notations : notons X_n la variable aléatoire égale à l'état de notre système au temps n .

Définition 1.59.

◇ Une suite de variables aléatoires à valeur dans un ensemble fini E est appelée chaîne de Markov si la loi de X_{n+1} conditionnellement à $(X_k)_{k \leq n}$ est égale à la loi de X_{n+1} conditionnellement à X_n .

◇ Une chaîne de Markov est dite homogène si, pour tout $(x, y) \in E^2$ et tout $n \in \mathbb{N}$, $P(X_{n+1} = y | X_n = x)$ ne dépend pas de n .

◇ Une chaîne de Markov est dite irréductible si, pour tout $(x, y) \in E^2$, il existe $k \in \mathbb{N}$, $P(X_{n+k} = y | X_n = x) > 0$.

EXEMPLE 1.60. Par exemple, la position (X_n) de notre singe savant est une chaîne de Markov : le lien qu'il va choisir (au hasard) ne dépend pas des pages déjà visitées donc il y a indépendance de la position présente conditionnellement aux positions passées.

Remarque.

◇ La propriété de chaîne de Markov correspond à la description d'un phénomène temporel aléatoire avec indépendance du passé lointain sachant le passé immédiat.

◇ La propriété d'homogénéité traduit l'existence d'un mécanisme de transition indépendant de l'instant. C'est ce mécanisme que nous allons décrire par une matrice et qui sera l'objet de l'application du théorème de Perron-Frobenius.

Définition 1.61. La matrice de transition d'une chaîne de Markov homogène $(X_n)_{n \in \mathbb{N}}$ d'états $(x_i)_{i \leq N}$ est la matrice $M \in \mathcal{M}_N(\mathbb{R})$ définie par les coefficients

$$\forall (i, j) \in \{1, \dots, N\}^2, \quad m_{i,j} = P(X_1 = x_i | X_0 = x_j).$$

La loi de la variable X_n est le vecteur colonne U_n dont les coefficients sont les $(P(X_n = x_i))_{i \leq N}$.

Proposition 1.62. Soit $(X_n)_{n \in \mathbb{N}}$ une chaîne de Markov homogène de matrice de transition M . Alors, pour tout $n \in \mathbb{N}$, $U_{n+1} = MU_n$.

PREUVE. Ce résultat n'est que l'application de la formule des probabilités totales (voir le chapitre de probabilités de ce volume). En effet, puisque $(\{X_n = x_j\})_{j \leq N}$ forme un système complet d'événements, on a, pour tout $i \leq N$.

$$P(X_{n+1} = x_i) = \sum_{j=1}^N P(X_{n+1} = x_i | X_n = x_j) P(X_n = x_j),$$

d'où la relation matricielle annoncée. ■

Convergence en loi

Si l'on considère une chaîne de Markov homogène dont la matrice de transition est ergodique, alors on peut appliquer le théorème de Perron-Frobenius. Puisque la valeur propre dominante est 1, il existe un unique vecteur propre μ à coefficients positifs et dont la somme des coefficients est 1. Ce vecteur μ s'interprète donc naturellement comme une loi de probabilité telle que, si X_0 est de loi μ , alors μ est la loi de chacun des X_n pour tout $n \in \mathbb{N}$ (autrement dit, μ est invariante par la matrice de transition).

La seconde assertion du théorème de Frobenius nous assure que la loi de (X_n) « converge » vers μ . Cette notion de convergence s'appelle la convergence en loi. Cela traduit que, pour une chaîne de Markov homogène de matrice ergodique, un régime stationnaire se met en place rapidement (*i.e.* à vitesse exponentielle) et que le système va, à terme, être gouverné par la loi μ .

EXEMPLE 1.63. L'algorithme *PageRank* consiste donc à déterminer la loi *stationnaire* vers laquelle (U_n) va converger, pour pouvoir s'en servir comme indicateur d'importance des différentes pages du réseau.